Towards Universal Login

Detlef Hühnlein[1], Tina Hühnlein[1], Gerrit Hornung[2], Hermann Strack[3]

Abstract: The present paper provides an overview of existing protocols and infrastructures for Identity Management on the Internet and discusses potential paths towards integrating the different approaches in a user centric manner into a "Universal Login" infrastructure, which allows Users to manage their authentication preferences and Service Providers to integrate with Identity Providers in an easy manner.

Keywords: SAML, OpenID Connect, FIDO, eIDAS

1 Introduction

Successful digital transformation relies on secure digital identities. In the light of the obvious need for user-friendly, legally compliant and trustworthy digital identities on the Internet, many different solutions for authentication and identification have emerged in recent years and hence there are many Identity Providers (IdP), which could perform the authentication and identification of Users on behalf a Service Provider (SP).

On the other hand, the large and seemingly still increasing number of IdPs leads to a rather fragmented market for identity services in which SPs and Users are often forced to use multiple IdPs to reach a sufficient service coverage. Furthermore, despite tireless standardisation and harmonisation efforts, the available infrastructures are not yet fully integrated in a seamless fashion, so that SPs either (1) would have to stick with one or a few IdPs, (2) undertake major, often uneconomic, integration efforts and engage in strategically unpleasant dependencies by supporting proprietary interfaces, or (3) completely forego the use of secure digital identities. To address this unfortunate situation, the present paper aims at paving the way for a "Universal Login" procedure in which the SPs are able to connect to arbitrary IdPs via a simple interface and the User (Subject) may select her favourite Credential or IdP for login at a certain SP.

To reach this goal, the rest of the paper is structured as follows: Section 2 recalls basics with resepect to Federated Identity Management. Section 3 introduces a refined reference architecture, which will form the technical basis for the "Universal Login" procedure presented in Section 4. The paper concludes with Section 5 by summarising the main aspects and providing an outlook towards potential future developments.

[1] {detlef.huehnlein, tina.huehnlein}@ecsec.de, ecsec GmbH, Sudetenstraße 16, 96247 Michelau, Germany
[2] gerrit.hornung@uni-kassel.de, Universität Kassel, Henschelstraße 4, 34127 Kassel, Germany
[3] hstrack@hs-harz.de, Hochschule Harz, Friedrichstraße 57-59, 38855 Wernigerode, Germany

2 An abstract model for Identity Management

Within the various approaches and infrastructures for Identity Management[4] one may recognise aspects related to *"Credential Management"*, in which a *"Subject"* (User) is equipped with some sort of digital credential, which allows to authenticate or prove certain claims, and aspects related to *"Federated Identity Management"* which allows that a *"Service Provider"* delegates the main tasks related to the management of credentials to one or more specialised *"Identity Providers"* while compensating this step with suitable *"Trust Management"* means.

2.1 Credential Management

The *Credential Management* comprises suitable procedures and protocols between the Subject and the IdP, whereas the credentials may involve multiple authentication factors[5] and provide a Level of Assurance (LoA)[6] ranging from "low" (e.g. user name and static password) over "substantial" (e.g. multiple factors within a dynamic authentication protocol) to "high" (e.g. highly secure and sophisticated credentials, which involve cryptographic hardware, which reliably prevent misuse of the credential protecting "against duplication and tampering as well as against attackers with high attack potential"[7]).

The Commission Implementing Regulation (EU) 2015/1502 specifies minimum requirements for the credentials to reach a certain LoA and [eID18] provides additional guidance for interpretation of the stipulations. There is a very wide range of possibilities for the implementation of credentials, which covers public-key based mechanisms with[8] or without certificates[9], with privacy-friendly features[10] or based on distributed ledger technology[11] as well as secret-key based mechanisms with a variety of protocols[12].

2.2 Federated Identity Management

The *Federated Identity Management* aspects especially comprise a suitable set of protocols for the secure integration of the three nodes of the system (Subject, SP and IdP), whereas the dominant protocol families in practice are [SAML] and [OpenID], which is

[4] See [KH14, SAML, OpenID, Ro12] for example.

