COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME
ICT Policy Support Programme (ICT PSP)

Towards pan-European recognition of electronic IDs (eIDs)

ICT PSP call identifier: ICT-PSP/2007/1
ICT PSP Theme/objective identifier: 1.2

Project acronym: STORK

Project full title: Secure Identity Across Borders Linked
Grant agreement no.: 224993

D5.8.3 Technical Design for PEPS, MW models and interoperability

Deliverable Id :	**D5.8.3**
Deliverable Name :	**D5.8.3 Technical Design for PEPS, MW models and interoperability**
Status :	**Final**
Dissemination Level :	**Public**
Due date of deliverable :	**December 31st 2011**
Actual submission date :	**November 11th 2011**
Work Package :	**5.1**
Organisation name of lead contractor for this deliverable :	**ES-MAP**
Author(s):	**John Heppe**
Partner(s) contributing :	**IT, PT, ES, BE, AT, DE**

Abstract: This document specifies the technical design, of which the mayor parts are described in 5 annexes:
1) D5.8.3a SoftwareArchitectureDesign is the software architecture design, which describes the software in architectural sense, as well for the PEPS as for the V-IDP.
2) D5.8.3b InterfaceDesign describes the interfaces of the common functionalities, which are between the PEPSes and V-IDPs
3) D5.8.3c Software design for the PEPS model, describes modules, packages, classes and methods which compose the systems.
4) D5.8.3d Security principles and practices
5) D5.8.3e Software design for the MW model, describes modules, packages, classes and methods which compose the systems.

Project co-funded by the European Community under the ICT Policy Support Programme

History

Version	*Date*	*Modification reason*	*Modified by*
0.1	04/10/2010	Initial version, being the approved D5.8.2	J. Heppe
0.2	28/10/2011	Updated version including comments from reviewers, updates of the interface specifications (see document history of D5.8.3b) and reference to D5.8.3e.	J. Heppe
Final 1.0	11/11/2011	Quality review and Finalization	S. Koppius, A. v. Overeem, R. Wannee

Intermediate internal versions, e.g. for quality reviews, have been omitted.

Table of contents

List of figures

List of abbreviations

<Abbreviation>	<Explanation>
AP	Attribute Provider
AT	Austria
BE	Belgium
DE	Germany
DOW	Description of Work
eID	electronic Identity
EC	European Commission
EE	Estonia
ES	Spain
EU	European Union
FR	France
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IDM	Identity Management
IDP	Identity Provider
IS	Iceland
MW	Middleware
MS	STORK Member State
NL	Netherlands
PEPS	Pan European Proxy Service
PT	Portugal
RA	Registration Authority
SP	Service Provider
STORK	Secure idenTity acrOss boRders linKed
STORK QAA	STORK Quality Authentication Assurance
UK	United Kingdom
WP	Work Package

Executive summary

This document specifies the technical design for the two common systems of STORK: a series of PEPSes and V-IDPs. The mayor part of this description is divided into 4 annexes:

1. D5.8.3a SoftwareArchitectureDesign is the software architecture design, which describes the software in architectural sense, as well for the PEPS as for the V-IDP. This document contains an exhaustive description for the V-IDP, including the complete software design. So for this system no chapter is defined in *D5.8.3c Software design*.
2. D5.8.3b InterfaceDesign describes the interfaces of the common functionalities, which are:
    a. Between the PEPSes and V-IDPs;
    b. Between the common functionalities of the PEPSes and the member state specific functionalities;
    c. Between the V-IDP and the SPWare.
3. D5.8.3c Software design for the PEPS model, describes modules, packages, classes and methods which compose the systems for the PEPS.
4. D5.8.3d Security principles and best practices.
5. D5.8.3e Software design for the MW model, describes modules, packages, classes and methods which compose the systems for this model.

In the rest of this document all of these parts are briefly described.

As this master document contains all introductory information, like executive summary, introduction, risk list, acceptance criteria, etc., all other documents have very short introductions, limiting themselves to only those topics that are really important to describe in their introductions.

The complete set of documents is primarily directed at the developers, who'll have to build the systems, based on this documentation. When reading it, please take into account that MS specific functions are to be included at the locations foreseen for such an integration.

All of these documents are *live* documents during the project. This means that, if during development or even production phase, the project team discovers that some topics should be implemented in a different way, this change will be applied to this document. That's the reason that this document has a sequence number 5.8.3, as a substitute of D5.8.2.

1 Introduction

1.1 Objective

This document, including annexes, describes the systems that compose the common functionalities of the STORK platform: a series of PEPSes and V-IDPs. The first annexes still have a view that probably can be understood by functional users with enough technical background. The most technical annexes (5.8.3c and 5.8.3e) are clearly oriented to be understood by the programmers who will build these functionalities.

This "master document", is meant to explain the contents of the annexes, and the relation between them. Furthermore it includes the common parts of STORK documents, like risk management issues and acceptance criteria.

1.2 Scope

This document only describes the common functionalities of the STORK Platform. Specific functionalities, organisational and infrastructure aspects are to be determined by each member state.

