ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.2310 (03/2026)

SERIES X: Data networks, open system communications and security

Digital identity

Security requirements for decentralized identity management systems using distributed ledger technology

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1749
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1899
METAVERSE AND DIGITAL TWIN SECURITY	X.2000-X.2149
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249
DIGITAL IDENTITY	**X.2300-X.2399**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.2310

Security requirements for decentralized identity management systems using distributed ledger technology

Summary

Recommendation ITU-T X.2310 identifies security threats to confidentiality, integrity and availability (CIA) of decentralized identity management systems using distributed ledger technology (DLT) and specifies security requirements to address the identified security threats.

Based on use cases for decentralized identity management systems using DLT, this Recommendation defines decentralized identity management models (such as the basic model, the custody and delegation model and the self-issue model) and assurance levels (such as AL1 (low), AL2 (substantial) and AL3 (high)) accordingly. For example, the basic model can be applied to AL2 or AL3. The custody and delegation model can be applied to AL2 or AL3. In addition, the self-issue model can be applied to AL1; for example, aspects of claims, a driving licence can be applied to AL3. A vaccination certificate can be applied to AL2, and a digital business card can be applied to AL1.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.2310	2026-03-16	17	11.1002/1000/16741

Keywords

Assurance level, decentralized identity, distributed ledger technology (DLT), Identity (ID), identity management, security requirement.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at https://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Overview	3
6.1	Introduction	3
6.2	Models for decentralized identity management	3
7	Security threats and security requirements	13
7.1	Security threats	14
7.2	Security requirements	15
8	Governance considerations for protecting holders	17
8.1	Lifecycle management for credentials	17
8.2	Lifecycle management for identity wallets	18
8.3	Verification of relying parties	19
8.4	History management of credential presentation	19
8.5	Identity wallet protection	19
Appendix I – Use cases of decentralized identity management systems using DLT		20
I.1	Digital certificate system using QR codes	20
I.2	Digital certificate system using PAN	20
I.3	Driving licence	21
I.4	Digital badge	22
I.5	Digital business card	22
Bibliography		24

Recommendation ITU-T X.2310

Security requirements for decentralized identity management systems using distributed ledger technology

1 Scope

This Recommendation identifies security threats to decentralized identity management systems using distributed ledger technology (DLT) and specifies security requirements to address the identified security threats. It defines decentralized identity management models using DLT and assurance levels accordingly and provides use cases.

This Recommendation does not address issues related to regulation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 assurance level [b-ITU-T X.1252]: A level of confidence in the binding between an entity and the presented identity information.

3.1.2 Bluetooth [b-ISO 13111]: Communication protocol for exchanging data over short distances.

3.1.3 claim [b-ITU-T X.1252]: [noun] Digital assertion about identity attributes made by an entity about itself or another entity. [verb] To state as being the case, without being able to give proof.

3.1.4 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.5 digital signature [b-ISO 19784]: Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery, e.g., by the recipient.

NOTE – To entry: Digital signatures may be used for purposes of authentication, data integrity, and non-repudiation.

3.1.6 distributed ledger technology (DLT) [b-ITU-T X.1400]: Technology that enables the operation and use of distributed ledgers.

3.1.7 distributed ledger technology system [b-ITU-T X.1400]: A system that implements a distributed ledger.

3.1.8 entity [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in context.

3.1.9 holder [b-ITU-T X.1252]: An entity that has been issued a claim by an issuer. If the claim supports zero knowledge proofs (ZKPs), the holder is also the prover.

3.1.10 issuer [b-ITU-T X.1252]: The entity that issues a claim.

3.1.11 personal area network (PAN) [b-ISO 15045]: Any electronic network that connects to enabled devices within the immediate vicinity of a person, generally within a 10 m radius including devices carried by that person.

3.1.12 prover [b-ITU-T X.1252]: Entity that issues a proof from a claim. The prover is also the holder of the claim.

3.1.13 QR code [b-ISO 22453]: Machine-readable code consisting of an array of black and white squares, used for storing information for reading by the camera on a smartphone.

3.1.14 relying party (RP) [b-ITU-T X.1252]: An entity that relies on an identity representation or claim by a requesting/asserting entity within some request context.

