Submitted to the EC on 30/04/2014

COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

Project acronym: e-SENS

Project full title: Electronic Simple European Networked Services

ICT PSP call identifier: CIP-ICT-PSP-2012-6

ICT PSP main theme identifier: CIP-ICT-PSP-2012-6-4.1 Basic Cross Sector Services

Grant agreement n°: 325211

e-SENS WP 5.2 eID Work Group: SD-DSS Change Request

Deliverable Id :	WP 5.2 internal
Deliverable Name :	SD-DSS Change Proposal and release
Version :	0.2
Status :	Draft
Dissemination Level :	Internal
Work Package :	WP5
Organisation name of lead partner for this deliverable :	FhGFOKUS
Author(s):	Soeren Bittins, Ben Kraufmann

Abstract:

Table of contents

1. Motivation

The e-SENS[1] WP 5.2 eHealth eID components are partially based on the FutureID client[2] as well as the Open eCard App[3]. With improving maturity of the e-SENS solution, concerns about the specific degree of reusability as well as licensing stability were raised by the work package management, stakeholders, and through piloting nations.

After investigating the available code portions, the FutureID client was found to be burdened by:

- proprietary, non-commercial, and non-OSS license for the eSign services that incorporates the OASIS Digital Signature Service[4]
- problematic linkage between a GNU Public License version 3 framework and proprietarily licensed software
- inability to evolve some portions of the client and its add-ins due to a closed code source
- prohibition of distributing some portions of the closed source code outside of the project

This primarily disqualified the e-SENS eID components to be freely handed over to the piloting nations (PN) as well as ultimately being merged with the CEF eHealth DSI. Without explicit permission, any further exploitation of eID by the PN outside of the e-SENS project scope or through a non-associated national organisation would also be hindered. Furthermore, the unavailability of the closed code portion slowed the continuous evolution of the eID solution, while the PN's were unwilling and unable to assume any potential liability or additional costs for acquiring the usage rights for those modules.

Consequently, the CEF eID group in collaboration with the e-SENS eID Task Force and WP5.2 recommended the integration of an officially sanctioned OASIS DSS tool, SD-DSS[5]. By substituting the eSign core technology with the solution provided by the CEF programme, the licensing issues can be mitigated by relying on an approved OSS license as well as sustaining the e-SENS eHealth eID solution by incorporating approved technology from the CEF eSignature Building Block[6].

However, the tool in its original form lacks critical features and compatibility for use with eID in the eHealth domain and had to be extended in order to fulfil the requirements. This documents outlines the changes as well as basic usage for the adapted SD-DSS for use within e-SENS.

The applied changes to SD-DSS, however, deviate from the stable development path of this external tool and it would be beneficial for the potential internal re-use of SD-DSS within e-SENS to outline a merge of the e-SENS adaption and the original development. This document is an informational only notice to highlight the changes and to propel a discussion on if and how a merging can be concluded.

The eSign core based on SD-DSS as well as the modified source code are published as OSS through e-SENS and integrated and made available in a prototype environment by the OpenNCP team.

---

[1] http://www.esens.eu

[2] http://futureid.eu/

[3] https://www.openecard.org/en/startpage/

[4] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

[5] https://joinup.ec.europa.eu/asset/sd-dss/description

[6] https://joinup.ec.europa.eu/asset/sd-dss/news/dss-now-provided-under-cef-programme

2. Issues and Changes

The e-SENS eHealth eID components rely on two different types of token to encode, transport, and validate the electronic identity of a given subject. JSON Web Token (JWT) are primarily used for the basic access means and do not carry any payload signatures. More advanced scenarios, in particular the providence of an epSOS Treatment Relationship Confirmation Assertion (TRC-A), employ a SAML Core version 2.0 compliant assertion featuring the signing format of an enveloped electronic signature. The following list of issues prevented the immediate integration of SD-DSS and motivated the described changes.

2.1. Signature Placement

Properly formed SAML assertions require the electronic signature to be placed as an "XPathAfter" the payload elements of the assertion in order to envelope the contents. OASIS DSS specifies two placement options configured through the <dss:SignaturePlacement> element, <dss:XPathAfter> and <dss:XPathFirstChildOf>.

The unmodified SD-DSS is placing the signature behind the root element of the SAML assertion only following the <dss:XPathFirstChildOf> notion, consequently breaking the schema adherence of the resulting signed assertion (a <ds:signatures> element must be placed right after the <saml:Issuer> element). This disqualifies any signature validation through the traditional frameworks or security appliances. The modified SD-DSS enables the correct signature placement through the addition of an "XPathAfter" option for SAML assertions.

2.2. Signing Transformation

Signatures in SAML are restricted towards acceptable transforms "other than the enveloped signature transform (with the identifier http://www.w3.org/2000/09/xmldsig#enveloped-signature) or the exclusive canonicalization transforms (with the identifier http://www.w3.org/2001/10/xml-exc-c14n# or http://www.w3.org/2001/10/xml-exc-c14n#WithComments).[7]"

When signing SAML assertions, SD-DSS offers and applies other transformations to the signature element. This burdens the validators and may cause otherwise valid assertions to be declined. The implemented change restricts the use of transformations and prevents incompliant transformations to be applied to SAML signatures.

2.3. Signature Element Reference

Valid signature placements in a SAML assertion must provide a value for the "ID" attribute in the root element of the signed assertion. The signature element itself must provide a singular <ds:Reference> attribute that holds the "ID" attribute of the signed assertion.

Although SD-DSS is populating the <ds:Reference> in the signature element, the contents of this attribute is not correlating correctly with the "ID" attribute of the assertion. This hinders an in-depth validation of the assertion as a validator cannot correctly link the signature and the signed artefact (assertion). This change is changing SD-DSS's internal processing to properly reflect the correct

[7] from: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0

correlation between the “ID” attribute of the SAML assertion and the <ds:Reference> within the signature element.