# Protecting Privacy of Identities in Federated Operator Environments

Benjamin Weyl, Pedro Brandão, Antonio F. Gómez Skarmeta, Rafael Marin Lopez, Parijat Mishra, Christian Hauser, Holger Ziemek

***Abstract*—Personalized, mobile, and location-aware services definitely require the federation of administrative domains, e.g., access network operators, content and service providers. Various federated operator scenarios, reflecting different levels of content and service aggregation, require the secure setup of a Circle of Trust. Standards and technologies, such as proposed by the Liberty Alliance Project or by application of the Security Assertion Markup Language (SAML), already support the idea of building federations by connecting identities, roles, and profiles. But the option of protecting different levels of privacy for the user is yet not guaranteed. This paper introduces a concept for the federation of identities and roles between administrative domains, while still protecting the privacy of the customer by the use of identity concealment and dynamically created federated identities. The concept enables a very efficient, secure and adaptive privacy protection for service registration at different layers, having access control to value-added services, as well as to network services.**

***Index Terms*—Federation, Identities, Identity Token, Privacy, SAML, Security.**

## I. Introduction

Future networks will necessitate various relationships between different entities, such as service providers, network operators and service consumers. Secure solutions will be required for the management of multiple contracts with their corresponding consumer identities, for the integration of authentication and authorization mechanisms, for providing service access to consumers as seamlessly as possible while protecting their privacy, and for integrating new entities (such as administrative domains or value-added service providers). It may be desirable to separate the service infrastructure from the access network infrastructure in order to deliver services regardless of specific access technologies or security mechanisms. These issues are currently being researched within the IST project DAIDALOS [1].

This paper focuses on future federated operator scenarios and their challenges for protecting privacy and managing identities and roles. In Section II, we will present the security infrastructure needed. We will state the scenarios that drive it in its requirements in II.A and the privacy threats we wish to deter in Sub-section II.C. In Section III, our model is described with an introduction to identity concepts in III.A, adding federation to our identity model in III.B. III.C defines a token used for authentication/authorization procedures. In III.D, we will describe the model usage and the privacy obtained. III.E mentions other utilizations of the concept in authorization on access network. Finally, Section IV presents the conclusions we reached and some future research needed.

Manuscript received February 06th, 2005.

B. Weyl is with BMW Group Research and Technology, Munich, Germany (e-mail: benjamin.weyl@bmw.de).

P. Brandão is with University of Oporto, Oporto, Portugal (e-mail: pbrandao@ncc.up.pt).

A. F. Gómez Skarmeta and R. Marin Lopez are with University of Murcia, Murcia, Spain (e-mail: {skarmeta, rafa}@dif.um.es).

P. Mishra is with Institute for Infocomm Research, Singapore (e-mail: parijat@i2r.a-star.edu.sg).

C. Hauser is with University of Stuttgart, Stuttgart, Germany (e-mail: hauser@ikr.uni-stuttgart.de).

H. Ziemek is with Fraunhofer FOKUS, Berlin, Germany (e-mail: ziemek@fokus.fraunhofer.de).

The work described in this paper is based on results of IST FP6 Integrated Project DAIDALOS. DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

## II. Distributed Security Infrastructures

### A. Federated Operator Scenarios

Future networks pose new challenges to service operators, service provisioning platform operators (SPPO), content service providers, and access network operators by introducing multiple administrative domains and federations, as well as by introducing users who simultaneously have multiple identities and maintain multiple sessions on different devices.

Provider deployment can and will be based on diverse settings: (a) Some providers will not possess any security framework and rely on SPPO to provide them with the complete infrastructure for hosting the service (accounting, decision points, enforcement points, etc.); (b) At the other extreme, there will be providers with a full-blown security infrastructure, where policies are defined and enforced in their own domains; (c) In between, there will be providers with only accounting servers or with only policy decision points, etc. These scenarios (in particular, "a" and "c") motivate us to use concepts of federation. Even the all-in-one provider (case "b") will be accessed by users of other domains, and will require some federation. Federation can allow for interconnections

between SPPO, service providers, and, in general, between administrative domains.