3.1.15 trust anchor [b-ISO 23644]: An entity, device or information that is trusted by a relying party; or a legal instrument establishing or recognizing an entity or information as trustworthy.

3.1.16 verifier [b-ISO/IEC 29115]: Actor that corroborates identity information.

NOTE – The verifier can participate in multiple phases of the entity authentication assurance framework and can perform credential verification and/or identity information verification.

3.1.17 wallet (identity wallet) [b-ITU-T X.1403]: An application that primarily allows a user to hold identifiers and credentials by storing the corresponding private keys on the user device.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 custodian: An entity that safekeeps holders' critical information, including private keys and claims, in order to mitigate the risk of their theft or loss, through delegated controls from holders.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES Advanced Encryption Standard

AL Assurance Level

DBMS Database Management System

DLT Distributed Ledger Technology

IoT Internet of Things

PAN Personal Area Network

PII Personally Identifiable Information

QR Quick Response

RP Relying Party

RSA Rivest Shamir Adleman

SR Security Requirement

ST Security Threat

USB Universal Serial Bus

ZKP Zero Knowledge Proof

5 Conventions

None.

6 Overview

6.1 Introduction

A decentralized identity management system is a user-centric identity management system which consists of a holder, issuer, service provider (relying party (RP)), verifier and so on. Using distributed ledger technology (DLT) provides a decentralized identity management system with advantages such as maintaining the integrity of data stored in a DLT system and transparently sharing data among participants as nodes of a DLT system.

The holder operates identity wallets which store public/private key pairs and claims from issuers. The private key of the holder should be used for digital signatures to present a credential to a service provider (relying party). According to the importance of the claim, the holder should securely keep private keys to prevent identity theft. Also, the holder is required to securely preserve private keys and claims which include personally identifiable information (PII).

In some cases, the holder could issue a claim by providing essential information including PII, and the decentralized identity management system does not require any third-party issuers. In other words, the holder is also the issuer. For example, this applies to digital business cards, attendance credentials, travel visitor credentials, food and beverage (F&B) order credentials, etc. In many countries, decentralized identity management systems using DLT have been applied to vaccination certificates, driving licences, digital IDs, digital certificates, ID for the Internet of things (IoT), etc.

6.2 Models for decentralized identity management

There are three types of models for decentralized identity management: the basic model, the custody and delegation model and the self-issue model.

As listed in Table 6-1, the relying party requires an assurance level (AL) for the credentials presented by the holder. AL1 is applicable to the self-issue model. AL2 is applicable to either the basic model or the custody and delegation model. AL3 is applicable to either the basic model or the custody and delegation model.

Table 6-1 – Assurance level for credentials

Assurance level	Descriptions
AL1	• Low confidence is provided to relying parties for the credentials presented by holders. • Trust anchors are not required when issuing claims. • For example, digital business cards, certificate of attendance, travel visitor credential, food and beverage (F&B) order credential, etc.
AL2	• Substantial confidence is provided to relying parties for the credentials presented by holders. • Trust anchors could be required when issuing claims. • For example, vaccination certificate, graduate certificate, employee ID card, etc.
AL3	• High confidence is provided to the relying parties for the credentials presented by holders. • Trust anchors should be required when issuing claims. • For example, driving licence, digital passport, digital ID card, etc.

6.2.1 Basic model

The basic model consists of trust anchors, issuers, holders, relying parties, verifiers and DLT systems. These are role-based components. The trust anchor and the issuer could be the same entity. The relying party and the verifier could be the same entity. Trust anchors can be governments or organizations authorized by governments. A relying party could be a service provider. A DLT system is a kind of registry. Figure 6-1 illustrates the architecture of the basic model.

