

Flexible Services

Ecosystem Design and Evolution (EDEN) D5.1.1 Mobile Authentication federation framework and Pilot

Document Name	Mobile Authentication federation framework and Pilot
Project/WP Title:	EDEN/WP5 Mobile Certificate
Document Type, Security	P (Public)

Document Title:	Mobile Authentication federation framework and Pilot
Agreed date of delivery	N/A
Actual date of delivery	
Editor	Olavi Karasti/Elisa
Version	Version 1.0
Date Last Change	11.2.2011
File:	Mobile Authentication federation framework and Pilot D5.1.1.doc

Participants	Name	e-mail
Elisa	Olavi Karasti	
	Ilpo Mäntykangas	
TeliaSonera	Olli Jussila	
Aalto	Sanna Suoranta	
	Tancred Lindholm	
	Tuomas Aura	

Table of Contents

1	List of Acronyms and Abbreviations.....	4
2	Executive Summary.....	5
3	Introduction	6
4	Definitions	7
5	Federation framework of an IAM system	8
5.1	Wireless PKI (wPKI).....	10
5.2	Mobile Certificate Pilot expectations	11
5.3	Strong Authentication Using Mobile Phone	13
6	Pilot system	14
6.1	Architecture.....	14
6.1.1	Functional entities.....	15
6.1.2	Sequence Diagram	16
6.2	Roles and Actors	18
6.3	Challenges	19
7	Conclusion	21
8	Next steps	22
9	References.....	24

List of Figures

Figure 1. Federated IAM system 9
Figure 2. Example of MSSP architecture with roaming and multiple CAs..... 11
Figure 3. Technical architecture 15
Figure 4. Sequence of messages in IAM-process 17
Figure 5. Roles in IAM system 19
Figure 6. Mobile Cloud architecture..... 22

1 List of Acronyms and Abbreviations

AM	Access management
CA	Certificate Authority
EDEN	Ecosystem Design and Evolution
FS	Flexible Services
FSE	Flexible Services Ecosystem
IAM	Identity and Access Management
IDP	Identity Provider
LDAP	Light Weight Directory Access Protocol
MC	Mobile Certificate
MCO	Mobile Cellular Operator
MSISDN	Mobile Subscriber Integrated Services Digital Network Number. i.e. "Phone number"
MSSP	Mobile Signature Service Provider
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign On
wPKI	Wireless Public Key Infrastructure

2 Executive Summary

This document presents Identity and Access Management (IAM) pilot made by EDEN project. EDEN was one project in the Flexible Services research program. Flexible Services research program was one program managed by the ICT SHOK company called TIVIT Oy. [TIVIT]

IAM-pilot demonstrated federated IAM system. Federation means in this context that there can be several actors providing Authentication or Access service to Users and Service Providers.

In this pilot Elisa Corporation provided Authentication and Access management service and Aalto University provided service to the user. Authentication used mobile network and its MSSP to provide authentication. Service was Aalto's already existing grading system called Rubyric.

Users were Aalto personnel and they used mobile phone with SIM card with keys. Elisa provided SIM card which included key for the authentication. MSSP and LDAP were real services which Elisa uses to provide services to customers. Access Manager and IDP were implemented in ElisaLabs which was Elisa's pilot and demonstration system.

3 Introduction

EDEN project found Identity and Access Management (IAM) system as one of the most important technical enabler for Flexible Services kind of ecosystem. Therefore it needed testing and piloting and it was decided to build a pilot for that.

This document presents as the name suggests Mobile Authentication federation framework and pilot. Pilot is made by Elisa and Aalto University. Aalto acts in this pilot as Service Provider and Elisa as Identity and Access provider and Users were Aalto personnel.

Service for the user was a Rubric-service. It is a rubrics-based assessment tool for evaluating students work. Authentication was made by wPKI and used wPKI SIM provided by Elisa.

First there is introduced federation framework for an IAM system. It consists of federation basics, wPKI, pilot and description about strong authentication using mobile phone. After that there is description about pilot and roles and challenges. Finally there are conclusions and next steps.

4 Definitions

Federation is about when service and ID is in different domain. There is needed process to connect certain features of identity to SP to SP to allow usage of the service.

Mobile Authentication is a method of authentication where user uses SIM with credential keys and phone to authenticate herself to MCO's MSSP.

5 Federation framework of an IAM system

Federation in an IAM system means ecosystem capability for user (or entity if user is not a human) to identify herself to one or number of service providers with same authentication action. In modern service ecosystems it is not restricted to one method but there are several means to make this authentication. Chapter 5.1 describes one authentication method called wPKI which is used in this pilot. It is an authentication method utilised in the mobile networks.

The Identity is usually dealt with life cycle concept. It is divided to three parts which are important especially for administration of digital identity. These phases are:

- Provisioning
- Maintenance
- Deprovisioning

[EDEN-D1.2.3]

Digital identity is in this pilot in Maintenance state and other phases are not dealt. Of course because this is real pilot, digital identities were created for the pilot and demolished after pilot but that processes were there just to have digital identities available and did not represent standard way of doing so.

Assumptions why federated IAM systems are needed are numerous.

- 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.

[Weyl05]

In Figure 1 there is illustrated an ecosystem where federation is used to authenticate user to different service providers. In Figure 1 U is User, IdP is Identity Provider, AM is Access Manager and SP service Provider. Authentication is federated to other service providers which services are utilised to build a service to the end user.

