14.12.2022

# Rebooting Trust Management in X-Road

Public Report

UNIVERSITY OF TARTU
1632

MTÜ Nordic Institute for Interoperability Solutions
Hobujaama 4, 10151 Tallinn, ESTONIA
Reg no 80419486

+372 7130 800
info@niis.org
www.niis.org

Nordic Institute for Interoperability Solutions (NIIS)

Hobujaama 4
10151 TALLINN
Estonia
+372 7130 800
info@niis.org
www.niis.org



ISBN 978-9916-9853-0-4 (pdf)

ISSN 2733-3345

# Credits

UNIVERSITY OF TARTU
Institute of Computer Science

AUTHORS

University of Tartu: Mariia Bakhtina
Prof. Dr. Raimundas Matulevičius
Prof. Dr. Ahmed Awad

NIIS: Petteri Kivimäki

# Table of contents

# Glossary

| Abbreviation | Description |
|---|---|
| API | Application Programming Interface |
| BCT | Blockchain Technology |
| CA | Certification Authority |
| CS | Central Server |
| CSR | Certification Signing Request |
| dApp | decentralised Application |
| DID | Decentralized Identifier |
| DKMS | Decentralised Key Management System |
| DLT | Distributed Ledger Technology |
| DPKI | Decentralized Public Key Infrastructure |
| GDPR | General Data Protection Regulation |
| HSM | Hardware Security Module |
| IdM | Identity Management |
| IS | Information System |
| OCSP | Online Certificate Status Protocol |
| PKCS | Public Key Cryptography Standards |
| PKI | Public Key Infrastructure |
| RoT | Root of Trust |
| RQ | Research Question |
| SS | Security Server |
| SSI | Self-Sovereign Identity |

| Abbreviation | Description |
|---|---|
| TSA | Time-Stamping Authority |
| UI | User Interface |
| VC | Verifiable Credentials |
| VP | Verifiable Presentation |
| WT | Waiting Time |
| ZKP | Zero Knowledge Proof |

# 1. Introduction

Enabled by rapid digitisation, organisations strive to benefit from collaborative work to get a competitive advantage by delivering unique products for end customers. Businesses create supply chains to deliver products and services. Governmental agencies collaborate to provide services that help the nation's well-being. What unites them is a business need for communication with external entities to deliver the expected value. Organisations need to know with which entities they exchange information, and to be sure that the communicating party is the one it claims to be. In turn, communication between organisations per se and their information systems (ISs) requires trust.

Trust is one of the basic concepts around which businesses and security are formed. A root of trust (RoT) is an axiomatically accepted point to be trusted. The most commonly used centralised RoT assumes that there is a third-party centralised authority the organisations choose to trust. Such authority is the key enabler and assurance of the security of the organisations' ISs. The authority claims which entities can be trusted, and organisations rely on the accreditation and quality of the authority's staff. The security of ISs heavily depends on the cryptography that is built over the root of trust. As a result, organisations that use ISs based on the centralised RoT are prone to a single point of failure.

Recent works have focused on developing the alternative to the centralised RoT – the self-sovereign identity (SSI) ecosystem [1, 2, 3, 4]. Self-sovereign identities are managed in a decentralised manner without relying on a single provider for storing and managing the identity's data. The algorithmic root of trust is decentralised and founded on the trust in the cryptographic mechanisms and the algorithms' correctness in the information system.

X-Road© is open-source software and ecosystem solution that provides unified and secure data exchange between organisations. In essence, X-Road is a data exchange layer between information systems that enables organisations to communicate securely. X-Road serves as the backbone of the Estonian, Icelandic, and Finnish digital government infrastructures. Moreover, it has been facilitating the digital government revolution in several other countries worldwide. Currently, X-Road relies on a centralised root of trust and identity management.

Our goal is to propose a decentralised approach for identity management in X-Road by embracing the SSI principles. The report presents the enterprise modelling results from the perspectives of functions, processes, resources, and trust. The lessons learnt are threefold. First, we have observed how embracing SSI through decentralised IdM could affect the trustworthiness of the secure data exchange system. Second, we have defined which enterprise system components and processes should be changed to enable automated identity management. Lastly, the results show how conceptual modelling supports the current state analysis and the transformation to be made in X-Road on the path toward SSI.

The report is structured as follows. Sec. 2 establishes the background. Sec. 3 describes the current state of the X-Road ecosystem and the objectives of the study. Sec. 4 presents the analysis procedure of the X-Road system case study. Sec. 5 provides modelling and analysis results. Here we also discuss

how the identity management system's transformation can affect X-Road's trust model and members' management processes, while Sec. 6 concludes the report.

# 2. Background

## 2.1. Identity Management and Verifiable Credentials

*Digital identity* is “a set of claims made by one digital subject about itself or another digital subject” [5]. *Identity management (IdM)* refers to the set of policies and technologies used to ensure that the resource users are eligible to access them based on their identity characteristics. The IdM operations include identification and verification, which rely on the usage of credentials.

*Verifiable credentials (VCs)* are ”any (tamper-resistant) set of information that some authority (issuer) claims to be true about the subject of the credential and which enables the subject to convince others (who trust that authority) of these truths“ [3]. Commonly, the subject of the VC is its holder. VCs are used as a baseline for providing the verifier with proof about the VC’s subject. Except for the proof of some statement about the VC’s subject, the verifier must be able to determine the following from the presented VCs: (i) who issued the credential; (ii) VC has not been tampered with since it was issued; (iii) VC has not expired or been revoked. Verifiable Credentials Data Model v1.1 [6] is an open standard of digital credentials format that ensures that credentials are cryptographically secure, privacy-respecting, and machine-verifiable.

The main components of any VCs are the following: (i) credential metadata; (ii) claim(s); (iii) proof(s). Credential metadata describes the credentials, e.g., specifying the credentials subject, issuer, date of issuance and data expiration. The claim describes what is claimed to be truth, e.g., having a driving license, ID card or another certificate with the defined attributes. The proof for a VC relies on the digital signature and aims to support the authenticity and integrity of a VC. The proof part of the VC proves that the claims and VC itself were created by a specific issuer (specified in the credential metadata) to the VC subject (that is defined by some identifier and specified in the credential metadata).

While different documents can play the role of verifiable credentials, each VC is characterised by an identifier. Such identifiers have been based on the public key infrastructure (PKI), where certificates are VCs issued by centralised certification authorities. With the emergence of self-sovereign identity (SSI), the idea of removing a centrally governed authority is getting its popularity as it allows removing a single point of failure and potentially bringing automation to the issuance of the credentials.

## 2.2. Conventional Public Key Infrastructure

Public Key Infrastructure using X.509 (PKIX) is the most used PKI implementation [7]. In the case of conventional PKI, there should be a root authority that accredits trusted third-party certification authorities (CAs). CA is responsible for the issuance of centralised identifiers connected to the issued certificate. Additionally, each CA holds a (centralised) certificate registry. CAs follow X.509 standard[8] for issuing digital certificates by publicly trusted Certification Authorities. However, while the whole

infrastructure is based on the CA's trust, compromising it or its registry of certificated negates the whole trust model. From the technical point of view, using a set of trusted certification authorities puts obligations on integration with each CA's system to verify credentials.

## 2.3. Decentralised Public Key Infrastructure

The main advantages of the decentralised PKI are based on decentralised identifiers (DIDs), which are permanent, resolvable, and cryptographically verifiable. Unlike X.509 certificate trees that rely on centralised registries under the control of a single authority, DIDs must help avoid single points of failure by using decentralised networks (i.e. verifiable data registry) for storage. A *verifiable data registry* (VDR) is commonly implemented using distributed ledger technology (DLT). Such a DLT can be presented by general-purpose public blockchain networks or special-purpose SSI distributed ledger networks. In principle, VDR can be implemented as distributed file systems (e.g., IPFS), key event log (e.g., KERI), and distributed hash tables, but in this report, we focus only on VDRs based on DLT.

