Gesellschaft für Informatik e.V. (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into
- seminars
- proceedings
- dissertations
- thematics

current topics are dealt with from the vantage point of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure high quality contributions.

The volumes are published in German or English.

Information: http://www.gi.de/service/publikationen/lni/

ISSN 1617-5468
ISBN 978-3-88579-631-2

Open standards and interfaces as well as open source technologies play a central role in the current identity management landscape as well as in emerging future scenarios based on cloud computing for example. While there are already plenty of successful applications in which those techniques are used to guarantee the authenticity and integrity of entities, there are still many closely related areas which demand further research. The aim of the "Open Identity Summit 2014" is to link practical experiences and requirements with academic innovations. Focus areas of this event are research and applications in the area of Identity Management and Open Source with a special focus on Cloud Computing.

D. Hühnlein, H. Roßnagel (Hrsg.): Open Identity Summit 2014

237

GI-Edition

Lecture Notes in Informatics

Detlef Hühnlein, Heiko Roßnagel (Hrsg.)

Open Identity Summit 2014

**4.–6. November 2014
Stuttgart, Germany**

Proceedings

GI

Detlef Hühnlein, Heiko Roßnagel (Hrsg.)

Open Identity Summit 2014

04. - 06.11.2014
Stuttgart, Germany

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-237

ISBN 978-3-88579-631-2
ISSN 1617-5468

Volume Editors
Detlef Hühnlein
ecsec GmbH
Sudetenstr. 16, D-96247 Michelau, Germany
E-Mail: detlef.huehnlein@ecsec.de
Heiko Roßnagel
Fraunhofer IAO
Nobelstr. 12, D-70569 Stuttgart, Germany
E-Mail: heiko.rossnagel@iao.fraunhofer.de

printed by Köllen Druck+Verlag GmbH, Bonn

Chairs' Message

Welcome to the "Open Identity Summit 2014", which has been jointly organized by the Special Interest Groups BIOSIG within the German Computer Science Society (Gesellschaft für Informatik), the EU-funded FutureID Project, the Open eCard Project, the European Association for eIdentity and Security (EEMA), the SSEDIC2020 project, the TeleTrusT IT Security Association Germany, the organization OpenLimit, the SkIDentity Project, which aims at providing trustworthy identities for the cloud, and last but not least the Trusted Cloud Program supported by the German government. The chair furthermore wants to thank the ENX Association, the platinum sponsor of the conference.

The international program committee performed a scientific review process according to the LNI guidelines with at least five reviews per paper and accepted 47 % of the 19 submitted papers as full scientific papers.

Furthermore, the program committee has created a program including selected contributions of strong interest (further conference contributions) for the outlined scope of this conference.

We would like to thank all authors for their contributions and the numerous reviewers for their work in the program committee.

Stuttgart, 4th November, 2014

Detlef Hühnlein
ecsec GmbH

Heiko Roßnagel
Fraunhofer IAO

Chairs

Detlef Hühnlein
ecsec GmbH, Germany (detlef.huehnlein@ecsec.de)

Heiko Roßnagel
Fraunhofer IAO, Germany (heiko.rossnagel@iao.fraunhofer.de)

Program Committee

Hosts and Partners

- **ENX Association (www.enxo.com/)**

  Founded in 2000 the ENX Association, a legally-independent union of the companies and national associations Audi, BMW, Bosch, Continental, Daimler, DGA, Ford, Magna, PSA Peugeot Citroën, Renault, Volkswagen ANFAC (Spain), GALIA (France), OSD (Turkey), SMMT (UK) and VDA (Germany) supervises the performance of the certified service providers, operates central services of the ENX network and supports its providers whenever they have to solve problems efficiently.

  The association operates a communications network for the European automotive industry. It enables all partners to exchange data between companies and across borders in a uniform, harmonised way. The ENX network is an IP based network just like the Internet, however it is significantly more secure and powerful.

- **Open Limit (www.openlimit.com/)**

  OpenLimit SignCubes AG was founded in 2002 and is a wholly-owned subsidiary of the publicly traded OpenLimit Holding AG. OpenLimit offers a modular system of software components for generating and verifying qualified and advanced signatures, for electronic authentication and revision-safe long-term archiving of electronic documents. We link up these modules into made-to-measure software products that can be applied as client-, server- or integration-solutions – enhancing security, quality and speed of processes.

- **SSEDIC (http://www.ssedic2020.com/)**

  The objective of SSEDIC.2020 is to provide a platform for all the stakeholders of eID (electronic identity) to work together and collaborate. SSEDIC.2020 builds on the success of SSEDIC .

- **BIOSIG – Biometrics and Electronic Signatures (www.biosig.org)**

  The special interest group "Biometrics and Electronic Signatures" (BIOSIG) within GI e.V. is dedicated to the fundamentals, methods, techniques, processes and implementations used to guarantee the authenticity and integrity of entities.

- **CRYPTO – Applied Cryptology (fg-krypto.gi.de)**

  The special interest group "Applied Cryptology" (CRYPTO) within GI e.V. connects users and researchers in the area of cryptology, whereas the scope of activities comprises the design, analysis, implementation and practical application of cryptographic systems.

- **FutureID Project (www.futureid.eu)**

  The EU-funded FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infra-structure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

- **Open eCard Team (www.openecard.org)**

  The Open eCard Team is an open community, which aims at providing an open source and cross platform implementation of the eCard-API-Framework (BSI-TR-03112) and related international standards such as ISO/IEC 24727 and OASIS DSS through which arbitrary applications can utilize authentication and signatures with arbitrary smart cards.

- **European Association for eIdentity and Security (EEMA) – (www.eema.org)**

  For 25 years, EEMA has been Europe's leading independent, non-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

- **SkIDentity Project (www.skidentity.de)**

  The SkIDentity Project aims at facilitating the use of electronic identity cards (eID) within existing and emerging cloud computing infrastructures in order to provide trustworthy identities for the cloud.

- **TeleTrusT – IT Security Association Germany (www.teletrust.de)**

  TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives.

- **Trusted Cloud Program (www.trusted-cloud.de)**

  The Trusted Cloud Program is an initiative of the German Federal Ministry of Economics and Technology in which 38 companies and 26 academic institutions are collaborating in 14 projects in order to develop innovative, secure and legally valid technologies for trustworthy Cloud Computing.

Table of Contents

Open Identity Summit 2014 – Regular Research Papers

Open Identity Summit 2014 – Further Conference Contributions

SAML Privacy-Enhancing Profile

Moritz Horsch[1], Max Tuengerthal[2], Tobias Wich[2]

[1] Technische Universität Darmstadt, Hochschulstraße 10, 64289 Darmstadt
horsch@cdc.informatik.tu-darmstadt.de
[2] ecsec GmbH, Sudetenstraße 16, 96247 Michelau
{max.tuengerthal,tobias.wich}@ecsec.de

Abstract: We present the SAML Privacy-Enhancing (PE) profile which empowers users to take control of the authentication process and their personal data. Users have the full control of the application flow and get detailed information about the involved participants and the revealed attributes. This enables users to give informed consent for the authentication. The new profile builds on well-established standards and technologies. We use the common SAML Authentication Request and provide the additional information as extensions based on SAML Metadata.

1 Introduction

The Security Assertion Markup Language (SAML) is a widespread framework for exchanging authentication and authorization information between entities. SAML in particular takes place in single sign-on solutions through which users authenticate to a dedicated identity provider (IdP) to get access to multiple service providers (SP). The SAML Web Browser Single Sign-On (Web Browser SSO) profile [HCH$^+$05, Section 4.1] covers the scenario of users requesting services through a browser and getting redirected to an IdP for authentication. To provide means for more sophisticated authentication and transmission protocols the SAML Enhanced Client or Proxy (ECP) profile [HCH$^+$05, Section 4.2] describes an client application which is capable of directly contacting the IdP.

However, there is a gap between the SAML Web Browser SSO and the ECP profile. SAML Web Browser SSO is restricted to the browser's capabilities. Thus, authentication methods more sophisticated than username/password need a browser extension, which is hard to develop and to maintain for the wide variety of web browsers. SAML ECP does not match the general user flow in the Internet, because the client application needs to determine the corresponding IdP which is challenging for new and unknown services. Thus, it lacks of the common use case in which the user uses a web browser and an additional client application for strong and more sophisticated authentication. The technical guideline TR-03124 [BSI14] somewhat covers this use case by piggybacking the SAML Authentication Request on the local HTTP-based client activation mechanism. However, this is restricted to the infrastructure and interfaces of the German Identity Card. Our SAML profile provides a more universal solution.

Furthermore, SAML Web Browser SSO has serious privacy issues. For instance, the automatic redirection to the IdP lacks user consent and reveals information about users even if they abort the authentication later. SAML also does not provide detailed information for users about the SP and the IdP like terms of usage, which makes it hard for users to see which attributes get revealed and to whom. In comparison to the STORK project, which developed an extension to the SAML Authentication Request including among other things the specification of an assurance level and required attributes [AMHAJ$^+$11], our presented SAML profile provides means for client applications and a more sophisticated informed user consent.

We present the SAML Privacy-Enhancing (PE) profile which provides means for using browsers to support the common browsing habits of users and client applications for more sophisticated authentication methods. The profile empowers users to take control over the authentication process and their personal data and provide detailed information of the participants and the authentication to enable an informed user consent. Our presented SAML profile builds on the existing messages flows, protocols, bindings, and data structures of the SAML standard [CKPM05] and in particular the SAML Web Browser SSO and SAML ECP profile [HCH$^+$05], TR-03124-1 [BSI14], and the Holder-of-Key binding [KS10]. This enables an easy integration in existing SAML infrastructures.

The usage of an additional application which performs the authentication cause issues regarding secure bindings. A solution as described in the technical guideline TR-03124 for the German eID card has certain drawbacks and cannot be applied to any other credentials to date. We present a method to use our proposed SAML profile with the secure Holder-of-Key binding [KS10] which also provides privacy preserving properties.

The paper is organized as follows. We give a brief introduction to SAML in Section 2. In Section 3 we present the SAML PE profile and we provide more technical details in Section 4. In Section 5 we describe how a secure channel binding is realized and we conclude the paper in Section 6.

2 SAML

The Security Assertion Markup Language (SAML) [CKPM05] is a framework for exchanging authentication and authorization information between entities. It specifies the syntax and processing of assertions about a user issued by an IdP. SAML specifies multiple protocols and bindings for message transport, which are combined in SAML profiles. Messages and assertions are encoded in XML.

Protocols SAML protocols are used to exchange messages between the participants and are based on the common request-response paradigm. The most common used protocol is the Authentication Request Protocol [CKPM05, Section 3.4] which comprises an `AuthnRequest` to request an authentication process and a `Response` representing the authentication result including an assertion.

Bindings Bindings specify how SAML messages are transported between the participants. For instance, the SAML SOAP Binding [CHK$^+$05, Section 3.2] specifies how SAML messages are mapped into SOAP messages. The SAML PAOS Binding describes the *Reverse HTTP Binding for SOAP* in which HTTP requests are used to transmit SOAP responses and HTTP responses to transmit SOAP requests. Furthermore, there exists SAML bindings for Redirect, POST, Artifact, and URI [CHK$^+$05].

Profiles A SAML profile describes the application flow for a scenario and specifies the data structures, protocols, and bindings which are used within the profile. The SAML standard specifies five SAML profiles [HCH$^+$05]. In the following we provide a short description of the two major profiles, the Web Browser Single Sign-on (Web Browser SSO) profile and the Enhanced Client or Proxy (ECP) profile.

The SAML Web Browser SSO profile [HCH$^+$05, Section 4.1] specifies a scenario in which a user agent (UA) requests a service or resource by a SP and gets redirected to an IdP to perform the user authentication. The UA is usually a plain-vanilla web browser and is used by the user to access services provided by the SP. As illustrated in Figure 1, the Web Browser SSO profile comprises a UA (i.e., web browser), a SP, and an IdP. In the first step the UA requests a resource by the SP. The SP responds with a SAML `AuthnRequest` in Step 2 using the POST, Redirect, or Artifact binding [CHK$^+$05]. In Step 3 the UA forwards the `AuthnRequest` to the IdP and performs the user authentication. The result of the authentication is returned in a SAML `Response` in Step 4. In Step 5 either the POST or Artifact binding can be used by the UA to transmit the `Response` to the SP. Finally, in Step 6 the SP transmits the requested resource to the UA and the SAML protocol finishes.

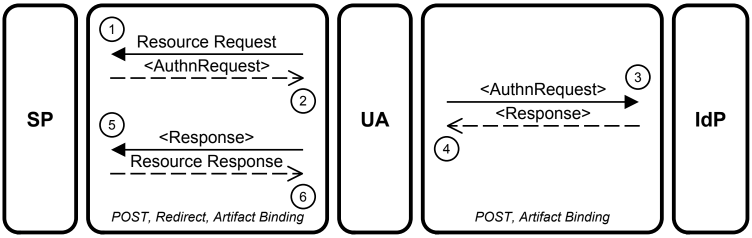


Figure 1: SAML Web Browser SSO profile.

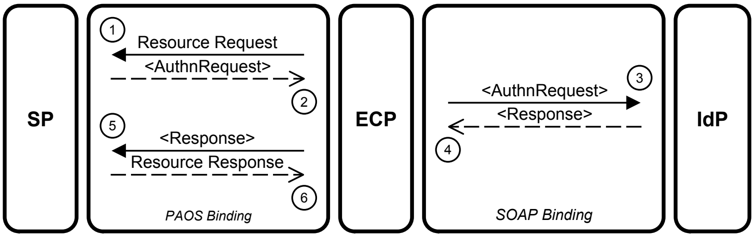


Figure 2: SAML ECP profile.

The SAML ECP [HCH+05, Section 4.2] profile is a single sign-on authentication profile and specifies a client application which is capable of directly determine and contact the user's IdP, without getting redirected by the SP. It is particularly useful for client-side and server-side applications with a fixed set of services. The ECP profile focuses on applications with enhanced functionality, for instance, supporting more sophisticated protocols and bindings like SOAP and PAOS. As illustrated in Figure 2, the ECP profile comprises an ECP application, a SP, and an IdP. The application flow starts with a service or resource request to the SP by the ECP using the PAOS binding. The SP responses with an SAML `AuthnRequest` in Step 2. In Step 3 the ECP determines the IdP and transmits the `AuthnRequest` using the SOAP binding to the IdP and performs the user authentication. The result of the authentication is returned in the SAML `Response` in Step 4. The ECP conveys the `Response` to the SP in Step 5. Finally, in Step 6 the SP transmits the requested resource to the ECP and the SAML protocol finishes.

3 SAML Privacy-Enhancing Profile

The SAML Privacy-Enhancing (PE) profile enables users to consume services through a web browser and use a client application for strong authentication. It provides a user-controlled data flow, which allows users to cancel the authentication process at any point in time. Furthermore, it provides detailed information about the participants and the revealed attributes to enable the user to give an informed consent for the authentication.

The profile is based on SAML Web Browser SSO and the profile defined in TR-03124-1. We extend the SAML `AuthnRequest` to include the additional information about the participants and the authentication (cf. Section 4). Most of this information (e.g., requested attributes and information about IdPs) is expressed using the standardized Metadata for SAML [CMPM05] and the SAML Metadata Extensions for Login and Discovery User Interface [Can12]. Our profile uses plain HTTP mechanisms rather than SOAP to simplify the integration in web applications and existing SAML libraries.

3.1 Setting

The setting comprises the following entities: (i) the Service Provider (SP), (ii) the User Agent (UA), (iii) the Enhanced Client Application (ECA), and, optionally, (iv) an Identity Provider (IdP). The SP provides a service like an online shop and requires a user authentication. The UA is running on the user platform and is usually a plain-vanilla web browser. The ECA is a universal application enabling authentication with various credentials and technologies. To be precise, it implements the user interaction, the authentication and transport protocols, the communication with credentials, and so forth. The ECA comprises a local HTTP-based interface which provides means to start authentication procedures or to fetch status information like supported application functionality. The assertion is optionally provided by an IdP, see below.

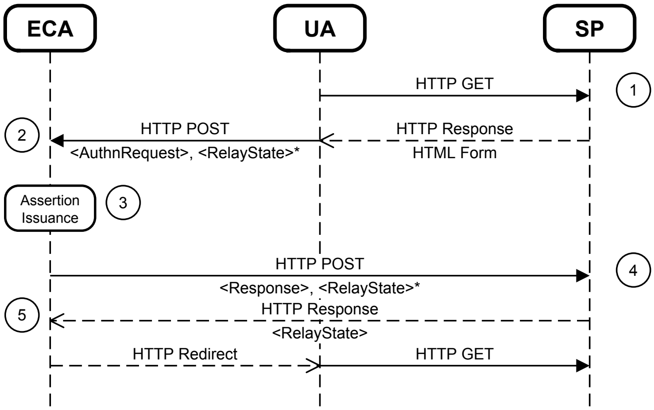


Figure 3: Protocol flow of the SAML PE profile.

3.2 Protocol Flow

The protocol flow of the PE profile comprises five steps and is illustrated in Figure 3. In the following we describe the steps in detail.

Step 1 – Service Request First, the user navigates its UA to a protected service or resource. The authentication process begins.

Step 2 – Issuance Request The SP returns a HTML form to the UA which includes the extended `AuthnRequest` and an optional `RelayState`[1] [CHK$^+$05, Section 3.5.3]. Both are forwarded to the ECA by submitting the HTML form via HTTP POST to the local HTTP-based interface[2].

The `AuthnRequest` represents the request from the SP to the IdP to issue an assertion about the user. It also includes detailed information of the participants and the authentication to enable the user to give an informed consent. The `RelayState` references to state information stored at the SP to enable a redirect to the requested service or resources after the authentication.

Step 3 – User Consent and Assertion Issuance The ECA then presents all information about the authentication and involved participants to the user and prompts him or her to select an authentication method and/or an IdP. The ECA obtains this information from the proposed SAML `AuthnRequest` extension (cf. Section 4). Based on the displayed information the user is able to give an informed consent for the authentication.

[1] Please note that the `RelayState` might cause severe security issues, therefore we recommend to protect it with confidentiality and integrity protection [HPM05, Section 6.4.6].

[2] `http://127.0.0.1:24727/eID-Client`

Subsequently, the ECA fetches the assertion, i.e., SAML `Response`. Depending on the authentication method this can be done, e.g., by performing the Authentication Request Protocol [CKPM05, Section 3.4] with an IdP or some local assertion generation based on attributed-based credentials. The used protocol and authentication method is out of scope of the PE profile, so that a wide variety of methods can be supported and new methods can be added easily.

Step 4 – Assertion Delivery The ECA conveys the `Response` together with the `RelayState`, if received in Step 2, to the SP. The delivery of the assertion by the ECA is necessary to provide means for secure bindings (cf. Section 5), because the channel specific parameters can in general not be securely transferred from the ECA to the UA.

Step 5 – RelayState Processing In response to the successful verification of the assertion the SP returns a `RelayState` to the ECA. This value is either the same as the one sent in the previous step, or a preconfigured value from the SP in case no `RelayState` was given. The process continues only after a successful validation of the RelayState's integrity protection.

Finally, the ECA responds to the request from the UA in Step 2 with an HTTP redirect to the received `RelayState`. The UA follows the redirect and gets access to the protected resource.

4 User Consent

The user consent, as described in the Section 3.2, Step 3, is the core of our SAML PE profile. Before any personal information is revealed or any communication with further services takes place the user gets detailed information and is able to give an informed consent for the authentication. The user chooses (i) the IdP he or she would like to perform the authentication with, (ii) which user credential (e.g., hardware token, software certificate, username/password) he or she would like to use (with the chosen IdP) for authentication, and (iii) the attributes that will be disclosed to the SP; or (iv) to abort the authentication procedure.

In the following sections we describe how the information about the authentication process is transmitted to the client and encoded in the message SAML Authentication Request.

4.1 Information about the Service Provider

The information of the SP is defined by a `SPSSODescriptor` element (cf. Listing 1). The requested attributes are part of a `AttributeConsumingService` element and defined as a list of `RequestedAttribute` elements. To display this information in a user-friendly way, we include an `UIInfo` element as defined in [Can12]. The information is used to display (localized) information (e.g., name and description) about the SP and in particular about the requested attributes to the user. Each requested attribute is represented by a RequestedAttributeInfo element (cf. Appendix A), which in particularly contains at least one Purpose element in which the SP must give a reason why this attribute is necessary for the provided service. Additionally, a URL for more information may be provided in the InformationURL element. Optionally, the index of the AttributeConsumingService may be given, if different services have different purposes for the same attributes. Finally, the SPSSODescriptor element includes at least one AssertionConsumerService element which defines different consumer services at the SP. For example, the SP in Listing 1 accepts SAML Bearer assertions.

```
<md:SPSSODescriptor
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:Extensions>
    <mdui:UIInfo>
      <mdui:DisplayName xml:lang="en">SP1</mdui:DisplayName>
      <mdui:Description xml:lang="en">Description.</mdui:Description>
      <pe:RequestedAttributeInfo AttributeName="urn:oid:2.5.4.42">
        <pe:Purpose xml:lang="en">To call you.</pe:Purpose>
      </pe:RequestedAttributeInfo>
      <pe:RequestedAttributeInfo AttributeName="urn:oid:2.5.4.41">
        <pe:Purpose xml:lang="en">Enhanced user experience.</pe:Purpose>
      </pe:RequestedAttributeInfo>
    </mdui:UIInfo>
  </md:Extensions>
  <md:AssertionConsumerService
    index="0" isDefault="true" Location="https://sp1.example.com/saml"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
  </md:AssertionConsumerService>
  <md:AttributeConsumingService index="0" isDefault="true">
    <md:ServiceName xml:lang="en">SP1</md:ServiceName>
    <md:RequestedAttribute
      Name="urn:oid:2.5.4.42" isRequired="true" FriendlyName="Forename"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    </md:RequestedAttribute>
    <md:RequestedAttribute
      Name="urn:oid:2.5.4.41" isRequired="false" FriendlyName="Name"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    </md:RequestedAttribute>
  </md:AttributeConsumingService>
</md:SPSSODescriptor>
```

Listing 1: Metadata of a SP. Namespaces: md = urn:oasis:names:tc:SAML:2.0:metadata is defined in [CMPM05], mdui = urn:oasis:names:tc:SAML:metadata:ui is defined in [Can12], samlp = urn:oasis:names:tc:SAML:2.0:protocol is defined in [CKPM05], and pe = urn:oasis:names:tc:SAML:profile:privacy is the namespace for the SAML PE profile.

4.2 Information about the Identity Providers

The information of an IdP is defined by a IDPSSODescriptor element (cf. Listing 2). To provide detailed information about the IdP to the user the IDPSSODescriptor element contains, in its extensions element, a `UIInfo` element. It includes information such as the name and a description of the IdP. One can imagine of including further details like terms of usage, data privacy statement, and so forth.

The `IDPSSODescriptor` element comprises at least one `SingleSignOnService` element, which is used to define different assertion issuance services at the IdP. The IdP in Listing 2 for instance issues SAML Bearer assertions.

Existing SAML metadata definitions do not allow to describe possible authentication options at the IdP, which allows the user to authentication with different credentials. However, this information is crucial for the user to make an informed decision (i.e., to decide which user credential to use at which IdP). To provide this information, we

```
<md:IDPSSODescriptor
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:Extensions>
    <mdui:UIInfo>
      <mdui:DisplayName xml:lang="en">IdP1</mdui:DisplayName>
      <mdui:Description xml:lang="en">Description.</mdui:Description>
      <mdui:PrivacyStatementURL xml:lang="en">
        https://idp1.example.com/privstat.html
      </mdui:PrivacyStatementURL>
    </mdui:UIInfo>
  </md:Extensions>
  <md:SingleSignOnService
    Location="https://idp1.example.com/saml/remoteauth"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
    <pe:AuthenticationOptions>
      <pe:AuthenticationOption
        index="0" Binding="urn:oid:1.3.162.15480.3.0.25">
        <pe:Accepts>
          <pe:CredentialList>
            <pe:CredentialEntry credentialType="eID-GOV-DE-v1.0"/>
            <pe:CredentialEntry credentialType="eID-gov-GB-v1"/>
          </pe:CredentialList>
        </pe:Accepts>
      </pe:AuthenticationOption>
      <pe:AuthenticationOption index="1"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
        <pe:Accepts>
          <samlp:Scoping>
            <samlp:IDPList>
              <samlp:IDPEntry ProviderID="http://idp2.example.com"/>
            </samlp:IDPList>
          </samlp:Scoping>
        </pe:Accepts>
      </pe:AuthenticationOption>
    </pe:AuthenticationOptions>
  </md:SingleSignOnService>
</md:IDPSSODescriptor>
```

Listing 2: Metadata of an IdP. See Listing 1 for namespace definitions.

define the new element `AuthenticationOptions` (cf. Appendix B), to be used in `SingleSignOnService`.

Every authentication option has an attribute `Binding` which defines the protocol of the authentication (e.g., TLS with X.509 client certificates or providing a SAML Bearer assertion from another IdP) and a list of accepted credential types (`CredentialEntry`) and/or IdPs (`IDPEntry`). Accepted IdPs are listed using the `Scoping` element.[3] The ECA must be able to obtain metadata for these IdPs as well (see Section 4.3). Accepted credentials are listed using the `CredentialList` element.

For example, the IdP in Listing 2 provides two authentication options: (i) Users may authenticate themselves using TLS with X.509 client certificates (provided by smart cards of different types) or (ii) they may authenticate themselves by presenting a SAML Bearer assertion issued by another IdP.

4.3 The SAML `AuthnRequest`

We extend the SAML `AuthnRequest` to provide the user with detailed information about the authentication. This information is provided as additional metadata.

The information, i.e. the metadata, of the SP is included by using an `EntityDescriptor` element. The `entityID` attribute of this element matches the `Issuer` of the request. The `EntityDescriptor` element contains the `SPSSODescriptor` element as described in Section 4.1.

The metadata of the IdP is included in the same way. The example in Listing 3 includes two additional `EntityDescriptor` elements which includes an `IDPSSODescriptor` element providing information about the IdPs.

Finally, the `Scoping` element is contained in the authentication request which contains the list of IdPs that are accepted by the SP. Please note that the SP might not accept assertions from all IdPs. However, the `AuthnRequest` must contain the metadata of all participants which might be involved in the authentication procedure. In the example in Listing 3 the SP only accepts assertions from the IdP 1. However, IdP 1 accepts assertions from IdP 2, thus, the metadata of IdP 2 must also be included in `AuthnRequest`. For privacy reasons it is very important that the SP resolves the transitive trust relation of the IdPs and provide all necessary metadata directly in the `AuthnRequest`.

```
<samlp:AuthnRequest
    IssueInstant="2014-04-22T12:00:00Z" Version="2.0"
    ID="b07b804c-7c29-ea16-7300-4f3d6f7928ad">
  <saml:Issuer>https://sp1.example.com/</saml:Issuer>
  <samlp:Extensions>
    <md:EntityDescriptor entityID="https://sp1.example.com/">
      <!-- Metadata of service provider 1 -->
    </md:EntityDescriptor>
    <md:EntityDescriptor entityID="http://idp1.example.com/">
```

[3] We note that the `Scoping` element is defined in [CKPM05] and used in the `AuthnRequest` to specify accepted IdPs.

```
      <!-- Metadata of identity provider 1 -->
    </md:EntityDescriptor>
    <md:EntityDescriptor entityID="http://idp2.example.com/">
      <!-- Metadata of identity provider 2 -->
    </md:EntityDescriptor>
  </samlp:Extensions>
  <samlp:Scoping>
    <samlp:IDPList>
      <samlp:IDPEntry ProviderID="http://idp1.example.com/"/>
    </samlp:IDPList>
  </samlp:Scoping>
</samlp:AuthnRequest>
```

Listing 3: A SAML AuthnRequest for the SAML PE profile. See Listing 1 for namespace definitions.

One can argue that the additional metadata of the SP and IdPs cause a lot of overhead. The amount of data can be reduced if the metadata is not included directly, but linked to a file stored at each IdP. However, then the ECA needs to fetch the metadata from each IdP which rise privacy issues.

5 Channel Binding

The commonly used SAML Web Browser SSO profile is susceptible to theft of the Bearer Token [HPM05]. In detail, if adversaries are able to steal the authentication assertion they can impersonate the user. To overcome this problem an assertion is bound to the service request as specified in the Holder-of-Key (HoK) profile for SAML. The user's web browser establishes a TLS [DR08] channel using a client certificate to the SP for requesting a resource. The browser uses the same certificate for the communication with the IdP to perform the user authentication. The IdP includes a reference of the certificate into the assertion. Thus, only the holder of the private key associated with the certificate is able to use the assertion at the SP for authentication. If an adversary steals the assertion, she cannot use it because she does not possess the required private key.

One of the key pillars is that the browser uses the same certificate for the TLS channel to the SP and to the IdP. In our scenario we face the challenge that we have two different applications, the browser, which requests the resource from the SP, and the ECA, which performs the user authentication and communicates with the IdP. To enable a channel binding as described in the HoK profile for SAML, we must use the same certificate in both applications and both TLS channels, respectively.

The simplest way would be to share the same key store for both applications. However, to provide enhanced privacy, we prefer ephemeral certificates which have a very short lifetime and are only used with a single SP. The certificates are self-signed and created on-demand. The idea is that the ECA creates ephemeral certificates for each SP and makes them available to the browser for the certificate-based TLS authentication.

We propose to use a PKCS#11 [RSA97] module for web browsers, which allows the ECA to act as a cryptographic device which provides tokens to the browser, which in turn can be use for the certificate-based TLS authentication. In essence, when the browser establishes the TLS channel to the SP it queries all PKCS#11 modules for available tokens. The ECA application creates an ephemeral certificate and returns it to the browser. The same certificate is then used by the ECA for the TLS channel to the IdP.

6 Conclusion

We presented the SAML Privacy-Enhancing profile which supports common service usage through the web browser as well as local client applications to provide means for strong authentication. The profile is based on the existing SAML standard and extends the Authentication Request Protocol. This allows for an easy integration in existing SAML infrastructures. It provides detailed information for the user to give informed consent for the authentication. It also tackles privacy issues related to SAML by giving the user the control of the application flow. Furthermore, it supports secure channel binding to prevent Man-In-The-Middle attacks between the ECA and the SP.

A RequestedAttributeInfo

```
<element name="RequestedAttributeInfo">
  <complexType>
    <sequence>
      <element name="Purpose" type="md:localizedNameType"
               maxOccurs="unbounded" />
      <element name="InformationURL" type="md:localizedURIType"
               minOccurs="0" maxOccurs="unbounded" />
    </sequence>
    <attribute name="AttributeName" type="string" use="required" />
    <attribute name="AttributeConsumingServiceIndex"
               type="unsignedShort" />
  </complexType>
</element>
```

B AuthenticationOptions

```
<element name="AuthenticationOptions">
  <complexType>
    <sequence>
      <element name="AuthenticationOption" maxOccurs="unbounded"
               type="pe:AuthenticationOptionType" />
    </sequence>
  </complexType>
</element>
<complexType name="AuthenticationOptionType">
  <sequence>
    <element name="Accepts" type="pe:AcceptsType" />
  </sequence>
  <attribute name="index" type="unsignedShort" use="required" />
  <attribute name="isDefault" type="boolean" use="optional" />
  <attribute name="Binding" type="anyURI" use="required" />
</complexType>
<complexType name="AcceptsType">
  <choice>
    <element ref="samlp:Scoping" />
    <element name="CredentialList" type="pe:CredentialListType" />
  </choice>
</complexType>
<complexType name="CredentialListType">
  <sequence>
    <element name="CredentialEntry" type="pe:CredentialEntryType"
             maxOccurs="unbounded" />
  </sequence>
</complexType>
<complexType name="CredentialEntryType">
  <attribute name="CredentialType" type="anyURI" use="required" />
</complexType>
```

References

[AMHAJ^{+}11] Joaquín Alcalde-Moraño, Jorge López Hernández-Ardieta, Adrian Johnston, Daniel Martinez, Bernd Zwattendorfer, Marc Stern, and John Heppe. D5.8.3b Interface Specification, Nov 2011.

[BSI14] Technical Guideline TR-03124-1 eID-Client – Part1: Specifications. Federal Office for Information Security, Version 1.1, 2014.

[Can12] Scott Cantor. SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0. OASIS Standard, Apr 2012.

[CHK^{+}05] Scott Cantor, Frederick Hirsch, John Kemp, Rob Philpott, and Eve Maler. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, Mar 2005.

[CKPM05] Scott Cantor, John Kemp, Rob Philpott, and Eve Maler. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, Mar 2005.

[CMPM05] Scott Cantor, Jahan Moreh, Rob Philpott, and Eve Maler. Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, Mar 2005.

[DR08] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), Aug 2008. Updated by RFCs 5746, 5878, 6176.

[HCH^{+}05] John Hughes, Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra, Rob Philpott, and Eve Maler. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, Mar 2005.

[HPM05] Frederick Hirsch, Rob Philpott, and Eve Maler. Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, Mar 2005.

[KS10] Nate Klingenstein and Tom Scavo. SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0. OASIS Standard, Aug 2010.

[RSA97] RSA Laboratories. PKCS #11: Cryptographic Token Interface Standard, Apr 1997.

eIDAS as guideline for the development of a pan European eID framework in FutureID

Colette Cuijpers, Jessica Schroers

ICIS/ICRI
Radboud University/KU Leuven
Mailbox 47, P.O. Box 9010
6500 GL NIJMEGEN
cuijpers@uvt.nl
Jessica.Schroers@law.kuleuven.be

Abstract: This paper addresses the Regulation on Electronic transactions in the internal market: electronic identification and trust services (eIDAS) and analyses this regulatory framework in relation to the pan European eID infrastructure being developed in the FutureID project. The aim of this paper is to identify if eIDAS sets forward any legal requirements that need to be implemented in the FutureID infrastructure. Even though the focus of this paper is on the development of the FutureID infrastructure, the description of eIDAS and the analysis of its main requirements for technical developers are in general relevant to the development of online identification and authentication schemes.

1. Introduction

With the possibility to use the Internet for an abundance of services, between all kinds of different actors - consumers, businesses and government - there is a current need for reliable online identity authentication. Most online service providers use registrations and then username/password systems for their identity management. Such systems are bothersome for the users since they have to remember a lot of different passwords. Moreover, such systems are not very reliable for service providers.

Solutions for these problems can be found in a system of federated identity management, defined by Smedinghoff as an approach: “(…) where an enterprise engages in online transactions in reliance on identity credentials issued by any one of several third parties, and individuals can use the same identity credential to engage in transactions with multiple organizations.” In simple terminology; a system of federated identity management makes it possible to answer the questions: “Who are you?” and “How can you prove it?" [Sm12]. The existing EU identity management landscape mainly consists of private initiatives on the one hand (e.g. Liberty Alliance Project/Kantara, OpenID), with the most familiar identification mechanism probably being log in with Facebook, Twitter and Google+ accounts. On the other hand, there are national public electronic identity schemes, which are often considered to be more reliable and trustworthy. Examples are the German nPA, the Austrian Citizen Card, the Belgian eID and the Dutch DigiD. These national systems are commonly used for national e-government services. There also exist public/private partnerships, mostly between banks and the government, whereby the government accepts the private identity means for their e-government services. This system is mostly used in the Nordic countries [St09]. Besides existing eIDs there is a lot of research on how to develop more trustworthy eIDs. Mention can for example be made of biometric authenticated transactions in eBanking and eBusiness, which is promoted by both the European Payment Council (EPC) and the European Banking Union (EBU) [Bu14].

In view of internationalisation - one of the characteristics of the online environment - electronic authentication services preferably are not confined to national borders. As the examples above illustrate, in a lot of EU Member States national eID systems are (being) developed, based on the use of eID cards.[1] However, the legal international and European standardization[2] of citizen cards lags behind in the early deployments of eID systems in Europe, such as in Germany and Belgium, leading to a very diverse landscape of different eID cards for which an infrastructure is needed that supports all these cards across Europe. Different large scale EU funded projects aim to realize such infrastructure. In this respect mention can be made of projects such as: Stork, Stork 2.0 and FutureID.[3]

Besides all kinds of complexities and requirements regarding the technical development of the infrastructure, one other important design requirement concerns compatibility with existing legislation. In this paper we zoom in on a very recent legislative accomplishment, the Regulation on Electronic transactions in the internal market: electronic identification and trust services (referred to as eIDAS).[4] Before addressing eIDAS in section 3, we will first in section 2 provide a brief introduction into the mentioned projects, and explain why we focus on the FutureID project. In section 4 we will analyse whether eIDAS provides requirements that need to be implemented in the FutureID infrastructure. The aim of this paper is to provide the technical developers some guidelines regarding these requirements. Even though this paper focusses on the development of the FutureID infrastructure, the description of eIDAS and the analysis of

[1] Part III of the Stork D2.2 report provides country reports concerning eID systems in the Member States.

[2] CEN TS 15480 and ISO/IEC 24727.

[3] Available 12 May 2014 at www.eid-stork.eu/; www.eid-**stork**2.eu/; www.futureid.eu/

[4] Official Journal of the European Union, L 257/73, 28.8.2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_257_R_0002&from=EN, available 10 September 2014.

its main requirements for technical developers are in general relevant to the development of online identification and authentication schemes.

2. EU eID projects

2.1 Brief Introduction

At the European level several projects are being carried out to develop a pan-European eID interoperability infrastructure.[5] While all these projects have a different focus or application domain, the common denominator is that these projects function as "Pillars for the development of interoperability of cross-border eID and trust. Identifying and using appropriate mechanisms to develop and engage "communities" – citizens and SMEs in particular - in promoting the use and uptake of eID and trust services".[6] The three main projects concerning the development of a cross-border infrastructure are Stork, Stork 2.0 and FutureID. Within these projects reference is made to a fourth project in which the concept of Attribute-Based Credentials is explored: ABC4Trust.[7] Attribute-based Credentials allow in a scenario of authentication to reveal only the minimal information required (e.g. this person is over 18), without giving away full identity information (e.g. this person is born on 19-04-1972). These credentials thus facilitate the implementation of a trustworthy and at the same time privacy-protecting digital identity management system.[8]

The project STORK[9] (Secure IdenTity acrOss boRders linked) was finished in 2012. The results of the project showed that it is possible to use national eIDs in cross border use cases by designing a system with two possibilities: either using the middleware so the user can communicate directly to the foreign system or using a Pan European Proxy Service (PEPS) which acts as a single gateway and intermediary for foreign eIDs towards domestic Service providers [Wp14]. STORK 2.0 follows up on STORK and uses the system in additional pilots, including further also representation and mandates.[10]

While the eIDAS Regulation most likely has been written with the results of the STORK project in mind, we will focus our analysis on the FutureID project, in which we are

[5] Without the aim of being exhaustive mention can be made of the following projects: STORK (https://www.eid-stork.eu/), STORK 2.0 (https://www.eid-stork2.eu/), SPOCS (http://www.eu-spocs.eu/index.php), PEPPOL (http://www.peppol.eu/), eCodex (http://www.e-codex.eu/home.html), epSOS(http://www.epsos.eu/).

[6] http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond

[7] https://abc4trust.eu/

[8] Available 12 May 2014 at https://abc4trust.eu/index.php/home/fact-sheet

[9] Available 12 May 2014 at www.eid-stork.eu

[10] Available 12 May 2014 at https://www.eid-stork2.eu/

involved as legal researchers. FutureID builds upon the findings in STORK and STORK 2.0 while also including the implementation of Attribute-Based credentials. Roßnagel et al. describe the project as: “The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims [Ro13]”. For users the interesting aspect of the project is that an eID is developed that can be used on ordinary desktop PCs, tablets and modern smart phones. From the perspective of service providers the advantage must come from an easy integration of existing services with the FutureID infrastructure. This will offer an effortless mechanism to benefit from strong security offered by eIDs without requiring service providers to make substantial investments. The idea is to offer the eID technology as a substitute for less secure alternatives currently in use such as username/password based systems. A third perspective described by Roßnagel et al. concerns existing and emerging trust service providers and card issuers “for which FutureID will provide an integrating framework, which eases using their authentication and signature related products across Europe and beyond.”

2.2 Scope

As described above, FutureID concerns an infrastructure integrating and linking different technologies, different (trust) service providers and different users to facilitate cross border online identification and authentication, and make the use of electronic signatures easier in the form of a common eSignature framework that is capable to process digital signature related tasks, like signature creation and verification, with which different existing formats of advanced electronic signatures can be used [LR13]. In this paper we refer to the FutureID infrastructure, meaning the components being developed and offered within the scope of the FutureID project, while realising that a complete eID architecture consists of more, e.g. the actual provision of identification and trust services in the strict sense of the eIDAS Regulation. We consider the FutureID project merely to offer the technical components that together form the infrastructure necessary for online authentication and electronic signatures. As such, FutureID is not an entity or legal person capable to provide e.g. qualified signatures or certificates. Therefore, the establishment and provision of trust services such as qualified signatures and certificates falls outside the scope of the development of the FutureID infrastructure, being the focus of this paper. This means that the eIDAS requirements pertaining such services, signatures and certificates, will only be dealt with considering the infrastructure provision of the eSignature service.[11]

3. eIDAS

3.1 Background

The European Commission recognized the problem of not having a “comprehensive EU cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions that encompasses electronic identification and trust services”.[12] In this respect, its Digital Agenda established an action on mutual recognition of electronic identification to provide a comprehensive and predictable legal framework in view of boosting user empowerment, convenience and trust in the digital world.[13] Providing such a legal framework is a necessary precondition to achieve modernization in public administration, mentioned in the European Commission’s ‘Annual Growth Survey 2013’ as “one of the five priorities for the Member States in the next 12-18 months (….). To underpin the digital transition in public services and to ensure they are available to all Europeans regardless of their place of residence, the Commission envisages deploying and rolling out digital services in key areas of public interest” [Ec12].

