CYBERNETICA

Integrating Sharemind HI into UXP

Version 1.0
21.01.2022

Table of Contents

1. Glossary

DCAP - Data-Centric Audit and Protection.

PET - Privacy-Enhancing Technologies.

SDC - Statistical Disclosure Control. SGX - Trusted execution environment (TEE) technology provided by Intel.

Sharemind HI - Sharemind HI (Hardware Isolation) is a software product provided by Cybernetica AS. It provides runtime encryption based on Intel SGX TEE.

TEE - Trusted Execution Environment.

UXP - Unified eXchange Platform is a software product provided by Cybernetica AS. It enables peer-to-peer data exchange over encrypted and mutually authenticated channels.

2. About This Document

This document describes the value proposition of Sharemind HI integration into UXP system. UXP (Unified eXchange Platform) is a software product provided by Cybernetica AS that enables peer-to-peer data exchange over encrypted and mutually authenticated channels. See reference [UXP homepage] for more information. This document discusses the circumstances where UXP customer can benefit from Sharemind HI. Two sample business cases and related customer challenges are described.

A simplified diagram of deployment describes combining Sharemind HI and UXP in a solution. The deployment diagram covers both sample business cases.

Proposed products and services are listed. Last chapters explain the combination of Sharemind HI and UXP addressing the challenges customer may have.

3. Introduction — Situations Worth Adding Sharemind HI Into UXP Solution

For IT solutions processing sensitive data, Sharemind HI addon for UXP creates an extra trust and helps to govern it. Sharemind HI is not required in cases when a sufficient trust level can be achieved with standard IT techniques. Such a situation is characterized as follows:

- All data owners trust the computations process "as is".
- Administrators of the IT systems can be trusted up to the level they have full access to the data and the processing pipeline.
- No legal constraints
- Reputation and financial risks have been evaluated as of low probability or not leading to significant damages.

If at least one of the conditions above is not true then Sharemind HI might be the answer. For

example:

- Data sources are from different owners. Each owner wants to retain full control over the data accesses, including the possible revocation of these at any moment.
- A requirement is raised the data processing pipeline should not be directly accessible by anybody.
- The presence or absence of each step of data processing or computation is required to be fully provable later.
- Direct or indirect costs of a possible data breach are estimated as too high.

These are typical challenges in data driven e-government domain.

3.1. Data Driven e-Government Activities

A data-driven government focuses on applying data to generate public value through three types of activity:

- Anticipation and planning – using data during policies design, while planning the interventions, or anticipating of possible change and forecasting the needs.
- Delivery – using data to inform and improve policy implementation, to improve the responsiveness of governments and the provision of public services.
- Evaluation and monitoring – using data to measure impact, to audit decisions and monitor performance.

The common challenge in achieving these goals is to respect the data rights of citizens, ensure transparency of usage, guarantee the security and the protection of privacy of data. For more discussion of challenges in this domain see "The OECD digital government policy framework: Six dimensions of a digital government." [Ubadi 2020, p.15]

4. Business Cases

In Business Case #1 all interactions with Sharemind HI are batch processing the tasks initiated by UXP member organizations. In Business Case #2 the pivotal actor is an individual patient exercising personal control over private data.

4.1. Business Case #1: Applying Data to Predict Health Service Needs

Hospitals have to treat emergency patients within a specified time period according to the applicable medical service standard.

Involving the patient-level historical data from hospitals, an analysis of big data can predict the expected patient load, the medical urgency and specialty, and the number of admitted and discharged patients. The analysis tools can be expanded to predict spreading of diseases such as influenza/Covid and hospital admissions of patients with chronic diseases. Applying Sharemind HI enables to reach these goals without affecting patient privacy.

The business case description is based on "Australian" example from section "Data-driven

country practices"[Ubadi 2020, p.18].

4.2. Business Case #2: Situation Analysis on Personal Level

In this usecase the citizens create a digital twin of themselves and manage their own data. The data is used to create situational profiles for context-aware personalised services. For example, during pandemics one could get warnings when exposed to high risk of infection. Other kinds of person level analyses and alerts are beneficial too, like disaster warning based on actual profile of the person, personalized medicine.