[5] Section 1 (2) of CIR (EU) 2015/1502 distinguishes "possession-based", "knowledge-based" and "inherent authentication factors".

[6] See Art. 8 of Regulation (EU) No. 910/2014 and CIR (EU) 2015/1502.

[7] See CIR (EU) 2015/1502/EU, Annex, Section 2.2.1.

[8] Among the widely used formats are X.509-based (see [RFC 5280]) and card-verifiable certificates (see [BSI15], Part 3, Annex C).

[9] See [Bh15, W3C19a] for example.

[10] See [Ch85, IBM, Micr, CL01, Br95, W3C19b] for example.

[11] See [Ja16, Li18] for example.

[12] See [BM03, RFC 4226, RFC 6283, RFC 6287] for example.

in turn based on OAuth 2.0 [RFC 6749].

Note that this kind of federation is optional in the sense that the duties of the IdP, such as the issuing, management and validation of credentials, could be assumed by the SP itself and hence there is no distributed setup, but the authentication and identification may be performed by the SP itself.

2.3 Trust Management

With suitable *Trust Management* measures the SP seeks to compensate the loss of control due to delegating the security sensitive Credential Management tasks to the Identity Provider. The Trust Management measures may in particular comprise the stipulation and verification of requirements for the Credential Management, as specified in CIR (EU) 2015/1502/EU and outlined in Section 2.1. That the specified requirements are indeed fulfilled could be ensured by appropriate self-assessments, peer-reviews, independent audits or formal certification procedures. The trust information could be aligned to the various requirements defined in CIR (EU) 2015/1502 and encoded and organised and communicated within “vectors of trust” as specified in [RFC 8485].

3 Reference Architecture for Universal Login and more

The “Reference Architecture” presented in Figure 1 below is a refinement and enhancement of the classical model for Federated Identity Management and related architectures developed within previous work conducted in pertinent research projects, such as SkIDentity[13] and FutureID[14]. The most important aspects of this reference architecture are outlined in the following.

3.1 Trust, Discovery & Collaboration Framework

The “Trust, Discovery & Collaboration Framework” realises the “Trust Management” in a Federated Identity Management architecture and is an enhancement of the eIDAS Trust Framework[15] in the sense that it also includes not (yet) notified eID-schemes and IdPs, which are not formally endorsed by some EU Member State. As for those providers, there is no formal peer review in the sense of Chapter III of CIR (EU) 2015/296, and therefore there needs to be an adequate enhancement, which aims at maintaining a high level of trust and transparency. A possible path might be to introduce a two dimensional trust system (see Figure 2), which on the one hand side assesses which LoA is reached for an eID solution and Identity Provider with respect to the different requirements defined in

[13] See [KH14] and https://project.skidentity.de/en/publikationen/.

[14] See [Ro12].

[15] See Chapter 2 of Regulation (EU) No. 910/2014 and related implementing acts, such as CIR (EU) 2015/296, CIR (EU) 2015/1501, CIR (EU) 2015/1502, CIR (EU) 2015/1984 as well as additional guidance documents, such as [eID18] for example.

[2015/1502/EU] and listed in Section 2.1 and which "Level of Confidence" (LoC) was used for this assessment.

