Establishing a Universal Service Model for Authentication Scenarios based on MNM Service Model

Jule Anna Ziegler[1]and David Schmitz[1]

Abstract: In today's diversity and heterogeneity of authentication protocols, standards, technologies and frameworks it is hard to compare or at all to combine, e.g., for multi factor authentication, different authentication scenarios. Above all, they all have different understanding or at least perspective on the term "service". This perspective on a service is normally only a technically one, not really taking into account a full IT service covering the whole life cycle from design, (trust) negotiation, operation to decommissioning. This paper proposes a Universal Authentication Service Model (UASM) in order to describe authentication scenarios in a generic scenario-independent service-oriented way. Requirements are derived from seven example authentication scenarios. It outlines the characteristics of the MNM Service Model (MSM) and how this approach can be reused for universally describing any authentication scenario. Since the work described here is still work in progress, in this paper, UASMs main terms and concepts are introduced. Finally, by using step-by-step refinement of MSM Basic View, UASMs Basic Views are described.

Keywords: Authentication, Identity Management, Service Management, MNM Service Model

1 Introduction

Today's landscapes consist of IT services of various types, webservices, e.g., social networks, cloud storage, but not limited to, also intra/inter-organizational services like email or collaborating tools, all requiring authentication and subsequent authorization to access the respective service. Authentication, in short **AuthN**, constitutes to be the verification of the authenticity of the entity or subject to be authenticated, e.g., user or thing in IoT, the permission about accessing a service is authorization, **AuthZ**. In the area of AuthN, which is the focus of this paper, many different AuthN protocols, standards, technologies and frameworks (abbreviated with **AuthN P/S/T/Fs**) have emerged.

Hence, before establishing a new or enhancing an existing AuthN service scenario, e.g. especially in terms of multi factor authentication, we think organizations profit by identifying at first existing AuthN components, roles, processes and their dependencies in place. Above all, a *complete* and *comparable* description of planned or existing AuthN service scenarios is also relevant with regard to performing analysis, in particular security analysis, but also in consideration of other criteria, such as, for example, effort or costs. Comparability is achieved by a uniform terminology whereas completeness is achieved by a holistic description of all processes and roles in a service (lifecycle) comprehensive way. Furthermore, many AuthN P/S/T/Fs have a different understanding or at least perspective on the term ”service”. This perspective on a service is normally only a technical one, not

[1] Leibniz Supercomputing Centre, Boltzmannstr. 1, 85748 Garching n. Munich, {surname}@lrz.de

really taking into account a full IT service covering the whole lifecycle from design, (trust) negotiation, operation to decommissioning.

Especially in regard to multi factor authentication, AuthN services are more and more composed out of different dependent AuthN services, e.g. SAML password AuthN realized by LDAP combined with Universal Second Factor (U2F) protocol for second factor AuthN. When dealing with concrete AuthN service scenarios, dependent services which use an AuthN service can be of interest as well. That is why, in this work an **AuthN (service) scenario** is a scenario, which includes at least one AuthN service which may be used by other dependent services and may itself be dependent or internally composed out of simpler AuthN services. Thereby, in order to perform holistic analysis, e.g., regarding security of a particular AuthN factor, for all involved AuthN services all service processes (e.g., proper authentication, registration, incident management) and their dependencies need to be identified and specified.

A proper basis for the overall description of service interactions are UML Use Case Diagrams and UML Activity Diagrams. Thus, there is a uniform language for interactions/processes, but service dependencies or, for example, relationships between roles and services are still missing.

Since many organizations and campuses in higher research & education participate in the service *eduGAIN* provided by GÉANT, they are most often faced with multiple AuthN P/S/T/Fs which can become challenging. E.g. taking into account various AuthN P/S/T/Fs like Security Assertion Markup Language (SAML) or OpenID Connect, entities acting in multiple roles but also considering involved resources like for instance an LDAP database. Above all, many AuthN P/S/T/F are using their own, diverse vocabulary, terminology and concepts (e.g. SAML Service Provider vs. OIDC Relying Party, SAML attributes vs. OIDC claims).

