Unified eXchange Platform (UXP)
White paper

April 12, 2018

12 pages

1 Background

The Unified eXchange Platform (UXP) is targeted at situations where several parties wish to establish a standardized communication channel that provides confidentiality, strong authentication and long-term proof value of the relayed messages. The model case for this situation is a **governmental data exchange infrastructure**. Here the communicating parties are governmental agencies, private companies and citizens who exchange data with each other by calling services (service-oriented architecture).

When connecting existing organizations operating under existing laws, it is imperative that the service providers retain control over their systems and data. In UXP, the service provider maintains and enforces an access control list for each service (the access control list handles request authorization on an organizational level, see Section 3.1 for details). Before using a service, the service client and service provider enter into an agreement that specifies the liabilities for both parties. On one side, the service provider agrees to provide a service with a given Service Level Agreement. On the other side, the service client agrees to use the service and process the received data according to the conditions defined by the service provider. This system allows service providers to control how their data is processed and fulfill their legal obligations (such as conformance to data protection laws).

In order to make connecting organizations simple and cost-efficient a unified set of standards should be developed. This is cost efficient because an organization does not have to implement a different standard for each communication partner. By implementing support for a set of protocols, it is possible to communicate with any number partners who are connected to the UXP. In UXP, standardization happens on two levels. First, all communication is implemented as SOAP or REST web services. For SOAP, WSDL (Web Services Description Language) is used to describe services. Using standard interfaces ensures that adding another communication partner does not involve major software development effort. However, the actual messages are defined by each specific application. Second, organizations must implement a standardized security solution and a set of security protocols. In order to ensure consistently high quality and a high degree of interoperability, all the UXP members use standardized security components, called **security servers**, developed by the central authority. The standardized security components are deployed at the member organizations and completely encapsulate security aspects of the UXP infrastructure. The application developers can thus concentrate on implementing the application-level protocol without getting involved with the security aspects of the communication.

The security requirements for this kind of communication are quite high. The exchanges usually contain personal information and are subject to regulation (for example, transmitting medical information is highly regulated). The communication between members must use

end-to-end encryption so that the private information is not revealed to any intermediaries. Some transactions are high value, such as making query to the social security database before paying out a disability pension. The exchanged messages should be usable as evidence in the court of law. Thus, there is need for **qualified signatures** issued using hardware signature creation devices and certificates from accredited certification service providers.

Given that the business processes depend on the data exchange infrastructure, the **availability** requirements are quite high. In particular, there cannot be any component that could potentially become a single point of failure or a global performance bottleneck. If two parties in the system have established a communication context, then continuing the communication should not depend on availability of other components (limited only by the expiration of cached information). Additionally, it must be possible to use redundancy and load balancing for critical components to ensure smooth functioning of the infrastructure.

With a governmental data exchange, the number of communicating parties can be quite large. Coordinating this communication requires presence of a **governing authority**. In addition to establishing standards for communication, the governing authority is needed to create and enforce standardized security policies and to provide technical support (such as standardized gateway software or public key certificates) to members of the infrastructure. In case of disputes, the governing authority may act as an arbitrator.

If several countries deploy compatible data exchange infrastructures, **cross-border services** become a possibility. This means that it is possible for a member of the infrastructure to call a service of a member of another infrastructure. In order to accomplish this, the governing authorities of the infrastructures must enter into an agreement to establish a trust relationship between the infrastructures and mutually agree to trust the trust service providers of the partner. When the agreement is made and the technical information is propagated to the members, the members of different infrastructures can communicate directly and securely.

The governmental data exchange infrastructure uses all the features of the UXP. When scaled down (wrt. both features and administration procedures), UXP can also be used to connect organizations joined to form a community or consortium, or even to connect separate information systems inside a single organization. In these cases, the policies and administrative procedures (e.g., adding a new member to the infrastructure) can be implemented in a simpler, faster manner or omitted altogether.

2 Overview of UXP

2.1 Basic Infrastructure

The UXP system provides solution to the situations described in the previous chapter. Next, we will describe how the UXP works by building the solution step by step.

In the simplest case, the system has the following participants (see Figure 1):

- **Members** – entities that wish to communicate with each other. The assumption is that each member has an information system that will be connected with other members' systems.
- **Governing agency** – coordinates communication activities, creates and distributes security policy, maintains and distributes registry of members, distributes gateway software (see below).
- **Trust service providers** – provide certification and time-stamping services. In the simple case, the trust services can be provided by the governing agency.

