

Flexible Services

Ecosystem Design and Evolution (EDEN) Pilot and principles of user acceptance of MC services D5.2.1

Document Name	Pilot and principles of user acceptance of MC services
Project/WP Title:	EDEN/WP5 Mobile Certificate
Document Type, Security	P (Public)

Document Title:	Pilot and principles of user acceptance of MC services
Agreed date of delivery	N/A
Actual date of delivery	
Editor	Olavi Karasti/Elisa
Version	Version 1.0
Date Last Change	17.3.2011
File:	Pilot and principles of user acceptance of MC services D5.2.1.doc

Participants	Name	e-mail
Elisa	Olavi Karasti	Olavi.karasti@elisa.fi
Elisa	Ilpo Mäntykangas	Ilpo.mantykangas@elisa.fi

Table of Contents

1	List of Acronyms and Abbreviations.....	3
2	Executive Summary.....	4
3	Introduction	5
4	Definitions	6
5	Pilot.....	7
6	Services in pilot for the user	8
7	User acceptance	9
7.1	User acceptance and pilot	10
7.2	Benefits for the user	11
7.3	Benefits for the Service Provider	11
7.4	Challenges	12
8	Conclusion	13
9	References.....	14

List of Figures

Figure 1.	User view	11
-----------	-----------------	----

1 List of Acronyms and Abbreviations

AM	Access Management
EDEN	Ecosystem Design and Evolution
FS	Flexible Services
IAM	Identity and Access Management
IDM	Identity Management
IDP	Identity Provider
LDAP	Lightweight Directory Access Protocol
MC	Mobile Certificate
MCO	Mobile Certificate Operator
MSSP	Mobile Signature Service Provider
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign On
wPKI	Wireless Public Key Infrastructure
ETSI	European Telecommunications Standards Institute
FiCOMM	Finnish Federation for Communications and Teleinformatics

2 Executive Summary

This document presents user acceptance for Identity and Access management systems. User acceptance is dealt in light of IAM-pilot constructed in 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]

EDEN 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 mPKI authentication method. 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.

First pilot is described briefly and then general aspects of user acceptance are presented. After that there is presented user acceptance issue meaningful for this pilot. Finally there are challenges and conclusions.

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 and federation framework with 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 IDP? 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 Pilot

Technical details of the pilot are described more detailed in deliverable D5.1.1. This description gives a brief overview about pilot.

In pilot users use Rubyric service. Users can access service by authenticating themselves with mobile phone with SIM card which has keys. This is called wPKI authentication. Basically authentication method can be something different if there is known that authentication is secure enough to be used in Access Management. Mobile network can be owned by any operator if the network's MSSP fulfils ETSI and FiCOM requirements.

Users use computer and their mobile phone to log on to service. Service expects Access Management to grant an access to service. Same time it is possible to grant different level of access to different services.

Access Management could also be served by some other actor. In this pilot it is managed by Elisa but in real world there are number of Access Management providers which can provide Access Management service. For the successful ecosystem all actors should accept that in all roles there can be different actor. And ecosystem should be designed to be open so that market size is maximised. This means competition between actors who have taken same role in IAM-ecosystem. This is still more profitable for the whole ecosystem because system is open and users can rely on openly working IAM ecosystem and therefore market size is larger.

6 Services in pilot for the user

End service for the user is Rubyric service. To be able to use that service user needs other type of services. This means Identity and Access Management Services.

For the user, authentication services appears to be mobile phone with SIM card which has the keys. User gives PIN when asked and that triggers in the end rights to use end service. Access is noticed when browser shows Rubyric service to be available.

End service is used via Laptop with browser and that is the user interface to an end service.

Other services for the user are Identity and Access services. They are not directly visible to user but are in between user and service. User sees identification part appearing as PIN request. There is MSSP service which authenticates user SIM and provides success of authentication information to forward. This success information is used to pass user attributes for access to Access Management.

Next thing for the user is service to be available in the browser to use.