### B. Security Requirements of a Federated Infrastructure

Maintaining a homogeneous level of security and guaranteeing a high level of seamless access to services in these environments is complex and challenging. The following issues are relevant:

- There will be multiple authentication mechanisms;
- Single-Sign-On (SSO) for multiple services and administrative domains which will be needed;
- Authorization may be distributed, i.e., policies located at different administrative domains may be combined to perform the authorization decision;
- One user may have multiple identities, with multiple providers;
- There will be multiple sessions of multiple users using multiple devices;
- There will be contracts between all participating entities.

Within DAIDALOS, we have chosen to use the Security Assertion Markup Language (SAML) [2] for integrating distributed authentication, authorization and SSO into federated, Beyond-3G operator concepts [3][4][5]. SAML standardizes the exchange of information about a user's authentication status, authorization decisions and attributes. By applying SAML, the authentication infrastructure can be made independent of the specific mechanism used for the authentication of users. In addition, SAML supports SSO across administrative domains.

The main advantages of introducing a standardized security infrastructure are: (a) Standardized exchange of security information between different administrative domains; (b) Facilitated mobility management and joint security services across different domains; (c) Independence from underlying specific security mechanisms provided within a single domain; (d) Easy integration and federation of independent services (value-added, content, etc.) into the security infrastructure.

These advantages result in a decoupling of value-added service provider's infrastructure from access network infrastructure on one hand (distributing services independently from specific access technologies), and on the other hand enabling the usage of the same security functionalities for network security and building secure federations among all participating entities.

### C. Threats Against Privacy

We assume that the authentication and authorization protocols are robust against passive and active attacks. That still leaves the user with some privacy concerns. We consider the following scenarios:

1. A user may wish that a passive attacker snooping on the network (a) is unable to find his/her "real" identity; and/or (b) is unable to connect multiple connections to a given service in order to build a usage profile;
2. A user may wish to achieve the same privacy levels (a), (b), as above, but with respect to the service provider whose service he/she is accessing.

With regard to the last concern, a service provider may still look for patterns of usage, etc. to link multiple service invocations back to the same user. We consider this risk acceptable.

## III. Privacy and Identity Model

### A. Overview of the Identity Model

In distributed networks users may have multiple contracts with different providers, using various digital identities. Future networks will have to provide an identity management framework which (a) ensures that services can be personalized, (b) allows users to keep control over their privacy, (c) and yet guarantees that a consumed service can be charged to the right person and (d) allows tracking of malicious service usage. The identity management framework must be able to facilitate private information to be flexible, ranging from allowing a user to access a service without the service getting any information about the user (and being nonetheless paid for providing the service), to letting the service access the user's private information (even when no *direct* contract exists between service and user) in order to provide the best possible service. In other words, it has to be able to provide different levels of security and privacy, allowing users to trade privacy against convenience when necessary. Access to any information, of course, has to be granted by its owner.

Leveraging on some current research [6][7], in the DAIDALOS project we developed a model for achieving the above goals. In our model, a user can choose the identity he/she wants to use to authenticate and register for services. When the user signs a contract, an identity under which the contract and the respective profiles and rights are defined is issued. This identity, called Registration Identity (RegID), holds the information necessary for charging its owner, and can be seen as the system representation of the signer of the contract. For the purpose of having different levels of privacy, Virtual Identities (VID) are defined on-the-fly. These identities are always related to a RegID and can share all or none of the RegID's attributes. As such, they are privacy-enabled and possibly anonymous representation of the RegID. The following key assumptions for identities are defined:

- Each operator assigns one RegID to each customer. This RegID is unique in the operator's domain. The RegID is operator confidential.
- Services are accessed only with VIDs. All customers will have to use at least one pre-defined VID. Additional VIDs can be defined by the user for the usage of specific services and federations across administrative domains.
- The operator's authentication, authorization and charging subsystems are the only components allowed to map the VID to the RegID. The RegID is not transmitted over the network.