The revision of the eSignature Directive (1999/93/EC) started on the 4th of June 2012 with a proposal of the European Commission for a Regulation on **e**lectronic **ID**entification and **A**uthentication **S**ervices (eIDAS). In February 2014 the representatives of the European Parliament (MEP), the Commission and the Council reached a political agreement regarding eIDAS.[14] The proposed Regulation was adopted by the MEP with 534 votes in favor, 73 against and 7 abstentions, on the 3rd of April 2014.[15] The Regulation has been adopted by the Council on the 23rd of July 2014. It is officially published in the OJ on the 28th of August 2014.[16] The eSignature Directive will be repealed with effect from July 1, 2016, which is also the date from when the

[11] E.g. we will not address the annexes I – IV of the Regulation concerning requirements for qualified certificates for electronic signatures, seals and website authentication, and requirements for qualified signature creation devices.

[12] Wording taken from the explanatory memorandum of eIDAS, available 12 May 2014 at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0238.

[13] See action 8 (revision of the eSignature Directive) in combination with action 83 (mutual recognition of electronic identification), available 12 May 2014 at http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-8-revision-esignature-directive

[14] Available 12 May 2014 at http://europa.eu/rapid/press-release_MEMO-14-151_en.htm

[15] Available 12 May 2014 at http://www.europarl.europa.eu/pdfs/news/expert/infopress/20140403IPR41931/20140403IPR41931_en.pdf

[16] Official Journal of the European Union, L 257/73, 28.8.2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_257_R_0002&from=EN

Regulation shall apply.[17] In order to make the transition smooth, some transitional measures are established. For example, qualified certificates issued under the eSignature Directive will be considered as qualified certificates until they expire.[18] A certification service provider issuing qualified certificates has to submit a conformity assessment report and shall then also be considered as qualified trust service provider under the Regulation.[19]

3.2 Main problems addressed by eIDAS

Derived from the key actions in the Digital Agenda mentioned above, the Regulation wants to address two problems. The first is that citizens can't use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes are not recognized in other Member States. This makes it difficult for all cross-border online services for which a higher level of trusted identification and authentication is necessary in order to be used, like for example cross-border healthcare or online public procurement.

The second problem that the Regulation will address is the diverging legal validity of trust services. Trust services are electronic services *"which consist of:*

> *(a)* *The creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to these services, or*
>
> *(b)* *The creation, verification and validation of certificates for website authentication; or*
>
> (c) *The preservation of electronic signatures, seals or certificates related to these services."*[20]

One of the points of criticism on the eSignature Directive was that it only focuses on electronic signatures and leaves out other important trust services. This criticism has been taken up in the Regulation and it provides now also a framework for electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

3.3 Approach of the Regulation regarding the problem of electronic identity

The Regulation does not try to introduce a common European electronic identification system. This would be problematic since identification of citizens is a core national

[17] Art. 52 eIDAS.
[18] Art. 51 (2) eIDAS.
[19] Art. 51 (3) (4) eIDAS.
[20] Art. 3 (16) eIDAS.

sovereignty. Instead, it provides for the possibility of cross-border use and mutual recognition of existing systems of the Member States by giving them the option to notify their electronic identification scheme to the Commission. The notification is only possible if the scheme fulfils certain criteria and is not obligatory for the Member States.[21] Member States are obliged to accept notified identification means of others if their own online public services can be accessed by electronic identification means.[22] They can start joining the system from July 1, 2015.[23] In section 3.5 we will discuss the liability regime regarding notified identification means.

The obstacle in mutual recognition is that not all Member States identification means have the same security levels. Member States, which have more secure means for accessing their online service, don't want to accept less secure means of other Member States. To enhance the trust of the Member States in each other's notified schemes the Regulation provides for 3 'Identity assurance levels'. These will be addressed in section 4.3.

3.4 Approach of the Regulation regarding Trust Services

The Regulation now provides for a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and qualified certificates services for website authentication. This is a closed list of trust services, but Member States remain free to recognize at a national level other types of trust services as qualified and maintain or introduce national provisions to non-harmonized trust services.[24]

The non-discrimination rule of the Directive applies in the Regulation also to the mentioned trust services (except the qualified certificates for website authentication), which means that those trust services can be used as evidence in legal proceedings.[25] But it is still up to national law to define the legal effect of trust services, except where the Regulation states the effect.[26] The Regulation permits for trust service providers complying with the Regulation to circulate their products freely in the internal market, but also includes liability of trust service providers, which will be discussed in the next section. Member States will establish trusted lists with information on the qualified trust

[21] Art.7 and 9 and recital (13) eIDAS.

[22] Art. 6 eIDAS.

[23] Committees Committee on Industry, Research and Energy, Plenary sessions [03-04-2014 - 13:36] available 12 May 2014 at http://www.europarl.europa.eu/pdfs/news/expert/infopress/20140403IPR41931/20140403IPR41931_en.pdf

[24] Recitals (25) and (24) eIDAS.

[25] Recital (22), art. 25, art. 35, art. 41, art. 43, art. 46 eIDAS.

[26] Recital (22)

service providers.[27] If a trust service provider is on such list it may use the EU trust mark.[28] Qualified trust service providers will be supervised by a designated national supervisory body, which will also take action if non-qualified trust service providers allegedly do not meet the requirements of the Regulation.[29] Section 3.6 will elaborate on the extended supervision in the Regulation compared to the Directive.

3.5 Approach of the Regulation regarding Liability

One of the crucial issues of eIDAS concerns the allocation of liability.[30] Liability for trust services is rather straightforward. Art. 13 states that trust service providers are liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. The intention or negligence of a qualified trust service provider shall be presumed unless a qualified trust service provider proves otherwise. The burden of proof regarding a non-qualified trust service provider lies with the claimant.

More interesting and questionable is the liability provision of Art. 11 eIDAS. Besides strict liabilities for the party issuing electronic identification means and the party operating the authentication procedure, strict liabilities also pertain to notifying Member States.[31] These Member States are liable for damage caused intentionally or negligently to any natural or legal person when the availability of online authentication is not ensured, or when it is not ensured that the person identification data uniquely represent the person in question. This only relates to cross border transactions in which it must be ensured that electronic identification means is attributed "in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8".[32] The liability of the notifying state has raised several critiques [DV12] [Vo13]. It is questioned whether the Member States will take responsibility for other parties than the State itself to provide online identification and authentication services. This does not conform to the market approach that is expressed in Recital 13 of eIDAS: "Member States should remain free to use or introduce means, for electronic identification purposes, for accessing online services. They should also be able to decide whether to involve the private sector in the provision of these means". It could even lead to Member States abstaining to notify electronic identification schemes, blocking the possibility of mutual recognition of such systems. Dumortier and Vandezande from a different perspective point to barriers for private

[27] Art. 22 eIDAS.
[28] Art. 23 eIDAS.
[29] Art. 17 eIDAS.
[30] Recitals (18) and (37). Art. 11 and 13 eIDAS.
[31] Art. 11 eIDAS.
[32] Assurance levels are discussed in section 4.3.

parties to enter the online identification market, as service providers may have to make substantial investments in order to comply with the liability requirements [DV12].

3.6 Approach of the Regulation regarding supervision

The eSignature Directive referred to supervision only in one article stating that each Member State shall ensure the establishment of a supervision system for qualified certification service providers[33], which resulted in a variety of supervision schemes in different Member States.[34] In response to this the Regulation contains much more extensive supervision provisions, however, supervision in eIDAS is only specified for trust services. The supervision remains at the national level, so there is no European supervisory body, but Member States designate a supervisory body in their territory with the necessary powers and adequate resources.[35] These supervisory bodies are considered to cooperate with each other and only in case of security breach with a cross border dimension ENISA will be informed.[36] In general is it the role of the supervisory body to ensure that the requirements of the Regulation are followed by supervising qualified trust service providers and taking action in case non-qualified trust service providers do not meet the requirements.[37] Penalties for infringements of the Regulation are up to the Member States assessment.[38] To ensure the conformity of the qualified trust service providers they shall be audited at least every 2 years and additionally the supervisory body may always request another audit or audit themselves.[39] The Commission may specify which standards should be followed for the audit.[40] For electronic identity the Regulation provides no independent supervision system that would guarantee a uniform level of protection see [SRA13, p. 144][By13]. Even after the modifications of the Regulation this is still the case]

4. Requirements of eIDAS for the development of FutureID

4.1 Introduction

In this section we address the requirements that can be derived from eIDAS that need to be taken into consideration in the technical development of the FutureID infrastructure.

[33] Art. 3 (3) eSignature Directive.

[34] Feasibility study, p. 57.

[35] Art. 17 eIDAS

[36] Art. 18, art. 19 eIDAS.

[37] Art. 17 lid 3 eIDAS.

[38] Art. 16 eIDAS.

[39] Art. 20 eIDAS.

[40] Art. 20 (4) eIDAS.

As explained and defined in section 2.2, we will focus the analysis of the requirements to the FutureID infrastructure.

4.2 Privacy and Data Protection

Privacy awareness and the need for adherence to strict privacy rules gained momentum in the development of eIDAS as can be witnessed by the fact that the current version of eIDAS, as accepted by Parliament, contains stronger data protection requirements than the original proposal of the Commission.[41] Recital 11 concerns a general obligation to apply the Regulation in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC.[42] Without addressing all the requirements that stem from this Directive, the recital does stress the need for data minimisation: "authentication for a service online should concern processing of only those identification data which are adequate, relevant and not excessive to grant access to that service online". In relation to trust service providers and supervisory bodies eIDAS explicitly states that the requirements of confidentiality and security must be respected.[43]

Article 12 of eIDAS concerns notified national electronic identification schemes. After establishing the requirement of interoperability of these schemes, the article requires further that the interoperability framework shall meet the following criteria in relation to data protection:

"(c) it shall facilitate the implementation of the principle of privacy by design; (d) it shall ensure that personal data is processed in accordance with Directive 95/46/EC".

Even though eIDAS stresses the need to incorporate privacy requirements into the architectural design of electronic identification schemes, the details of what these requirements entail are not part of eIDAS.

It was even feared that some provisions of the eIDAS Regulation would prohibit the notification of special privacy advancing solutions, like the solution of the German nPA with mutual authentication requirement and user-centric transfer of personal data using a certificate that is subject to costs [By13] [Qu13]. Art. 6 about the notification requirements has been adjusted and, in the last version, no longer requires that the Member State ensures the availability of the authentication possibility at any time, free of charge and for any relying party, but restricts it for services online provided by a

[41] Original proposal available 12 May 2014 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:en:PDF.

[42] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31.

[43] Recital 11 eIDAS.

public sector body and specifies further that Member States shall not impose any specific disproportionate technical requirements on relying parties where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes (art. 7 (f)).

Data minimisation, confidentiality and security are only a few of the requirements stemming from an extensive EU legal framework regarding data protection.[44] All requirements of this legal framework must be taken into account in developing the FutureID infrastructure. However, it goes beyond the scope of this paper to discuss all the relevant data protection requirements. These requirements stem from a different legal framework, while the focus of this paper is to address requirements stemming from eIDAS. Moreover, the EU legal framework regarding data protection is currently under review, replacing Directive 95/46/EC with a Regulation. More clarity on the exact provisions of the Data Protection Regulation is expected later this year, or even next year, as the Council has postponed its hearing until after the elections of May 2014.[45] Presumably, the text the Council ultimately approves will contain amendments to the text adopted by the Parliament.[46] In view of the explicit reference in eIDAS to the principles of privacy by design and privacy by default, we do want to stress the importance to try and build into the FutureID infrastructure privacy requirements that can be derived from the current *and* prospective EU legal framework regarding data protection.[47] At this point in time, however, it is difficult to predict what the exact implications of these new principles will be. To give an example we point to the current developments in the Netherlands. Dutch government is still in the process of developing a coordinated, national system of electronic identities, including a publicly eID card with a high level of reliability. An interesting question the principles of Privacy by Design and Default raise, concerns the room for Dutch government not to make use of certain technologies, such as attribute based credentials, if experts agree such tools to be the most privacy-friendly solution. [Mi13]

Besides the requirements pertaining to data protection, article 12 furthermore demands the interoperability framework to be technology neutral and non-discriminatory between any specific national technical solutions for electronic identification within the Member States. These requirements, just as data protection and privacy compliance, are explicitly

[44] Currently consisting of Directive 95/46/EC, but also the ePrivacy Directive (2002/58/EC as amended by 2009/136/EC) and the Data Retention Directive (2006/24/EC).

[45] See http://europa.eu/rapid/press-release_MEMO-14-186_nl.htm

[46] Text adopted by the Parliament available 12 May 2014 at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf and http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

[47] More on the revision of the data protection legal framework and privacy by design [Ku12] [CKP14].

stated to be the main goals of FutureID, and thus are an integral part of the technical development strategy of FutureID. A final requirement of Article 12 concerns the obligation to follow, when possible, European and international standards. This requirement is the subject of the next section.

4.3 Assurance levels and standards

Even though art. 12 does not in a strict sense oblige developers of FutureID to adhere to assurance levels and standards as some room is left in the phrasing: “when possible”, we do address them as it will offer great advantages to implement these assurance levels into the FutureID infrastructure since these levels will provide one common European system.

Depending on the negative impact of a wrong authentication the risk level of a service can vary [Jø14]. For this reason different national governments and several EU projects defined frameworks that specify different Authentication Assurance Levels (AAL) for user authentication, to balance different levels of risk with corresponding appropriate authentication assurance [Jø14]. Also in eIDAS the EU legislator has defined 3 different assurance levels: “low”, “substantial” and “high”.[48] “Low” provides a limited degree of confidence and its aim is to decrease the risk of misuse and alteration of the identity, while the purpose of “substantial” is to substantially decrease the risk.[49] “High” will provide the highest level of confidence and its purpose is to prevent misuse or alteration of the identity.[50] Only means with an equal or higher assurance level than the level required for the online service can be used to access the service, so it will not be possible to access a high level online service with low level identification means.[51]

These criteria are quite vague and to specify them the Commission provides that, ultimately 12 months after entry into force of the Regulation, the Commission shall by implementation acts set out minimum technical specifications, standards and procedures.[52] These shall be established by reference to the reliability and quality of the identity registration (identity proofing, issuance procedure, issuing entity), the authentication method (which mechanism is used) and the specifications of the issued electronic identification means.[53] Despite the fact that no implementing acts are available yet, the direction in which these will go are clear. Recital 16 of the Regulation

[48] Art. 8 eIDAS.
[49] Art. 8 (2) (a) and (b) eIDAS.
[50] Art. 8 (2) (c) eIDAS.
[51] Art. 6 (1) (b) eIDAS.
[52] Art. 8 (3) eIDAS.
[53] Recital 16 and Art. 8 (3) eIDAS. See also [Jø14, p. 75].

refers to the Large Scale Pilot STORK[54] and ISO 29115[55] and inter alia, to their levels 2, 3 and 4, "which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurances levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to proofing of identity for issuing qualified certificates."[56] eIDAS also states that requirements should be technology neutral and that "it should be possible to achieve the necessary security requirements through different technologies."[57]

The implication for pan European eID frameworks lies less in how the exact definition of the assurance levels is and more in the fact that there will be binding levels for notified eID means and that those will be specified. While in case of only national eID systems the service provider normally can assess the reliability and trustworthiness of their well-known own national eID, this is not the case for eIDs from other Member States. Therefore, pan European eID frameworks need to provide a solution for this problem and assurance levels are there for this reason. However, currently it is problematic that there are different assurance level systems and different ways to map them. The implementation acts of the Regulation will now set out three levels with hopefully clear specifications. Additionally, the Member States who notify their schemes must indicate the assurance level and they have to ensure that the means have been attributed to a person in accordance with the technical specifications, standards and procedures set out by the implementing acts.[58] This provides a high grade of reliability for pan European eID frameworks and service providers. However this will still be only for government notified eID schemes, therefore a reliable system for private eID solutions is not defined by the eIDAS Regulation [SRA13 p. 45]. Nevertheless also private eID providers, whose schemes are not notified can use the assurance level system in cross-border situations, therefore the assurance levels can provide a framework also for not notified eID solutions.

4.4 Usability

To conclude this section on requirements, we address usability and user friendliness. Recital 47 of eIDAS states that: "Confidence in and *convenience of* online services are

[54] Described in STORK D2.3, Quality authenticator scheme, available 12 May 2014 at https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312. The STORK Quality Authentication Assurance (QAA) model defines 4 assurance levels (named 1: no or minimal assurance, 2: low assurance, 3: substantial assurance and 4: high assurance).

[55] ISO/IEC 29115:2013 Information technology-Security techniques-Entity authentication assurance framework. ISO29115 provides also 4 levels of assurance (called LoA 1 low; LoA 2: medium; LoA 3: high and LoA 4: very high).

[56] Recital (16).

[57] Recital (16).

[58] Art. 9 (1) (a), art. 7 (e).

essential for users to fully benefit and consciously rely on electronic services" (emphasis added). Even though this sentence is the introduction to create an EU trust mark, it also hints to usability and user friendliness as more general requirements in the development of online identification and authentication schemes. Article 15 of eIDAS concerns the usability of a specific group of users, as it requires, where feasible, the accessibility for persons with disabilities. This requirement does not only pertain to trust services, but also to end user products used to provide these services. This is an important requirement for the eSignature service of FutureID which should be taken into account.

5. Conclusion

eIDAS does not contain a lot of requirements directly relevant to the development of the FutureID infrastructure. This mainly relates to the scope of the FutureID project and the fact that a substantial part of eIDAS is focused on the actual provision of Trust Services. The main goals of the FutureID infrastructure align with important focus points of eIDAS, such as interoperability and compliance with data protection. Even though the relevance of eIDAS for the development of FutureID as such is limited, the implications of eIDAS for the overall pan European online authentication environment are substantial. At this point it is hard to predict whether eIDAS will indeed lead to a vivid cross border electronic identification and authentication landscape. The eSignatures Directive was stipulated as 'used by few and ignored by many' [DV08, p. 19], if this will change with the Regulation relates e.g. to the existence of actual use cases and how the liability regime of eIDAS will affect the mutual recognition of online identification and authentication schemes. Liability for notifying Member States may cause barriers for private parties to enter the market and could even lead Member States to abstain from notifying any scheme.

References

[Sm12] Smedinghoff, T.J., Solving the legal challenges of trustworthy online identity, Computer Law & Security Review 28 (2012) p. 532.

[St09] STORK D2.2 Report on legal interoperability, p. 152, available 12 May 2014 at https://www.eid-stork.eu/dmdocuments/public/D2.2_final._1.pdf

[Bu14] Buchmann, N.; Rathgeb, C.; Baier, H.; Busch, C.; Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area, in Proceedings of the 2nd Annual Privacy Forum (APF'14), 2014, p. 172.

[Wp14] Written report of the Article 29 Data Protection Working Party Biometrics & eGovernment Subgroup on STORK, available 12 May 2014 at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_15_letter_artwp_atos_origin_annex_en.pdf

[Ro13] Roßnagel, H.; Camenisch, J.; Fritsch, L.; Gross, T; Houdeau, D.; Hühnlein, D.; Lehmann, A.; Shamah, J.; FutureID – Shaping the Future of Electronic Identity, p. 1, available 12 May 2014 at http://ec.europa.eu/digital-agenda/events/cf/ict2013/document.cfm?doc_id=25733

[LR13] Lipp, P.; Rath, C.; et. al.: "FutureID D33.1 Requirements Report". Available at 10 September 2014 at http://www.futureid.eu/data/deliverables/year1/Public/FutureID_D33.01_WP33_v1.0_Requirements%20Report.pdf.

[Ec12] European Commission Annual Growth Survey, Brussels, 28.11.2012, COM(2012) 750 final.

[DV12] Dumortier, J.; Vandezande, N.; Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (September 26, 2012). ICRI Research Paper 9. Available at 12 May 2014 at SSRN: http://ssrn.com/abstract=2152583.

[Vo13] Voulon, M.B.; Een Europese verordening voor identity management (IdM), Computerrecht 2013/118, p. 196-204.

[SRA13] Spindler, G.; Rockenbauch, M.: Aufsatz, Die elektronische Identifizierung, MMR 2013, p. 138-149.

[By13] Byszio, F.; Houdeau, D.; Meister, G.; Wolfenstetter, K-D.: Aufsatz, Elektronische Identifikation in Europa: die neue EU-Verordnung, DuD 2013, p. 171.

[Qu13] Quiring-Kock, G.; Aufsatz, Entwurf EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, DuD 2013, 20-24, p. 21.

[Ku12] Kuner, C.; The European Commission's Proposed Data Protection Regulation: A Copernican revolution in European data protection law (2012) 11 Privacy & Security Law Report 6, 1–15.

[CKP14] Cuijpers, C.; Kosta, E.; & Purtova, N.; Data Protection Reform and the Internet: The Draft Data Protection Regulation. In Savin, A.; Trzaskowski, J.; (eds) (2014) Research Handbook on EU Internet Law. Cheltenham: Edward Elgar, p. 543-568.

[Mi13] Ministry of the Interior and Kingdom Relations, Dutch eID system. Strategic Outlook and proposal for follow-up. Available at 15 September at http://www.eid-stelsel.nl/fileadmin/eid/documenten/20130812_Strategic_Outlook_and_proposal_for_follow-up_eID_Stelsel.pdf

[Jø14] Jøsang, A.; Identity management and trusted interaction in Internet and mobile computing, IET Information Security, Vol. 8, Iss. 2, 2014, pp. 67-79.

Secure Cloud Computing with SkIDentity: A Cloud-Teamroom for the Automotive Industry

Michael Kubach, Fraunhofer IAO
Nobelstr. 12, 70569 Stuttgart
michael.kubach@iao.fraunhofer.de

Eray Özmü, Universität Stuttgart
Nobelstr. 12, 70569 Stuttgart
eray.oezmue@iat.uni-stuttgart.de

Guntram Flach, Fraunhofer IGD
Joachim-Jungius-Str. 11, 18059 Rostock
guntram.flach@igd-r.fraunhofer.de

Abstract: A major security-challenge in the automotive industry is to enable the secure and flexible engineering cooperation with changing partners in complex development projects. Therefore an effective interorganizational identity management is needed to control access to cooperative development platforms. This identity management has to be based on reliable identification of engineers of various partners with different credentials. The SkIDentity-Project, that aims to build trusted identities for the cloud, addresses this scenario. By integrating the existing components, services and trust infrastructures into a comprehensive, legally valid and economically viable identity infrastructure the technology enables to provide trusted identities for the cloud and secure complete business processes and value chains. One pilot-application of the project is the "Cloud-Teamroom for the Automotive Industry". It is adjusted to the specific requirements of the value chains in the automotive industry. Thanks to the SkIDentity-Technology, and via the so-called eID-Broker, engineers from different partners can access the cloud-teamroom. For the required strong authentication they can use the credentials that are already available in their company. This paper presents the SkIDentity-technology and exemplifies it by means of the pilot-application.

1 Introduction

Trustworthy cloud computing requires secure and reliable mechanisms for authentication. At the same time user interfaces and authentication processes have to be designed as user-friendly as possible to achieve a high user acceptance [Se14]. Only systems that are accepted by users and that are actually used can make the authentication to cloud computing systems sustainably safer. This highlights that security is not merely a technological challenge. Therefore the goal is a solution that combines good usability with high technical security.

The SkIDentity project[1] accordingly strives to create an architecture that is designed to flexibly work together with solutions from multiple vendors [Sk14]. Through a federated identity management (FidM), organizations will be able to offer one or multiple authentication services or make use of external identity information and authentication for applications operated by them; a multitude of combinations being possible. Both the technical and organizational aspects, as well as the legal requirements are taken into account by the project. As a result, the user should be able to use her preferred "identity card" (credential) for strong authentication in various applications. This reduces the number of authentication information to remember or credentials to manage by the individual user. Moreover, it saves her from having to become acquainted with new authentication procedures with every new service she uses. At the same time this simplification increases security because the authentication steps and sequences are always familiar, comprehensible, understandable, and recognizable for the user.

However, the user is not the only stakeholder that has to be considered for an identity management system. As Roßnagel and Zibuschka have argued, all relevant stakeholders for an identity management system have to be taken into account [ZR12]. This means that we have to look at the service providers' requirements as well. They have to implement and operate the system, which means that they have to make significant investments in terms of money and other resources [KRS13]. Therefore, they will only be willing to implement a specific identity management system if these investments are likely to pay off. So there needs to be a business case for the service providers to implement the identity management system. For example this could be (a) the possibility to raise the number of potential customers or users of the provided service or (b) to reduce the costs induced by the authentication process. The SkIDentity-Technology enables both: (a) As users can perform a strong authentication with the service using the credentials they already possess, the number of potential users and customers is raised. And (b) the handling of credentials is facilitated as there is no need for the service to give out its own credentials. Already available credentials such as national electronic ID-Cards (eIDs) or other identity tokens such as OTP-Generators or even mobile phones can be easily integrated. Therefore cost savings can be achieved.

The third relevant stakeholder for an identity management system is the identity provider. It can be assumed that the goal of the identity provider is to gain a large base of users and service providers that rely on its identity provision services. The business model of the identity provider could be that both or one of these groups of users pay for the identity provider's service. Thus, a higher number of users and service providers should raise the revenue of the identity provider. At the same time, as we have already

[1] SkIDentity is among the winners of the "Trusted Cloud" technology competition (www.trusted-cloud.de) of the Federal Ministry of Economics and Energy (BMWi) and aims at providing trusted electronic identities for cloud computing services. It brings together an interdisciplinary team of experts led by the ecsec GmbH with the participation of the ENX Association, the Fraunhofer Institutes IAO and IGD, the Open SignCubes GmbH, Ruhr University Bochum, the University of Passau, the Urospace GmbH and VDG Versicherungswirtschaftlicher Datendienst GmbH. Additionally, the SkIDentity-project is supported by relevant organizations such as the Federal Association for Information Technology, Telecommunications and New Media (BITKOM), EuroCloud Deutschland_eco e.V., ProSTEP iViP e.V. and TeleTrusT – IT Security Association Germany e.V. and renowned companies such as DATEV eG, easy Login GmbH, media transfer AG, SAP AG und SiXFORM GmbH.

described above, a higher number of users is in the interest of the service provider as well. Moreover, a higher number of potential services that can be used with a specific credential already in the hands of a user is in the user's interest. From an economic science perspective this illustrates that network effects apply to identity management systems so that in this case we are faced with a multi-sided market [ZR12], [Ha04], [Ev03].

The article shows how the SkIDentity-Technology achieves what is described above and exemplifies this by means of the pilot-application. Thus, it is organized as follows. Section 2 outlines the scenario in the automotive industry in greater detail. In section 3 we describe the system architecture of the SkIDentity-Technology. Subsequently, in section 4, we present the pilot-application "Cloud Teamroom" as realized in the project, before we conclude our findings in section 5.

2 Pilot-Application Scenario: Automotive Industry

The automotive industry can be characterized as highly competitive and globalized. A relatively small number of car makers (original equipment manufacturers – OEMs) are spread over the world. Most of them target the world-market and therefore compete against each other on a global scale. This industry has always been driven by new technologies and technological advances are often quickly adopted into new products. Within the last one or two decades, this led to a tighter integration and interconnection of simple parts into more complex systems. The OEMs have reacted to these new challenges by outsourcing the production and even the development of those systems. Thus, the tasks of the suppliers have grown from manufacturing simple parts to manufacturing complex systems. As these systems require a highly specialized knowledge, they are often not only made, but also designed by the supplier according to the OEM's specification [WRZ12], [Vo04].

The development described above has led to the current situation in which a significant amount of the value is not generated by the OEM itself, but by the extended workbench consisting of its suppliers. Yet, these suppliers (Tier1-suppliers) usually have an extended workbench with suppliers (Tier2-suppliers) as well. Here, we can see the distributed value chain of the automotive industry [Vo04].

The intense competition in the automotive industry makes a continuous reduction of the time-to-market of new products imperative. This is achieved inter alia through an interactive collaboration between the engineers at OEMs and suppliers in multi-user applications [VS02]. However, due to the complex network-like structure of competition in the automotive industry, OEMs, Tier-1 and Tier2-suppliers at the same time cooperate for different components each with numerous competing partners. For this reason, an effective access control for sharing and collaboratively editing of technical specifications and component design is absolutely necessary to protect the intellectual capital of each partner.

The effective interorganizational access control that is required already constitutes a major challenge for the identity management (IdM) inside of a single organization. However, if several independent companies (OEMs, Tier1-, Tier2-suppliers and, where appropriate, Service/Cloud providers) are involved, the complexity of the task of a trusted authentication of all engineers involved increases significantly. For example, different companies use their own authentication methods and security policies that must be implemented by service/cloud providers. In addition, dependent on the specific demand, engineers are assigned to or withdrawn from projects by their mother company. Therefore, access rights and permissions permanently have to be kept up-to-date (Enrolement/De-Provision/De-Enrolement). The economic and technical capabilities, particularly of smaller organizations without major IT departments thus quickly reach their limits, due to the variety of requirements that need to be fulfilled. Moreover, the complexity of the task can provoke errors, leading to security problems and, in the end, costly loss of intellectual capital or the termination of working relationships.

In a scenario as depicted, a SkIDentity-based solution could address the identity management-specific challenges. But before this solution is presented, we'll outline the system architecture of the SkIDentiy-Technology in the following section.

3 SkIDentity System-Architecture in Brief

SkIDentity builds upon the concept of Federated Identity Management (FIdM) [HRZ10]. The architecture enables the use of various authentication methods, services and protocols in a consistent and secure way in any application. Particularly, the SkIDentity-technology renders it possible to use government-issued electronic Identity Cards (eIDs) for a great variety of services. These eIDs or similar documents, such as the German "neuer Personalausweis" (nPA), are increasingly available in the general population all over Europe, as they are being issued by more and more states [Fu13]. Thanks to the official trust anchor, due to being issued by the public authorities, these credentials are perceived as very save and over time they will be widespread. The design of the SkIDentity system-architecture therefore pays particular attention to compliance with the requirements of the German eID-law.

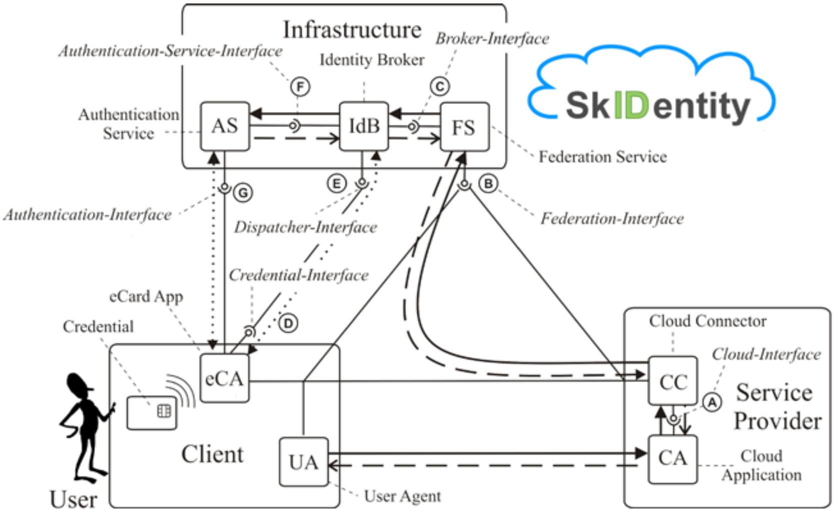


Figure 1: SkIDentity reference-architecture

The SkIDentity reference-architecture for strong and trustable authentication in the cloud can be broken down into three major components. As shown in Figure 1, these are located at the user/client, the service provider and infrastructure components.

Identity Broker (IdB)

The IdB is the central component in the SkIDentity-infrastructure. When an authentication request is sent by the Cloud Connector (CC) or Federation Service (FS), he determines which credentials are available from the user, so that an appropriate service for the user authentication can be selected.

Federation Service (FS)

The FS is an optional service that supports protocols for identity federation such as [Ha12], [Op07], or [Ca05]. If the authentication policy supports it, a single-sign-on becomes possible. In this way a user only needs to authenticate once to use a multitude of applications (for a certain time).

Cloud Connector (CC)

Via the CC, the Cloud Application (CA) is integrated into the SkIDentity-infrastructure. The CA represents the cloud application that the user actually wants to access. The CC is operated at the CA. It enables the CA to use identities and authentication with a protocol that is supported by an IdB or a FS. CAs that already support such functionality have already implemented a CC. But the CC can also be integrated directly into a CA afterwards by using a program library if the functionality hasn't been implemented right from the start. Alternatively, it can work as an independent process that receives the data from an IdB or FS to transmit it in a compatible format to the CA.

Authentication Services (AS)

To perform the actual user authentication the IdB calls the AS. Dependent on the credential, a suitable authentication protocol is used for this communication. As an example: to authenticate with the nPA the Extended Access Control (EAC) protocol according to [Fe12] is used.

The following chapter will show how the now outlined SkIDentity system-architecture can be used to build an application that addresses the challenges of the automotive scenario described earlier in this paper.

4 Pilot-Application: Cloud-Teamroom for the Automotive Industry

The pilot-application that has been developed in the SkIDentity project is a cloud-teamroom for the automotive industry. It provides a cloud-based collaborative workspace that can be accessed by different users with specific, variable permissions. By utilizing the Identity Broker for the authentication, credentials that are already available in the organizations can be used. It is not necessary to give out (and after termination of the project collect) special credentials to engineers of partner organizations that are supposed to work on the platform. The cloud-teamroom was integrated into the architecture of SkIDentity and developed in a way so that it can serve as an experimental system for further research and development work in the sense of agile software development [PEM03] as well as public presentations.

The overall concept of the cloud-teamroom is pictured in Figure 2. One or more companies in a manufacturer-supplier network in the automotive industry opt for the use of the SkIDentity-infrastructure for the secure authentication at a shared cloud-service. The cloud-teamroom of the realized pilot-application is an example for this application scenario.[2] Technically, it is based on the Open Source software system ownCloud for cloud storage and data synchronization [Ow14]. While the company names used below are fictitious, the whole scenario is realistic. It was developed according to the results of five qualitative interviews with major OEMs and suppliers from the European automotive industry. These interviews were conducted in 2012 and 2013, recorded and transliterated for analysis.

[2] The pilot-application can be accessed via: https://www.skidentity.de/de/demo/ .

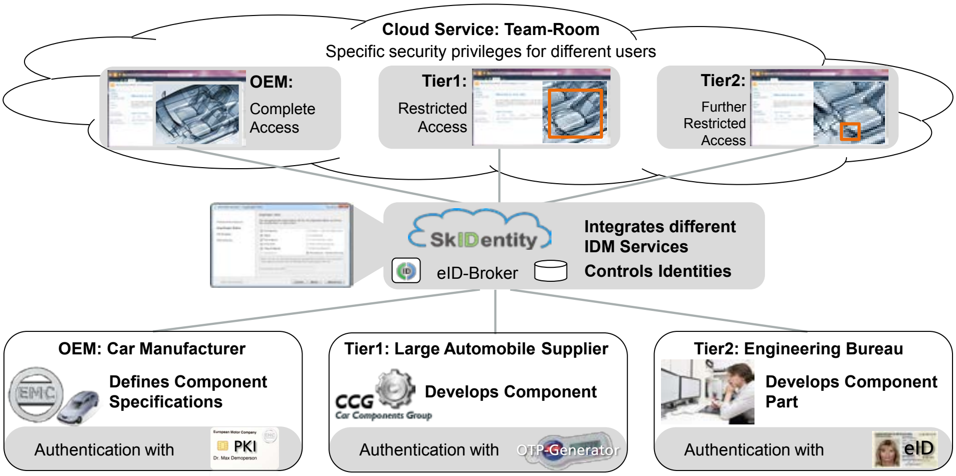
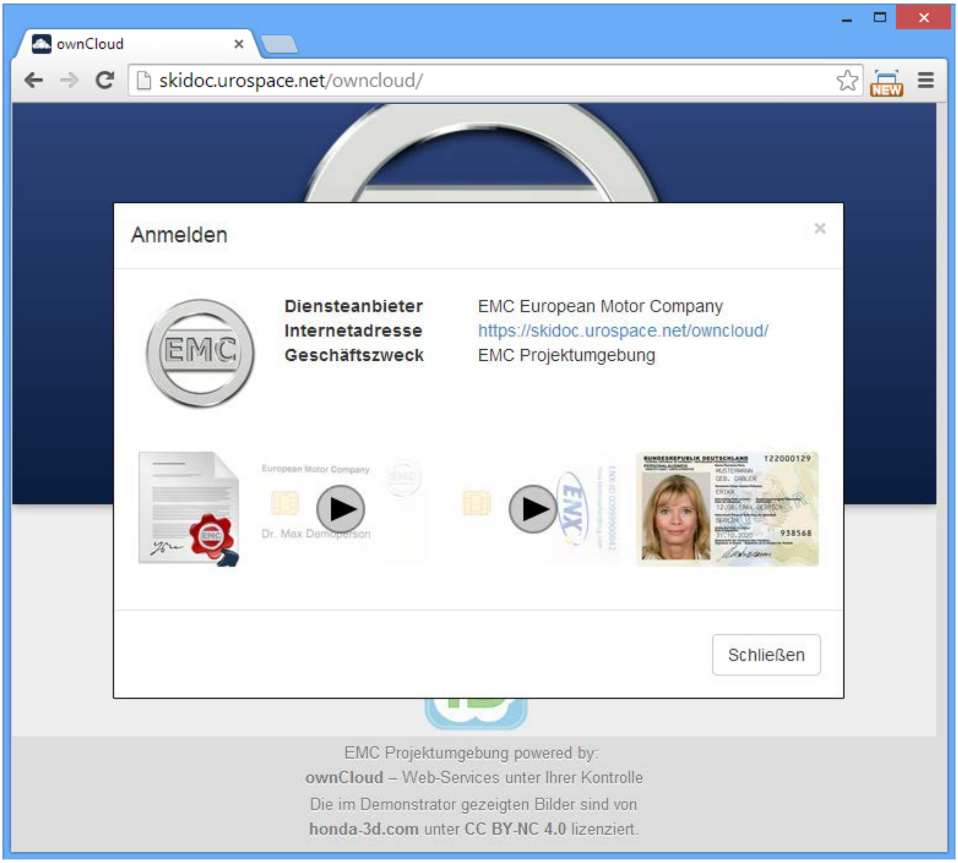


Figure 2: Concept of the Cloud-Teamroom for the Automotive Industry

The authentication through SkIDentity to log on to the service can be done by clicking on the SkIDentity-Button embedded into the login-screen of the cloud-service. The SkIDentity Identity Selector pops up to show the user which credentials are available for authentication at the cloud service (see Figure 3). After the user has selected his available/preferred credential she gets redirected to the IdP to perform the authentication process there. If the authentication is successful, the user is granted access and she gets logged on to the service to use it as intended. For example he can access 3-D-Model-Data (see Figure 4). Specific read/write-permissions for individual engineers are handled in the cloud service (here: the ownCloud solution), not through the SkIDentity-Technology.



Anmelden

Diensteanbieter	EMC European Motor Company
Internetadresse	https://skidoc.urospace.net/owncloud/
Geschäftszweck	EMC Projektumgebung

EMC Projektumgebung powered by:
ownCloud – Web-Services unter Ihrer Kontrolle
Die im Demonstrator gezeigten Bilder sind von
honda-3d.com unter **CC BY-NC 4.0** lizenziert.

Figure 3: Login to the Cloud-Teamroom with the Identity Selector by SkIDentity

According to the qualitative interviews the Open Source platform ownCloud, which is originally designed for data storage in the cloud, was customized to fit the needs of users in an automotive scenario. Depending on the role a user holds, the design and the functions presented in the cloud-teamroom vary.

By using the SkIDentity-infrastructure each user obtains a unique ID which is used inside ownCloud as the specific user ID. This user ID corresponds to an ownCloud user which then can be authorized inside the ownCloud user management settings. By assigning the user to a user group the administrator can easily manage their access rights and available functions inside the cloud-teamroom.

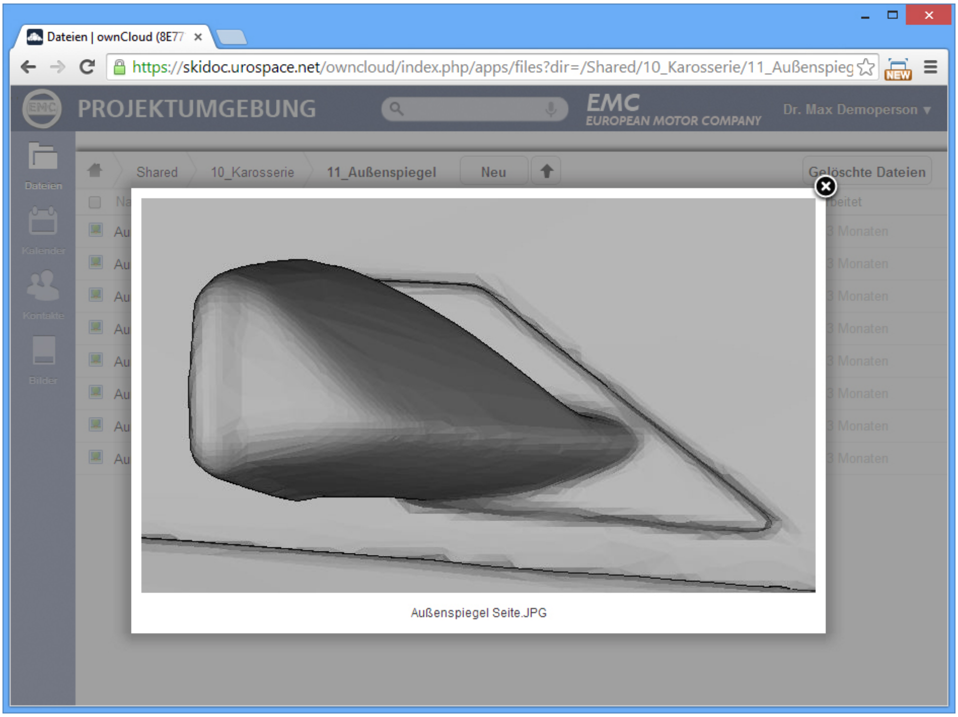


Figure 4: Exemplary Functionality of the Cloud-Teamroom: View of 3D-Model-Data

In a fictitious case study for the pilot-application, based on the results of the qualitative interviews, three companies from the automotive cooperate in a development project. The cloud-teamroom is operated by the fictitious car maker EMC – European Motor Company. It is a big global player in the automotive industry with a highly capable IT-department and considerable resources. In the development project it cooperates with CCG - Car Components Group and Ingenieurbüro Schneider on a new car component. CCG is a Tier1-Supplier of medium size. Ingenieurbüro Schneider is a small independent engineering bureau that is very specialized on a specific part of the component (Tier2-Supplier). In the pilot-case four possible credentials are available:

1. A software certificate, stored on the desktop PCs of EMC. This OEM operates the cloud-teamroom in this case study and his desktop PCs are operated in a safe environment and protected by physical as well as software (PKI-based) access control. Therefore a software certificate is highly convenient while at the same time being very secure.
2. EMC-Company Smartcard, based on a PKI-Infrastructure. This Smartcard allows engineers of EMC to access the cloud-teamroom from any computer with a suitable card-reader that fulfils the company's security policy.
3. CCG-Smartcard, provided to the company by the ENX-association (ENX-ID). ENX is a respected organization in the automotive industry that already

provides a secure communications network to the industry [En14]. Moreover, as it is founded and supervised by most major OEMs and suppliers it serves as a trust anchor for the electronic identities assigned with the smartcard. Thus, ENX serves as an IdP for CCG. Engineers of CCG can use this Smartcard to use internal services as well as to access the cloud-teamroom.