*Decentralised Identifier (DID)* identifies the subject. The DID subject can be a human, organisation or any resource that should be identified. An entity that has the capability to change the information associated with a DID and use it in a VC is called a *DID controller*. DID controller and DID subject may or may not be the same entities. *DID document* is an artefact of DID resolution controlled by the DID controller that is used to describe the DID subject [3]. DID document is not a resource that is defined by the DID, but it does not have a separate unified resource identifier. *Resolution* of DID refers to the transformation of the given DID to a DID document using the defined method. Regardless of the nature of the subject, the DID created using the selected DID method always resolves to the same DID document. The standardisation of identification is guaranteed for all the subjects. DID document is not stored in plain text form in the ledger. Instead, it is dynamically constructed by the *DID resolver* based on the provided DID and the transactions connected to this DID in the ledger.

*DID method* specifies the implementation of a specific DID method scheme, i.e., how DIDs and DID documents are created, resolved, updated, and deactivated (CRUD operations) [9]. DID methods are commonly associated with a concrete verifiable data registry. An organisation may use any of the existing DID method schemes registered in the registry [10] or implement a new one. Each implementation of DID method scheme should follow the requirements defined by W3C in their specification [9], namely, method syntax, operations, security and privacy requirements. Among the operations defined by the DID method is authentication, that in turn governs the verification method. A comprehensive analysis and comparison of the DID methods can be found in [11].

DIDs are globally unique identifiers, and there is no central authority that manages them. The controller creates the DID on its own and has complete control over the data that can be accessed using the identifier. DID is an analogue to the HTTP URLs – identifies its associated resource and is used to locate the artefact that describes the resource - DID document. DID Document is a JSON (JavaScript Object Notation) object in which the associated public keys, lifecycle properties, service endpoints and meta information are included [3, 12]. So, when a holder presents the proof to a verifier, the verifier uses

the holder's and/or issuer's DID to look up DID document in a VDR to get the public key required to verify the proof.

*Digital wallet* stores the holder's credentials. *Digital agent* is software that enables the VC holder to operate their digital wallet. Additionally, digital agents establish secure connections with other agents to exchange credentials and DIDs. Commonly, a digital wallet is a part of a digital agent that enables secure storage of credentials. While digital agents may vary by their type (mobile and cloud), the interoperability on the client layer allows holders to select the preferred agent regardless of which agents are used by other entities or which registry is used for storing DIDs (by means of the universal resolver). Finally, the digital agent allows the VC holder to define *Verifiable Presentations* (VP). VP is a data artefact containing data from one or more VCs shared with a verifier. VP may allow a holder to present a claim in a synthesized form instead of the original VC (e.g., through zero-knowledge proofs) to preserve the holder's privacy.

*Zero Knowledge Proof* (ZKP) is a cryptographic method (or protocol) which enables one party (the prover) to prove to another party (the verifier) that he knows some specific piece of information without revealing any part of this information. For example, ZKP allows proving that the government agency has classified you as a national registry without revealing any other personal identifiable information contained on the permission. There are a few use cases of the ZKP mechanism by the credentials holder [6, 3]: (*i*) combine multiple VCs into a single VP without revealing VC or subject identifier to the verifier; (*ii*) selective disclosure of the claims from the VC to a verifier without the need to issue multiple atomic VCs; (*iii*) produce a derived VC that is formatted according to the verifier's data scheme instead of the issuer's; (*iv*) the holder can produce a proof of non-revocation so that a verifier can check this proof against the revocation registry on a public ledger.

## 2.4. Distributed Ledger Technology

*Distributed ledger technology* (DLT) refers to an approach to recording and sharing data across multiple data stores (or ledgers). DLT allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants [13].

*Blockchain technology* (BCT) is one way of implementing DLT. Blockchain is a particular type of data structure used in some distributed ledgers that stores and transmits data in packages called "blocks" that are connected to each other in a digital chain. Blockchains employ cryptographic and algorithmic methods to record and synchronize data across a network in an immutable manner.

# 3. X-Road Description

*X-Road* is a centrally-managed distributed data exchange layer between information systems that provides a standardised and secure way to produce and consume services over the web within the trusted network [14].

From the organizational point of view, there are four key roles in the trusted network (see Fig. 1). *(X-Road) Governing Authority* is an organization that owns an instance and defines regulations and practices which must be followed in the ecosystem. *(X-Road) Operator* is an organization that manages an instance of the X-Road ecosystem. *(X-Road) Member* is an organization that can join the X-Road instance to provide and/or consume services by exchanging messages with other Members. *Trust Services Provider(s)* are organizations that are time-stamping authorities (TSA) and/or certification authorities (CA) that can be either third-party or owned by the Operator.

The X-Road ecosystem consists of a trusted network of organisations that use the same instance of the software for providing and consuming services. The X-Road system has two main components - Central Server and Security Server. *Central Server* (CS) is managed by the Operator of the X-Road instance and acts as a registry of Members and their Security Servers' addition, authentication, and removal. *Security Server* (SS) is an entry point to X-Road that mediates service calls and service responses between information systems of Members.

Currently, the management of Members' and their SSs' identities relies on PKI. To become an X-Road Member, an organization should have *a signing certificate* issued by one of the trusted CAs. X-Road Members may use one or a few Security Servers as a proxy for mediating service calls and service responses between the information systems of different Members. Each Security Server has its own authentication certificate. Moreover, an X-Road member should have a separate signing certificate for each Security Server it uses. The X-Road Operator defines the list of trusted third-party CAs. Alternatively, the Operator may play a role of a certification authority. However, the process of obtaining such a certificate depends on the

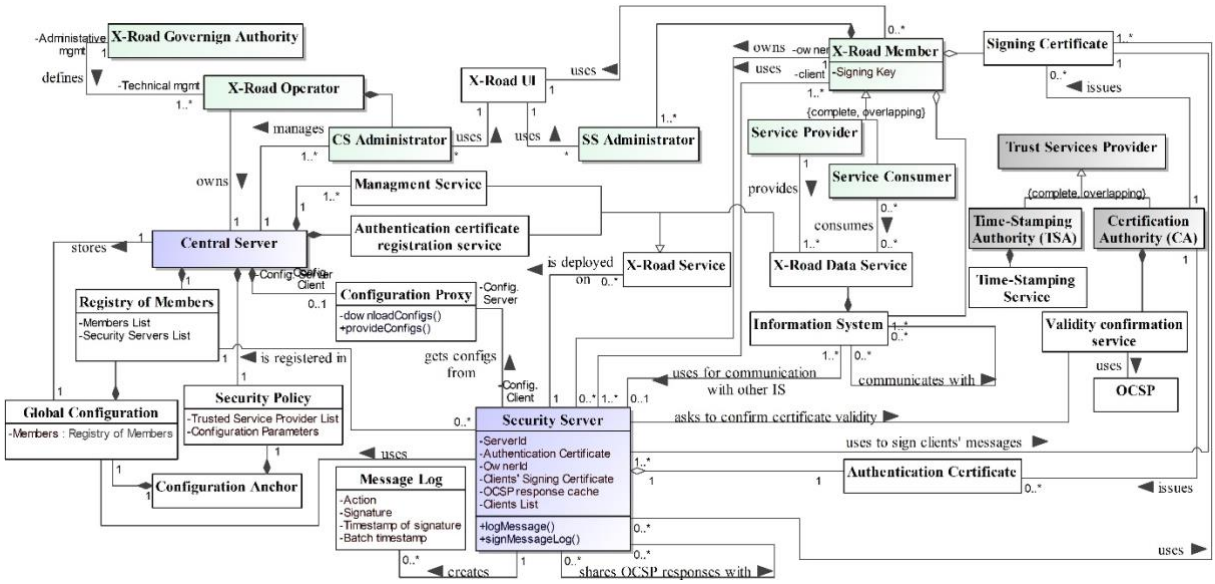



*Figure 1: Entities in the X-Road ecosystem (green – network participant and their roles; purple – core system components; gray – external trusted service providers)*

speed of processing certificate signing requests (CSR) from third-party certificate authorities. This process includes several manual steps, and it might require days, weeks or even months to complete. Worth mentioning that each Security Server has one owner, but few Members may use the same Security Server.

