Contribution ID: **9** Type: **Long Talk**

Establishing and Verifying Trust for Data Products and Processing

Thursday, 3 October 2024 09:40 (20 minutes)

Establishing and Verifying Trust for Data Products and Processing

Motivation and Challenge

In today's infrastructures, the collection, exchange and continues processing of geospatial data takes place at pre-defined network endpoints of a spatial data infrastructure. Each participating operator hosts a predefined static functionality at a network endpoint. Some network endpoints of an operator may provide data access, other endpoints may provide processing functionality or uploading capabilities. Security context constraints are fundamental for installing services in production environments. Several legislations from security technical implementations guides to information security policies apply. Recent legislation like EU Data Act entered into force on 11 January 2024, and will become applicable in September 2025. Because of this regulation, connected products will have to be designed and manufactured in a way that empowers users (businesses or consumers) to easily and securely access, use and share the generated data. The EU DSA Data Service Act states applicability for simple websites, Internet infrastructure services and online platforms.

Approach

Our novel approach introduces an agile decentralized eco-system that is concerned with trust and authenticity by introducing Smart Certificates which can be applied to data products, workflow processes and services. The Smart Certificates enable the flexible and trustworthy creation, distribution and verification of data products. The certification process can either take place manually or automatically if the data has appropriate Identity-Integrity Provenance and Trust I2PT-enabling metadata.

Our approach differs from well-known X-509 certificates by schema definition of the information contained in Smart Certificates. The schema - hence the structure of the certificate - is stored on a Blockchain to become immutable. Supporting Zero-Knowledge-Proof as well as requesting information from the certificates during the verification procedure supports a wide range of use cases.

Example implementation: The Satellite Imagery Reprojection

For illustrating the use of Smart Certificates, a process - Reprojection - allows a user or a workflow engine to reproject an image for which the user has a Smart Certificate. For the output image, the process creates a Smart Certificate. The process itself is verifiable because it also has a Smart Certificate associated. The bundling of image data and Smart Certificates allows the process to check for authentic input but also to verify the usage of the image. If the usage is not appropriate for the trusted process, the execution in refused.

The Trusted Reprojection process was implemented in Python and deployed using the OGC API Processes Standard and a modified version of pygeoapi. The deployed process validates the input image Smart Certificates and creates a Smart Certificate for the created output product - the reprojected image. The Hyperledger Indy Blockchain and Aries Cloud Agent are used as the backbone.

Conclusion

Our approach introduces trusted computing in a distributed environment by leveraging Hyperledger Indy, Aries Cloud Agent and specific business logic. The solution can be used to verify and issue Smart Certificates for data products and trusted processes. The introduced eco-system is one example solution to support the EU Data Act.

Topic

Trust and Security: Trusted computing:

Primary author: Dr MATHEUS, Andreas (Secure Dimensions GmbH)

Co-author: Dr COLAIACOMO, Lucio (European Union Satellite Centre)

Presenter: Dr MATHEUS, Andreas (Secure Dimensions GmbH)

Session Classification: Trust & Security