4. German national ID-Card: neuer Personalausweis (nPA). As Ingenieurbüro Schneider is a Company with only a hand full of employees it doesn't have an IT-department, not to mention a PKI-Infrastructure. However, the engineers possess an nPA which they can use for strong authentication at the cloud-teamroom.

This shows how strong authentication in the complex value chain of the automotive industry can be achieved by making use of the SkIDentity-technology and with limited resources. Each partner just uses the credential that is most convenient for him. At the same time a high level of security and trust is achieved.

4 Conclusion

With the example of a cloud-teamroom for the automotive industry, this paper has shown how an effective interorganizational identity management can be realized with the SkIDentity-technology. The approach enables reliable identification of engineers of various partners with different credentials while being easy to implement into existing structures and processes.

In addition to the evaluation of the approach used in the current pilot-application, future work will be especially concerned with the further analysis of the results of a qualitative market study on Federated Identity Management in the automotive industry. First results of this analysis have already been integrated into the design of the pilot-application. The combined results will be used to revise the SkIDentity reference-architecture as a whole. Moreover, they will be used to iteratively refine the pilot-application and to conceptualize business models for SkIDentity in the successive project phases.

References

[Se13] C. Senk, "Future of Cloud-Based Services for Multi-factor Authentication: Results of a Delphi Study," in *Cloud Computing*, vol. 112, M. Yousif and L. Schubert, Eds. Springer International Publishing, 2013, pp. 134–144.

[Sk14] SkIDentity, "Skidentity-Project Website," *Skidentity-Project Website*, 2014. [Online]. Available: http://www.skidentity.de/.

[ZR12] J. Zibuschka and H. Roßnagel, "Stakeholder Economics of Identity Management Infrastructures for the Web," in *Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012)*, Karlskrone, Sweden, 2012.

[KRS13] M. Kubach, H. Roßnagel, and R. Sellung, "Service providers' requirements for eID solutions: Empirical evidence from the leisure sector," in *Open*

Identity Summit 2013 - Lecture Notes in Informatics (LNI) - Proceedings, D. Hühnlein and H. Roßnagel, Eds. Bonn, 2013, pp. 69–81.

[Ha04] A. Hagiu, “Two-sided platforms: Pricing and social efficiency,” 2004.

[Ev03] D. S. Evans, “The Antitrust Economics of Two-sided Markets,” *Yale J. Regul.*, vol. 20, no. 2, pp. 235–294, 2003.

[WRZ12] I. Wehrenberg, H. Roßnagel, and J. Zibuschka, “Secure Identities for Engineering Collaboration in the Automotive Industry,” presented at the MIGW 2012 - Conference on Mobility in a Globalised World, Bamberg, 2012, pp. 1–12.

[Vo04] G. Volpato, “The OEM-FTS relationship in automotive industry,” *Int. J. Automot. Technol. Ldots*, vol. 4, no. 2/3, pp. 166–197, 2004.

[VS02] G. Volpato and A. Stocchetti, “The role of ICT in the strategic integration of the automotive supply-chain,” *Int. J. Automot. Technol. Manag.*, vol. 2, no. 3/4, p. 239, 2002.

[HRZ10] D. Hühnlein, H. Roßnagel, and J. Zibuschka, “Diffusion of Federated Identity Management,” in *Sicherheit 2010*, F. C. Freiling, Ed. Bonn: Köllen Druck + Verlag GmbH, 2010, pp. 25–36.

[Fu13] FutureID Project, “Survey and Analysis of Existing eID and Credential Systems, Deliverable D32.1,” 2013.

[Ha12] D. Hardt, Ed., “The OAuth 2.0 Authorization Framework, IETF RFC 6749.” 2012.

[Op07] OpenID Foundation, “OpenID Authentication 2.0.” 2007.

[Ca05] S. Cantor, J. Kemp, R. Philpott, and E. Maler, *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0*. 2005.

[Fe12] Federal Office for Information Security (BSI), “Advanced Security Mechanism for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authentication Connection Establishment (PACE), and Restricted Identification (RI),” Technical Directive (BSI-TR-03110) Version 2.10, 2012.

[PEM03] F. Paetsch, A. Eberlein, and F. Maurer, “Requirements engineering and agile software development,” in *2012 IEEE 21st International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2003, pp. 308–308.

[Ow14] ownCloud, “ownCloud, Your Cloud, Your Data, Your Way!,” 2014. [Online]. Available: www.http://owncloud.org/.

[En14] ENX Association, “ENX Association,” *ENX - The communications network of the European automotive industry*, 2014. [Online]. Available: http://www.enxo.com/.

Making authentication stronger and more cost efficient with web of trust

Bob Hulsebosch[1], Maarten Wegdam[1], Martijn Oostdijk[1], Joost van Dijk[2] & Remco Poortinga – van Wijnen[2]

[1] InnoValor, PO Box 321, 7500 AH, Enschede, the Netherlands
[2] SURFnet, PO Box 19035, 3501 DA, Utrecht, the Netherlands

e-mail: Bob.Hulsebosch@innovalor.nl, Martijn.Oostdijk@innovalor.nl, Maarten.Wegdam@innovalor.nl, Joost.vanDijk@surfnet.nl, Remco.Poortinga@surfnet.nl

Abstract: Solid registration processes for identity registration including proofing, vetting and binding are essential for strong authentication solutions. Solid typically implies a face-2-face component in the registration process, which is expensive and not user friendly. Alternatives that rely on remote registration often result in weak binding or are overly complex. We propose a web of trust approach in which users can indicate trust in the identity of other users. It combines the best of remote and physical registration practices. There is no need for a physical registration desk as other users in the web of trust take over the identification task. This paper describes how to achieve web of trust enhanced authentication assurance.

1 Introduction

Service providers traditionally use the familiar username and password combination to authenticate users on their websites. Unfortunately, this approach provides a relatively low level of security for users: passwords can be easy to guess, too short, and difficult to manage. Adding a second factor, e.g., combining what a user knows with something he has, to the authentication process can help to address these issues. Commonly referred to as two-factor authentication, it adds additional security to authentication and raises the level of trust from the service provider to the user.

More and more service providers are beginning to rely on two-factor authentication solutions to stop escalating online fraud, identity theft and to comply with regulations. Many financial organisations such as banks and insurance companies have been using text message- or token-based authentication solutions for transaction verification for years, but recently major websites and businesses not in regulated industries are recognizing the need for stronger online authentication. Not so long ago, Google, Facebook and LinkedIn made two-factor authentication available to all users. The drawback of these two-factor solutions is that their binding to the user's identity is relatively weak. They only ensure with increased reliability that it is the same user, not who the user actually is. Binding an authentication solution to a user whose identity has been verified and registered is not trivial. It often requires physical presence and verification against authentic sources which is cumbersome and expensive.

This paper describes an approach for enhancing the authentication strength by using web of trust in a federated identity ecosystem. The idea is to use the web of trust concept to establish the authenticity of the binding between an authentication solution (e.g. public key) and its owner via third party user attests. For instance, if person A claims that user B is using a particular authentication solution, it can provide extra confidence for the service provider to allow access to resources that require stronger authentication. Person C can also claim to know B and his authentication mechanism, thereby even further increasing the trust in the identity of B. This approach is a kind of "crowdsourcing of trust" about the identity of the user without requiring a physical registration.

The structure of the paper is as follows. Section 2 provides background information about strong authentication and web of trust. Several illustrative use cases are described in section 3. Based on these use cases the functional requirements for web of trust enhanced authentication are derived. Section 4 describes a protocol for leveraging web of trust for authentication enhancement. Implementation details are provided in section 5. The challenges are discussed in section 6. Finally, section 7 draws conclusions and describes ideas for future work.

2 Background

2.1 Strong authentication and Levels of Assurance

The strength of the entire authentication system is usually expressed in terms of levels of assurance (LoA). The LoA specifies the degree of confidence in identifying a user to whom the credential was issued, i.e. the combination of the strength of the authentication solution used and the quality of the registration process (see Figure 1). The combination of the two – stronger authentication and identity registration – is basically what is needed in order to achieve true strong authentication.

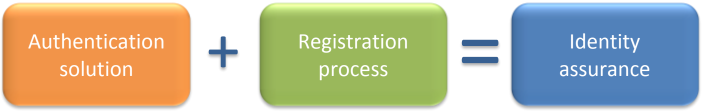


Figure 1: factors that determine the stength of the authentication.

There are several standards for the specification of LoAs. Examples are the ISO/IEC 29115 Entity authentication assurance framework [ISO13] and the STORK Quality Authentication Assurance framework [HLE09]. Both frameworks define four discrete assurance levels varying from almost no assurance in the user identity (LoA 1) to medium (LoA 2), high (LoA 3) and very high assurance (LoA 4).

The LoA paradigm allows service providers to specify assurance levels that correspond to the sensitivity or criticality of the service. Highly sensitive or critical services typically require a higher LoA. This means strong authentication solutions and robust registration processes.

Strong authentication solutions are available and typically consist of two-factor solutions (see e.g. [KUP10] for an overview).

The registration process by which a physical person is linked to his/her digital identity information and to his/her authentication credential is critical to deter registration fraud. If this process results in a weak link of the person to either the credential or the identity, there can be little or no assurance that the person using that credential to authenticate and access services and information is who he/she claims to be. It could be anyone including impostors that impersonate a claimed identity, it could be multiple people over time, or even subscribers that were denied registration. If the linking is weak, even the most complete personal information and the strongest credential will not improve the assurance of identity.

The registration process is designed, to a greater or lesser degree depending on the assurance level, to ensure that the registration authority knows the true identity of the applicant. Specifically, the requirements include measures that:

1. Increase proof in the identity of the user.
2. Increase trust in the binding between the user's identity and his digital identity.
3. Increase trust in the binding between the user and a second authentication credential.

This authentication triangle of binding is illustrated in Figure 2 below.

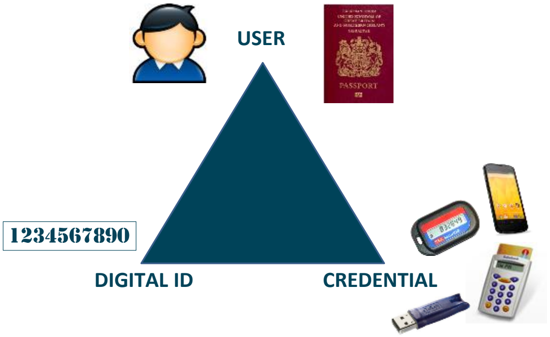


Figure 2: Binding triangle of user ID – digital ID – authentication credentials.

Different registration processes and mechanisms applied to identity vetting, proofing and credentialing result in different registration assurance levels. An applicant may appear in person to register, or the applicant may register remotely.

In-person registration is the most reliable identity proofing process during user registration. It is considered suitable for cases where there is a strong need to be able to determine that a service provider (e.g. a student information system) is dealing with a legitimate user, thus necessitating a stringent identity proofing process during user registration (i.e. a face-to-face process). In case the user is somehow not able to register in person, video conferencing tools such as Skype could be used. In this case the user identifies himself via the video conference and shows his passport or other valid photo-ID to the registrar. The use of video conferencing tools for identification, however, has several drawbacks: it introduces scheduling overhead and it makes it harder to detect a forged ID. Other – less attractive and/or appropriate – alternatives (such as use of physical address, email & mobile phone, use of bank account) are discussed in [HUL11]. The STORK and ISO29115 frameworks require physical registration for LoA 4.

Remote registration is limited to levels 1 through 3 and is more vulnerable to threats and technically complex to achieve. Remote registration relies on the availability of trusted sources to cross-reference and validate the provided assertions such as name, home address, age, social security number, and photo. Examples of such sources are the institution's HR-system or the government/municipal administration. Consultation of the latter source is restricted by legislation and not available for step-up authentication purposes; the HR-system on the other hand could be used as an alternative source. Typically, after a successful validation, a registration activation code is sent to the applicant's home address. This is cumbersome and expensive.

2.2 Web of trust

The web of trust concept is based on the idea of decentralized trust and social networks. It is used in Pretty Good Privacy (PGP[1]) as an alternative to the centralized trust model that is the basis of a public key infrastructure. In a web of trust, each user of the system can choose for himself whom he elects to trust, and whom not. Instead of trusting a single entity to validate identities, one validates the identities of the people one knows and exports this information to a public database. Then one relies on friends to vouch for the people they know, and those friends to vouch for still more people, and so on until a trust chain between any two arbitrary identities can be created. This approach avoids the inherent problems of central authorities, but in practice it is barely used due to usability issues of tools involved and the lack of user incentives.

A successful web of trust must be built very much like a social networking site, because that is how people connect and share information, and that is the model that hundreds of millions of people all over the world are already comfortable with using. As such, the web of trust model can be used to establish the authenticity of the binding between an authentication solution and its owner via third party user attests. Existing trust

[1] See PGP website for more information: http://www.pgpi.org/.

infrastructures such as PGP, identity federation, social or professional networks can be readily used to enhance the registration part of the overall LoA. Particularly in the context of virtual collaboration organizations in which users know each other, web of trust based LoA enhancement could be executed in an efficient manner. Moreover this approach also makes it easier to use social identities provided by e.g. Facebook and Google. The registration LoA part of these popular social identity providers is relatively weak (LoA 1) despite the fact that an increasing number of them are using two-factor authentication (LoA 2 or higher). Web of trust based enhanced LoA could help increase the registration LoA part of these providers and thus could help in increasing the overall LoA.

The web of trust approach combines the best of remote and physical registration practices. There is no need for a physical registration desk as other users in the web of trust take over the identification task. Users in the web of trust may use physical presence, phone or email practices for this purpose. Somehow, the attestations from the web of trust need to be related to the claimant's digital identity. This needs to be catered for by some kind of federated attestation service that enhances the assurance in the claimant's federated identity with attestations from the web of trust.

3 Use case scenarios

The following use cases illustrate the use of web of trust for enhancing authentication.

3.1 Use case 1

A group of collaborating researchers from various institutions requires access to a highly sensitive database. Access to the database requires strong authentication. The researchers know each other and their institutions participate in a single identity federation. One of them, Alice, however, does not have a strong authentication solution, i.e. she can only authenticate with an unverified username and password. Consequently she cannot access the database. To solve this issue, the other members assert claims about Alice's identity towards a special Attestation Service. They do this by logging in to the Attestation Service and indicate that they want to vet for the user's identities. After successful vetting, Alice's authentication level of assurance is increased by the Attestation Service. During the authentication process of Alice, the service provider can check at the Attestation Service for the authentication level and can decide based on the obtained information whether or not to grant her access to the database.

3.2 Use case 2

Bob has a LinkedIn account. The account is protected with a username and password combined with SMS-authentication. That the account indeed belongs to Bob, however, hasn't been verified by LinkedIn. The consequence is that the overall authentication level of assurance is low. To increase the level, Bob logs in at the Attestation Service with his LinkedIn credentials. This allows the Attestation Service to select several of Bob's connections that it trusts. It asks Bob to contact and request them to vet for his identity. Three connections vet for Bob's identity and the fact that at least one of the connections already has a higher authentication assurance level means that Bob's level can be raised as well by the Attestation Service. Next time Bob logs in with his LinkedIn account, the Attestation Service asserts that Bob has been authenticated with LoA 2.

3.3 Use case 3

Eve asks project manager John to become a member of the team. John does not know Eve and wants to know more about her. John asks the Attestation Service to validate Eve's identity. The Attestation Service looks for connections in the social graphs of Eve and Bob that overlap. Eve is asked to contact several overlapping connections and asked them to attest for her identity at the Attestation Service. The Attestation Service aggregates the attestations and informs John about the outcome. Based on this outcome John decides to grant Eve access to project team resources.

3.4 Analysis

A number of requirements can be derived from the use cases:

- The need for an attestation service that facilitates and coordinates the enhancement of the authentication solution. Specific requirements for the attestation service are:
    - Determines identity of user;
    - Links social network accounts of users;
    - Selects suitable candidates from the social network that could attest;
    - Collects and validates attestations from the social network web of trust;
    - Determines the authentication strength;
    - Communicates the outcome to the service provider;
    - Optionally: Asks the web of trust to verify other personal attributes of the user such as first name, last name, telephone number, and age.
- The availability of a web of trust that can be exploited by the service to achieve enhancement;
- The need for a federation infrastructure that facilitates the communication of the LoA to the service provider.

3.5 Functionality

A dedicated Attestation Service is required that facilitates the process of authentication LoA enhancement. Preferably the Attestation Service is part of the identity federation. The Attestation Service must be able to select suitable helper candidates from one or more web of trusts that could vouch for a user that is asking for an authentication enhancement. For instance, Helpers of institutions that participate in the same identity federation that the Attestation Service and Asker's institution belong to are preferred. Other candidates are social networks like LinkedIn or Facebook. If Asker has a PGP key, the PGP web of trust could be utilized as well. In that case the Attestation Service can ask Asker to provide her PGP key and verify its signatures until it finds a trusted anchor point. In the PGP web of trust a number of anchor points exist. These anchor points are e.g. reputable users that only sign the PGP key of other users when they have physically met or so-called centers of trust whose key is signed most by others. The shorter the path between the Attestation Service's trust anchors and the Helpers, the higher the assurance of the Asker's identity will be. We stress that the Attestation Service reuses existing web of trust structures and does not create its own web of trust (unlike many other reputation or web of trust based systems such as Ebay or AssertID [CTAID]).

4. Protocol description

We propose the following protocol for web of trust enhanced authentication:

***Step 1**: Registration of Asker.* Asker registers at Attestation Service by logging in with her federated identity and requests for enhancement of authentication. The federated authentication response of the identity provider contains identity information of Asker and is used by the Attestation Service to enhance Asker's authentication assurance. The information at least contains a LoA attribute and value and Asker's federated user identity identifier. Asker is asked to link her federated institution account with e.g. her LinkedIn account by logging in with her LinkedIn credentials. Asker may also be asked to provide her PGP key.

***Step 2**: Web of trust scoping.* Attestation Service determines who is able to vet for Asker's identity by imposing its trust requirements on the available web of trust of Asker. Once the web of trust has been determined (in this case LinkedIn or PGP) the Attestation Service should know which Helpers and how many are required. Or, in case PGP keys are used, when it should stop with PGP key validation. Asking too many Helpers will burden the Asker as she has to contact them. Subsequently, Asker is given a vouching code and is asked to contact the Helpers by phone or physically and give them the code. The use of e-mail is prohibited or deprecated; Asker has to affirm that she will adhere to this policy.

***Step 3**: Passing of vouching code.* Asker calls or meets Helpers and gives them the vouching code. During the phone call or meeting, the Helpers implictly authenticate the Asker (e.g. via voice or face recognition or by asking questions); this will be used by the Attestation Service to enhance the stength of the authentication of Asker eventually.

***Step 4**: Helper vouching.* The Helper logs in to the Attestation Service with his federated identity credentials. The authentication solutions he is using must have a higher assurance level than Asker's current level. After successful authentication, the Attestation Service asks the Helper to enter the vouching code and vouch for Asker's identity. Optionally the Attestation Service may show Asker's personal attributes and asks Helper to validate them. After that the Helper logs out.

***Step 5**: LoA determination.* 1. The Attestation Service determines the LoA of Asker based on Helper feedback. Aspects that should be taken into account are:

- Number of Helpers. A simple algorithm could be:

  New LoA = LoA + LoA*(1 – (1 – H1)*(1 – H2)*(1 – H3)….)

  With H = amount of trust [0..1] for each Helper.

  H depends on:

  - LoA of Helper
  - Coherency of Asker – Helpers web of trust such as
    - Duration relationship between Asker and Helper
    - Overlap between multiple WoTs (e.g. LinkedIn or Facebook)
    - Trust relations between Helpers
    - Number of paths between Helpers and Asker in PGP
    - Path length between Helper and Asker PGP[2]
    - Overlapping skills and endorsements in LinkedIn
- The number of invited Helpers that did not vouch. These may be considered as negative vets. They have a negative effect on the new LoA. A simple algorithm is to multiple the New LoA with the number of positive vets divided by the number of negative vets.

The Attestation Service informs Asker about the new LoA via e-mail.

***Step 6**: LoA communication.* Next, Asker can go to a service provider and authenticate via her federated identity provider. The service provider requires LoA 2 authentication. The identity provider authenticates Asker at LoA 1 and communicates this to the service provider. The service provider decides that this is not sufficient and makes a LoA attribute validation request at the Attestation Service. The Attestation Service returns a LoA 2 attribute. This convinces the service provider to allow Asker access to the service.

The different steps are illustrated in Figure 3 below.

[2] The ideal scenario in PGP key validation is to have multiple, short paths between the Asker and the anchors the Attestation Service trusts. This provides a strong guarantee that the Asker is indeed who he claims to be. The price, of course, is that it is more difficult to validate keys since the trust anchors must personally sign more keys than if fewer and longer paths are accepted.

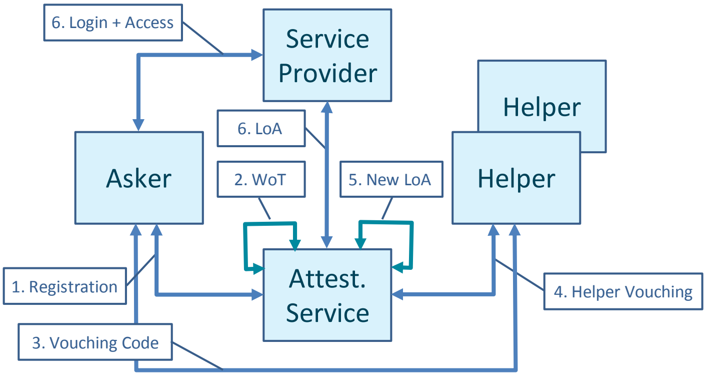


Figure 3: Web of trust protocol flow.

The protocol is inspired by the work of Brainard on using vouching by which helpers leverage their strong authentication in order to assist another user, the asker, to perform emergency authentication in case of loss of a second authentication token [BJR06].

5. Implementation

A proof-of-concept Attestation Service has been implemented. The Attestation Service is part of the test environment of SURFconext[3], the identity federation of higher education and research in the Netherlands. It allows the Asker to login with her federated account. The attributes that are provided by the identity provider during authentication at the Attestation Service could be used for validation purposes. Furthermore, the Attestation Service offers the user the opportunity to link the identity provider account to her social network account such as LinkedIn. This allows the Attestation Service to select Helpers from the LinkedIn web of trust of the Asker. The vouching code is alphanumeric and consists of five characters. Helpers kan login to the Attestation Service with their federated account. The algorithm for calculating the new LoA is relatively simple for the moment. It takes the number of Helpers into account, their authentication LoA that is provided during login, and the number of Helpers that did not vouch. The communication between the Attestation Service and the service provider for LoA validation is based on a RESTful API[4].

6. Discussion

This web of trust based LoA approach, however, raises several challenging questions that need to be addressed.

[3] SURFconext federation and collaboration infrastructure, see http://www.surf.nl/en/services-and-products/surfconext/index.html.
[4] Representational state transfer (REST), see http://en.wikipedia.org/wiki/Representational_state_transfer.

6.1 Weaknesses of web of trust approaches

One of the challenges is related to a number of weaknesses that are inherent to a web of trust approach. ENISA has summarized the possible threats such as whitewashing attack, sybil attack, impersonation and reputation theft, bootstrap issues related to newcomers, extortion, denial-of-reputation, ballot stuffing and bad mouthing, collusion, repudiation of data and transaction, recommender dishonesty, privacy threats for voters and reputation owners, social threats such as discrimination or risk of herd behaviour, attacking of the underlying infrastructure and the exploitation of features of metrics used by the system to calculate the identity assurance [CH07]. Our proposal does not mitigate all of these threats. Most of them, however, are related to the quality of the Attestation Service's reasoning algorithms that it uses to select candidate Helpers and to determine the new LoA. Registration fraud can be deterred by making it more difficult to accomplish or by increasing the likelihood of detection. It is relatively easy for an Asker to create e.g. multiple LinkedIn accounts under fake identities and establish via these accounts a web of trust of LinkedIn connections. The requirement for Helpers to have a higher LoA than the Asker makes it more difficult to enhance the LoA via this approach. Given the potential weaknesses, the web of trust approach may not be suitable to achieve LoA 4 assurance, but we certainly see the potential to achieve LoA 3.

A potential improvement to traditional web of trust systems would revolve around reducing the validity period of the claims made by other users regarding a specific user account and to allow for automatic prolongation of the trust-based claims associated to the account by subsequent authentication sessions. This would allow for both verification of use of the account and the identity associated to it and user revocation of 'stale' or otherwise undesired credentials. During the refresh process, the user can choose whether to continue to continue or stop endorsing others' accounts; this helps the dynamics of the web by helping to cull out untrusted persons more rapidly.

Further, providing the option for anti-claims, to specifically call out an account as untrusted to others, would significantly mitigate the effect of malicious persons such as spammers gaining access to a web of trust. Allowing for this anti-measure could also form the basis of a sliding trust scale, with trust and anti-trust counting against each other and allowing for unconnected persons to see that a particular account may or may not be trustworthy. Paths connecting persons would be deprecated by paths containing anti-claims; determining whether or not to trust someone with a significant number of anti-claims would be assisted by allowing short comments with them similar to twitter messages (i.e. "this person is a spammer" or "this person is a liar").

6.2 Calculating Levels of Assurance

Various approaches to calculate reputation values exist, see [Ne11] for an overview. The most important ones are:

- Summation and average based: It aggregates the ratings and the overall single reputation score is calculated by summing or averaging. The most well-known summation system is eBay and ratings in this system are represented by numeric rating.

- Discrete trust models: These models use discrete labels to represent the reputation. By using discrete labels, users can quickly determine a meaning for a reputation measure.
- Bayesian frameworks: Reputation models based on Bayesian frameworks depict reputation values as probabilities between [0,1]. These models are popular for peer-to-peer networks and sensor systems, rely on ratings being either positive or negative, and use probability distributions for reputation scores.

Since LoAs are expressed in discrete values, the discrete trust model approach seems the most straightforward approach. For the other two approaches, translation functionality will be required to map a certain reputation value to a LoA value. Calculating trust from social network aggregation is not new [SAN07], [HEI13]. These approaches, however, are solely based on the number of claims about a user and do not take into account other trust aspects such as the duration of the connection, presence of the connection in multiple social networks, or overlapping features like skills.

Another challege is related to liability. The Attestation Service becomes the authority regarding the authentication LoA of the user. It can, however, not easily be made liable for its LoA claims. The service provider has to trust the web of trust based LoA claims of the Attestation Service. The fact that both parties are in the same federation may help establishing this trust. Additionally a mechanism could be devised that allows service providers to somehow specify trust anchors it ‘knows’ (e.g. specific persons within institutions) along with their representation in various web of trust networks.

6.3 Relation to existing LoA frameworks

Closely related to the previous challenge is another one: How does the web of trust approach fit in the existing LoA frameworks defined by e.g. ISO/IEC 29115 and STORK QAA? These frameworks assume there is a central authority that issues the authentication solution and takes care of its binding to a user identity after some form of identity verification. In the web of trust based model, the verification role of this central authority becomes less important, i.e. this is done via claims of other users. Adoption of the web of trust model in these framework is one approach but could take a long time. Another approach is to register web of trust based assurance profiles at the global IANA registry that has been setup for this purpose[5].

7. Conclusions

There is an increasing need for stronger authentication solutions that go beyond username and password. The use of second factor authentication credentials is growing but lack of solid processes by which to link a physical person to his/her digital identity

[5] See http://levelofassurance.org/process.html for more information.

information and to his/her authentication credentials during enrolment weaken the overall authentication strength. If this is done poorly, there is little or no assurance that the person using that credential is who he/she claims to be. A solid registration process, however, is expensive as it usually requires the establishment of a registration desk and is not very user friendly, as he/she has to go to the registration desk. The latter requirement can even be impossible to meet for remote users.

We propose the use of web of trust to enhance the registration part of the overall authentication process. The web of trust approach replaces a physical registration at an authority by outsourcing the actual identity proofing and vetting to a user community. The outcome of the vetting allows for enhancement of the authentication assurance level. Due to various weaknesses of the web of trust model and challenges related to the determination of the actual LoA and due to liability issues, the proposed approach is unlikely to achieve LoA 4 assurance but LoA 3 seems feasible and is suitable for most online services. Future work will involve further optimisation of the algorithms for determining the authentication LoA based on claims from the web(s) of trust and pilots to collect user feedback in order to evaluate the approach.

Acknoledgements

This work is sponsored by the Géant3plus Open Calls program.

References

[BJR06] Brainard, J.; Juels, A.; Rivest, R.L.; Szydlo, M.; Yung, M.: Fourth Factor Authentication: Somebody You Know, CCS'06, October 30–November 3, 2006, Alexandria,Virginia, USA.

[CH07] Carrara, E.; Hogben, G.: Reputation-based Systems: a security analysis, ENISA position paper, October 2007.

[CTAID] Choi, J.N.; Trilli, K.: AssertID – Leveraging Social Networks for Online Identity Verification, http://www.assertid.com.

[HEI13] Heisnam, R.S.; Neelima, A.; Singh, L.S.; Singh, S.I.: A Model of Computing Trust in Web Based Social Network Using New Aggregation and Concatenation Operators, Int. Journal of Computer Science and Network, Volume 2, Issue 4, August 2013.

[HLE09] Hulsebosch, B.; Lenzini, G.; Eertink, H,: STORK Quality Authenticator Scheme, Deliverable D2.3, March 2009, see https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577.

[HUL11] Hulsebosch R. J.: Step-up Authentication-as-a-Service, SURFconext Adoption, 2011.

[ISO13] ISO/IEC 29115:2013 Entity authentication assurance framework, see http://www.iso.org/.

[KUP10] Kuppinger Cole: Market Overview Strong Authentication, 2010, see http://www.kuppingercole.com/report/srmo_stronauth_80310.

[Ne11] Neisse, R.: Trust and privacy management support for context-aware service platforms. PhD thesis, University of Twente. CTIT Ph.D. Thesis Series No. 11-216 ISBN 978-90-365-3336-2, 2011.

[SAN07] Noh, S.: Calculating trust using aggregation rules in social networks, in Proceedings of the 4th international conference on Autonomic and Trusted Computing, pages 361-371, 2007.

Towards a seamless digital Europe: the SSEDIC recommendations on digital identity management

Maurizio Talamo (1), Selvakumar Ramachandran (2), Maria-Laura Barchiesi (2)
Daniela Merella (3) and Christian Schunck (3)

(1) Nestor Lab University of Rome Tor Vergata
(2) University of Rome Tor Vergata
(3) Fondazione Inuit University of Rome Tor Vergata
Via dell'Archiginnasio snc
00133 Rome, Italy
lastname@nestor.uniroma2.it

Abstract: The SSEDIC ("Scoping the Single European Digital Identity Community") thematic network has concluded an intensive 3-year consultation period together with over 200 European and international digital identity management experts and many stakeholder organizations to establish recommendations that address key issues regarding the usability and interoperability of electronic identity management solutions. The resulting recommendations are presented in this paper and should support the European Commission as well as other public and private stakeholders to set priorities for the path towards a Single European Digital Identity Community and the Horizon 2020. The key areas that need to be addressed as a priority are: mobile identity, attribute usage, authentication, and liability.

1 Introduction

Digital identity management plays a fundamental role in securing trust and cooperation in digital and interconnected societies [Axe84, Che05]. The challenges in developing digital means that enable humans to extend their highly developed ability to recognize people and groups in the offline-world into the cyber sphere are significant. Apart from technical also psychological, cultural, legal, ethical, economic, and social issues need to be considered in the process of designing solutions which should be interoperable and convenient to use.

The objective of the SSEDIC thematic network [1] is to provide a platform for all the stakeholders of eID (electronic identity) to work together and collaborate to prepare the agenda for a proposed Single European Digital Identity Community as envisaged by the Digital Agenda (DAE) in its Key Action 16. To achieve this goal the SSEDIC consultation got in contact with as many and diverse stakeholders as possible. SSEDIC met with eID experts from the NSTIC program [Hou11] in Mountain View, Washington and London, SSEDIC

[1] SSEDIC is a EU funded thematic network (ICT PSP Call4), coordinated by Nestor Lab, University of Rome Tor Vergata, Italy. For an overview of the more than 60 SSEDIC partners and associate partners see http://www.eid-ssedic.eu

developed ties to stakeholder organizations in Russia, Turkey and Asia, SSEDIC engaged with international eID experts at ITU in Geneva and ISO/IEC in Rome, and had regular meetings in Western and Eastern Europe. SSEDIC and other European initiatives were presented and discussed at numerous conferences across the European member states as well as in India, Hong-Kong, Dubai, and Moscow. SSEDIC members met with diverse audiences including banking, law, law enforcement as well as representatives from the online entertainment industry and tourism [SSE12c, RZHM14, KRS]. SSEDIC partner organizations represent eID related experience gained in part through EU funded research projects with a total budget of more than 150 million euro [2].

The recommendations in this document are an essential outcome of three years of work by the SSEDIC community [SSE12c]. The process of drafting these recommendations in 2013 involved a short SSEDIC partner survey, a row of monthly meetings and conference calls which lead to an intensive two day meeting in Rome in which the recommendations were prepared. The resulting recommendations were sent to the SSEDIC community in October 2013. All partners were given a two week time window to vet the recommendations and to inform SSEDIC management of any concerns. The recommendations were also presented to a general audience at a workshop at ISSE in Brussels and at the ICT 2013 meeting in Vilnius. The recommendations reported below therefore express the consensus of all SSEDIC partners on how to address key-issues related to digital identity management in order to achieve the ambitious goal of a single European digital identity community.

The key areas that have been identified to be addressed as a priority are: mobile identity, attribute usage, authentication and liability, see figure 1. SSEDIC has summarized the central tasks for these priority areas in the recommendations which are presented in the following sections. SSEDIC strongly believes that these priority areas should be addressed as a matter of urgency and in view of their impact on public-private cooperation, eID governance (including trust frameworks, regulation and privacy), standardization and education.

2 Encouraging Mobile eID eGov Services Adoption

Mobile eID is a key enabler for Banking, eCommerce, eGovernment and eHealth because of ubiquitous nature of mobile technology. It is therefore to be expected that in the future a majority of eCommerce and eGovernment interactions will be done via mobile devices. An increasing number of companies adopts a “mobile first” strategy by designing their products for mobile phones or devices before making correlate designs for traditional desktop and laptop computers. In countries where mobile eID solutions have been introduced for eGovernment (e.g. Austria and Estonia) uptake is fast and citizens show a clear preference for the mobile solutions. Where no national eID systems exist, states may consider to first deploying mobile ID and mobile signatures: a core part of the infrastructure - the end-user devices - are already widely deployed. It might, however, be necessary to negotiate free

[2] The following projects have been considered: ABC4TRUST, eCODEX, epSOS, e-SENS, FutureID, GINI, SEMIRAMIS, SPOCS, STORK, and STORK 2.0

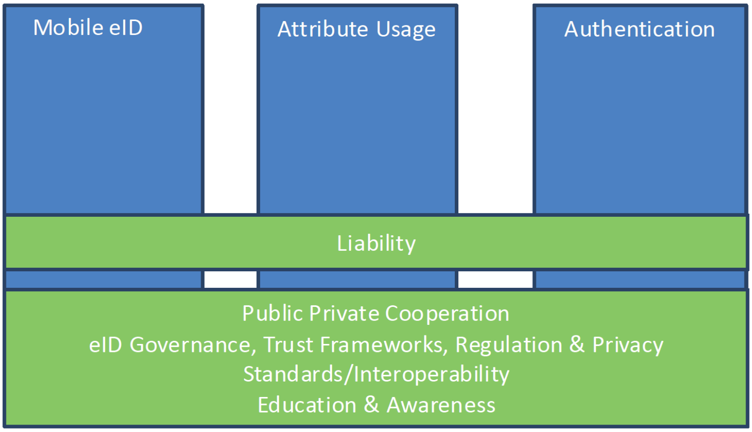

Mobile eID
Attribute Usage
Authentication
Liability
Public Private Cooperation
eID Governance, Trust Frameworks, Regulation & Privacy
Standards/Interoperability
Education & Awareness

Figure 1: Key focus areas of SSEDIC recommendations

of charge access to certain critical services (similar to emergency calls). This will require close public-private cooperation. To ensure continued uptake and success of mobile eID solutions SSEDIC therefore makes the following recommendations:

2.1 Mobile eID recommendations

1. EC Member States should be encouraged to accept Mobile eIDs, (either server-centric or device based) as being an acceptable and notifiable credential for eGov use.

2. The EC should review Mobile eSignature / Wireless PKI standards relating to eIDs as soon as possible.

3. The EC should invest in research of suitable multi-factor authentication mechanisms using personal mobile devices.

4. The EC should invest in a coordinated approach to education in identity domains such as internet, telecommunications, citizens-eIDs, Travel, Health etc.

5. The EC should stimulate faster mobile eID and mobile signature take-up by rewarding fast adoption.

6. The EC should ensure that all citizens are able to access eGov services via mobile devices regardless of contractual relationship with mobile providers (similar to emergency calls).

3 Harmonizing Attribute Management and Exchange

The management and exchange of certified attribute grows considerably in importance: attribute assurance may in fact become the commercially most important area in digital identity management, with significantly more applications than those focussing on "identification". Attribute management poses several new challenges that have not yet been comprehensively addressed. These challenges include standardization [TBMS14, VPSK12], procedures and assurance measures for linking attributes to existing eIDs [MC12, STO13], managing hierarchies and dependencies in sets of attributes [AFNT04, ACN$^+$02, TV97, TV99], verification of certified attributes, revocation, interoperability including semantic interoperability, privacy, attribute exchange/trade vs. user control and minimum disclosure. Public-private cooperation is highly desirable in the management and exchange of certified attributes.

Both public and private sector play important roles as attribute providers as well as relying parties. Close cooperation is therefore required to obtain user- and privacy friendly solutions across both sectors. Users need to be educated about user control mechanisms and the impact of attribute trade. A sensitive topic is the linking of attributes (including unique identifiers) to eIDs which can - also from the user's perspective - be useful in certain situations and undesirable in others depending on the context.

3.1 Attribute management recommendations

1. Linking: The EC should support the development and evaluation of procedures for linking attributes to eIDs while paying close attention to privacy threats.

2. Harmonization: The EC should initiate or revitalize the decision processes towards a harmonization of attribute semantics (semantic interoperability) and legal value.

3. Standardization: The EC should act on the need for standardization in the attribute management area; organize workshops and projects that bring together stakeholders to initiate standardization. The need for standards should be clearly communicated to policy makers.

4. Privacy: The EC should develop a normative framework to balance the user's right to privacy with the need of online service providers/e-government services to use, process and exchange user attributes. Attention should be paid on how this can be done adequately in an interoperability scenario. Special attention should be paid to attribute trade and reputational/behavioural attributes that are generated through the use of online services (like ratings on ecommerce websites).

5. Verification: The EC should study and evaluate procedures for efficient attribute verification. Appropriate mechanisms (technical and procedural) to ensure accountability and dispute resolution should be developed and implemented.

6. Dialogue: The EC should build on the interest in certified attributes by many e-commerce and industry stakeholders to gain their attention for the goal of creating a European eID ecosystem.

4 Rationalizing the choice of authentication assurance

Currently authentication is achieved by a variety of means. Authentication assurance frameworks are well established and understood (e.g. Stork QAA and NIST) and a number of relevant standards are available or under development [ITU08, ISO11a, ISO11b, ISO11c, ITU13, ISO13, ISO12a, ISO12b, ISO]. Many authentication assurance frameworks focus on traditional two factor authentication, but new data-enabled and probabilistic approaches to authentication are being developed. There are also approaches that allow levelling up an authentication method for example to allow a social networking ID to become higher assurance. The private sector seems open to alternative authentication technologies, especially those which offer reduced deployment and management costs.

At this stage it is unclear how effective these approaches are in reducing the cost of identity management and improving privacy. Further it is difficult to compare and assess such methods when mediating between different trust domains. Future standards therefore should not push a particular solution but should enable interoperability. New approaches to authentication need to support a wide range of uses and contexts and must work for small and large organizations while considering usability and user convenience as key factors [SSE12a].

4.1 Authentication recommendations

1. The EC should promote the establishment of an appropriate, easy-to-use framework for the assessment of authentication technologies including alternative authentication methods (so that they can be exploited where appropriate or discounted where not suitable.)

2. The EC should strongly promote internationally the establishment of an interoperability framework for authentication based on results and experiences like the ones provided by STORK, FutureID and other European projects on electronic identification.

3. The EC should encourage the development of services that are usable by the average citizen and complement this with appropriate education.