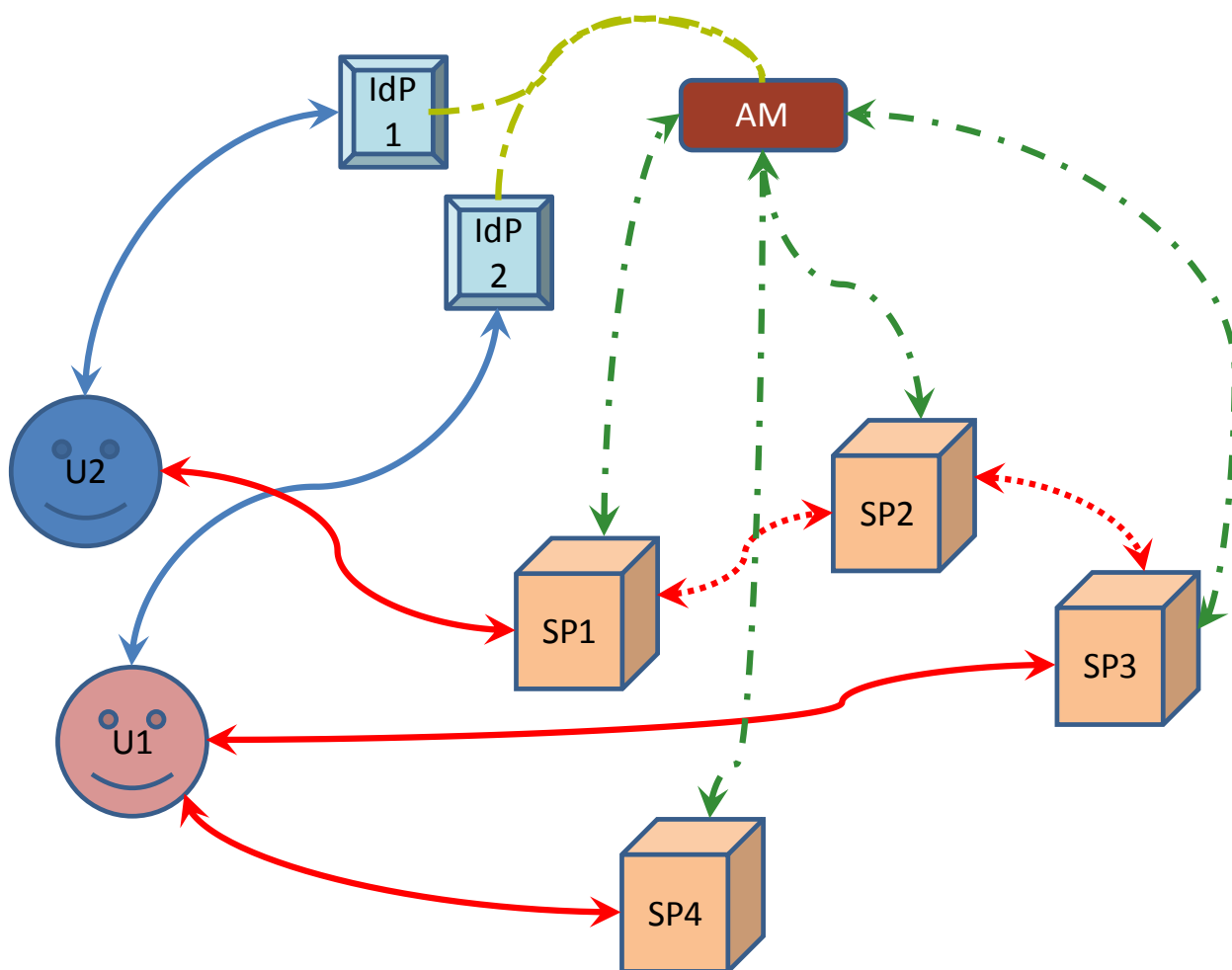


Figure 1. Federated IAM system

Identity and access management in the case illustrated in Figure 1 is described next. User 2 needs a service which SP1 can provide but it needs services from SP2 which needs a service from SP3. In all these instances same authentication can be used to provide access to needed services so that finally End User needs is fulfilled. For the End User this action appears to be as SSO. The User 1 uses IdP2 to authenticate to be able to use services from Sp3 and 4. Same Access Manager is use for both U1 and U2.

Access Manager gives access attributes to SP. SP can then give access to User to use service. Different services may have different requirements for the access. E.g. user needs for certain service only weak authentication and that is selected for that service. Next User needs strong authentication to use her bank account and then strong authentication is used at IdP and AM to enable that service.

For the flexible service ecosystem there can also be several Identity Providers and also Access Managers. All these identity providers, Access Managers and services providers should be able to use federated identity and access.

5.1 Wireless PKI (wPKI)

The PKI on a mobile terminal is called Wireless PKI (wPKI) where mobile phone operators act as CAs. With advanced implementations, a secure smart card storing subscriber information called SIM-card is used for on-card key generation and storage for asymmetric keys. The key-pairs can be also pre-generated and are stored in the SIM card and protected with secret PIN(s). A SIM card must have for support wPKI technology.