The objective of the research is to present a road map and a design document of using decentralised public key infrastructure (DPKI) that relies on the decentralised identifiers (DIDs) as an alternative to public key infrastructure (PKI) supported by trusted (third-party) Certification Authorities (CAs). To this end, the research aims to answer the following research question (RQ): *How the shift to the decentralised public key infrastructure can contribute to the X-Road trust model and member management?*

The research results include but are not limited to: (i) an updated trust model; (ii) a roadmap of the changes to be done in X-Road to migrate to the SSI concept and DPKI usage (in terms of affected technologies, stakeholders, update of the trust model, onboarding processes. Among the limitations of the research is the need for assurance of the compliance of newly introduced verifiable credentials with eIDAS regulations. However, the analysis of DID-based verifiable credentials on compliance with the eIDAS regulation is left out of the current research scope as it would highly depend on the concrete implementation and selected method of credentials issuance.

# 4. Research Design

The research process starts with the analysis of the current X-Road system. During this stage, we define (i) the aim of signing and authentication certificates in X-Road; (ii) the procedure of issuing signing and authentication certificates for X-Road Member; (iii) the onboarding process of an X-Road Member; (iv) the trust model. For this purpose, we use the following input: (i) X-Road Academy courses [14], (ii) official documentation of X-Road on GitHub [15], and X-Road Document Library [16].

The next stage of the research is mapping the current verifiable credentials and actors in XRoad to the analogue verifiable credentials and actors in the context of decentralised public key infrastructure. This step should result in the redefined trust model and identified actors, entities and processes that should be changed to migrate to DPKI.

Finally, we assess the effectiveness of the system changes by comparing the assessed identity management system trustworthiness. Following [17], we regard trustworthiness as the beliefs of the system users in expected attributes. Therefore, we assess and compare the trustworthiness of the X-Road system delivered by PKI and DPKI identity management approaches (see Sec. 5.3) based on the following quality criteria: (i) *reliability* - how often the IdM system implementation causes downtimes or delays in the operations; (ii) *security* - to which security attack the IdM system implementation is prone to; (iii) *control* - how much control over the credentials the identity holder has. The description of measurement values is presented in Table 1.

*Table 1: Measurement scale for the criteria of system trustworthiness*

| | Reliability | Security | Control |
|---|---|---|---|
| Low | System is off or behaves not in accordance with the business rules regularly that causes downtime or delays in the business operation | System is vulnerable to a considerable number of security threats that threaten confidentiality, integrity and availability of business assets | System is fully responsible for and has access to all the user's identity data (including all the identity's attributes, VCs and keys) |
| Medium | System is prone to delays which may hinder effective business flows | System is vulnerable to threats of medium probability which may have a significant influence on the business operations | System is responsible for and has access to the predefined identity's attributes and may control the keys |
| High | System is working stable, and the risk of the system not being accessible is low | System is vulnerable only to the threats which are of low probability due to the complexity of implementation | User chooses to which VCs and their presentations the system has access; the user is responsible for keys |

# 5. Modelling and Analysis Results

This section provides the results of modelling the X-Road system and the identity management implementations.

## 5.1. Centralised Identity Management

### 5.1.1. VCS ISSUANCE AND VERIFICATION

There are two identities managed in X-Road – the identity of each Security Server and Members. A set of trusted CAs issues the credentials in the form of certificates which are used by the X-Road components to identify that the Member or SS is the one it claims to be (see Fig. 2).

| Use Case of Auth. Certif. Verification | *Member Communication: UC MESS_05 Initiate a Secure Connection* | *Member Communication: UC MESS_06 Establish the Secure Connection* |
|---|---|---|
| **Holder and Subject** | Service Provider's Security Server | Service Client's Security Server |
| **Verifier** | Service Client's Security Server | Service Provider's Security Server |
| **Claim** | Provider's SS has a valid auth. key pair | Client's SS has a valid auth. key pair |
| **Issuer** | Trusted CA | |
| **What is verified** | (1) Holder's SS has a valid auth. key certificate issued by the trusted CA<br>(2) Holder sent the certificate for the SS from which the message is sent<br>(3) The provided certificate is an auth. certificate | |

| Use Case of Sign. Certif. Verification | *Member Communication: UC MESS_02 Process X-Road SOAP Request* | *Member Communication: UC MESS_03 Process X-Road Request Message* |
|---|---|---|
| **Holder and Subject** | X-Road Member | X-Road Member |
| **Verifier** | Service Client's Security Server | Service Provider's Security Server |
| **Claim** | X-Road Member has a sign. key pair | |
| **Issuer** | Trusted CA | |
| **What is verified** | (1) Holder has a valid sign. key certificate issued by the trusted CA<br>(2) Signing certificate was issued to the X-Road member who sent the message the signature was attached to<br>(3) The provided signature value is correct | |

*Figure 2: Use cases of verifiable credentials - authentication and signing certificates*

For identification and verification of Members, the $VC_{sign}$ credentials (i.e. *signing certificates*) are used. The $VC_{sign}$ credentials are issued to a Member (*holder* and *subject*) by one of the trusted CAs (*issuer*) with the claim "The Member *client_ID* has a valid signing key pair". These credentials $VC_{sign}$ are used when the Member joins the X-Road instance, sets up a SS, or registers as a SS's client. CS plays the role of *verifier* by verifying the proof. After the onboarding process, $VC_{sign}$ is verified by (Service Provider's) SS when the Member makes an X-Road request for the service. In such case, $VC_{sign}$ are used to verify that the Member who initiates the request with the SS: (1) has a valid signing certificate issued by the trusted CA, (2) is a legitimate holder of the $VC_{sign}$, and (3) the provided signature value is correct.

The identity of the Security Server is managed using the $VC_{auth}$ credentials (i.e. *authentication certificates*). The $VC_{auth}$ are issued to SS (*holder* and *subject*) by the CA (*issuer*) with the claim "The Security Server *SecServer_ID* owned by the client *client_ID* has a valid authentication key pair". During the onboarding process, $VC_{auth}$ are used when a SS is set up (Member provides proof of having $VC_{auth}$ as a part of the authentication certificate registration request). CS plays the role of *verifier* by verifying the proof. Later on, after the onboarding process, $VC_{auth}$ is verified by Service Provider's or Client's Security Server when the secure connection between parties is established. In such case, $VC_{auth}$ are used to verify that the SS which initiates the connection with another SS: (1) has a valid authentication certificate issued by the trusted CA, (2) is a legitimate holder of the $VC_{auth}$, and (3) the provided certificate is an authentication certificate.

The current system analysis started with modelling the processes manipulating VCs. The business process of a new Member onboarding is modelled using Business Process Model and Notation (BPMN 2.0). Upon the conclusion of the legal agreement between the Governing Authority and the prospective Member, the Operator registers the Member in the system. The key part of a Member's onboarding is becoming a client of the SS that in the end allows the Member to provide/consume service via X-Road (see Fig. 3).

If the Member wants to use its own SS, first, the Member sets it up. For this, the signing key and corresponding certificate should be obtained for the Member; the authentication key and the corresponding certificate should be obtained for the SS (the procedure of obtaining the authentication certificate is analogue to the sub-process 'Configure signing key and certificate'). Upon obtaining the certificates, they should be imported and activated in the SS. After obtaining the authentication certificate, the authentication certificate registration request (signed with the Member's signing key) is sent to the Central Server for approval. Once Central Server approves the request of registering the SS, Members of the network can initiate registration as the SS's clients.