1.3 Version control

This document describes the ***final*** view on the common functionalities of the STORK Platform. This means that, compared with the D5.8.2 document, this document has been updated with

- several minor changes due to comments by the reviewers.
- several minor changes and enhancements in the interface specifications (see detailed description in D5.8.3b)
- inclusion of the Software Design for the MW model (the D5.8.3e document)

1.4 Quality management & risk management

The most important topic within the quality is the assurance that all member states of this project agree on the contents of this document, and even those partners in the project who don't contribute to this WP. This assurance was already achieved in the previous version of this document (D5.8.2), and the updates have been verified by all member states between publishing the draft.

1.5 Glossary

The glossary can be accessed at the corporate STORK Website, clicking the following link: http://www.eid-STORK.eu/index.php?option=com_smf&Itemid=33&topic=42.0.

For readability, a brief enumeration can be found on page 6 of this document.

2 D5.8.3a Software Architecture design

2.1 Introduction

This document describes the architecture of the systems that compose the common functionalities of the STORK platform. This description is made from various points of view, each described in a separate chapter. The relevant points of view are applied to each of the two systems: PEPS and MiddleWare (MW), this last one including the Virtual IDP.

Each of these systems is described in a separate chapter subdivided in subchapters.

In the PEPS chapter, the view is by business process (Authentication and Certificate Validation). In next document (D5.8.3c) views by components and classes will be offered.

In the V-IDP chapter, the view is by components and classes, which are detailed and completed in the D5.8.3e document.

2.2 Methodology

The methodology is based on the *RUP (Rational Unified Process) 4+1* view model. This model considers 5 views as normally sufficient to describe a system, the first one being the use case view. Nevertheless, in different publications, different views are described for the other 4 views, although all agree on the most important one: the logical view.

In this logical view the system is divided in subsystems, and for each subsystem the different business processes (Authentication and Certificate Validation) are described. As agreed by all participants in WP5, attribute transfer is not relevant for the pilots, so will be done afterwards.