5 Liability

The issue of liability is fundamental for the usability of identity information since it plays a critical role in establishing trust. Assessing the assurance of identity information is closely tied to the associated liability. SSEDIC found that the European eIDAS regulation [Com12] as originally proposed was unclear with regard to important aspects regarding liability provisions [SSE12d]. The recommendations below point to some critical issues that must be addressed to create a viable liability framework for digital identity management in the EU. Some of the suggestions have been taken up in part in the position adopted by the European Parliament on April 3, 2014 [Par14]. Others should be considered in the delegated and implementing acts of the regulation.

5.1 Liability recommendations

1. Liability provisions in the eID and Trust Services Regulation need to be revised and updated, taking into account the different roles of identity providers in the Member States, who can be either public or private sector entities. It may therefore be necessary to consider separating the liability of Member States from identity providers, as they may be separate entities.

2. The liability provisions in the eID and Trust Services Regulation need to be reviewed to ensure that they are clear with respect to liability limitations and any possibility of liability caps. Various options are possible, ranging from no liability, unlimited liability to explicitly specifying liability caps in terms of financial amounts (possibly linked to eID quality levels); this topic must be carefully considered. The primary requirement is that liability implications are clear to anyone who relies on the trustworthiness of identities covered by the Regulation.

3. If EC policies on electronic identification intend to cover attribute provision as well (i.e. including in cases where end users will not be personally identifiable on the basis of the provided identity information), then a legal framework needs to be defined that also covers the responsibilities and liabilities of attribute providers. The currently proposed Regulation does not do this.

6 Implementation of recommendations

For the implementation of these recommendations SSEDIC suggests to consider the following aspects.

6.1 Stakeholder involvement

SSEDIC urges the European Commission to involve stakeholders from a wide range of sectors including the internet, telecom, finance, travel, postal services as well as the European Union Member States. In all these areas eID solutions are being developed or are in use which enable transactions in many societal domains like healthcare, finance, work and income, commerce and free movement of EU citizens.

6.2 Local adoption

The adoption of eID solutions for e-government and small businesses at the local level has too often been neglected. Residents have much more frequent interaction with local entities and businesses than with regional or national agencies. However, at the local level sufficient technical competence is not necessarily available, and often expensive changes to back-office procedures are required which do not generate immediate financial payoffs. Especially municipalities and small businesses often lack the required financial and human resources to broadly implement even national eID solutions. Being prepared to accept credentials issued cross-border is an even tougher challenge and will likely be more expensive than cost saving for many small cities even in the long term.

6.3 International Cooperation and Standardization

European activities should further actively seek to engage with related efforts in other parts of the world like NSTIC/IDESG in the United States and the eID programs in Asia. Participating and obtaining a distinct voice in the world-wide dialogue on eID was found to be essential for the success of the SSEDIC project as well. SSEDIC recommends that representatives of past, ongoing (like STORK, STORK 2.0 and in particular e-SENS), and future EU projects send representatives to standardization organizations to explain and promote their technical results. These representatives should not only explore the relation between results of their projects and existing or evolving standards but also take an active lead in developing new standards and make all the necessary efforts to make a contribution to shape those standards already in discussion.

6.4 The end user

Over the course of the last 3 years, SSEDIC has conducted two large surveys on user attitudes towards eID and use of eIDs [SSE11, SSE12b]. Taking a step back from the results and asking what might be particularly noteworthy characteristics of the respondents to the survey we find that end users are

- Sceptical: expect to see clear benefits from the use of eID technologies
- Convenience seeking: use convenient, readily available tools (also in a professional environment) even if they have experienced or are aware of some associated security issues
- Internationally oriented: engage in cross-border online commerce and banking transactions
- With high expectations: expect their national governments and the EU to take action towards improving the current situation and to ensure cross-border usability of eIDs not only for public but also for private sector applications

These attitudes should be carefully considered when proposing digital identity management solutions to citizens.

7 Conclusion

The SSEDIC recommendations presented in this paper point to required actions in key areas that are essential to provide interoperable and convenient digital identity management solutions in a seamless digital Europe. The SSEDIC network has consciously decided to focus its recommendations on the four key areas shown in figure 1 to give an appropriate weight to its recommendations and the important consensus reached.

However, the SSEDIC thematic network has worked on other areas relevant for digital identity management and produced more than 20 white papers on eID and its use within the EU which contain important background material and further recommendation for specific eID related challenges for example in the areas of criminal justice, dematerialization, education, and business models. For an complete overview we refer the reader to ref. [SSE12c].

The European Union and its Member States are strongly encouraged to act on these recommendations as a high priority in a fast changing world-wide environment. While the eID programs in most European member states are government driven and focus on e-government applications other countries like the United States [Hou11] strive to enable the private sector to provide eID services. The private sector might be able to incorporate technological advances faster and be more sensitive to usability than government lead programs. However, if private sector applications should become the standard, governments run the risk of losing digital sovereignty to private service providers, identity providers and possibly to the governments in which jurisdiction these service providers are based. Other emerging risks include the requirement of mandatory authentication (explicit or implicit) where it is not strictly required leading to attribute aggregation and surveillance. These threats become particularly relevant in context of geo-tagging/tracking and in e-health related areas. The SSEDIC recommendation shall support the EU in recognizing, addressing, and overcoming such challenges.

The EU funded SSEDIC project concluded its work but many challenges as the ones mentioned above remain and require continuing efforts by think-tanks such as SSEDIC. The network SSEDIC created is prospering and will continue to grow as SSEDIC.2020. SSEDIC.2020 will expanding on existing SSEDIC themes, support the implementation of the SSEDIC recommendations, providing advisory and project validation services and promoting international liaison and knowledge sharing.

8 Acknowledgments

The authors would like to thank the entire SSEDIC community for their thoughtful work in drafting the SSEDIC recommendations presented in this paper and in particular Roger Dean, Hugo Kershot, and Jon Shamah as members of the SSEDIC management team and Eric Blot-Lefevre, Hans Graux, Jaap Kuipers, Herbert Leithold, Steve Pannifer, and Heiko Rossnagel for leading work streams and workshops that directly contributed to the development of these recommendations.

References

[ACN$^+$02] Franco Arcieri, Elettra Cappadozzi, Paolo Naggar, Enrico Nardelli, and Maurizio Talamo. Coherence maintainance in cooperative information systems: the Access Key Warehouse approach. *International Journal of Cooperative Information Systems*, 11:175–200, 2002.

[AFNT04] Franco Arcieri, Fabio Fioravanti, Enrico Nardelli, and Maurizio Talamo. A layered IT infrastructure for secure interoperability in Personal Data Registry digital government services. In *Research Issues on Data Engineering: Web Services for e-Commerce and e-Government Applications, 2004. Proceedings. 14th International Workshop on*, pages 95–102. IEEE, 2004.

[Axe84] R. Axelrod. *The evolution of cooperation*. Basic Books, New York, 1984.

[Che05] Ramnath K Chellappa. Consumer's Trust in Electronic Commerce Transaction, Los Angeles, CA, University of Southern California, Marshall School of Business, 2005. 2005.

[Com12] European Commission. Regulation on electronic identification and trust services for electronic transactions in the internal market; available at http://eur-lex.europa.eu, 2012.

[Hou11] The White House. National Strategy for Trusted Identities in Cyberspace; available at http://www.nstic.gov, 2011.

[ISO] ISO/IEC. Information technology - security techniques - a framework for access management. Technical Report ISO/IEC CD 29146:Under Development, International Organization for Standardization, Geneva, Switzerland.

[ISO11a] ISO/IEC. Information technology – security techniques – a framework for identity management – part 1: Terminology and concepts. ISO/IEC 24760-1:2011, International Organization for Standardization, Geneva, Switzerland, 2011.

[ISO11b] ISO/IEC. Information technology – security techniques – a framework for identity management – part 2: Reference architecture and requirements. ISO/IEC 24760-2:2011, International Organization for Standardization, Geneva, Switzerland, 2011.

[ISO11c] ISO/IEC. Information technology – security techniques – a framework for identity management – part 3: Practice. ISO/IEC 24760-3:2011, International Organization for Standardization, Geneva, Switzerland, 2011.

[ISO12a] ISO/IEC. Information technology – security techniques –identity proofing. Technical Report ISO/IEC WD1 29003:2012, International Organization for Standardization, Geneva, Switzerland, 2012.

[ISO12b] ISO/IEC. Information technology - security techniques - requirements for partially anonymous, partially unlinkable authentication. Technical Report ISO/IEC 29191, International Organization for Standardization, Geneva, Switzerland, 2012.

[ISO13] ISO/IEC. Information technology – security techniques – entity authentication assurance framework. Technical Report ISO/IEC 29115:2013, International Organization for Standardization, Geneva, Switzerland, 2013.

[ITU08] ITU. Information technology - open systems interconnection - the directory: Public key and attribute certificate frameworks. Technical Report ITU-T X.509, International Telecommunication Union, Geneva, Switzerland, 2008.

[ITU13] ITU. Framework for discovery of identity management information. Technical Report ITU-T X.1255, International Telecommunication Union, Geneva, Switzerland, 2013.

[KRS] Michael Kubach, Heiko Roßnagel, and Rachelle Sellung. Service providersâ requirements for eID solutions: Empirical evidence from the leisure sector. In *Gesellschaft für Informatik eV (GI), Bonn: Open Identity Summit 2013 : 10.-11.09.2013, Kloster Banz, Germany*, page 69.

[MC12] Talamo M. and Schunck C.H. Re-thinking the Evaluation of eID Credentials to Simplify Interoperability. *European Journal of ePractice*, 14:51–62, 2012.

[Par14] European Parliament. European Parliament legislative resolution of 3 April 2014 on the proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; available at http://www.europarl.europa.eu, 2014.

[RZHM14] Heiko Roßnagel, Jan Zibuschka, Oliver Hinz, and Jan Muntermann. Usersâ willingness to pay for web identity management systems. *European Journal of Information Systems*, 23(1):36–50, 2014.

[SSE11] SSEDIC. SSEDIC eID adoption survey, SSEDIC Deliverable 2.3.1; available at http://www.eid-ssedic.eu/deliverables.html, 2011.

[SSE12a] SSEDIC. Consumer Facing Authentication Assurance, SSEDIC Deliverable 4.2.1; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[SSE12b] SSEDIC. SSEDIC 2012 eID adoption survey 2.3.2; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[SSE12c] SSEDIC. SSEDIC recommendations & roadmap, SSEDIC Deliverable 6.3; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[SSE12d] SSEDIC. A summary swot analysis for eid in europe under the proposed regulation, SSEDIC Deliverable 5.2.1; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[STO13] STORK2.0. STORK2.0 Deliverable 3.2; available at https://www.eid-stork2.eu/, 2013.

[TBMS14] Maurizio Talamo, Maria Laura Barchiesi, Daniela Merella, and Christian H Schunck. Global convergence in digital identity and attribute management: Emerging needs for standardization. In *Proceedings of the 2014, ITU Kaleidoscope Academic Conference: Living in a converged world-Impossible without standards?, St. Petersburg, Russia,10.1109/Kaleidoscope.2014.68584752014*, pages 15–21. IEEE, 2014.

[TV97] Maurizio Talamo and Paola Vocca. A data structure for lattice representation. *Theoretical Computer Science*, 175(2):373–392, 1997.

[TV99] Maurizio Talamo and Paola Vocca. An efficient data structure for lattice operations. *SIAM journal on computing*, 28(5):1783–1805, 1999.

[VPSK12] F Veseli, P Paillier, J Schallabock, and I Krontiris. D8.4 architecture for standardization v1; available at http://www.ec.europa.eu, ABC4Trust, 2012.

Secure and trustworthy file sharing over cloud storage using eID tokens

Eduardo Duarte, emod@ua.pt [1], Filipe Pinheiro, filipepinheiro@ua.pt [2], André Zúquete, andre.zuquete@ua.pt [3], and Hélder Gomes, helder.gomes@ua.pt [4]

[1]University of Aveiro
[2]University of Aveiro
[3]DETI/IEETA, University of Aveiro
[4]ESTGA/IEETA, University of Aveiro

Abstract: This paper presents a multi-platform, open-source application that aims to protect data stored and shared in existing cloud storage services. The access to the cryptographic material used to protect data is implemented using the identification and authentication functionalities of national electronic identity (eID) tokens. All peer to peer dialogs to exchange cryptographic material is implemented using the cloud storage facilities. Furthermore, we have included a set of mechanisms to prevent files from being permanently lost or damaged due to concurrent modification, deletion and malicious tampering.

We have implemented a prototype in Java that is agnostic relatively to cloud storage providers; it only manages local folders, one of them being the local image of a cloud folder. We have successfully tested our prototype in Windows, Mac OS X and Linux, with Dropbox, OneDrive, Google Drive and SugarSync.

1 Introduction

In recent years we assisted a widespread usage of cloud storage for centrally storing personal files (e.g. Dropbox). Such cloud storage can either be used for personal benefit or for sharing information with others. In this last case, cloud storage providers manage the mechanisms to send sharing invitations and to keep the shared files synchronized among all the hosts effectively using them. To ease the usage of such shared folders, storage providers enable users to use in their hosts specific software to handle a mount point in the local file system to access cloud folders.

In this paper we propose a system, **Protbox**, for securely sharing files among strongly authenticated people through many different cloud storage services. The secure sharing includes four different protection features: (i) confidentiality, to prevent non-authorized readings, (ii) integrity control, to detect malicious tampering, (iii) protection against unwanted file removals, either by malicious or legitimate persons, and (iv) access control to the shared data based on strong identification and authentication of people, using the nowadays widespread electronic, personal identity tokens (eIDs for short).

Many governments worldwide have been or are introducing eIDs to allow the identification of people in the scope of Internet interactions. Unfortunately, there are several kinds of eID types being deployed, which reduces the possibilities of using all of them in a single system requiring the authentication of persons. In our system we considered the case of the Portuguese eID (Cartão de Cidadão), which enables the owner to perform two kinds of signatures upon providing a proper PIN: (i) authentication signature, for online identity proofs and (ii) qualified signatures, for document signing. In this work we used only authentication signatures.

Comparing Protbox with similar solutions, it has two main distinctive characteristics: (i) the key distribution between file sharing persons is performed by means of special files exchanged through the exact same cloud storage space used for file sharing, thus no extra services are required other than the trustworthy national PKIs (Public Key Infrastructures) used to validate eID signatures; and (ii) the files exposed to others by means of cloud sharing are protected from malicious or involuntary tampering or removal.

Protbox has just two requirements regarding a cloud storage solution for folders and files: (i) it should allow the sharing of folders by many persons and (ii) it should allow client operating systems to have a local mount point of the shared folder. Nowadays, most file-oriented cloud storage solutions, if not all, fulfill these requirements; in our experiments we managed to explore it successfully with Dropbox, SkyDrive, Google Drive and SugarSync (see Section 3).

We developed a Protbox prototype in Java. It runs in any operating system with a suitable Java Virtual Machine (JVM) and is capable of recognizing any file system. It features a background folder synchronization engine and a graphical user interface for dealing with key distribution requests. Protbox randomly generates and uses a key per folder to protect all its contents, including files and sub-directories. Files are encrypted with AES and their integrity is ensured with HMAC-SHA1. Encrypted file names, which contain bytes that are not acceptable for naming files in existing file systems, are coded in a modified Base64 alphabet, which should work in most file systems. The prototype was successfully experimented in Windows, Mac OS X and Linux with all of the above referred cloud storage providers.

2 Protbox architecture

2.1 Deployment overview

Protbox depends on the local replica of **Cloud Folder**, which we call **Shared Folders** for the effective sharing of protected content. Users must define one-to-one associations between those Shared Folders and the local folders containing the relevant files to protect, which we call **Prot Folder** and may be located anywhere in the host file system. The cloud storage system will be responsible for synchronizing the contents of Shared Folders with the correspondent Cloud Folders, which may be shared by a set of cloud storage users. This cloud synchronization is completely transparent to Protbox, which only has to deal with the local synchronization between associated Shared Folder - Prot Folder pairs (see

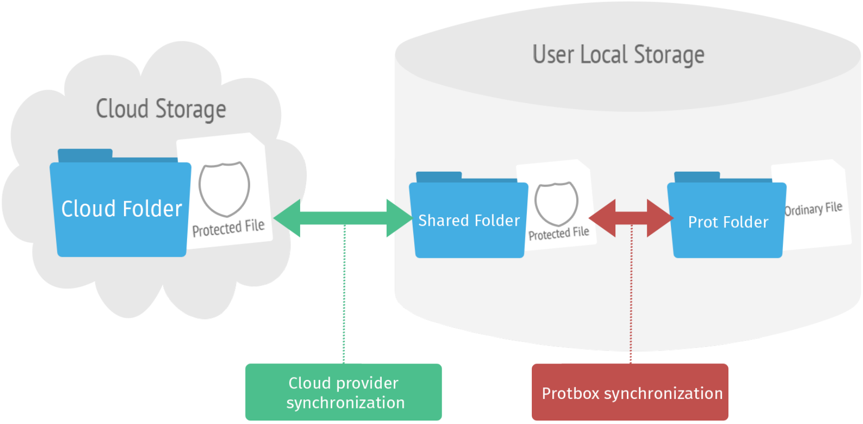


Figure 1: Overview of the Protbox deployment architecture. The Protbox synchronization will take place upon Protbox Pairs, which are pairs formed by one Shared Folder and a Prot Folder.

Figure 1). We will refer such pairs as **Protbox Pairs**.

The Protbox synchronization actions are not simple file copies, but rather content encryptions (when updating files in a Shared Folder) or decryptions and integrity validations (when updating a Prot Folder). Files in a Prot Folder are in their original formats, as produced by the creating applications, but their protected replicas in Shared Folders and Cloud Folders are encrypted, ensuring their confidentiality. The file names of the encrypted files are also encrypted to reduce the leakage of file-related information through the cloud provider.

2.2 Integrated file protection

Protbox attempts to introduce and build a confidential, trustworthy and dependable environment on top of existing cloud storage services without disrupting normal usage and functionality provided by these.

For confidentiality, Protbox encrypts files with a symmetric cipher (e.g. AES). A key is generated and maintained for each Protbox Pair (hereafter we will call it a **Pair Key**). Pair Keys are stored by Protbox in its private, local data repositories and not stored in the cloud. Each Pair Key is either (i) randomly generated by Protbox (when the first protected file is created in the corresponding Shared Folder) or (ii) imported by Protbox from other users sharing the corresponding Shared Folder (when the Shared Folder is not empty). Besides file's contents, their names are also encrypted with the same key and written in a modified Base64 alphabet.

For trustworthiness, file updates in Shared Folders must also be validated taking the corresponding Pair Keys into consideration: an update can only be accepted if it was made by someone knowing the correct Pair Key. Otherwise, tampered files in Shared Folders could originate files with garbage contents in Prot Folders. Therefore, protected files contain a cryptographic checksum, computed with their Pair Key (e.g. with HMAC-SHA1).

Considering a hierarchical rank of power, a Prot Folder outranks its corresponding Shared Folder, thus a Prot Folder file cannot ever be permanently damaged or deleted upon a synchronization event originated from the cloud provider (regardless of the ultimate origin of the event). Therefore, for dependability the files in each Prot Folder should always be available for restoring at any time, regardless of the cloud provider's interpretation of the files' status.

The coherence of the files in both of these folders (Prot Folders and Shared Folders) is assured by maintaining a parallel control data structure containing structural information about both folders (files and directories, encrypted and decrypted names, last modified dates, lengths of contents). Coherency checking and synchronization tasks would run on a periodic basis and use that structural information and the effective contents of each Protbox Pair to take the appropriate data transfer decisions. Hereafter we will refer to this structural information as **Protbox Registry** (**PReg** for short). Pair Keys are also part of PReg.

Note that a PReg is a local, private data structure that helps a local Protbox instance to take the appropriate, local decisions regarding file synchronizations, encryptions/decryptions and recovery actions. In particular, a PReg is never synchronized with another one.

Because we are essentially dealing with asynchronous copies of files from one folder to another, with encryption and decryption of contents and file names depending on which folder the file is placed, concurrent file update conflicts can occur. These file conflicts can be detected because the synchronization method uses the PReg to evaluate each situation prior to the synchronization itself. On each run of the coherence checking task we create a index of the files updated (i) only in the Prot Folder, (ii) only in the Shared Folder and (iii) in both folders. The last ones are our subject of interest in what concerns conflicts. Consequently, they will be synchronized in a different way, which will lead to the production of two versions of the updated file, while the other files will be synchronized in a straightforward way. This feature also adds dependability to Protbox, because it assures that conflicting updates are never destructive.

2.3 Agnosticism and autonomy towards cloud storage providers

Some cloud storage solutions do not provide any cryptographic measures to protect the files they store (e.g. Microsoft's OneDrive[1]). Other solutions implement security mechanisms to back up and encrypt files, both in transit and at rest (e.g. Dropbox[2]), rendering the service HIPAA-compliant[3]. However, they cannot guarantee that stored files are only

[1] http://answers.microsoft.com/en-us/onedrive/wiki/sdfiles-sdperms/onedrive-and-data-encryption-is-your-data-secured/43ff303b-a6aa-4f02-8c47-b547d6a5ef14

[2] https://www.dropbox.com/help/27/en

[3] http://onr.com/secure-server-hosting/what-is-hipaa-compliance/

decrypted by user request, since the symmetric encryption keys used are managed by the cloud storage providers. To emphasize the safeguard of files, some providers claim they have strict privacy policies that prohibit company's employees from viewing the content of stored files (e.g. Dropbox[4]), but while this may be a deterrent measure, it does not effectively prevent it from happening[5].

By realizing this, we designed Protbox as an agnostic solution regarding cloud storage providers, being independent of both (i) how they store and transfer files and (ii) how they implement confidentiality and authentication mechanisms [BHH$^+$12]. For Protbox the only requirements from cloud storage providers are the availability of what we called a Shared Folder, a replica available in the local file system of a Cloud Folder, and the synchronization of contents between several Shared Folders for the same Cloud Folder.

Other than the cryptographic methods adopted in order to establish a confidential environment, it was equally important that Protbox allowed users to share protected files with each other. Access to the original contents of protected files by a user should be controlled within Protbox, regardless of who effectively has access to the Cloud Folder, as determined by the cloud-storage provider. To do so, Protbox implements request-response dialogs between Protbox instances for exchanging Pair Keys associated to Shared Folders. These dialogs are implemented with special files stored in Shared Folders. When a Protbox instance first establishes an association between a Prot Folder and a Shared Folder, if the Shared Folder is populated with files then it sends a request to obtain the key to decrypt them. Such a request will be available to all Protbox instances with Prot Folders associated with replicas of that Shared Folder, and any of them (upon a user consent) may send a response with the requested key. This way, Protbox is completely autonomous regarding key distribution, it does not require any external key distribution service.

2.4 Synchronization of Protbox Pairs

Protbox allows the user to configure a arbitrary number of local Prot Folders to be securely shared by means of Protbox Pairs. This means that it must be able to properly synchronize data between the Prot Folder and the Shared Folder that form each Protbox Pair. In addition, while useful metadata provided by native file systems can be used to detect updates and synchronization details, it does not contain enough information, such as an history of modifications and deletions, to properly deal with conflicting scenarios. Therefore, we cannot fully depend on the native file systems for tacking synchronization decisions.

Consequently, each Protbox instance uses PReg for this task. For each Protbox Pair the PReg stores its Pair Key and information to detects differences between the Pair's Prot Folder and Shared Folder: (i) encrypted and decrypted names of each file of the Pair, (ii) last modification date, (iii) file length and (iv) file's cleartext contents. For the Pair's directories only the names are stored.

[4] https://www.dropbox.com/privacy

[5] https://www.pcworld.com/businesscenter/article/260254/dropbox_gets_a_black_eye_in_spam_attack.html

It should be possible to have two or more Protbox Pair for the same Prot Folder; it enables to share the same Prot Folder through several cloud providers, using a different Pair Key for each of them. However, the contrary should be impossible: a single Shared Folder cannot be used by more than one Protbox Pair. The reason for this is that all the contents of a Shared Folder must be protected with a single Pair Key.

Each encrypted file name results from the encryption of the original name with the Pair Key, encoded in a modified Base64 alphabet. In this alternative alphabet we replaced the "/" symbol, which is very often used as a path separator, by "-" (hyphen). For the encryption/decryption operations we chose the ECB mode and PKCS #5 padding. The padding helps to hide the real length of the original name.

Protbox monitors the folders of each Pair to detect modifications relatively to the PReg information. When the modification corresponds to a file insertion in one of the folders, a new entry is inserted in PReg and the file is replicated in the other folder with the appropriate encryption or decryption transformation.

When the modification corresponds to a removal of a file or directory, they are similarly removed from the other folder but not from PReg, where they become marked as hidden. Furthermore, in the case of files removed in the Shared Folder, the cleartext replica in the Prot Folder is stored in PReg along with the hidden entry prior to removing them from the file system, thus enabling Protbox to restore them afterwards upon a user request.

When the modification corresponds to an update of a file in only one of the Pair's folders, in practice for Protbox it corresponds to a combined removal of the file and insertion of a new one in that folder. Upon both these steps, all the parties sharing the same Cloud Folder with Protbox that receive a new encrypted version of a file will store the old (cleartext) replica in their PReg.

When the modification corresponds to an update of the same file in both folders of a Pair, then we have a conflict. In this case, Protbox renames the file in the Prot Folder to include the name of the local user. Then, it considers both the renamed file and the updated file in the Shared Folder (which are no longer linked) as independent file insertions. The overall, distributed outcome of this operation may not be always the same, since several Protbox instances may compete in this process, in different hosts, without central coordination. Nevertheless, no files are lost, since these files are never deleted by Protbox.

2.5 Identification and authentication of users

For supporting well-informed decisions by Protbox users to respond positively to Prot Folder key requests we had to choose a method for identifying and authenticating Protbox users. We decided to use national eID tokens to achieve both goals, by using their X.509 authentication certificates and their public keys to validate signatures on Pair Key requests and responses, signed with the corresponding private keys.

By using national eIDs, the access to protected files shared through the cloud only occurs after a two-factor authentication: the possession of the eID token and the knowledge of a personal identification number (in order to unlock the token's cryptographic functionalities). This way, the risk of personification by others, namely cloud storage providers, is dramatically decreased.

In our protection model we didn't consider the hiding of the users' identity, expressed in signatures performed with their eID, from the cloud storage providers. Therefore, these providers can obtain the real identity of the persons exchanging secure files with Protbox. Dealing with this security issue is a topic for future work.

2.6 Key Distribution

For the distribution of Pair Keys to individual persons sharing the same Cloud Folder via Protbox we designed a protocol based on the exchange of special files through the Cloud Folder. These special files, which are not engaged by Protbox synchronization functions, are identified by starting with "_", which does not belong to our modified Base64 alphabet.

A Protbox instance places a Pair Key request in the Cloud Folder when it needs it to properly decrypt the contents of a related Shared Folder. The request contains an encryption public key (belonging to a **Key Distribution Key Pair**, **KDKP**) signed by the requester. This public key should be used by anyone knowing the Pair Key to send it back to the requester. The signature is made with the eID authentication private key, and the corresponding certificate should go along with the request.

A Pair Key request file has a name that is formed by a leading "_" and an hexadecimal representation of a 128-bit random number. This number is generated by the requester and will be used to match the Pair Key response. Several persons can place simultaneous requests in the same Cloud Folder, the probability of collision is nearly null. A Pair Key response will have a similar file name, but with an additional extension formed by an hexadecimal representation of another 128-bit random number. This number is generated by the responder and allows many persons knowing the Pair Key to respond without colliding.

Whenever a Protbox instance detects a Pair Key request in a Shared Folder for which it knows such key, it checks the request signature and presents the identity of the requester to the local user, prompting for key distribution authorization. Upon the user authorization, the Pair Key is ciphered with the requester public key and the response is signed with the eID of the responder. The goal of this signature is twofold: (i) it allows the requester to know who provided the Pair Key and (ii) it prevents anonymous attackers from injecting tampered responses in the Cloud Folder. Note that we cannot prevent Denial-of-Service (DoS) attacks against the key distribution protocol (attackers may be able to tamper or delete Pair Key requests and responses), but we can prevent Protbox users from being mislead by anonymous attackers providing wrong Pair Keys. We can still have attacks providing wrong Pair Keys, but since the responses are signed, they are not anonymous.

Pair Key responses are signed tacking into account the request, i.e., the signature is made upon a hash including the original request (file name and contents). This way, responses cannot reused, which is advisable to prevent users to be fooled by replayed responses.

Pair Key requests and the corresponding responses are deleted upon successfully processing a response. It may happen, however, that some responses may be placed in the Cloud Folder after the deletion of the request. In this case, lost responses (easily detected because they have no counterpart requests) can be deleted by anyone sharing the Cloud Folder after an acceptable timeout upon detection of the incoherence.

In our protection we didn't consider any mechanism to revoke accesses to files in a Shared Folder. Ultimately, this needs to be explored at the sharing service provided by the storage provider. Furthermore, we assumed that each person with access to a Shared Folder can provide a Pair Key response to a key pair request for that folder. More restrictive response politics (e.g. only one participant is allowed to respond) must be managed at a higher level with some form of personal agreement. Dealing with such policies is a topic for future research.

2.7 Management of file content restoration

As previously mentioned, each time a Shared Folder file is updated, the corresponding file in the Prot Folder is updated accordingly and a backup copy of the replaced file contents is created. With this basic behavior, files shared among several users by means of Protbox that go through many small updates are likely to create long lists of backup contents in many Protbox instances.

To deal with this issue, Protbox instances offer different policies for managing the backup of updated files, such as: (i) never keep a backup copy (ii) limit the number of backups to a maximum number of copies (iii) ask the user each time a backup copy is to be made. Because files have different relevancy levels, these policies can be deployed on a per file basis.

3 Prototype implementation and experience

A prototype implementing all the features specified in the architecture was developed using Java, and is available as a open-source project at `https://github.com/edduarte/protbox` . Aspects like Java's native file system recognition were used in order to emphasize maximum compatibility. Moreover, because it runs on any implementation of the Java Virtual Machine, it is compatible with popular operating systems, such as Windows, Mac OS X and Linux. Licensed third-party libraries that were used for the development of this prototype (SwingX, ImageJ, JGoodies, Apache Commons, Guava) are all freely distributed and open-source.

Each Protbox instance uses a different PReg for each local user and uses the user's home directory to store it. The PReg is formed by a directory for storing backed up files and an encrypted file containing a serialized Java data structure with all the user's Protbox metadata. This file is encrypted with AES in ECB mode with a key derived from a user password. This file keeps the user's KDKP and the random identifiers used in his Pair Key requests; KDKP is generated by Protbox on the first execution.

Pair Key requests are produced by Protbox instances at most once on each run, since they can be reused for different Shared Folders (while stored in request files with different names, for preventing response replay attacks). This way, the user signature with his eID for producing a Pair Key request is required at most once each time his Protbox runs. Note, however, that the user may be asked to make other signatures with his eID, namely for producing Pair Key responses.

During start-up, our prototype checks for configuration files added by the user, which should specify the local path of a eID token PKCS#11 provider and the alias of the authentication certificate contained within said eID token. With this, Protbox allows dynamic support for any national eID token to sign Pair Key requests and responses.

Protected files always start with an integrity control value. After that, they may contain an optional initialization vector for an encryption mode (e.g. CBC). Finally, they have the actual file contents encrypted. The cipher algorithms used for protected files are defined independently for each Shared Folder. The person that decides it is the same that defines its Pair Key, which is the first that creates a protected file on it.

Pair Key requests' and responses' signatures contain the complete certificate chain of the signer's certificate, excluding the root certificate. This facilitates the validations of the signatures, at the cost of adding more data to those files. But since they are transient, this is not an issue. Besides the Pair Key, a response also contains the names of the cryptographic algorithms that are being used to protect the files in the Shared Folder. For such names we used the strings that are actually used to instantiate cipher objects using the Java Cryptography Algorithm factory model. Examples of such strings are "`AES/CBC/PKCS5Padding`" for a symmetric encryption cipher and "`HmacSHA`" for computing an integrity control value.

The prototype was tested in Windows 7, Ubuntu 12.04.4 and Mac OS X Mavericks 10.9.4 operating systems with four of the current major cloud storage providers on the market: Dropbox, Google Drive, Microsoft OneDrive and SugarSync. Multiple tests were performed to check if the provider's synchronization methods displayed considerable loss of performance, since file encryption is known to interfere with the provider's synchronization techniques [Gee13]. Tests included (i) the creation of a single and of multiple files in a Prot Folder, (ii) sharing of a Pair Key between several persons, (iii) simultaneous creation of files in different Prot Folders in different hosts for the same Cloud Folder, (iv) detection of tampered files in Shared Folders and (v) file deletion detection and (vi) recovery of deleted files. Unfortunately, it is impossible to describe here all the interactions with the users that are triggered within many of these tests.

Under normal conditions, the prototype executed every task successfully with all of these providers and presented no distinguishing differences between them in terms of behavior. Under conditions where the cloud storage service's permissions features could be set, when reducing the users' permission from "read/write" to "read-only", Protbox could not cope with it, since it could not even post a Pair Key request in the Shared Folder. However, since Protbox is by design agnostic from specific features provided by cloud storage providers, such as this file protection mechanism, this is an expected limitation.

4 Related Work

In this section we will give an overview of features present in other existing cloud storage security solutions, implemented as third-party software applications, and effectively compare the overall operations and design of these against Protbox. The analyzed solutions are BoxCryptor[6], Viivo[7], CloudFogger[8], Sookasa[9], TrueCrypt[10] and CCE (Citizen Card Encrypted) [ZSTD13].

Similarly to Protbox, all of these solutions encrypt files from the installed cloud service with locally generated 256-bit AES keys. As an added effort, Protbox implements integrity checking of encrypted files to prevent files with garbage from being produced in Prot Folders of peers. This feature could not be found in the documentation of any of the analyzed solutions, though it may be in place.

With BoxCryptor and TrueCrypt, plaintext replicas of encrypted files are maintained in a local virtual disk drive that is created in the user host, which requires a strong integration with the operating system kernel of the user machine. Other solutions, such as Viivo and Sookasa, detect a set of well-known, locally installed cloud storage providers, and are limited to encryption of a single folder (and its sub-files and sub-folders) at the target cloud storage service (naturaly, the local cloud replica). In contrast, Protbox integrates in a transparent way with the native file system and prompts the user to freely specify the cloud replica and prot folders that define a Protbox Pair, making it a more intuitive and flexible solution. In addition, this flexibility allows the configuration of multiple Pairs based on the same Prot Folder and different cloud replicas, introducing simultaneous synchronization and encryption of contents into multiple Cloud Folders, a feature that is not available in other works.

In regards to local protection, CloudFogger and Sookasa do not replicate files between two different local folders, instead encrypting and decrypting cloud folder files on-the-fly according to their actual local usage. Local files, placed at the cloud folder, are always encrypted, and are only decrypted to plaintext to the user when the user authenticates himself within the provided application [11] [12]. TrueCrypt's keeps a local mountable file with the encrypted files, which contents can only be accessed when TrueCrypt is running. Protbox, like BoxCryptor and Viivo, keeps the decrypted view (prot folder) available locally at all times, and because the established objective was to just protect files residing in the cloud folder, it does not have any local protection measures on the prot folder.

For the majority of these solutions, encryption keys and the sharing logic of these is handled within a backend platform available in a web server. Users must implicitly trust web server's safeguard. For example, in BoxCryptor, file sharing is targeted to individual files,

[6] https://www.boxcryptor.com/en/boxcryptor

[7] http://www.viivo.com

[8] https://www.cloudfogger.com/en/

[9] https://www.sookasa.com/

[10] http://www.truecrypt.org/

[11] http://support.cloudfogger.com/index.php?/\\Knowledgebase/Article/View/10/7/how-secure-is-cloudfogger

[12] https://sookasa.zendesk.com/hc/en-us/articles/200045197-How-do-I-encrypt-files-

where a random key is generated to encrypt every different file that can be shared with another single user or with a group of users. This key is then stored in the BoxCryptor Key Server and made accessible to the intended user or group. As security measures, these keys are encrypted with cryptographic material generated from the user's credentials and stored locally[13]. The remaining solutions allow the sharing of whole directories with specific users, generating an encryption key per directory and storing it in the application's backend servers, with access limited to those users. The encryption material relevant to file protection is said to be kept locally, without ever being transferred to these backend servers. This claim cannot be verified because they are not open-source. Protbox also bases its file encryption on whole directories, allowing the setting up of multiple simultaneous Pair sharing, but by structuring a whole key distribution protocol by transferring files in the shared folder, Protbox avoid the need to implement a sharing and encryption logic in a backend service.

The authentication paradigm for all of these solutions, except for CCE, is knowledge-based, using character-based credentials. These credentials identify different users and allow intuitive sharing of files, where a user can specify who should obtain access to encrypted files by stating the corresponding accounts. Protbox, in contrast, uses a strong ownership-factor authentication method based on national eID tokens to identify different users during sharing operations.

The usage of eID tokens for authentication in cloud-security was already used by CCE [ZSTD13]. CCE implemented file confidentiality by using the token's provided encryption and decryption mechanisms, which also means that they are dependent on these mechanisms being supported by the eID token. Many eID tokens, like the Portuguese Citizen Card, currently do not support such capabilities, hence cannot provide file confidentiality on their own. Protbox does not rely on national eIDs having these features. Instead, it only requires signature capabilities to allow verification of human identity by peers.

For a more controlled sharing protocol, Viivo proposes a mediator-based implementation where every shared folder has a user with 'moderator' privileges, which, by default, is the first user to attain access to said folder. New users must request for permission of access to the encrypted contents directly to the moderator, and this moderator must constantly check for and manage these requests. Since there is only one moderator per folder, this moderator must be familiar with all of the requesting users. With this, a user that is only known as trustworthy by single or a few users of the shared folder excluding the moderator will, more likely than not, have his request denied. With Protbox, every single sharing request is sent in a "multicast" fashion, and the requirements for one of these request to be accepted is to provide a valid certificate chain and a valid signature and to have at least one user accept such a request. The reason for our policy is that we don't have a central authority for controlling ownership rights over Shared Folders; everyone that has access to the Shared Folder is a peer with equal rights.

Finally, all of the available solutions place complete trust in the cloud storage provider's capacity of protecting files from illegitimate or unwanted deletions and the capability of backing up files to allow eventual restore of file contents. With that said, and in tune with

[13] https://www.boxcryptor.com/en/technical-overview#anc02

Protbox's intended agnosticism, intentional or accidentally deleted files can be recovered without depending on the cloud service provider's own mechanisms.

5 Conclusions

This paper proposed Protbox as a multi-platform solution for cloud storage security, where data confidentiality and sharing is performed with agnosticism and autonomy towards the cloud storage service provider. It adapts to the native file system and to existing cloud storage services without trusting nor requiring their capabilities other than the process of synchronization to the cloud. Features that might already be implemented by providers like data recovery are also provided by Protbox as an independent and secure way of restoring content without the provider's acknowledgement.

Regarding other similar existing solutions, Protbox does not store and manage user credentials in a central or distributed service in order to provide key sharing functionality. Instead, it uses the cloud environment and the synchronization of files on Shared Folders to enable peer-to-peer exchange of cryptographic material. In addition, while other solutions use convenient but weak password-based authentication measures to identify users, Protbox uses a strong eID-based identification and authentication paradigm exploring national eID tokens. The end result of this is that, while other cloud security solutions rely on transferring trust from the storage service systems to their own systems, with Protbox the user does not need to trust any additional services other than existing PKI infrastructures for eID exploitation.

Finally, Protbox protects the files shared through cloud storage from being deleted or damaged intentionally or accidentally. This is achieved by keeping local backup copies of files modified upon a modification triggered by the cloud provider.

References

[BHH+12] Moritz Borgmann, Tobias Hahn, Michael Herfert, Thomas Kunz, Marcel Richter, Ursula Viebeg, and Sven Vowé. On the Security of Cloud Storage Services. Technical report, Fraunhofer Institute for Secure Information Technology, 2012.

[Gee13] Stephen Geerlings. Measurements for the Paranoid: The Effect of Encrypting Files in Cloud Storage. 2013.

[ZSTD13] Bernd Zwattendorfer, Bojan Suzic, Peter Teufl, and Andreas Derler. Secure Hardware-Based Public Cloud Storage. *Open Identity Summit*, 2013.

Towards a privacy-preserving inspection process for authentication solutions with conditional identification

Felix Bieker, Marit Hansen, Harald Zwingelberg

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel, Germany
{fbieker|marit.hansen|hzwingelberg}@datenschutzzentrum.de

Abstract: Anonymous, yet accountable authentication solutions such as privacy-enhancing attribute-based credentials do not only provide various privacy features, but also contain an option of conditional identification of specific attributes of the user. While the technical functionality of this so-called inspection is available, it has not yet been examined how the inspection operation can be embedded in the organizational framework of a service provider and which inspection grounds have to be considered. This text proposes a model inspection process with clearly defined roles and workflows derived from legal obligations and guidelines from European primary law and the EU data protection regime. Thereby implementation of privacy-preserving authentication solutions in practice is facilitated, as it has been shown in a pilot of an online communication platform in a Swedish school.

1 Introduction[1]

Data minimization is one of the fundamental principles of privacy by design and also acknowledged in the European data protection framework, for instance in the discussion on a potential European General Data Protection Regulation. Under the current European Data Protection Directive 95/46/EC (in the following: DPD) the principles of necessity and proportionality demand minimization of personal data as far and as soon as possible. In many cases, e.g. when browsing the web, collection or storage of personal data would not be needed. Even when users have to authenticate, their identity information could often be omitted as long as proof is given that the users are authorized to access the resource. In the last years, several solutions for privacy-preserving authentication, guaranteeing anonymity of users and unlinkability of transactions, have been proposed (e.g. [Br00], [CL01]). Solutions such as privacy-enhancing attribute-based credentials (Privacy-ABCs) provide options for attribute selection and attribute aggregation by the user; they also support accountability by allowing conditional identification under specified circumstances [Kr13]. However, in order to unleash the full potential of

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust).

