ETSI GS INS 003 V1.1.1 (2010-11)

Group Specification

Identity and access management for Networks and Services; Distributed User Profile Management; Using Network Operator as Identity Broker

Reference

DGS/INS-003

Keywords

access, ID, manegement, network, profile, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification (ISG) Identity and access management for Networks and Services (INS).

1 Scope

The present document analyses the telecommunication operator's role acting as Identity Broker to facilitate the anchor functionalities for the management of distributed user profile information, which is currently handled in an ad-hoc or proprietary way without standardized way. The present document also defines the protocol specifying the procedure to access to the user profile information via Identity Broker, the extensible user profile data model as core and the user profile data model for the telecommunication area, to be standardized.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] Liberty Alliance Data Services Template v2.1.

NOTE: Available at http://www.projectliberty.org/liberty/content/download/879/6213/file/liberty-idwsf-dst-v2.1.pdf.

[2] OASIS Security Services (SAML) TC.

NOTE: Available at http://www.oasis-open.org/committees/security/.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 122 985: "Universal Mobile Telecommunications System (UMTS); Service requirements for the User Data Convergence (UDC) (3GPP TR 22.985)".

[i.2] ETSI TS 123 335: "Universal Mobile Telecommunications System (UMTS); LTE; User Data Convergence (UDC); Technical realization and information flows; Stage 2 (3GPP TS 23.335)".

[i.3] ETSI TS 129 240 (V8.0.0): "Universal Mobile Telecommunications System (UMTS); LTE; 3GPP Generic User Profile (GUP); Stage 3; Network (3GPP TS 29.240 version 8.0.0 Release 8)".

[i.4] ETSI TS 129 335: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; User Data Convergence (UDC); User data repository access protocol over the Ud interface; Stage 3 (3GPP TS 29.335)".

[i.5] Liberty ID-WSF Web Services Framework Overview.

NOTE: Available at http://www.projectliberty.org/liberty/content/download/889/6243/file/liberty-idwsf-overview-v2.0.pdf.

[i.6] OpenID.

NOTE: Available at http://openid.net/.

[i.7] Open Mobile Alliance.

NOTE: Available at http://www.openmobilealliance.org/.

[i.8] Open Mobile Alliance™, OMA-ERP-GSSM-V1-0: "OMA General Service Subscription Management".

NOTE: Available at http://www.openmobilealliance.org/.

[i.9] Open Mobile Alliance™, OMA-RD-SUPM-V1-0: "Service User Profile Management Architecture".

NOTE: Available at http://www.openmobilealliance.org/.

[i.10] Open Mobile Alliance™, OMA-ERP-NGSI-V1_0: "OMA Next Generation Service Interfaces".

NOTE: Available at http://www.openmobilealliance.org/.

[i.11] ETSI EG 202 325 (V1.1.1): "Human Factors (HF); User Profile Management".

[i.12] ETSI ES 202 746 (V1.1.1): "Human Factors (HF); Personalization and User Profile Management; User Profile Preferences and Information".

[i.13] ETSI TS 102 747 (V1.1.1): "Human Factors (HF); Personalization and User Profile Management; Architectural Framework".

[i.14] Schema for Open ID Exchange (AX Schema).

NOTE: Available at http://www.axschema.org/.

[i.15] Organization for the Advancement of Structured Information Standards.

NOTE: Available at http://www.oasis-open.org/.

[i.16] ETSI GS INS 002: " Identity and Access Management for Networks and Services; Distributed Access Control for Telecommunications; Use Cases and Requirements".

[i.17] ETSI GS INS 001: "Identity and access management for Networks and Services; IdM Inter-operability between Operators or ISPs with Enterprise".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

circle of trust: federation of service providers and identity providers that have business relationships based on Liberty (or similar) architecture, and operational agreements, with whom users can transact business in a secure and seamless environment

identity broker: Service Provider that receives requests for Identity information from another Service Provider and subsequently requests that information from other Provider(s)

NOTE: The Identity Broker aggregates the data and responds to the originating Service Provider.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AX	Attribute Exchange
CRUD	Create Read Update and Delete
DTS	Data Services Template
FE	Front Ends
GSSM	General Service Subscription Management
GUP	Generic User Profile
HLR	Home Location Register
HSS	Home Subscriber Server
IdP	Identity Provider
ID-WSF	Identity Web Services Framework
NGSI	Next Generation Service Interface
OASIS	Organisation for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
OSS	Operation Support System
RAF	Repository Access Function
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SUPM	Service User Profile Management
UDC	User Data Convergence
UDR	User Data Repository
UML	Unified Modeling Language
VOD	Video-On-Demand
XML	Extensible Markup Language

4 User Profile Management in Cross-Domain Cases

Today, the user profile information is stored / managed / used at different service providers fully distributed. Application service provider needs to retrieve profiles of a user from different attribute providers in order to perform personalized services to that user. At the same time, users want to manage their distributed profile in an easy yet privacy protected way. To fulfil these requirements, there are needs for the anchor point for accessing all the user profile information by users and service providers, and this anchor point must have sufficient trust both by users and application service providers.

The involvement of trusted Identity Provider as this anchor point is straightforward approach for distributed user profile management. The user profile information is already maintained at Identity Provider as attribute, where the standards for the attribute exchange mechanism already exists, which and should be extendable to the fully distributed user profile cases.

These trusted Identity Providers are considered as telecommunication operators. Many of the telecommunication operators already serve as Identity Providers, have trust relationship with their users, and have secure network infrastructure, which provide secure and privacy protected way of accessing data, technically and socially, thus considered as suitable for the anchor point of the distributed user profile management.

Thus, this work item proposes for the study and standardization of the distributed user profile management by extending the Identity Provider, where the Identity provider is considered as telecommunication operator, taken both the business and technical aspects into consideration.

This clause provides the overview of the existing standard works relevant to the distributed user profile management, identifies the problems/missing points to realize the distributed user profile management in cross-domain cases and proposes the approach to address those points.

4.1 Current Landscape

4.1.1 OASIS SAML

SAML [2] is an XML-based framework for communicating user authentication, authorisation, and attribute information developed by the Organization for the Advancement of Structured Information Standards (OASIS) [i.15]. SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. Thus, SAML can be considered as the transport protocol standard for federated identity management. SAML supports federation in multiple ways and focuses on the mapping of attributes into a uniform namespace and the secure, reliable transport of assertions.

SAML is defined in terms of assertions, protocols, bindings, and profiles.

An assertion is a package of information that supplies one or more statements made by a SAML authority. The protocols define the procedure to request for assertions, authentication, identifier registration/de-registration and mappings, and logouts. The bindings describe the integration of SAML into HTTP or SOAP. The profiles define constraints and extensions in support of the usage of SAML for a particular application.

The SAML protocol allows different identity management solutions to communicate with each other, providing platform neutrality, loose coupling of directories and linking of identities with respect to the user's privacy. It provides communication mechanisms required for single sign-on with distributed identity data, including user profile. The user can be authenticated by its identity provider, while the authorisation of his login takes place at the service provider.

SAML assertions are usually transferred from identity providers to service providers. Assertions contain statements that service providers use to make access control decisions. Three types of statements are provided by SAML:

- authentication statements;
- attribute statements; and
- authorisation decision statements.

Authentication statements assert to the service provider that the principal did indeed authenticate with the identity provider at a particular time using a particular method of authentication. The authentication context may be disclosed in an authentication statement. An attribute statement asserts that a subject is associated with certain attributes to be used for access control decisions by the service provider. An authorisation decision statement asserts that a subject is permitted to perform an action on a certain resource.

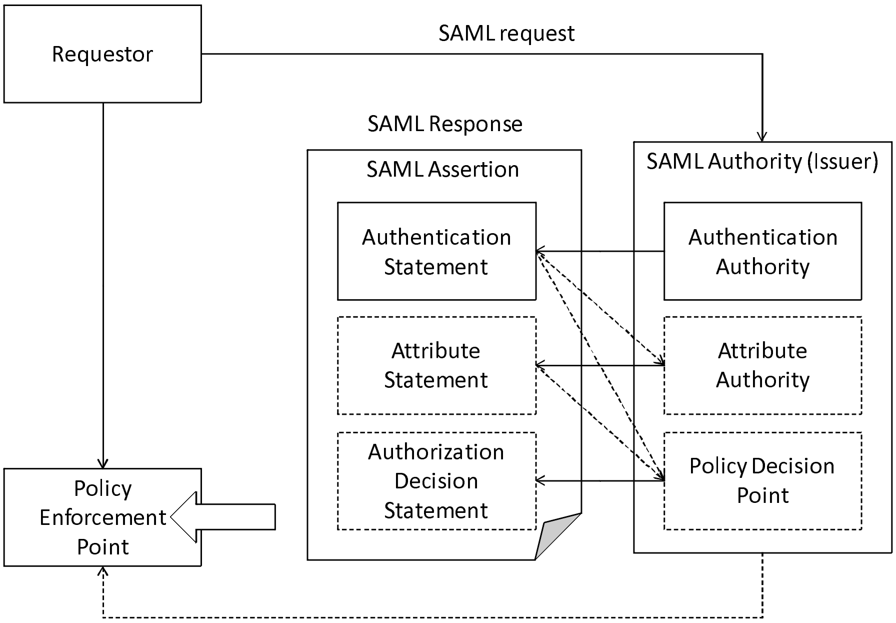


Figure 1: Overview of SAML framework

By definition, SAML can be used for exchanging attribute information and can be used as a base protocol for exchanging distributed user profile data among entities.

4.1.2 Liberty Alliance ID-WSF and DST

Liberty ID-WSF Web Services Framework [i.5] defines a framework for identity-based web services in a federated network identity environment, including attribute exchange mechanism. The ID-WSF Data Services Template [1] provides the building blocks when implementing a data service on top of the ID-WSF.

The Data Services Template (DST) [1] is an XML-based protocol for the exchange and management of user information that is distributed over several authorities. Additionally it provides mechanisms that allow a consumer of user data to subscribe to changes of that data. The providing authority can then notify the consumer of such changes. DST provides protocols for the creation, query, modification, and deletion (a.k.a. "CRUD") of data attributes, exposed by a data service, related to a Principal. Some guidelines, common XML attributes and data types are defined for data services.

A data service is a web service that supports the storage and update of specific data attributes regarding a Principal. A data service might also expose dynamic data attributes regarding a Principal. Those dynamic attributes may not be stored by an external entity, but the service knows or can dynamically generate their values. An example of a data service would be a service that hosts and exposes a Principal's profile information (such as name, address and phone number). An example of a data service exposing dynamic attributes is a geolocation service.

DST is supposed to be used as a template to support different services with necessary extensions for individual services. The data services using the present document can also support other protocols in order to support to other features, such as supporting actions (e.g. making reservations).