- Each RegID should be associated with a RSA key pair issued by the operator. This can be used for the signature in the ID-token (see III.C).
- Each VID can be associated with a RSA key pair issued by the operator. This key pair can be used for different cryptographic functions (e.g., they can be used for the ID payload in IKE negotiation of an IPsec tunnel [8]).
- SSO over multiple operator domains will require either a globally defined name space guaranteeing ID uniqueness, or "identity mappings" (e.g., mapping/federation of VIDs) between operators.

These key assumptions result in the design of an identity management system with the relationships shown in Fig. 1. The Identity Manager of the operator (being a core component of the authentication, authorization and charging unit) maps VIDs to RegIDs. VIDs can have different roles and profiles. These profiles hold the attributes that are allowed to be given to the service accessed with the VID, including service specific attributes and rules. Since at generation time, attributes of a VID can be easily copied from a template, multiple VIDs can be generated and used to access a service in a consistent, personalized manner.

The normal usage of VIDs protects privacy on scenarios 1 (a) and 2 (a) mentioned in Section II.C, as the user's real identity is never revealed. By changing VIDs often, levels 1 (b) and 2 (b) can be achieved as well. If the user wants to have a maximum level of privacy, VIDs will have to be used randomly or even for one time only, requiring the generation of VIDs dynamically[1].

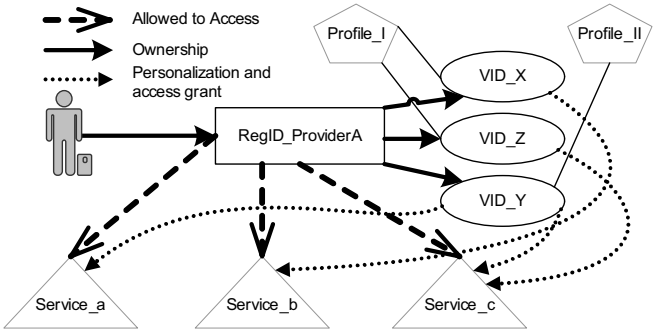

Fig. 1: Mapping of identities with profiles

### B. Identity Federation

The federation of identities between administrative domains implies the setup of a trusted relationship and the sharing of various identities, attributes and profiles. Privacy has to be controlled from the user-perspective and thus be flexible. Hence, the user defines the federation rules, i.e., the policies and restrictions for the federation of specific identities and profiles. These issues strongly demand a component able to operate as an independent and trusted entity building up secure federations, but also being able to handle identity and access management between administrative domains protecting the users' privacy.

The Federation Manager, as shown in Fig. 2, handles the needed federation of Identity Managers and (SAML) Asserting Authorities across administrative domains.

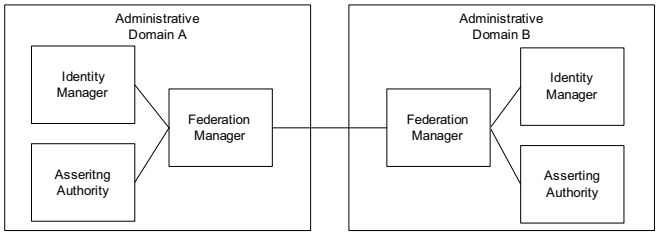

Fig. 2: Federating identities between administrative domains

Various types of federations related to the described identity model are possible:

- "Virtual domain" federation, based on mapping RegIDs: In this case, the user decides to federate administrative domains revealing all VIDs and profiles to all participating entities within the federation. Federation based upon a RegID is only reasonable, if the user wants to define one single "virtual" domain, i.e., all data about RegIDs is shared between administrative domains.
- Privacy enabled "virtual domain" federation based on mapping RegIDs: In this case, too, the user decides to reveal all identities and profiles, but the information is anonymized to entities belonging to the other domain. This is done by a translation between the RegIDs of both domains within the Federation Manager.
- Federation based on mapping VIDs: In this case, the user selects specific VIDs of each administrative domain to be federated, in order to control his/hers privacy. The user can define specific rules for this federation. The Federation Manager controls the type of federation, rules and policies the user has defined. The mapping of the identities then takes place within the Federation Manager.