Summarized, we identified the following problem statements:

- How to describe AuthN scenarios in a generic scenario-independent service-oriented way?
- What are the requirements for such a model?
- Is it possible to reuse/extend an existing approach?

To the best of our knowledge, models for describing AuthN scenarios in a generic but also scenario-independent way and simultaneously covering the full IT service lifecycle do not exist and do not address to the above-mentioned problem statements.

The remainder of this paper is structured as following: In section 2 we derive requirements from seven example scenarios. Section 3 outlines characteristics of MNM Service Model and why this approach can be reused for universally describing AuthN service scenarios. Following, in section 4 the refinement of MNM Service Model for AuthN service scenarios by introducing main terms and concepts is described. The last section 5 concludes the paper and since the work described in this paper is still work in progress an outlook to future work is provided. A list of abbreviations is attached at the very end of this paper.

2 Authentication Service Scenarios and Requirements

For requirement gathering, we use both universally valid AuthN service scenarios but also specific AuthN service scenarios occuring within eduGAIN representing different AuthN P/S/T/Fs. Here, AuthN service scenarios are exemplary introduced from the point of view of the service lifecycle phase *operation*, which implies that service establishment (especially design, trust negotiation) has already taken place.

2.1 Authentication Service Scenarios

eduGAIN [GÉ18] provided by GÉANT is an identity inter-federation which interconnects (national) identity federations to facilitate access to resources and services (e.g., wiki, survey tools, e-Learning) needed by the global research and education community. Based on a federated identity, which is typically assigned by the user's home organization, e.g., university, school, research center, users can access various external services provided by eduGAINs participating service providers. While AuthZ is performed by the service provider itself, AuthN is performed by the respective home organization of the user. Here, AuthN is mostly not limited to one specific AuthN P/S/T/F.

In this section we describe seven possible AuthN scenarios, SC0 to SC6, including single factor AuthN scenarios, i.e., using only one factor of something you know/have/are but also multi factor AuthN (in short: MFA) scenarios using at least two of the four different factor types. In particular, such combination arises for the case of the example scenarios SC4 to SC6. Before, scenarios SC0 to SC3 represent examples for applying a single particular AuthN P/S/T/F.

SC0 (Scenario 0) represents a simple AuthN scenario, where a user authenticates to a local/not distributed system, e.g., an employee enters his/her password to log on to the system of his/her working station. Here, AuthN is performed by the system itself, by comparing username and password with the corresponding attributes stored in the organizational internal LDAP database.

SC1 describes AuthN within a SAML (inter-)federation. While trying to access a particular web service, the user, in SAML called principal, is redirected by the SAML Service Provider (SAML SP) via discovery service to its home SAML Identity Provider (SAML IdP). After successful AuthN at the SAML home IdP, for example by means of username and password, the SAML home IdP responds with an AuthN response which serves as basis for the SAML SPs authorization decision.

SC2 outlines AuthN using OpenID Connect (OIDC). If a user wants to log on to a service, the OIDC Relying Party (OIDC RP) generates an AuthZ request which is sent, using a discovery service (e.g., Webfinger) to the corresponding OpenID Provider (OIDC OP) of the user, also including the additional parameter scope=openid to indicate that user AuthN at the OIDC OP is required. The identity of the user and information about the AuthN is transferred in form of an ID token from OIDC OP to OIDC RP.

In **SC3**, U2F protocol is used for second factor AuthN with a USB, NFC oder Bluetooth device in connection with a U2F server.

While the four previous examples scenarios presented so far apply only to a single AuthN P/S/T/F, e.g., either SAML, OIDC, or U2F, the following ones, all concerned with MFA, will at least be a combination of two AuthN P/S/T/Fs and so demonstrating the need for universal, generic terms and concepts.

SC4 is a MFA scenario within a SAML-based federation using a proxy pattern. The Dutch Identity Federation SURFnet is implementing a Hub&Spoke federation architecture, where all SAML home IdPs and SAML SPs are connected via a central hub, a SAML proxy. Between the central hub and the SAML SPs sits their so called Step-up Authentication as a Service [va17], also a (transparent) SAML proxy, which offers 2nd factor IdPs for each supported 2nd factor type, e.g., YubiKey, Tiqr. In case a SP sends an AuthN request, the Step-up Authentication Service requests 1st factor AuthN from the home IdP, then requests second factor AuthN from the respective Step-up 2nd factor IdP, then the proxy sends an AuthN response to the SAML SP.