Privacy-ABCs these features must be implemented in a rights-centered way and with a view to the current and future legal concepts such as privacy by design.

Such technology is piloted in the EU-funded ABC4Trust project (www.abc4trust.eu), in particular in the online communication platform of a Swedish school, based on Privacy-ABCs, where students can securely discuss matters of class life. While there are forums (Restricted Areas) for political discussion, which are used fully anonymous, others are labeled as inspectable. Thus, content in violation of pre-defined inspection grounds can be reported and the relevant User(s) may be identified (see [BO13], pp. 11 and 41).

The challenge is to design the inspection process in a way that ensures it is not misused as a kind of "backdoor", but that it works in a controlled and transparent way. Only then can the full potential of Privacy-ABCs be realized. It is to be noted that use cases without the need of inspection should stick to full anonymity (which is also offered by Privacy-ABCs). However, the careless collection and storage of all kinds of user data, as prevailing in today's digital society, could be replaced by solutions such as Privacy-ABCs that are strongly influenced by privacy by design principles. With level of user-friendliness achieved in the project's use cases, privacy-aware users can easily create a market for such privacy-enhancing services. However, to further facilitate practical implementation, a more detailed elaboration of the inspection process is required – especially from a legal and organizational perspective, as presented in the following.

The paper is structured as follows: Section 2 gives an overview on the development in the field of conditional identification in general and Privacy-ABCs in particular. The core of the inspection process is the decision when and how far inspection should be executed – or prevented. This is based on the inspection grounds that Section 3 diligently derives from the European legal framework. A model process of the inspection-related procedures, as well as the implementation in the school pilot, is explained in Section 4. Section 5 summarizes the benefits of implementing the inspection process properly, and the final Section 6 provides an outlook on future developments.

2 Authentication solutions with conditional identification

Since the 1990s, the possibility of optional or mandatory escrow of cryptographic encryption keys has been vividly discussed (see e.g. [Ho95]). It did not take long to extend this discussion on approaches for "identity escrow" [KP98] where "escrow agents" use information forwarded by the verifier (service provider) for a second-tier identification if necessary. Developments within the area of Privacy-ABCs, such as minimal-disclosure tokens [Br00] and anonymous credentials [CL01], provide data-minimizing, yet accountable authentication solutions and have been further developed during the last decade. Whereas early publications use terminology such as "revoking anonymity", this has changed to prevent confusion with regard to the revocation of certificates, for instance in the case of a lost token. We follow the terminology of Privacy-ABCs and use the term "inspection" for the operation to recover specific attributes under predefined circumstances [Kr13].

Other work in this field has discussed different options for realizing “trustee-controlled conditional anonymity” [Cl03] – here it is pointed out that “revocation of anonymity” is not always the best solution, similar to the approach taken by Privacy-ABCs that start with anonymity and provide “conditional identification” [ZS13]. Further, ISO/IEC has published the standard 29191 on requirements for partially anonymous, partially unlinkable authentication [IS12]. This standard acknowledges the privacy-preserving potential of such authentication solutions and introduces terms like the “designated opener” who can identify the user (“claimant”) in an identity management scenario.

Although technical solutions on the issues of identity escrow, trustees for identification, or inspection are well-discussed in literature, to our knowledge there is no guidance paper that elaborates in detail how to deal with inspection requests in practice when employing privacy-preserving authentication solutions that involve one or more third parties. This gap may be explained by the fact that there are hardly any implementations in practice, yet. This contribution is meant to achieve some remedy by describing a model procedure framework on inspection.

This work has not only been discussed among computer scientists, lawyers, and practitioners on an abstract level, but has been realized in pilot applications in the ABC4Trust context [Kr13]. Figure 1 shows the main building blocks of the setting used in the project. However, the results presented in the remainder of the paper do not rely on the exact technical architecture, but can be applied to other authentication solutions with conditional identification as well.

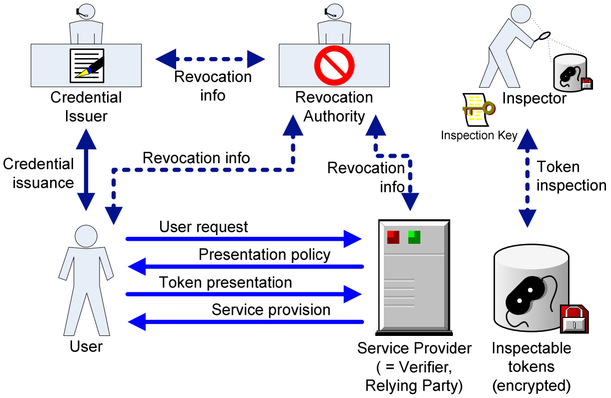


Figure 1: High-level architecture of attribute-based credentials

In a Privacy-ABC scenario a User acquires attribute-based credentials from the Credential Issuer who vouches for the correctness of the information contained in the credential. When requesting a service from a Service Provider (in the identity management terminology also known as “verifier” or “relying party”), the User may be asked to present proof of certain attributes, e.g. “being over 18” or “being a student”. The Service Provider communicates which information is required in its presentation policy. The User chooses the appropriate credential(s) and generates a token to present to the Service Provider. The presentation tokens are not linkable and do not identify the

User. The Service Provider may allow anonymous access, but may also demand the possibility of a later inspection of certain attributes under specific circumstances stated in the presentation policy. In this case, the User is made aware of this fact and generates specific “inspectable tokens”. These are encrypted so that even the Service Provider cannot see the information; only an Inspector – often a third party – holds the secret key and can perform the inspection if the pre-defined circumstances occur. The Inspector itself creates the private key, which is not shared with any other of the entity involved. However, to add another element of checks and balances the Inspector can consist of two separate entities, who operate with split keys. Alternatively, this split-key solution could involve a dedicated Inspection Decision Entity. In order to enable the creation of the appropriate tokens, only the complementary part of the key is provided to the Service Provider. For reasons of completeness, but not in focus of this text, the Revocation Authority should be mentioned, whose task it is to revoke credentials if the need arises.

3 Inspection grounds

In order to fully benefit from the privacy-preserving elements of conditional identification, inspection should be extremely limited. This requires a well-defined and narrow list of inspection grounds, which provides transparency for the Users and facilitates the assessment of inspection requests. The conditions under which identification of a User is allowed must be presented before any personal data is submitted.

In the Swedish school pilot, the inspection grounds are strictly limited to instances where the school itself is bound by legal obligations and they are therefore linked to its official functions. As the school has a duty of care towards its students, the identification of Users may be necessary in cases of emergencies concerning suicide threats or threats of physical violence against others. Further, the school and all guardians (i.e. the principal, teachers, and parents) are legally obliged to comply with an official policy against discrimination and degrading treatment. It strives to prevent discrimination based on gender, sexual orientation, ethnic background, religion by sanctioning harassment and other threats to the safety of students, including offensive language ([BO13], p. 91). Yet, there are further legal obligations with regard to the rights of the Users. Article 1 para. 1 of the DPD states that its purpose is to protect the fundamental rights of persons, and according to its Article 7 (f) the necessary processing of data for legitimate purposes of the controller can be overridden by fundamental rights of the data subject. Yet, secondary law does not define necessity or how it is to be assessed, especially with regard to fundamental rights [Fr14]. However, the DPD implements the general guarantees of primary law, i.e. the Charter of Fundamental Rights (CFR), which gained binding legal status with the entry into force of the Lisbon Treaty in 2009.

For cases where the Service Provider is an official authority exercising public powers – such as the school in the Swedish ABC4Trust pilot – compliance with European fundamental rights is a legal obligation. Where the Service Provider is a private party, the Charter does not apply directly [Jr13], yet obligations regarding inter alia the right to data protection can be deduced from general principles of European law. These general principles have, on several occasions, been applied in relations between private parties

[EC10a], [EC05]. Therefore, the inspection grounds have to balance the needs of the Service Provider and Users. Where necessary and justified, the Service Provider must be able to identify the User. After all, under the current legislation Service Providers have the right to collect and store any type of personal data necessary for the purpose – even if it is only necessary in specific cases. The voluntary step to refrain from obtaining clear text data should therefore not infringe own legitimate interests. However, the inspection grounds are the means to limit the identification to exactly those cases.

Types of inspection grounds: In practice, the list of inspection grounds will consist of two categories: (1) formal reasons and (2) substantive reasons.

(1) All state-issued court orders or those of other competent official authorities belong to the former category. When such an official order is presented, the weighing of the rights and interests has already occurred. However, in most instances these decisions can be challenged in legal proceedings under national law, which might even have suspensory effects.

(2) Any other kind of ground is a substantive reason and a weighing of the interests at issue has to be performed by the Inspection Decision Entity. As in the Swedish use case, public entities should generally limit the grounds to their assigned tasks.

The CJEU has developed a proportionality test ([EC86], para. 38), which is used as starting point for a scheme to determine whether a User may be identified. This procedure is inspired by the concept of Privacy Impact Assessment, which serves to evaluate a measure's implications for the right to privacy [De12]. Thus, the interests and rights at issue have to be determined, before their relationship can be assessed.

Legitimate aim of inspection: Firstly, the identification of a User must pursue a legitimate aim. These can be interests and rights of the Inspection Request Sender. Many interests which can clearly be affected by abusive behavior of Users can be linked to fundamental rights. If the Inspection Request Sender is victim of defamation or threats this affects this person's right to private and family life (Article 7 CFR) or their freedom to conduct business (Article 16 CFR). Where a violation of copyrights is at issue, the owner can rely on the right to intellectual property of Article 17 CFR. Another interest of the Inspection Request Sender could be the instigation of civil or criminal proceedings against the User for abusive behavior. In this case she can rely on the right to an effective remedy according to Article 47 CFR. However, there may also be interests of the Service Provider at issue, for instance the school's duty of care towards its students in the Swedish use case. However, as a public authority, it cannot rely on fundamental rights. These are legal positions of the citizen against the state, they cannot be applied in the opposite direction.

The enumeration of rights provided here and in the following are by no means exhaustive, there may be other interests to be identified. It serves to illustrate the interests most likely to be considered. In order to present a legitimate aim for inspection, the interest concerned does not have to correspond to a fundamental right. However, where this is the case it has a higher value than other interests. The relevant legitimate aims must be included in the inspection grounds, so it is foreseeable for the User, which of her actions can result in an inspection. If the Inspection Request Sender's (or the aggrieved party's) right or interest is not covered by the inspection grounds, she has to obtain an official order, to trigger a formal reason for inspection.

Rights and interests of the User: In virtually every instance, rights of the User will also have to be considered. Whenever the identity of the User is to be revealed, her rights to privacy and data protection according to Articles 7 and 8 CFR are affected (related assessment in [Cl03]). Additionally, when a User expresses an opinion, she enjoys the right to free speech laid down in Article 11 CFR. Further, it should be borne in mind that discrimination against a person based on grounds of inter alia sex, religion, age and sexual orientation is prohibited by Article 21 CFR. The User also has the rights to be heard, be granted access to her file (in line with the data subject's rights under the DPD) and receive a reasoned decision according to Article 41 CFR. While this provision is binding only for official authorities, the procedural guarantees should also be observed amongst private parties. Involving the User in the process serves to minimize risks of lawsuits, instigated by a User who finds that her identification was unwarranted.

Weighing of rights and interests: Lastly, the rights and interests of the parties involved have to be weighed. Fundamental rights are not absolute and may be limited, when the restriction pursues a legitimate aim or there is a collision with another fundamental right (Article 51 para. 1 CFR). This balancing is best achieved in a two-step process.

Firstly, it should be ascertained whether the identification of the User is suitable for attaining the legitimate goal, i.e. to defend the rights and interests of the other party. As identification of the User allows holding her responsible this will usually be the suitable.

Secondly, it has to be ensured that the data processing does not go beyond what is necessary. In assessing whether identifying the User is necessary, it has to be determined whether there are less invasive measures (for a diligent assessment of necessity [EC10b], paras. 67-87). In the context of Privacy-ABCs it has to be stressed that identifying the User has *ultima ratio* character. It may therefore only occur when there is no other measure that would protect the rights of the other party equally, while respecting the privacy of the User. Thus, it should generally be considered whether removing the content under objection would be a remedy. Additionally, informing the User that an inspection is impending if the situation is not remedied gives the User an incentive to become proactive. As the User is not known to the Service Provider, there can technically not be any requirements to hear her before she is identified, but the principle of transparency comes into play here: even when the process of inspection is initiated, the User should be informed during all stages, as this can serve to de-escalate the conflict.

It should be pointed out at this stage, that in cases where there are high-level rights at issue, e.g. in case of threats of violence or suicide, this process does not require additional time. When the right to life or the right to integrity of the person are concerned it is obvious that the User's right to data protection does not take precedence. Furthermore, a well-defined and documented Inspection Procedure facilitates the production of a reasoned decision to the User to justify her identification.

4 A model process for inspection

When applying inspection possibilities in a use case, the workflow has to be well-defined, in particular with respect to legal compliance. Although the requirements and options may vary per use case, common ground can be identified as a model process for inspection. The following subsections describe this process and illustrate how it has been put into practice in a pilot of the ABC4Trust project [BH14].

4.1 Modelling the inspection process

The task of the Inspector is embedded in a more complex procedural framework where the process starts with an inspection request: It has to be checked whether this request is justified and whether other solutions with less infringement of the User's privacy may be advised. Often, the rights of different parties involved have to be balanced for this purpose. Further, the process does not terminate as soon as the Inspector has performed the decryption: The inspection result or, even better, derived inspection conclusions have to be communicated to the appropriate stakeholders. Figure 2 gives an overview on the procedure framework for inspection and the roles involved [BH14]. Note that some of the roles may be fulfilled by the same entity, and it can also vary which parts belong to the Service Provider's domain.

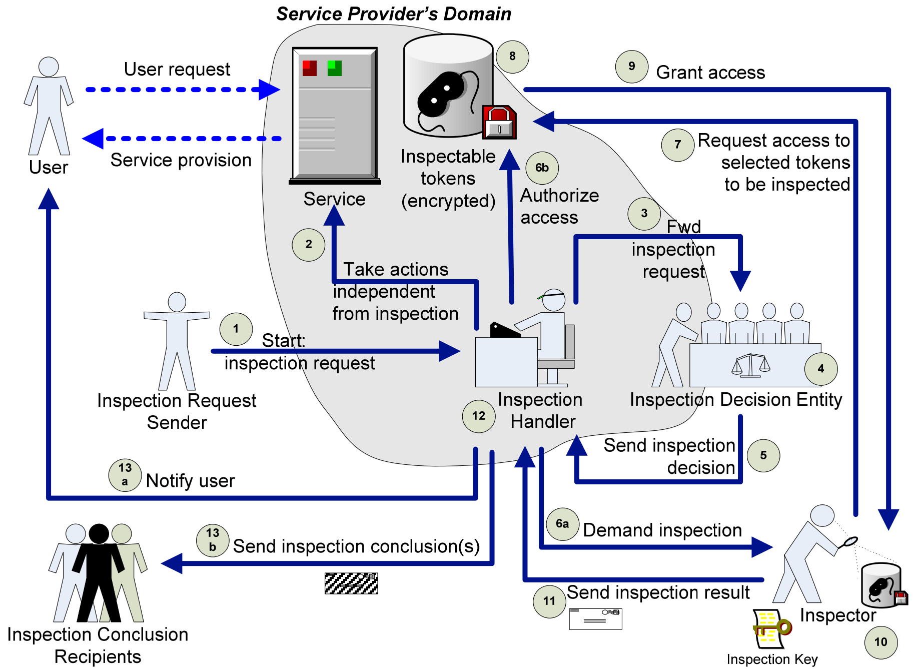


Figure 2: Model inspection process

The numbered steps shown in Figure 2 are explained in the following walkthrough:

Phase I (prior to involvement of Inspector)	Step 1	The Inspection Request Sender, possibly via a report function, submits an inspection request to the Inspection Handler. As response an automated ticket system creates an automatic reply to the Inspection Request Sender.
	Step 2	The Inspection Handler filters requests that can be solved otherwise, acts as first-level support and may abort the process, where abuse of the report function is evident or when a solution that avoids inspection is favorable (e.g. deletion or blocking of the reporting content).
	---Abort possible before an inspection is initiated---	
	Step 3	The Inspection Handler forwards the inspection request to the Inspection Decision Entity.
	Step 4	The Inspection Decision Entity has the obligation to render a reasoned decision whether the given inspection grounds are fulfilled and thus as to whether or not inspection should happen. This decision may be enriched by suggestions on the scope and further requirements of the inspection.
	Step 5	The Inspection Decision Entity reports the inspection decision to the Inspection Handler: “perform inspection” (proceed with Step 6), “no inspection” (proceed with Step 2 for de-escalation or immediately abort the process).
	---Abort possible---	
Phase II (activity of the Inspector)	Step 6	The Inspection Handler instructs the Inspector to carry out an inspection according to the inspection decision (6a). For this, the Inspection Handler authorizes access to the selected encrypted tokens in the database (6b).
	Step 7	The Inspector requests access to the encrypted tokens to be inspected (scope as defined by the Inspection Decision Entity in Step 4).
	Step 8	The authorization of the Inspector’s request is technically checked before granting access.
	---Abort if not authorized---	
	Step 9	Access to the selected encrypted tokens is granted and logged as part of the audit trail to enable oversight by the Inspection Handler.
	Step 10	The Inspector decrypts the tokens and prepares the inspection result.
	Step 11	The Inspector sends the inspection result to the Inspection Handler.
Phase III (post-processing)	Step 12	The Inspection Handler transforms the inspection result into target-specific responses (inspection conclusions) for those who should be informed or otherwise should take actions (possibly according to inspection request (e.g. judicial decision) or inspection decision).
	Step 13	The Inspection Handler (a) to promote transparency notifies affected User(s) (unless legally prohibited, e.g. by the judicial decision) and – potentially simultaneously – (b) sends the inspection conclusions generated in Step 12 to the Inspection Conclusion Recipients.

These steps are based on a process of escalation, which aims to avoid identification of users due to the effort and expenditure it entails and with the goal of solving any issues on the lowest level possible. Service Providers will already have a process for user complaints in place, which – while not including an Inspector or the Inspection Decision Entity – includes a system for handling of requests and subsequent notification. The additional role of the Inspector is a technical requirement serving the implementation of Privacy-ABCs. In order to further enhance user privacy and operationalize a user rights-centered approach in order to conform to their fundamental rights, the Inspection Decision Entity is created. This entity may be a board and can possibly also be independent from the Service Provider. In emergency cases only may the Inspection Handler skip the involvement of the Inspection Decision Entity by directly requesting inspection from the Inspector.

This process has been discussed with the participants of the 2014 IFIP Summer School on Privacy and Identity Management for the Future Internet in the Age of Globalisation, who provided constructive and much appreciated feedback from the perspective of multiple disciplines. Participants were confronted with various scenarios in several use-cases, one of which was the school online communication platform, which will be discussed below. Without any knowledge of the process, they were asked to make decisions on whether a given behavior constituted one of the inspection grounds enclosed with the scenarios and whether a user's identity should be revealed. The discussions of the Summer School participants showed that the process as detailed above follows from the operationalization of a privacy- and user rights-centered approach.

Concerning the process, participants stressed the importance of the separation of the Inspection Decision Entity and the Inspector. Ideally, the Inspection Decision Entity should consist of all relevant stakeholders in the implementation, i.e. not only representatives of the Service Provider, but also Users. Additionally, it is desirable to also incorporate an element of external supervision to the Inspection Decision Entity, in the form of an external expert focused on ethical or legal implications of the decision. It was further discussed, that the Service Provider's Data Protection Officer could partake in the deliberations of the Inspection Decision Entity, as he or she is an expert with a certain level of autonomy. On the other hand, the Data Protection Officer could also be involved in reviewing and auditing the process. This review is enabled by an audit trail that logs any activity within the process on all its stages, comprising e.g. technical access log entries as well as manually generated reasoning for inspection decisions. This could be supported by an automated ticketing system, which can provide check lists and assist the various entities in the execution of the process.

As the scenarios included instances of emergencies, such as threats to the life or physical integrity of persons, participants agreed that there was a need to ensure a quick response, which can be realized through break-glass procedures. This could include fast-tracking decisions of the Inspection Decision Entity or allowing the Inspection Handler in emergency instances – which have to be defined clearly and should be limited to threats to life or the physical integrity of persons – to trigger an inspection.

However, participants generally concluded that specific implementations have their own factual and legal requirements and thus implementation always has to be use case specific. Thus, the implementation of this model process for the Swedish school pilot will be detailed in the following.

4.2 Applying the inspection model to a school online communication platform

As the Restricted Areas (RA) are used by students, parents, teachers, and counselors alike, all of these parties may find content they wish to report and can thus become Inspection Request Senders. The inspection request does not necessarily have to be submitted through the report-button in the relevant RA, but can also be submitted offline, e.g. by directly approaching the Inspection Handler. It is further conceivable that an Inspection Request Sender, in matters of great concern, turns to an official authority outside the school, such as the police or a court, rather than reporting it to the Inspection Handler. As the ultimate authority and responsibility in the school context rests with the principal, he assumes the role of Inspection Handler. Additionally, due to strict legal obligations on responsibility in Swedish law, the principal also functions as Inspector (the technical process is detailed in [BO13], pp. 41 et seq). The Inspection Decision Entity is comprised of all stakeholders in school life, i.e. the principal, a counselor, the school nurse, and parents.

If an inspection is eventually carried out, the inspection conclusion(s) can be sent to any of the Inspection Request Senders or another entity, for instance a school counselor or teacher to initiate an educational response. Where the police or a court were informed, the inspection conclusion(s) can be sent exclusively to this entity.

As the national Swedish law provides extensive rules on freedom of information, any decisions taken in the process, which have to be logged, have to be made available to the public. This is a welcome requirement worth consideration for any implementation due to the transparency added by allowing extensive external oversight.

5 Benefits of proper implementation of the inspection process

Through the proper implementation of the proposed inspection process the following benefits can be achieved, if the above detailed requirements are met:

Transparency:

- Foreseeability of inspection for Users through:
  - well-defined inspection grounds
  - clear presentation of the inspection grounds
  - information before User action
- Information of and communication with Users once inspection process is triggered
- Intervenability for Users throughout inspection process
- Reasoned decision for User including circumstances of Inspection Request
- Information of Inspection Request Sender at end of process through closing ticket

Central oversight and efficiency:

- Inspection Handler as central authority
- Responsibility for inspection process:
  - Monitoring of all actors
  - Handling enquiries by outside entities (e.g. User, Inspection Request Sender, Inspection Conclusion Recipients)
  - Performing of tests to verify Inspector can produce inspection result
  - Authorizing access of Inspector
- Definition of the scope of review by determining Users to be identified and Inspection Conclusion Recipients
- Responsibility for logging of all activities
- Predefined process allows quick production of reasoned decisions

Separation of powers: • All tasks are divided between mutually independent actors: Inspection Handler / Inspection Decision Entity / Inspector
Rights-centered approach: • Identification and weighing of rights and interests of all concerned parties

6 Conclusion and outlook

Privacy-ABCs offer notable advantages: As fewer data is stored and processed, the risk of misuse is limited considerably. Especially in comparison to full identification which is the current standard, the rights of Users are awarded higher protection. Even though an identification of Users may eventually occur, there is a process of escalation, which also allows for de-escalation in virtually every phase. The process defined above therefore does not automatically lead to an inspection. Rather, inspection is the exception, which requires additional effort and is documented in a transparent way to allow for internal and external review. Internally, there further is a system of checks and balances installed to enforce shared powers, while the ultimate responsibility, to comply with legal requirements, rests with the Inspection Handler as the responsible party. Thus, the process proposed brings measurable benefits for privacy and the rights and interests of all concerned parties and thereby shows an exemplary implementation of Privacy-ABCs.

While the process proposed would add complexity to legacy systems, this could be remedied by clearly defining the phases beforehand. In the future this may be achieved through a “Setup wizard”, which allows for easy adaption and implementation. Further, there is potential to automate certain steps, while others require human involvement. However, as the discussions with the Summer School participants illustrated, each scenario has different requirements for implementation. Yet, it should be explored whether this can even be further operationalized. Additionally, even with the level of harmonization within the EU, each jurisdiction poses specific legal challenges to implementation. More generally, there should be a unified and intuitive way of informing Users about the fact that they are in an inspectable area, especially when there is not issue of full identification but only parts of attributes are revealed instead. In this regard, standardization would be much needed to alleviate risks of proliferation, which run counter to the goal of transparency. In a variation of the proposed process, the Inspector could also be implemented as data controller in the sense of the DPD. He would then assume responsibility for his own data processing instead of acting on behalf of the Service Provider / Inspection Handler. Alternatively, the legal concept of “joint controllership” may be applied. Under the scope of this paper this issue has to remain open for future analysis.

Another development which can be anticipated is the further implementation of electronic identification (eID) services in the European Member States. This field is currently subject to European legislation, in particular with an upcoming eIDAS Regulation [ZS13]. The eID technology increases risks for Users if full identification is the default. However, the European legislator could counterbalance this through recourse to Privacy-ABCs.

References

[BH14] Bieker, F.; Hansen, M.: Privacy-preserving authentication solutions – Best practices for implementation and EU regulatory perspectives. In: eChallenges 2014; forthcoming.

[BO13] Bcheri, S.; Orski, M. (eds.): Necessary hardware and software package for the school pilot deployment. ABC4Trust Deliverable D6.2, Söderhamn/Frankfurt, https://abc4trust.eu/download/ABC4Trust-D6.2.Hard-and-Software-Package-for-School-Pilot.pdf, 2013.

[Br00] Brands, S.A.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge, MA, USA, 2000.

[CL01] Camenisch, J.; Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: EUROCRYPT 2001. LNCS, vol. 2045, Springer, Heidelberg, 2001; pp. 93-118.

[Cl03] Claessens, J.; et al.: Applications requirements for controlled anonymity. Deliverable 7 of the project APES – Anonymity and Privacy in Electronic Services. Leuven, http://www.cosic.esat.kuleuven.be/publications/article-106.pdf, 2003.

[De12] De Hert, P.: A Human Rights Perspective on Privacy and Data Protection Impact Assessments. In (Wright, D.; De Hert, P. eds.): Privacy Impact Assessment, Springer, Heidelberg, 2012; pp. 33-76.

[EC86] Case 222/84 Johnston v Chief Constable of the Royal Ulster Constabulary, ECR 1651, 1986.

[EC05] Case C-144/04 Mangold v Helm, ECR I-9981, 2005.

[EC10a] Case C-555/07 Kücükdeveci v Swedex GmbH & Co. KG, ECR I-365, 2010.

[EC10b] Joined Cases C-92 and 93/09 Schecke and Eifert, ECR I-11063, 2010.

[Fr14] Feretti, F.: Data Protection and the Legitimate Interests of Data Controllers: Much Ado about Nothing or the Winter of Rights? In: Common Market Law Review 2014, vol. 51; pp. 843-868.

[Ho95] Hoffman, L.J.: Balanced Key Escrow. Technical Report, The George Washington University, Institute for Computer and Telecommunications System Policy, 1995, http://coast.cs.purdue.edu/pub/doc/cryptography/hoffman_balanced_escrow.html

[IS12] ISO/IEC 29191: Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication, 2012.

[Jr13] Jarass, H.: Charta der Grundrechte der Europäischen Union. C.H. Beck, München, 2013.

[KP98] Kilian, J.; Petrank, E.: Identity Escrow. In: Advances in Cryptology – CRYPTO '98. LNCS, vol. 1462, Springer, Heidelberg, 1998; pp. 169-185.

[Kr13] Krontiris, I. (ed.): ABC4Trust Architecture for Developers. ABC4Trust Heartbeat H2.2, Frankfurt, https://abc4trust.eu/download/ABC4Trust-H2.2_ABC4Trust_Architecture_for_Developers.pdf, 2013.

[ZS13] Zwingelberg, H.; Schallaböck, J.: The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective. ABC4Trust Heartbeat H2.4, Kiel/Frankfurt, https://abc4trust.eu/download/ABC4Trust-H2.4_Privacy_Perspective_on_the_eIDAS_regulation.pdf, 2013.

Strengthening Web Authentication through TLS - Beyond TLS Client Certificates

Andreas Mayer[1], Vladislav Mladenov[2], Jörg Schwenk[2], Florian Feldmann[2], and Christopher Meyer[2]

[1]Adolf Würth GmbH & Co. KG, Künzelsau-Gaisbach, Germany
[2]Horst Görtz Institute, Ruhr-University Bochum, Germany

Abstract: Even though novel identification techniques like Single Sign-On (SSO) are on the rise, stealing the credentials used for the authentication is still possible. This situation can only be changed if we make novel use of the single cryptographic functionality a web browser offers, namely TLS. Although the use of client certificates for initial login has a long history, only two approaches to integrate TLS in the session cookie mechanism have been proposed so far: Origin Bound Client Certificates in [DCBW12], and the Strong Locked Same Origin Policy (SLSOP) in [KSTW07].

In this paper, we propose a third method based on the TLS-unique API proposed in RFC 5929 [AWZ10]: A single TLS session is uniquely identified through each of the two Finished messages exchanged during the TLS handshake, and RFC 5929 proposes to make the *first* Finished message available to higher layer protocols through a novel browser API. We show how this API can be used to strengthen all commonly used types of authentication, ranging from simple password based authentication and SSO to session cookie binding.

Keywords: SSL, TLS, Session Cookies, Password based Authentication, Single-Sign-On, TLS-unique, Strong Locked Same Origin Policy

1 Introduction

Today, the most prevalent method for user authentication towards a server in a network environment consists of a username/password combination, where the username is usually a publicly known value and the password is a secret value known only to the corresponding user. By providing the correct password for a given username, the user proves his identity to the server.

After a correct initial authentication, the server issues a *cookie* containing a unique string identifying an authenticated session between user and server. Subsequent queries from the user to the server will then include this cookie and thus do not require another explicit authentication.

Nowadays, every user is working with various services on the Web, thus, a user has to create and manage multiple passwords. To mitigate the overhead of creating and remembering multiple secure passwords, SSO systems can be utilized. These systems allow a user to authenticate himself to an Identity Provider (IdP) which acts as a trusted third party towards both the user and the Service Provider (SP) (the server providing the desired service). After the user authenticated himself to IdP, the IdP authenticates the user towards an SP by issuing a cryptographically secured authentication token. The user can use this token to prove his identity to SP without requiring further explicit authentication by username/password.

Attacks on Authentication Methods In practice, many problems can arise in such authentication contexts. Passwords can be leaked, either via Phishing or during transport.

Cookies and authentication tokens can be eavesdropped or stolen via various attack techniques and used by an attacker to impersonate the user.

And even though the authentication data sent between the participants is almost always protected by secure channels, i.e. TLS sessions, it has been shown in the past (e.g., [Mar09] or [BDLF^{+}14]) that TLS sessions are susceptible to Man-in-the-Middle (MitM) Attacks, potentially enabling an attacker to steal passwords, cookies and/or authentication tokens during transport.

Contribution Motivated by the existing threats and serious vulnerabilities found within today's authentication processes and the associated identity management, we propose a novel approach to strengthen authentication and trust between the participants.

Our main goal is to use certain features of the TLS session between participants to enhance the protection of the entire communication within the current HTTP-session. The distinct contributions of this paper are the following:

- Introduction of a novel binding of passwords to the applied TLS session during the login phase in order to prevent MitM attacks regarding the transmitted credentials.
- Reinforcement of the session cookies in conjunction with a TLS channel to mitigate the theft via XSS, CSRF and UI-Redressing attacks.
- Amplification of SSO protocols by cryptographically binding the issued security tokens to the applied TLS session.
- Only minor adjustments to the existing infrastructures are proposed, enabling an easy implementation and integration of the introduced mechanisms.

The security mechanisms introduced in this article are based on the sole assumption that the simple TLS-unique interface from RFC5929 [AWZ10] is implemented in the browser.

The paper is organized as follows: Section 2 discusses related work pointing other approaches and their respective differences to our approach. Section 3 explains the technical foundations our solution is based on. We define the threat model in Section 4 and list the technical preconditions in Section 5. Section 6 explains the theory behind our proposed solution and Section 7 provides information regarding possible implementations of the concept. We conclude our paper in Section 8.

2 Related Work

Several efforts have been proposed [PS00, FSSF01, LKHG05] to secure cookies by deploying modern public key-based authentication mechanisms. However, neither signing nor encrypting cookies prevents an adversary from transferring a cookie from one browser to another, thus rendering these efforts ineffective against cookie theft and similar attacks.

In 2007, Karlof et al. [KSTW07] proposed to strengthen the web browser's Same Origin Policy (SOP) by taking the server's TLS certificate into account. They recommended two variants, called *weak-* and *strong-locked Same Origin Policy*, respectively. The weak-locked SOP is easier to implement and enforces that web objects are sent only to servers with valid certificate chains (e.g. certificates included in the chain can neither be selfsigned nor expired). The strong-locked SOP tags each web object with the server's public key and solely returns them to a server if that public key matches the key from the TLS certificate of the current TLS connection to the server.

A similar approach called *Web Server Key Enabled Cookies* (WSKECookies) was presented by Masone et al. [MBS07]. In this concept, the browser stores cookies along with the public key of the web server which initially set them. A WSKECookie is only returned to a web server which proved possession of the same key pair in following TLS sessions. In both concepts stolen web objects or WSKECookies are not cryptographically bound in any way – neither to the TLS channel nor to the client. Therefore, the attacker can potentially steal them and then use them to authenticate as the victim.

In 2008, Gajek et al. [GJMS08] proposed a variant of a browser-based Kerberos scheme using TLS client certificates. The concept has been standardized as *SAML Holder-of-Key Web Browser SSO Profile* by OASIS[1] [KS10]. In contrast to our proposed solution, the Holder-of-Key approach protects neither HTTP cookies nor password-based logins, but only the SAML assertion within the Single Sign-On based authentication.

RFC 5929 [AWZ10] was published in 2010 as proposed standard. The document describes three channel binding types for TLS, namely *tls-unique*, *tls-server-endpoint*, and *tls-unique-for-telnet*. TLS-unique specifies the API for our proposed binding solutions.

A solution specifically designed for channel bindings within SAML frameworks has been described in [KSJG10].

In 2012, Dietz et al. [DCBW12] proposed a TLS channel binding called *Origin-Bound Certificates* (OBC) by using a TLS extension. Their approach changes server authenticated TLS channels into mutually authenticated channels by using client certificates created on the fly by the browser. In consequence, their idea requires changes to the TLS protocol, which would affect all current TLS implementations. They propose to use the issued OBC by cryptographically binding them to HTTP cookies or SSO tokens.

Google introduced another TLS extension called *Channel ID* [BH12], which again requires fundamental changes to underlying TLS implementations. In summary, the browser creates an additional asymmetric key pair during the TLS handshake and uses the private key to sign all handshake messages up to the `ChangeCipherSpec` message. Subsequently, the signature, along with the public key, is sent encrypted through the TLS channel using the established TLS key material. This is done, before finishing the TLS handshake. The browser uses the public key as ”Channel ID” that identifies the TLS connection.

In 2013, OASIS published the *SAML Channel Binding Extensions* allowing the use of channel bindings in conjunction with SAML [Can13]. This standard allows the proposed TLS channel bindings to be integrated in all SAML related services, e.g. SSO.

3 Technical Foundations

In order to exchange sensitive data between a client and a server, first a mutually authenticated secure channel has to be established between the two communication partners. Establishing such a channel requires multiple steps, where server side authentication and data protection during transport are usually handled via Transport Layer Security (TLS). Section 3.1 briefly discusses the details of a TLS handshake phase, resulting in establish-

[1] https://www.oasis-open.org/

ment of a server-side authenticated secure channel between the parties. Usually, the client then has to provide an authentication for himself. This client authentication can be done directly towards the server by using a mutual secret, i.e. a password, between client and server, as described in Section 3.2. Section 3.3 describes means to make this authentication persistent, so the user does not have to enter the password for every HTTP-request. Alternatively, authentication can be done indirectly with the help of a trusted third party in an SSO scenario, as shown in Section 3.4.

3.1 Transport Layer Security (TLS)

Transport Layer Security (TLS) [DR08] provides multiple security goals, such as

(1.) *Confidentiality* (2.) *Authenticity* (3.) *Integrity* and (4.) *Replay protection.*

These goals are achieved by different cryptographic primitives like encryption, Keyed-Hash Message Authentication Codes (HMACs), sequence numbers and nonces. However, TLS protects data only during transport and does not provide any end-to-end payload security. Thus, message level security requires additional mechanisms at a higher level in the protocol stack.

TLS consists of a two-phase architecture: The handshake phase and the application phase (see Figure 1).

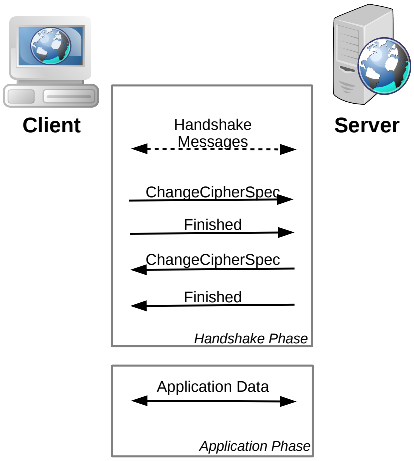


Figure 1: TLS Handshake Phase and Application Phase.

The handshake phase includes multiple messages sent between client and server and serves to establish algorithms, cryptographic primitives and an authenticated agreement on a shared secret between the participants. All key material required for a secure communication is derived from this secret.

Handshake messages are exchanged unencrypted until the `ChangeCipherSpec` protocol is invoked to activate cryptographic protection at the corresponding party (thus, after both parties sent their corresponding `ChangeCipherSpec` messages, all communication between the two parties will be encrypted). All handshake messages may only occur in an exactly specified order and must follow the predefined workflow.

A parameter of interest for the concept of TLS Unique is the first Finished message (*Finished*) message. This *Finished* message is the first message encrypted with the negotiated keys and contains a hash value of all handshake messages previously exchanged between client and server. The hash especially includes all random values exchanged within the handshake, thus, the *Finished* message can be seen as a unique fingerprint of the TLS session in use.

After both parties have established the shared secret and confirmed this by sending the proper *Finished* message, the protocol continues with the application phase where the actual payload data is exchanged via the secure communication channel.

3.2 Initial Client Authentication

The initial client authentication describes authentication of a user against a server by proving the possession of a shared secret. The authentication process in most cases is visible to the user and requires interaction.

For our approach, we focus on *Form-based Authentication*, where the server provides an HTML form with one or more input fields into which the user enters his credentials. Then the form including the user's input is sent to the server for validation. On client side, e.g., JavaScript could be utilized to provide protection of integrity, authenticity and/or confidentiality, before sending the data. On server side, any application logic designed to validate authentication data, can read and process the received data. No specific client side enhancements have to be performed to support this authentication type.

Our approach could also be used in conjunction with either *HTTP Basic Authentication* or *HTTP Digest Authentication* (both described in [FHBH$^+$99]), but this would require several client side modifications.

3.3 Persistency of Authentication

HTTP is a stateless protocol. Without additional mechanisms, a user would be forced to re-enter his login information for each HTTP request. Cookies [Bar11] are used to transform stateless HTTP requests into stateful user sessions by explicitly linking them together. They are sent with every HTTP request from the browser to the web server. Cookies consist of name-value pair containing session information. A web server can instruct a browser to store a cookie by sending an additional HTTP header, embedded in an HTTP response, as follows:

```
Set-Cookie: SessionID=280-9757248-2350101;
            domain=docs.foo.com; path=/accounts;
            expires=Sun, 30 Mar 2015 05:23:00 GMT
```

A cookie can have further attributes, such as `domain` and `path` that define the scope of a cookie (e.g. `docs.foo.com/accounts`). The `expires` attribute indicates when a cookie expires.

Stored HTTP cookies are automatically sent back to the server by adding the additional HTTP header `Cookie` containing the set cookie(s). This simple mechanism is supported by all browsers. HTTP cookies are often used to store the result of an initial authentication; we will call such cookies Session Cookies.

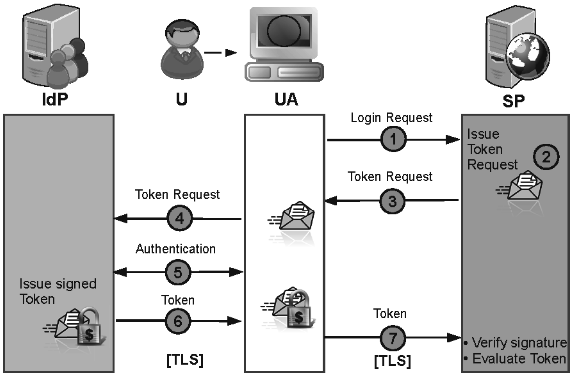


Figure 2: Single Sign-On overview.

3.4 Single Sign-On (SSO)

Single Sign-On (SSO) is a mechanism for identity and access management within a federation between related but independent parties. SSO allows a user to authenticate himself to a trusted party (called IdP) to get a security token. This token facilitates the access to a federated party (called SP) without any further login requests. Because an IdP can be federated with multiple SPs, SSO provides great usability and flexibility within the identity management and reduces the configuration and support costs.

Figure 2 shows an overview of an SSO login procedure: User **U** with a user agent **UA**, e.g. browser, tries to get restricted resources from a given SP (1). The SP generates a token request (2) and redirects the client to the IdP (3,4). In the following step, the user authenticates himself to the IdP (5) according to the supported authentication mechanisms (e.g. username/password, mutual authentication, two-factor authentication, and/or biometrics). As a result of the successful authentication, the security token is issued and sent through the user agent to the SP, where it can be verified (6,7). Please note the mandatory prerequisite of TLS secured communication channels between the participants.

4 Threat Model

For our security analysis, we assume an active attacker with full access to the communication network. Therefore, in addition to passively eavesdropping on the victim's communications, the attacker is capable of actively altering all messages sent or received by the victim and his communication partners (cf. [DY83]). We assume that the attacker is able to impersonate (e.g., by means of DNS and PKI spoofing) any server towards the victim.