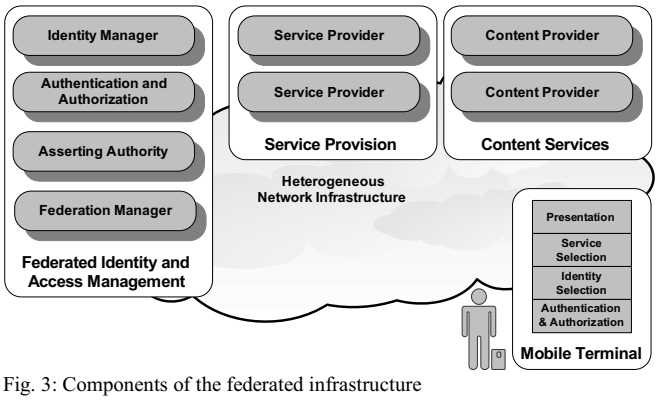

Fig. 3: Components of the federated infrastructure

It is important for the user that his/her level of privacy, although controlled by him/her, is the least obstructive as possible. Fig. 3 shows all components necessary to build up a secure identity federation based on the described model.

[1] VID generation is not discussed in this paper; however, in summary, VIDs need to be registered or cryptographically linked to the RegID. This is even more necessary for VIDs with keys associated.

### C. Identity Token Concept

In the DAIDALOS project, there will be innumerous authentication/authorization requests for the user. A small credential that can be reused several times and mapped to a user's authorizations settings is needed. The SAML artifact poses as a good candidate, as it is a pointer to an assertion where the user's authorization statements could be kept. It has the problem of not being reusable. Thus, the artifact has to be enhanced for providing sufficient security over the network. This led to the Identity Token (ID-token) containing (see Fig. 4):

- The VID as the identity used for the specific service request whose identifier is of the form string@realm,
- A random number that makes the ID-token different each time it is sent,
- A sequence number to help avoid replay-attacks; its value is maintained by the Asserting Authority,
- A SAML artifact that references the appropriate SAML assertion referring to the RegID,
- *Signature* is a digital signature made over the whole ID-token by using the sender's private key—in most cases the key associated to the RegID.

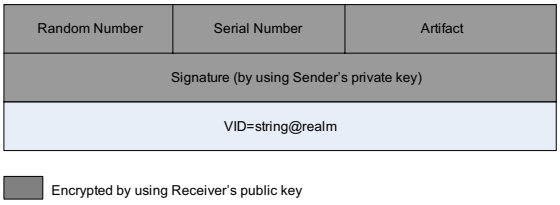


Fig. 4: Content of an ID-token

### D. Identity Concealment for Authentication/Authorization

The Asserting Authority, in conjunction with the Identity Manager, plays an important role in concealing identities and protecting users' privacy. The RegID is never revealed and is concealed by using VIDs.

The Asserting Authority has the following main functionalities for concealing the RegID:

- Asserting and providing information on a user's successful authentication via an authentication assertion. Authentication takes place based on a user's VID. The VID is mapped to the respective RegID (by accessing the Identity Manager) and an authentication assertion is generated and stored. Thus, the Asserting Authority can prove one's authentication to another entity within the federation.
- Issuing authorization decisions: For authorizing a specific user to a requested value-added service, the Policy Enforcement Point of the service can request authorization decisions from the Authority. The Asserting Authority issues the authorization decision based on the policies and profiles it holds connected to the binding of the VID and the Service Identifier (the access grant from Fig. 1).
- Collecting and issuing users' attributes and profiles: If a service has to be personalized for the user, it may require some attributes and profiles. The authority can collect the required attributes from the profile associated to the VID and issue them via an attribute assertion.