SC5 represents an integrated MFA scenario in a SAML federation, where first factor AuthN is provided by the SAML IdP, second factor AuthN is performed within the SAML IdP internally, e.g., U2F, which requires high adaption in IdP realization/implementation.

SC6 is based on a SAML federation for first factor AuthN, but second factor AuthN integration is done by the SAML SP instead of the SAML IdP. Hence, second factor AuthN is decoupled from first factor AuthN, which needs high adaption in each SPs realization/implementation.

As we can see from the diversity and heterogeneity of today's AuthN service scenarios, especially in regard to terminology and concepts, there is a lack of a unique generic model, which allows a comparable, complete and common understanding of AuthN service scenarios.

2.2 Requirements

Based on the scenarios described above and the problem space outlined in section 1, we derived the following requirements for describing AuthN scenarios:

- **Generic and universal AuthN terminology:** The model should provide a universal, uniformly applicable AuthN terminology, leading to better understanding between all involved roles, i.e. customers, users, and providers of any involved services, but also regarding different AuthN P/S/T/Fs being used for AuthN. Maybe also in parallel in a single given scenario.
- **Consideration of usage functionality** (user aspects) and **management functionality** (customer aspects, including trust negotiation/mangement, registration of each factor and user centric right management).
- **Recursive application** of the model in order to support nested hierarchies of AuthN, e.g. for MFA.

- **Scenario-independent modeling templates:** Any abstract or specific AuthN scenario is representable by using scenario-independent modeling templates.

3 Munich Network Management (MNM) Service Model

We checked existing models, such as tmforum Information Framework (SID) [tmf18] and MNM Service Model [Ga01a, Ga01b, Ga02] against the requirements in section 2 and identified the MNM Service Model as a suitable approach to describe AuthN scenarios in a generic scenario-independent service-oriented way. In this section we outline the characteristics of the MNM Service Model, abbreviated in the following with **MSM**.

MSM proposes a systematic methodology used for analyzing and identifying actors of services including their inter/intra-organizational relationships. For this, MSM introduces a generic scenario-independent service model which covers the whole lifecycle of IT services. MSM distiguishes between three different views: **MSM Basic Service Model** (here, unified into **MSM Basic View**) identifies roles, i.e. user, customer and provider, and their associations. Based on this as a refinement **MSM Service View** describes services independently from its service implementation always differentiating between customer side, provider side and side independent aspects of a service. **MSM Realization View** represents the provider-internal realization of IT services. MSM uses an abstraction of interaction classes by classifying interactions in usage and management (functionality) and also supports chaining of MSM, a recursive application of services, i.e., sub services.

We decided to use MSM due to its suitable and useful language with generically, commonly defined terms / model specification formalism between customer and provider side (MSM Service View). But also because of its specification of internal realization at provider side (MSM Realization View) and its splitted consideration into usage functionality (user aspects) and management functionality (customer aspects, including trust negotiation and management). Moreover, MSM Basic View allows the consideration of entities, roles and services along with their sub service relationships.

4 Using MNM Service Model for AuthN Service Scenarios

In this section, we refine the MNM Service Model (MSM) in order to achieve a generic scenario-independent service-oriented model for AuthN scenarios. The existing MSM with all its generic classes and associations/relationships in Basic/Service/Realization View is referenced hereafter as generic MSM, while its refinement to AuthN scenarios, i.e., refined classes, associations/relationships specifically for AuthN, is named **Universal Authentication Service Model (UASM)**. For UASM, we propose to describe, specify, and model **AuthN service scenarios**, i.e., IT service scenarios involving AuthN P/S/T/Fs like SAML, OIDC, Radius or U2F (see scenarios SC0 to SC6) but also in general, independently of used AuthN P/S/T/F, based on MSM. We restrict ourselves in this paper to the step-by-step refinement of MSM Basic View towards four different types of UASM Basic Views that can be used for any AuthN scenario. Before, main terms and concepts are introduced.

