Technical Interoperability issues between of STORK and SAML eGov deployment profiles

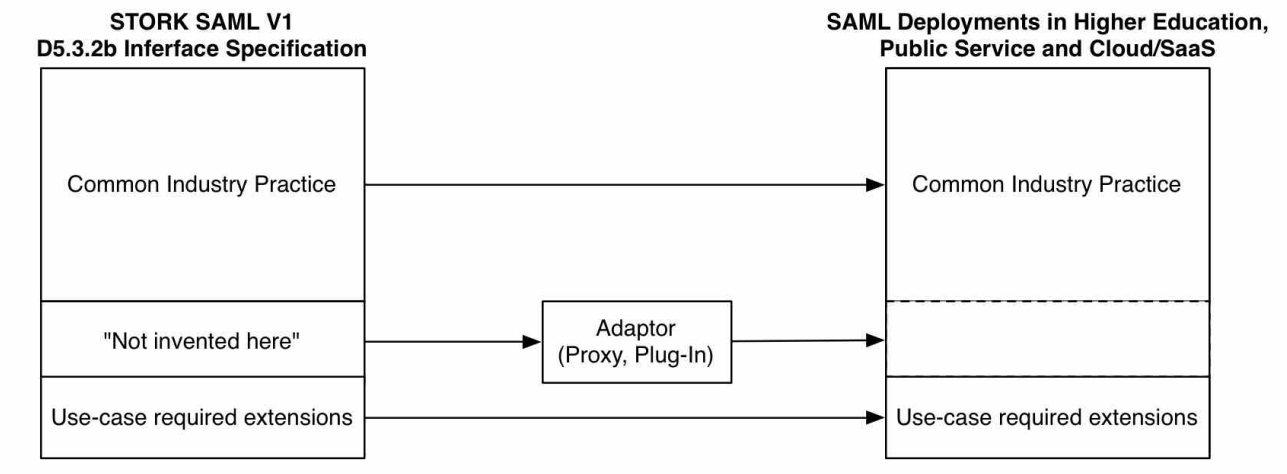
Author: Rainer Hörbe, Kantara Initiative eGov WG
Date: 22 June 2012 (2)

Summary

Summary

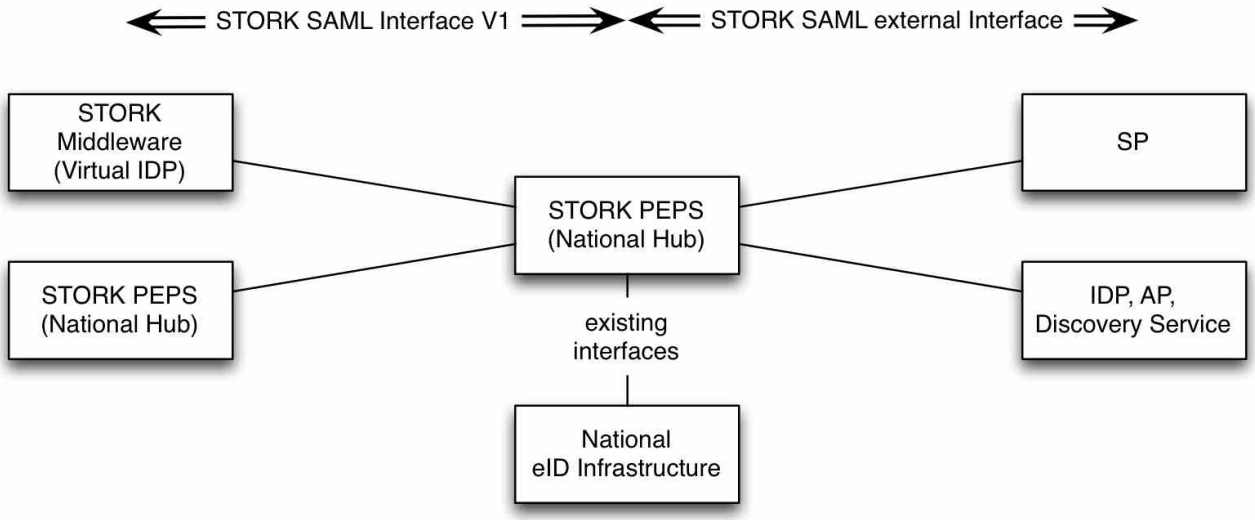
There is a significant potential benefit in making STORK interoperable with industry-standard SAML profiles. STORK could provide low-cost, high assurance eIDs, and the established SAML ecosystem could enrich STORK with a broad set of products, services and tools. This could help STORK to gain significantly faster access to existing federations.