7 User acceptance

Davis presented in 1989 the Technology Acceptance Model (TAM) to explain the determinants of user acceptance of a wide range of end-user computing technologies. In this model key issues to use service are perceived Ease of Use and perceived Usefulness. [Davis 1989]

Comparing these issues to this pilot Ease of Use is reached because pilot is SSO (can combine other services as well) and giving PIN to the mobile device is simple. Usefulness is reached but there are other technologies than wPKI which are secure and useful. So advantage in this point is not so obvious although wPKI is useful for the user because it is regarded secure and simple way to authenticate.

Usability means mainly easy to use and a feel to user that actions are secure and users' trust and privacy is transparent to the user.

Easy to use is reached by appropriate UI in the mobile device and in login functions. This is not directly IAM issue but must be taken care when designing UIs.

Security for the user can be divided into two main categories: Security Action, Usability Issues and Security Conclusion Usability Issues. These two main categories include several aspects:

Security Action Usability

- The users must understand which security actions are required of them.
- The users must have sufficient knowledge and the practical ability to make the correct security action
- The mental and physical load of a security action must be tolerable
- The mental and physical load of making repeated security actions for any practical number of transactions must be tolerable.

Security Conclusion Usability Principles

- The user must understand the security conclusion that is required for making an informed decision. This means that users must understand what is required of them to support a secure transaction.
- The system must provide the user with sufficient information for deriving the security conclusion. This means that it must be logically possible to derive the security conclusion from the information provided.
- The mental load of deriving the security conclusion must be tolerable.
- The mental load of deriving security conclusions for any practical number of service access instances must be tolerable.

[Jøsang07]

In most cases user doesn't actually understand the security conclusions they are going to make because they don't have the needed knowledge and experience to IAM systems. And it is also so that even if there is an IAM expert to make a conclusion, she doesn't necessary know all the details how this IAM system is implemented and therefore conclusion may be difficult to make. This leads to fact that improved

security is not necessarily achieved by strengthening cryptography but making improved usability to strengthen users' ability to authenticate to services.

Security mechanisms are effective when used correctly. Strong cryptography and sound protocols are not secure if they are not used correctly. If user forgets to click encrypt button when needing privacy or when she is too confused about security keys needed and selects wrong choices making accidentally their private data public.

There are studies which claim that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical

[Alma99]

7.1 User acceptance and pilot

The key issue for the user in this pilot was to provide single strong authentication method which is simple to use and with tools users normally have. Usually there is needed different method to services which require different level of security. Then user normally needs to authenticate herself several times to be able to use different services. Using strong authentication and using user attributes in service side there is needed only one authentication from user whether she is using weak or strong authentication.

For the user, authentication appears to be mobile phone with SIM which has keys. Mobile Network (MSSP) asks PIN to secure authentication and this is what user sees in this authentication.

In Figure 1 there is illustrated what user sees when she uses wPKI authentication to be able to use Rubyric service. User sees her mobile phone and browser in her PC where Rubyric service sends log on window and actual service after authentication. As described in deliverable D5.1.1 there is large number of functions between user and Rubyric service in order to grant access to the user to to use service.

Good user experience is found if user doesn't feel procedures inconvenient and with the fact that user feels that she is in the charge and can rely on the IAM system which is making her possible to use needed service. User has to feel that trust and privacy issues are in order and she can control them.

Federation is one issue which increases user acceptance. Without federation SSO is difficult to reach in a secure way. An if SSO is not used user experience is not good.