While MSM also could be applied for each particular AuthN P/S/T/F-specific service scenario singly and independently, e.g., particular for a SAML or OIDC-based AuthN service, here we first abstract from the concrete AuthN P/S/T/F to yield a refinement of MSM. That is, refined classes and maybe based on that, refined associations/relationships in MSM Basic/Service/Realization View, which can in turn be instantiated to any AuthN service scenario.

The refinement for UASM is based on the generic concept of **AuthN Information (AuthNI)**. Here, AuthNI is defined as an information about the authentication of a real-world identity, in UASM called **Real-World AuthN Subject (RAS)**. In most of the use cases the RAS is typically a human, in other cases it can be also whole organizations or divisions of it (technical accounts). Considering Internet of Things a real-world ”Thing” is possible, too. AuthNI includes in particular the **Trustworthy AuthN Subject (TAS)**, which is the digital counterpart of RAS, both being subsumed under the term (AuthN) subject. So, AuthNI is actually an information about the AuthN of the TAS. In addition to the TAS, AuthNI may include a multitude of fixed and dynamic AuthN attributes, also including meta attributes, e.g., name of user, email address of user, number and type of factors used for AuthN, timing, but also the time of the last change of a factor, strength of the factors actually used.

To demonstrate the usage of the term ”AuthNI” let’s regard two examples: On the one hand, AuthNI can appear and be used internally by an entity, e.g., in SC1, SC4-SC6 at a SAML IdP when comparing user-provided AuthNI (e.g., first factor credentials) to registered values in a local resource used for verification of user-provided AuthNI, e.g., an LDAP directory. Here, the LDAP directory is a resource for realizing the trusted AuthNI provisioning in the SAML IdP. On the other hand, AuthNI is often communicated between entities in a trusted way, e.g., in SC1-SC2, SC4-SC6, between a SAML IdP and SAML SP, or between an OIDC OP and OIDC RP. In this case, the receiving entity trusts the sending one in order to get a trusted and trustful statement about the AuthN of the respective Real-World AuthN Subject (RAS) via its digital counterpart (TAS). Both cases are covered by the term AuthNI, not differentiating what the particular (possibly meta) attributes are. It may contain the plain text password (ideally only if used internally to an entity), only the hash of the password, or only a statement that the password has been (successfully) checked (together with some verifiable context for the performed AuthN in that case), and/or similiar information about other factors beyond first-factor passwords.

If communicated between trusted entities AuthNI normally is enriched by means to ensure the trustfulness (i.e., to ensure authenticity, integrity) of it, typically by employing cryptographic means for the envelope of the AuthNI used (e.g., certificates, signatures, hashes) or for the communication channel used to transmit AuthNI (e.g., encryption, certificates). This requires that such communicating entities establish and manage appropriate trust between themselves in advance. In this context the AuthNI can be more specifically named **Trustworthy AuthNI (TAuthNI)**.

UASM introduces as a refinement to MSM two kind of sub classes of (generic) services: **Trustworthy AuthNI Administration Service (TAAS)** and **Trustworthy AuthNI Provisioning Service (TAPS)**, both dealing with TAuthNI.

The former service type, TAAS, is the original or principal source of AuthNI, so it is responsible for the registration and administration of AuthNI, especially mapping digital identities to real-word identities. This includes the administration of fixed and dynamic AuthN attributes, also including (typically dynamic) meta attributes, like the time of the last change of a factor or the last time of the verification of a factor.

The latter service type, TAPS, is used for communicating TAuthNI, which is known to him - either from local resources realizing AuthN functionality and so sharing these with an corresponding TAAS or recursively from another TAPS, i.e., as a sending entity to another receiving entity. The main focus in this paper is on the TAPSs independent of the used AuthN P/S/T/F, while the TAASs are introduced to provide a complemented view on AuthNI regarding its principal origin.

This functionality of TAPS and TAAS is more concretized by splitting the functionality of each service into **usage** and **management functionality**: Interactions needed by the user to fulfill the purpose of the respective service, e.g. at the TAPS the authentication itself, are called usage functionality. Interactions for managing the service, such as the trust negotiation or the provisioning of an interface to report incidents, is subsumed under management functionality.