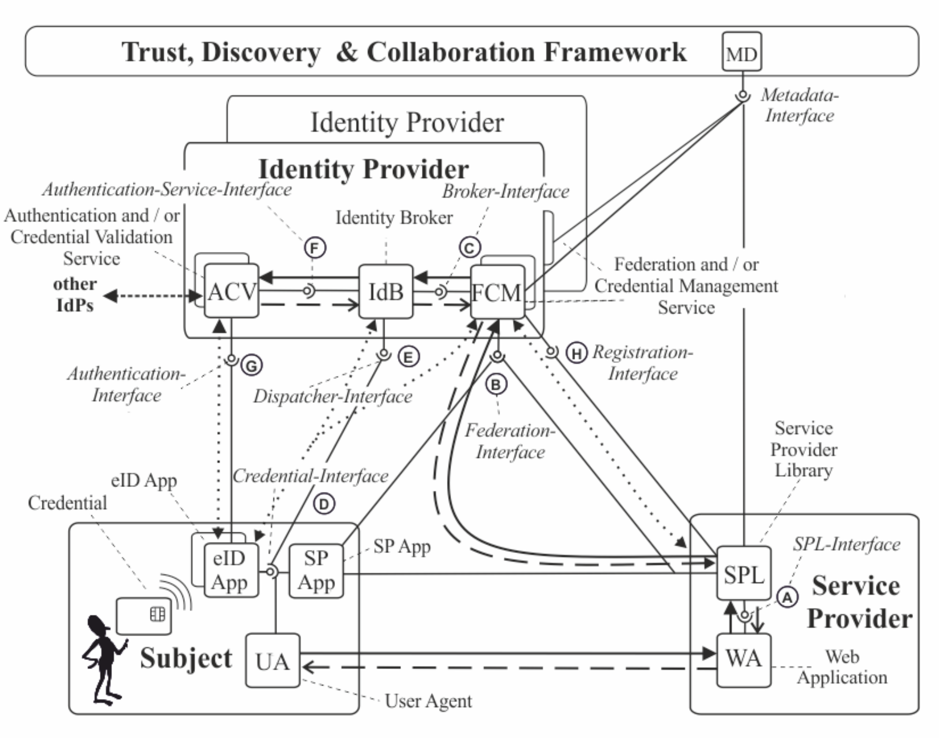
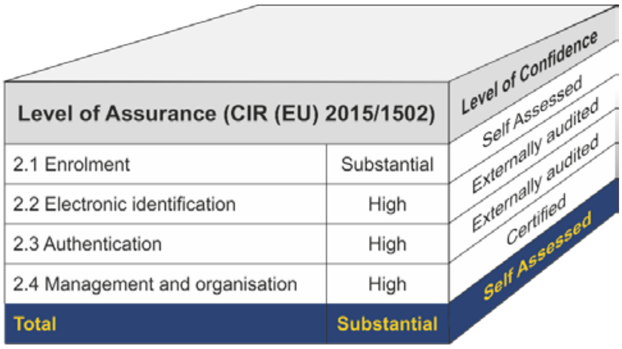


Figure 1: Reference Architecture for "Universal Login" and more

While the current eIDAS Trust Framework[16] only has one LoC-level, which corresponds to the formal notification according to Art. 9 of Regulation (EU) No. 910/2014, the enhanced trust system could have a graded approach with multiple levels, which could range from a simple self-assessment with or without validation (1) over external audits (2) and formal certifications (3) to the formal notification (4) of an eID scheme.

As the overall system is more open than the current eIDAS Trust Framework, it is important that there is some possibility for the trustworthy registration and retrieval of metadata for Identity Providers and SPs in standardised formats including [Ca05, Ca19a, Ca19b, Sa14a, Sa14b, RFC 8414, RFC 7591].

[16] For the legal background of this framework see [Ho16].



Level of Assurance (CIR (EU) 2015/1502)	
2.1 Enrolment	Substantial
2.2 Electronic identification	High
2.3 Authentication	High
2.4 Management and organisation	High
Total	Substantial

Figure 2: Enhanced Trust System with "Level of Confidence"

To enable a user friendly “Universal Login” procedure in which a User may select and persist its authentication preferences for a SP in its local storage, it is necessary (see also [Op19] and [Seamless] that the envisioned Trust, Discovery & Collaboration Framework allows to serve some “trustworthy JavaScript”[17] from a “neutral and trusted domain”[18], in order to support the management of the user preferences and persistence of the data in the local storage of the browser for the neutral and trusted domain.

3.2 Identity Provider

There may be a large number of Identity Providers, which may be “monolithic” in the sense that they support a single federation protocol and a single credential and authentication protocol, or “modular” in the sense that they may contain multiple Federation Services and Authentication Services, which are integrated via some Identity Broker. The latter approach also gives rise to the issuance and validation of credentials in various formats (see Section 2.1) and the invocation of other IdPs.