While STORK is SAML-compliant in many respects, it had failed so far to use certain established SAML specifications - in particular the Kantara eGov Interoperability profile. Partially that is owned to use case specific conditions, partially that happened without compelling technical reason. This is no issue within the STORK cross-border infrastructure, but less desirable for the national interfaces.



The alignment of the STORK SAML interface towards SPs (and IdPs in a lesser degree) with industry standards should be pursued to promote the integration of STORK into existing and future federations, and to reduce deployment and operational cost. The goal of this effort is to achieve a technical harmonization that is depicted like this:

STORK's internal mechanics between PEPS and other actors that already use the STORK Interface spec would work unmodified. Towards other deployments STORK would provide a standardized interface that is easy to deploy and supported by a variety of products.



Background

The European Commission's DG INFSO set proliferation and interoperability of eIDs as a key target in its ICT work programme and have been funding several projects to promote the topic. The flagship project is the STORK large scale pilot that aims for providing cross-border interoperability between national eID schemes. For the technical protocol STORK chose SAML WebSSO as template and modified it to the needs of the pilot.

Kantara Initiative, as successor of Liberty Alliance, has been active in the area of SAML interoperability for many years. How did this come about? SAML was developed by OASIS as a very flexible framework that supports a broad field of use cases related to identity management. Some common ones were specified by OASIS, most prominently the Single-Sign-On (WebSSO) and Single-Sign-Out (SLO) use cases for web browsers.

However, these and other OASIS profiles are too general to make products fully compatible. This is where interoperability profiles step in. The most common interoperability profile is the Kantara SAML eGov Interop Profile. Several governments in Europe and elsewhere had derived deployment profiles based on the eGov profile. Deployment profiles specify configuration options and constraints for particular federations[1].

Problem Statement and Motivation

STORK's SAML interface specification for the integration of IdPs and SPs deviates in several points[2] from current industry practice, which is reflected in eGov and SAML2int profiles. Some points can be explained by specific conditions of STORK's core use case, the citizen to government authentication. For some other points the design decisions (which are not available to the public) are unclear and could be attributed to a lack of time and/or focus on interoperability with existing SAML practice and paraphernalia[3].

STORK 2 started in April 2012. It does not seem to address the improvement of interoperability with industry standards nor to facilitate the standardization with an SDO[4]. STORK 2 puts emphasis on expanding use cases from G2C to G2B and B2C types.

Interoperability between both protocols is desirable. A rich ecosystem of products, libraries, supporting tools and extensions exists that STORK deployments could tap into if technical interoperability would be improved. On the other hand, existing federations based on mature enterprise or OSS products could benefit from STORK, as it proposes a government-backed and low-cost solution with high-assurance credentials.

Options and Benefits

To fix the issues described above the STORK interface specification needs to be adapted. There are basically two options that take care of both existing pilots and future developments. One can decouple both protocols with a proxy or implement STORK in the existing product. Both options would benefit from better interoperability if STORK would be aligned with the industry standard.

Proxy-based Approach

A proxy translates between different protocols and shields actors on each side to be unaware of the differences of the communication partner. However, it does limit the functionality, because there is no motivation on both sides to align their protocols. Pitfalls might be in the operation of a federation, when setting up new actors, changing attribute policies.

Protocol-enhancement Approach

This approach attempts to create a superset of both protocols by minimizing the differences first, and allowing for all features for both variants. The obstacle of protocol enhancement is the resistance of vendors and users to any kind of change in products and production environments. However, if a clear benefit can be argued, changes can have success. The benefits of better alignment of both protocols would be:

---

[1] Besides the Kantara Profile the higher education sector adopted a similar deployment profile called SAML2int for the national research and education networks.

[2] A summary of differences is available at the Kantara wiki http://kantarainitiative.org/confluence/download/attachments/38929505/diff+eGov20+STORK.xls

[3] It might be attributed to the fact that STORK was driven more by legal than technical challenges, and SAML was chosen as protocol rather late in the process.

[4] SDO: Standards Development Organization like ISO, CEN, OASIS, ETSI and others.

- Federations will support both protocols out-of-the-box;
- All actors (like IdPs and SPs) could be managed with a single set of meta data;
- Tools and products like test suites, proxies and administrative consoles could be shared;
- Most significantly, any standardization at a common SDO working group would foster further alignment of the protocols, reducing future cost in making both worlds work together.

Benefits of Interoperability between eGov Profile and STORK

Identity federation is an area suitable for cooperation, even between otherwise competitive stakeholders. The reason is that there are no "killer business cases". Only a significant quantity of business cases sharing the IDM infrastructure can have success.

As cooperation in identity federation is beneficial on a business level, standardization is advantageous on the technical level. The resulting ecosystem will provide more products, tools, suppliers and service offerings that will drive economics of scale. In addition the export-oriented industry in Europe is better off with open standards, because this expands market opportunity.