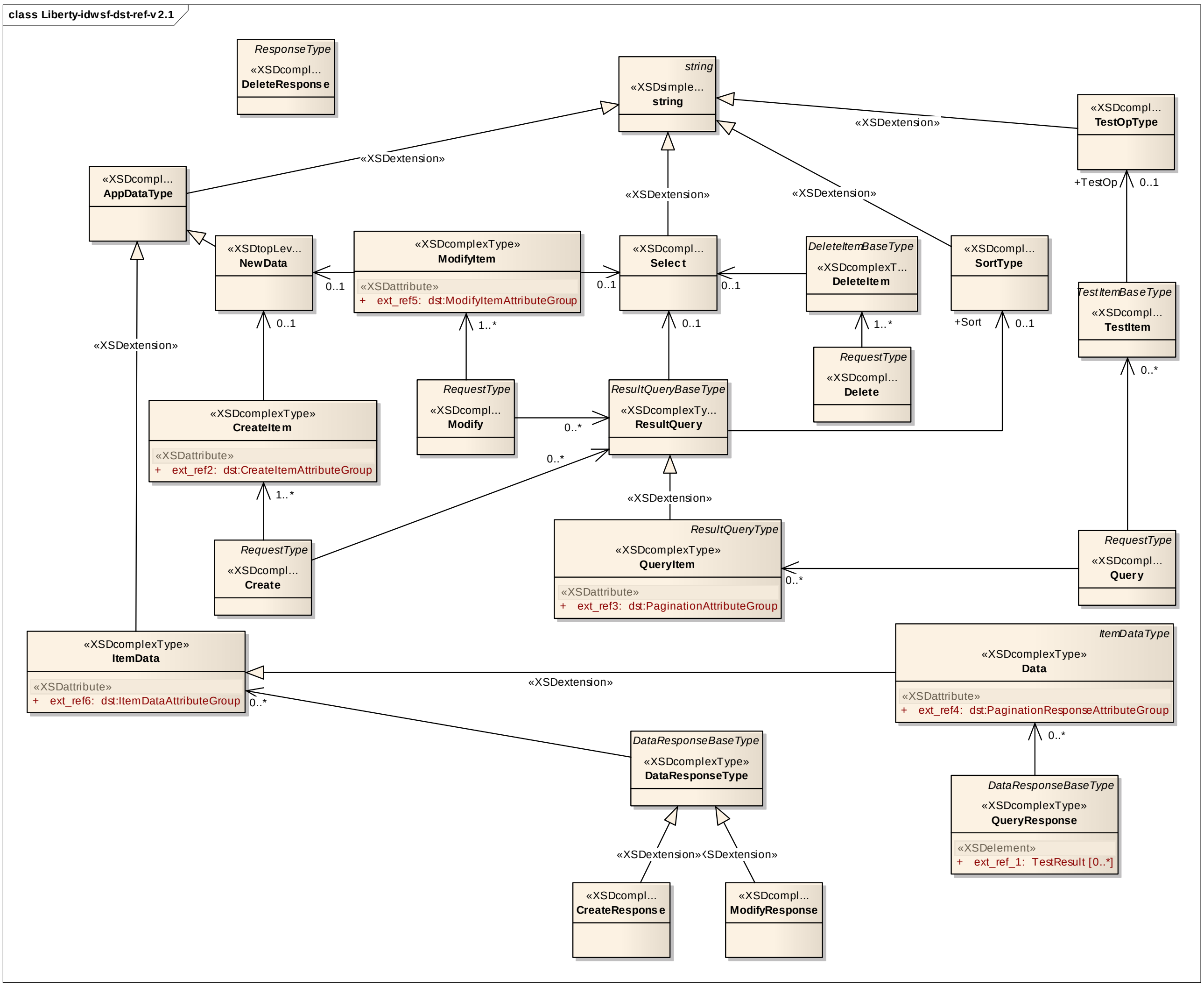

class Liberty-idwsf-dst-ref-v2.1
ResponseType «XSDcompl... DeleteResponse
string «XSDsimple... string
«XSDcompl... TestOpType
«XSDextension»
«XSDcompl... AppDataType
«XSDextension»
«XSDextension»
+TestOp 0..1
«XSDtopLev... NewData
«XSDcomplexType» ModifyItem
«XSDattribute» + ext_ref5: dst:ModifyItemAttributeGroup
«XSDcompl... Select
DeleteItemBaseType «XSDcomplexT... DeleteItem
«XSDcompl... SortType
TestItemBaseType «XSDcompl... TestItem
0..1
0..1
0..1
0..1
1..*
0..1
1..*
+Sort 0..1
0..*
«XSDextension»
«XSDcomplexType» CreateItem
«XSDattribute» + ext_ref2: dst:CreateItemAttributeGroup
RequestType «XSDcompl... Modify
ResultQueryBaseType «XSDcomplexTy... ResultQuery
RequestType «XSDcompl... Delete
0..*
0..*
1..*
«XSDextension»
RequestType «XSDcompl... Create
ResultQueryType «XSDcomplexType» QueryItem
«XSDattribute» + ext_ref3: dst:PaginationAttributeGroup
RequestType «XSDcompl... Query
0..*
«XSDcomplexType» ItemData
«XSDattribute» + ext_ref6: dst:ItemDataAttributeGroup
ItemDataType «XSDcomplexType» Data
«XSDattribute» + ext_ref4: dst:PaginationResponseAttributeGroup
«XSDextension»
0..*
0..*
DataResponseBaseType «XSDcomplexType» DataResponseType
DataResponseBaseType «XSDcomplexType» QueryResponse
«XSDelement» + ext_ref_1: TestResult [0..*]
«XSDextension»«XSDextension»
«XSDcompl... CreateResponse
«XSDcompl... ModifyResponse

Figure 1a: DST structure in UML class diagram

4.1.3 OpenID Attribute Exchange

OpenID [i.6] is a user centric identity management solution. It allows a user to authenticate to a website using a URL.

The relying party, i.e. the site the user authenticates to, queries the asserting party for an authentication. The asserting party is the Identity Provider that can provide a proof of authentication for the user.

The main advantage of OpenID is to allow a user to use a single password for multiple sites. It is light-weight and easy to implement. It neither provides single-sign-on nor does it allow the usage of privacy-enhancing techniques such as pseudonyms.

While OpenID deals primarily with the authentication of the user, an extension to support Attribute Exchange (AX) was made part of core specification in OpenID2.0. This extension defines the information model, discovery and message exchange for AX on top of OpenID. The protocol follows the same steps as in the Open ID base exchange and is usually combined in a single run of the protocol where both the attributes and the authentication step is completed simultaneously.

Since the base protocol does not specify a data schema to be used with OpenID AX, a community initiative called AX Schema [i.14] has made a base schema which is widely used with OpenID AX.

4.1.4 3GPP GUP and UDC

4.1.4.1 Generic User Profile

The 3GPP Generic User Profile (GUP) [i.3] provides a conceptual description to enable a harmonized usage of user-related information located in different entities and normally accessed through a variety of protocols. In short, GUP provides a virtual, centralized, user database. GUP defines architecture, data description and interfaces along with mechanisms to handle the data and is currently aligned with Liberty Alliance specifications.

4.1.4.1.1 General Architecture

Generally speaking GUP was defined by 3GPP to manage the user-centric data repository architecture. GUP's architecture provides data description and interfaces with mechanisms to handle user's data. GUP architecture is presented in Figure 2. The components of the architecture are described in the following clauses.

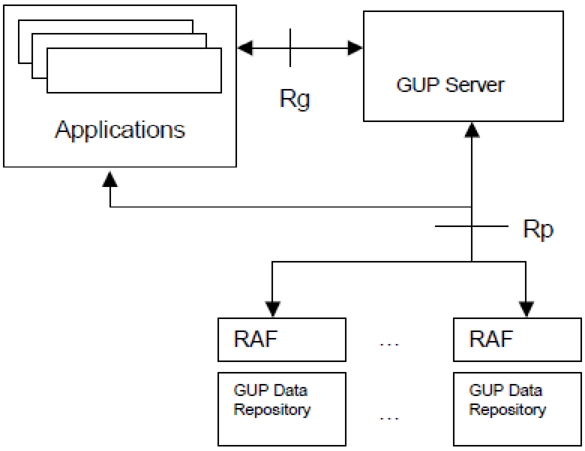


Figure 2: GUP Reference Architecture

4.1.4.1.2 GUP Server

GUP Server contains the metadata that holds the knowledge of the location of the data components and the different data repositories. It also acts as a gatekeeper by authorizing or denying access to profile data. The GUP server either operates in proxy mode (collects the requested data and provides it to the requestor), or in redirect mode (provides the addresses of the respective data repositories to the requestor). It acts therefore as a data "federator" and offers a single point of entry to the Operation Support System (OSS).

The user-centric data repository architecture may offer operators the possibility of facilitating the operations, administration and maintenance of the network. This is achieved through:

- Single point of access to the user profile data of the operator's network.
- The architecture's applicability to all carriers: fixed, mobile, wireless and converged.
- Harmonized access interface.
- Authentication and Authorization of profile access.
- Privacy control.
- Synchronization of data storage.
- Access profile from visited networks.
- Location of profile components.
- Charging for profile access.

The requests from the operator or from a 3rd party application through the Rg interface can be authenticated in two different schemes. The authentication can be done either by a separate (trusted) entity or based on the identification (e.g. IMS Public Identity) of the requesting application and/or of the possible subscriber requesting the user profile data.

4.1.4.1.3 Repository Access Function (RAF)

The Repository Access Function (RAF) works as an abstraction that hides the implementation detail of the repositories where the user's profile is stored. It performs protocol and data transformation where needed between the repositories and the GUP. It could also take part in the authorization process regarding the data in the corresponding GUP data repository. Examples of an GUP data repository is the HSS (Home Subscriber Server) or the HLR (Home Location Register).

4.1.4.1.4 Applications

GUP architecture provides support for both operator and 3rd party applications. Operator can access directly RAF elements using Rp interface. By using Rg interface, applications have a single point of contact to retrieve user's profile information.

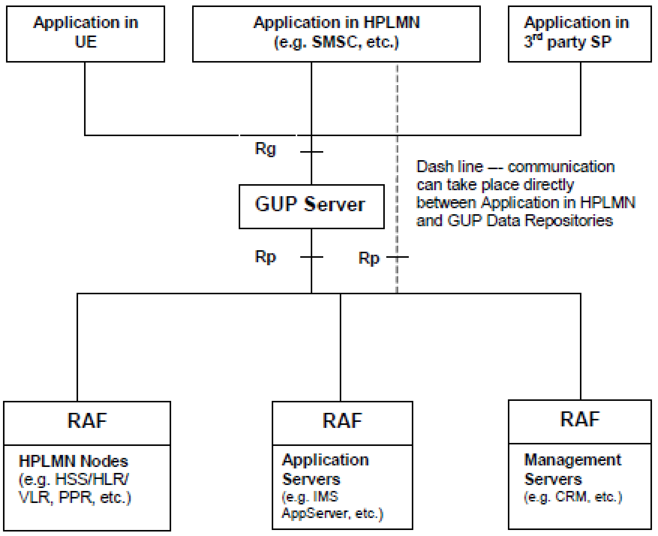

Application in UE
Application in HPLMN (e.g. SMSC, etc.)
Application in 3rd party SP
Rg
GUP Server
Dash line — communication can take place directly between Application in HPLMN and GUP Data Repositories
Rp
Rp
RAF
HPLMN Nodes (e.g. HSS/HLR/VLR, PPR, etc.)
RAF
Application Servers (e.g. IMS AppServer, etc.)
RAF
Management Servers (e.g. CRM, etc.)

Figure 3: Example of the Mapping of GUP Architecture

4.1.4.2 3GPP User Data Convergence

User Data Convergence appears as a means to converge user data profile within the scope of 3GPP subscriber data [i.1], [i.2], and [i.4]. It defines a middleware approach between the actual databases and the Application Front Ends which make use of this data. It defines the protocol to be used for user subscriber data between the UDR, which abstract the data storage, and the Application Front Ends which relate to the consumers and providers of this data.