For this kind of analysis, one has to combine the diverse sources of sensitive private data, e.g. a close contact with an infected person could be detected by using individual geographical trajectory data from mobile positioning, bank card usage locations, public transport usage, and patient health records as inputs.

High barriers exist to this kind of an analyse due to legal regulations, risk of leakage of sensitive data, as well as perceived or real risks of privacy violations from authorities.

People tend to be more cooperative with data-driven solutions when the system is transparent and they retain sufficient control over usage of their private data. If these conditions are satisfied, a significant value is generated for individuals themselves.

The business case description is inspired partially by "AuroraAI (Finland)" example of data-driven situational profiling proof-of-concept solution [Ubadi2020, p.18].

4.3. Customer Challenges Related to the Business Cases

Customer challenges in described business cases fall into following categories: * Consolidate data using a trusted channel.

- Have transparency of what data is exchanged and processed.
- Analyse the consolidated data in a privacy-preserving way.
- Ensure conformance to legal regulations.
- Audit the whole process.
- Provide individual persons with direct control over usage of their personal data.

The chapter How UXP+Sharemind HI solution addresses customer challenges below provides more detailed explanations about solving these challenges.

5. Our Product Proposal

Our solution is comprehensive—we propose the software and also a strong support to the customer while creating full custom solutions together with the processes and necessary documentation. Sharemind HI is novel and knowledge-rich, thus at least some consulting will be needed during the first Sharemind HI projects of the customer.

5.1. Products

- Sharemind HI Software framework enabling to conduct "trust-critical" data processing
- Business process templates and sample process descriptions
- Contract templates and sample documentation

5.2. Services

- Consultation on Organisational Governance and Data Governance
- Cybersecurity consulting
- On request—implementing custom functionality using PET.
- On request—analysing cybersecurity of customer IT assets, penetration testing.

6. Example: Deploying Sharemind HI and UXP Into a Solution

On Figure 1 below the following situation is depicted:

- 3 Organisations A,B,C export data into a Sharemind HI server.
- Organisation B also hosts the Sharemind HI server in this example.
- All organisations are UXP members and communicate via UXP to get maximum transparency of what data is exchanged and processed.
- A web application server is hosted by organisation A accessing the Sharemind HI server via UXP.
- Citizens use a web-based application and initiate requests to Sharemind HI server. These Sharemind HI requests are formed and forwarded by the web application server. TEE technology guarantees that the private data from citizens is decrypted and processed strictly inside TEE by the audited software and nobody can see the uploaded personal data in clear, not even the administrators of the servers that host the solution.
- The organisation C hosts also a Report Generator application that uses Sharemind HI server as a backend for sensitive calculations.
- Organisations A, B exchange larger datasets with Sharemind HI server. Large encrypted data transfers can bypass UXP for optimization purposes. The organisations can request data transfers to/from Sharemind HI server via UXP and Sharemind HI can connect to the data service in organisation.