A certificate is not stored on the SIM card. Certificate Authorities (CA) provides interfaces to access certificates for the parties performing validation or usage of a certificate for other purposes. ETSI Mobile Signature Service Provider (MSSP) standards binds together CAs, certificates, interfaces and communication between service providers, mobile signature providers and wPKI application and key-pairs on the SIM card.

Using the implementation of ETSI Mobile Signature Service Provider (MSSP) standards a service provider sends authentication or eSignature request to wPKI application on the SIM card. A user approves a request with personal secure PIN code. wPKI application on the SIM-card signs a request with a private key. A signed respond is returned with MSSP. Mobile operator and services provider verify and validates the signature using the certificate and public key of the end user. All fundamental PKI-validation operations like Certificate Revocation Lists (CRL) are used.

Implementing Public Key Infrastructure (PKI) using SIM card enables several opportunities for IAM solutions. First of all wPKI is two-factor strong authentication method utilizing asymmetric keys for encryption. More than one key-pair is supported (role based certificates). Typically one key-pair is reserved for authentication and other for electronic signatures. However, the issuer of wPKI defines certification policy and how key-pairs are implemented. A certificate issued for the end-user typically contains some basic identity information of the user like full name, gender, birthday and unique identifier. Typically a mobile certificate issuing process includes the strong physical or electronic identification and authentication of the end user by an authority (government, bank, mobile operator, a company (for business usage)). This means that wPKI solutions has strong authentication with identity information in a same package. In practice, an IDP of IAM solution can use wPKI for user registration and for strong authentication and eSignatures.

wPKI supports several different service channels because the authentication and eSignature channel is separated from the service channel. End users can be authenticated with wPKI when they are accessing internet services with PC or mobile phone but also during a phone call or in the face-to-face situation. MSSP communicates with wPKI application over SMS-bearer. With SIM-Toolkit (STK) user interface wPKI application is able to interact with user even during active phone call.

ETSI MSSP (Mobile Signature Service Provider) is based on four entities:

Home Entity - HE (has connection to individual clients/end-users, sometimes also called Home MSSP HMSSP)

Acquiring Entity - AE (acquires signatures)

Routing Entity -RE (handles roaming in multiple operator environments)

Verification Entity may be as part of first two.

All above may be combined together or alternatively be separate entities (like for example a bank having Acquiring Entity which connects to mobile operator's Home Entity). ETSI MSSP standards include interfaces between entities and for integrating any application to use mobile signature service. Application Provider (AP) or Service Provider connects to AE with ETSI TS 102 204. AE communicates with RE using ETSI TS 102 207. RE, after routing decision, forwards request to other RE or to HE using ETSI TS 102 207

In Finland mobile operators have been active to support and implement MSSP roaming based on ETSI TS 102 207 specification. REs use Numpac (Finnish HUB supporting mobile phone number portability) for routing decisions.

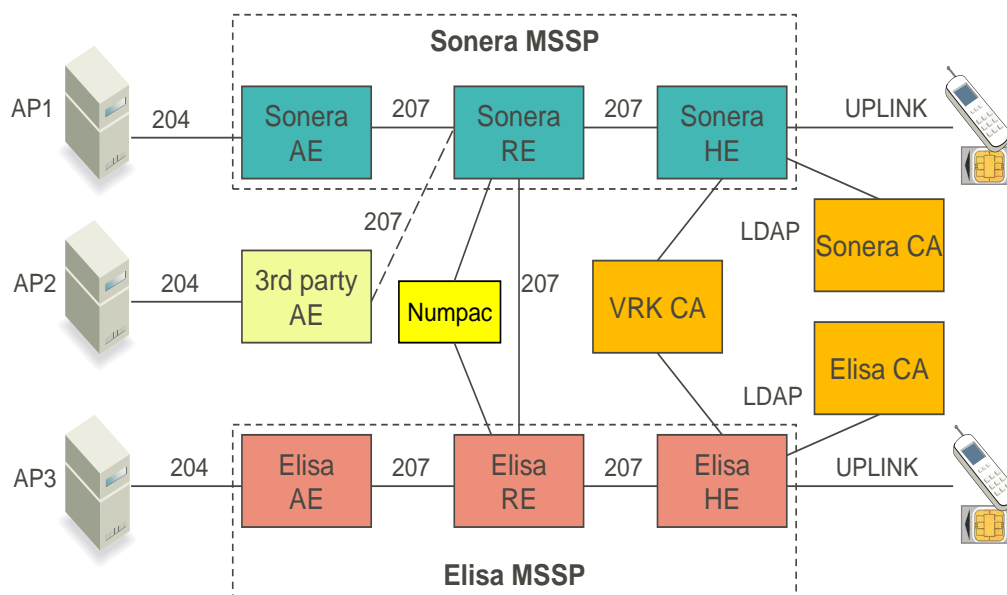


Figure 2. Example of MSSP architecture with roaming and multiple CAs

Thanks to MSSP roaming a service provider or an IDP can reach all wPKI customers of all mobile operators by using ETSI TS 102 204 interface to one Mobile Operator.