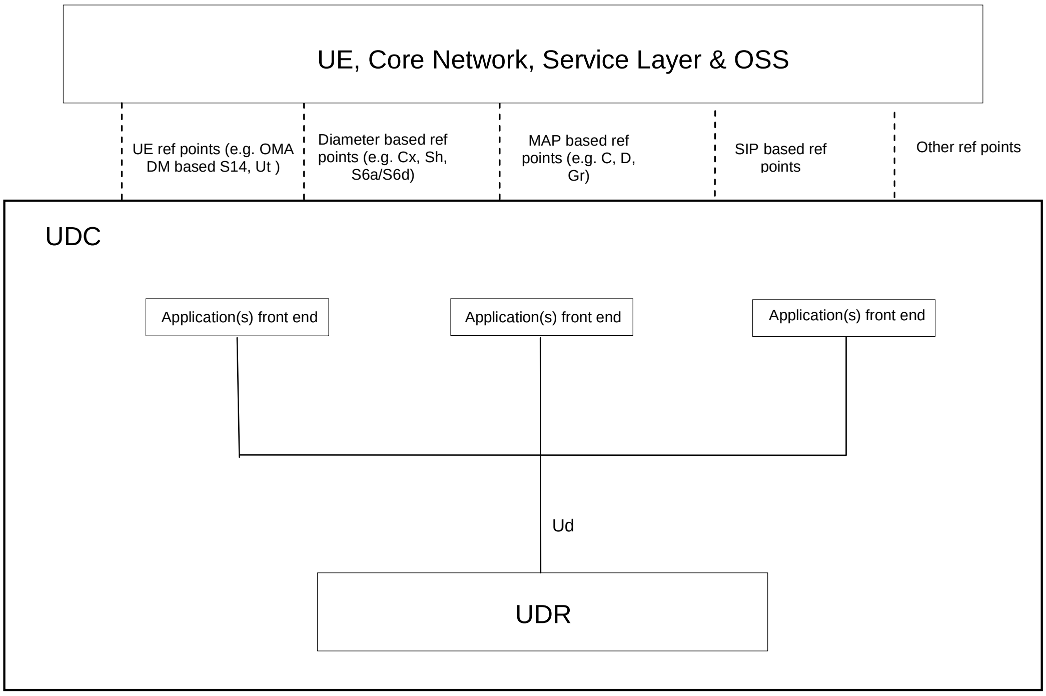

UE, Core Network, Service Layer & OSS
UE ref points (e.g. OMA DM based S14, Ut)
Diameter based ref points (e.g. Cx, Sh, S6a/S6d)
MAP based ref points (e.g. C, D, Gr)
SIP based ref points
Other ref points
UDC
Application(s) front end
Application(s) front end
Application(s) front end
Ud
UDR

Figure 4: UDC reference architecture

4.1.4.2.1 Entities

4.1.4.2.1.1 Application Front End

Application Front Ends (FE) keep the application logic related to the data stored in UDC. The usual operations performed by, for example, an HSS are now performed in an Application Front End with HSS functionality. The data is first retrieved from the UDR and then processed here.

FEs may also provide interfaces to services or applications outside of the UDC scope.

4.1.4.2.1.2 Provisioning Front End

Similar to the previous case, the creation, update or removal of user data and/or subscriptions may also come from outside UDC. In this case, a Provisioning Front End is a kind of FE which can create, delete, modify and retrieve user data.

Provisioning may be associated to an application/implementation and may comprise semantic control specific to this application. It may correspond to different types of provisioning FEs corresponding to different applications logics.

4.1.4.2.1.3 User Data Repository

The User Data Repository (UDR) is a functional entity that acts as a single logical repository of user data and is unique from Application Front End's perspective. Entities which do not store user data and that need to access user data stored in the UDR are collectively known as application front ends.

The UDR functional entity may be distributed over different locations or be centralized; it may support replication mechanisms, back up functions and geographical redundancy to secure the storage of data.

4.1.4.2.2 Message Types

UDC defines 6 message types in an interface usually referred to as *Ud*:

- Querying data from the UDR.
- Creating data within the UDR.
- Deleting data from the UDR.
- Updating data within the UDR.
- Subscription to Notifications.
- Notification of data modification.

4.1.5 OMA GSSM, SUPM, NGSI

The Open Mobile Alliance (OMA) is an international organization, developing technical specifications for global adoption of multimedia data services over the telecommunication network, which was originally targeting the mobile network but has evolved to target the fixed network as well [i.7]. In OMA, there are several activities which are relevant to the distributed user profile managements. Originally, GSSM (General Service Subscription Management) defines an architecture and protocols to accessing user relevant data via GSSM and SUPM (Service User Profile Management) defines data schema which are conveyed over GSSM, while SUPM also defines the protocols to fulfil new requirements. NGSI (Next Generation Service Interface) is offering an application interface for enhanced communication and also considers identity management.

As its name indicates, GSSM more focuses on the aspect of subscription data and provides the functionalities for service subscription handling, service subscription validation and service subscription notification and confirmation [i.8]. As user profile can be considered as part of subscription data, this mechanism can be used for user profile management as well.

SUPM focuses on the data aspects of user profile and provides data model for a converged view [i.9]. SUPM is an ongoing activity and the drafting of the architecture has just started. It may use GSSM as an underlying infrastructure but it may define specific interface for it.

NGSI targets application interfaces to access network capabilities as well as to enhance existing communications including Identity Control as one of the key functionalities [i.10]. NGSI version 1.0 provides specific functionalities to manage the Identifiers and Pseudonyms being used to address a given Identity usually a user in the network operator domain. This identifier could be used to access further information regarding this user. Different identifiers could be used at services or towards other users, the functionality for resolving the identifiers is provided by NGSI and is controlled through policies specified by the user.

While OMA work provides technologies for manipulating user relevant data stored at different places, it is still defined to handle user relevant data inside a single network operator. Other cases are not excluded, but cross domain cases are not explicitly defined.

4.1.6 ETSI STF 342

The Personalization and User Profile Management Standardization Specialist Task Force 342 has produced standards that are necessary for the understanding of the user's preferences to offer an expected user experience. The STF 342 has produced two ETSI deliverables as follows:

- **Deliverable on standardized objects:** ES 202 746 [i.12] is an ETSI Standard (ES) on standardized objects (including settings, values and operations) related to personalization and user profile management, a rule definition language for defining automatic activation of profiles and a common terminology. This deliverable will describe objects related to a range of services and devices with the goal to suit all users' needs including disabled, young and elderly people. The intended readers of this deliverable are service developers and device manufacturers who wish to develop services and devices that can be personalized by their customers, as defined by the user profile management concept described in EG 202 325 [i.11].

- **Architectural framework:** TS 102 747 [i.13] is a Technical Specification (TS) on issues related to networks, terminals and SmartCards. The intended readers of this deliverable are profile providers, telecom companies and device manufacturers who will implement and provide the underlying infrastructure and architecture of network and devices necessary to achieve the user profile management concept described in EG 202 325 [i.11].

4.2 Problem Statement

As described in clause 4.1, there are relevant technologies to exchange the user profiles stored distributed.

OASIS SAML and Liberty DST define the standard mechanism to exchange the information, which are used as underlying technologies of some of the attempts to have standardized mechanism to manage the user profile distributed by 3GPP and OMA. Those mechanisms provide the concepts of single access point. However, the existing attempts are mainly to offer the mechanism to manage user profiles physically distributed but under the domain of one "operator", while accessing parties can be third parties. Those mechanisms may be applicable for the cross domain cases, while the explicit study for allowing the user profile management across different domains.

OpenID Attribute Exchange specifies the mechanism to exchange the data between two parties, i.e. Relying Party and Identity Provider. In that sense, it can be considered as an underlying technology to exchange the data rather than the mechanism for the distributed profile management. Thus in the present document, it is treated as one of the protocols.

Considering the fact that it is a common approach to introduce the Identity Provider as a linking point when multiple entities are involved in providing a service, the use of Identity Provider as anchor point is straight forward approach and should be explicitly stated for the cross domain cases. Involvement of Identity Provider allows the account linking and in many cases, the support of the pseudonyms to protect the user's privacy.

4.3 Potential Network Operator Role

The Identity Provider being used as anchor point must provide trust for both users and application services.

The telecommunication operators already act as Identity Providers, providing authentication functionalities, providing a limited set of attribute data of their subscribers and are suitable for act as an anchor point for the management of distributed user profile information.

Note that the required functionality of Identity Provider for this purpose is the brokering of Identity and Identity Provider may not necessarily include the functionality as a provider of identity.

5 Use Cases

5.1 My personal profile service

5.1.1 Short Description

"My personal profile service" provides users with a portal to administrate their personal data via Identity Broker. The actual data may be stored at multiple sites of different services, to which users have subscription.

Andrew, one of the subscribers of this service plans a business trip for half a year and he decides to update his address for the shipment. While his address is registered to the multiple places, he can updates this information by accessing to the "my personal profile service" portal once.

5.1.2 Actors

- Andrew, a user of "My personal profile service".
- Service Providers where Andrew has subscriptions.
- Network operator offering "My personal profile service", consisting of Portal, Identity Broker service and Identity Provider service (with attribute provider functionality) as option.

5.1.2.1 Actor Specific Issues

- Andrew:
  - Wants to easily manage and control his own personal data across multiple services.
- Service Providers:
  - Store the data about their subscribers.
  - Want to have updated user data about their subscribers.
- Network operator (as My personal portal service provider):
  - Provides authentication and authorization (Identity Broker) functions.
  - Acts as Identity Provider for Identity Federation.
  - Provides a single contact point to access to the distributed data of the user.
  - Provides a portal for the user to administer (CRUD) his own data.

5.1.2.2 Actor Specific Benefits

- Andrew:
  - Easily manages his own personal data across the services with control (no need to type, re-type).
- Service Providers:
  - Easily get the updates about the profiles of their subscribers.
  - Can rely on the strong authentication mechanism provided by the network operator.
  - Have access to the profile information which they do not have by themselves.
- Network operator (as My personal portal service provider):
  - Establishes agreements with service providers, as Identity Brokers offering authentication and brokering functionality to increase its revenues and enrich services portfolio.
  - Offers users a generic easy way to manage their profile information across different service providers to reduce the churn rate.

5.1.3 Pre-conditions

- IdentityBroker and service providers are in the same Circle of Trust.
- Andrew agrees that his Identity can be federated among service providers within the Circle of Trust.
- Andrew is authenticated to the "My personal profile service" portal via the Identity Broker.
- Andrew plans to update his address for the upcoming travel.

5.1.4 Post-conditions

- Andrew has his location (delivery address) at the hotel he is staying, as an address information for the service providers of his choose.

5.1.5 Normal Flow

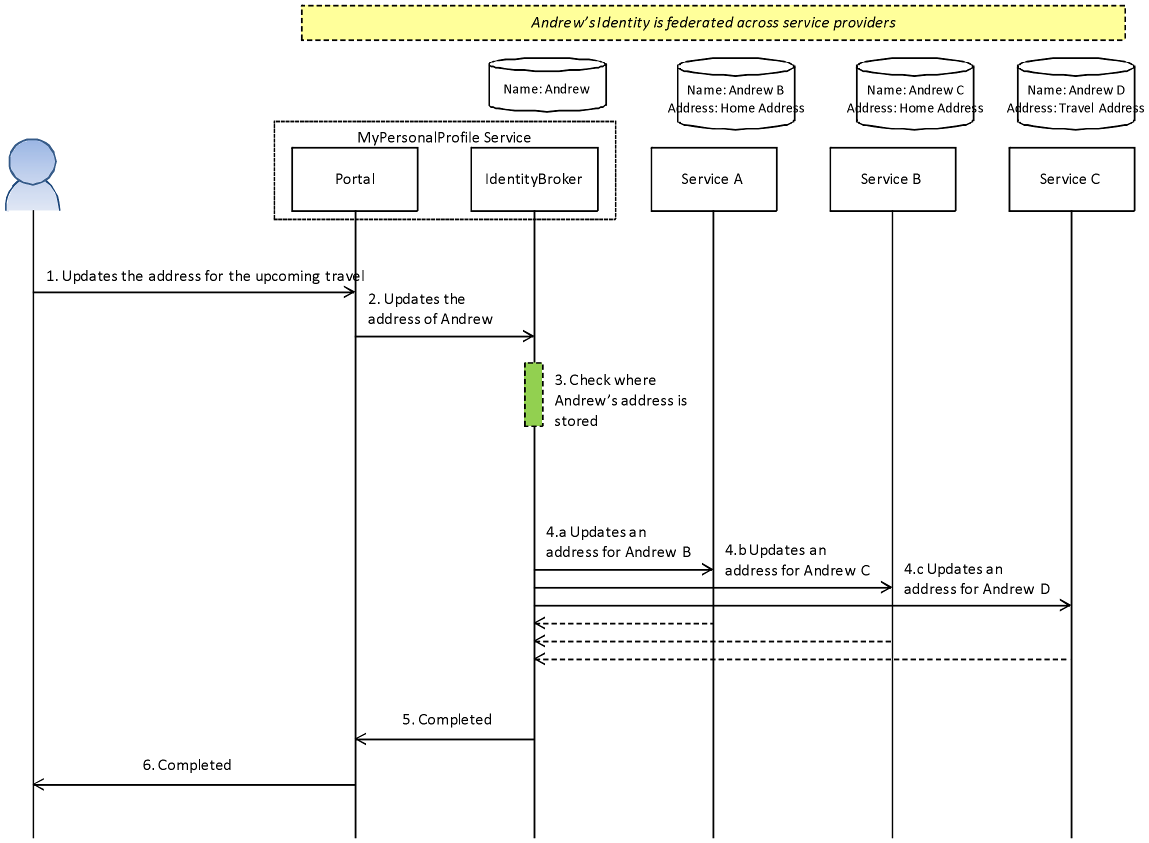

Andrew's Identity is federated across service providers
Name: Andrew
Name: Andrew B
Address: Home Address
Name: Andrew C
Address: Home Address
Name: Andrew D
Address: Travel Address
MyPersonalProfile Service
Portal
IdentityBroker
Service A
Service B
Service C
1. Updates the address for the upcoming travel
2. Updates the address of Andrew
3. Check where Andrew's address is stored
4.a Updates an address for Andrew B
4.b Updates an address for Andrew C
4.c Updates an address for Andrew D
5. Completed
6. Completed

Figure 5: Profile updates via "My personal profile" (Normal Flow)

1) Andrew accesses to the portal of "My personal profile" and requests for the updates to his address.