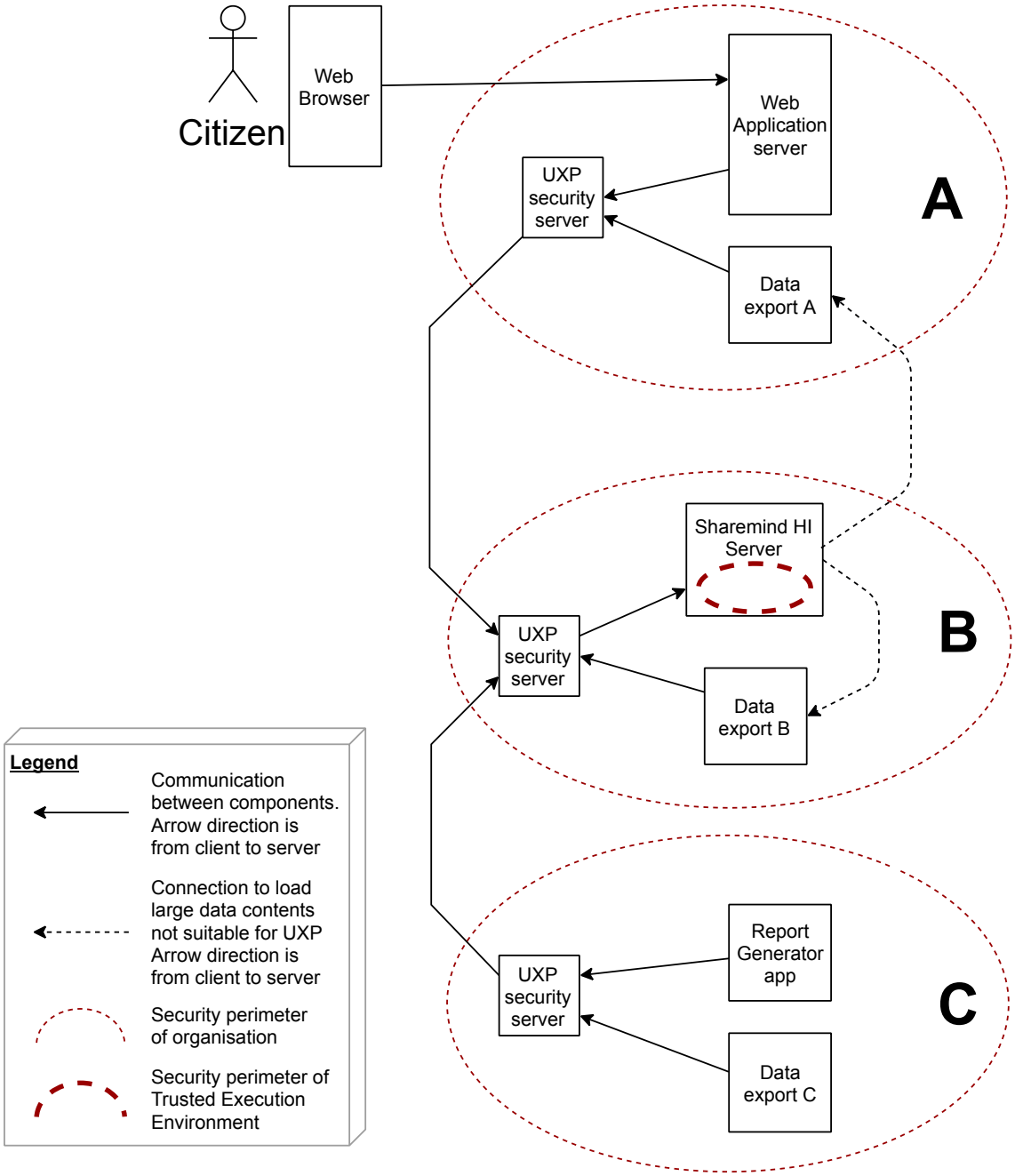

Figure 1: Simplified component diagram. Only connections related to Sharemind HI scenario are shown.

7. How UXP+Sharemind HI Solution Addresses Customer Challenges

7.1. Consolidate Data Using a Trusted Channel

UXP is targeted at situations where several parties wish to establish a standardized communication mechanism that provides confidentiality, strong authentication and long-term proof value of the relayed messages.

Sharemind HI as a consolidation endpoint provides extra layer of protection by applying hardware assisted TEE technology to enforce a controlled access to data and code and to ensure the authenticity of a server. Even during the computations, data are protected by hardware-assisted extra layer of security.

Combination of UXP and Sharemind HI provides tools to handle data in move and data in use.

7.2. Have Transparency of What Data is Exchanged and Processed.

- UXP has a set of strong cryptographic features to provide a long-term proof value of the relayed messages.
- Sharemind HI has an audit log providing cryptographically strong proof of the performed actions.

Together these two layers provide the full proof of activities.

Strong security guarantees and transparency of auditing can be leveraged also in public relations, to convince the public that the system really is privacy-preserving and the declared data processing policies really can and will be followed.

7.3. Analyse the Consolidated Data in a Privacy-Preserving Way.

Sharemind HI ensures that only the computations pre-agreed among the owners of the linked data sources can be run on the data. This way the processing algorithms will remain transparent for data owners while the data is kept secret and secure.