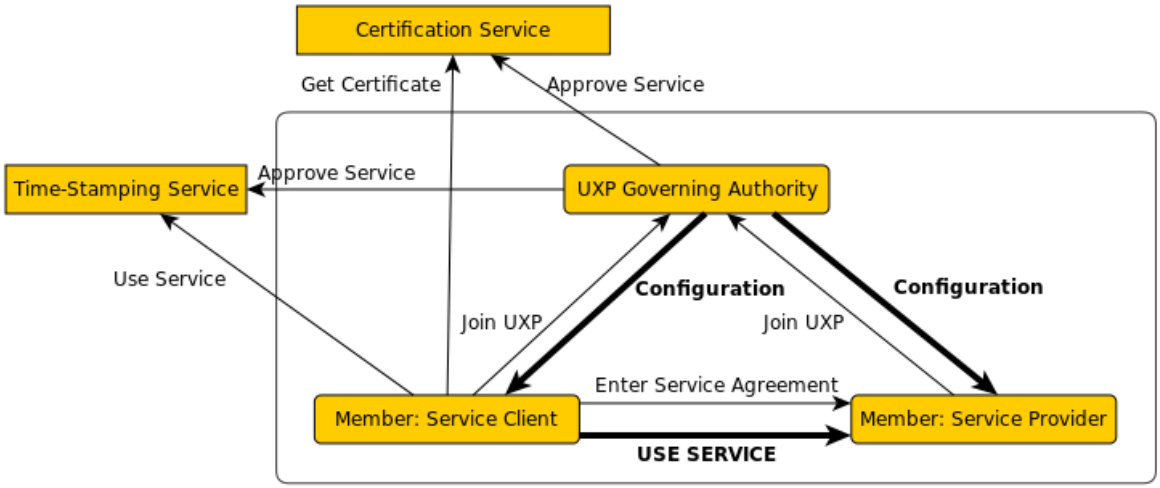

Figure 1. Participants of the UXP system

In the UXP the communication is organized as synchronous **service calls**. The service providers design and implement services and make them available for service clients. Access to the services is controlled by service provider. In order to use a service, the service client and the service provider enter into agreement that specifies the terms of the service, the service level agreement (SLA) offered by the provider, and the security requirements that the client must meet in order to use the service. When this is done, the service provider

adds the client to its access control list. The UXP system provides the technical means to manage the access rights of service clients. Different infrastructures can have different rules for providing access to services (e.g. a lightweight informal process for a corporate infrastructure or a pilot environment or a formal process with formal service usage agreements, that state the service levels, conditions and obligations of the parties).

In the UXP system, members **communicate directly** without intermediaries. All the messages (requests and responses) are **signed** and **time-stamped** and sent over **encrypted and mutually authenticated channel**.

The governing agency does not take part in the actual message exchange. Instead, it acts as a coordinator and facilitates the communication by

- defining a list of trusted certification service providers and time-stamp providers,
- managing a member directory,
- optionally maintaining a directory of services offered by service providers,
- monitoring the system to help debug any problems and to collect data for planning purposes,
- maintaining and distributing the security security server software.

The trust lists and the directory are distributed to members who use this information to find the connection parameters of a given service provider or service client. In addition to the technical tasks, the governing agency is responsible for defining security requirements that must be met by the members of the infrastructure, such as requirements to user authentication.

2.2 Peer to Peer Communication

The security-related functionality that the UXP members must implement is encapsulated into reusable components called security servers. The governing authority distributes the security server software that the infrastructure members install as part of their information systems. To the application software, the security server is an almost transparent gateway that accepts standard SOAP or REST requests from the client and forwards them to the service (via the service provider's security server). The application software does not need to implement any part of UXP's security protocol.

UXP members communicate directly with each other. The communication uses the TLS (Transport Layer Security) protocol to establish a secure channel between the security servers. The security channel uses mutual certificate-based authentication (both the server and client must present a valid certificate). The authentication certificates are registered at the governing authority and connected to security servers. Thus, when creating a connection, the security server verifies that the partner's security server presents a registered authentication certificate and that the partner's security server is indeed allowed to represent the partner.

The security server signs all the outgoing messages with the member's signing key. It saves all the signed messages to a log. The log is periodically time-stamped to ensure long-term validity of the signatures. The time-stamped signatures can be extracted from the log and presented to third parties for verification. Additionally, UXP uses blockchain technology to protect the message archives against tampering.

The members communicate directly with approved trust service providers. When joining the communication infrastructure, each member must acquire a certificate for signing the messages and another certificate for transport security. The member must also select a time-stamping service provider that will be used to provide long-term security to the exchanged messages. During communication, the member interacts with service providers to acquire certificate validity information and to time-stamp the signed messages.

3 Advanced Topics

3.1 Working with Physical Persons

The UXP divides the authentication and access control to two levels/tasks. **Inter-organizational level** is standardized and implemented in security servers. On that level, the service provider and service client mutually authenticate themselves (as organizations). The requests and responses are signed by the originating security server using a key issued to the organization. On the service provider side, the security server enforces access control on the organization level – the access control list contains information on whether a service client is allowed to access a given service. These access rules are based on service provision agreements between service provider and service client.