2) The portal sends the update request to the Identity Broker.

3) Identity Broker checks its repository where Andrew's address is stored.

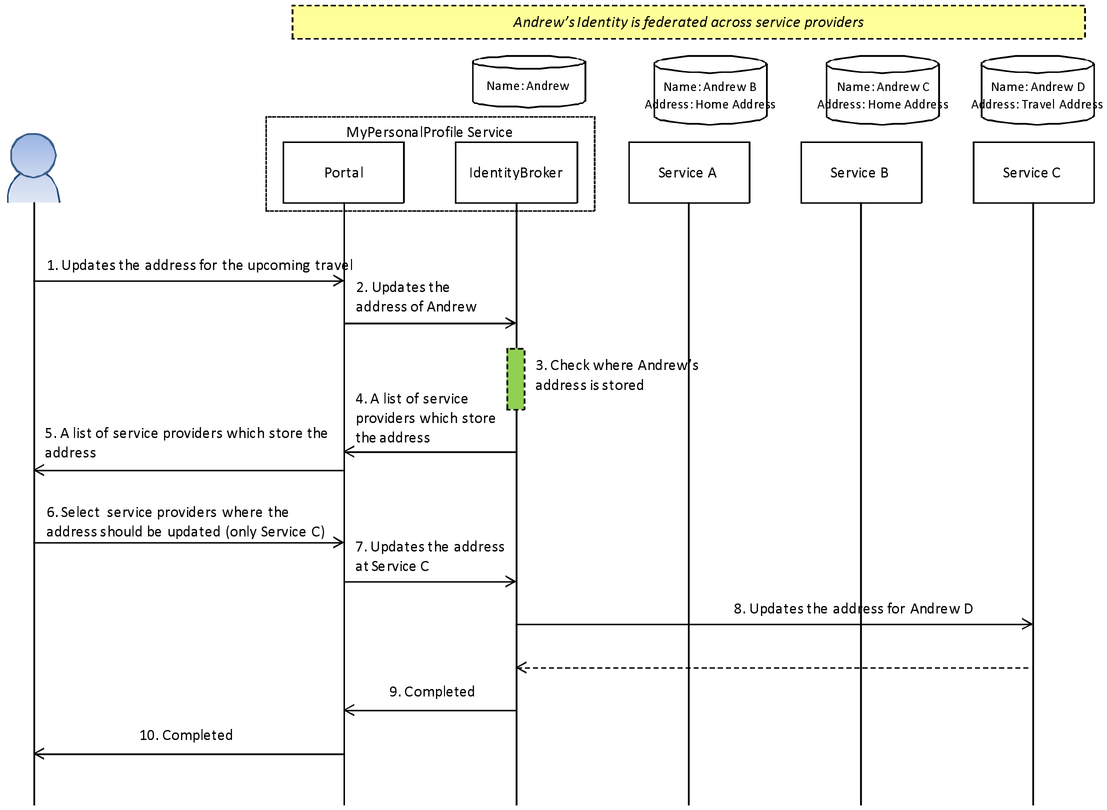
4) Identity Broker sends the update requests to multiple service providers where Andrew's address is stored. Note that Andrew is known by different name at different service providers and Identity Broker use the name which is also used for the Identity Federation.

5) Identity Broker sends back the response indicating the completion of the procedure.

6) The portal shows the updated information to Andrew.

Instead of proxying the requests (or handling them by itself) the Identity Broker may direct Andrew to service provider where his address information is stored (redirect mode of operation).

5.1.6 Alternative Flow 1: Updates the data with selected services



Andrew's Identity is federated across service providers
Name: Andrew
Name: Andrew B
Address: Home Address
Name: Andrew C
Address: Home Address
Name: Andrew D
Address: Travel Address
MyPersonalProfile Service
Portal
IdentityBroker
Service A
Service B
Service C
1. Updates the address for the upcoming travel
2. Updates the address of Andrew
3. Check where Andrew's address is stored
4. A list of service providers which store the address
5. A list of service providers which store the address
6. Select service providers where the address should be updated (only Service C)
7. Updates the address at Service C
8. Updates the address for Andrew D
9. Completed
10. Completed

Figure 6: Profile updates via "My personal profile" with selected services (Alternative Flow)

1-3) (Same as step 1-3 of Normal Flow.)

4) IdentityBroker send back a list of services where Andrew's address is stored.

5) Portal asks Andrew to choose services for which he likes to update his address.

6) Andrew chooses a service (Service C), from which he likes to have goods delivered at the hotel during his stay.

7) The portal requests IdentityBroker to update Andrew's address at Service C.

8) Identity Broker sends the update requests to Service C where Andrew is known as Andrew D.

9-10) (Same as step 5-6 of Normal Flow.)

5.1.7 Alternative Flow 2: MyPersonal Portal Service with Identity Provider storing data

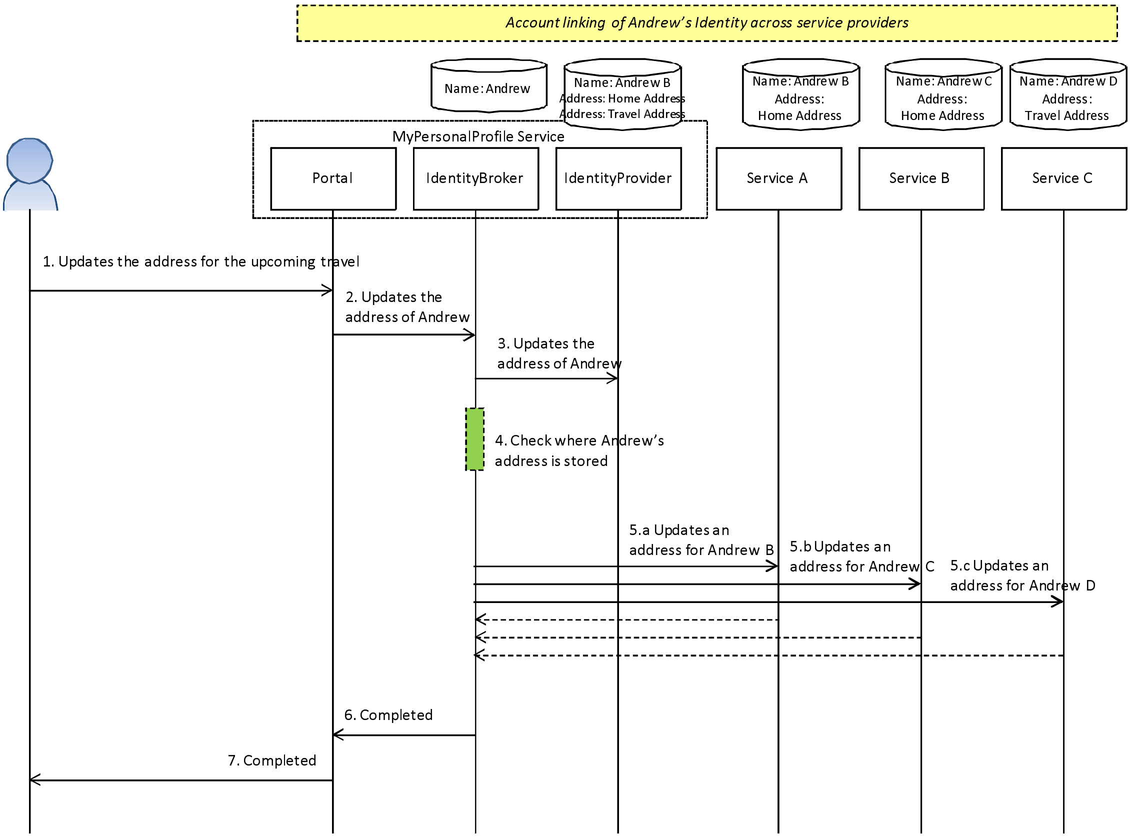

Account linking of Andrew's Identity across service providers
Name: Andrew
Name: Andrew B
Address: Home Address
Address: Travel Address
Name: Andrew B
Address:
Home Address
Name: Andrew C
Address:
Home Address
Name: Andrew D
Address:
Travel Address
MyPersonalProfile Service
Portal
IdentityBroker
IdentityProvider
Service A
Service B
Service C
1. Updates the address for the upcoming travel
2. Updates the address of Andrew
3. Updates the address of Andrew
4. Check where Andrew's address is stored
5.a Updates an address for Andrew B
5.b Updates an address for Andrew C
5.c Updates an address for Andrew D
6. Completed
7. Completed

Figure 7: Profile updates via "My personal profile" with selected services (Alternative Flow)

1-3) (Same as step 1-3 of Normal Flow.)

4) Identity Broker sends update request to the Identity Provider where all the data is stored.

5-7) (Same as step 4-6 of Normal Flow.)

5.2 Use Case 2: Web Shop usage without subscription

5.2.1 Short Description

During his trip, Andrew finds a local video shop site which provides a good selection. He decides to use this site without creating any account with them.

5.2.2 Actors

- Andrew, a user of "My personal profile service".
- LocalVideoShop, which offers video delivery service for the local area where Andrew is staying during his trip.
- Service Providers where Andrew has subscriptions.
- Network operator offering "My personal profile service".

5.2.2.1 Actor Specific Issues

- Andrew:
  - Wants to receive the service from LocalVideoShop but he does not want to create a new account.
  - Wants to easily manages and controls his personal data across multiple services.
- LocalVideoShop:
  - Wants to offer their services to the tourists as well (non-membership basis).
  - Wants to have a minimum profile information necessary to serve the user.
- Service Providers:
  - Stores the data about its subscribers.
  - Provides the user data about their subscribers.
- Network operator (as My personal portal service provider):
  - Provides authentication and authorization (Identity Broker).
  - Acts as Identity Provider for Identity Federation.
  - Provides a single contact point to the distributed data of the user.

5.2.2.2 Actor Specific Benefits

- Andrew:
  - Can use the personalized services without revealing too much information.
  - Can use the personalized services without having an account.
  - Easily manages his own personal data across the services with control (no need to type, re-type).
- LocalVideoShop:
  - Can access the profile information via Identity Broker.
- Service Providers:
  - Can rely on the strong authentication mechanism provided by the network operator.
- Network operator (as Identity Broker):
  - Establishes agreements with service providers, as Identity Brokers offering authentication and brokering functionality to increase its revenues and enrich services portfolio.
  - Attracts users (and keeps them as customers) by offers users a generic easy way of manage their profile information across different service providers (reduction of the churn rate).

5.2.3 Pre-conditions

- IdentityBroker and service providers are in the same Circle of Trust.
- Andrew agrees that his identity can be federated among service providers in this Circle of Trust.
- Andrew is authenticated with Identity Broker.
- Andrew wants to buy a video during the trip.

5.2.4 Post-conditions

- Andrew has purchased a video at LocalVideoShop, which will be delivered to his hotel address.
- Andrew does not have his account at LocalVideoShop.