The concept has been successfully integrated within the DAIDALOS testbed. Fig. 5 illustrates the process for the purpose of authentication and authorization.

(1) A specific VID for authenticating at the Authentication Authority is either autonomously chosen or selected by the user (depending on user's previous configuration). Using AAA (Authentication, Authorization and Accounting) mechanisms [9], the VID and its credentials are routed to the authentication unit at the "home provider." (2) Provided credentials are verified and the user authenticates against the access management system. (3) The Authentication Authority requests the generation of an authentication assertion (based on the successful authentication) from the Asserting Authority. The Asserting Authority (4) maps the VID to the RegID, (5) creates an authentication assertion and ID-token, both directly related to the RegID, and stores the data. (Tying the assertion to the RegID, instead of the VID used for performing the authentication, guarantees that the authentication assertion is mapped to all VIDs related to the RegID.) The ID-token including the SAML artifact, is sent to the Mobile Terminal (MT), where it is stored for further service requests and network access authorizations.

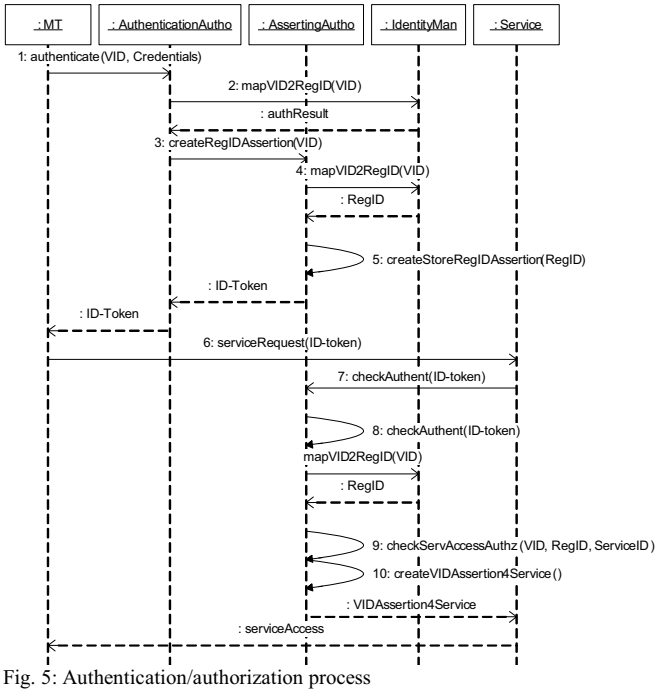


Fig. 5: Authentication/authorization process

(6) A specific VID is used for accessing a service or network. Valid VIDs can be requested from the Identity Manager. The ID-token is included in the request to the specific enforcement point of a value-added service or a network service. (7) The enforcement point of the service

requests information on the user's successful authentication and authorizations from the Asserting Authority. After (8) validation of the ID-token, (9) authorization to access the service is checked. Because the service is not allowed to obtain the authentication assertion related to the RegID directly, a new assertion for the currently used VID is generated (10), which contains profile, attribute and authorization information. This information is then transferred to the enforcement point.

The described scenario presupposes all components in the same domain. An inter-domain process would involve the Federation Manager to map the VID according to the federation model used (as described in Sub-section III.B).

The identity model and the federation architecture described make possible that the user's real identity RegID is kept within a few trusted components (the home operator's AAA infrastructure) and that the user is able to "disguise" him/herself by using how many VIDs he/she wishes.