5.2 Mobile Certificate Pilot expectations

This pilot tested implementation of a federated IAM system, especially access management using wPKI as an authentication method in a federated environment where Elisa acted as a SAML IdP and wPKI MSSP for services of the Aalto University. The functionalities implemented in the pilot tested the most important enabling technologies of IAM:

1. Every service does not need its own separate user database

2. Existing user databases of the organizations can be used
3. Authentication is based on a strong method, wPKI, using existing devices
4. Single sign-on and single logout are possible
5. Firewalls do not cause problems since standards, certified systems and technologies are used

Usually, when two companies want to use a federated IAM system, they first negotiate an agreement. The negotiation can be time-consuming and difficult since it has various participants, for example lawyers, service owners, system architects and technicians, but when the agreement is reached, the technical implementation of IAM is easy. Similarly, different organizational units of a large company have to agree on how to use a common IAM system. Sometimes the negotiation in the large company is even more difficult than between the two companies because the company units do not often make agreements between each other and thus there is no common procedure for making the internal agreements. For example, service owners, maintenance staff and other persons need also adjust the organizational requirements of their units in order to use a common federated IAM system. To summarize, the IAM negotiations can be divided into two phases: political and technical phase.

The mobile certificate pilot was a good example of both political and technical challenges described above. Politically, the federated IAM is more easily promoted for administrative staff with following terms:

- A. Easier manageability
- B. Better usability
- C. Better security
- D. Less expenses

The greatest impact for the administrative staff is a combination of issues described above. These can be grouped and ranked to show how this staff normally values IAM issues. First is the greatest impact and fifth is the least one:

1. A, B, C, D
2. A, B, C
3. C, D
4. B, D
5. A, C, D.

5.3 Strong Authentication Using Mobile Phone

Mobile phone technology offers possibilities for strong authentication. In addition to mobile certificates, mobile phones will have a trustworthy storage for secrets and capability to execute strong cryptographic operations.

In his master's thesis, Sandeep Tamrakar has implemented a prototype where a mobile phone emulates a smartcard reader and smartcard. The prototype provides same functionalities to applications as is done by the smartcards: . The phone is connected to a computer using USB CCID driver interface, and the computer presents it as a smartcard reader that has a smartcard inserted. The device can use secure hardware for storing the certificates in a tamperresistant way. The work is done using Maemo and Nokia N900.

In her master's thesis Marcia Villalba is implementing hardware-assisted one-time password authentication that uses Nokia's On-board Credential (ObC) technology. On the server side, a web service uses one-time passwords for client authentication, and a provisioning server creates and distributes the one-time passwords for the devices. When the mobile device is used for authenticating to the web service, either stand-alone widget is used or the authentication is integrated into the web service. The client is challenged with an index, and ObC provides the corresponding one-time password. In addition to one-time passwords, other credentials can be stored using ObC.

In his master's thesis, André Andrade is implementing a prototype that allows identity provider of Shibboleth use a mobile phone as authentication tool. First, the user connects to a service provider using a computer. The service provider connects to an identity provider that returns a session ID. Then the user connects the identity provider using his mobile phone and authenticates his identity strongly using onboard credentials stored on the tamper-resistant hardware of the mobile phone. The identity provider returns the same session ID, that the user compares between the mobile phone and the computer. The service provider polls the identity provider if the authentication has been done successfully. When this is the case, the service is given to the user.

More information:

Sandeep Tamrakar. Phone as a smart card. Master's thesis, Aalto University School of Science and Technology, under work, 2010.

Laura Marcia Villalba Monné, Remote credential management tool for an On-board credential application, Master's thesis, Aalto University School of Science and Technology, under work, 2010.

André Palas de Andrade. Strong authentication using mobile phone. Master's thesis, Aalto University School of Science and Technology, under work 2010.

6 Pilot system

Pilot was implemented between Aalto University and Elisa Corporation. Pilot demonstrated federated IAM system. In this pilot Aalto acted as Service Provider providing Rubyric service and Elisa acted as an IAM provider. Rubyric is a rubrics-based assessment tool for evaluating students work. Graders give pre-written feedback phrases to construct feedback, which speeds up assessment as all feedback does not have to be written manually. It also ensures consistent grading across graders, as the submissions are graded according to pre-defined evaluative criteria, as opposed to "gut feeling".

Technical issues implemented in this pilot were:

- Object stores (LDAP)
- Registration (user to LDAP, MC to LDAP, User to service)
- Attributes (LDAP, SAML)
- Mobile Certificate (CA, Certificates, keys)
- Access to Service (Rubyric)

6.1 Architecture

In the following chapters technical architecture is presented. First there are presented functional entities and then sequence of communication in the IAM ecosystem.

Figure 3 shows entities which active in this pilot. These entities can be in most cases divided to sub entities. In this deliverable however description is in this level because it is actual implementation which dictates what kind of sub entities there can be found in detail. Implementation can be slightly different depending on vendors who implement IAM systems.

In Figure 3 there are shown few of the technical entity owners in the pilot. These are marked by blue background and they are Elisa Production, ElisaLabs Services and Aalto.