5.2.5 Normal Flow

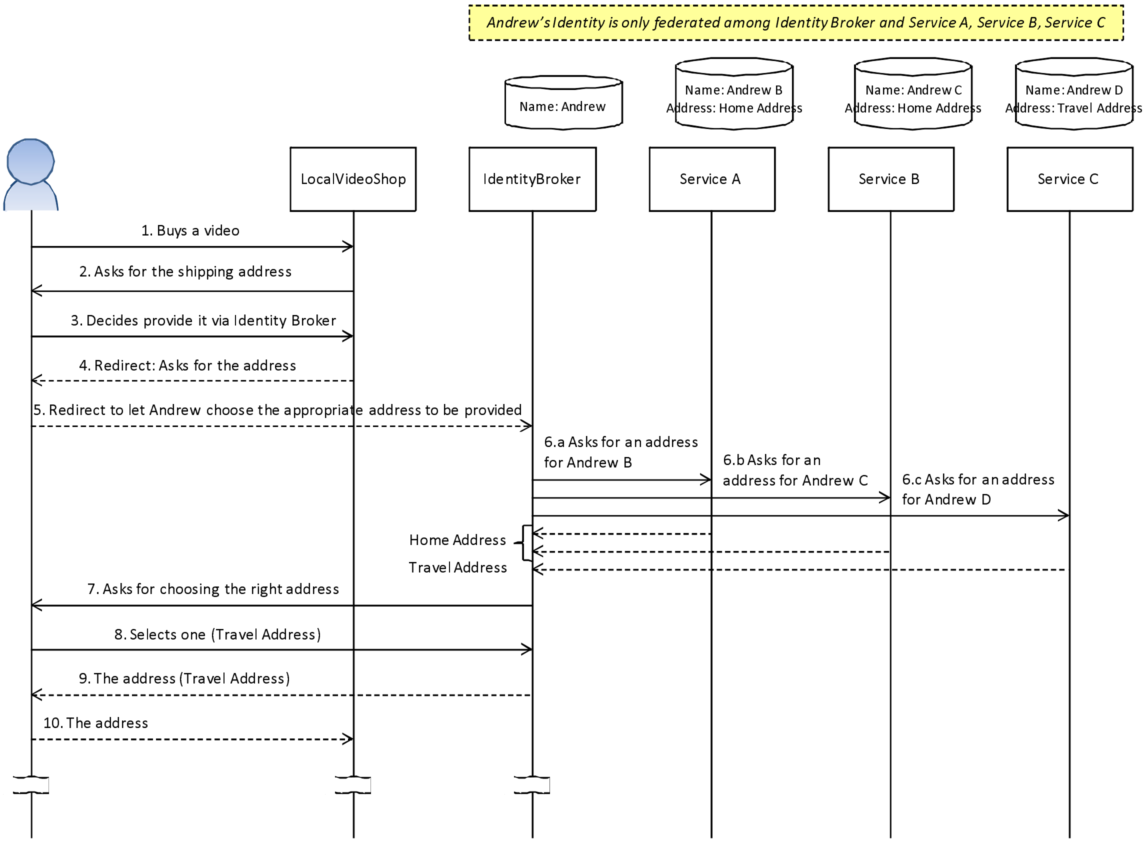

Andrew's Identity is only federated among Identity Broker and Service A, Service B, Service C
Name: Andrew
Name: Andrew B
Address: Home Address
Name: Andrew C
Address: Home Address
Name: Andrew D
Address: Travel Address
LocalVideoShop
IdentityBroker
Service A
Service B
Service C
1. Buys a video
2. Asks for the shipping address
3. Decides provide it via Identity Broker
4. Redirect: Asks for the address
5. Redirect to let Andrew choose the appropriate address to be provided
6.a Asks for an address for Andrew B
6.b Asks for an address for Andrew C
6.c Asks for an address for Andrew D
Home Address
Travel Address
7. Asks for choosing the right address
8. Selects one (Travel Address)
9. The address (Travel Address)
10. The address

Figure 8: Video Purchase (Normal Flow)

1) Andrew accesses to the portal of "LocalVideoShop" and decides to purchase a video.

2) "LocalVideoShop" asks for the shipping address with the option of direct input or via the Identity Broker.

3) Andrew decides the Identity Broker option and provide the information of his Identity Broker.

4-5) Andrew is redirected to the Identity Broker.

6) Identity Broker sends the requests to multiple service providers where Andrew's address is stored. Note that Andrew is known by different name at different service providers and Identity Broker use the name which is also used for the Identity Federation.

7) IdentityBroker asks Andrew which address should be provided to "LocalVideoShop".

8) Andrew chooses his temporary address during his trip (provided by Service C).

9-10) The address is redirected back to the "LocalVideoShop".

Any purchase procedure continues.

5.2.6 Alternative Flow 1: Video Purchase with Federation

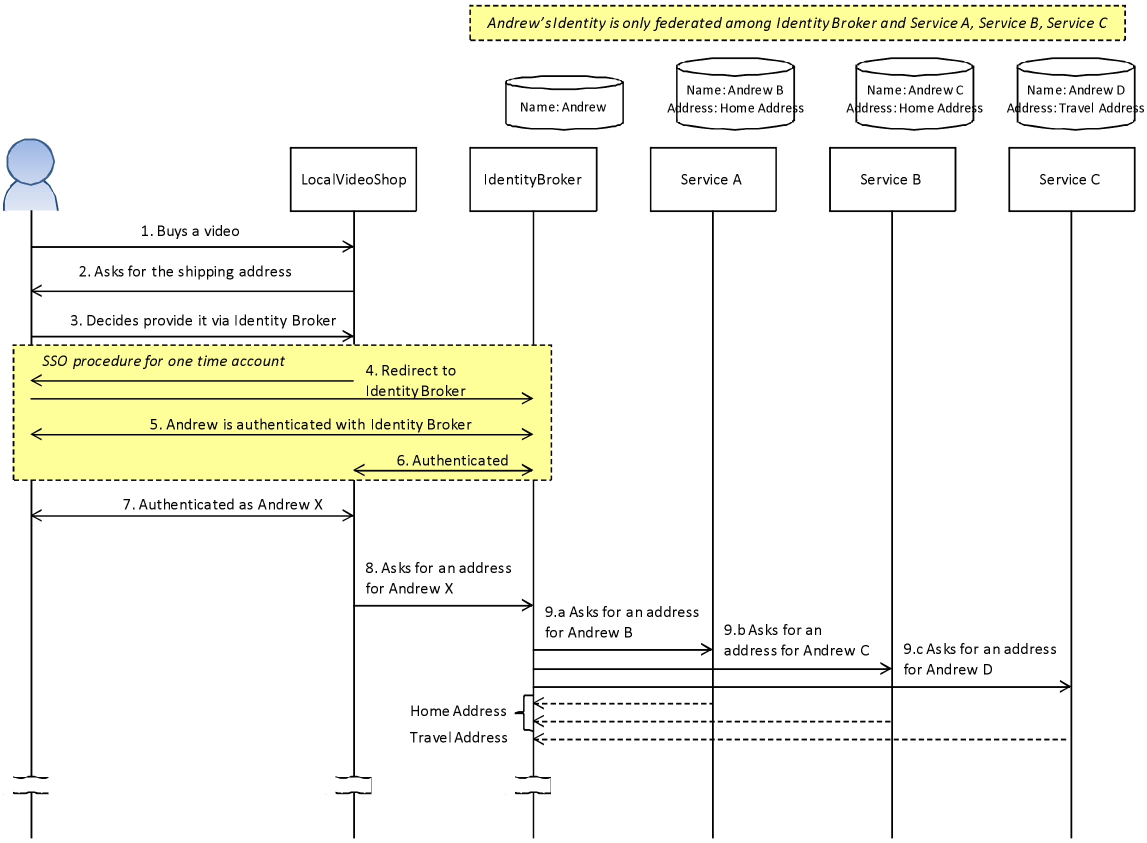

Andrew's Identity is only federated among Identity Broker and Service A, Service B, Service C
Name: Andrew
Name: Andrew B
Address: Home Address
Name: Andrew C
Address: Home Address
Name: Andrew D
Address: Travel Address
LocalVideoShop
IdentityBroker
Service A
Service B
Service C
1. Buys a video
2. Asks for the shipping address
3. Decides provide it via Identity Broker
SSO procedure for one time account
4. Redirect to Identity Broker
5. Andrew is authenticated with Identity Broker
6. Authenticated
7. Authenticated as Andrew X
8. Asks for an address for Andrew X
9.a Asks for an address for Andrew B
9.b Asks for an address for Andrew C
9.c Asks for an address for Andrew D
Home Address
Travel Address

Figure 9: Video Purchase with one time Federation (Alternative Flow)

1-2) (Same as step 1-2 of Normal Flow.)

3) Andrew chooses to perform one time Federation and indicate his Identity Broker.

4) Andrew is redirected to the Identity Broker.

5) Andrew is authenticated with Identity Broker.

6) Andrew's identity is federated between LocalVideoShop and Identity Broker.

7) Andrew is authenticated as Andrew X to LocalVideoShop via Identity Broker.

8) LocalVideoShop asks Identity Broker for Andrew's address.

9) Identity Broker sends the queries to multiple service providers where Andrew's address is stored. Note that Andrew is known by different name at different service providers and Identity Broker use the name which is also used for the Identity Federation.

LocalVideoShop will be informed by the Identity Broker about the valid Andrew's address. A selection of the right address can be done between Andrew and Identity Broker before LocalVideoShop is informed, or can be done via LocalVideoShop. See also the Use Case 2-b.

5.3 Use Case 2-b: Web Shop usage with subscription

5.3.1 Short Description

WorldVideoShop offers the video delivery services over the world with the collaboration with local video shops. Andrew has subscriptions to the service, but instead of having his address at the site, he uses Distribute User Profile Management offered by Identity Broker.

5.3.2 Actors

- Andrew, a user of "WorldVideoShop" and Identity Broker service.
- WorldVideoShop, which offers video delivery services across the world with collaboration with the local video shops.
- Service Providers where Andrew has subscriptions.
- Network operator offering "Identity Broker".

5.3.2.1 Actor Specific Issues

- Andrew:
  - Wants to receive the service from WorldVideoShop but he does not store too much information about him at the site.
  - Easily manages and controls his personal data across multiple services.
- WorldVideoShop, Service Providers:
  - Stores the data about its subscribers.
  - Wants to have the access to the updated information about their subscribers to offer users with personalized services. The information is not necessarily to be stored at its own site.
- Network operator (as My personal portal service provider):
  - Provides authentication and authorization (Identity Broker) functions.
  - Acts as Identity Provider for Identity Federation.
  - Provides a single contact point to access to the distributed user data.

5.3.2.2 Actor Specific Benefits

- Andrew:
  - Can use the personalized services without revealing too much information.
  - Can easily manage his own personal data across the services with control (no need to type, re-type).
- WorldVideoShop, Service Providers:
  - Have access to the profile information which they do not store and manage by themselves.
  - Easily get the updates about the profile of their subscribers.
  - Can rely on the strong authentication mechanism provided by the network operator.
- Network operator (as Identity Broker):
  - Establishes agreements with service providers, as Identity Broker offering authentication and brokering functionality to increase its revenues and enrich services portfolio.
  - Attracts users (and keeps them as customers) by offers users a generic easy way of manage their profile information across different service providers (reduction of the churn rate).

5.3.3 Pre-conditions

- IdentityBroker and service providers are in the same Circle of Trust.
- Andrew agrees that his identities can be federated among service providers in this Circle of Trust.

- Andrew is authenticated to the WorldVideoShop via Identity Broker.
- Andrew wants to buy a video during the trip.

5.3.4 Post-conditions

- Andrew has purchased a video at WorldVideoShop, which will be delivered to his hotel address.
- Andrew's address information is not stored at WorldVideoShop.