The second level is the **intra-organizational level**, that concerns proceedings within the service client organization. In UXP, authenticating the end users and applying suitable access control policy is responsibility of the service client organization. When joining the UXP, the organization must prove that it has implemented user authentication and access control procedures that are compliant with the security requirements established by the governing authority. In addition, the members can be labeled with security categories that can be used to differentiate between several levels of assurance that is provided by the service client. For example, a service provider can declare that a given service can only be accessed by clients who are labeled with security category “ISO 27001” meaning that they have implemented an ISO 27001 compliant information security management system. This label is assigned to organizations by the governing authority based on certification audit. The service provider’s security server automatically checks for the presence of required security category and denies access if the requirements are not met.

The two-level approach used by UXP has two main benefits. First, the point of user authentication and the enforcing of an access control policy is close to the source of user and access control information. If, for example, the end user access control would be performed by the service provider, there would be a need to create and maintain an up to date copy of the user database at the service provider. In the current solution, the access rights are checked by the same organization that is responsible for assigning the access rights for users. However, the identity of the end user who initiated the transaction is transmitted to the service provider who can use it to enforce additional data-based access control rules (e.g., allowing a doctor to only view patients she is currently treating).

Second, separating inter- and intra-organizational access control mechanisms avoids the need to standardize end user authentication and access control across the whole infrastructure. Instead, each organization can choose to implement this functionality in a manner that is optimal for this particular case. Additionally, there is no need to rewrite existing sys-

tems – if the current authentication and access control scheme conforms to requirements of the UXP, then it is possible to keep using it.

Implementing services for private **citizens** imposes somewhat different requirements than implementing services for government officials. The citizens do not have their own information systems for accessing the services. UXP solves this problem by introducing a **citizen portal** – a special kind of information system. The citizen portal authenticates citizens using ID-cards, passwords or external authentication services (e.g., banks). Once authenticated, a citizen has access to specifically designed services for managing data about themselves. For example, they can query state registries for data about themselves or submit applications (such as registering for child support). The citizen portal sends the citizen's identifier to the back-end service which uses it to filter the query results.

3.2 Using Remote Hosting

In the simplest case, each organization is responsible for installing a security server that connects its information system to the UXP. This assumes that the organization has a budget large enough and an IT department capabile of maintaining the information system and security server. Another very common case, however, is a smaller organization that does not maintain its own information system but instead uses hosting services offered by an application service provider (ASP). In this case, it is reasonable to also use hosting services for the security server.

UXP has explicit support for hosted security servers. Each security server has an **owner** – an entity that is responsible for installing and maintaining the security server. The owner has physical access to the security server and can, for example, upgrade hardware or back up the system. In the simplest case the owner is also the only user of the security server. In addition to the owner each security server can have one or more **clients**. The security server client is an organization which uses the security server to access or provide services. For signing messages, each client uses its own signing key that is stored on the security server (either in software or in a hardware security module, depending on the configuration).

The connection between a client and a security server is registered at the governing authority and distributed to all the members of the infrastructure. The connection must be separately approved by the client and the security server owner in order to prevent abuse cases (e.g., when an owner adds a new client to their security server without the client's consent). When establishing a connection between two organizations, both security servers check that the other server is authorized to represent the partner organization.

When using hosted security servers, one must pay attention to the fact that the security servers have cleartext access to all the data that passes through them. This means that a security server is subject to the same security requirements that apply to an information system that produces or consumes the data.

3.3 Connecting UXP Infrastructures

UXP allows for the connection of several infrastructures to create support for **cross-border services**. The requirements for cross-border services are the same as for regular services.

- The two members communicate directly with each other using end to end encryption. There are no intermediaries that see the data neither is there an opportunity for a communication bottleneck.
- Connection of two UXP infrastructures does not require manual distribution of security-critical configuration to all the UXP members.
- The governing authority is responsible for defining the security policy of a UXP instance.

Before cross-border services can be used, the two UXP infrastructures must enter into a **federation relationship**.

1. The governing authorities of the UXP infrastructures sign a federation agreement. With this agreement the governing authorities state that the security policies of both UXP infrastructures are compatible. In particular, both parties agree to trust the certification authorities used by the other party.
2. The governing authorities exchange technical data that is used to download and verify the configuration of their UXP infrastructure. This configuration contains a list of trusted certification authorities, a list of members and their security servers as well as several technical parameters used for exchanging the messages.
3. Both governing authorities enter the download parameters of the other UXP infrastructure into configuration that is distributed to their members. This allows the members to download and use the configuration of other UXP infrastructures without any special effort in their part.

When participating in a cross-border service call, each party determines the UXP instance to which their partner belongs to and downloads the corresponding configuration. After that, it is possible to establish a secure channel with the other party and start exchanging messages.