Fig. 3 depicts the configuration of a signing certificate (sub-process 'Configure signing key and certificate'). The process starts when the Member uses the SS UI (to which they have access as a Member of the network) to generate a signing key pair. The Security Server REST management API could be used as an alternative to the SS UI as it provides the same functionalities as the UI. The pair is saved as a PKCS #12 file. Based on this file, the Member applies for the certificate by sending a certificate signing request (CSR) following PKCS #10 format to the selected CA. Receiving the CSR, CA checks the request, conducts some checks of the applier's identity (which could be done either manually or automated depending on each CA), and in the case of approval, CA generates the certificate for the provided authentication key pair. The certificate is stored in the certificate base to be accessed on-demand for verification. The credentials configuration happens off X-Road mostly manually, causing the waiting time WT_1.

The configuration of signing and authentication certificates is essentially analogous. There are two peculiarities of the signing certificate configuration. First, the generation of signing key pairs may be outsourced to the CA. In this case, the signing key pair is stored in the HSM (hardware security module) device, and the SS administrator does not have to create it. Second, depending on the X-Road instance

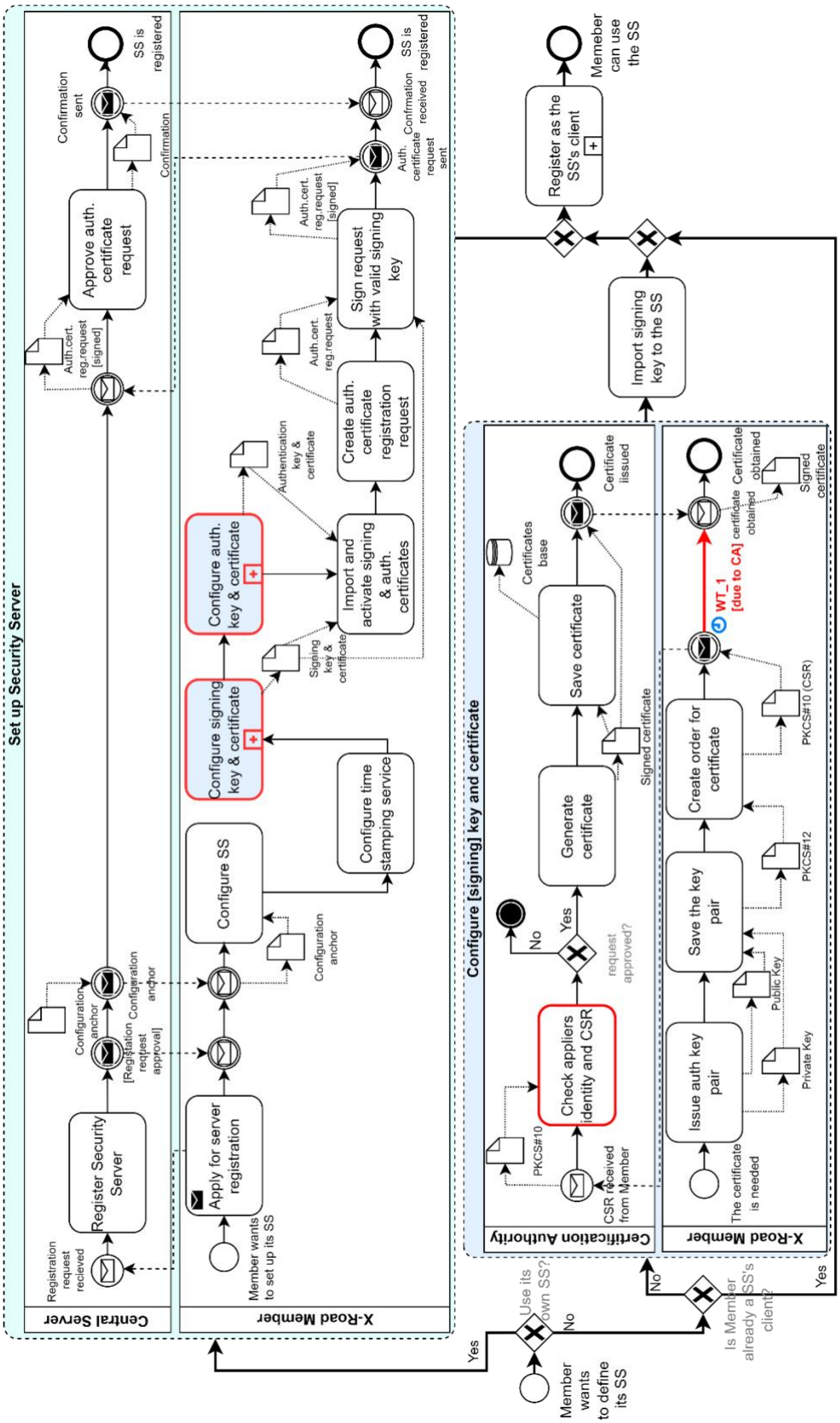



*Figure 3: X-Road Member onboarding to become the Security Server client*

policy, the Operator may be an intermediary party between the Member and CA when the Member sends a CSR.

Regardless of the type of VC, the verification process is essentially the same, and it is shown in Fig. 4. When an identity holder (SS or Member) wants to exchange a message with a verifier (another SS or Member), the former sends the message signed using the private key corresponding to the signing credentials certificate together with the VC's ID and the certificate itself. An authentication certificate is only used for establishing TLS connections between the Security Servers. The verifier checks the credentials issued by the trusted CA and searches for information about the validity of the credentials (OCSP response) in the message. When issuing a connection between two SSs, In case of a missing OCSP response for $VC_{auth}$, the verifier requests it from the holder, who requests it from the certification authority that issued credentials. When it comes to $VC_{sign}$, the OCSP response is included in the message (request or response), and therefore, the verifier does not have to request it separately.

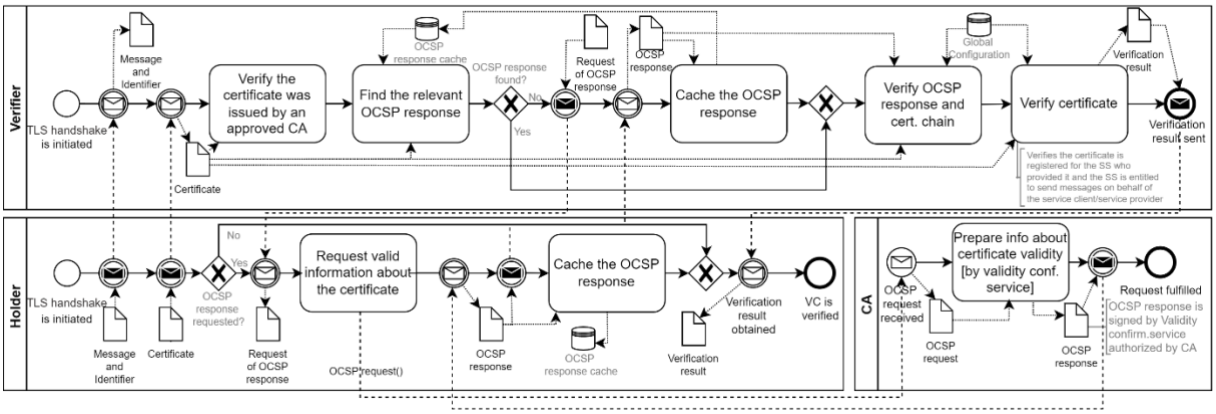


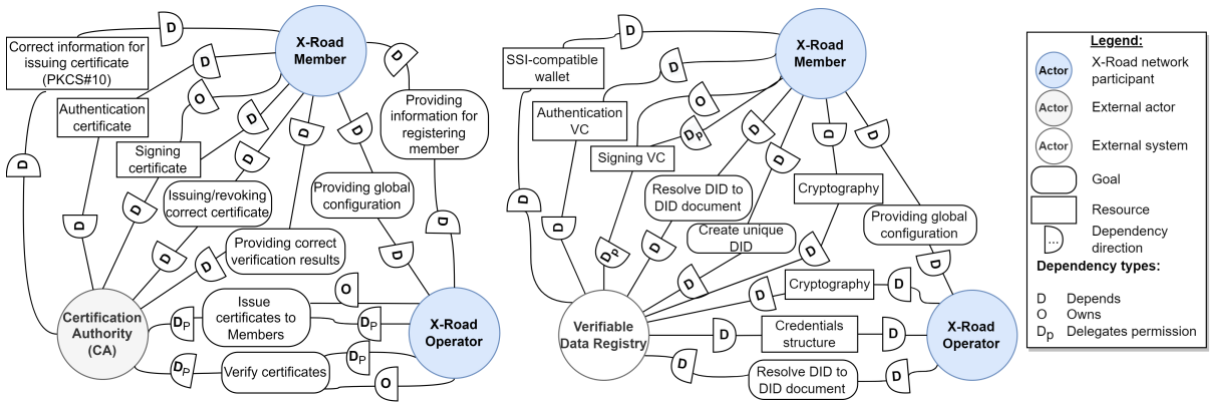

*Figure 4: Credentials verification based on the trusted certification authority*