5.3.5 Normal Flow

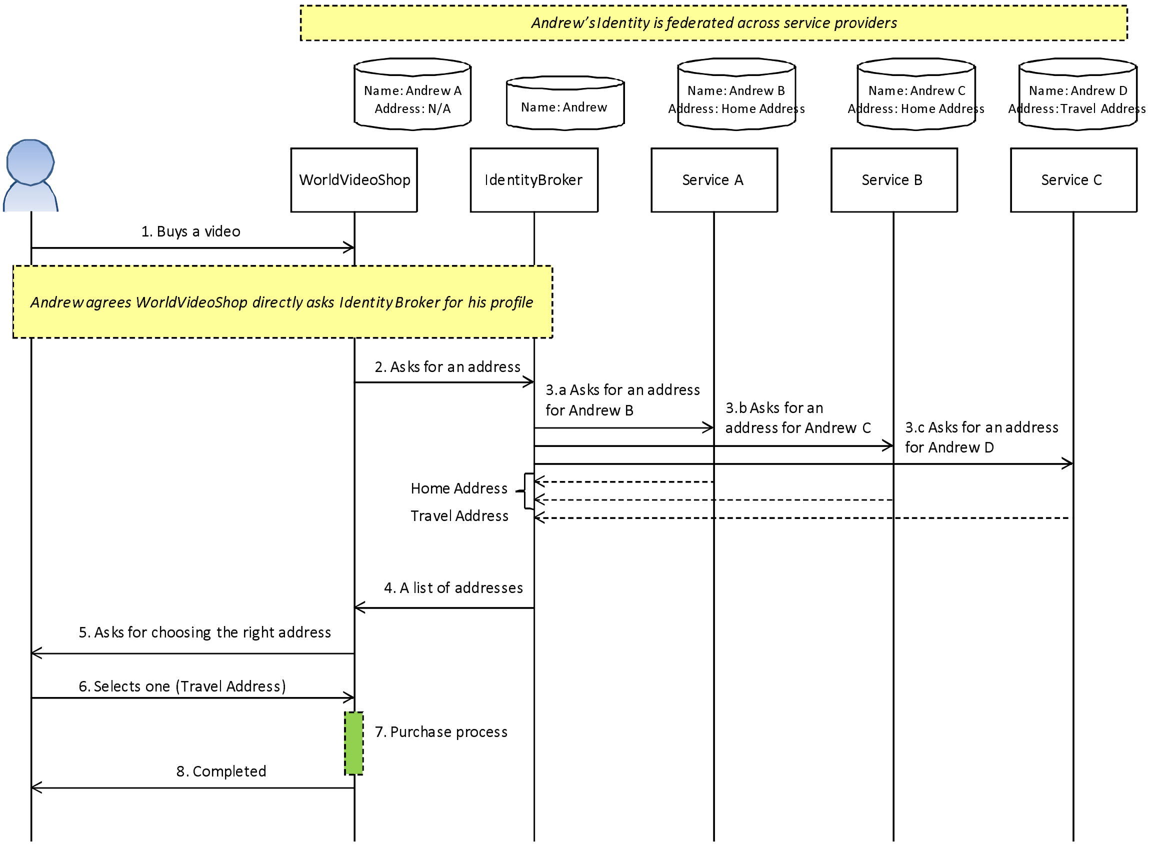


Figure 10: Video Purchase (Normal Flow)

1) Andrew accesses to the portal of "WorldVideoShop" and decides to purchase a video.

2) "WorldVideoShop" asks the Identity Broker for Andrew's address.

3) Identity Broker sends the queries to multiple service providers where Andrew's address might be stored. Note that Andrew is known by different name at different service providers and Identity Broker use the name which is also used for the Identity Federation.

4) Identity Broker sends back a list of Andrew's addresses to the "WorldVideoShop".

5) "WorldVideoShop" asks Andrew which address should be used.

6) Andrew chooses his temporary address during the trip (provided by Service C).

7) "WorldVideoShop" processes the purchase request (there might be further interaction between different actors).

8) "WorldVideoShop" informs Andrew about the completion of his purchase.

5.3.6 Alternative Flow 1: Video Purchase with User's interruption

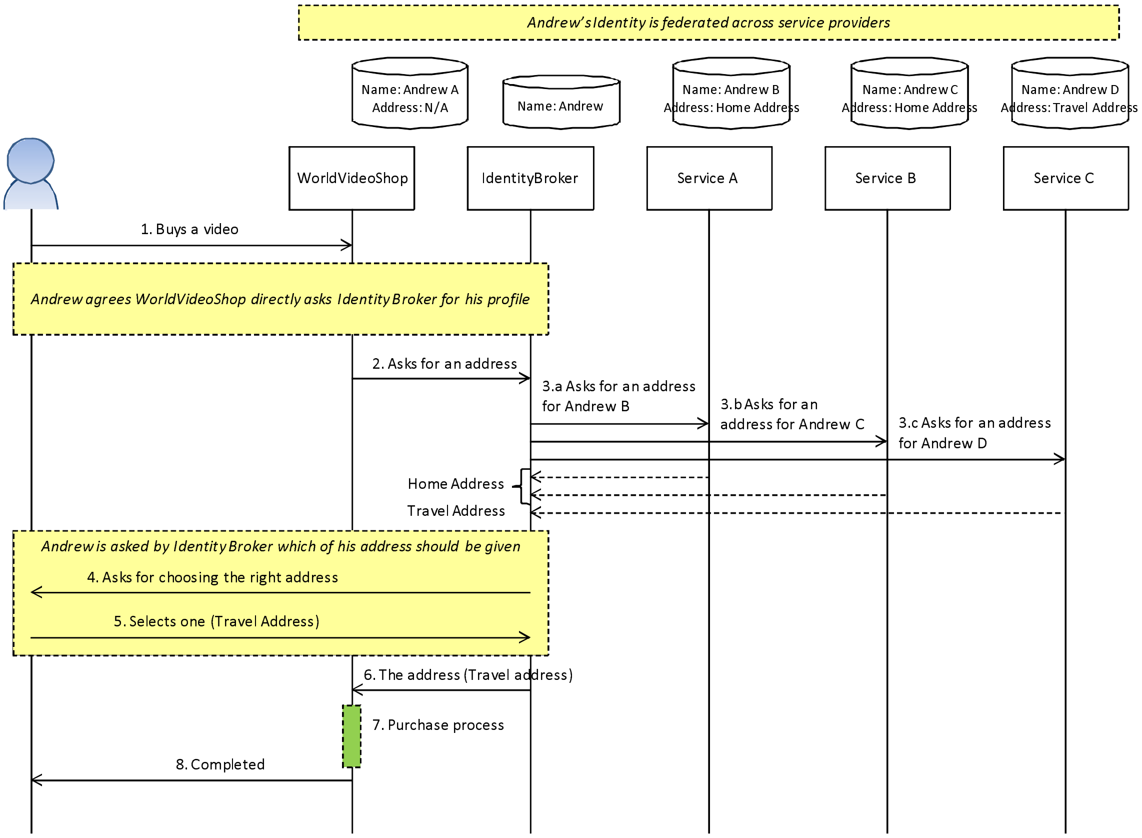

Andrew's Identity is federated across service providers
Name: Andrew A
Address: N/A
Name: Andrew
Name: Andrew B
Address: Home Address
Name: Andrew C
Address: Home Address
Name: Andrew D
Address: Travel Address
WorldVideoShop
IdentityBroker
Service A
Service B
Service C
1. Buys a video
Andrew agrees WorldVideoShop directly asks Identity Broker for his profile
2. Asks for an address
3.a Asks for an address for Andrew B
3.b Asks for an address for Andrew C
3.c Asks for an address for Andrew D
Home Address
Travel Address
Andrew is asked by Identity Broker which of his address should be given
4. Asks for choosing the right address
5. Selects one (Travel Address)
6. The address (Travel address)
7. Purchase process
8. Completed

Figure 11: Video Purchase with user's interruption on the address selection (Alternative Flow)

1-3) (Same as step 1-3 of Normal Flow.)

4) IdentityBroker asks Andrew which address should be provided to "WorldVideoShop".

5) Andrew chooses his temporary address during his trip (provided by Service C).

6) Identity Broker provides the address to the "WorldVideoShop".

7-8) (Same as step 7-8 of Normal Flow.)

5.4 Profile updates from individual services

5.4.1 Short Description

Andrew decides to update his address at the WorldVideoShop, one of the services he has a subscription to, for his upcoming half-year trip. With the Distributed User Profile Management service provided by the Identity Broker, he can eventually updates the address stored at other services.

5.4.2 Actors

- Andrew, a user of "My personal profile service".
- WorldVideoShop, which offers video delivery services across the world in collaboration with the local video shops.
- Service Providers where Andrew has subscriptions.
- Network operator offering "My personal profile service".

5.4.2.1 Actor Specific Issues

- Andrew:
    - Wants to receive the service he is subscribing to during his trip.
    - Easily manages and controls his personal data across the services.
- WorldVideoShop, Service Providers:
    - Stores the data about their subscribers.
    - Wants to have the access to the updated information about their subscribers to offer users with personalized services. The information is not necessarily to be stored at its own site.
- Network operator (as Identity Broker):
    - Provides authentication and authorization functions.
    - Acts as Identity Provider for Identity Federation.
    - Provides a single contact point to access to the distributed user data.

5.4.2.2 Actor Specific Benefits

- Andrew:
    - Easily manages his own personal data across the services with control (no need to type, re-type).
- WorldVideoShop, Service Providers:
    - Easily get the updates about the profile of its subscribers.
    - Can rely on the strong authentication mechanism provided by the network operator.
    - Have access to the profile information which they do not have by themselves.
- Network operator (as My personal portal service provider):
    - Establishes agreements with service providers, as Identity Brokers offering authentication and brokering functionality to increase its revenues and enrich services portfolio.
    - Attracts users (and keeps them as customers) by offers users a generic easy way of manage their profile information across different service providers (reduction of the churn rate).

5.4.3 Pre-conditions

- IdentityBroker and service providers are in the same Circle of Trust.
- Andrew agrees that his identities can be federated among service providers in this Circle of Trust.
- Andrew is authenticated to the WorldVideoShop via Identity Broker.

- Andrew wants to buy a video during the trip.

5.4.4 Post-conditions

- Andrew has purchases the video at WorldVideoShop and his address at the service has been updated to travel address.
- Andrew has his location (delivery address) at the hotel he is staying, as an address information for the selected service providers (varies across scenario).

5.4.5 Normal Flow

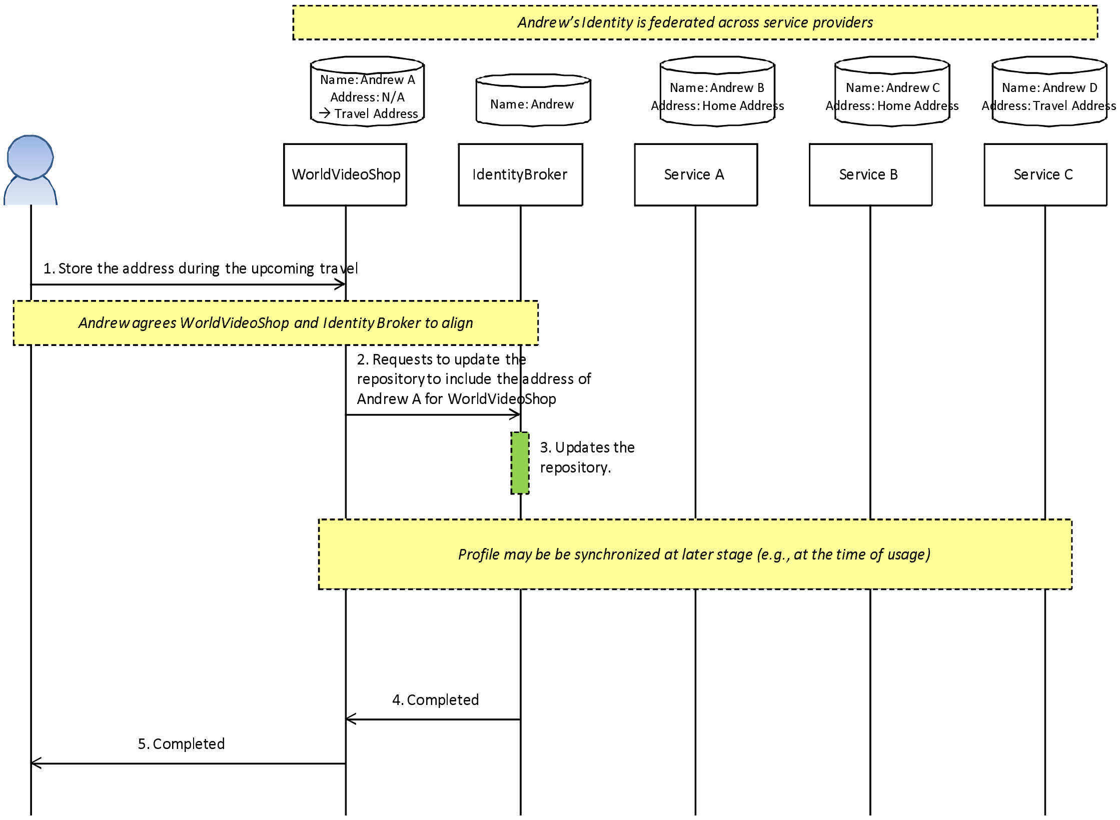

Andrew's Identity is federated across service providers
Name: Andrew A
Address: N/A
→ Travel Address
Name: Andrew
Name: Andrew B
Address: Home Address
Name: Andrew C
Address: Home Address
Name: Andrew D
Address: Travel Address
WorldVideoShop
IdentityBroker
Service A
Service B
Service C
1. Store the address during the upcoming travel
Andrew agrees WorldVideoShop and Identity Broker to align
2. Requests to update the repository to include the address of Andrew A for WorldVideoShop
3. Updates the repository.
Profile may be be synchronized at later stage (e.g., at the time of usage)
4. Completed
5. Completed

Figure 12: Profile updates via "My personal profile" (Normal Flow)

1) Andrew accesses to the portal of "WorldVideoShop" and registers his hotel address as a shipment address.