For our *password-based login* approach, we assume that the victim shares a distinct secret (password) with each of his intended communication partners[2]. In the case of our *SSO* approach, we assume that the victim shares a secret (password) with the IdP, and the federation is set up such that every SP possesses the correct certificate and trusted public key of the IdP. Thus, the attacker is *not* able to impersonate the IdP towards any honest

[2] Please note that for security reasons instead of the password often only a salted hash value of the password is stored on server side.

SP.

We further assume, the attacker does *not* have direct access to the victim's device or actual servers (other than those possibly created by himself). This means the attacker cannot simply read out and steal the secrets shared between the victim and his communication partners, e.g., by utilizing a keylogger or manipulating the victim's browser's DOM. Similarly, we assume the victim is not prone to Phishing attacks intended to steal his password.

5 Technical Preconditions

In addition to the abilities and limitations of the attacker stated previously, several technical preconditions must be fulfilled for our approach to be feasible:

- The user's User Agent (UA) must provide an interface to access the first Finished message of each TLS connection.
- Client and server share a symmetric secret in form of a password. This password has been exchanged beforehand via a secure channel and is stored in a secure way.
- The optional TLS features *TLS session resumption* and *TLS renegotiation* must be disabled on client as well as server side. The usage of any of these features will automatically result in a Finished message differing from the one originally used for the binding. This will invalidate all previous channel bound authentication information.

6 TLS Unique

In this section we describe our solution by applying a secure cryptographic binding using TLS Unique to three practical use cases: (1) Password-Based Login, defined in Section 6.1. (2) HTTP cookies, described in Section 6.2. And finally (3) SSO, shown in Section 6.3. In this section, we also put these building blocks together and present a novel holistically secured browser-based SSO protocol.

6.1 Password-Based Login

As already discussed, authentication using passwords can be unsafe for many reasons. In order to strengthen the password-based login, we propose a novel approach binding the credentials to the TLS session. The protocol run is sketched in Figure 3.

(1.) The user requests a restricted resource on the Web server through his UA.

(2.) The server redirects the user to the authentication module via an HTTP Redirect. In addition, the HTTP Redirect message contains the HTTP-Header *tls-unique-auth: true*, which triggers the TLS Unique module in the UA.

(3.) The TLS channel between UA and server is established.

  3.1) The UA extracts the first Finished message fin via the RFC 5929 interface and stores it.

  3.2) The server acts accordingly on his end of the TLS connection and extracts and stores the first Finished message fin'.
  Note: If no MitM attack between UA and the server is active, it should hold that $fin == fin'$.

(4.) The user enters his *user_id* into the corresponding form field provided by the server.

(5.) The server provides the corresponding salt which was used to build the stored password hash on server side.

(6.) The user enters his password pw. Consequentially, the TLS Unique module in the

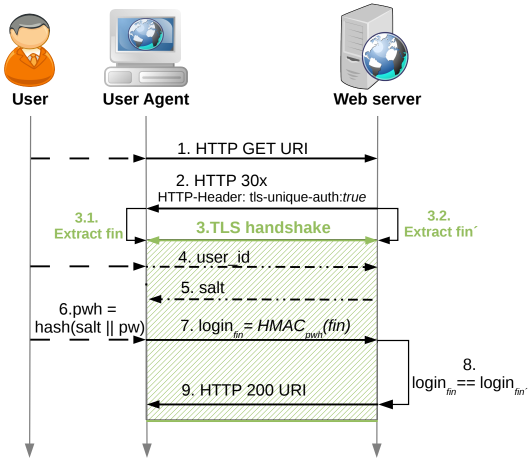


Figure 3: Password-Based Login bound to TLS Unique.

UA computes a hash value of the concatenation of the received salt and the user's provided password: $pwh = hash(salt||pw)$.

(7.) The TLS Unique module then computes an HMAC $login_{fin} = HMAC_{pwh}(fin)$, which is transmitted to the server.

(8.) After receiving this value the server computes $login_{fin'} = HMAC_{pwh}(fin')$. Only if $login_{fin} == login_{fin'}$, the server will accept the credentials and successfully authenticate the client.

(9.) The server grants access to the requested resource.

Note 1: Management of passwords on server side is out of scope of this paper. Thus, for the purpose of the protocol described here, usage of salts is optional (see steps 4 and 5). However, based on existing incidents, we highly recommend their usage within the authentication process.

Note 2: Using the TLS Unique binding during the login phase does not prevent the interception of the packages and their analysis by the given adversary controlling the network traffic. However, the $login_{fin}$ token contains only an HMAC over the related credentials and does not reveal the used password. Due to the TLS Unique binding, $login_{fin}$ can only be used in the TLS session uniquely identified by fin (resp. fin'); an adversary trying to use the stolen token in his own TLS session with the server will fail to authenticate himself as the victim because the Finished message fin'' on server side will not match the token.

Note 3: The security of $login_{fin}$ against brute-force attacks depends on the complexity of the chosen password. By this means, the password should have high entropy.

6.2 HTTP Session Cookies

Next, we extend the TLS Unique binding of the password based login protocol from Section 6.1 to HTTP cookies to maintain the authentication state in subsequent HTTP requests. Since session cookies are set and read by the server, a cookie binding to the TLS session has to take place at the server side of the communication.

We propose the following procedure to bind the HTTP session cookie to the TLS channel:

(1.) **Secure user authentication:** The user authenticates using the TLS Unique Password-Based Login protocol as described above.

(2.) **Set TLS Unique cookie:** After successful authentication, the server immediately sets an HTTP cookie $cky_{bound} = hash(fin')$ with the value of the Finished message of the TLS session used in step 1. The value of this cookie serves as a session identifier on server side[3].

(3.) **Verifying the Session cookie:** In all subsequent HTTP requests the browser automatically provides the cky_{bound} by adding it to the HTTP header of the request. The server accepts the cookie if the following comparison holds: $cky_{bound} == hash(fin')$. Thus, the server verifies that the session cookie belongs to the corresponding TLS channel.

Note: Even if the attacker is able to steal the session cookies of the user, he cannot establish a parallel TLS session to the server with the same Finished message $fin == fin'$. As a result, using the stolen cookies to authenticate through a different TLS channel is not possible.

6.3 Single Sign-On (SSO)

A major problem of SSO protocols are MitM attacks on involved TLS connections [SB12]. If TLS is badly configured, or if the adversary succeeds to mount a DNS/PKI spoofing attack, he may read authentication credentials from the network. The TLS Unique binding from RFC 5929 offers a way for the authenticating party to check if there is a malicious MitM on the network. A usage scenario for a TLS Unique binding within general SSO protocols is sketched in Figure 4.

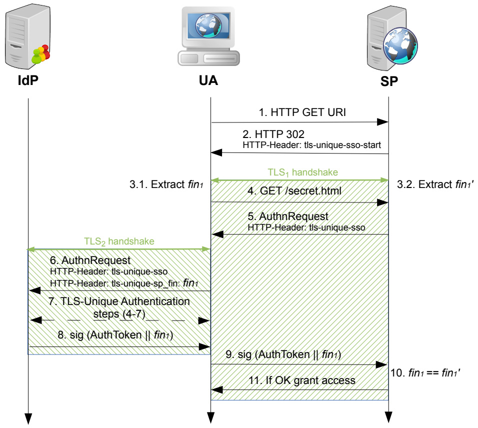

IdP
UA
SP
1. HTTP GET URI
2. HTTP 302
HTTP-Header: tls-unique-sso-start
TLS$_1$ handshake
3.1. Extract fin_1
3.2. Extract fin_1'
4. GET /secret.html
5. AuthnRequest
HTTP-Header: tls-unique-sso
TLS$_2$ handshake
6. AuthnRequest
HTTP-Header: tls-unique-sso
HTTP-Header: tls-unique-sp_fin: fin_1
7. TLS-Unique Authentication steps (4-7)
8. sig (AuthToken || fin_1)
9. sig (AuthToken || fin_1)
10. $fin_1 == fin_1'$
11. If OK grant access

Figure 4: TLS-unique usage scenario in SSO.

In an SSO protocol, typically at least two TLS sessions are involved: TLS_1 between UA and SP, and TLS_2 between UA and IdP. Often the first request to SP is not protected by

[3] Additional cookie properties (e.g., confidentiality or integrity protection) can also be applied in the sense of [LKHG05].

TLS, but in order to be able to apply the TLS-unique binding, setting up a TLS channel immediately in response to Step 2 is essential: After receiving the authentication request from SP, the User Agent (UA) extracts the first Finished message fin_1 (Step 3.1) from TLS_1, using the API described in RFC 5929. This value is added as a parameter to the authentication request and forwarded to the IdP in Step 6.

Note: Technically, SP could immediately include the corresponding value fin'_1 into the authentication request in Step 5. However, it is important that this value is included on client side, as fin_1 is intended to be checked against fin'_1 in Step 10 by SP.

The link between UA and IdP can also be protected by TLS Unique: If fin_2 is included into the authentication process in Step 7 (e.g., like described in Section 6.1), IdP can check whether an MitM is present or not. Alternatively, authentication methods may range from password based authentication as described to arbitrary cryptographic protocols [JKSS10].

After successful authentication of the user, IdP will include fin_1 into the issued authentication token (Step 8). This token is cryptographically secured – either by a digital signature or by an HMAC. Thus, the content of the token cannot be altered by an MitM.

In Step 9, the UA forwards the token to the SP through the previously opened session TLS_1.

Note: TLS_1 has to be kept active between UA and SP all the time. This is important, so the Finished message of the current TLS connection is still the same as was extracted as fin'_1 in Step 3.2. The TLS connection can, e.g., be preserved by sending keep-alives on the TCP connection below.

When SP receives the authentication token in Step 10, he compares fin'_1 to the value fin_1 read from the token. Access is granted in Step 11 if and only if both the authentication token is valid and $fin_1 == fin'_1$.

Based on the modification, the protocol can resist network based attacks, e.g. MitM. In this case, an attacker can act undetected until after Step 9 in Figure 4, because SP only sees a TLS connection with an anonymous browser up until then, and the MitM has tricked the UA into accepting a TLS connection with him.

Nevertheless, the Finished messages for the TLS sessions between UA and MitM and between MitM and SP differ from each other. Even if the attacker is able to intercept the authentication token during Step 9, he is not able to redeem it, because the token will be issued for $fin_{UA,MitM}$, whereas the MitM attacker is connected to SP via a TLS session described by $fin_{MitM,SP}$.

7 TLS Unique Implementation

This section provides an overview of necessary changes to client software and required Application Programming Interfaces (API) for successful integration of the proposed concept. As the solution has to be implemented at client side, it is necessary to modify the user's client software, such as the browser. For convenience, the solution can be provided as a browser plugin, integrating seamlessly and without user interaction. The plugin performs all required steps and only becomes visible in case of failures.

Additional Header-Fields To simplify HTTP message processing, it is beneficial to introduce a new HTTP Headers:

- `tls-unique-auth:` {`boolean`} – initiates the password-based login via TLS Unique.
- `tls-unique-sso:` {`boolean`} – initiates SSO via TLS Unique.
- `tls-unique-sp_fin:` {`char[]`} – contains the value of the *Finished* message.

The integrated browser plugin only activates if this particular HTTP Header-Field is encountered, otherwise it remains inactive as a background process.

API Implementation Unfortunately, the plugin requires additional APIs for access to lower SSL/TLS functionality - *the SSL/TLS PreMasterSecret, MasterSecret and derived key material MUST be kept secret and unaccessible*. We propose an API that provides low-level access to all SSL/TLS handshake messages - *this MUST only include access to raw messages, as they are supposed to be sent over the network, explicitly excluding outputs of decryption processes and access to internal states*.

With direct access to the necessary TLS messages, it is possible to extract the information needed for channel binding (eg. encrypted Finished message).

8 Conclusion

Current authentication mechanisms are prone to a variety of attacks, e.g., cookie theft or MitM. This way, an attacker may steal credentials or authentication tokens and use them to impersonate the victim.

The introduced TLS Unique approach holistically secures the whole login and/or SSO protocol flow by binding the authentication information to specific TLS sessions. We use the first Finished message to uniquely identify a TLS session and then cryptographically bind this identifier to the authentication data. Our approach covers the transport of credentials (e.g. a username/password combination), session cookies, and SSO authentication tokens. By using this approach, the exploit of a large number of previously found authentication flaws can be prevented.

TLS Unique can be implemented as a browser plugin, provided that the corresponding API is available to allow access to the required parameters (especially the first Finished message) from the TLS handshake. A few new HTTP headers have to be provided by the server to activate and trigger the plugin. Our solution describes a generic approach which can be easily adapted to other SSO protocols (e.g. OAuth and OpenID).

References

[AWZ10] J. Altman, N. Williams, and L. Zhu. Channel Bindings for TLS. RFC 5929 (Proposed Standard), July 2010.

[Bar11] A. Barth. The Web Origin Concept. IETF, RFC 6454, December 2011. `http://tools.ietf.org/html/rfc6454`.

[BDLF^{+}14] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Alfredo Pironti, and Pierre-Yves Strub. Breaking and Fixing Authentication over TLS. 2014.

[BH12] D. Balfanz and R. Hamilton. Transport Layer Security (TLS) Channel IDs. Internet-Draft, November 2012.

[Can13] Scott Cantor. SAML V2.0 Channel Binding Extensions Version 1.0, 2013. `http://docs.oasis-open.org/security/saml/Post2.0/saml-`

channel-binding-ext/v1.0/cs01/samlchannel-binding-ext-v1.0-cs01.html.

[DCBW12] Michael Dietz, Alexei Czeskis, Dirk Balfanz, and Dan S. Wallach. Origin-bound certificates: a fresh approach to strong client authentication for the web. In *Proceedings of the 21st USENIX conference on Security symposium*, Security'12, pages 16–16, Berkeley, CA, USA, 2012. USENIX Association.

[DR08] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. Updated by RFC 5746.

[DY83] D. Dolev and A. Yao. On the security of public key protocols. *Information Theory, IEEE Transactions on*, 29(2):198–208, March 1983.

[FHBH$^+$99] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart. HTTP Authentication: Basic and Digest Access Authentication. RFC 2617 (Draft Standard), June 1999.

[FSSF01] Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. Dos and Don'ts of Client Authentication on the Web. In *Proceedings of the 10th conference on USENIX Security Symposium - Volume 10*, SSYM'01, pages 19–19, Berkeley, CA, USA, 2001. USENIX Association.

[GJMS08] Sebastian Gajek, Tibor Jager, Mark Manulis, and Jörg Schwenk. A Browser-based Kerberos Authentication Scheme. In Sushil Jajodia and Javier López, editors, *Computer Security - ESORICS 2008, 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings*, volume 5283 of *Lecture Notes in Computer Science*, pages 115–129. Springer, August 2008.

[JKSS10] Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk. Generic Compilers for Authenticated Key Exchange. In *ASIACRYPT*, 2010.

[KS10] Nate Klingenstein and Tom Scavo. SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0: Committee Specification 02. "http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-holder-of-key-browser-sso-cs-02.pdf", August 2010.

[KSJG10] Florian Kohlar, Jörg Schwenk, Meiko Jensen, and Sebastian Gajek. Secure Bindings of SAML Assertions to TLS Sessions. In *ARES*, pages 62–69, 2010.

[KSTW07] Chris K. Karlof, Umesh Shankar, Doug Tygar, and David Wagner. Dynamic pharming attacks and the locked same-origin policies for web browsers. Technical Report UCB/EECS-2007-52, EECS Department, University of California, Berkeley, May 2007.

[LKHG05] Alex X. Liu, Jason M. Kovacs, Chin-Tser Huang, and Mohamed G. Gouda. A Secure Cookie Protocol. In *Proceedings of the 14th IEEE International Conference on Computer Communications and Networks*, pages 333–338, San Diego, California, October 2005.

[Mar09] Moxie Marlinspike. More Tricks For Defeating SSL In Practice. *Black Hat USA*, 2009.

[MBS07] Chris Masone, Kwang-Hyun Baek, and Sean Smith. WSKE: web server key enabled cookies. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security*, FC'07/USEC'07, pages 294–306, Berlin, Heidelberg, 2007. Springer-Verlag.

[PS00] Joon S. Park and Ravi S. Sandhu. Secure Cookies on the Web. *IEEE Internet Computing*, 4(4):36–44, 2000.

[SB12] San-Tsai Sun and Konstantin Beznosov. The devil is in the (implementation) details: an empirical analysis of OAuth SSO systems. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 378–390, New York, NY, USA, 2012. ACM.

ENX ID – An Architecture for Practical and Secure Cross Company Authentication

Michael Kubach & Heiko Roßnagel, Fraunhofer IAO
Lennart Oly & Immo Wehrenberg, ENX Association

michael.kubach@iao.fraunhofer.de
heiko.rossnagel@iao.fraunhofer.de
lennart.oly@enx.com
immo.wehrenberg@enx.com

Abstract: This paper introduces a development approach and a novel architecture for cross company identity management and authentication. It aims to design an architecture, which is practically implementable in the highly collaborative environment that exists in the automotive industry. The paper sketches the conducted marked research to obtain such a model and presents an architecture design based on a trusted intermediary.

1 Introduction

The automotive industry was among the first industries that had a high need on authentication, as it was among the first to rely on internetworked information technology to optimize its supply chain even across company borders [KWB03].

Today, use of internetworked IT is no longer limited to supply chains. It has been extended to many applications starting with the exchange of research and development data, reaching to real-time collaboration using telepresence and live collaboration systems like multi-user CAD systems, and even administration of production systems – the so called “shop-floor IT” [SRW05a]

A detailed description of the dense mesh of collaborating companies that exists in the European and worldwide automotive industry today is given in [WRZ12]. This mesh of interconnections is especially relevant to the development of new systems and whole cars. Nowadays, about 300 companies are involved in the development of a new car and more than 80 percent [IK07] of the value in a typical new car project is created by suppliers.

Generally, IT systems are secured by two major measures:

Perimeter-based security is the outermost security measure possible. It prevents even basic access to systems by limiting the access possibilities to a network. The most common method is to restrict critical systems to a non-public network – often enforced by firewalls. In the collaboration with many partners, these internal networks are no longer company-internal but instead cross-company as well [MR08].

Authentication to the system in question is the second measure. The most common authentication method again is username and password-based authentication [MO07].

In the automotive industry, as in all other industries, perimeter security is enforced by firewalls. Moreover, the automotive industry has an additional method of perimeter security that is called the *ENX Network*.

The ENX Network is a secure, interoperable and at the same time cross-company and multi-provider network. ENX Network access is restricted to user companies within the industry. Communication within the network is protected by cryptographic measures. Every user company connected to the network is authenticated cryptographically by a public key infrastructure. The network and its central services are controlled by an industry-steered independent association: the ENX Association [Ri11].

ENX Association is neither controlled by one particular company of the industry, nor controlled by a profit-oriented provider but instead by its members consisting of large automotive companies and associations. This made it possible in a unique way to create a global, widely accepted industry standard that reduces complexity significantly.

The ENX Network is an important building block of the increasingly interconnected structure in the automotive IT. However, even such a very strong perimeter protection is no longer sufficient to cope with all the different threats faced by the industry. Therefore, authentication as the second line of defense becomes more and more important. The significance of password-based authentication that came with its broad adoption as the standard IT authentication method has also revealed its many weaknesses [IWS04], [Pe94], [RR06].

Authentication is a vital part of identity management (IDM) as it ensures that the identity (ID) and its associated capabilities can only be used by the legit entity [Sc06]. If authentication fails, an ID may be stolen and used maliciously. A stolen ID enables all kinds of attacks on computer systems that cannot only create damage in computer systems, but has significant economic impact as well [ADS08]. It can even become a matter of life and death if one thinks of manipulated production robots within the shop-floor IT or gas-based fire extinction systems.

Therefore, it is evident that stronger methods of authentication are necessary [CF07]. From the user experience perspective, it is desirable to limit the number of authentication methods and credentials per user [DD08]. However, authentication methods and credentials are often difficult to implement across company borders or even industry-wide.

This paper presents an economically, legally and technically viable architecture to enable industry-wide authentication based on secure multi-factor authentication. The paper is structured as follows. In section 2 we describe the conducted research to identify the industrial requirements of the ENX ID cross company IDM architecture described in section 3. We conclude the paper in section 4 by summarizing the major results and discussing the limitations of our work.

2 Expert Interviews

2.1 Methodology

We chose the method of a qualitative analysis based on semi-structured interviews. The respondents were IT specialists with expertise in identity management (IDM) working for car manufacturers and suppliers in the automotive industry. The goal of the qualitative analysis was to reconstruct how these respondents see the challenges and chances of a viable IDM. Because the theoretical foundation of this topic is so far relatively underdeveloped, this approach does not aim to test concrete pre-formulated theories or hypotheses. Instead, the creation of a deeper understanding for the research subject was considered appropriate. For these reason, semi-structured interviews are the tool of choice for this research project. Interviews of this form constitute an established research-tool for such tasks [MN07].

The guide for the semi-structured expert interviews included targeted and open-ended questions and left room for further inquiries. It was derived from the theoretical analysis from the work in [Ro14], [WRZ12], and [RZ12].The interviews were conducted in the period from mid-2012 to mid-2013. Each interview took approx. 120 minutes. In three cases, the respondents agreed to an audio recording of the interview, which was fully transcribed. Audio recordings of other interviews were not possible due to company regulations, so the three interviewers each took handwritten notes, which were later combined.

Three interviews were conducted with three European automobile manufacturers and two European automotive suppliers. Geographically the focus of the study was located in and around Germany. Together with their Asian and American competitors, European automotive companies certainly are the leaders of the industry. Our respondents represent major and influential companies and are therefore well suited for our approach.

Most of the interviewees held senior positions in middle management with relations to IT security. In one case, we directly spoke with the Chief Information Officer (CIO). It can be assumed that the respondents have the necessary competence in terms of both function and of their position. Thus, we are following a key informant approach [Ho12].

The evaluation of the resulting transcripts from the interviews was carried out using MAXqda in version 11, a software for qualitative data analysis. We followed a thematic coding process, as there was no predefined coding scheme due to the underdeveloped theoretically foundation of the research. Without a set of established theories, no coding scheme could be derived ex-ante.

2.2 Results

Four main clusters where identified while looking at the results of the expert interviews: State-of-the-art, the drivers, the hurdles and the challenges for federated IDM.

State-of-the-art: The protection of intellectual property is a top priority for the companies in the automotive industry and has been gaining importance in the last years. Corporate IDM systems are state-of-the-art in our sample. Moreover, a clear trend towards strong and multi-factor authentication is evident. A respondent stated: *"Especially the security issue is on the rise. There is a trend away from passwords towards strong authentication. However, it always depends on the area of application."*

The close connection of the value-chain was made clear as well. Engineering departments of suppliers directly work in the development environments of the manufacturers. Smaller engineering bureaus access development data of larger suppliers via web-access. For strong authentication often own company smart cards or one-time-password-tokens are issued to partner companies. Traditional password-based authentication is used if handing out smart cards or tokens is not viable.

Drivers: The distributed value chain and the changing of partner causes a lot of work adjusting the IDM to different partners. In general, the transaction costs for enrolment/de-enrolment are significant. One respondent said that for smaller partners it is not always worth the effort. Strong authentication with PKI smart cards given out by one company is not always feasible. A security expert from an automobile manufacturer explained it like that: *"We have 2,500 supplier users. We cannot distribute 2,500 PKI smartcards to externals. This is logistically impossible as they are distributed all over the world."* Asked if ID federation allowing supplier company users to use their company tokens to authenticate and use services of the manufacturer would be seen as possible, the security specialist replied*: "I think so, but we care a lot about our security."*

These factors can be seen as drivers for a federated IDM. All companies in the sample have therefore started to think about ID federation. Some have completed or at least started pilot projects. A large association of the automotive industry is running a project on federated IDM. However, no company is using it in larger production processes yet.

Hurdles: Several hurdles for federated IDM were mentioned in the interviews. Security and control are major issues in this sensible area. Companies want to stay in control and are hesitant delegating to other partners that might be competing in some areas. As one respondent stated: *"We are blessed to work with foreign partners, but we are clearly obliged to define what is necessary to limit the access and the authenticity of the exchange."*

Other aspects that the respondents mentioned are more of legal or organizational nature. One respondent from an automotive supplier said that while technical challenges had been solved in a pilot project it went into hibernation in the hands of their lawyers. *„From a technical point of view everything worked in the end. Organizational and legal challenges were the problem."* Questions of liability in case of incidents like security breaches or downtimes are seen as difficult. The challenge of intra- and inter-organizational coordination between the divisions responsible for what and how the processes work in the case of such incidents are mentioned as additional hurdles.

Challenges: There are challenges related to the different systems and standards used by applications at different partners. These challenges were not seen as insurmountable. The technical problems in pilot projects of companies in the sample were solved or seen as not too significant. Frameworks like SAML are seen as valuable here.

Privacy is seen as an issue, as it is not yet clear which personal information can be shared with other organizations. First ideas how this could be solved by restricting the visibility of certain details of the information exist.

Organizational and control aspects are an issue when sensitive functions are to be delegated to customers or even competitors for the federation of identities. Interorganizational trust plays a major role here. Some of the respondents indicated that such a delegation could be possible with an independent intermediary serving as a trust anchor. A respondent from an automobile manufacturer stated*: “Definitely, I would prefer a model with an independent authority that is able to deliver identity or authentication. From my point of view, it’s a longer process to go through alliance-partner Y and the process isn’t preferred. Also, it’s difficult to trust the competitor in this matter or a third party because it is trusted by our competitor.”*

3 The ENX ID Architecture

3.1 Architecture Design Considerations

As confirmed in the interviews, companies already use corporate identity management (IDM) systems and do already support multiple secure multi-factor authentication methods. So far, all of these identities are limited to the particular companies itself. The solution to make these authentication methods available across multiple IT infrastructures is called federation. In the standard federation scenario, two companies would federate their IDM systems in order to make the identities from one domain available to the other and – if necessary – vice versa.

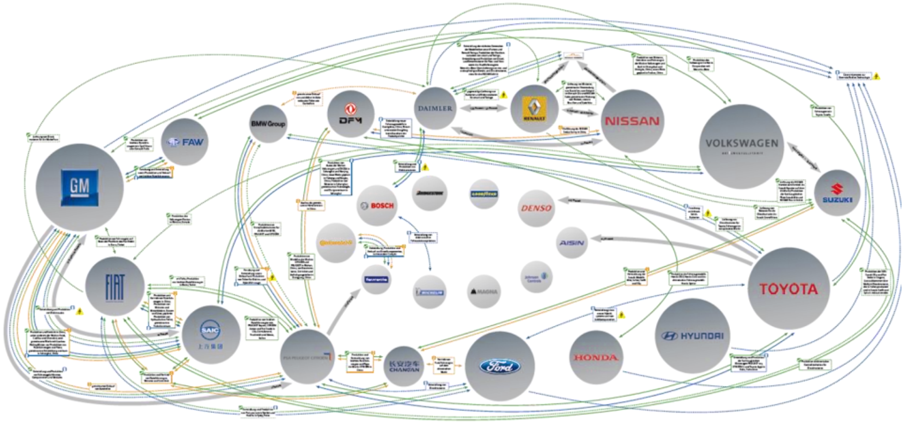


Figure 1: Who Cooperates With Whom - The Largest Automotive Manufacturers and the 10 Largest Suppliers [Vi12]

In the automotive scenario, this might be sufficient for individual cooperation between the manufacturers and large suppliers, but it is not practical to create an industry-wide direct federation. In that case, any company in the industry would have to federate with all its business partners. Figure 1 shows large development projects between the largest OEMs and the 10 largest suppliers. Even only focusing on those, the figure visualizes that this is already very complex. If one also considers simple contract work and includes the smaller and more specialized suppliers, it immediately becomes clear that such a setup would be far too complex to be practical.

Moreover, becoming relying party of a federated system requires trust in the assuring parties regarding the identities and authentication assurances received from the federated system. It was clearly stated in all interviews, that the establishment of this trust is seen as one of the biggest challenges for a broad federation. As shown in the interviews, this trust must be established in multiple areas:

Trust in the technical construct is the trust in the technical security and soundness of the architecture and all the systems involved. This trust can be established by creating clear and transparent criteria required to participate and an openly and transparent designed architecture. The compliance to these requirements must be auditable. As these audits especially at participating companies might reveal sensitive information, they must be conducted by an independent and trusted third party.

Trust in the legal construct can be established by creating a fitting, reliable, and transparent contractual construct. The contractual model must not require all companies to be direct contract partners but has to ensure a fair distribution of liability. Additionally, ID data is personal data and protected by law, so the architecture must respect data protection regulations. This becomes even more challenging as the automotive industry is actively engaged around the world and with that affected by several data protection laws.

Trust in the economical construct can be established by creating an architecture that supports a realistic business model and is backed by economically stable and conservative organizations.

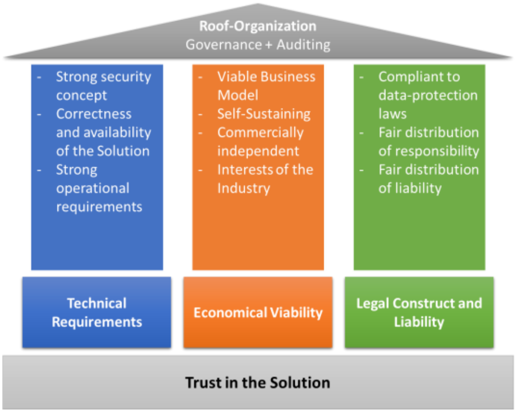

Roof-Organization
Governance + Auditing
- Strong security concept
- Correctness and availability of the Solution
- Strong operational requirements
- Viable Business Model
- Self-Sustaining
- Commercially independent
- Interests of the Industry
- Compliant to data-protection laws
- Fair distribution of responsibility
- Fair distribution of liability
Technical Requirements
Economical Viability
Legal Construct and Liability
Trust in the Solution

Figure 2: Three Pillars to Establish Trust

In all of these areas, the easiest way to establish trust is using a trust anchor. The trust anchor governs the whole construct, defines or assesses the technical criteria and conducts or coordinates the audits for the technical construct. Moreover, the trust anchor designs and is part of the contractual construct to distribute the liability reasonably. It also develops a business model, ensures that economic interests of all involved parties are addressed and with that, the economic viability of the architecture is ensured. The trust anchor must be accepted by all parties. As supported by the results of the interviews, the OEMs, representing different interests as they are in direct and strong competition, are unlikely to become a joint trust anchor for the architecture. Similarly, service providers having an interest to exploit the federated setup commercially are not well suited. A good trust anchor would be an established third party that represents the interest of the industry and does not represent the interest of a specific company.

ENX Association was founded by the industry for exactly this purpose within the ENX Network. The axiom of ENX Association is that cross-company services in a branch with the size and the level of cross-linking as given in the automotive industry have to be

- Sufficiently standardized and centralized in order to reduce complexity
- Offer the branch or industry a fair level of steering in order to govern the service and to the trust anchor
- Open enough in order to allow for competition among services offered

Therefore, ENX Association is proposed to take over a comparable role concerning the architecture described here.

3.2 Identity Intermediary for Federation of Existing Identity Management Systems

In order to reduce the complexity, the architecture does not aim to federate all companies with each other directly. Instead, companies federate with a central identity (ID) intermediary. This intermediary reduces complexity by requiring only one federation per partner instead of one for each partner at each partner. It can reduce complexity even further by solving two major challenges:

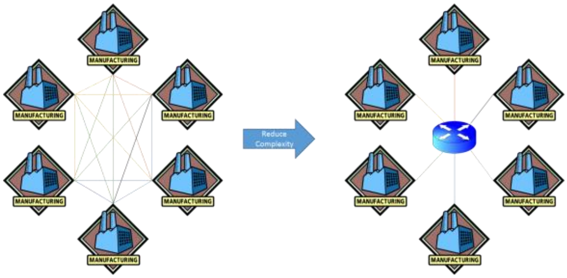


Figure 3: Complexity Reduction by Introduction of an Intermediary

To sanitize and normalize the input received by the parties that participate in the federation. As the federated parties have different systems and protocols are not always 100 percent compatible, the intermediary is able to sanitize the information received and forward it in a normalized way that is appropriate to the receiving party.

To translate different protocols. There are several ID federation protocols in different modes and versions available. The most important protocol nowadays is a specific mode of SAML 2.0. Examples for other protocols are OAuth, OpenID and WS-Federation. The intermediary allows participating parties to focus on one federation protocol and resolves the necessity of an industry-wide agreement on one. Figure 3**Fehler! Verweisquelle konnte nicht gefunden werden.** visualizes the complexity reduction by the intermediary.

3.3 One or More Independent Sources for Multi-Factor Authentication Methods

As explained before, the technical and procedural requirements for the federation are significant. This is completely acceptable for larger companies that have similar requirements on their internal IT. However, a important part of the automotive industry consists of small and medium-sized enterprises with very limited IT capabilities. For most of those, it would require a serious investment to fulfill the requirements.

This would consume the benefits of the participation in such a system. To overcome this challenge, the architecture proposed includes one or more identity providers (IDP) that supply identities to foreign users. This centralized IDP would issue secure ID tokens to its customers in a way compliant with the federation requirements. To ensure the highest security requirements, two-factor authentication is necessary. The interviews 3.1.2 have indicated that the industry sees ENX Association as an appropriate IDP. In the pilot implementation of the architecture, the IDs (“ENX-IDs”) will therefore be issued indeed by ENX Association. In an advanced production environment, a model with several competing IDPs offering different kinds of authentication methods federated with the central component in a varying manner is appropriate.

On a technical level, ENX Association has chosen modern cryptographic smart card based authentication method for the pilot. As described before, cryptographic smart cards provide high security based on a PKI, in this case the existing ENX PKI that is already trusted by the ENX user companies, which are a significant part of the industry.

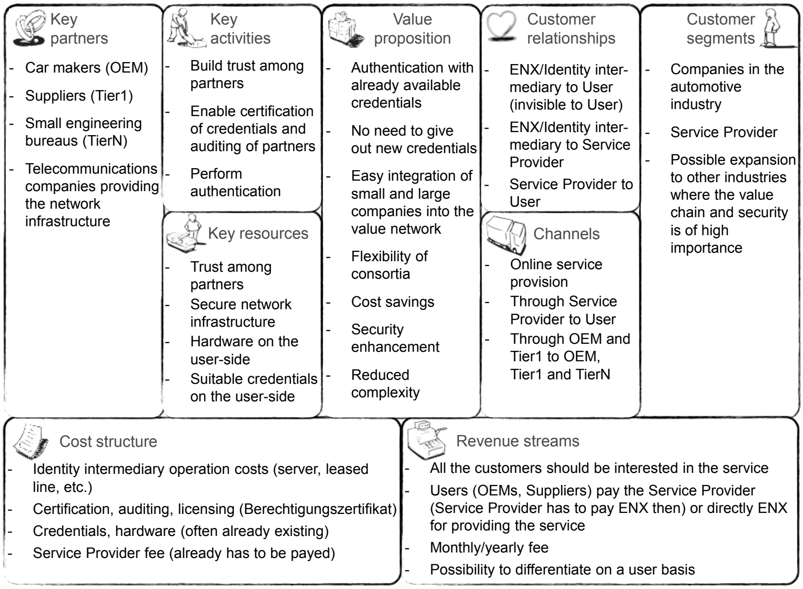
The processes and IT policies of medium-sized to large companies can make it very difficult to install security-relevant software on the client systems and almost impossible to integrate new hardware. Therefore, it was necessary to choose a solution that works with most hardware already available and requires minimal software support. Therefore, the chosen ENX-ID smart card can communicate using the contact-based interface as standardized in ISO/IEC 7816 as well as the contactless interface standardized in ISO 14443 and commonly referred to as NFC. The prototype card is running with the CardOS 5.1 operating system from ATOS due to its widely adoption and therefore minimizes the software requirements on the client systems.

The key feature of the ENX-ID is its ability to authenticate against the ENX-ID provider. The ENX-ID therefore hosts a secret RSA key suitable for authentication coming with a certificate issued by the ENX PKI. This certificate can also be used to authenticate to a Windows domain that is configured accordingly.

Smart cards are commonly used for other purposes that benefit from a secure key storage method. To add further value to the ENX-ID smart card, it can also be equipped with a key and a corresponding certificate of the ENX PKI for email signing. Finally, the user may store its email and hard disk encryption keys on the ENX-ID smart card.

3.4 Business Model

The business model structured according to [OP09] is outlined in Figure 4. In [Ro13] the different aspects of the business model are described in more detail.



Key partners

- Car makers (OEM)
- Suppliers (Tier1)
- Small engineering bureaus (TierN)
- Telecommunications companies providing the network infrastructure

Key activities

- Build trust among partners
- Enable certification of credentials and auditing of partners
- Perform authentication

Key resources

- Trust among partners
- Secure network infrastructure
- Hardware on the user-side
- Suitable credentials on the user-side

Value proposition

- Authentication with already available credentials
- No need to give out new credentials
- Easy integration of small and large companies into the value network
- Flexibility of consortia
- Cost savings
- Security enhancement
- Reduced complexity

Customer relationships

- ENX/Identity intermediary to User (invisible to User)
- ENX/Identity intermediary to Service Provider
- Service Provider to User

Channels

- Online service provision
- Through Service Provider to User
- Through OEM and Tier1 to OEM, Tier1 and TierN

Customer segments

- Companies in the automotive industry
- Service Provider
- Possible expansion to other industries where the value chain and security is of high importance

Cost structure

- Identity intermediary operation costs (server, leased line, etc.)
- Certification, auditing, licensing (Berechtigungszertifikat)
- Credentials, hardware (often already existing)
- Service Provider fee (already has to be payed)

Revenue streams

- All the customers should be interested in the service
- Users (OEMs, Suppliers) pay the Service Provider (Service Provider has to pay ENX then) or directly ENX for providing the service
- Monthly/yearly fee
- Possibility to differentiate on a user basis

Figure 4: Business Model Overview – Presentation Based on [OP09]

Even though ENX Association is operating the architecture as a service for the automotive industry without the need to maximize profit, it must nevertheless be able to cover its expenses for running the infrastructure. A possible business model with respect to the trust services builds on ENX Association's existing structure. Again, ENX Association can fill the role of the legal and organizational roof of a business model based on competition among service providers.

Following the general ENX approach, central authentication services can be provided by ENX Association while implementation of central ID services like the ENX-ID could be executed through specialized and certified ID service providers. Additionally, any application provider can use the central authentication services for a variety of individual use cases if the usage complies with the general usage policies and legal regulations.

If implemented in this way, the ENX Association will use its position of trust and apply it to new business. The complexity of the authentication between business partners in the industry is significantly reduced, without interfering with the free competition of providers and users and without restricting users in their selection of the service providers or services itself.

The cash flows in this model are initially similar to the original ENX business model. The stream of revenue goes from the automotive companies to the IDP who is charged by ENX Association for providing the central authentication service. Moreover, the companies participating directly in the federation would pay directly to ENX for the use of IDs from the central infrastructure. At least for an initial pilot period where ENX Association acts also as a central IDP, costs for direct management of individuals, organizational units, legal entities, credentials, roles and rights are expected to be higher compared to the current cost of the present model as it is based on the administration of corporate identities only.

3.5 Legal Aspects

Federated IDM including a third party that mitigates between different companies can be considered critical regarding data protection as personal data is distributed to a third party. However, [Sä13] shows, that the architecture is at least in Europe legally feasible if the contracts are designed carefully.

It is well imaginable to reuse the existing ENX contractual triangle as shown in Figure 5**Fehler! Verweisquelle konnte nicht gefunden werden.**. The performance and the cash flows are terminated by the triangle between ENX Association, certified service providers (CSPs) and users. All service components making up ENX today are offered to the user by a CSP in a bundle. Accordingly, a continuing obligation in respect of all recurring deliverables exist between service providers and users.

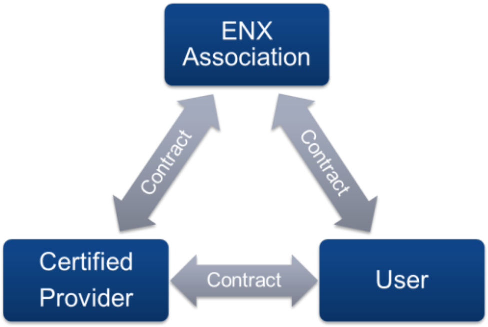


Figure 5: Contractual Relationship between the Involved Parties in the ENX Network

The ENX CSP provides these services to its customer. Based on an elaborate key (number of connections, bandwidth, quality levels, etc.) the service provider then pays a fee to the ENX Association for the central services in the overall construct.

The responsibilities of the participating parties are much higher than in the ENX Network scenario and have to be distributed fairly and carefully. It will be a major task of a pilot installation to include all legal requirements and to establish a working and agreeable contractual model that is trustworthy to all involved parties, supports the described setup and fits into the economic model.

4 Conclusion

The ENX ID architecture is an approach to make identities available in a community consisting of many companies of all sizes. It aims to reduce the complexity of secure authentication in a whole industry significantly and thus to make it practical for many applications. This is done by two key design decisions.

First of all, the ENX ID architecture reduces the federation configuration complexity per user from O(n) to O(1) by introducing an intermediary. Companies can chose to federate with this intermediary and immediately are able to accept user information and authentication data from all other federated companies.

Secondly, the architecture introduces one or more identity provider with secure multi-factor authentication methods that are also federated with the intermediary. These identity providers can be used by companies that are not federated with the intermediary.

The architecture relies on the ENX Association as an independent but controllable third party to generate trust. The ENX Association enables companies to trust into the federation by ensuring trustworthiness in three key areas. It enables the technical security by defining strong security criteria as a perquisite for federation and it certifies and audits. It ensures economical trust by establishing a business model that has proven its viability in a similar setup already. It will finally enable legal trust by a carefully designed contractual model and a careful analysis of the data protection law relevant issues.

References

[ADS08] Anderson K.B.; Durbin E. und Salinger M.A. (2008): Identity Theft. *Journal of Economic Perspectives*, 171-192.

[CF07] Clarke N.L. und Furnell S.M. (2007): Advanced user authentication for mobile devices. *Computers & Security 26*, 109-119.