When exchanging configuration between UXP infrastructures, the governing authorities can use filtering. Filtering can be applied both for incoming and outgoing data. Filtering can be used to restrict the access to cross-border services. For example, if a governing authority filters outgoing configuration to remove a class of members (e.g., private companies), these members will not be able to communicate with members of the other infrastructures.

3.4 Scaling and Reliability

UXP is designed from the ground up to enable building scalable and reliable infrastructures. The two central design principles are:

1. there must be no single point of failure nor any central bottlenecks; and
2. it must be possible to increase the reliability and performance of any component by adding redundancy.

The primary method for achieving the first objective is the decentralized architecture of UXP. The security servers communicate directly without any intermediary and thus avoid central bottlenecks. The centralized services (central configuration and PKI services) are not queried for every incoming message. Instead, they are queried once and the relevant information is cached. This prevents the security servers from overloading the centralized

services and allows them to continue operating when the central services encounter minor downtime.

UXP supports implementing redundancy for all the components: the registry server, the client's security server and the service provider's security server. The redundancy solution for the registry server uses an active-active system so that all the connected servers can be used to make changes to the configuration. The registry servers can be distributed between several locations. Security servers can be clustered on both the service client's and the service provider's side. On the client's side, it is possible to install a load balancer to distribute the load between several security servers. On the service provider's side, the load balancing is built into the UXP protocol. If the service provider has several security servers, the clients automatically detect the security server that has the fastest response time and connect to it.

3.5 Monitoring

Monitoring of UXP servers takes place on two levels. On the local level, the member organization's systems administrator monitors the security servers managed by the organization. On the global level, the governing authority has overview of all the security servers on UXP. This overview is needed to support members in diagnosing problems, determining performance bottlenecks and measuring compliance with SLA. Global statistics can also be used to guide further development of the ecosystem (such as which members and services get the most traffic).

UXP monitoring system processes three kinds of information. First, the monitoring system collects information about the current system state, such as processor load, amount of free memory, etc. This is used to monitor the general health of the security servers. Second, the monitoring system receives information about any faults that occur during message processing. Especially on the global scale, it is important to know which parts of the UXP are working and which parts are not. Third, the monitoring system collects statistical information about messages processed by security servers. This can be used to diagnose and predict performance bottlenecks (e.g., whether some service is growing more popular and more resources must be added to support the increased load) and also to discover any usage that does not conform to typical patterns and can therefore indicate unauthorized use of the services.

The UXP monitoring system is built in a modular manner. The servers send monitoring data to a monitoring agent that distributes the data using different back-end plugins. UXP comes with plugins for the Zabbix and Nagios monitoring systems and offers APIs for developing additional plugins.

4 Deployment

This chapter describes two cases of implementing UXP. The first case has minimal security requirements and is suitable for piloting environment or for communication between trusting parties (e.g. departments inside one organization). The second case provides high security and is suitable for governmental data exchange infrastructure.

4.1 Simple Case

In the simple case, UXP can be set up in the following manner.

- The governing authority also provides certification and time-stamping services. The certification policy is tailored to match the security requirements. For example, the certificates can be issued using fully automated procedures that make use of existing authentication schemes (company-wide authentication system, digital signatures, etc.).
- The procedures for registering members and security servers are also fully electronic and rely on existing identities and authentication schemes.
- Software keys (stored on the hard disk of a security server) are used for authentication between security servers and message signing.

4.2 Complex Case

In the high-security case, UXP can be set up in the following manner.

- Officially recognized services are used for certification and time-stamping. The certification policies and time-stamping policies are compliant with the requirements for legal digital signatures.
- Signing keys are stored in secure signature creation devices (SSCD). Depending on the performance requirements, either smart cards/USB tokens or hardware security modules may be used.
- If necessary, the governing authority creates regulations that allow signed UXP messages to be used as digital signatures or digital stamps.
- In addition to a high-security production environment where the signed messages carry legal force, a piloting/testing environment is set up, possibly according to the relaxed requirements outlined in the previous section. This is used by service providers and service clients to test new services before using them in production.
- High availability solutions are used both for central services and providers of critical services.

When setting up the infrastructure, the governing authority defines a security policy that may include different security categories. This makes it possible to support services with different security requirements. The security policy contains or references:

- a list of approved certification services and time-stamping services;
- any security requirements that must be fulfilled by organizations before they can join the UXP; and
- procedures for managing membership of the UXP (joining, leaving, changing contact information, etc.).

In addition to the security policy the governing authority defines a template for service provision contracts and service level agreements.

In order to ensure the smooth running of the infrastructure and respond quickly to errors, the governing authority sets up a global monitoring system to receive information about the status of security servers and any faults that occur in message processing.