2) "WorldVideoShop" informs the Identity Broker about the updates of Andrew's address at their site. Note that Andrew is known as Andrew A at WorldVideoShop.

3) Identity Broker updates its repository.

4) Identity Broker sends back the response indicating the completion of the procedure.

5) The portal shows the updated information to Andrew.

5.4.6 Alternative Flow 1: Updates the data according to the pre-define rules

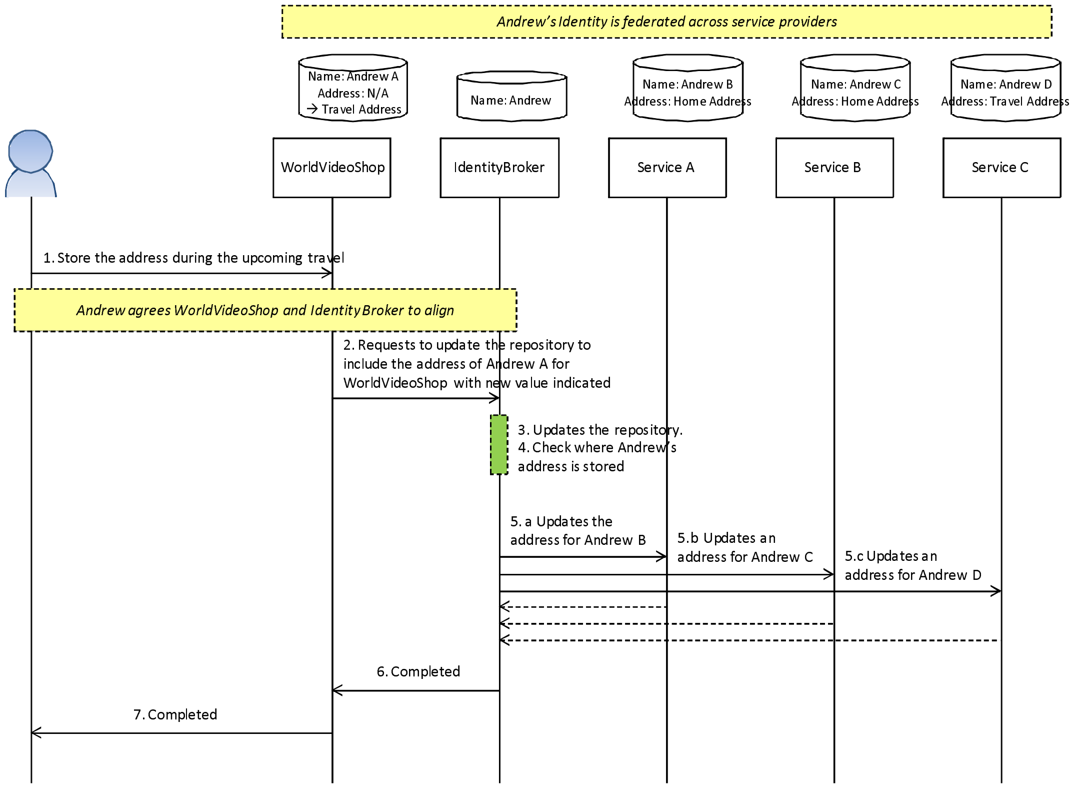

Andrew’s Identity is federated across service providers
Name: Andrew A
Address: N/A
→ Travel Address
Name: Andrew
Name: Andrew B
Address: Home Address
Name: Andrew C
Address: Home Address
Name: Andrew D
Address: Travel Address
WorldVideoShop
IdentityBroker
Service A
Service B
Service C
1. Store the address during the upcoming travel
Andrew agrees WorldVideoShop and Identity Broker to align
2. Requests to update the repository to include the address of Andrew A for WorldVideoShop with new value indicated
3. Updates the repository.
4. Check where Andrew's address is stored
5. a Updates the address for Andrew B
5.b Updates an address for Andrew C
5.c Updates an address for Andrew D
6. Completed
7. Completed

Figure 13: Profile updates via "WorldVideoShop" with services selected by Identity Broker (Alternative Flow)

1-3) (Same as step 1-3 of Normal Flow.)

4) IdentityBroker checks its repository where Andrew's address is stored.

5) Identity Broker sends the update requests to the multiple service providers which were resolved in the step 4 as service providers where Andrew's address are stored. Note that Andrew is known by different name at different service providers and Identity Broker use the name which is also used for the Identity Federation.

6-7) (Same as step 4-5 of Normal Flow.)

NOTE: In this example, the pre-defined rule is to update all, while any selection can be done by Identity Broker.

5.4.7 Alternative Flow 2: Updates the data with User's interruption

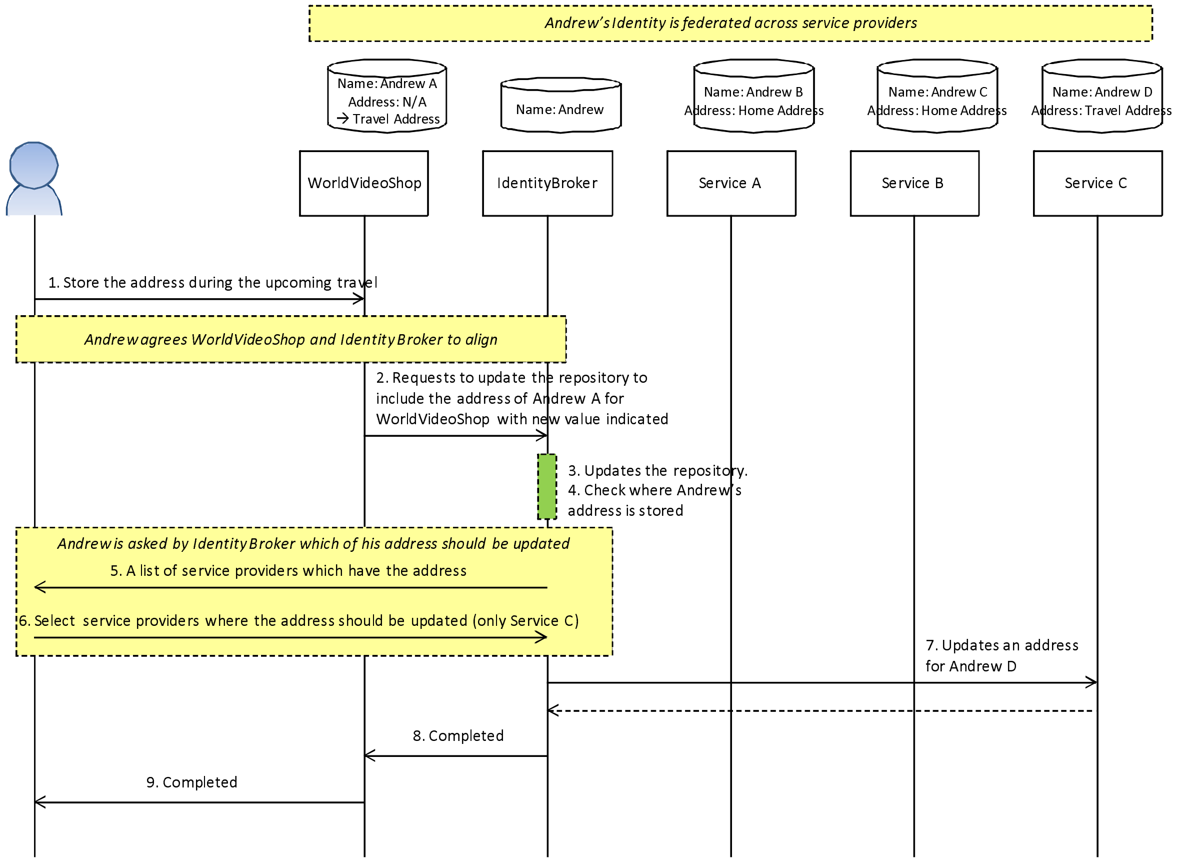

Andrew's Identity is federated across service providers
Name: Andrew A
Address: N/A
→ Travel Address
Name: Andrew
Name: Andrew B
Address: Home Address
Name: Andrew C
Address: Home Address
Name: Andrew D
Address: Travel Address
WorldVideoShop
IdentityBroker
Service A
Service B
Service C
1. Store the address during the upcoming travel
Andrew agrees WorldVideoShop and Identity Broker to align
2. Requests to update the repository to include the address of Andrew A for WorldVideoShop with new value indicated
3. Updates the repository.
4. Check where Andrew's address is stored
Andrew is asked by Identity Broker which of his address should be updated
5. A list of service providers which have the address
6. Select service providers where the address should be updated (only Service C)
7. Updates an address for Andrew D
8. Completed
9. Completed

Figure 14: Profile updates via "WorldVideoShop" with services selected by user (Alternative Flow 2)

1-3) (Same as step 1-3 of Normal Flow.)

4) (Same as step 4 of Alternative Flow 1.)

5) Identity Bro asks Andrew to choose services for which he likes to update his address.

6) Andrew chooses a service (Service C), from which he likes to have goods delivered at the hotel during his stay.

7) Identity Broker sends the update requests to Service C where Andrew is known as Andrew D.

8-9) (Same as step 4-5 of Normal Flow.)

5.5 User identity attribute sharing between operator/ISP and web enterprise

5.5.1 Description

User requests e.g. a video-on-demand (VOD) provided by a web enterprise over the Internet. He changes his default screen resolution and likes this value to be used across different web enterprise applications. For this the attribute has to be stored at the identity provider, to be further used by other Web providers.

5.5.2 Actors

- User.

- Operator/ISP (Identity Provider).
- Web enterprise (Service Provider) offering a VOD service.

5.5.2.1 Actors specific Issues

- User:
  - Wants to have his default values automatically used by different web enterprise services.
- Operator:
  - Provides service of Identity Provider
- Web Enterprise:
  - Provides a service to users.
  - Utilizes different attributes to customize service.

5.5.2.2 Actors specific benefits

- User:
  - Needs to do customization only once.
- Operator:
  - Provides service of attribute sharing to different web enterprises.
  - Is trusted partner of web enterprise.
- Web Enterprise:
  - Can personalize a service according to the needs of user, regardless if first time at service or frequent user.

5.5.3 Pre-Condition

- The operator/ISP has stored User identity attributes such as "screen resolution" (of the User's display on which the User wants to watch the VOD) and "available bandwidth" (a value that characterizes the bandwidth available to the User).
- The User wants the operator/ISP to act as IdP on behalf of the User.