[DD08] Dhamija R. und Dusseault L. (2008): The seven flaws of identity management: usability and security challenges. In: *IEEE Security & Privacy*.. S. 24-29.

[Ho12] Homburg C.; Klarmann M.; Reimann M. et al. (2012): What Drives Key Informant Accuracy? *Journal of Marketing Research*, 49. S. 594-608.

[IK07] IKB Deutsche Industriebank (2007): *Investitions-Outsourcing in der Automobilindustrie von Automobilindustrie*. http://www.automotive-rheinland.de/content/TOP_2_Kraus_IKB_071113.pdf2, [IWS04] Ives B.; Walsch K.R. und Schneider H. (2004): The domino effect of password reuse. *Communications of the ACM 47(4)*, 75-78.

[KWB03] König W.; Wigand R.T. und Beck R. (2003): Globalization and E-Commerce: Environment and Policy in Germany. *Communications of the AIS 10*, 33-72.

[MN07] Myers M.D. und Newman M. (2007): The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17. S. 2-26.

[MO07] Mannau M. und Oorschot P.C.v. (2007): Using a personal device to strengthen password authentication from an untrusted computer. In: *Conference of Financial Crypto*. Scarborough Trinidad and Tobago: S. Dietrich; R. Dhamija. S. 88-103.

[MR08] Maler E. und Reed D. (2008): The venn of identity: options and issues in federated identity management. In: *IEEE Security & Privacy*.. S. 16-23.

[OP09] Osterwalder A. und Pigneur Y. (2009): *Business Model Generation*. Amsterdam.

[Pe94] Neumann P.G. (1994): Risks of passwords. *Communications of the ACM 37(4)*, 126.

[Ri11] Riske A. (2011): ENX: Geschützte Datenübertragung in der Industrie. *iX 8/2011*.

[Ro13] Rossnagel H.; Sellung R.; Fähnrich N. et al. (2013): *FutureID Deliverable D21.5 Business and Use-case Analysis*.

[Ro14] Roßnagel H.; Zibuschka J.; Hintz O. et al. (2014): Users' willingness to pay for web identity management systems. *European Journal of Information Systems*, 23. S. 36-50.

[RR06] Recordon D. und Reed D. (2006): OpenID 2.0: a platform for user centric identity management. In: *ACM Workshop on Digital Identity Management*. Alexandra VA: ACM Press. S. 11-16.

[RZ12] Zibuschka J. und Roßnagel H. (2012): Stakeholder Economics of Identity Management Infrastructures for the Web. In: *Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012)*. Karlskrone, Sweden.

[Sä13] Sädtler S. (2013): Identity management in cloud computing in conformity with European Union law? Problems and approaches pursuant to the proposal for a regulation by the European Commission on electronic identification and trust services for electronic transactions in the i. In: Hühnlein D. und Rossnagel H. (Hg.): *OpenIdentity Summit*. Kloster-Banz. S. 116-127.

[Sc06] Schläger C.; Sojer M.; Muschall B. et al. (2006): Attribute based authentication and authorisation infrastructures for e-commerce provides. In: Bauknecht K.; Pröll B. und Werthner H. (Hg.): *E-Commerce and Web-Technologies*. Berlin: Springer. S. E-Commerce and Web Technologies.

[SRW05a] Spath D.; Renner T. und Weisbecker A. (2005): Inter-company business processes and ecollaboration. In: *The Pratical Real-Time Enterprise*. Berlin: Springer. S. 13-28.

[Vi12] Viavision (2012): Wer mit Wem? Die Verpflechtungen der Autobranche. *Viavision 04*.

[WRZ12] Wehrenberg I.; Roßnagel H. und Zibuschka J. (2012): Secure Identities for Engineering Collaboration in the Automotive Industry. In: *MIGW 2012 - Conference on Mobility in a Globalised World*. Bamberg. S. 1-12.

IT trends with impact on privacy and security

Petra Hoepner, Maximilian Schmidt, Christian Welzel
Kompetenzzentrum Öffentliche IT
Fraunhofer FOKUS
Kaisierin-Augusta-Allee 31
10589 Berlin
petra.hoepner@fokus.fraunhofer.de
maximilian.schmidt@fokus.fraunhofer.de
christian.welzel@fokus.fraunhofer.de

Abstract: Based on the revelation of broad surveillance programs and fundamental security risks, social discussions arise on security and privacy issues. This paper suggests a fundamental change in such discussions. Outlining current IT trends it recommends to focus on innovative perspectives rather than acquired behaviour.

1. Introduction

Privacy can be seen as the right of a person to act, feel and think decoupled from the community, unobserved and (at least actively) uninfluenced. In the digital world, privacy is primarily a matter of data protection and security. Identity management maps an analog identity to one or several digital identities and results in a filtered essence of privacy related information. Data integrity is essential to retain the value of such personal and identity-related data. Security is required to maintain that integrity and authenticity and is as such an important part for data protection and thus also for privacy. From a 2014 perspective, digital security mechanisms have been breached in many cases and therefore digital privacy as well. Stolen user data is no longer a rarity, even for large internet providers. Identity theft is one of the fastest growing forms of cybercrime (cf. [BSW$^+$11]), and thus a key challenge for the digital society in general. Additionally the apparent extent of monitoring by intelligence agencies combined with the helplessness of individuals and entire countries makes visible, that by simple means there is no absolute security. At least by means of usability, security seems to be always a compromise. Today the digital society is at a breaking point that can be seen as a chance to review and revise the understanding of privacy, data protection and data analysis.
To address the issue as a whole, this paper will not suffice. However, by outlining current IT trends it may stimulate the discussion and raise questions to fundamental issues that need to be worked on.

2. Future IT-Trends

This chapter briefly describes the latest trends ([WGA$^+$14]) of the digital discourse and connects them to the terms of privacy and identity management.

Ambient World
Ambient Assisted Living (AAL) describes technical systems that disburden everyday life. For this purpose, networked and partially autonomous installations of sensors, actuators and computers regulate, control and automate situational aspects of domestic life. However, providing automation and simplicity in everyday tasks and satisfying individual needs at the same time is a balancing act. It may result in an atmosphere of social isolation or helplessness, instead of improving comfort and safety and therefore strengthen freedom and independence. Crucial for trust in such systems is to safeguard against active or passive influences. This also includes an integrated identity management, which authenticates and distinguishes users. Additionally. when external systems are connected, issues about privacy and ownership of collected data become relevant.

Data- Philanthropy
Data Philanthropy means, that data is voluntarily provided in order to serve the common good. Based on such data, new knowledge can be found and new trends or changes discovered. Data donors can be individuals, businesses or public administrations.

For digital data resources to be used for the public good, trust and confidence in the data analysts are required. One way to gain confidence would be a free license model for data. Similar to the licensing model Creative Commons, it would offer the donor to determine the possibility for what purposes he wants to make its data available. Regarding anonymization of such data, it has to be taken care that individual data is proper handled and does not allow inferences about identities on its own.

Digital Integrity
The right to physical integrity is one of the main rights in many constitutions and one of the most fundamental human rights. With the increasing digitalization of society, the question arises, whether and how the fundamental right to physical integrity can be transferred to the digital world. Digital identities can be "stolen" and used to cause financial or personal damage. However, there are also substantial differences between physical and digital identity. In the digital world injuries might be undetected by the victim for years. Nevertheless these injuries coincide with significant consequences. Despite the virtual nature of digital humiliation and threats, the impact on the life of the victims can be serious and real.

Necessary but not necessarily sufficient conditions for ensuring digital integrity are the technical requirements for data protection and IT security: availability, integrity, confidentiality and authenticity. But digital integrity goes far beyond, in such as the goal of the users should be to handle their own data in a self-determined way. This includes deletion of published data, which is still an unsolved technical and social challenge.

Smart Data
The Internet has enabled entirely new forms of communication between human beings. New communication possibilities between objects, called "*Internet of Things*" open up technical requirements and social effects. These can by far surpass the first information technology revolution of the Internet with respect to observation, data production control, and self-coordination. This includes current trends like *wearables* and *drones*.

Wearables are one of many variations of inter-object communication and are best described as portable miniature electronics with sensors that occur as a standalone product, integrated into materials or even as an implant in organs. As such, they can be understood as the most personal form of IT utilization. They are becoming increasingly important in areas such as health, self-management, or for day to day assistance in various tasks. The price of such functional support is the disclosure of personal and sensitive data - especially if the *wearables* communicate with services on the Internet.

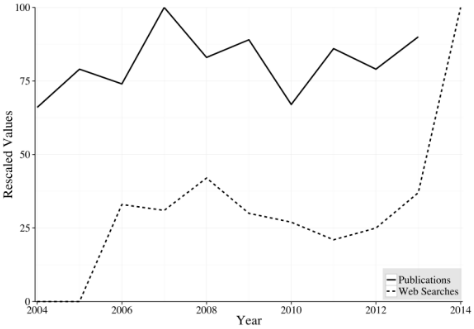


Figure 1: Relevance of "Wearables" in publications ([WGA+14])

Drones generally refer to unmanned aircraft, which are remotely controlled from drone pilots or operate autonomously. UAVs are mostly equipped with one or more sensors to detect the characteristics of the environment. Drones are another variation of object communication but are usually ignored in the broader discourse, since they directly attract attention in public and trigger an entirely different debate.

The trend word "*Internet of things*", as well as the latest developments of *wearables* and *drones* open up completely new social debates that can be bundled in the core theme of "Smart Data". And it is "Smart Data" that describes the actual problem: the accumulation, processing and analysis of personal data leads from a technical and legal point of view to questions about privacy, data integrity, data ownership and security regarding the underlying infrastructure.

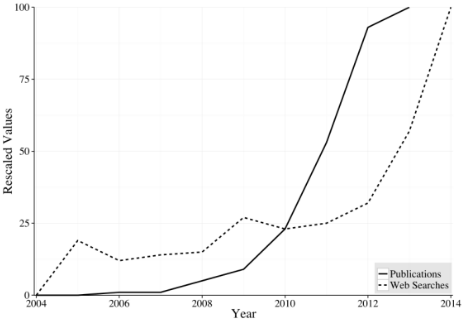


Figure 2: Relevance of "Internet of things" in publications ([WGA+14])

Prosument

With industrialization, there came a separation of production, reproduction and consumption. With today's *prosumer*, these separate spheres are reconnected by IT and evolve previously passive consumers to active producers. Information and electricity as well as music and media were the initial priority product groups, but a dramatic decline in prices by means of production (such as 3D printers) provides a potential of significant expansion of the phenomenon.

Where there are decentralized generated goods, there must be distribution platforms and a higher-level operational management. These instances have access to the give and take of *prosumers* and thus hold important and critical data. Depending on the application, such data partially allows for concrete conclusions to private data and thus requires specific technical policies for safeguarding and access.

Emerging authentication methods

Instead of using username/password or other single-factor authentication methods, future authentication methods must meet higher standards and incorporate several independent factors. In addition to the knowledge factor (secret, such as a password or PIN), factors of physical property (e.g. possession of a card) or biometrics (immutable physical characteristic) are of interest. Comprehensive solutions for 2-factor-authentication are researched and developed in various associations such as the FIDO alliance [SBT14], the initiative Liberty Alliance Project, or the Kantara initiative [SB10]. Lately, biometric characteristics and approaches with smartphones hit the market for innovative 2-factor authentication methods. Examples of biometric variants are smart phones with fingerprint scan, face recognition using cameras, iris scan, vein scan, bracelets for heart rate or other bio-profiles and head attachments for the evaluation of certain brain areas. Many, if not most, of these biometric technologies can be fooled by simple means and are not suitable for security-critical applications. Smartphones as a second authentication factor are a more realistic option, however great emphasis should be placed on data integrity, prevention of profile tracking and the security of communication channels.

3. The digital society

The term "*Digital Natives*" describes people who have grown up with the current up-to-date digital infrastructure. They possess and expect other approaches to knowledge supply, selection and processing, and implicate a new behavior and understanding of their environment (cf. [SDG+14]). They are "embedded" in a technical infrastructure that has always been there, and they are confronted with "Digital Outsiders” - people with traditional ways of thinking, etiquette and behavior. “Digital Immigrants” on the other hand describes a group between “Digital Natives” and “Digital Outsiders”, that has followed the digital revolution and adopted its tools and techniques. The terms are controversial and there is at least another group that might be called "Digital Mediators". "Digital Mediators" partly originate at "*Digital Natives*", partly at "*Digital Immigrants*" but have a broader understanding of the technical and organizational background. The question is, what the main differences in understanding and approaching the Internet are and how these groups can learn from each other.

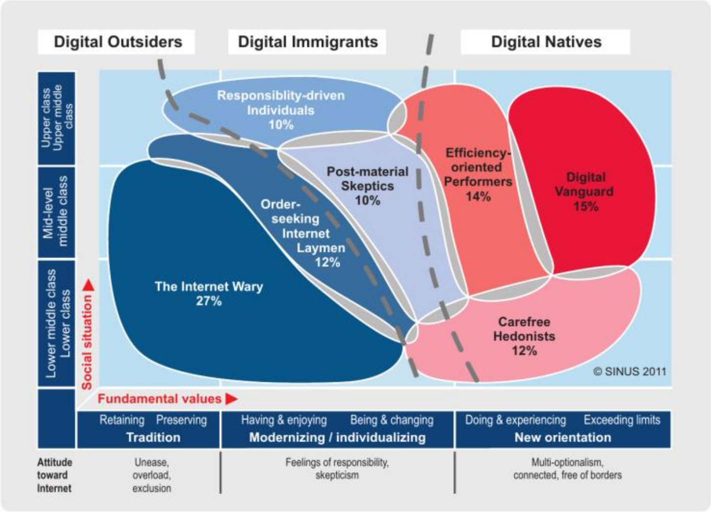

Digital Outsiders
Digital Immigrants
Digital Natives
Upper class Upper middle class
Mid-level middle class
Lower middle class Lower class
Social situation
Responsiblity-driven Individuals 10%
Post-material Skeptics 10%
Efficiency-oriented Performers 14%
Digital Vanguard 15%
Order-seeking Internet Laymen 12%
The Internet Wary 27%
Carefree Hedonists 12%
© SINUS 2011
Fundamental values
Retaining Preserving
Tradition
Having & enjoying Being & changing
Modernizing / individualizing
Doing & experiencing Exceeding limits
New orientation
Attitude toward Internet
Unease, overload, exclusion
Feelings of responsibility, skepticism
Multi-optionalism, connected, free of borders

Figure 3: Social environments to trust and security in the net ([SBR+13])

The key to an answer is the actual object and media of observation: the Internet and its different perception and use. While some are philosophizing about Industry 4.0, Internet of Things, Digital Estate, Copyright and privacy protection, others are busy playing with new gadgets, uploading their fitness rank to improve and compare their performance, or are collecting achievements using augmented reality tools.

Each of these actions and buzzwords operates a different viewing angle on a few basic requirements: It's about usability at maximum user experience, ease of data use and innovative data linkage. At the same time it questions data protection and privacy, high security and established moral principles. The question actually is, which of those requirements are in their definition still up-to-date and whether the different viewing angles from the aforementioned groups can be narrowed somehow to provide solutions or at least a common understanding that we can agree upon.

4. Conclusion

Summing up future IT trends

As seen in the "Future Trends of IT," many current topics cover the collection and linkage of data and identities. For this, systems are being used that can be questioned in terms of security and data protection. Currently, new and partly innovative variations of identity management and 2-factor-authentication are being designed and offered. However, all of them are based on the same old fragile infrastructure. With new authentication methods, security concepts are created, that may be invalidated by simple approaches on a more fundamental layer and are as such only partially convincing. Trends like the aforementioned add new aspects and requirements to digital identity management that need may not be covered by current technologies.

Questions on the future of identity management and privacy

With a view on the groupings of persons in the digital landscape, it might be a good idea to ask questions on the needs of "*Digital Natives*", because here lays the innovation. A mere glance at the current trend of crowd funding shows, that new ideas and methods are en vogue and yet find support - against the clichés of the convenience and laziness of the “average” user. Perhaps it is precisely the task of established companies to promote such innovations and to define privacy in a less constricting perspective? Do seemingly thoughtless posts in social networks really blur the boundaries between private and public or is it just a boundary shift? Facebook and Google have already set new standards of identity management and authentication with the adaptation of OpenID and OAuth, but we should not assume that they are able to redefine society. This task is a generational issue and is contrary to various dystopian fictions still decided by the masses of users themselves. With respect to that, "Digital Mediators" are in demand to take up the ideas of "*Digital Natives*" and bring them closer to the less tech-savvy users. The Internet was, is and will be always subject to attempts of control by governments or companies. However it will remain open and accessible since the fundamental idea and need for it is already there. Herein lays also an opportunity for change and renewal.

References

[BSW+11] Borges, G.; Schwenk, J.; Stuckenberg, C.-F.; Wegener, C.: Identitätsdiebstahl und Identitätsmissbrauch im Internet. Springer, 2011

[SB10] Soutar, C.; Brennan, J.: Identity Assurance Framework: Overview. Kantara Initiative, 2010. Available at https://kantarainitiative.org/confluence/download/attachments/38371432/Kantara+IAF-1000-Overview.pdf (Last access: August 2014)

[SBR+13] Schmölz, J.; Borgstedt, S.; Roden, I., Schäuble, N.; Tautschner, M.: DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet. DIVSI, 2013, Available at https://www.divsi.de/wp-content/uploads/2013/12/DIVSI_Milieu-Studie_Aktualisierung_2013.pdf (Last access: August 2014)

[SBT14] Srinivas, S.; Balfanz, D.; Tiffany, E.: Universal 2nd Factor (U2F) Overview. Fido Alliance, 2014, Available at http://fidoalliance.org/specs/fido-u2f-overview-v1.0-rd-20140209.pdf (Last access: August 2014)

[SDG+14] Schmölz, J.; Demattio, M.; Graudenz, D.; Borgstedt, S.; Roden, I.; Borchard, I.; Rätz, B.; Ernst, S.: DIVSI U25-Studie. DIVSI, 2014, Available at https://www.divsi.de/wp-content/uploads/2014/02/DIVSI-U25-Studie.pdf (Last access: August 2014)

[WGA+14] Weber, M.; Gauch, S.; Amini, F.; Kaiser, T.; Tiemann, J.; Schmoll, C.; Henckel, L.; Goldacker, G.; Hoepner, P.; Menz, N.; Schmidt, M.; Stemmer, M.; Weigand, F; Welzel, C: ÖFIT Trendschau – Mantelblätter. ÖFIT, 2014, Available at http://www.oeffentliche-it.de/documents/18/0/OeFIT-Trendschau-Vollversion (Last access: August 2014)

Analyzing the State-of-the-Art of Scientific Publications on Identity Management: Is there an Economic Perspective?

Nicolas Fähnrich, Michael Kubach

Fraunhofer IAO
Nobelstr. 12
70569 Stuttgart
firstname.lastname@iao.fraunhofer.de

Abstract: Although sophisticated identity management (IdM) technologies have been developed for quite a while, they are not as broadly used as could be expected – in the corporate but especially in an end-user context. Some authors have argued that the reason for this lack of diffusion is not to be found in technological or privacy shortcomings. Rather, it is attributed to the disregard of an economic perspective in the research on IdM and the development of IdM-technologies. This argument, has so far not been scrutinized in a systematic way. Therefore, this article performs a literature analysis of scientific publications to analyze whether there is indeed a lack of publications on IdM that employ an economic perspective. The results of the analysis seem to support the argument that the economic perspective is neglected in the current research on IdM.

1 Introduction

The business processes of modern companies these days are handled increasingly through networked information systems. These range from document management, through resource planning to human resource management. Use of these modern networked systems enables significant time savings and increased productivity, but involves in return a significantly higher risk that an unauthorized third party obtains access to confidential data. Especially in the recent years, the number of cyber-attacks has increased greatly. A report published by the company McAfee in July 2013 quantifies the worldwide damage from cybercrime to $300 billion per year [Ce14]. The dangers of such cyber-attacks are wide-ranging. Possible scenarios are image damage by the loss of customer data or a know-how loss due to industrial espionage. To protect the systems against the dangers of cybercrime, companies are forced to invest in preventive technologies of IT-security. It is predicted that global expenses in IT-security will increase from $55 billion in 2011 to $86 billion in 2016 [Ga12]. An important part of these IT-security-technologies represents the IdM in which the identities of the employees and the corresponding access rights are managed. The aim is to secure the data by ensuring that only authorized employees have access. Although the necessary technology is already available, it is so far not that widely used in the corporate sector and in the general population [KRS13]. As possible reason for this lack of diffusion it is stated IdM solutions oftentimes have been developed without the performance-relevant economic context with a focus mainly on technological aspects. Market structures and user requirements have barely been considered. To date, however, a systematic investigation of this argument based on the state-of-the-art of scientific publications is missing. The aim of this work is the literature-based evaluation of the state-of-the-art of scientific publications on IT-security with focus on IdM from an economic perspective. For this purpose, a research methodology is derived to identify relevant publications on this subject. These are then examined through a short qualitative analysis.

The structure of the paper is as follows. In the next chapter we describe and justify the development of the methodology employed for the literature analysis. Then, in chapter 4, we present the results of the quantitative and qualitative literature analysis. Finally, we give some concluding remarks in chapter 5.

2 Methodology

A literature review has two objectives in general. First, a summary of the existing literature with the goal to recognize patterns is created. Second, the conceptual content is identified. This allows uncovering previously unexplored scientific areas and supports developing new theories [KSM05]. A literature review is defined by Fink as follows: "A research literature review is a systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars, and practitioners" [Fi05]. A central problem in the analysis of literature is the scope of results that can be very large depending on the topic, making it virtually impossible to read everything. Only in emerging issues, or with search criteria that focus on a very narrow topic, a complete analysis is possible. Therefore, our analysis is divided into a quantitative and a qualitative part. According to e.g. Brewerton and Milward, these methods are not mutually exclusive but can be used in combination to increase the quality of results [BM01].

The research questions arise from the problem that underlies this paper. As described it was observed that there is a low diffusion of IdM in the population and in companies although IT-Security threats are significant and companies spend large amounts on IT-Security-measures. It was brought forward that the reason for this is a lacking focus on economic aspects in the development and the general research on IdM. Therefore, the literature analysis focuses on papers with an economic approach to IdM to explore, whether this perspective has indeed been disregarded so far. The search for publications on the topic of IdM that meet the defined boundary conditions (focusing on IdM while also considering an economic perspective) is done online with different search engines for scientific papers. For practical reasons, the search is limited to three search engines. After an internet research and literature review, the following potential search engines were identified: ACM (dl.acm.org), Google Scholar (scholar.google.de), IEEE Xplore (ieeexplore.ieee.org), LexisNexis (lexisnexis.com) and Scopus (scopus.com). In order to identify the three most effective engines a trial run with the keyword "identity management" was carried out. With 37.100 results Google Scholar provides by far the most extensive search result, with 995 results LexisNexis reached only 2.68 percent of this number. However, the number of results is not the only relevant factor for the selection of search engines. High numbers of results often come about through documents containing the search string, however, used in another context. This bias must be limited by setting detailed parameters. To achieve a balanced combination of search results, Google Scholar is chosen due to the high quantity and IEEE Xplore and Scopus are chosen for their subjectively high-quality results. Moreover, to provide for relevant high-quality results, the search strings are defined very specific and adjusted to the corresponding engines since not all search algorithms use the same syntax. The goal is to identify as many documents relating to IdM with economic aspects as possible. Therefore, "identity management" is used as the central keyword. To align the results to documents with economic considerations, this keyword is linked through Boolean operators with phrases such as "economic", "revenue", "cost" or "investment".

Quantitative content analysis is commonly known as "objective, systematic, quantitative and manifest" [La05]. In the given application, quantitative analysis however does not refer to a single document, but on the detected results. The quantitative analysis, as it is employed in this study, is mainly used to study parameters such as year of publication or the thematic direction. Then, building on the results of these analyzes possible trend developments are to be uncovered. The findings are presented in graphical form for all search engines that were eventually selected. The quantitative analysis enables an efficient analysis procedure, since the publications found are not read individually, but only need to be identified and quantified. This is useful to get an overview of a specific scientific issue as in our case. The meta-analysis is performed with a consolidated list of all results after removing all the duplicates. The result obtained following this method forms the basis for the subsequent qualitative analysis. In this step the content of the found publications is processed and presented.

3 Literature analysis

The search with the keywords derived as shown above, was performed with Google Scholar, IEEE Xplore and Scopus. The exact choice of keywords is highly dependent on the specifics of each of the search engines that can vary greatly. Therefore, no detailed derivation of the search strings is shown here but available on request. Although the search terms are explicitly chosen to find publications with economic context, it is expected that many publications from a technical background will be found.

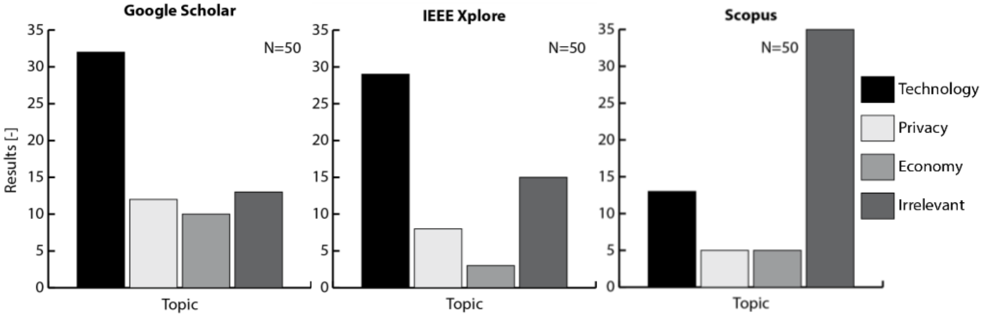


Figure 1: Thematic distribution of the first 50 search results from various engines

The results presented are categorized into papers covering the aspects of: Technology, Privacy, Economy and Irrelevant (for papers found with the chosen keywords but nevertheless covering none of the aspects relevant for this paper). The first 50 results for all engines are shown and categorized in figure 1. Google Scholar achieved 10 results with economic context and with that the largest number of relevant results. Scopus provides 5, IEEE Xplore 3 relevant results. For the quantitative analysis, all results from the years 2000 to 2013 without a limitation are taken into account. The data collection is performed by setting the release year parameter to the respective time period.

Figure 2 shows the distribution of the search results by years for all search engines (all results, no categorization into different topics). For Google Scholar, a steady increase in the number of results from 155 in the year 2000 to 2393 in 2011 is evident. The curve is almost linear in this period until it reaches its first peak from which the values remain more or less constant. IEEE Xplore provides only few results for the beginning of the period considered, followed by a fluctuating increase in the number of articles found up to the maximum of 61 in 2009. Then, the value drops significantly to 10 results in 2013. Scopus delivers results that form a curve pretty much similar to IEEE Xplore. Here, the peak is already reached in 2008, but this time with 43 results fewer are found by Scopus, with a less severe drop down to 28 articles in 2013. When comparing the curves of the three search engines, to some extent a similar development can be observed. For all curves, a strong increase of results in the years 2003 to 2008 comes evident. Furthermore, all graphs do have a maximum turning point. The decline in the number of results is particularly evident in IEEE Xplore and Scopus. The Google Scholar curve also drops at the end of the observation period, however only to a small extent.

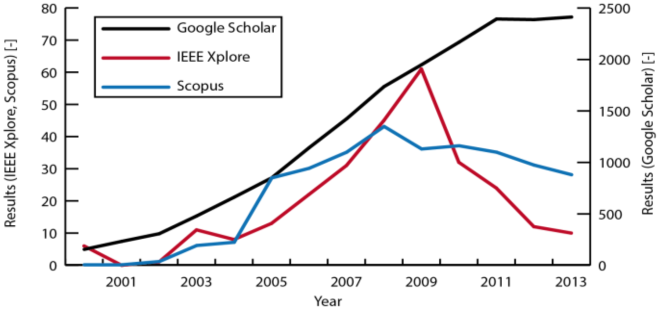


Figure 2: Distribution of the search results by years (2000-2013) for all search engines

A closer look at the curves shows some striking similarities between the quantitative development of the research on IdM and the so called Hype-Cycle. The Hype-Cycle is a graphical tool originally developed by IT research/advisory firm Gartner [Ga14] to represent the maturity, adoption and social application of specific technologies and innovations. Therefore, it must be highlighted that it can by no means be understood as a theoretically and empirically well-founded scientific method. However, it is an easily understandable tool and well suited for a first rough assessment in a case like this. The y-axis of the Hype-Cycle-Diagram represents the visibility or the expectations of a new technology, the x-axis represents time. The cycle is divided into five key phases of a technology's life cycle. Figure 3 shows the results of IEEE Xplore and Scopus compared with the Hype-Cycle. The visibility of the technology is measured by the number of search results. This seems to be a suitable indicator for the scientific community. When comparing the curves, obvious parallels can be recognized. As a maximum turning point was always reached or exceeded, the IdM technology is, based on this theory, currently between phase 2 and 3 of the Hype-Cycle. Of course, although the curves currently have a comparable course, the future development in direction of the phases 3 to 5 can't be predicted so far. A new comparison in 5 to 10 years could provide more evidence. However, it became clear that the first IdM hype has cooled down recently.

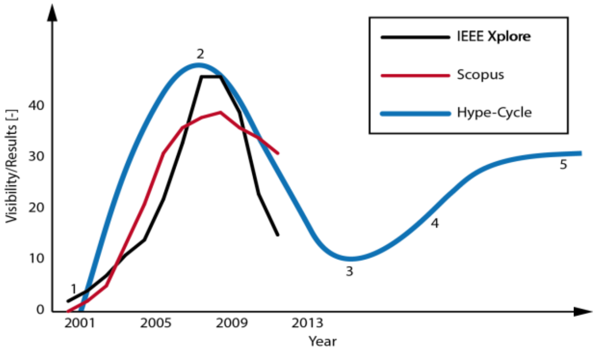


Figure 3: Results of IEEE Xplore and Scopus (moving average) compared to the Hype-Cycle

Now a qualitative screening of articles is performed to manually identify only articles that consider the economic perspective on IdM. Therefore, the first 50 relevant results of each search engine are categorized into the four categories described above. This time, however, only articles that fit into the category "Economy" are considered. Besides economic aspects, some of these articles also consider privacy and technology aspects. We mark this accordingly. Figure 4 presents the distribution of the articles according to the year of publication. Some of the publications have a thematic overlap with the categories privacy and technology.

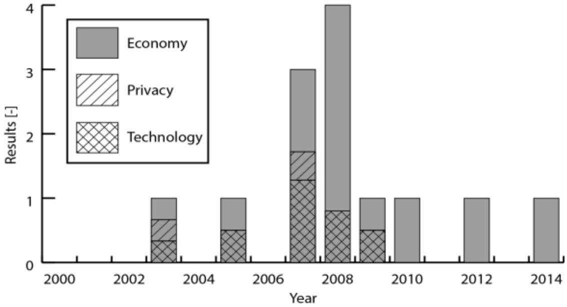


Figure 4: Results of the meta-analysis

The total number of relevant results amounts to 13 and the characteristic curve with a maximum turning point in 2008 as seen in the quantitative analysis is recognizable. A table listing the identified and categorized publications is available on request. Considering the original total quantity of search results was 150, then only 8.7 percent of the publications really cover economic aspects. Most of these articles were published in the past 6 years. This clearly shows that only very few publications so far employ an economic perspective and that this perspective is a relatively young stream of research.

4 Conclusion

Even though IdM technologies have been developed for quite a while, they are not as commonly used as could be expected – in the corporate but especially in an end-user context. Some researchers see the reason for this lack of diffusion not in technological or privacy shortcomings. Rather, they attribute it to the disregard of an economic perspective in the research on IdM and the development of IdM-technologies. As this argument has so far not been scrutinized in a systematic way, such an investigation was performed in this paper. Therefore, a literature analysis of scientific publications was performed to analyze whether there is indeed a lack of publications on IdM that employ an economic perspective. First, a keyword-based search of relevant scientific databases was performed. Then, articles were qualitatively screened and categorized. The results of the analysis actually seem to support the argument that the economic perspective is neglected in the current research on IdM.

Of course limitations to our approach have to be considered. Due to resource constraints we had to limit the number of search engines to three and only screened the first 50 publications found with each of these engines. However, we hope that this approach already gave some valuable insights into the research topic and can serve as the foundation for an analysis covering more search engines and results in the future. What we think our paper definitely showed is that research in this area is still scarce and there are still plenty of pieces missing from the puzzle of the economic factors in IdM.

6 References

[Ce14] Center for Strategic and International Studies, "The Economic Impact of Cybercrime and Cyber Espionage," McAffee, 2014.

[Ga12] Gartner Inc., Forecast Overview: Security Infrastructure, Worldwide, 2010-2016, 2Q12 Update, 2012.

KRS13] M. Kubach, H. Roßnagel and R. Sellung, "Service providers' requirements for eID solutions: Empirical evidence from the leisure sector," in *Open Identity Summit 2013*, 2013.

[KSM05] H. Kotzab, S. Seuring and M. Müller, Research Methodologies in Supply Chain Management, Springer, 2005.

[Fi05] A. Fink, Conducting Research Literature Reviews: From the Internet to Paper, SAGE Publications, 2005.

[BM01] P. Brewerton and L. Millward, Organizational research methods: a guide for students and researchers, SAGE, 2001.

[La05] S. Lamnek, Qualitative Sozialforschung: Lehrbuch, Beltz PVU, 2005.

[Ga14] Gartner Inc., "Gartner Hype Cycles,". Available: http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp. [Acc. 18 04 2014].

A DNSSEC-based Trust Infrastructure

Bud P. Bruegger, Eray Özmü

Fraunhofer IAO,
Universität Stuttgart
Nobelstr. 12,
Allmandring 35
70569 Stuttgart
bud.bruegger@iao.fraunhofer.de
eray.oezmue@iat.uni-stuttgart.de

Abstract: The management of trust issues is central to a wide variety of digital systems, including systems dealing with electronic signature, authentication, or signing of applications. The common approach to trust management is the use of possibly signed trust lists and trust stores that enumerate trusted issuers. This approach fails to scale well and is thus unsuited for the implementation of larger trust infrastructures, as, for example, in support of a regional authentication infrastructure that enables a marketplace of services.

This paper proposes to use the domain name system (DNS) with security extension (DNSSEC) as a base for the creation of a globally scalable and flexible trust infrastructure. As opposed to trust lists or stores, this also provides a vehicle for the efficient and secure dissemination of trust information among stakeholders.

1 Introduction

Trust decisions are crucial in identity and access management. While trust is an overloaded term, in this paper, it refers to the decision of whether a certain assertion can be accepted or whether it has to be rejected with an error message [Ca14].

Although being a central issue, the details of how to manage trust are often excluded from the scope of standards and systems. This is for example documented in [Ca14] for the case of the SAML 2.0 standard and the Shibboleth system. Instead, users of the technology are finally responsible for how they actually implement trust management.

The most common approaches to trust management are local trust stores and trust lists. Particularly for larger scale systems, they put a significant burden on relying parties who need to securely provision trust data (e.g., certificates or trust lists), keep them up to date, and query them for individual trust decisions.

To overcome these issues the authors present a trust infrastructure that is based on the Domain Name System (DNS) which scales very well, eases the burden on relying parties, and allows for highly efficient queries to support individual trust decisions.

While the proposed approach is applicable in many areas, for simplicity, the present description is limited to the use case of federated authentication. In particular, a relying party receives an assertion from some Identity Provider and needs to determine whether this assertion is trustworthy.

The STORK project [KO11] gives an example, how issuers of identities for authentication can be managed in various trust schemes (level 1 through 4) as determined by national trust scheme authorities.

The described trust infrastructure is part of the FutureID project [Ma13]. A minimal prototype has already been implemented.

The remainder of this paper is structured as follows. The next section describes previous and related work, also showing how the proposed approach solves problems experiences with the currently used trust lists. The main ideas of the approach are described in section 3. Section 4 draws conclusions.

2 Previous and related work

This section discusses the shortcomings of trust lists that are the most common current solution for large scale trust management. It then describes recent DNS-based technologies that have strongly influenced the proposed approach.

This paper focusses on a globally scalable trust infrastructure that supports an open number of trust schemes by arbitrary issuers. Relying parties make use of trust schemes to make individual trust decisions.

The most common solution for this problem are signed Trust Service Lists (TSLs) [ETSI09]. One of the best known examples is that of qualified certificates managed by the European Commission in support of legally binding signature [Ma13]. The Commissions TSL contains pointers that delegate the issuance of national TSLs to Member States who contain data of accredited issuers of qualified certificates. This single trust scheme is thus implemented by multiple TSLs.

Using TSLs, a relying party needs to locate and download the European and all national TSLs and keep them up to date. For individual trust decisions, it needs an efficient mechanism to query the data contained in the various TSLs.

Assuming that in a context such as that envisioned in FutureID, a relying party has to manage a significant number of trust schemes, relying parties also require a secure mechanism for locating the authentic TSLs of the various issuers.

The proposed approach eases the burden of relying parties as follows. Issuers of TSLs publish their data via DNS. Individual trust decisions can thus be based on a highly efficient single DNS query. Relying parties are relieved from managing updates. Also, the domain name is used to securely locate the desired trust data and thus largely facilitates the provisioning of trust anchors. DNS also provides native mechanisms for delegation.

The trust infrastructure proposed in this paper is an adaptation of DNS-based Authentication of Named Entities (DANE) [HS12] which uses DNS with its security extension to manage trust in TLS server certificates. Our approach thus joins a family of DANE adaptations in support of various trust problems, e.g., the association of OpenPGP public keys with email addresses [Wo13]. A master thesis [Jo00] illustrates how DNS queries are more efficient compared to LDAP queries for a similar problem.

3. A DNS-based trust infrastructure

This section gives an overview of how to use DNS to manage trust in assertions.

Figure 1 shows the three stakeholders and system components. Identity providers (IdPs) and relying party are well-known from federated identity managment. The trust scheme authority evaluated IdPs and publishes which IdPs have been found to be trustworthy. For this purpose, they operate a DNS server; relying parties use a DNS resolver.

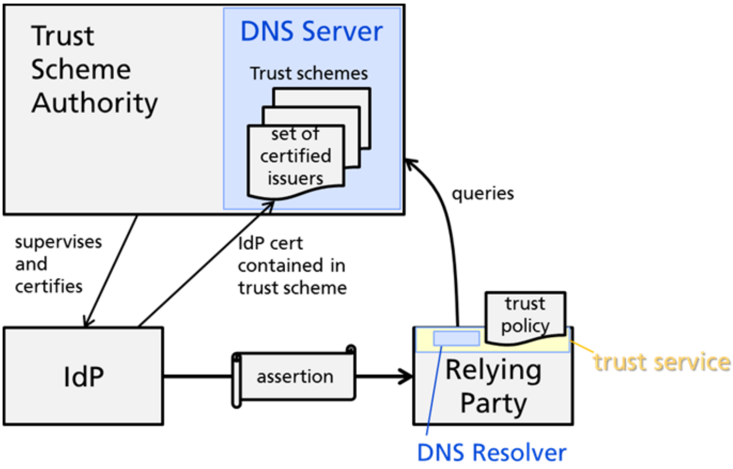


Figure 1 Overview DNS-based trust infrastructure for authentication

In the figure,a relying party receives an assertion from the identity provider. The relying party has to validate this assertion based on its issuer certificate and a trust policy.. The trust policy determines the trust schemes an acceptable IdP can belong to. Whether a given IdP belongs to a given scheme is established via a DNS query where the scheme corresponds to a DNS domain and an issuer to a host. If the IdP is contained in the scheme, the query returns a digest of the issuer certificate.

3.1 Publication of sets of certificates by trust scheme authorities

This section describes how trust scheme authorities use the DNS to publish sets of IdP certificates. The use case is an Europe-wide certification of IdPs following the proposal by STORK.

A trust scheme authority is uniquely identified by its domain name. For example, the atrust scheme authority of the European Commission could use *tsa.ec.eu*. A trust scheme authority can manage several trust schemes. Each schema is represented by a sub-domain. For example, the European Commission may manage a scheme for authentication under *auth.tsa.ec.eu*.

Optionally, a trust scheme may be divided into several sub-schemes. For example, the STORK trust scheme distinguishes four assurance levels: *level1.auth.tsa.ec.eu* through *level4.auth.tsa.ec.eu*.

It is common that a trust scheme authority may delegate authority to geographic or other kinds of sub-authorities. Again, using common mechanisms provided by DNS, this can be expressed in terms of sub-domains: *at.level4.auth.tsa.ec.eu*, *uk.level4.auth.tsa.ec.eu*, etc.

Once all necessary schemes and sub-schemes are defined, the resulting sub-domains need to be populated with IdP certificates. To use DNS as dissemination vehicle, certificates thus need to be mapped to host labels.

Several options of how to map certificates to DNS host labels exist[1]. For the first prototypical implementation of the trust infrastructure only the base32-encoded digest of the certificate is considered. An example for a host label is *PX2NO4LVPA4WHCBLYXHIKRWVRE.at.level4.auth.tsa.ec.eu.*

3.2 Validation of electronic artifacts

A relying party who receives an electronic artifact must verify whether its certificate is permitted by the trust policy. The trust membership claim provided by the issuer helps to efficiently validate the artifact in two steps:

- Verify that the claimed membership satisfies the policy,
- Validate the claimed membership relative to a locally defined set or remotely with a trust scheme authority.

In the case where the set is defined by a trust scheme authority, DNS with DNSSEC extension offers all necessary mechanisms to securely validate membership. DNSSEC makes it possible to transfer data about set membership securely, in the sense that the relying party can verify that the information was provided by the trust scheme authority who controls the according domain name and that the data has not been tampered with in transit. DNSSEC further enables a trust scheme authority to assert the absence of a certificate from one of its sets.

With its delegation and caching mechanisms, DNS is proven to solve these kinds of queries in a globally scalable manner.