7.4. Ensure Conformance to Legal Regulations

The product can help compliance analysis in two ways:

1. Legal analysis shows that the data that is protected by means of such rigorous properly audited TEE mechanisms provides the legal reasoning for treating this data as anonymous, see reference [Siil 2021, p27] which is a result of legal analysis performed by Cybernetica AS upon the request of Eurostat. Less stringent legal regulations are applied to processing the anonymous data, compared to pseudonymized or personally identifiable data. Also, the participating organisations will have more trust if the security is built in by design and is based on proven strong cryptographic methods and corresponding certification and auditing processes.
2. The customer can create its custom solution based on ready examples and the compliance analysis templates provided as a part of the product. Cybernetica AS can also provide the support during the design and launch phases of the solution. This way the customer can benefit from the expertise and long-term experience of Cybernetica AS in the field of cyber security.

7.5. Audit the Whole Process

UXP has built-in the mechanisms to audit all the data exchanges. Sharemind HI has built-in mechanisms for auditing data processing. Both of them provide strong authentication and a long-term proof value of the activities.

7.6. Provide Individual Persons with Direct Control over Usage of Their Personal Profile.

UXP provides a central easy-to-integrate consent registry, where consent preferences of individual users can be registered. UXP can enforce these preferences in UXP communication.

Sharemind HI provides means to create solutions where private data can be processed and stored inside TEE in a way that nobody has access to it except the persons themselves.

8. Effects on Operations

8.1. Data Transfer

The number of expected queries as well as the data volume associated with a query are a subject of moderation in UXP. For productivity reasons, the large bulk data transfers initiated by UXP can be redirected to bypass the UXP security servers (as indicated on Fig 1 above for organisations A,B).

8.2. Data Governance

A new class of data protection is to be introduced—data visible only inside of a TEE. With Sharemind HI, the administration and cyber security risk analysis are performed as usual, taking into account these new possibilities.

8.3. API Governance

UXP API governance principles are used to access the Sharemind HI server(s). Sharemind HI server internally authenticates and authorises the requests according to the business logic implemented and audited in Sharemind HI. Sharemind HI performs logging of the request layer and optionally that of an application. These logs duplicate and complement the UXP logging.

8.4. Security

The organisation has to set up the processes and perform the installation of the solution. It also has to set up the update procedures as these are essential for the continuous reliance on the Sharemind HI trust model.

Monitoring security notifications from Intel and installing the security-related Intel CPU firmware upgrades are mandatory.

Connection to a remote Intel Attestation Server is necessary or alternatively, an SGX DCAP service must be maintained internally.

8.5. End User Privacy

In case of using a TEE, some tasks of the personal data processing can be considered as anonymous data processing. Therefore, the solution with Sharemind HI can reduce the burden of acquiring consents from end users.

8.6. Auditing

There is a certain overhead as the solution requires an involvement of an auditor and all stakeholders. Clear guidelines are provided for auditing a Sharemind HI solution.

8.7. Agility

Sharemind HI must obey full trust from each stakeholder, thus any code update code needs an audit by the security auditor and approval from all the stakeholders. Therefore, initiating and updating the processes with Sharemind HI involve extra steps compared to usual installation practices without TEE protection.

8.8. Productivity

Designing highly secure software requires specific techniques. Producing new code for Sharemind HI tasks is somewhat slower and requires special skills.

During the deployment and launch phases the extra efforts needed mainly are: auditing the code, securely transporting the certificates of each stakeholder, approving the solution. All these steps, with the exception of auditing, can be semi-automated and require only a short interaction from each stakeholder.

8.9. Resilience

The solutions involving Sharemind HI can be configured with load balancing facilities that provide horizontal scalability and high availability.

Sharemind HI does not affect the resilience of other processes that do not use Sharemind HI.

9. References

- Siil, Triin. "ESTAT 2019.0232 Data Protection Impact Assessment – Evaluation Report" (2021)
- Ubaldi, Barbara. "The OECD digital government policy framework: Six dimensions of a digital government." (2020). https://www.oecd-ilibrary.org/deliver/f64fed2a-en.pdf?itemId=%2Fcontent%2Fpaper%2Ff64fed2a-en&mimeType=pdf
- UXP homepage. https://cyber.ee/products/secure-data-exchange/