3.3 Subject

The Subject may in general be a natural or legal person, a (mobile) device, a computation node or even a service. Depending on the used credentials there may be one or more eID Apps besides the plain browser (User Agent) and a SP specific app (SP App), which complements the server side SP. A pivotal role plays the “Credential Interface” (D), as it may allow to discover that there is a specific eID App and credential or to initiate a protocol for issuing such a credential.

[17] For obvious reasons, the “trustworthy JavaScript” shall be available as open source.

[18] It needs to be ensured, by suitable privacy-specific certifications for example, that the neutral and trusted domain does not create any unwanted User or communication profiles, but only serves the said JavaScript in a reliable manner.

3.4 Service Provider

The SP typically contains a "Service Provider Library" (SPL), which handles the protocol flow based on [SAML] or [OpenID] after the corresponding metadata (see Section 3.1) have been registered at the supported IdPs and/or the central metadata repository. The SPL plays an important role in the practical and user friendly realisation of the envisioned "Universal Login" procedure outlined in Section 4 by letting (1) the SP configure its requirements including the acceptable LoA/LoC, IdPs and credentials and (2) by persisting the necessary history and previously chosen preferences of the User, such as the used credential, IdP and authentication options, for a specific SP.

4 Universal Login

The "Universal Login" procedure outlined in the present paper aims at enabling

- the SPs to easily support the relevant IdPs via standardised interfaces based on [SAML] or [OpenID] and
- the Users to manage their authentication preferences for the accessed SPs and involved IdPs and credentials in a suitable local storage on their device.

The IdPs benefit from the proposed approach by an increased number of participating SPs and Users.

After a suitable registration procedure, the metadata[19] of the participating IdPs is available in the "Trust, Discovery & Collaboration Framework" and can be retrieved from there by the SPs via a suitable interface[20]. Next, the SP is installing a suitable SPL, which supports [SAML] and/or [OpenID] and allows to register itself at the selected IdPs via some protocol along the lines of [Sa14a] and [RFC 7591]. Such SPLs may be built upon existing "Cloud Connector"[21] components, which have been created within the SkIDentity project.

Now the „Universal Login" system is set up and can be used. The process starts at the SP when the User wants to access a resource. If there are no authentication preferences stored or upon explicit request to enter the "configuration mode", the User is prompted to select the preferred authentication means (IdP, credential etc.) she wants to use at the specific SP. This information is stored within the local storage of the User via the trustworthy JavaScript, which is shipped via the neutral and trustworthy domain for example. In subsequent authentication processes the User's preferences can simply looked up, before the regular authentication process based on [SAML] or [OpenID] is performed. Besides this basic use case (User-driven management of authentication preferences), there may also be more advanced use cases which involve trustworthy identity attributes, which have

[19] See [Ca19a, Ca19b, Sa14b, RFC 8414].

[20] This interface can be built upon an enhanced version of [Hü19] and will allow to list the participating IdPs, which satisfy a set of specific criteria.

[21] See https://skidentity.com/cloud-connector and [KH14].

been retrieved from the User's credential or the storage of the IdP. This set of identity attributes may be signed and notarised by a suitable trust service, such as the "YourCredential" notarisation service, which has been developed in the StudIES+ EU CEF project [St19].

5 Conclusion and Outlook

In the present document we outlined a "Universal Login" framework, which allows Users to manage their authentication preferences for the accessed SPs and involved IdPs and SPs to easily integrate with IdPs via standardised interfaces based on [SAML] or [OpenID]. In the next step, the components and procedures sketched here will be specified technically and implemented within the SHIELD project[22], which will be supported by the German Federal Ministry of Economics.