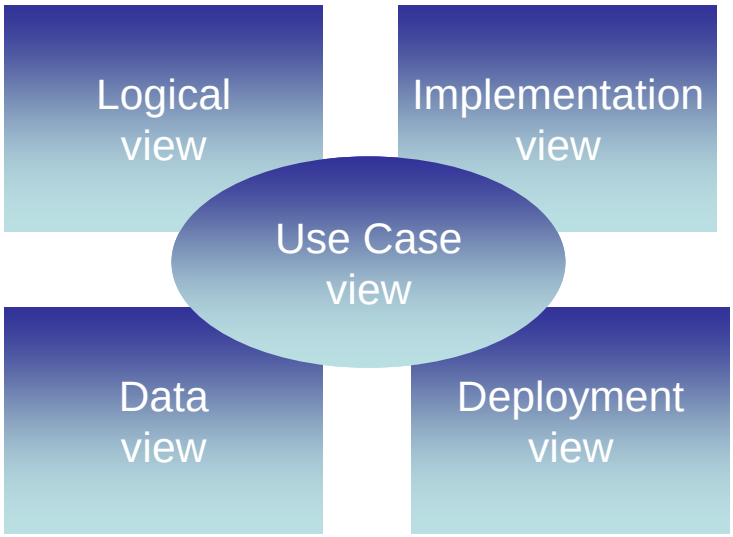

Figure 1: RUP 4+1 view model

2.3 System Context

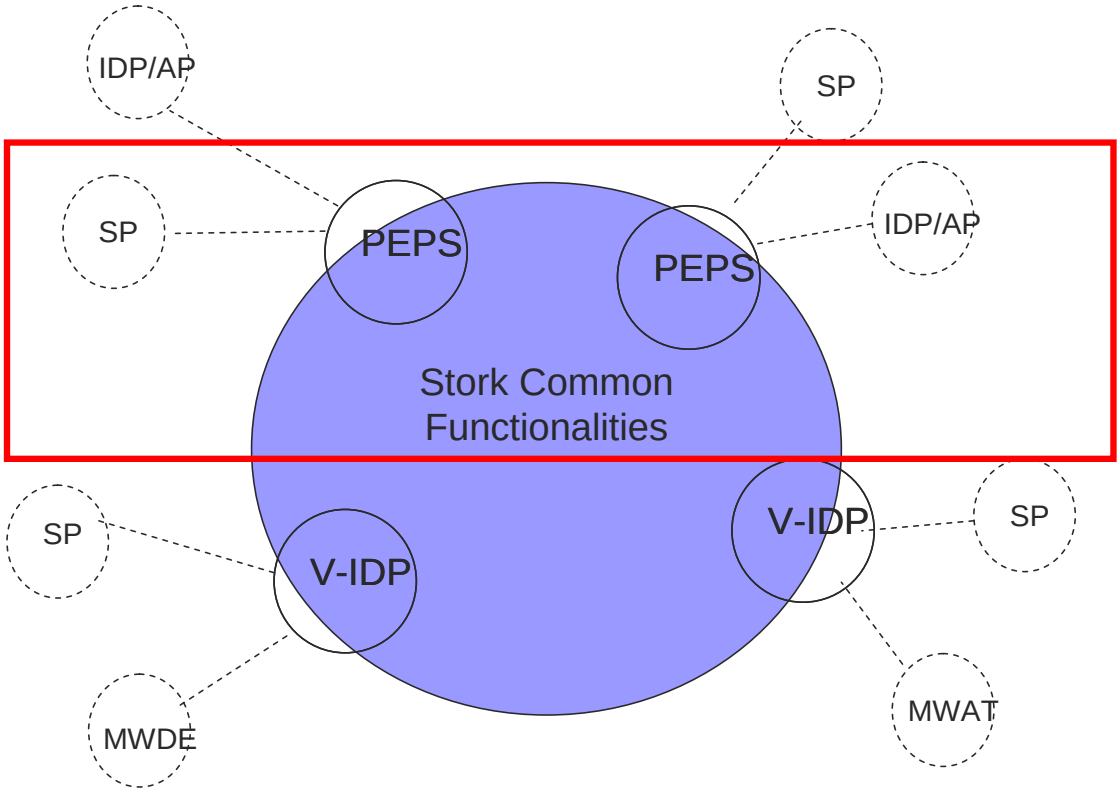

Figure 2: System Context Diagram

In each instance of a PEPS there are 2 roles: the one that attends to SP requests, and the one in the country which issued the ID of the citizen will use. Please note that the nationality of the ID issuer need not be the same as the nationality of the citizen.

For each received request, the first one forwards this request to his colleague PEPS or V-IDP, and the second (role of the) PEPS resolves the requests received from his colleague PEPS or V-IDP.

Each PEPS may include the functionalities which are specific to its member state, which are typically the interfaces with the local Id providers and attribute providers. On the other hand, the interface with Service providers (SPs) may also be different from one country to the other one.

But the communication between PEPSes and V-IDP, and the common functionalities are standard. This blue part of the above diagram, within the red rectangle is object of description in the PEPS chapter of this document. The communication between a PEPS and a V-IDP is the same as between 2 PEPSes.

The other important chapter in this document describes the V-IDP, which is in charge to translate the common communication to the communication agreed between the MW countries.

This system also includes both roles, attending requests from their SPs and forwarding them to the corresponding PEPS, as well as attending requests from PEPSes.

3 D5.8.3b Interface specification

This document is the interface specification for the STORK platform, whose aim is to achieve the interoperability of electronic identifiers all over the 14 participating states.

SAML 2.0 is the chosen messaging standard to be used between the STORK components (PEPSes and V-IDPs) in each member state. The STORK authentication request and response formats are defined. The STORK protocols (bindings and profiles) used by the STORK components to inter-communicate are also defined. Nearly the same protocol is defined for the communication between SPWare and V-IDP; those minor changes are indicated in the document.

Communicating information between states requires a shared understanding about what identity attributes are available and what each attribute means. A list of STORK attributes that each country may understand [but not necessarily provide] is defined.

4 D5.8.3c Software design for the PEPS model

This document presents the Software design of the PEPSes. It pretends to specify the behaviour of these components, in such a way that programmers can work with it.

The view which was offered by D5.8.3a, by business process, is now complemented with views by components and classes.

5 D5.8.3d Security principles and best practices

This document aims at the description of security requirements that have to be fulfilled by the interoperability layer developed in the STORK project, as well as practical recommendations to be implemented. As the STORK project is concerned with interoperability issues between governmental institution within the EU, personal data of EU citizens are processed, transmitted and temporarily stored by the interoperability layer. Hence, the assets to protect in STORK are personal information of citizens, issued by governmental or other institutions. Security in this context is concerned with the protection of these assets. A security-specific impairment of the assets typically includes the loss of asset confidentiality, loss of asset integrity or loss of asset availability. The STORK interoperability layer must provide sufficient security functions that counter the identified threats. This document gives a detailed description of identified threats, derived security objectives and necessary security functions that shall be implemented by the STORK system. The threats, objectives and functions define a sound set of security requirements to be fulfilled by the STORK system.

To find and describe security requirements, a methodology and approach is applied, conforming to the most accepted standard: the Common Criteria. First, the threats the system could face are given, which are partly motivated by known attacks. Then security objectives are derived from the identified threats and from requirements coming from the over-all project. Thirdly, security functions are defined that implement the security objectives and counter the threats. Lastly, the document gives some practical recommendations how to put the abstract security functions in practice. These security technical recommendations receive input from commonly accepted security mechanisms and best practices.

The security requirements which have to be included in the STORK common software has been brought in into the various discussions, and are thus integral part of the design (D5.8.3a up to D5.8.3c).

6 D5.8.3e Software design for the MW model

This document presents the Software design of the components of the MW model. It pretends to specify the behaviour of these components, in such a way that programmers can work with it.

The view which was offered by D5.8.3a, by business process, is now complemented with views by components and classes.

This document was elaborated after the construction of the V-IDP, as often during the construction additional tools, environments, etc. are decided to be included, which change the software design. For this reason this document wasn't part of the D5.8.1 and 5.8.2 documents.