Relying parties require a high-level language to express which issuers of electronic artifacts they trust. A key element to reach a high level of expressiveness is to use named sets of certificates much rather than enumerating individual certificates. This provides a simple, but highly expressive language to express trust policy. An example for a trust policy could look like the following:

badGuys := [<PEM1>, <PEM2, .., <PEMn>]

employees:= [<PEM1>, <PEM2, .., <PEMm>]

trusted := (employees & level4.white.authentication.tsa.ec.eu) – badGuys

3.3 Trust Membership Claims by Issuers

In support of efficient verification of electronic artifacts, their issuer should use mechanisms to indicate to relying parties that they have been certified in a given trust scheme by some authority. We call this trust membership.

In the best case the trust scheme authority's sub-domain is already included in the certificate or the public key is directly listed in the assertion. Depending on the assertion this could be achieved in different ways. The fields Subject, or Issuer Alt Name in a certificate could be used give the respective information (e.g. *issuerAltName: PX2NO4LVPA4WHCBLYXHIKRWVRE.it.qualified-white.tsa.ec.eu*). In SAML assertions the same information could be inserted into one of the available fields. The trust membership claims could also be located on a specific domain of the issuer's webserver. This must be on a standardized location relative to the issuer's domain (e.g. www.someissuer.de/tsa-meta.txt).

The authors want to emphasize that the trust membership claims are not security critical and are not needed to be signed, since the trust membership claims are verified by the relying parties.

4 Conclusions

This paper has proposed a DNS-based approach for managing a globally scalable trust infrastructure. It operates the application domain that is currently covered by Trust Service Lists (TSLs) and adds a vehicle for efficient querying and validation of individual elements of such lists, thus avoiding the need to operate a local cache of data from a potentially large numbers of such lists and the complexity of keeping such a cache up to date. To facilitate large scale deployment, the proposed infrastructure makes use of the existing global name registration provided by the DNS and the existing DNSSEC trust anchors.

The proposed approach joins a growing number of initiatives, led by DANE, that apply DNS with security extension to trust-related application areas. It thus shares the objective of finding more secure alternatives to the traditional PKI-based management of trust. Thanks to the significant innovation of DANE, only a relatively small effort is necessary to extend its concepts to an interesting domain of application that is important for the large scale use of digital signature and large scale identity management infrastructures as those foreseen by the EC in support of an evolving single market of online services.

The proposed trust infrastructure has been conceived as part of the FutureID project that develops such an identity management infrastructure. It follows the same philosophy of decentralization used by the project. The proposed infrastructure will be implemented and demonstrated in this context.

References

[Ca14] S. Cantor, “TrustManagement,” Shibboleth, 25-Jan-2010. [Online]. Available: https://wiki.shibboleth.net/confluence/display/SHIB2/TrustManagement. [Accessed: 13-Jun-2014].

[ETSI09] “ETSI TS 102 231 V3.1.2 (2009-12) Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information.” ETSI, Dec-2009.

[HS12] P. Hoffman and J. Schlyter, “The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.” Internet Engineering Task Force (IETF), Aug-2012.

[Jo00] S. Josefsson, “Network Application Security Using The Domain Name System.” Jun-2000.

[KO11] Körting, Stephan and Diana Ombelli, “Mapping security services to authentication levels - Reflecting on STORK QAA levels.”. 2011 .

[Ma13] Martens, Tarvi, Keskel, Maili, Hühnlein, Detlef, Özmü, Eray, Ituarte, Nuria, and Rath, Christof, “WP43 - Trust Service.” FutureID, 11-Dec-2013.

[Wo13] P. Wouters, “Using DANE to Associate OpenPGP public keys with email addresses.” 21-Oct-2013.

Using a whatsapp vulnerability for profiling individuals

Sebastian Kurowski

Competence team identity management
Fraunhofer institute for industrial engineering IAO
Nobelstr. 12
70569 Stuttgart
sebastian.kurowski@iao.fraunhofer.de

Abstract: This paper aims at raising awareness on the issue of using unfixed vulnerabilities for targeted attacks in order to harness private or even corporate information. We demonstrate an attack by using a well-known, yet not fixed whatsapp vulnerability, enabling us to eavesdrop the cell-phone number of a victim. We identified the concrete states, in which whatsapp leaks the cell-phone number of a victim. By using a volunteering individual, we demonstrate the feasibility of profiling the individual and provide further steps on how to disclose private and corporate information by using the leaked cell-phone number and the profiled information to introduce the adversary into a trust relationship with the victim. Once the victim trusts the adversary, social phishing can be used to retrieve further private or even corporate information.

1 Introduction

The Whatsapp Instant Messenger App[Wh14] has so far provided a working and usable alternative to the short messaging service (SMS). Whatsapp uses the internet connection of a smartphone to deliver short messages free of charge. Due to this advantage, Whatsapp was able to emerge as the most popular instant messaging application for smartphones, and currently delivers 500 million customers[Ec14]. However, this application was in the past not very successful in providing sufficient security and privacy features. Up to 2011, text messages, and cell phone numbers were transmitted unencrypted, despite of the App using the SSL protocol, which could have been used to encrypt the data [Yo11]. Additionally, various attacks were possible on both user authentication, and user data [SFK12]. In a reaction to this finding, Whatsapp implemented encryption of the transmitted data, between the Whatsapp client and the servers, however the cell phone number of the Whatsapp user was still transmitted as plaintext [He12]. In this paper, we describe a way of profiling an individual, taking advantage of the cell phone number being transmitted as plain text.

2 Retrieving the cell phone number

The attack described in this paper, uses a known vulnerability in the Whatsapp messenger. The current implementation of Whatsapp leaks the cell phone number [He12], which can easily be read by using a TCP sniffer, such as Wireshark or TCPDump.

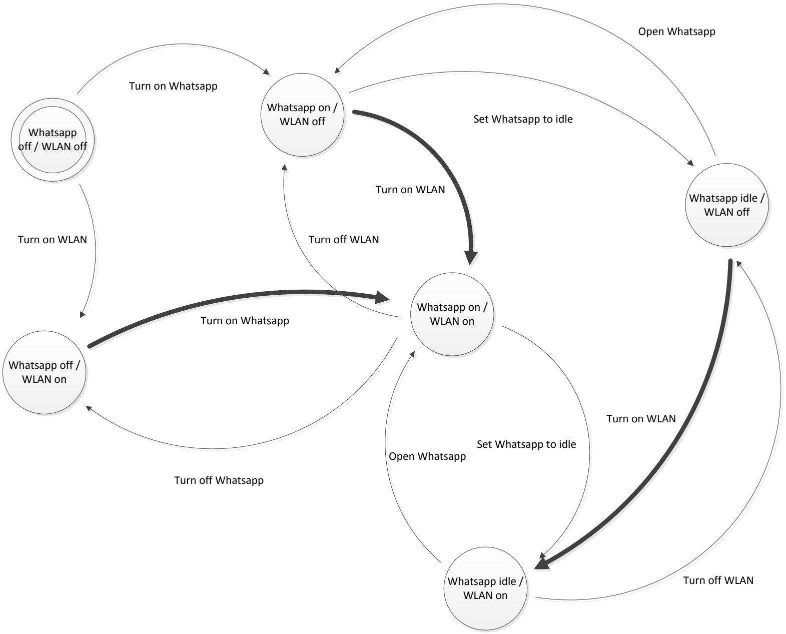


Figure 1 State diagram of the vulnerability analysis. Circles refer to tested WLAN adapter and Whatsapp states, lines depict a state transition (e.g. by opening Whatsapp). The bold lines indicate where the cell phone number is being leaked.

While the vulnerability of the leaked cell-phone number was already reported on, sufficient detail on when exactly this information is transmitted unencrypted was entirely missing. Therefore we conducted an analysis, showing the states in which the Whatsapp messenger leaks the cell-phone number, in order to evaluate the feasibility of retrieving this critical part of information. The test setup included both an iOS Version of Whatsapp (iOS 7.1), and the android version (Android 2.11). The Whatsapp version was 2.8.11. In the testing environment, a laptop equipped with Wireshark was used, to analyze the resulting traffic. All devices were connected with the same wireless LAN access point.

Using this setup, three different states of the Whatsapp app (on, idle, off), and two states for the WLAN adapter of the mobile devices (on, off) were used. The states for the

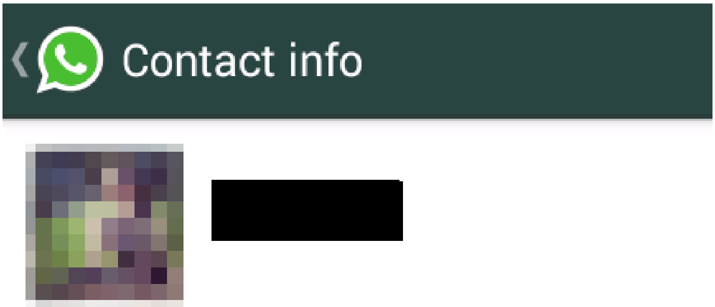
Whatsapp messenger app, referred to the app running and currently being opened by the user (on), the app running in background (idle), and the app not running at all (off), while on and off as states for the WLAN adapter, refer to the WLAN adapter of the mobile devices being turned on and off. Tested combinations of these states are shown in Figure 1. During the analysis the state transitions, which are depicted as lines in the diagram, were tested, e.g. the app was turned on and the resulting traffic was analyzed. This test was conducted with all possible states, allowing the exact identification of the states, in which the cell phone numbers are being leaked. These state transitions are marked bold in the diagram. The analysis showed, that the cell phone number was not leaked with every Whatsapp message, but only when (1) Whatsapp was being turned on, or (2) the wireless adapter was being turned on. This yields some restrictions for the described attack, meaning that the cell phone number can only be retrieved, when the app of the victim is not running, or the victim should not be connected to our used WLAN, before we start the TCP sniffing. Yet, the impact of this restriction remains questionable, as e.g. WPA2 secured WLANs require any TCP sniffer to obtain the handshake of targeted devices, before the attacker is able to decrypt the captured traffic. This means, that in WPA2 secured WLANs, the attacker must be sniffing before the victim connects to the same access point anyway.Knowing, when exactly to look for the cell phone number, we are now able to use a TCP sniffer, to obtain this attribute of the victim. In order to identify the cell phone number, we used tcpdump and regular expressions, to search for numbers. Hereby tcpdump runs on a laptop, dumping the captured traffic of the WLAN into a file. This file is then being analyzed by using a short and simple python script, which is searching the TCP dump for german cell phone numbers, using a regular expression.

By using this combination, it was conveniently possible to passively dump the traffic, while analyzing and finding the cell phone numbers, after collection. Therefore, an attacker is able to remain covered, e.g. by hiding the laptop with the TCP sniffer in a bag. The identified cell phone numbers were then parsed into a separate file, allowing easy access.

3 Using the cell-phone number for a targeted attack

Knowing how and when to retrieve a cell phone number from a potential victim, we are now able to use this knowledge for obtaining further attributes. The following describes an attack, which uses feasible and manual profiling, and the cell-phone number in order to establish a trust relationship between the adversary and the victim, and to retrieve private or corporate information by social phishing [QUOTE]. We conducted a small demonstration using a volunteering individual, showing the simplicity of the required profiling.

As we already described the concrete setup required for obtaining the cell phone number in Section 2, we will only briefly discuss this scenario. In this case, the adversary aims at being connected to the same W-LAN, as the victim. Identifying the victim could either be untargeted, or targeted. For instance, an adversary could connect to a W-LAN in a bar, obtaining cell-phone numbers and using the information provided via Whatsapp to pick a random victim. However, the adversary could also identify possible persons-of-interest, e.g. by observating persons leaving a corporation in the evening and trying to follow them to a bar. In the latter case, the adversary would just simply wait in the same W-LAN for the victim to enter and use its smartphone. As soon as the victim opens the Whatsapp messenger in the W-LAN the adversary is able to retrieve the cell-phone number of the victim as described in Section 2. However, the cell-phone number is a relatively weak attribute. While we could, e.g. subscribe the victim to certain services, we are probably not able to retrieve any further information about the victim, and thus not able to phish for private or corporate information. Luckily for us, Whatsapp users usually use a pseudonym along with a profile picture in their Whatsapp profile (see Figure 2).



[redacted]

Figure 2 Whatsapp profile of a victim.The name was blanked out, as the screenshot was made after the profiling was finished, and the contact could be included with the real name of the victim

These initial attributes can already provide sufficient information to kick-off a profiling of the individual. However, Whatsapp allows users to adjust their privacy settings, e.g. only individuals in the victims contact list are able to see the pseudonym or the profile picture. Yet, as the privacy settings are only retrievable by choosing “Settings”, “Account”, and then “Privacy” and thus relatively hidden, we are quite optimistic that this retrieval maybe promising. Additionally, recent events, such as the reset of the privacy settings due to software updates in Whatsapp to default settings, and thus full disclosure of some attributes [Sü14], allows for further optimism on this issue. As we want to obtain further attributes of the victim, in order to be able to access, e.g. facebook/linkedin/xing profiles, our primary interest is in obtaining the victims name. We used Google image search on the profile picture of the victim. By doing so, we were able to identify a second hand clothing platform, holding a pseudonymized profile of the victim.

By using this profile we were able to identify the city, the victim is living in. Additionally, our victim provided information on the current job position, which enabled us to use this attribute for further information gathering. Using google search with the pseudonym of the victim and the gathered attributes, however did not provide any results, as the victim did not seem to have reused the pseudonym. The clothing platform provided a follower list, showing a total of 20 followers on this particular accoiunt. Out of these 20 followers, only 2 were in the same city as the victim. Additionally we could identify one of those 2 followers (from hereon refered as friend A) as having the same affiliation as the victim. The profile page of friend A provided us with a picture. As with our initial picture search, we were able to obtain instagram pages related to friend A. However, the privacy settings of friend A, prevented us from viewing the profile directly. Yet, a friend of friend A, from hereon refered to as friend C, used less restrictive privacy settings, enabling us to retrieve an additional pseudonym of friend A. By searching for this pseudoynm, we discovered, that friend A reused this value on a facebook page, enabling us to find a past event, where friend A had participated, by using google on the pseudonym. Having obtained the facebook profile of friend A, which again prevented us from viewing any friends or any contents, due to privacy settings, we were still able to retrieve the groups, to which friend A had subscribed. By searching the publicly available member lists of these open groups, we finally discovered our victim and were able to obtain the full name.

As an attacker, we are now in posession of the victims name, cell phone number, pictures, affiliation, and we know with which persons our victim is befriended or otherwise associated. As our demonstration showed, it was relatively simple to retrieve the cell-phone number, the name of the victim, affiliation, pictures and friends of the victim. These attributes were collected in a relatively short timeframe: In the experiment we required approximately 10 mins, even though the victim had high privacy standards associated with their facebook profile. In the context of social phishing [JJJ07] we could already possess enough knowledge of the victim to obtain private or corporate information. The adversary could now contact the victim and provide a fake identity, e.g. the identity of one of the friends. This introduces the adversary directly into a trust relationship with the victim. As the adversary possesses a trusted attribute of the victim (the cell-phone number), providing a fake identity would result in more credibility of the attacker.

A possible conversation could thus look like this:

> Adversary: "*Hi this is Maria, I have a new cell-phone number but I am still using the old one from time to time.*"

Hereby "Maria" could stand for a friends name, which the attacker could easily obtain via facebook in our previous experiment. Now, let's assume the adversary wanted to obtain private information. In this case it would be feasible for the adversary to fake the identity of e.g. a family member in the same manner. In the case of targeting corporate information, the adversary would fake the identity of a working colleague, or associate of the same organisation. As soon as this message is sent, it is quite likely that the victim associates the adversary with the fake identity, and thus inserts the adversary into a trust relationship.

Finally, in the case of corporate information, this leads the adversary to sending a message to the victim containing a request, such as:

> Adversary: "*Hi, could you send me the last state of your CAD drawings? We require some information in there… Also I somehow cannot access my mails, so could you send it to my private one? adversary@SomeMailProvider.com*"

Et voila. We now have obtained corporate information, by using 10 minutes of manual profiling and retrieving the cell-phone number of a victim. Interestingly, in this attack the cell-phone number is not a strong attribute, as it cannot be used for profiling. However, possessing the cell-phone number allows the adversary to enter a trust relationship with the victim, while remaining anonymous. This offers the opportunity to either stalk the victim and exploit or retrieve private information [My05], or to phish for corporate information. The latter is based on social phishing [JJJ07], [KHH13], which exploits the trust relationship of a victim in order to retrieve information. Hereby this technique can exploit available information, in order to retrieve information, while contacting the victim via trusted channels. Experiments show, that this form of phishing is relatively promising, leading to success rates as high as 76% [JJJ07].

5 Conclusion

This paper describes an attack, by exploiting a Whatsapp vulnerability, basic Google searches and a small amount of time in order to retrieve private or even corporate information. We showed how to conretely retrieve a cell-phone number and discussed the severity of the adversary possessing an individuals cell-phone number, as being able to integrate itself into an anonymous trust relationship with the victim. We suggested social-phishing to retrieve corporate information, which proved to be quite effective in past resarch [JJJ07]. Other attacks would of course still be possible, once the adversary received details about the victim and its' cell-phone number, e.g. by using the knowledge for a pretexting attack in order to obtain access to a system [Ne08].

An interesting finding throughout the demonstration showed to be the low effort required to profile an individual even with high privacy standards associated with the individuals account. Due to not adjusted privacy settings in Whatsapp, we were able to obtain a picture, and thus collect information of the individual. While the full name of the victim could not be initially retrieved, due to privacy settings, and while privacy settings of befriended accounts of the victim prohibited us from accessing the profiles, a lack of privacy settings at the friends, of the individuals friends enabled us to retrieve enough information to finally obtain the full name. Having access to information rich profiles, such as facebook, could now enable us to extend our attack, and e.g. actively stalk the individual.

Whereas this is mainly a privacy issue, in combination with social phishing for corporate information, the privacy issues of the individual in a private setting, suddenly emerge towards security issues for a corporation.

Another interesting aspect which arised throughout the demonstration lies in the applicability of the retreived attributes in Whatsapp. The google image search, merely produced usable results and completely failed in providing similar images of the individual, except for large amounts of false-positives. Yet, the reuse of the Whatsapp profile picture, led us directly to an associated account which we could easily use for profiling the individual.

Therefore, this contribution raises awareness on the issues of privacy and security and their alignment with regard to corporate information. Whereas the privacy issues may create a risk for the well-being of the individual in this setting [My05], they can also create security issues and the disclosure of sensitive corporate information in combination with social-phishing [JJJ07], [KHH13].

References

[Wh14] WhatsApp Inc, „Whatsapp“, 2014. [Online]. Verfügbar unter: http://www.whatsapp.com.

[Ec14] M. Eckstein, „Whatsapp knackt halbe milliarde“, *connect*, Apr-2014. [Online]. Verfügbar unter: http://www.connect.de/news/whatsapp-nutzerzahlen-rekord-halbe-milliarde-wachstum-2246210.html.

[Yo11] YourDailyMac, „WhatsApp leaks usernames, telephone numbers and messages“, *YourDailyMac*, Mai-2011. .

[SFK12] S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, und E. Weippl, „Guess who’s texting you? evaluating the security of smartphone messaging applications“, in *Proceedings of the 19th annual symposium on network and distributed system security*, 2012.

[He12] heise, „WhatsApp versendet keinen Klartext mehr“, *Heise Security*, Aug-2012. [Online]. Verfügbar unter: http://www.heise.de/newsticker/meldung/WhatsApp-versendet-keinen-Klartext-mehr-1673054.html.

[Sü14] Süddeutsche.de, „Whatsapp-Nutzer plötzlich wieder gläsern“, *Süddeutsche.de*, Sep-2014. [Online]. Verfügbar unter: http://www.sueddeutsche.de/digital/beschwerde-von-nutzern-whatsapp-aendert-online-status-nach-update-automatisch-1.2124693.

[JJJ07] T. N. Jagatic, N. A. Johnson, M. Jakobsson, und F. Menczer, „Social phishing“, *Commun. ACM*, Bd. 50, Nr. 10, S. 94–100, 2007.

[My05] M. Secret Mysterypants, „Stalking for beginners“, *VICE*, Nov-2005. [Online]. Verfügbar unter: http://www.vice.com/read/stalking-v12n10.

[KHH13] K. Krombholz, H. Hobel, M. Huber, und E. Weippl, „Social engineering attacks on the knowledge worker“, in *Proceedings of the 6th International Conference on Security of Information and Networks*, 2013.

[Ne08] J. P. Nehf, „Pretexting: Protecting Consumer Telephone Records from Unauthorized Disclosure“, *Fed Comm LJF*, Bd. 60, Nr. 53, 2008.

Approach to Vendor Authentication

Detlef Houdeau, Amit Kumer Meher

Infineon Technologies AG,
Am Campeon 1 – 12
D 85579 Neubiberg

Detlef.Houdeau@infineon.com,
Amit.Meher@infineon.com

1 Background

With the remarkable and ever increasing technology growth, we need various products and services from different vendors, such as:

- Home appliances
- Furniture
- Mobile
- Internet

To deliver these products and provide services, representatives from concerned companies visit our place. We somehow need to ascertain if the person visiting is an authentic representative from the concerned vendor. In many countries, there are cases where an imposter visits as a company representative and indulge in theft or even murder of the persons at home.

2 Objective

The main objective of the Vendor Authentication Technique is to prevent customers from being cheated by impostors visiting them as a customer support official of a certain organization.

2 Method

Current Solution:

To examine the authenticity of the vendor representative the customer generally asks the vendor representative to produce an Office ID Proof and Government ID Proof. However, this procedure may not always be secure enough and the customer may become a subject to fraud in lieu of fake ID Proof provided by the so called vendor representative.

Proposed New Solution:

Following are the steps need to be followed by the customer and the vendor representative there by visiting the customer place in person for a successful establishment of vendor authentication. Figure_1 gives a pictorial representation of the same.

1. The customer will ask the vendor to provide his/her official ID or registered mobile number.
2. The vendor representative provides the same detail asked by the customer.
3. The customer will send an SMS to SMS Server, which is supported by the vendor for vendor authentication procedure.
4. The SMS Server will check the authenticity of the vendor representative's official ID or mobile number and will generate a secret code.
5. The SMS Server will send one SMS to the customer with the necessary detail about the vendor representative and the secret code.
    a. Name
    b. Gender
    c. Designation
    d. Any Government ID number
    e. Visible identification mark
    f. Photo (Optional)
6. The SMS Server will send another SMS to the vendor representative with mobile number of the customer and the secret code.
7. The vendor representative can now communicate the alphanumeric secret code information to the customer to establish his/her authenticity to the customer.

Setup Required by Vendor:

For all vendors who want to extend this trusted level of service providing mechanism to their customers they need to setup an environment for this new approach of vendor authentication.

- Need to have a SMS Server with some customer support numbers for receiving customer SMS as an enquiry. The customer support numbers should be made publicly known through various advertising media.
- All vendor representatives of the vendor shall be registered at the SMS Server with their office ID, mobile numbers, Name and other necessary details.
- SMS Server should be capable of processing the query received as an SMS from the customer and forward necessary vendor authentication information to both the customer and the vendor representative visiting the customer.
- Customers shall have the appropriate knowledge of using the vendor authentication procedure.

Choices of SMS formats:

- VA ID <ID Number>
- VA MOB <Mobile Number>

Advantages:

1. Easy to authenticate the vendor representative with little knowledge on usage of mobile sms.
2. The vendor organization can keep a track of time on vendor representative's visit to customer place.
3. Vendor authentication can be possible for conversations done on phone/mobile between customer and vendor.
4. Prevention of Fraud vendor representative visit to customer can bring honour to organization reputation.

Disadvantage:

1. Not Cost effective as it requires sophisticated setup and skilled man force to support vendor authentication.
2. Vendor authentication with request for photo of the vendor representative's can be time taking.

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Lan-guage to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Er-fahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Ad-hoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): "Heute schon das Morgen sehen"

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98	Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices
P-99	Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik
P-100	Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik
P-101	Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten
P-102	Otto Spaniol (Eds.): Mobile Services and Personalized Environments
P-103	Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)
P-104	Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme
P-105	Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007
P-106	Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops
P-107	Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications
P-108	Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures
P-109	Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1
P-110	Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2
P-111	Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik
P-112	Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis
P-113	Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1st Conference on Social Semantic Web (CSSW)
P-114	Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics
P-115	Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.) German conference on bioinformatics GCB 2007
P-116	Witold Abramowicz, Leszek Maciszek (Eds.) Business Process and Services Computing 1st International Working Conference on Business Process and Services Computing BPSC 2007
P-117	Ryszard Kowalczyk (Ed.) Grid service engineering and manegement The 4th International Conference on Grid Service Engineering and Management GSEM 2007
P-118	Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.) European Conference on ehealth 2007
P-119	Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.) Enterprise Modelling and Information Systems Architectures Concepts and Applications
P-120	Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.) Coordination of Collaborative Engineering - State of the Art and Future Challenges
P-121	Korbinian Herrmann, Bernd Bruegge (Hrsg.) Software Engineering 2008 Fachtagung des GI-Fachbereichs Softwaretechnik
P-122	Walid Maalej, Bernd Bruegge (Hrsg.) Software Engineering 2008 - Workshopband Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT:
Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikationstechnologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting. CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik –
Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informationssysteme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)
Datenbanksysteme in Business, Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional Knowledge Management

P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP 2009

P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)
9th International Conference on Innovative Internet Community Systems
I^{2}CS 2009

P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn, Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 3rd Int'l Workshop
EMISA 2009

P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und Schule«

P-157 Ivo Grosse, Steffen Neumann, Stefan Posch, Falk Schreiber, Peter Stadler (Eds.)
German Conference on Bioinformatics 2009

P-158 W. Claupein, L. Theuvsen, A. Kämpf, M. Morgenstern (Hrsg.)
Precision Agriculture
Reloaded – Informationsgestützte Landwirtschaft

P-159 Gregor Engels, Markus Luckey, Wilhelm Schäfer (Hrsg.)
Software Engineering 2010

P-160 Gregor Engels, Markus Luckey, Alexander Pretschner, Ralf Reussner (Hrsg.)
Software Engineering 2010 – Workshopband
(inkl. Doktorandensymposium)

P-161 Gregor Engels, Dimitris Karagiannis Heinrich C. Mayr (Hrsg.)
Modellierung 2010

P-162 Maria A. Wimmer, Uwe Brinkhoff, Siegfried Kaiser, Dagmar Lück-Schneider, Erich Schweighofer, Andreas Wiebe (Hrsg.)
Vernetzte IT für einen effektiven Staat
Gemeinsame Fachtagung
Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010

P-163 Markus Bick, Stefan Eulgem, Elgar Fleisch, J. Felix Hampe, Birgitta König-Ries, Franz Lehner, Key Pousttchi, Kai Rannenberg (Hrsg.)
Mobile und Ubiquitäre Informationssysteme
Technologien, Anwendungen und Dienste zur Unterstützung von mobiler Kollaboration

P-164 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2010: Biometrics and Electronic Signatures Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-165 Gerald Eichler, Peter Kropf,
Ulrike Lechner, Phayung Meesad,
Herwig Unger (Eds.)
10th International Conference on
Innovative Internet Community Systems
(I^2CS) – Jubilee Edition 2010 –

P-166 Paul Müller, Bernhard Neumair,
Gabi Dreo Rodosek (Hrsg.)
3. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-167 Robert Krimmer, Rüdiger Grimm (Eds.)
4th International Conference on
Electronic Voting 2010
co-organized by the Council of Europe,
Gesellschaft für Informatik and
E-Voting.CC

P-168 Ira Diethelm, Christina Dörge,
Claudia Hildebrandt,
Carsten Schulte (Hrsg.)
Didaktik der Informatik
Möglichkeiten empirischer
Forschungsmethoden und Perspektiven
der Fachdidaktik

P-169 Michael Kerres, Nadine Ojstersek
Ulrik Schroeder, Ulrich Hoppe (Hrsg.)
DeLFI 2010 - 8. Tagung
der Fachgruppe E-Learning
der Gesellschaft für Informatik e.V.

P-170 Felix C. Freiling (Hrsg.)
Sicherheit 2010
Sicherheit, Schutz und Zuverlässigkeit

P-171 Werner Esswein, Klaus Turowski,
Martin Juhrisch (Hrsg.)
Modellierung betrieblicher
Informationssysteme (MobIS 2010)
Modellgestütztes Management

P-172 Stefan Klink, Agnes Koschmider
Marco Mevius, Andreas Oberweis (Hrsg.)
EMISA 2010
Einflussfaktoren auf die Entwicklung
flexibler, integrierter Informationssysteme
Beiträge des Workshops
der GI-Fachgruppe EMISA
(Entwicklungsmethoden für Informationssysteme und deren Anwendung)

P-173 Dietmar Schomburg,
Andreas Grote (Eds.)
German Conference on Bioinformatics
2010

P-174 Arslan Brömme, Torsten Eymann,
Detlef Hühnlein, Heiko Roßnagel,
Paul Schmücker (Hrsg.)
perspeGKtive 2010
Workshop „Innovative und sichere
Informationstechnologie für das
Gesundheitswesen von morgen“

P-175 Klaus-Peter Fähnrich,
Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für
die Informatik
Band 1

P-176 Klaus-Peter Fähnrich,
Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für
die Informatik
Band 2

P-177 Witold Abramowicz, Rainer Alt,
Klaus-Peter Fähnrich, Bogdan Franczyk,
Leszek A. Maciaszek (Eds.)
INFORMATIK 2010
Business Process and Service Science –
Proceedings of ISSS and BPSC

P-178 Wolfram Pietsch, Benedikt Krams (Hrsg.)
Vom Projekt zum Produkt
Fachtagung des GI-
Fachausschusses Management der
Anwendungsentwicklung und -wartung
im Fachbereich Wirtschafts-informatik
(WI-MAW), Aachen, 2010

P-179 Stefan Gruner, Bernhard Rumpe (Eds.)
FM+AM`2010
Second International Workshop on
Formal Methods and Agile Methods

P-180 Theo Härder, Wolfgang Lehner,
Bernhard Mitschang, Harald Schöning,
Holger Schwarz (Hrsg.)
Datenbanksysteme für Business,
Technologie und Web (BTW)
14. Fachtagung des GI-Fachbereichs
„Datenbanken und Informationssysteme“
(DBIS)

P-181 Michael Clasen, Otto Schätzel,
Brigitte Theuvsen (Hrsg.)
Qualität und Effizienz durch
informationsgestützte Landwirtschaft,
Fokus: Moderne Weinwirtschaft

P-182 Ronald Maier (Hrsg.)
6th Conference on Professional
Knowledge Management
From Knowledge to Action

P-183 Ralf Reussner, Matthias Grund, Andreas
Oberweis, Walter Tichy (Hrsg.)
Software Engineering 2011
Fachtagung des GI-Fachbereichs
Softwaretechnik

P-184 Ralf Reussner, Alexander Pretschner,
Stefan Jähnichen (Hrsg.)
Software Engineering 2011
Workshopband
(inkl. Doktorandensymposium)

P-185 Hagen Höpfner, Günther Specht,
Thomas Ritz, Christian Bunse (Hrsg.)
MMS 2011: Mobile und ubiquitäre
Informationssysteme Proceedings zur
6. Konferenz Mobile und Ubiquitäre
Informationssysteme (MMS 2011)

P-186 Gerald Eichler, Axel Küpper,
Volkmar Schau, Hacène Fouchal,
Herwig Unger (Eds.)
11th International Conference on
Innovative Internet Community Systems
(I^{2}CS)

P-187 Paul Müller, Bernhard Neumair,
Gabi Dreo Rodosek (Hrsg.)
4. DFN-Forum Kommunikations-
technologien, Beiträge der Fachtagung
20. Juni bis 21. Juni 2011 Bonn

P-188 Holger Rohland, Andrea Kienle,
Steffen Friedrich (Hrsg.)
DeLFI 2011 – Die 9. e-Learning
Fachtagung Informatik
der Gesellschaft für Informatik e.V.
5.–8. September 2011, Dresden

P-189 Thomas, Marco (Hrsg.)
Informatik in Bildung und Beruf
INFOS 2011
14. GI-Fachtagung Informatik und Schule

P-190 Markus Nüttgens, Oliver Thomas,
Barbara Weber (Eds.)
Enterprise Modelling and Information
Systems Architectures (EMISA 2011)

P-191 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2011
International Conference of the
Biometrics Special Interest Group

P-192 Hans-Ulrich Heiß, Peter Pepper, Holger
Schlingloff, Jörg Schneider (Hrsg.)
INFORMATIK 2011
Informatik schafft Communities

P-193 Wolfgang Lehner, Gunther Piller (Hrsg.)
IMDM 2011

P-194 M. Clasen, G. Fröhlich, H. Bernhardt,
K. Hildebrand, B. Theuvsen (Hrsg.)
Informationstechnologie für eine
nachhaltige Landbewirtschaftung
Fokus Forstwirtschaft

P-195 Neeraj Suri, Michael Waidner (Hrsg.)
Sicherheit 2012
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 6. Jahrestagung des
Fachbereichs Sicherheit der
Gesellschaft für Informatik e.V. (GI)

P-196 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2012
Proceedings of the 11th International
Conference of the Biometrics Special
Interest Group

P-197 Jörn von Lucke, Christian P. Geiger,
Siegfried Kaiser, Erich Schweighofer,
Maria A. Wimmer (Hrsg.)
Auf dem Weg zu einer offenen, smarten
und vernetzten Verwaltungskultur
Gemeinsame Fachtagung
Verwaltungsinformatik (FTVI) und
Fachtagung Rechtsinformatik (FTRI)
2012

P-198 Stefan Jähnichen, Axel Küpper,
Sahin Albayrak (Hrsg.)
Software Engineering 2012
Fachtagung des GI-Fachbereichs
Softwaretechnik

P-199 Stefan Jähnichen, Bernhard Rumpe,
Holger Schlingloff (Hrsg.)
Software Engineering 2012
Workshopband

P-200 Gero Mühl, Jan Richling, Andreas
Herkersdorf (Hrsg.)
ARCS 2012 Workshops

P-201 Elmar J. Sinz Andy Schürr (Hrsg.)
Modellierung 2012

P-202 Andrea Back, Markus Bick,
Martin Breunig, Key Pousttchi,
Frédéric Thiesse (Hrsg.)
MMS 2012:Mobile und Ubiquitäre
Informationssysteme

P-203 Paul Müller, Bernhard Neumair,
Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
5. DFN-Forum Kommunikations-
technologien
Beiträge der Fachtagung

P-204 Gerald Eichler, Leendert W. M.
Wienhofen, Anders Kofod-Petersen,
Herwig Unger (Eds.)
12th International Conference on
Innovative Internet Community Systems
(I2CS 2012)

P-205 Manuel J. Kripp, Melanie Volkamer,
Rüdiger Grimm (Eds.)
5th International Conference on Electronic
Voting 2012 (EVOTE2012)
Co-organized by the Council of Europe,
Gesellschaft für Informatik and E-Voting.CC

P-206 Stefanie Rinderle-Ma,
Mathias Weske (Hrsg.)
EMISA 2012
Der Mensch im Zentrum der Modellierung

P-207 Jörg Desel, Jörg M. Haake,
Christian Spannagel (Hrsg.)
DeLFI 2012: Die 10. e-Learning
Fachtagung Informatik der Gesellschaft
für Informatik e.V.
24.–26. September 2012

P-208 Ursula Goltz, Marcus Magnor,
Hans-Jürgen Appelrath, Herbert Matthies,
Wolf-Tilo Balke, Lars Wolf (Hrsg.)
INFORMATIK 2012

P-209 Hans Brandt-Pook, André Fleer, Thorsten
Spitta, Malte Wattenberg (Hrsg.)
Nachhaltiges Software Management

P-210 Erhard Plödereder, Peter Dencker,
Herbert Klenk, Hubert B. Keller,
Silke Spitzer (Hrsg.)
Automotive – Safety & Security 2012
Sicherheit und Zuverlässigkeit für
automobile Informationstechnik

P-211 M. Clasen, K. C. Kersebaum, A.
Meyer-Aurich, B. Theuvsen (Hrsg.)
Massendatenmanagement in der
Agrar- und Ernährungswirtschaft
Erhebung - Verarbeitung - Nutzung
Referate der 33. GIL-Jahrestagung
20. – 21. Februar 2013, Potsdam

P-212 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2013
Proceedings of the 12th International
Conference of the Biometrics
Special Interest Group
04.–06. September 2013
Darmstadt, Germany

P-213 Stefan Kowalewski,
Bernhard Rumpe (Hrsg.)
Software Engineering 2013
Fachtagung des GI-Fachbereichs
Softwaretechnik

P-214 Volker Markl, Gunter Saake, Kai-Uwe
Sattler, Gregor Hackenbroich, Bernhard Mit
schang, Theo Härder, Veit Köppen (Hrsg.)
Datenbanksysteme für Business,
Technologie und Web (BTW) 2013
13. – 15. März 2013, Magdeburg

P-215 Stefan Wagner, Horst Lichter (Hrsg.)
Software Engineering 2013
Workshopband
(inkl. Doktorandensymposium)
26. Februar – 1. März 2013, Aachen

P-216 Gunter Saake, Andreas Henrich,
Wolfgang Lehner, Thomas Neumann,
Veit Köppen (Hrsg.)
Datenbanksysteme für Business,
Technologie und Web (BTW) 2013 –
Workshopband
11. – 12. März 2013, Magdeburg

P-217 Paul Müller, Bernhard Neumair, Helmut
Reiser, Gabi Dreo Rodosek (Hrsg.)
6. DFN-Forum Kommunikations-
technologien
Beiträge der Fachtagung
03.–04. Juni 2013, Erlangen

P-218 Andreas Breiter, Christoph Rensing (Hrsg.)
DeLFI 2013: Die 11 e-Learning
Fachtagung Informatik der Gesellschaft
für Informatik e.V. (GI)
8. – 11. September 2013, Bremen

P-219 Norbert Breier, Peer Stechert,
Thomas Wilke (Hrsg.)
Informatik erweitert Horizonte
INFOS 2013
15. GI-Fachtagung Informatik und Schule
26. – 28. September 2013

P-220 Matthias Horbach (Hrsg.)
INFORMATIK 2013
Informatik angepasst an Mensch,
Organisation und Umwelt
16. – 20. September 2013, Koblenz

P-221 Maria A. Wimmer, Marijn Janssen,
Ann Macintosh, Hans Jochen Scholl,
Efthimios Tambouris (Eds.)
Electronic Government and
Electronic Participation
Joint Proceedings of Ongoing Research of
IFIP EGOV and IFIP ePart 2013
16. – 19. September 2013, Koblenz

P-222 Reinhard Jung, Manfred Reichert (Eds.)
Enterprise Modelling
and Information Systems Architectures
(EMISA 2013)
St. Gallen, Switzerland
September 5. – 6. 2013

P-223 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)
Open Identity Summit 2013
10. – 11. September 2013
Kloster Banz, Germany

P-224 Eckhart Hanser, Martin Mikusz, Masud
Fazal-Baqaie (Hrsg.)
Vorgehensmodelle 2013
Vorgehensmodelle – Anspruch und
Wirklichkeit
20. Tagung der Fachgruppe
Vorgehensmodelle im Fachgebiet
Wirtschaftsinformatik (WI-VM) der
Gesellschaft für Informatik e.V.
Lörrach, 2013

P-225 Hans-Georg Fill, Dimitris Karagiannis,
Ulrich Reimer (Hrsg.)
Modellierung 2014
19. – 21. März 2014, Wien

P-226 M. Clasen, M. Hamer, S. Lehnert,
B. Petersen, B. Theuvsen (Hrsg.)
IT-Standards in der Agrar- und
Ernährungswirtschaft Fokus: Risiko- und
Krisenmanagement
Referate der 34. GIL-Jahrestagung
24. – 25. Februar 2014, Bonn

P-227 Wilhelm Hasselbring,
Nils Christian Ehmke (Hrsg.)
Software Engineering 2014
Fachtagung des GI-Fachbereichs
Softwaretechnik
25. – 28. Februar 2014
Kiel, Deutschland

P-228 Stefan Katzenbeisser, Volkmar Lotz,
Edgar Weippl (Hrsg.)
Sicherheit 2014
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 7. Jahrestagung des
Fachbereichs Sicherheit der
Gesellschaft für Informatik e.V. (GI)
19. – 21. März 2014, Wien

P-230 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2014
Proceedings of the 13th International
Conference of the Biometrics Special
Interest Group
10. – 12. September 2014 in
Darmstadt, Germany

P-231 Paul Müller, Bernhard Neumair,
Helmut Reiser, Gabi Dreo Rodosek
(Hrsg.)
7. DFN-Forum
Kommunikationstechnologien
16. – 17. Juni 2014
Fulda

P-232 E. Plödereder, L. Grunske, E. Schneider,
D. Ull (Hrsg.)
INFORMATIK 2014
Big Data – Komplexität meistern
22. – 26. September 2014
Stuttgart

P-233 Stephan Trahasch, Rolf Plötzner, Gerhard
Schneider, Claudia Gayer, Daniel Sassiat,
Nicole Wöhrle (Hrsg.)
DeLFI 2014 – Die 12. e-Learning
Fachtagung Informatik
der Gesellschaft für Informatik e.V.
15. – 17. September 2014
Freiburg

P-234 Fernand Feltz, Bela Mutschler, Benoît
Otjacques (Eds.)
Enterprise Modelling and Information
Systems Architectures
(EMISA 2014)
Luxembourg, September 25-26, 2014

P-235 Robert Giegerich,
Ralf Hofestädt,
Tim W. Nattkemper (Eds.)
German Conference on
Bioinformatics 2014
September 28 – October 1
Bielefeld, Germany

P-236 Martin Engstler, Eckhart Hanser,
Martin Mikusz, Georg Herzwurm (Hrsg.)
Projektmanagement und
Vorgehensmodelle 2014
Soziale Aspekte und Standardisierung
Gemeinsame Tagung der Fachgruppen
Projektmanagement (WI-PM) und
Vorgehensmodelle (WI-VM) im
Fachgebiet Wirtschaftsinformatik der
Gesellschaft für Informatik e.V., Stuttgart
2014

P-237 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)
Open Identity Summit 2014
4.–6. November 2014
Stuttgart, Germany

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de