## 5.1.2. TRUST MODEL

The current trust model enabled by PKI is depicted in Fig. 5a. There are three main actors who depend on each other with some goals and trust. Fig. 5 is created using *i** language to depict social dependencies.

X-Road Operator has a goal of *issuing certificates to Members* (both signing and authentication). X-Road Operator delegates meeting the goal (i.e. delegates its permission) to CA. So, X-Road Operator trusts the CA on meeting this goal. Similarly, X-Road Operator trusts the CA on meeting the goal of *verifying certificates* (both signing and authentication). Meanwhile, the trust dependencies between Member and CA are tighter. Member depends on CA with *issuing/revoking a correct certificate*, providing *correct verification results*, providing an *authentication certificate* to a Security Server owned by the Member, providing a *signing certificate* for identifying Member's identity. In turn, CA trusts Member on providing *correct information for issuing a certificate*. Additionally, Member depends on X-Road Operator with the goal of *providing global configuration* while X-Road Operator depends on a Member with the goal of

*providing information for registering Member*. In summary, CA is an RoT, and X-Road ecosystem members are highly dependent on it.




(a) Context of PKI (b) Context of DPKI

*Figure 5: X-Road Trust Dependency Model*

## 5.2. Decentralised Identity Management

Following the spirit of SSI, we introduce the decentralised public key infrastructure to the X-Road ecosystem. In this section, we describe how the DPKI can be integrated in the data exchange system and how the newly introduced credentials should be used by the Members and SSs to prove their identities.

### 5.2.1. CONCEPTUAL ARCHITECTURE

The conceptual architecture of the DPKI-based X-Road is depicted in Fig. 6. The components coloured in purple are part of the X-Road system, and the other black-coloured components are external entities. A verifiable Data Registry (VDR) in the DPKI-enabled X-Road should be used for storing the DID-related transactions. It is recommended to have VCs not publicly accessible, so they are stored only in the holder's digital wallet. Though, VDR may contain some extra information (except for the public key and verification method) like service endpoints or any other externally defined extensions. In Fig. 6, dApp corresponds to the decentralised application for the VDR. The dApp should define rules for credentials validation. For this Zero-Knowledge proof (ZKP) procedure should be used for checking Member's attributes when issuing and verifying credentials and their presentations. Additionally, the *credentials registry* and *revocation registry* may be optionally maintained in VDR.

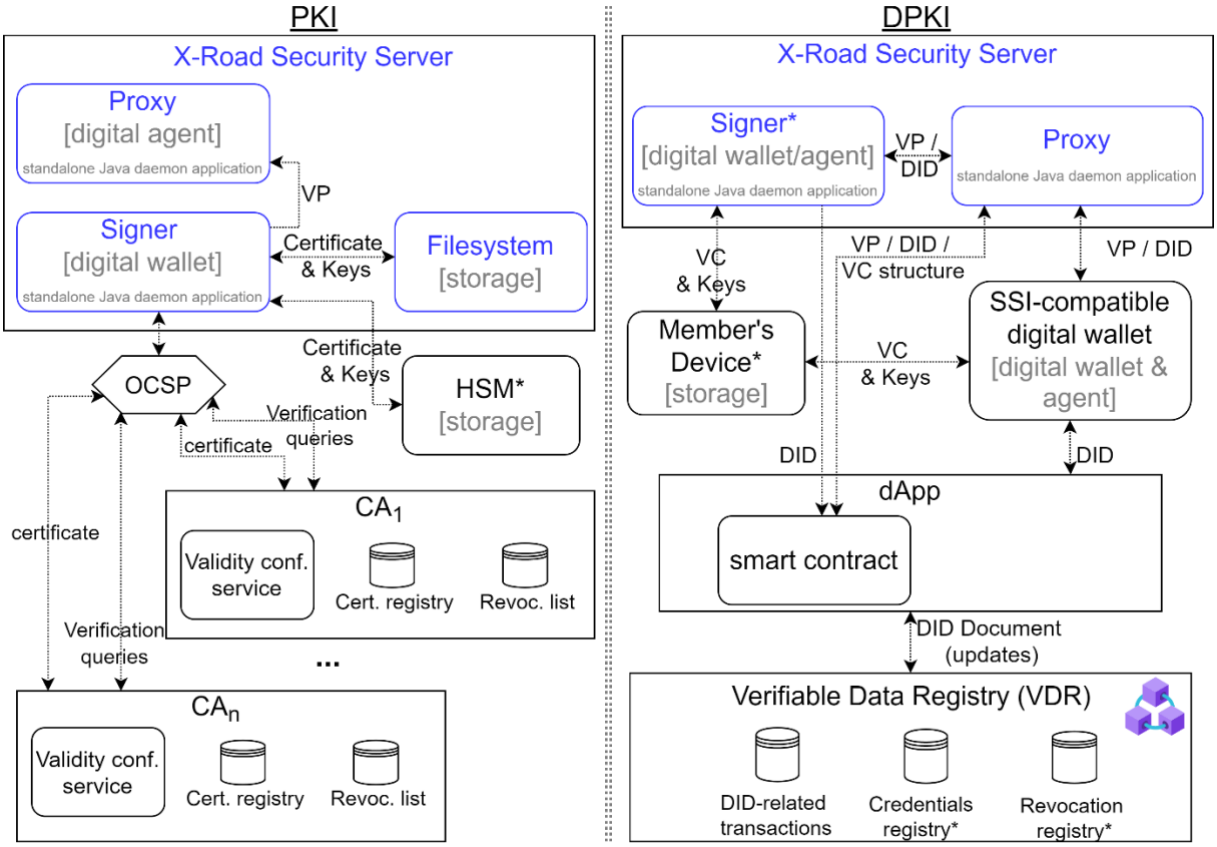



*Figure 6: Conceptual architectures of the X-Road ecosystem*

Let us start with the preliminary decisions the X-Road system owners should make. First, select the verifiable data registry (VDR) and the DID method to be used by Members for DIDrelated transactions. A decentralised application (dApp) for the selected registry is integrated, and its smart contracts enable issuance of the DIDs based on the provided VCs and proofs, call of DID resolver and access to the credential and revocation registries (if any). Second, the distributed IdM allows the Members to use an external SSI-compatible digital wallet as an alternative to the Signer component of the SS. Thus, the X-Road SS should enable integration with such SSI-compatible digital wallets. The Signer component in the to-be system stores the credentials and key locally on the Member's device. Thereby, Members become in control of their identity. Thereby, the usage of the Online Certificate Status Protocol (OCSP) is eliminated.

