NOBID METADATA PROJECT

Lessons learned

Abstract

This is the final report of the NOBID metadata project. This project was carried out during 2020 to determine whether eIDAS node trust configuration can be enhanced by a centralized metadata service.

All services and tools used in this project has been provided by IDsec Solutions Sweden (https://idsec.se) under contract with NOBID.

Stefan Santesson

stefan@idsec.se

IDsec Solutions

2020-11-26

Executive summary

The NOBID metadata project has successfully demonstrated the benefit from a centralized metadata service to support maintenance of trusted keys between national eIDAS nodes.

The benefits are:

- Less burden on member states to maintain services
- Increased security
- Reduced service disruptions in the eIDAS network

The recommendations of this project are that member states should be given the necessary tools to export their trusted keys in a trustworthy manner using the **Metadata Service List** (MDSL) format or using the PKI model as specified in the eIDAS technical specifications. It is however recommended to fix shortcomings in the PKI model specifications in next release of the technical specifications, or to rely on MDSL only.

Secondly this project recommends that the EU commission assumes the task to provide a central metadata service that can be used by national eIDAS nodes to enhance trust configuration of eIDAS nodes from other countries by just having to bootstrap the signing key of the central metadata service.

Background

Problem statement

One of the hardest problems to overcome when setting up a network of trusted services is to define a security process for how to bootstrap trust anchor keys. A trust anchor key in this context is a key that is not verified by another pre-existing and securely exchanged trusted key. In this context the trust anchor is a key that needs to be manually exchanged and manually verified by authorized administrators. Once the trust anchor is installed, any future key exchange can be verified by that trust anchor key for as long as it is used and trusted.

Secure exchange of trust anchor keys often comes with the cost of significant administrative burden. This becomes increasingly harder if the relationship with the counter party from which the trust anchor is received, isn’t based on a well-established procedure delegated to known and authorized individuals.

It is today a well-established practice in complex infrastructures of mutually trusted services, to reduce the number of trust anchor keys as much as possible, ideally to a single trusted key through which all other keys can be verified. In fact, it has been demonstrated that security increases with fewer trust anchor keys for the simple reason that it is harder to replace a single trust anchor key with a fake key without this being noticed and detected almost immediately. It is quite a lot easier to replace a key that is used in a more limited context in a way that may pass unnoticed. This fact is proven over and over again in public environments such as large identity federations, web-trust and in global infrastructures such as the DNS system.

The eIDAS node environment is an environment where exchange of trust anchor keys is both problematic, time consuming, and challenging to perform in a secure manner. This is mainly caused by the following factors:

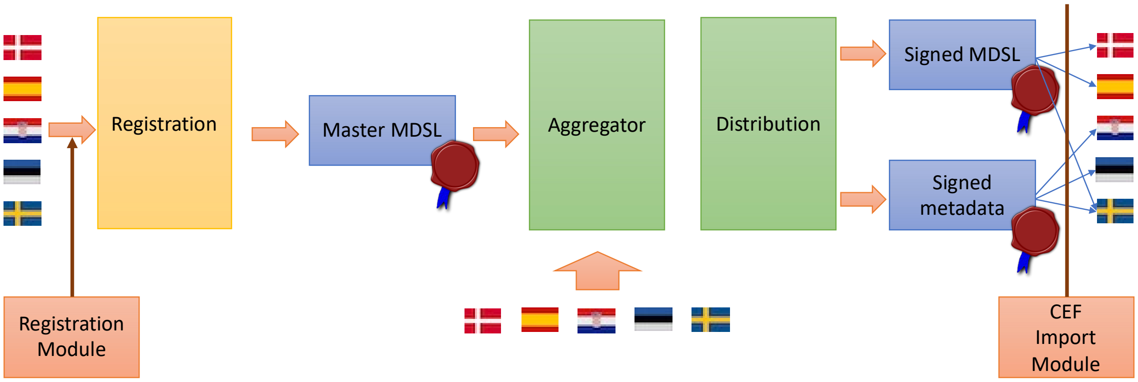
- Several eIDAS nodes from well over 30 member states need to exchange trust anchors bilaterally. This results in well over 1000 individual instances of bilateral manual key exchanges.
- It's hard for each member state to maintain knowledge about authorized representatives from each participating member state and to keep track of when people retire, change roles or just have their authorization revoked.
- Lack of key rollover procedures and capabilities in deployed software products cause service disruptions each time a member state eIDAS node changes its keys.

Mission

The mission of the NOBID metadata project is to demonstrate how a modern metadata service can be applied to drastically reduce trust anchor bootstrapping burden on participating countries and at the same time increase security and reduce service down time.

Metadata service environment

The building blocks of the NOBID eIDAS metadata infrastructure are illustrated in the following schematic:



The central metadata service is composed of the following components:

- **Registration component**: This is the service responsible for collection of data from participating member states. This module collects and store all data necessary to aggregate metadata from each country. The output of this module is the Master MDSL.

- **Master MDSL**. This is the collective configuration data used by the Aggregator necessary to continuously download and validate current metadata from each country. This use the MDSL data format defined in the eIDAS technical specifications version 1.2.
- **Aggregator**: This component collects and validates metadata from each country based on the Master MDSL.
- **Distribution component**: This component distributes aggregated and validated metadata and signed MDSL information to participating eIDAS nodes to support their security configurations.