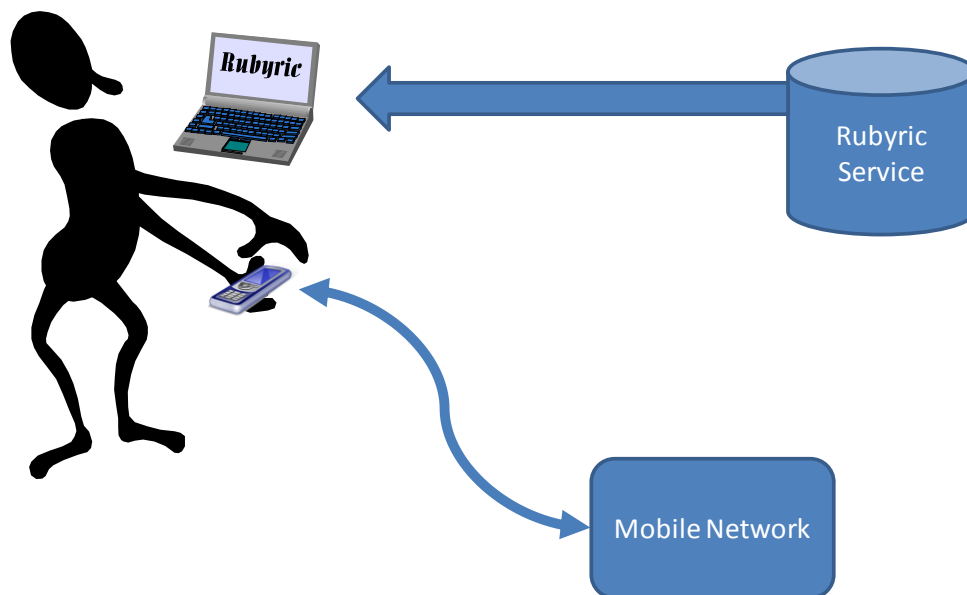


Figure 1. User view

7.2 Benefits for the user

User must understand what kind of security actions is required from her when using federated IAM systems. This means simple actions for the user. In this pilot this is to select mobile authentication and remembering and giving PIN needed for the SIM keys.

Also SSO is a feature for the user which increases user acceptance. If every service needs own authentication user must understand needed security aspects for different services. That is probably a tedious job and can lead to decreasing security as described in the beginning of this chapter. SSO means for the user that she authenticates herself only once in a session and different access requirements are handled by IAM system. User needs only to remember the PIN for the SIM keys.

7.3 Benefits for the Service Provider

Although this deliverable deals mainly with user acceptance there are issues which are relevant to SP if good end user experience is reached.

SPs are interested in providing services and making business with it. And to make business there is needed customers. If SP chooses authentication and access systems which are not easy to use users are not very willing to use services.

Security is one of the key issues for the SP. This is also important for the user. When designing an IAM system it must be kept in mind that e.g. making cryptography stronger is not necessarily more secure as described in this chapter 7 above.

7.4 Challenges

Challenge is to make IAM systems secure so that it is simple and easy to use by user. As described in chapter 7 complex and technically secure systems are not necessarily more secure if user doesn't know how to act correctly.

Transparent view of IAM system to user is also a challenge. IAM can be in details very complicated and difficult to understand by user. User must have a feel that she sees everything what is happening and there is no cumbersome functioning which give an idea that there is something hided in the system.

SPs have to understand above user issues, to be able to define sound and working ecosystem where users are willing to act.

8 Conclusion

User acceptance is needed and without it IAM ecosystem can not exist. There are a few issues which have to be present in a good IAM system.

Federated IAM with SAML can be provided to User if certain requirements are fulfilled:

- Good Usability
- SSO
- Trust & Privacy issues
- Actors have to accepts that there are many actors in most roles in the business ecosystem

9 References

- [Jøsang07] Audun Jøsang, Mohammed AlZomai, Suriadi Suriadi, Usability and Privacy in Identity Management Architectures, Australasian Information Security Workshop: Privacy Enhancing Technologies (AISW 2007)
- [Alma99] Alma Whitten J. D. Tygar, Proceedings of the 8th USENIX Security Symposium (Washington, D.C., Aug. 23-36, 1999), 169-184.
- [Davis89] Davis F. D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quartely, 13/1989, pp. 319-339.
- [TIVIT] www.tivit.fi