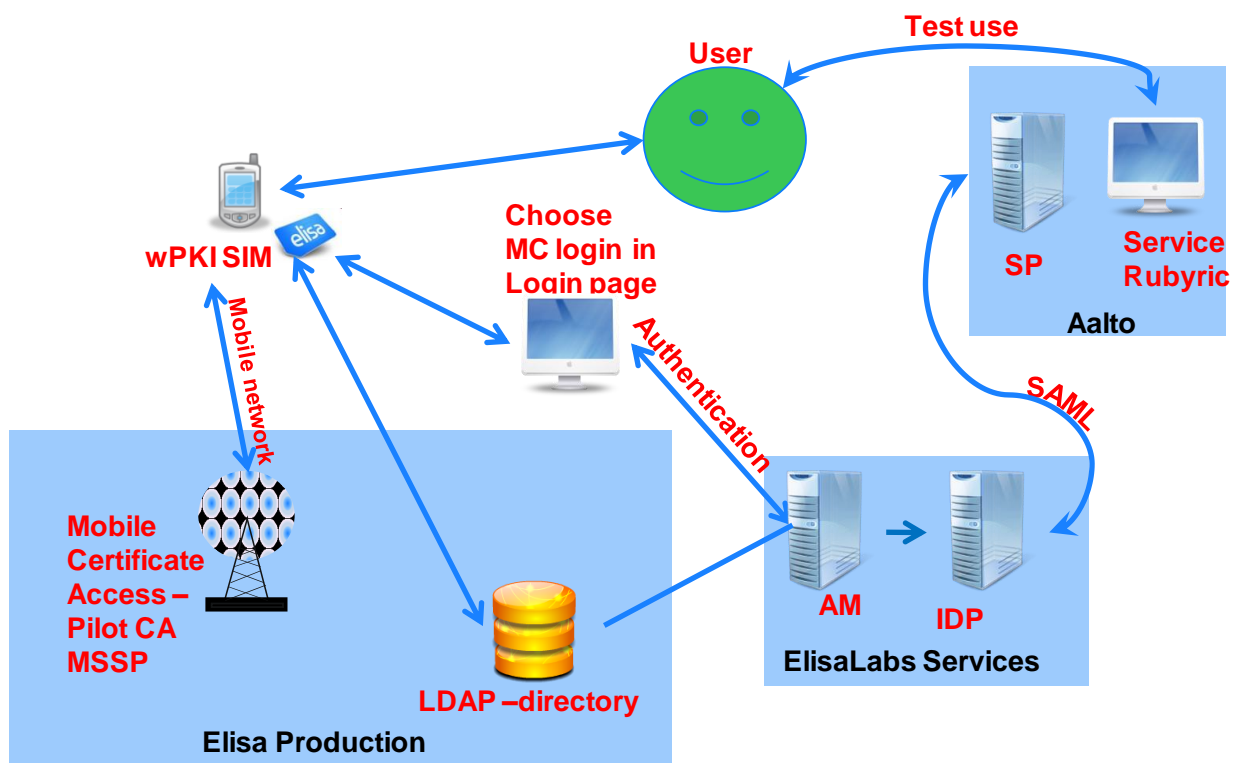


Figure 3. Technical architecture

6.1.1 Functional entities

Main Technical entities in this pilot are **Authentication**, **Access Management** and **Service**. Different implementation of IAM system can lead different categorisation to entities. This division is however regarded as a basic implementation and therefore represents a basic categorisation.

Authentication technical entity consists of:

- User mobile device with SIM card with keys
- Mobile network capable to provide certificate using MSSP (see chapter 5.1)
- User devices to choose and use MC login
- LDAP directory

LDAP directory can be regarded to partly belong to Access Management and partly to Authentication in this pilot because directory information is used in Access Management. Functionalities inside Mobile Network are explained in more detailed in chapter 5.1 in this document. Elisa provided all functionalities inside this entity except user mobile device and User login device. Inside of Elisa, LDAP and MSSP were actual and real functionalities in Elisa's Production and are used in real world services to Elisa's employers and customers.

Access Management function consists of Access Management System and IDP to provide authorisation information to SP using SAML. This was implemented in Elisa's demonstration and development environment called ElisaLabs.

Service function in this pilot is Rubyric service which is used by graders. Service function is provided by Aalto.

6.1.2 Sequence Diagram

Sequence of communication in federated SAML based IAM systems which use wPKI and MSSP don't have a great variation between them. The communication presented in this chapter and used in this pilot is very much common for all these kind of IAM systems. Still there are some differences and this presentation can not be regarded as design rule for IAM systems. Especially when dealing with details there are differences.

In *Figure 4* there is presented UML sequence diagram of communication in this pilot. This description is on high level and there can be found more detailed communication inside of communication arrows and between entities, but it is not dealt here. In the top there are functional entities. These entities communicate with each other, which is presented with arrows connecting different functional entities. Communication is chronological so that time goes downwards.

User is Aalto personnel and he/she uses PC (Browser) and Phone with SIM (wPKI). Elisa hosts Mobile Network/MSSP, LDAP, AM and ODP. Aalto University is a SP and hosts Rubyric service.