5.5.4 Post-Condition

- The attributes of a user are stored at Identity Provider by web enterprise.

5.5.5 Normative Flow

1) The User requests a video-on-demand (VOD) provided by a web enterprise (Service Provider) over the Internet.

2) The web enterprise asks the operator/ISP for User identity attributes such as "screen resolution" and "available bandwidth".

3) The operator/ISP sends the values of the requested User identity attributes to the web enterprise.

4) The user performs some changes to his user profile, e.g. update of phone number, or change in layout.

5) The Service Provider pushes a new value of the attribute to the Telco Identity Provider.

6) The Telco Identity Provider stores the new value, which can be further accessed by other service providers.

NOTE: There are a lot of variations of this use case if you replace the attributes "screen resolution" and "available bandwidth" by, e.g. "bank account number", "credit card number", or "email address".

6 Requirements

6.1 User

- The user shall be able to control his own profile data easily, including the selection and control of which type or which amount of profile information to disclose as well how they should be handled (DGS-INS-002). [Requirements from Use Case 1, 2, 3].
- The user shall be able to allow the services to be customised using his profile [Requirements from Use Case 2, 3].
- The user shall be able to transfer his own profile data stored at one site to another site to receive the service. [Requirements from Use Case 2, 3].

6.2 Service Provider

- The service provider shall be able to authenticate the user. [Precondition for Use Case 2, 3].
- The service provider shall support the account linking. [Precondition for Use Case 1, 2, 3].

6.2.1 As provider of user profile

- The service provider shall be able to allow the indirect updates of the user profile data (via Management portal or triggered by the updates of same information at other sites). [Requirements from Use Case 1, 3].
- The service provider shall provide user profile data to other service providers on behalf of the user. [Requirements from Use Case 2].

6.2.2 As consumer of user profile

- The service provider shall be able to retrieve the user profile data stored at other service providers on behalf of the user. [Requirements from Use Case 2].

6.3 Identity Broker

- Identity Broker shall be able to authenticate the user. [Precondition for Use Case 1, 2, 3].
- Identity Broker shall support account linking under different identifier of the user. [Precondition for Use Case 1, 2, 3].
- Identity Broker shall support the discovery functionality. I.e. Identity Broker shall have the information about where to contact to retrieve a certain user profile data of a certain user. [Requirements from Use Case 1, 2, 3].
- Identity Broker shall provide a mechanism to transfer a data at one site to another site via Identity Broker or direct. [Requirements from Use Case 2, 3].
  Note: the re-direct of the request to another site may be supported.
- Identity Broker shall be able to control the data to be transferred among different service providers via Identity Broker. [Requirements from Use Case 2, 3].

Use case may be updated or added to include the following aspects:

- Identity Broker shall be able to control the data exposure according to the user's preference.
- Identity Broker shall be able to control of the exposure of user's identifier using pseudonym.
- Identity Broker shall be able to control on exposing the information about who provides a specific data about the user against the requester of this information.
- Identity Broker shall be able to control on exposing the information about who is requesting a specific data about the user against the provider of this information.

7 Technical Details

This clause identifies the relevant components and interfaces for the distributed user profile It also provides the technical detail for the protocols and the basic data schema to be used over the interfaces between different functional entities In order to provide an interoperable way for the distributed user managing profile management,

Note that the present document focuses on the proxy mode, while the redirect mode may be possible.

Note that authorization and access control will be discussed in INS-002 [i.16] and is out of scope of the present document. Privacy concerns related to the access and distribution are key subjects of INS-002 [i.16] and are out of scope of the present document as well.

7.1 Architecture

The basic relationship among different functional entities is depicted as Figure 15. User Profile Provider is one of the service providers which store the user information and provide it upon a request from the user or other service providers via Identity Broker.

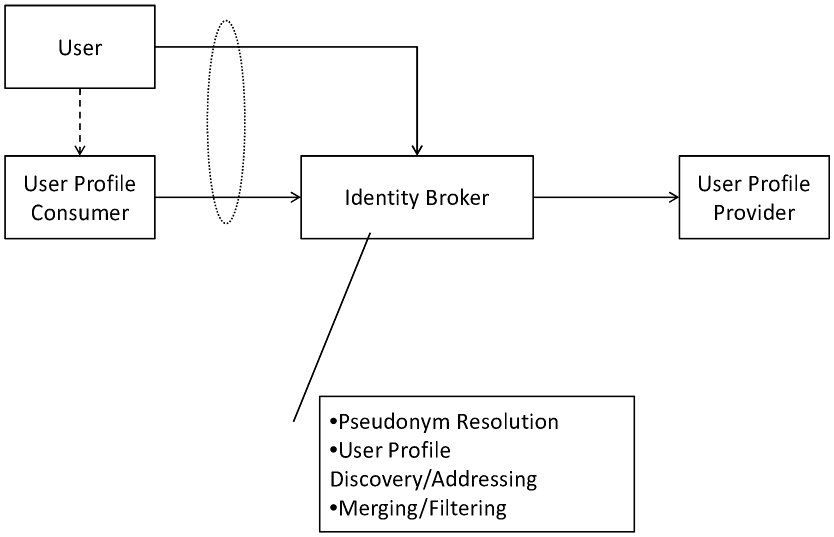


Figure 15: Relationship among functional entities relevant to Distributed User Profile Management

NOTE: The relationship with other functional components identified are described in GS INS 001 [i.17].

7.2 Components

- **User:** provides a request to manage his own user profile as CRUD (Create Read Update and Delete) operations. While a separate configuration is needed for authentication and authorization, the functional role in the distributed management is the same as User Profile Consumer. User is also the requester of the service provided by the User Profile Consumer, but this aspect of user role is out of scope of the distributed user profile management itself.

- **User Profile Consumer:** is a requester of the management functionality of user profile as CRUD operations.

- **Identity Broker:** brokers the request from User Profile Consumer to appropriate User Profile Providers. In order to perform the brokerage functionality, it also provides the functionality for pseudonym resolution, provider discovery, and user profile aggregation.

- **User Profile Provider:** stores the user profile data and provides the data upon request. It also provides the management interface. It offers CRUD operations.

7.3 Interfaces: Interface between User Profile Consumer (and User) and Identity Broker

This interface should convey the request from User Profile Consumer to manage and access to the user profile data of a certain user .The request may include the following information:

- Identifier of the User Profile Consumer.

- Identifier of a user, pseudonym known to the User Profile Consumer.

- A set of attribute names of user profile.

- Operations to be performed over the specified attributes.

This interface should convey the response from Identity Broker to User Profile Consumer indicating the result of the request. The response may include the following information:

- Status.

- Identifier of a user, pseudonym known to the User Profile Consumer.

- Updated/Consolidated user profile with attribute names and its value.

- Identifier of the User Profile Provider, if the policy allows to convey this information. The policy may be specified by the user, the service provider (User Profile Provider) and/or the Identity Provider for different purposes (e.g. privacy protection).

7.4 Interface between Identity Broker and User Profile Provider

This interface should convey the request from Identity Broker to User Profile Provider to access and manage the user profile data of a certain user upon a receipt of the request from the User Profile Consumer. Note that Identity Provider resolves User Providers and as a result, a single request may be split into requests towards multiple User Profile Provider.

The request may include the following information:

- Identifier of the User Profile Consumer or the Identifier of the Identity Broker.

- Identifier of a user, the resolved pseudonym which is known to the User Profile Provider.

- A set of attribute names of user profile.

- Operations to be performed over the specified attributes.

This interface should convey the response from User Profile Consumer to Identity Broker Consumer indicating the result of the request. The response may include the following information:

- Status.
- Identifier of the User Profile Provider, if the policy allows to convey this information.
- Updated/Consolidated User profile with attribute names and its value.
- Identifier of a user, pseudonym known to the User Profile Provider. This identifier should be the same identifier as the one provided by the request

7.5 Accessing Protocol

This clause describes the message structure of Access Protocol by two Interfaces described above. In principle, those interfaces convey the same set of information and thus the same message structure can be used.

As described in State of Art section, SAML[2] is considered as a basic protocol in the Telecommunication area especially when it interwork with the Enterprise domain. Also, the use of DST [1] over the SAML to convey User Profile information is also adapted by the Telecommunication domain as well. Thus, SAML-DST is suitable for the Distributed User Profile Management with the involvement of the operator as Identity Broker.

This clause specified how SAML and DST can be used for the User Profile Management, by introducing the concept of SAML-DIST message.

The SAML-DST message as depicted in Figure 16 contains the relevant User Profile as a DST message, which can also convey the operation information which should be applied to the data (User Profile), which is then encapsulated into the SAML message with information identifying the User, including his pseudonym.

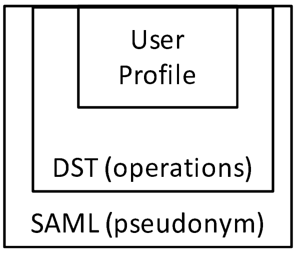


Figure 16: SAML-DST message concepts

7.5.1 DST usage

DST is used as a container of any types of user profile data. The type of each user profile should be identified by the defined name space for that specific user profile. DST also contains the operation information as request type.

The defined set of operations are as follows:

- Create: to create a new user profile data, which can be either the entire user profile or a partial data within a user profile.
- Read: to read a specified user profile data.
- Modify: to updated a specified part of user profile data.
- Delete: to delete a specified user profile data, which can be either the entire user profile or a partial data within a user profile.

NOTE: The original DST only allows the Create and Delete operations against the entire set of the user profile, while the proposal here is to use those two operations for the creation and deletion of the data inside the user profile. As it is more suitable in the case where the User Profile Consumer does not know exactly where those data are stored.

7.5.2 SAML-DST

SAML-DST is an extension to SubjectQueryAbstractType of SAML message.

SAML-DST request contains the necessary data for the Identity Broker performing identity management and also contains DST message to manage and access to the User Profile information.

SAML DST response may contain multiple DST responses, issued by different User Profile Providers, while Identity Broker may merge those responses into one DST response according to its policy.

The SAML-DST request and response are depicted as Figures 17 and 18 respectively.

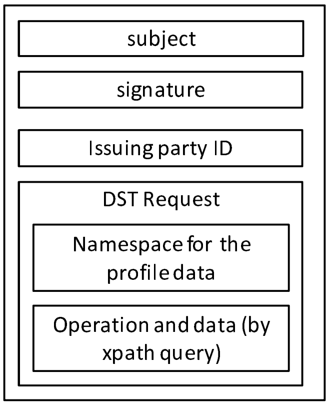

subject
signature
Issuing party ID
DST Request
Namespace for the profile data
Operation and data (by xpath query)

Figure 17: SAML DST Request

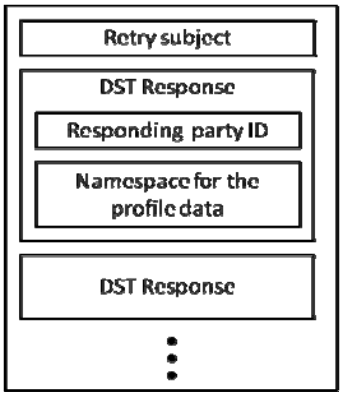


Figure 18: SAML DST Response

7.6 User Profile Schema

A set of User Profile types is defined by the Liberty Alliance and additional types can be defined according to the necessity.

8 Conclusion

The existing standards works such as SAML and DST well fit the requirements for using Identity Broker as an anchor points to manage distributed user profile. If the SAML and DST can be adopted by the telecom domain as well, the telecom operator can easily play the role as Identity Broker.

Annex A (informative): Authors and contributors

The following people have contributed to this specification:

Rapporteur:
Naoko Ito, NEC

Other contributors:
Joerg Abendroth, Nokia Siemens Networks

Ricardo Azevedo, Portugal Telecom

Hervais C. Simo Fhom, Fraunhofer Institute for Secure Information Technology

Joao Girao, NEC

Mario Lischka, NEC

Wolfgang Steigerwald, Deutsche Telekom AG

History

Document history		
V1.1.1	November 2010	Publication