### *E. Further Applications*

Up to now, XML technologies like SAML were supposed to be transported via SOAP and HTTP, thus being mainly integrated on the application level. For that reason, SAML is applied for security within the service infrastructure. In order to benefit from these technologies for authentication and authorization within an access network infrastructure as well as on the link and network layer, existing protocols used on this layer have to be adapted and extended properly. In fact, some proposals like those suggested in "Using SAML for SIP" [10] have started to envision a new usage of SAML within the context of service authorization. In the area of network authentication, current, well-established protocols are the Extensible Authentication Protocol (EAP) [11], performed over the link layer, PANA [12] for carrying EAP packets over IP between terminals and the access network server via the network layer, and DIAMETER [9] for transporting the authentication protocol to the desired backend authentication and service infrastructure. In this context, network access, and especially QoS enabled network services, could be considered just like any other service being managed by authorization procedures. Within the DAIDALOS architecture, there is ongoing work to use the model described here coupled with PANA, EAP and DIAMETER for network authentication. A separation of initial authentication and service authorization has been considered, where the initial authentication takes place when the network session is being created and the user is not in possession of an ID-token yet. In this process, the user will recover an ID-token to enable the federation service access for him/her.

For the purpose of network re-authentication and fast-handover, the integration of the ID-token concept and SAML within EAP is being considered and evaluated as well. The intention is to have a very efficient mechanism for network re-authentication and authorization supporting the protection of a user's privacy. Using the ID-token concept for access network re-authentication enables a simpler and direct "pointer" to the authentication/authorization status of the MT, so complex authentication mechanisms and round-trips are reduced to a minimum. A detailed analysis of the additional signalling load incurred by the SAML-based Id-token approach and its performance aspects have to be left for further study.

## IV. CONCLUSION

In beyond-3G systems, very complex relations between entities and administrative domains emerge, and security is a challenging task. In order to support various future federated operator scenarios, a very flexible security infrastructure is required. The federation of identities, profiles and attributes on one hand is a requirement for enabling personalized and mobile location-aware services. On the other hand, controllable and adjustable privacy has to be covered. The described concept enables a highly flexible and privacy-protecting identity and role management for federated operator scenarios. Identities are concealed but service-consumption is personalized, thus protecting the users' privacy. By applying this concept, applications such as network and value-added service authorization, fast hand-over, QoS and context-transfer can be optimized. An extensive comparison to the Liberty Alliance Project [13] will be described in future work.

One of the aspects requiring future analysis is the trade-off between the dynamic creation of VIDs and the associated cryptographic material needed for the security functions. In that sense, the possibility of several VIDs sharing a pair of RSA keys could help to reduce the computational cost of the management, although reducing the privacy of the system.

## REFERENCES


[1] DAIDALOS Project, http://www.ist-daidalos.org/.

[2] Ph. Hallam-Baker, E. Maler (eds.), "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1," OASIS Standard, Version 1.1, September 2nd 2003, http://www.oasis-open.org.

[3] B. Weyl, "Single Sign-On and Web Services Security for an Open Telematics Market," Technical University of Munich, 2003.

[4] B. Weyl, H.-J. Vögel, H.-U. Michel, "Integrated Authentication for Telematic Services and Beyond-3G Access Infrastructures using SAML", in Proceedings of IST Mobile & Wireless Communications Summit, Lyon., France, June 2004, pp. 212-217.

[5] DAIDALOS Deliverable 341,"A4C Framework Design Specification".

[6] U. Jendricke, M. Kreutzer, A. Zugenmaier, "Mobile Identity Management", UBICOMP 2002, October 2002.

[7] A. Durand,"How the Nature of Identity Will Shape Its Deployment",www.digitalidworld.com/misc/LayersofIdentityArticle.pd, November 2003.

[8] D. Maughan, M. Schertler, M. Schneider, J. Turne "Internet Security Association and Key Management Protocol (ISAKMP)", IETF RFC 2408, November 1998.

[9] P. R. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", IETF RFC 3588, September 2003, http://www.diameter.org/drafts/latest/draft-ietf-aaa-diameter-17.txt.

[10] H. Tschofenig, "Using SAML for SIP", draft-tschofenig-sip-saml-02 (work in progress), December 2004, http://www.ietf.org/internet-drafts/draft-tschofenig-sip-saml-02.txt.

[11] L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz "Extensible Authentication Protocol (EAP)", IETF RFC 3748, June 2004.

[12] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-07 (work in progress), December 2004.

[13] Liberty Alliance Project, http://www.projectliberty.org/.