For shortness, an entity acting as a provider of TAPS is named **Trustworthy AuthNI Provider (TAP)**, and an entity acting as a customer of TAPS is named **Trustworthy AuthNI Consumer (TAC)**. Always depending on the specific AuthN scenario, here, for sake of simplicity, the TAP acts as both the provider of the TAPS and the TAAS.

4.1 UASM$_{\text{generic}}$ Basic View

After analyzing the AuthN scenarios of section 2 (predominantly eduGAIN AuthN scenarios), we discovered two main characteristics:

- There are high-level services which rely on the TAuthNI communicated by the TAPS. So, the user of the relying service is also user of the TAPS.
- Explicitly the RAS is user of the TAPS.

Consequently, the RAS is also user of the relying (high-level) service. However, there are AuthN scenarios aside from eduGAIN being less specific, which should be covered by UASM as well, e.g. AuthN of Things in IoT. Therefore, the general idea was to build the model step-by-step (see Figure 1). UASM$_{\text{subject-service}}$ Basic View in Figure 5 covers exactly eduGAIN AuthN scenarios. By looking at the two characteristics individually, we get two more generic cases also covered by UASM. They are described in section 4.2 (UASM$_{\text{service}}$ Basic View) and section 4.3 (UASM$_{\text{subject}}$ Basic View).

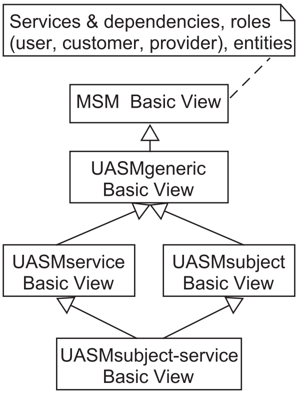
Services & dependencies, roles (user, customer, provider), entities
MSM Basic View
UASMgeneric Basic View
UASMservice Basic View
UASMsubject Basic View
UASMsubject-service Basic View

Figure 1: Step-by-Step refinement

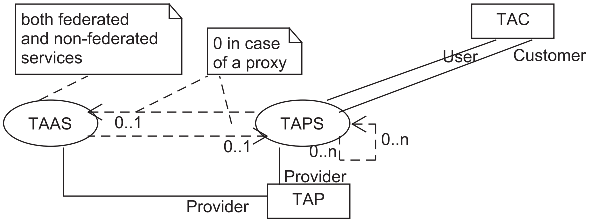

Figure 2: UASM$_{\text{generic}}$ Basic View

With the help of the introduced terms and concepts, we introduce at first **UASM$_{\text{generic}}$ Basic View** (see Figure 2), which is based on MSM Basic View. UASM$_{\text{generic}}$ Basic View is the very fundamental structure and will be used for further refinement to meet the characteristics described above. Services are depicted as ellipses whereas (legal) entities as rectangles, roles (user, customer, provider) like UML association roles and dependencies between services as dashed arrows. Comments like in UML.

In UASM$_{\text{generic}}$, the TAPS serves as a completely generic TAPS and represents an abstract top level class without considering dependent high-level services. Also, in UASM$_{\text{generic}}$ a potentially human real-world subject (RAS) and its digital counterpart TAS, which are to be authenticated, are not considered as acting entities (in the sense of a user/customer) as far as the model and its AuthN services are concerned. That is why they are not present in Figure 2.

TAPSs can be chained, potentially in nested hierarchies with **high-level** TAPSs, e.g., SAML-Proxies, depending on **low-level** ones. In the case of proxies, the providing entity does typically not provide a corresponding TAAS.

The TAC is the user of the TAPS and depending on the AuthN scenario either a **direct** or an **indirect** customer of the TAPS. For example in eduGAIN, a SAML SP of one federation typically does not share a common bilateral contract with a SAML IdP of another federation and thus embodies an indirect customer relationship.