The central service based on these collective components follow established specifications for the aggregation and distribution components as well as for the MDSL format. The functionality of the registration component is however a matter for further study within this project due to a lack of trustworthy and agreed procedures for exchange of keys and other security critical data. Current procedures using e-mail and wiki pages for information exchange should be replaced with procedures and technical formats that meets the requirements for trustworthy data exchange by participating countries.

Similarly, the data output formats of the distribution component is well specified, but the manner in which national eIDAS nodes is consuming this information will be a critical task to address within this project. A number of problems must be addressed such as:

- CEF code is deployed currently using both 1.x and 2.x versions. A solution must probably work for both versions.
- Current CEF code use a common key store both for the service private key as well as trust store for trusted metadata signing keys used to verify metadata from other nodes. A module updating this trust store must therefore have access to the most security critical data component.
- A solution to the former point may be to change the CEF code instead of just altering configuration data, but this may create problems with future updates of the CEF code.

Two components are defined to address the needs related to registration and consumption of distributed metadata:

- **Registration Module**: A module that would allow a country to distribute configuration data in a suitable format in order to minimize the amount of data that have to be exchanged using a manual registration process as well as the frequency at which this data must be updated manually. This format is presumably the MDSL format but could also be a complete Metadata feed for all national eIDAS nodes or something else defined in this project.
- **CEF import module**: This is a configuration component that is either a code plugin for an eIDAS node based on the CEF software, or a separate configuration component assisting a standard unmodified CEF node. This component uses the output from the metadata service to automatically update metadata configuration for a defined set of countries.

This metadata service is available at: https://md.eidas-trust.com

Tools

The NOBID metadata project developed and provided a "CEF import module" as described above, for integrating eIDAS nodes based on the CEF eIDAS integration packages with the NOBID metadata service.

Integration tools for eIDAS node versions 1.4.5, 2.3.1, 2.4.0 and 2.5.0 are available from https://github.com/idsec-solutions/nobid-mdimport

Once installed with the CEF eIDAS node, these modules allow the eIDAS node to verify and collect trusted metadata signing keys from selected countries from the metadata service. This completely eliminates the need for manual key exchange with eIDAS nodes in those countries. This module also handles key updates so that, in case a country updates it's metadata key, the new key will be imported, verified and installed automatically by the participating eIDAS nodes without any service disruption.

Test results

The test of the metadata service was performed with eIDAS nodes from 6 real and/or fictious countries:

- SE – Swedish eIDAS nodes using the Swedish eIDAS node software for proxy service and connector
- EE – Estonian proxy service and connector test nodes
- FI – Test nodes from Finland
- XA – Test country using CEF node version 2.4.0 and later 2.5.0
- XB – Test country using CEF node version 2.3.1
- XC – Test country using CEF node version 1.4.5

All participating nodes installed the "CEF import module" provided by the project except for the SE nodes who have native support for metadata source such as the NOBID metadata service.

All tests were successful, demonstrating successful automated import of trust anchor keys for all participating country nodes after bootstrapping trust with the NOBID metadata service.

Demonstration videos:

- XC (eIDAS node 1.4.5) to EE proxy : https://www.youtube.com/watch?v=9WyD6oDKwcs
- EE connector to XA proxy (CEF 2.4.0): https://www.youtube.com/watch?v=D5cL7L_7Elo
- EE connector to XC proxy (CEF 1.4.5): https://www.youtube.com/watch?v=OZ5vvCGfWqw

A test was also conducted where XA, XB and XC had its metadata and service keys updated and where the XA node was updated to version 2.5.0. Tests confirmed that key rollover was achieved without service disruption.

Conclusions and recommendations

The NOBID metadata project confirms that a centralized metadata service can be used to:

- Materially reduce the burden of trust anchor bootstrapping between eIDAS nodes.
- Materially reduce downtime and service disruptions caused by node key change

Metadata and keys stored in the NOBID metadata service was updated manually in this project. This is not considered a sustainable solution in the long run. A more stable and sustainable solution for member state reporting of key updates is needed.

One such method was tested in the NOBID metadata service where trusted keys from SE nodes were imported from published and signed MDSL (Metadata Service List) according to the eIDAS technical specifications version 1.2. If all participating member states would publish information about national nodes and keys to verify metadata for these nodes using MDSL, then a central metadata service could use that information to automatically update trusted keys from these countries.

Adding these results indicates that the progression of enhanced trust anchor exchange could be achieved in two steps:

- **Step one** – Participating member states publish signed MDSL for national nodes
- **Stop two** – Establishment of a central metadata service

Note: As an alternative to MDSL, participating member states could also offer a PKI where all metadata signing certificates can be verified to a common root that are exclusively used to verify eIDAS node metadata signer certificates. This solution does however currently lack some level of standardization, such as how to bind a certificate to a metadata entity and to the role (connector or proxy service). This should be fixed in future releases of the eIDAS specification. Until then we recommend using MDSL.

To provide the best experience for member states eIDAS nodes and thus for the citizens of member states using them, the project recommends that:

- The EU commission takes lead to establish a metadata service to which member states continuously can report their current metadata signing certificates.
- The EU commission update the CEF eIDAS node software to support export of metadata signing certificates to the central metadata service as well as import of metadata signing certificates from other member state nodes from the central metadata service.