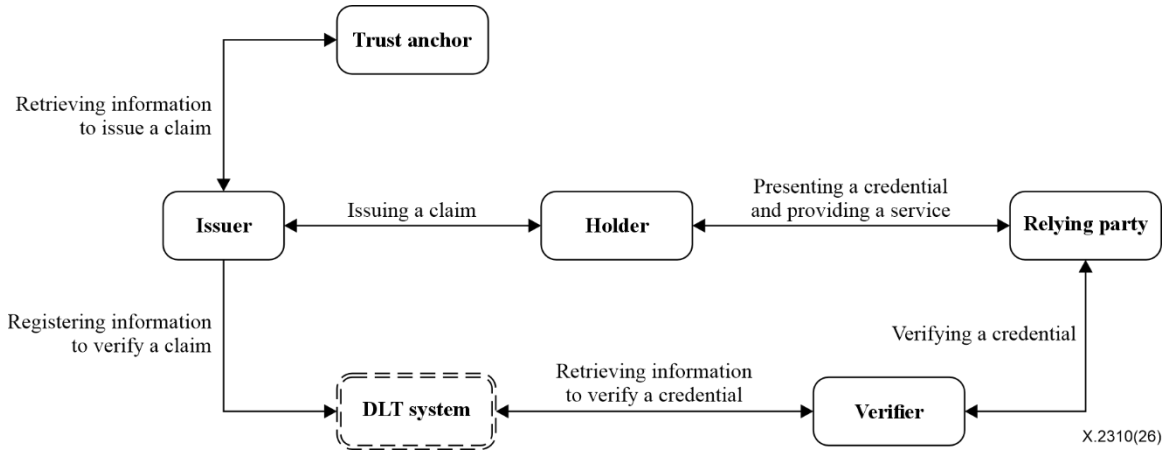


Figure 6-1 – Architecture of the basic model

In Figure 6-1, the roles of the components in the basic model are described as follows:

- The trust anchor stores and maintains information about the identity and/or entitlement of the holder and provides the issuer with this information.
- The issuer issues claims to the holder and registers information in a DLT system to verify those claims.
- The holder requests the issuer to issue claims and then receives the claims from the issuer. The holder presents credentials to a relying party in order to be provided with the services.
- The relying party provides services to the holder after verifying the credentials received from the holder. The relying party verifies the holder's credentials through the verifier.
- The verifier verifies the credentials received from the relying party through the DLT system and then responds to the relying party with the results of the verification.
- The DLT system stores and maintains information to verify the claim of the holder using distributed ledgers and it provides the verifier with the information.

In Figure 6-2, the service scenario and data flow in the basic model is described as follows:

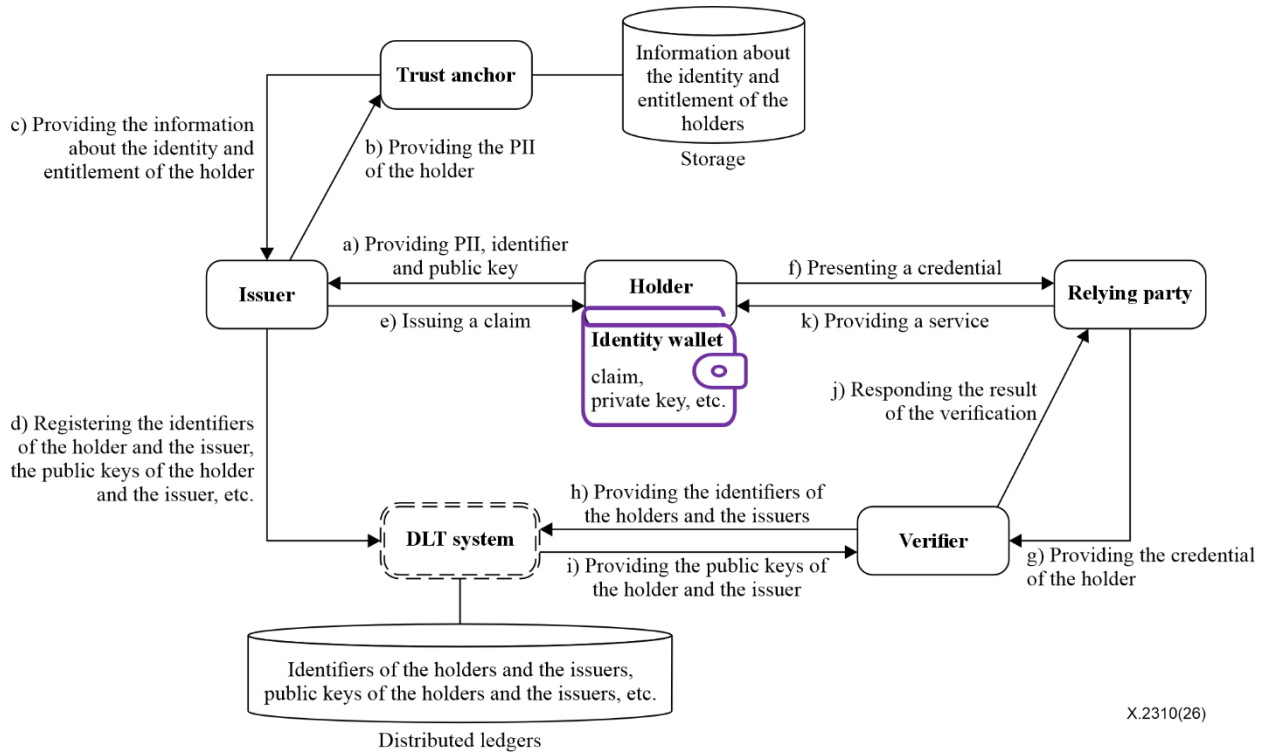


Figure 6-2 – Service scenario and data flow in the basic model

a) The holder provides an issuer with his/her personally identifiable information (PII), identifier and public key.

b) The issuer provides a trust anchor with the PII of the holder.

c) The trust anchor provides the issuer with the information about the identity and/or entitlement of the holder.

d) The issuer registers the identifiers of the holder and issuer, the public keys of the holder and issuer, plus other information to verify the claims.

e) The issuer issues claims to the holder. The claims include the digital signature of the issuer.

f) The holder presents credentials to a relying party. The credentials include the digital signatures of the issuer and holder. Either a quick response (QR) code or a personal area network (PAN) (e.g., Bluetooth, WiFi direct, etc.) could be utilized to present the credentials. Utilizing a PAN instead of a QR code could make it easier to simultaneously present multiple credentials (e.g., a digital passport and a vaccination certificate, etc.) to the relying party.

g) A relying party provides the verifier with the credentials received from the holder.

h) The verifier provides the DLT system with the identifiers of the holder and issuer.

i) The DLT system provides the verifier with the public keys paired with the identifiers of the holder and issuer.

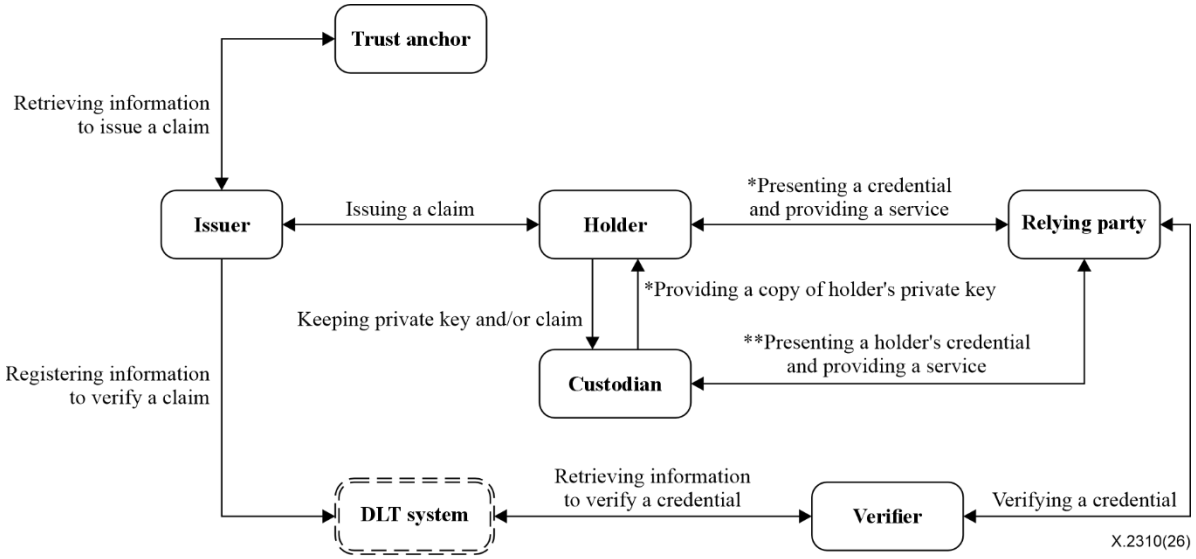
j) The verifier verifies the authenticity and validity of the credentials, the authenticity of the issuer and the authenticity of the holder (i.e., prover) and then returns the results of the verification to the relying party.

k) The relying party provides the holder with services in accordance with the results of the verification.