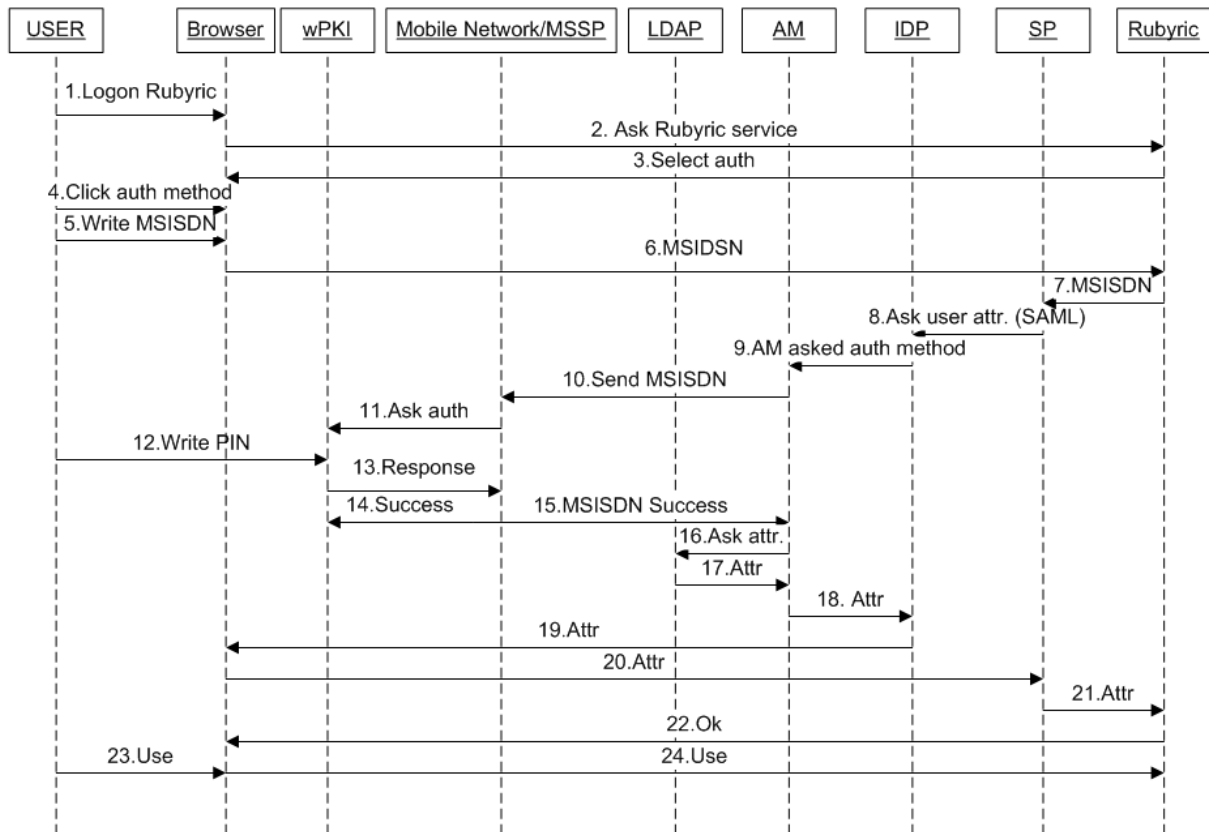


Figure 4. Sequence of messages in IAM-process

Description of communication is following:

1. User needs to use Rubyric service and logs on to Rubyric page via Browser
2. Browser forwards this log on inquire to Rubyric service
3. Rubyric ask to select Authentication method
4. User clicks and selects MC access to browser
5. User writes her phone/SIM number to the browser
6. Browser sends this to Rubyric service
7. Rubyric service send MSISDN to SP
8. SP asks user attributes from SP using SAML
9. Am is asked what about authentication methods
10. Am send MSISDN MSSP
11. MSSP asks from wPKI and from user for authentication

12. User writes the PIN to the phone
13. Phone sends Response to the MSSP
14. MSSP signals that authentication is ok
15. MSSP signals to AM that authentication with this MSISDN is ok
16. AM asks for attribute for this authenticated user from LDAP
17. LDAP provides user attributes to AM
18. AM sends user attribute to IDP
19. IDP signals User or user's browser about attributes
20. Browser contacts Sp about access to service
21. SP provides attributes to Rubyric service
22. Rubyric service signals to User and user browser that logging is ok
23. User starts to use browser
24. Browser is connected to Rubyric service

6.2 Roles and Actors

In this pilot primary roles were Authentication provider, Access provider, Service Provider and User. Elisa acted as Authentication provider and Access Provider and Aalto as Service Provider. Users were personnel in Aalto University.

A primary role consists of several roles which can be managed by different entities. An operator can be only acting as Mobile Certificate provider. Access provider can be another company which can utilise mobile operators' certificate to create attribute for access.

Authentication provider role consists of SIM provider, Mobile network owner and LDAP manager. These roles can be divided further but are not important in this context.

Access provider includes Access Manager and IDP system to provide identities to service provider.

User is a user of a Rubyric service.

Service provider hosts service and grants access based on information which it gets from IDP using SAML base communication.