Bibliography

[Bh15] Bharadwaj, V. & al. Web API for accessing FIDO 2.0 credentials, W3C Member Submission. https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/, 2015

[BM03] Boyd, C., Mathuria, A.: Protocols for authentication and key establishment, Springer, 2003

[Br05] Brands, S.: Secret-key certificates. Technical Report CS-R9510 CWI, 1995

[BSI15] Bundesamt für Sicherheit in der Informationstechnik (BSI): Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token, BSI TR-03110, 2015-2016

[Ca05] S. Cantor, J. Moreh, R. Philpott, E. Maler. Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf, 2005

[Ca19a] S. Cantor. SAML V2.0 Metadata Interoperability Profile Version 1.0, OASIS Standard. https://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop-os.pdf, 2019

[Ca19b] S. Cantor. SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, OASIS Standard. https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/os/sstc-saml-metadata-ui-v1.0-os.pdf, 2019

[Ch85] Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM, 28 (10), pp. 1030-1044, 1985

[CL01] Camenisch, J., Lysyanskaya, A.: Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. EUROCRYPT 2001, LNCS 2045, pp. 93-118. Springer, 2001

[22] See https://shield24.de.

[eID18] eIDAS-Cooperation Network. Guidance for the application of the levels of assurance which support the eIDAS Regulation, 2018

[Ho16] Hornung, G.: Rechtliche Perspektiven des Identitätsmanagements in Europa. In C. E. G. Hornung, Der digitale Bürger und seine Identität (pp. 153-185). Nomos, 2016

[IBM10] IBM: Specification of the Identity Mixer Cryptographic Library. Version 2.3.0. http://domino.research.ibm.com/library/cyberdig.nsf/papers/EEB54FF3B91C1D64852 5759B004FBBB1/$File/rz3730_revised.pdf, 2010

[Ja16] Jacobovitz, O.: Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf, 2016

[KH14] Kubach, M., Hühnlein, D.: Vertrauenswürdige Identitäten für die Cloud: Arbeiten und Ergebnisse des SkIDentity-Projekts. Fraunhofer Verlag, 2014

[Li18] Lim, S. & al.: Blockchain technology the identity management and authentication service disruptor: a survey. International Journal on Advanced Science, p. 1735., 2018

[Micr] Microsoft: U-Prove. https://www.microsoft.com/en-us/research/project/u-prove/.

[Hü19] Hühnlein, D. (ed.): Digital Signature Service Metadata Version 1.0, OASIS CSD 02. https://docs.oasis-open.org/dss-x/dss-md/v1.0/dss-md-v1.0.html, 2019

[Op19] OpenID WG: Account Chooser & Open YOLO (You Only Login Once) Working Group Home Page. https://openid.net/wg/ac/, 2019

[OpenID] OpenID Foundation. Specifications. https://openid.net/developers/specs/

[Ro12] Roßnagel, H., Camenisch, J., Fritsch, L., Gross, T., Houdeau, D., Lehmann, A., & Shamah, J. (2012, 36 3). FutureID – Shaping the Future of Electronic Identity. DuD, pp. 189-194.

[Sa14a] N. Sakimura, J. Bradley, M. Jones: OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 1, https://openid.net/specs/openid-connect-registration-1_0.html, 2014

[Sa14b] N. Sakimura, J. Bradley, M. Jones, E. Jay: OpenID Connect Discovery 1.0 incorporating errata set 1, https://openid.net/specs/openid-connect-discovery-1_0.html, 2014

[SAML] OASIS. SAML Wiki. https://wiki.oasis-open.org/security/FrontPage

[Seamless] Welcome to SeamlessAccess.org. We offer seamless access. You get research as it should be. https://seamlessaccess.org/, 2019

[St19] Strack, H., Otto, O., Klinner, S., & Schmidt, A.: eIDAS eID & eSignature based Service Accounts at University environments for cross-border/domain access. Open Identity Summit 2019 (pp. 171-176). Bonn: GI, LNI 293, 2019

[W3C19a] W3C: Web Authentication: An API for accessing Public Key Credentials Level 1. W3C Recommendation. https://www.w3.org/TR/webauthn-1/, 2019

[W3C19b] W3C: Verifiable Credentials Data Model 1.0 - Expressing verifiable information on the Web. W3C Recommendation. https://www.w3.org/TR/vc-data-model/, 2019