6.2.2 Custody and delegation model

The custody and delegation model consists of trust anchors, issuers, holders, custodians, relying parties, verifiers and DLT systems. These are role-based components. The trust anchor and the issuer could be the same entity. The relying party and the verifier could be the same entity. The trust anchors can be governments or organizations authorized by governments. A relying party could be a service provider. A DLT system is a kind of registry.

In Figure 6-3, the roles of the components in the custody and delegation model-1 are described as follows:



*: When the holder entrusts only the private key to the custodian
**: When the holder entrusts both the private key and claim to the custodian

Figure 6-3 – The architecture of the custody and delegation model-1

- The trust anchor stores and maintains information about the identity and/or entitlement of the holder and provides the issuer with this information.
- The issuer issues claims to the holder and registers information in a DLT system to verify those claims.
- The holder requests the issuer to issue claims and then receives the claims from the issuer. The holder entrusts the custodian with his/her private keys and/or claims. The holder presents his/her credentials to a relying party in order to be provided with the services, and the credentials should be digitally signed with a copy of the holder's private key stored and maintained by the custodian. The holder should remove the copy of the holder's private key after presenting the credentials.
- The custodian keeps private keys and/or claims received from the holder. If a holder is a legal person, a child, an elderly person or a digitally disabled person, a custodian, on behalf of the holder, presents the holder's credentials to the relying party in order to be provided with the services, and the credentials should be digitally signed with the holder's private key stored and maintained by the custodian. When a holder requests his/her private key from the custodian, the custodian provides a copy of the holder's private key to the holder.
- The relying party provides services to the holder or custodian after verifying the credentials received from the holder or custodian. The relying party verifies the holder's credentials through a verifier.
- The verifier verifies the credentials received from the relying party through the DLT system and then responds to the relying party with the results of the verification.

- The DLT system stores and maintains information to verify the claim of the holder using distributed ledgers and provides the verifier with the information.

In Figure 6-4, the first service scenario and data flow in the custody and delegation model-1 are described as follows:

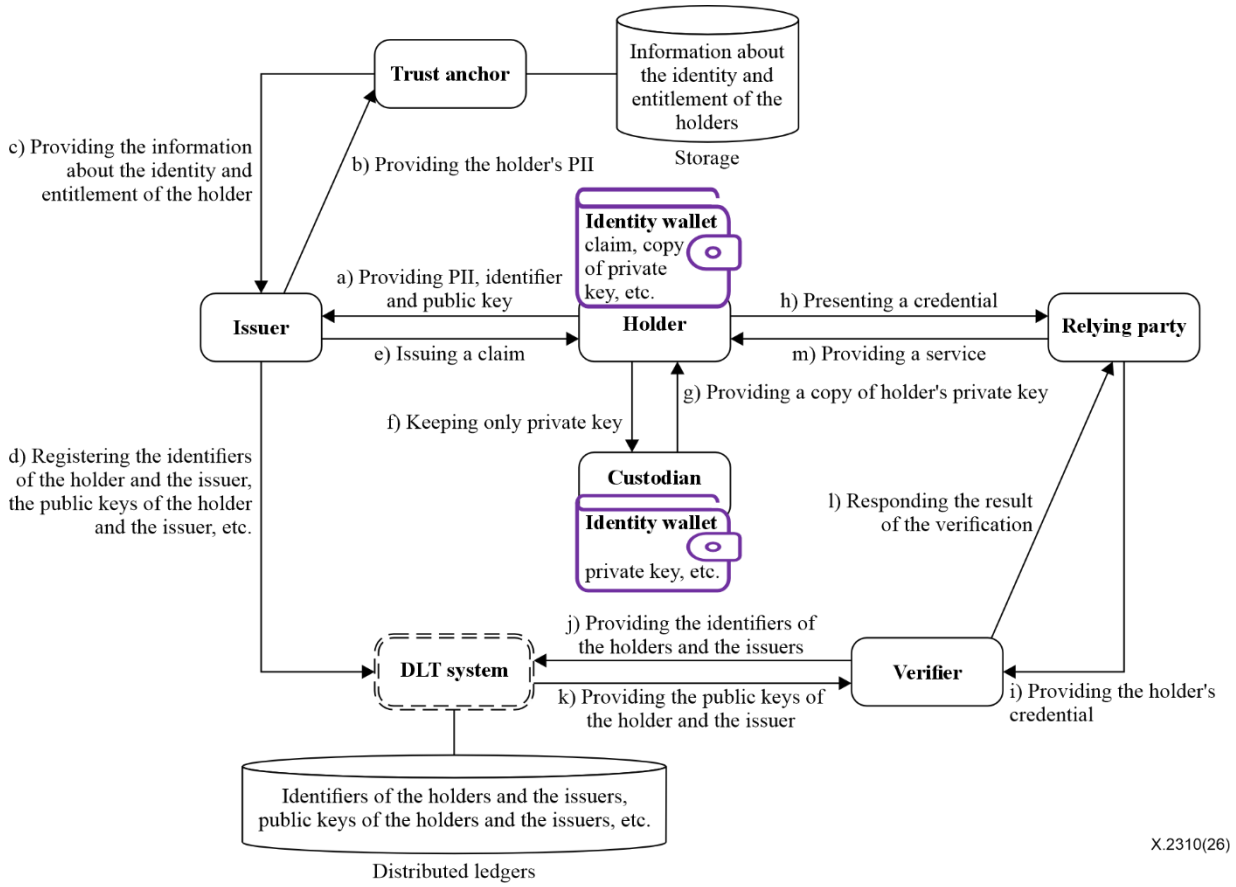


Figure 6-4 – First service scenario and data flow in the custody and delegation model-1

a) The holder provides the issuer with his/her PII, identifier and public key.

b) The issuer provides the trust anchor with the holder's PII.

c) The trust anchor provides the issuer with information about the identity and/or entitlement of the holder.

d) The issuer registers the identifiers of the holder and issuer, the public keys of the holder and issuer, plus other information to verify the claims.

e) The issuer issues claims to the holder. The claims include the digital signature of the issuer.

f) The holder entrusts only the private key to the custodian.

g) The custodian provides a copy of the holder's private key to the holder.

h) The holder presents credentials to the relying party. The credentials include the digital signatures of the issuer and holder. Either a QR code or a PAN (e.g., Bluetooth, WiFi direct, etc.) could be utilized to present the credentials. Utilizing PAN instead of a QR code could make it easier to simultaneously present multiple credentials (e.g., a digital passport and a vaccination certificate, etc.) to the relying party. The holder should remove the copy of the holder's private key after presenting the credentials.

i) The relying party provides the verifier with the credentials received from the holder.

j) The verifier provides the DLT system with the identifiers of the holder and issuer.

k) The DLT system provides the verifier with the public keys paired with the identifiers of the holder and issuer.

l) The verifier verifies the authenticity and validity of the credentials, the authenticity of the issuer and the authenticity of the holder (i.e., prover), and then returns the results of the verification to the relying party.

m) The relying party provides the holder with services in accordance with the results of the verification.

In Figure 6-5, the second service scenario and data flow in the custody and delegation model-1 are described as follows:

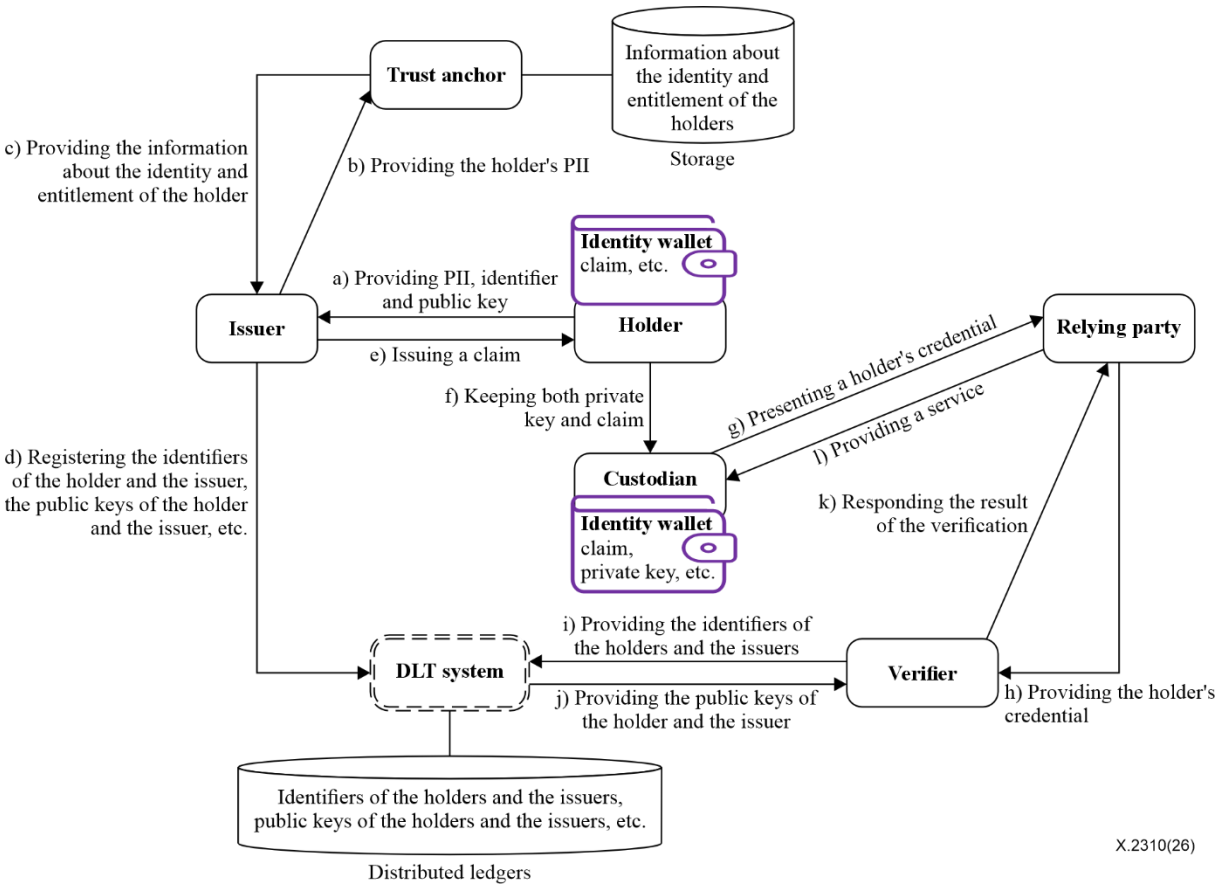


Figure 6-5 – Second service scenario and data flow in the custody and delegation model-1

a) The holder provides the issuer with his/her PII, identifier and public key.

b) The issuer provides a trust anchor with the holder's PII.

c) The trust anchor provides the issuer with information about the identity and/or entitlement of the holder.

d) The issuer registers the identifiers of the holder and issuer, the public keys of the holder and issuer, plus other information to verify the claims.

e) The issuer issues claims to the holder. The claims include the digital signature of the issuer.

f) The holder entrusts both the private key and claim to a custodian.

g) The custodian, on behalf of the holder, presents the holder's credentials to a relying party. The credentials include the digital signatures of the issuer and holder. Either a QR code or a PAN (e.g., Bluetooth, WiFi direct, etc.) could be utilized to present the credentials. Utilizing a PAN instead of a QR code could make it easier to simultaneously present multiple credentials (e.g., a digital passport and a vaccination certificate, etc.) to the relying party.

h) The relying party provides the verifier with the credentials received from the custodian.