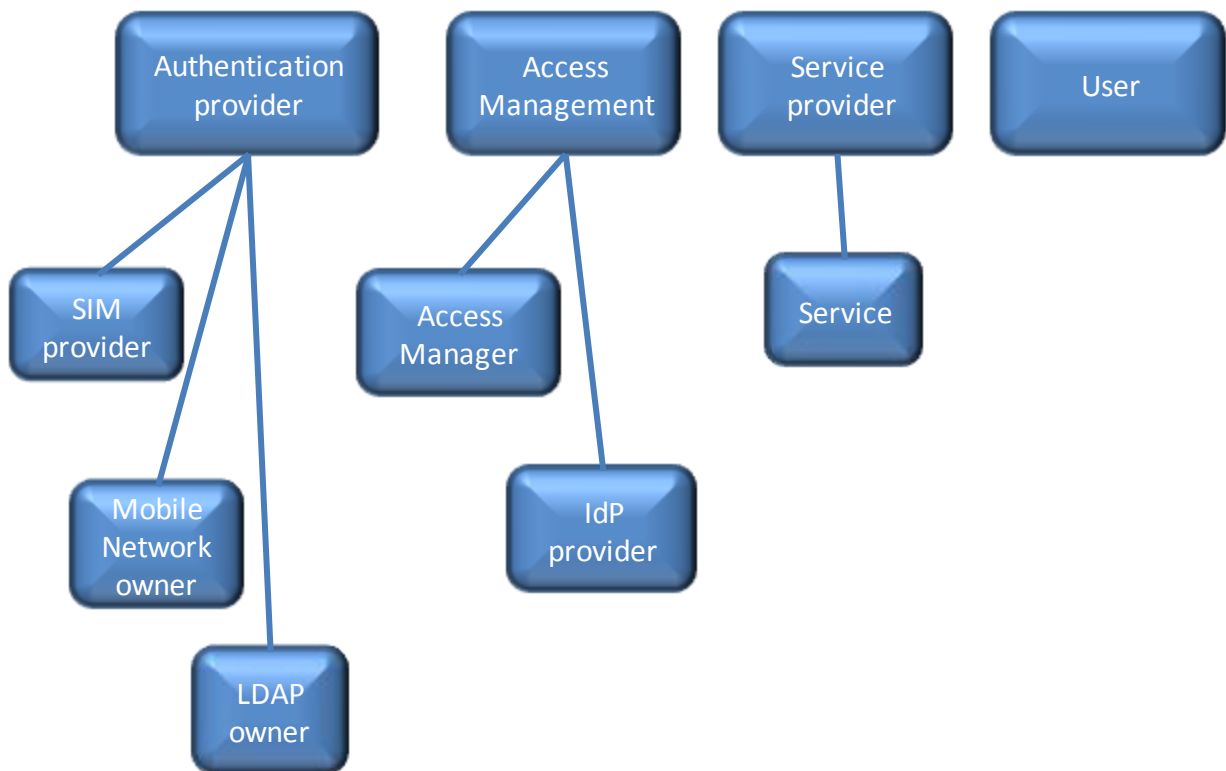


Figure 5. Roles in IAM system

Actors in this pilot were Elisa, Aalto, and Users which were Aalto personnel. Elisa took roles all in Authentication provider and Access provider. Aalto acted as Service provider.

6.3 Challenges

Today many ecosystems, using web for providing services, are designed in the **SP point of view**. This is obvious because often these systems are designed or at least started by SP. This leads mostly to a system where IAM is different for each SP who is acting in this ecosystem. For the SP this is ok but for the user situation can be tedious. Each SP requires for example different user name and password and the UI is different. Also there is often very little information given to User about SP. [Jøsang05]

IAM systems should take care also about User because with out good **usability** security of system is risked. This is discussed in more detailed in EDEN project deliverable D5.2.1.

Biggest **business challenge** is perhaps that actors in ecosystems don't realise that User Acceptance is reached only by federated IAM and with the fact that IAM ecosystem must be open. In this way there is enough room for the market to start and grow. If actors keep all functions in their infrastructure trying to act in a monolithic way where all activities of IAM are inside of one actor without federation of identity, the market is differentiated and size is much smaller.

In this pilot there were many organisations involved although main actors were only Aalto and Elisa. Inside of these main actors there are organisations fulfilling their tasks to accomplish needed results. Inside of both main organisations there were needed negotiations between different organisation levels to be able to arrange this pilot. Sometimes it is easy but it is possible that in the worst case some part of the organisation can deny to make this kind of a pilot because it could threaten in some way them to achieve their goals.

User information used in this pilot is taken from HAKA database which is based on SAML. Haka is the identity federation of the Finnish universities, polytechnics and research institutions. Users are able to access federation services using a single user account and password. User identities are provided by the users' home organizations. Metadata information in HAKA is huge in size. In this pilot only a fraction of information was used and huge amount of data brings complexity to the system

Also different vendors have slightly different interfaces and adjusting system to work can be tedious. Firewalls in whole ecosystem can be in some cases a challenge. IAM communication protocols should be defined so that firewalls don't block communication.

7 Conclusion

From service administrator point of view, important issues are:

- Using federation, there is not need to do user management their selves, nor checking if the user is still in the position where they were when they started using service. User credentials are taken from their “owner” SP and that that takes care of validation and existence of required attributes. SAML federation is used same way than OpenID, but in opposite, the owner is known and channel is secured.
- When using MC and phone, someone else takes care of the mobile device (user, employer,...) and SIM-card (owned by Operator). MCO takes care of revocation lists of SIM-card mPKI keys and PIN checking.
- Implementing federated IAM environment needs from start some extra work. Arranging certifications for servers/services and agreements takes time, but it is normally one time job in the beginning and can be done with specialists, who are not needed any more afterwards. Use and management is not time consuming.
- Using wPKI is more secure than username with password. wPKI enables more services with same IAM action than usage with username and password. If username with password is used to services needing strong authentication, there is needed something extra (e.g. VPN, tokens) to enable secure service usage. Often there are cumbersome compliance reasons which assume that security is handled in this way.
- SSO using MC is a secure way for user to use services. If SSO is not used with strong authentication security reasons sometimes prevent using SSO in this way.