4.2 UASM$_{\text{service}}$ Basic View

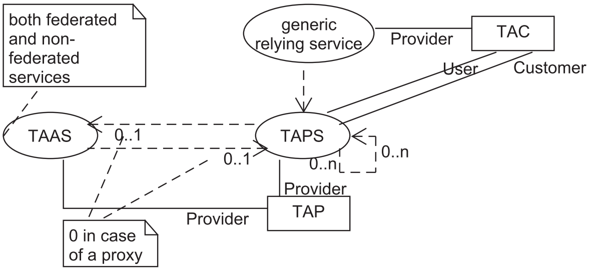

Figure 3: UASM$_{\text{service}}$ Basic View

Often in an AuthN scenario, e.g., in the case of SAML or OIDC, TAPS are **used as sub services** for a dependent high-level service. To differentiate this case from UASM$_{\text{generic}}$, it is called **UASM$_{\text{service}}$**.

In UASM$_{\text{service}}$, the dependent high-level service is called **TAuthNI-relying service** or **generic relying service** and is provided by the TAC (see Figure 3). The generic relying service in turn depends on the TAPS. Here, anything can be authenticated, without being explicit user (/customer) of the generic relying service or TAPS respectively. E.g., animals within an animal shelter, given that the animal does not use/manage authentication itself.

4.3 UASM$_{\text{subject}}$ Basic View

In the case called **UASM$_{\textbf{subject}}$**, illustrated in Figure 4, the RAS is explicitly seen as user of the TAAS and TAPS without considering dependent high-level services.

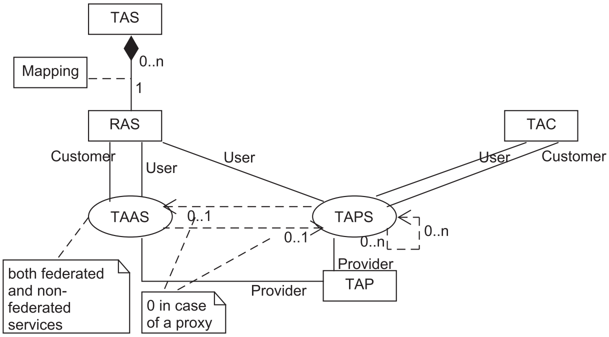

Figure 4: UASM$_{\text{subject}}$ Basic View

4.4 UASM$_{\text{subject-service}}$ Basic View

Often, in such AuthN scenarios the authenticated real-world identity is a human user which is the actual user (/customer) of the high-level service. This is especially the case in SAML, as in SC1, SC4-SC6 and was one of the main motivation to design for and test with UASM. For explicitly such AuthN service scenarios, UASM$_{\text{generic}}$ is first refined to UASM$_{\text{service}}$ / UASM$_{\text{subject}}$ and than extended to **UASM$_{\textbf{subject-service}}$** (see Figure 5). As a further refinement in this case, the dependent high-level service is called here **TAuthNI-relying subject-service (TRSS)**.

Here, the real-world identity is user (/customer) of the TRSS which is depending on the low-level TAPS. That is why, the real-world identity is recursively user/customer (either transparent or intransparent) of the low-level TAPS.

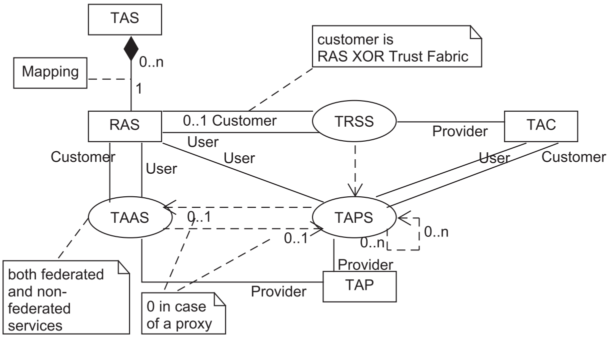

Figure 5: UASM$_{\text{subject-service}}$ Basic View

Moreover, in UASM$_{\text{subject-service}}$ scenarios the real-world identity is typically also explicit user and customer of a TAAS corresponding to the original/principal source of AuthNI regarding his digital identity. So the generic introduction of TAAS as a service (abstraction) shows its usefulness especially in this case.

As being based on MSM, all these service-entity-relationships can be specified and modeled explicitly in UASM$_{\text{subject-service}}$, either in MSM Basic View or recursively applied in MSM Service View/Realization View. Thereby, after having introduced the overall UASMs generic modeling scheme (general UASM definitions and refined MSM classes), Figure 5 provides the resulting UASM$_{\text{subject-service}}$ Basic View in MSM Basic View notation.