Additionally, Governing Authority should decide whether to use VDR for maintaining credentials and revocation registry. *A credential registry* can be used for duplicating VCs issued to Member/SS (they contain the same claims as in the original VCs, but the holder is the Credentials registry instead of the subject itself). Such architecture makes th e credential registry responsible for publishing the credentials so that they can be searched, discovered, and verified by any qualified verifier. If the credential registry is used, the issued DID-based $VC_{sign}$ and $VC_{auth}$ should not contain any claims or attributes to be classified as special category data under the GDPR terminology. If special category data should be a part of credentials or the VC's privacy want to be preserved, it can be either included in the encrypted format on-chain or stored off-chain. Similarly, a *revocation registry* may be used as an additional way for

checking the validity of the credentials by means of ZKP. The holder should create proof of non-revocation, and the verifier can check this proof against the revocation registry in VDR. If the VDR supports ZKP cryptography, a verifier can check only the revocation status of the presented proof without revealing any information about the credentials themselves. The operation of decentralised identity management is possible under a few assumptions. Mostly the assumptions are related to the infrastructural settings and prerequisites for the stakeholders.

- X-Road Governing Authority and Operator have DID-based credentials to be able to prove their identities to the prospective X-Road Members upon their onboarding to the X-Road instance. As a result, Members are sure they are connecting to the legitimate X-Road instance.
- The (decentralized) distributed ledger to be used for the management of the DIDs for VCs should be SSI-compatible. Thus, the ledger should provide the mechanism and features for DIDs and functioning including DID resolver.
- X-Road Governing Authority either defines a list of trusted credentials issuers, enumerating their DIDs in the Global Configurations or specifies characteristics the trusted credentials issuers should have and which Members should be able to verify through the DID-based credentials.
- The trusted issuers of the authentication and signing credentials for the Members should have DID-based credentials that are created following the selected by Governing Authority DID method. Alternatively, self-certifying identifiers managed in the VDR should be allowed eliminating the need for specialised trusted issuers.
- The Member should have the credentials required by issuers (for obtaining the authentication and signing credentials) in the DID-based format stored in any SSI-compatible digital wallet.
- The issued DID-based $VC_{sign}$ and $VC_{auth}$ do not contain any claims or attributes to be classified as special category data under the GDPR terminology. If special category data should be a part of credentials, it can be either included in the encrypted format on-chain or stored off-chain. Thus, as soon as the credentials stored in a public decentralised distributed ledger do not contain any sensitive data, X-Road Member should not be concerned by the possibility of network members accessing such credentials or keeping the pace of the credentials story.
- The issuance of the authentication and signing DID-based credentials is not facilitated by any means of X-Road.

The digital wallet provider should enable the decentralised key management system (DKMS). Thus, if the Member uses an external digital wallet, the key management for $VC_{sign}$ and $VC_{auth}$ should be conducted by the selected digital wallet. To enable the DKMS within the X-Road's digital wallet, first, the Signer component of each SS, which plays the role of a digital wallet, should store keys and credentials locally on the Member's device. Second, the Signer should enable the backup file and recovery keys. For this, the Signer must conduct an automatically encrypted backup copy of the wallet in the location of the Member's choice. In case of loss or corruption of the local device where the wallet stores credentials, the system should allow restoring the most recent state of the wallet from the backup copy using the

recovery key. The recovery key can be stored (i) offline on the HSM or (ii) cryptographically split into *N* secret shares, which are provided to other (randomly selected) X-Road Members (see secret sharing techniques for more details).

### 5.2.2. VCS ISSUANCE AND VERIFICATION

Fig. 7-8 depicts the proposed processes of issuing and verification of credentials enabled by the DPKI. The signing certificate used as a VC for verifying the identity of a Member is changed to the DID document. The DID document should be generated based on the public and private signing key pair that is equivalent to the current signing certificate. However, the DID document should be generated within the selected distributed ledger network and stored in its ledger (i.e. verifiable data registry). There are a few options for the distributed ledger network: it can be explicitly created for X-Road, or the existing special-purpose SSI distributed ledger networks can be used (e.g., Sovrin, Veramo).

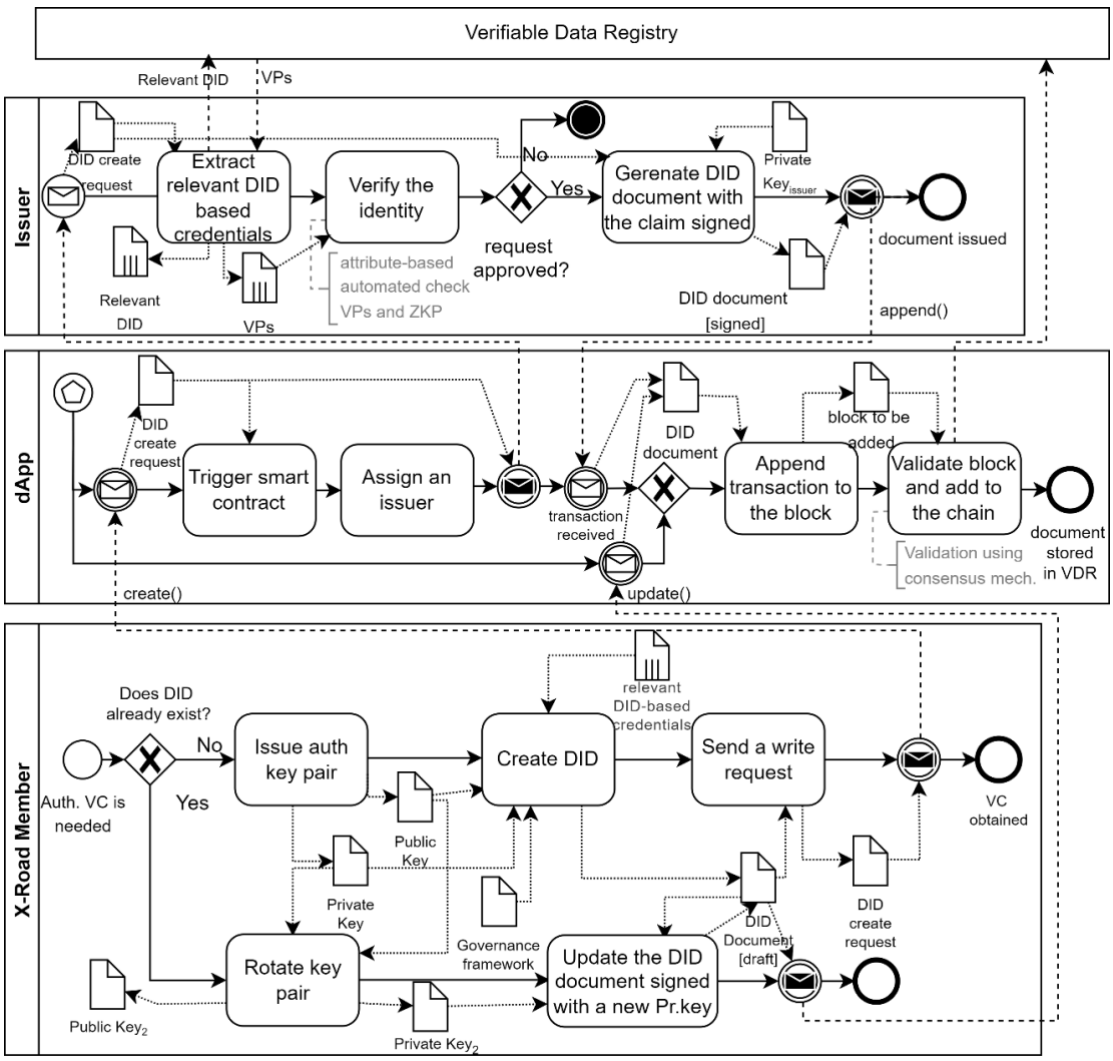



*Figure 7: Credentials issuance based on the DPKI*

Among the possible current implementation of SSI ecosystems and digital agents are the following: (*i*) *Sovrin* is a non-profit open-source identity network that manages the governance framework of SSI and its implementation on the Hyperledger Indy public permissioned blockchain. The credentials follow the Sovrin DID Method rules. Sovrin ledger stores public DIDs, issuer credential definitions (schemas), and revocation updates; (*ii*) *Veramo* (previously known as uPort) is a framework for verifiable data supported with a digital agent for decentralised credentials. The Veramo agent works based on the Ethereum public permissionless blockchain following the ETHR DID Method. Veramo uses an Ethereum blockchain for storing the DID document modification events; (*iii*) *Hyperledger Aries* is a digital agent for the decentralised identity that is intended to be agnostic to the underlying ledger, DIDs or verifiable credentials layer [18]; (*iv*) *ShoCard*; (*v*) *Blockstack*; (*vi*) *Jolocom*; (*vii*) *Namecoin*; (*viii*) *IDUnion*; and others.