8 Next steps

WP1 in EDEN project defined architecture for Flexible Service Ecosystem which was in fall 2009 entitled to **Mobile Cloud**. In Figure 6 there is illustrated layered Mobile Cloud ecosystem.

The center of the figure is divided into three layers. The top layer denotes the long tail of services, the middle layer focuses on extension of enterprise cloud, while the bottom layer focuses on mobile users.

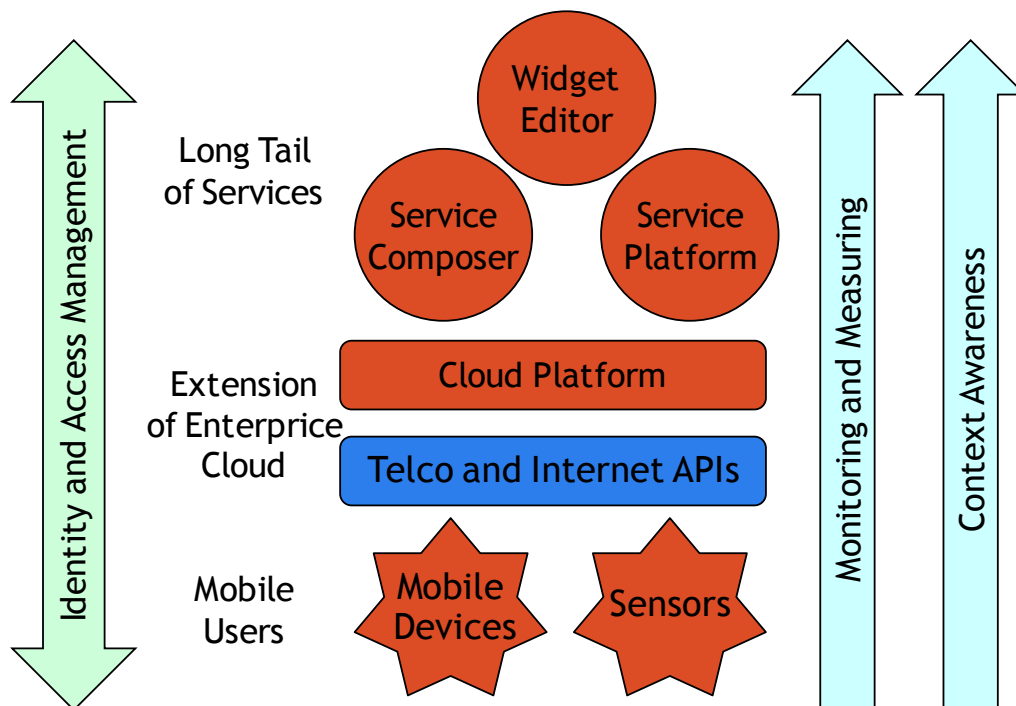


Figure 6. Mobile Cloud architecture

More information can be found on deliverable made in WP1 in EDEN project. [EDEN-D1.2.3]

In Mobile Cloud Ecosystem, IAM is vital and necessary technical enabler for the system. When services are in the cloud where number of different Service Providers act there is needed feasible federated IAM system which all parties can trust. And when there are even more players in other parts of the ecosystem federation of Identities is the only possible solution to enable IAM to work in these kinds of Mobile Cloud Ecosystems.

This federation of Identity is the key technical enabler for these kind of architectures and it should be next issue to pilot. Unfortunately Flexible Services program is not continuing and therefore this piloting has to be continued elsewhere.

Cloud security means IAM system where IAM services are more or less in the cloud. Cloud security provider uses cloud technology to provide needed Identity and Access services and attributes when needed. Customers for this provider can be companies using? Saas services, employees of a company or SP with Web Services. Idea behind cloud security is that there are wide variety type of actors which need IAM services. Their needs are best fulfilled if IAM provider uses cloud security to IAM services.

Cloud Security means scalable IAM system where recourses can be utilised only when needed and using SSO. This brings savings and flexible services to the customers.

This type of security should be demonstrated in a trial but again because Flexible Services program is not continuing it has to be implemented in other forums.

9 References

- [EDEN-D1.2.3] EDEN Project, D1.2.3 Flexible Services Ecosystem architecture September 2010.
- [McQuaide03] Bill McQuaide, Identity and Access Management, Transforming E-security into a Catalyst for Competitive Advantage, Information Systems Control journal, Volume 4, 2003
- [Steven06] A. Steven and M. Baladi and D. Mowers and C. Owen and J. T. Rasmussen. Microsoft Identity and Access Management Series Provisioning and Work Microsoft Solutions for Security and Compliance (MSSC), 2006.
- [Weyl05] Benjamin Weyl, Pedro Brandão, Antonio F. Gómez Skarmeta, Rafael Marin Lopez, Parijat Mishra, Christian Hauser, Holger Ziemek Protecting Privacy of Identities in Federated Operator Environments
- [Jøsang05] Audun Jøsang and Simon Pope, User Centric Identity Management AusCERT Conference 2005
- [TIVIT] www.tivit.fi