5 Conclusion and Further Work

In this paper we highlighted the importance of a generic scenario-independent service-oriented model for AuthN scenarios. For this purpose, seven AuthN scenarios were used to derive requirements, which in turn were used to examine to what extent an existing approach could be reused. The characteristics of the MNM Service Model (MSM) were outlined and shown to match very well to the requirements derived from the example AuthN scenarios. Following, main terms and concepts of the Universal Authentication Service Model (UASM), based on MSM, were introduced. The step-by-step refinement of MSM Basic View towards $\mathrm{UASM}_{\mathrm{generic}}$, $\mathrm{UASM}_{\mathrm{service}}$, $\mathrm{UASM}_{\mathrm{subject}}$ and $\mathrm{UASM}_{\mathrm{subject\text{-}service}}$ Basic View were depicted, which can be used to model and specify any AuthN scenario at an overview level.

Since the work described in this paper is still work in progress, but also due to space constraints, future work will show the instantiation of the example AuthN scenarios using UASM Basic View, which is based on MSM Basic View. Then, as a refinement of UASM Basic View, UASM Service View and UASM Realization View will be introduced. In addition to that, UASMs main terminology and concepts will be complemented, e.g., by the concept of external versus internal TAPS and the way to describe chaining of TAPS. Furthermore, more AuthN scenarios as well as on a higher refinement level need to be instantiated to show UASMs applicability, especially in regard to UASM Service View and UASM Realization View. Additionally, predefined technology specific UASM templates as building blocks for easier application need to be addressed.

References

[GÉ18] GÉANT. eduGAIN Homepage, 2018. https://www.geant.org/Services/Trust_identity_and_security/eduGAIN, accessed: 10/01/2018.

[Ga01a] Garschhammer, M.; Hauck, R.; Hegering, H.-G.; Kempter, B.; Radisic, I.; Rolle, H.; Schmidt, H.; Hegering, H.-G.; Langer, M.; Nerb, M.: Towards generic service management concepts a service model based approach. In: 2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No.01EX470). IEEE, pp. 719–732, 2001.

[Ga01b] Garschhammer, M.; Hauck, R.; Kempter, B.; Radisic, I.; Roelle, H.; Schmidt, H.: The MNM service model - Refined Views on Generic Service Management. Journal of Communications and Networks, 3(4):297–306, dec 2001.

[Ga02] Garschhammer, M.; Hauck, R.; Hegering, H.-G.; Kempter, B.; Radisic, L.; Roelle, H.; Schmidt, H.: A case-driven methodology for applying the MNM service model. In: NOMS 2002. IEEE/IFIP Network Operations and Management Symposium. ' Management Solutions for the New Communications World'(Cat. No.02CH37327). IEEE, pp. 697–710, 2002.

[tmf18] tmforum. Information Framework (SID), 2018. https://www.tmforum.org/information-framework-sid/, accessed: 20/01/2018.

[va17] van der Meulen, P.: Step-up Authentication as-a Service. In: TNC17 - The Art of Creative Networking. 2017.

List of Abbreviations

AuthN	Authentication
AuthN P/S/T/F	AuthN protocols, standards, technologies and frameworks
AuthNI	Authentication Information
AuthZ	Authorization
MFA	Multi Factor Authentication
MNM	Munich Network Management
MSM	MNM Service Model
OIDC	OpenID Connect
OIDC OP	OpenID Provider
OIDC RP	OIDC Relying Party
RAS	Real-World Authentication Subject
SAML	Security Assertion Markup Language
SAML IdP	SAML Identity Provider
SAML SP	SAML Service Provider
TAAS	Trustworthy Authentication Information Administration Service
TAC	Trustworthy Authentication Information Consumer
TAP	Trustworthy Authentication Information Provider
TAPS	Trustworthy Authentication Information Provisioning Service
TAS	Trustworthy Authentication Subject
TAuthNI	Trustworthy Authentication Information
TRRS	Trustworthy Authentication Information relying subject-service
U2F	Universal Second Factor
UASM	Universal Authentication Service Model