Among the limitation of using blockchain as storage for the credentials are (1) storage of public keys on-chain may be expensive or impossible (depending on the size of the PK and size of blocks); (2) there should be a limited number of developers (blockchain participants responsible for the code update, i.e. X-Road Operator representatives), validators (blockchain miners/validator, who are responsible for creating new blocks and authorizing transactions) and full nodes (that store the whole blockchain) in order to prevent 51% security attack (that may take place in any DLT, and not only blockchain).

The comparison of the state-of-the-art blockchain-based SSI solutions [19] shows that Sovrin [20, 21] and Veramo are the solutions which are compliant with the most SSI principles compared to other existing solutions Also, the method for generating DID in the ledger can be selected from the set of existing methods [10] or explicitly created for X-Road.

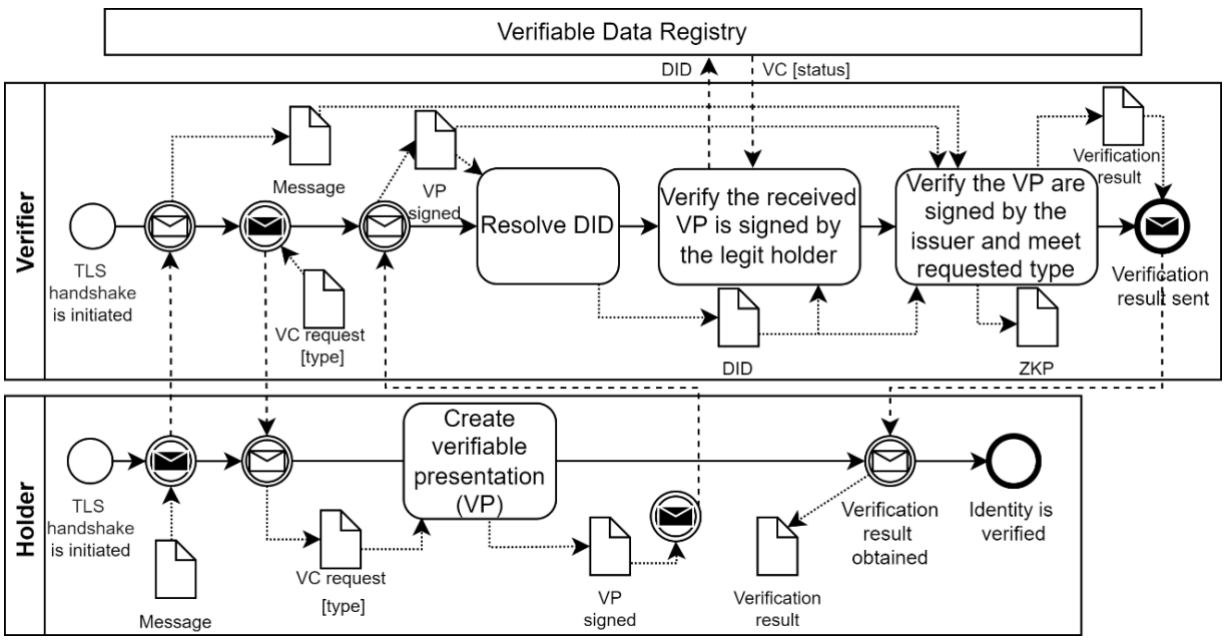



*Figure 8: Credentials verification based on the DPKI*

### 5.2.2. ADDITIONAL DLT-ENABLED FEATURES

Credentials privacy preservation. Moving to the DLT enables also preserves the privacy of the credentials holder. As such, instead of creating public verifiable credentials signed by the issuer which later are to be presented to a verifier, a zero-knowledge verifiable claim is issued to the holder who provides zero-knowledge proofs to the verifier. Such privacy preservation is delivered, for example, by the Sovrin ledger [20], which provides built-in support for zero-knowledge proofs.

Credentials revocation. One of the mechanisms enabled by the Sovrin network is revocation registries [21]. It is a decentralised, asynchronous and private data structure maintained in the Sovrin ledger by the issuer of the credentials.

Also, we propose the unification of the credentials storage. Currently, Members should have a separate $VC_{sign}$ for each SS and store such $VC_{sign}$ in SS's filesystem. We suggest that the Member should have one digital wallet to store all its VCs to use for the proof presentation for any verifier. As mentioned above, the Member can choose either an external SSI-compatible digital wallet that will be used or provided by X-Road. We propose to have one $VC_{sign}$ per Member, so when the Member wants to prove the identity to another Member, Security Server requests the corresponding $VP_{sign}$ from the global digital wallet.

### 5.2.4. TRUST MODEL

Fig. 5b depicts the enabled by DPKI trust between the X-Road network participants. The external system of the Verifiable Credentials Registry represents the distributed ledger network that enables decentralised storage and access of the DIDs and DID documents. Instead of trust to a centralised certification authority (in the case of PKI), the RoT in the DPKI shifts to the used distributed ledger of VDR and the cryptography on which the ledger is based.

## 5.3. System Trustworthiness

### 5.3.1. ASSESSMENT OF PKI

The main weakness of the current system is its reliability. The third-party CA checks the applicant's identity, which may include a manual check of the organisation's characteristics. Stakeholders highlight that such an identity check (for some CAs) causes waiting time from days to months (see Fig. 3) during the new Member's onboarding. As a result, prospective Members experience delays at the beginning of the X-Road system usage as they cannot provide/consume services through the data exchange system. Due to the same reason, Members may experience downtimes when their certificates expire, but Member forgets to renew them beforehand. In contrast, the OCSP caching system is highly fault-tolerant and very configurable [22]. Therefore, the integration of Members' Security Servers with the

CAs' validity confirmation services through the usage of OCSP and sharing the cached results of credentials verification between SSs provide a high level of system accessibility during the credentials usage. Thereby, we assess the *reliability* as medium level (see Table 2) due to the delays during the issuance of the credential.

From a security point of view, the public key infrastructure is prone to a single point of failure. In case of compromising the root certification authority, the integrity, confidentiality and availability of the credentials are compromised, and the identity management system implementation becomes untrustworthy. Therefore, we assess the *security* level as of medium level.

Finally, we consider how much control an identity holder has over its data. The usage of PKI and certificates implies that whatever information, except for the public key, is mentioned in the credentials (certificate), it is accessible to any verifier, and the identity holder cannot control the verifiable presentation of credentials. In terms of control over the keys, PKI may allow Members to recover the lost private keys (if the service provider generated them), giving the Members some flexibility and the right to make mistakes, sacrificing some control over their identity. As a result, we assess the level of *control* as low.

### 5.3.2. ASSESSMENT OF DPKI

To assess the trustworthiness of DPKI in X-Road, we use the presented earlier models and the surveys of the building blocks of the DPKI [1, 2, 3, 19, 23]. Thereby, we conduct a theoretical assessment of the X-Road system design before the actual implementation of the system prototype.

Following the made assumptions, the initial identities check, and decision about the issuance of the DID-based credentials should be conducted based on the attributes of other SSIcompatible VCs. As DIDs are unique within the DID method namespace, there is no need to check their uniqueness to allow the holder to use them. In essence, the issuance of the credentials and the update of expired credentials are automated. As Members and SSs can start using their credentials right after applying for their issuance, we assess the system *reliability* as high.

*Table 2: Results of trustworthiness assessment of IdM systems*

| IdM | Reliability | Security | Control |
|---|---|---|---|
| **PKI** | Medium | Medium | Low |
| **DPKI** | High | Medium | High |

The decentralisation of credentials and the root of trust allows us to eliminate a single point of failure in X-Road. However, the DPKI-based X-Road system becomes vulnerable to threats specific to

distributed ledgers (e.g., consensus mechanism attacks). Thereby, the *security* of the system is medium level.

Finally, the shift to the DPKI enables identities to have more control over their data. Moving to the DLT enables to preserve the privacy of the credentials holder because instead of creating public VCs signed by the issuer, which later are to be presented to a verifier, a zero-knowledge verifiable claim is issued to the holder who provides zero-knowledge proofs to the verifier. Such privacy preservation is delivered, for example, by the Sovrin ledger [20]. Thereby, the DPKI XRoad is supposed to enable control high level of *control* over the identities.

Among the limitation of using blockchain as storage for the credentials are (1) storage of public keys on-chain may be expensive or impossible (depending on the size of the PK and size of blocks); (2) there should be a limited number of developers (blockchain participants responsible for the code update, i.e. X-Road Operator representatives), validators (blockchain miners/validator, who are responsible for creating new blocks and authorizing transactions) and full nodes (that store the whole blockchain) in order to prevent 51% security attack.

# 6. Conclusion

The analysis of alternative system designs from the perspective of trustworthiness found that some designs were more trustworthy than others. The decentralised root of trust enabled by DPKI may help to improve system reliability as it enables the automated issuance and verification of credentials. DPKI gives users to have more control over their identity by letting them manage keys and credentials, which, on the other hand, poses higher responsibility. The ease of meeting prerequisites for a new system may vary depending on the industry, the specifics of the system, and the number of current system users.

Our work is limited to a theoretical design and assessment of the X-Road ecosystem. The next step is to develop a proof-of-concept prototype to apply the proposed identity management infrastructure. The prototype assessment will help to support the estimation results (or reject) of the system's trustworthiness and efficiency improvements of SSI-enabled members management in X-Road. While the current report presents the analysis of the decentralised root of trust in X-Road, in [25], we offer a more generalised approach to system analysis that should guide organisations that considers the transition to decentralised identity management.

Among the other aspect left out of the scope of the current research is the transportation layer of SSI. While DID-based credentials can rely on web-based protocol design using HTTPS [3], attention should be paid to the usage of DID Auth [24] for exchanging challenges and responses between an identity owner and a relying party during the TLS handshake.

It is vital to consider the following open discussion points for future work based on the current research results. First, while the current research considers the complete shift of the credentials to DID-based, there is a possibility to choose a hybrid IdM model, including PKI and DPKI. In the model, DPKI could be applied only to Member identities and sign certificates. In that case, Security Server identities were still based on PKI and certificates. Of course, having two different models would increase the overall complexity, but on the other hand, using PKI for authentication certificates does not pose any challenges for the business operations (namely, members onboarding) and would not cause any challenges with HTTPS and TLS. Second, it is unclear how much time it will take for current Members to prepare their SSI-compatible credentials and infrastructure to support the shift in X-Road. Finally, we believe that reliance on the DID-based credentials in X-Road also opens new possibilities and prospect functionalities for the information system and businesses in a broad sense. Thus, except for the mentioned speed up and mitigation of one point of failure, X-Road enabled by DPKI could allow Members to be more transparent in the network. For example, when a new service provider joins the network, others can check the provider's background and characteristics that are essential for them, such as whether the provider is accredited by the ISO 27000 standard. Meanwhile, SSI gives control over Member's identity, so they would choose which level of details they want to share (e.g., Member could prove to the network they have the mentioned certification but without revealing the issuer or the date of certification if it is sensitive information they want to protect). Following SSI principles can help information systems (including X-Road) support reputation systems and sharing economy.

# Bibliography


[1] C. Allen, A. Brock, V. Buterin, J. Callas, D. Dorje, C. Lundkvist, P. Kravchenko, J. Nelson, D. Reed, M. Sabadello, *et al.*, "Decentralized public key infrastructure. a white paper from rebooting the web of trust." https://github.com/WebOfTrustInfo/rwot1-sf/blob/ master/final-documents/dpki.pdf, 2015.

[2] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[3] A. Preukschat and D. Reed, *Self-sovereign identity*. Manning Publications, 2021.

[4] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *Available at SSRN 2580664*, 2015.

[5] K. Cameron, "The laws of identity," *Microsoft Corp*, vol. 12, pp. 8–11, 2005.

[6] World Wide Web Consortium (W3C), "Verifiable Credentials Data Model v1.1." https: //www.w3.org/TR/vc-data-model, March 2022.

[7] A. J. Slagell and R. Bonilla, "PKI scalability issues," *CoRR*, vol. cs.CR/0409018, 2004.

[8] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280, May 2008.

[9] World Wide Web Consortium (W3C), "Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations: Methods." https://www.w3.org/TR/ did-core/#methods.

[10] World Wide Web Consortium (W3C), "DID specification registries. the interoperability registry for decentralized identifiers." https://www.w3.org/TR/ did-spec-registries/#did-methods.

[11] M. Schaffner, "Analysis and evaluation of blockchain-based self-sovereign identity systems," Master's thesis, Technical University of Munich, Munich, Germany, 2020.

[12] B. Maier and N. Pohlmann, "Gaia-X secure and trustworthy ecosystems with Self Sovereign Identity," white paper, Gaia-X European Association for Data and Cloud AISBL, eco – Association of the Internet Industry, May 2022.

[13] H. Natarajan, S. Krause, and H. Gradstein, "Distributed ledger technology and blockchain," 2017.

[14] Nordic Institute for Interoperability Solutions (NIIS), "X-Road Academy." https:// x-road.thinkific.com/, 2020.

[15] Nordic Institute for Interoperability Solutions (NIIS), "X-Road Documentation." https: //github.com/nordic-institute/X-Road/tree/develop/doc.

[16] Nordic Institute for Interoperability Solutions (NIIS), “X-Road Resources.” https:// x-road.global/xroad-library.

[17] J. Huang, M. D. Seck, and A. Gheorghe, “Towards trustworthy smart cyber-physical-social systems in the era of internet of things,” in *SoSE*, pp. 1–6, 2016.

[18] S. Y. Lim, O. B. Musa, B. A. S. Al-Rimy, and A. Almasri, *Trust Models for BlockchainBased Self-Sovereign Identity Management: A Survey and Research Directions*, pp. 277– 302. Cham: Springer International Publishing, 2022.

[19] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, S. Bhatia, A. Mashat, A. Kumar, and M. Kumar, “Self-sovereign identity solution for blockchain-based land registry system: A comparison,” *Mobile Information Systems*, vol. 2022, pp. 1–17, April 2022.

[20] S. Foundation, “Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust,” white paper, January 2018.

[21] A. Tobin, “Sovrin: What Goes on the Ledger?,” white paper, Evernym, October 2018.

[22] P. Kivimäki, “Resisting Failure.” https://www.niis.org/blog/2020/11/20/ resisting-failure, 2020.

[23] R. Soltani, U. T. Nguyen, and A. An, “A survey of self-sovereign identity ecosystem,” *Security and Communication Networks*, vol. 2021, 2021.

[24] M. Sabadello, K. D. Hartog, C. Lundkvist, C. Franz, A. Elias, A. Hughes, J. Jordan, and D. Zagidulin, “Introduction to DID Auth.” https://github.com/WebOfTrustInfo/ rwot6-santabarbara/blob/master/draft-documents/did_auth_draft.md, 2018.

[25] M. Bakhtina, R. Matulevičius, A. Awad, and P. Kivimäki, “On the shift to decentralised identity management in distributed data exchange systems,” Accepted at *SAC’23: The 38th ACM/SIGAPP Symposium on Applied Computing, March 27 – April 2, 2023, Tallinn, Estonia, ACM, 2023*.