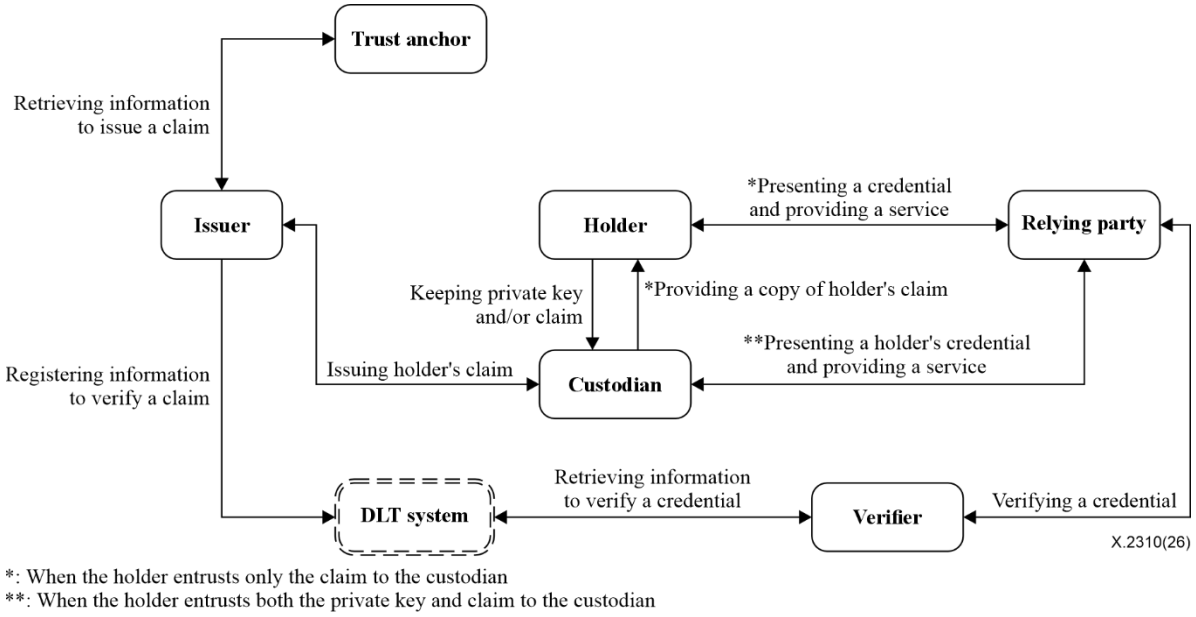
i) The verifier provides the DLT system with the identifiers of the holder and issuer.

j) The DLT system provides the verifier with the public keys paired with the identifiers of the holder and issuer.

k) The verifier verifies the authenticity and validity of the credentials, the authenticity of the issuer and the authenticity of the holder (i.e., prover), and then returns the results of the verification to the relying party.

l) The relying party provides the custodian with services in accordance with the results of the verification.

In Figure 6-6, the roles of the components in the custody and delegation model-2 are described as follows:



*: When the holder entrusts only the claim to the custodian
**: When the holder entrusts both the private key and claim to the custodian

Figure 6-6 – The architecture of the custody and delegation model-2

- The trust anchor stores and maintains information about the identity and/or entitlement of the holder and provides the issuer with this information.
- The issuer issues the holder's claims to a custodian and registers information in the DLT system to verify those claims.
- The holder requests the custodian to issue claims. The holder entrusts the custodian with his/her private keys and/or claims. The holder presents his/her credentials to a relying party in order to be provided with the services, and the credentials should include the holder's digital signature and the information from a copy of the holder's claim stored and maintained by the custodian. The holder should remove the copy of the holder's claim after presenting the credentials.
- The custodian requests that the issuer issues the holder's claims and then receives the claims from the issuer. The custodian keeps private the keys and/or claims received from the holder or issuer. If a holder is a legal person, a child, an elderly person or a digitally disabled person, a custodian, on behalf of the holder, presents the holder's credentials to a relying party in order to be provided with the services, and the credentials should be digitally signed with the holder's private key stored and maintained by the custodian. When a holder requests his/her claim from the custodian, the custodian provides a copy of the holder's claim to the holder.

- The relying party provides services to the holder or custodian after verifying the credentials received from the holder or custodian. The relying party verifies the holder's credentials through a verifier.
- The verifier verifies the credentials received from the relying party through a DLT system and then responds to the relying party with the results of the verification.
- The DLT system stores and maintains information to verify the claim of the holder using distributed ledgers and provides the verifier with the information.

In Figure 6-7, the first service scenario and data flow in the custody and delegation model-2 are described as follows:

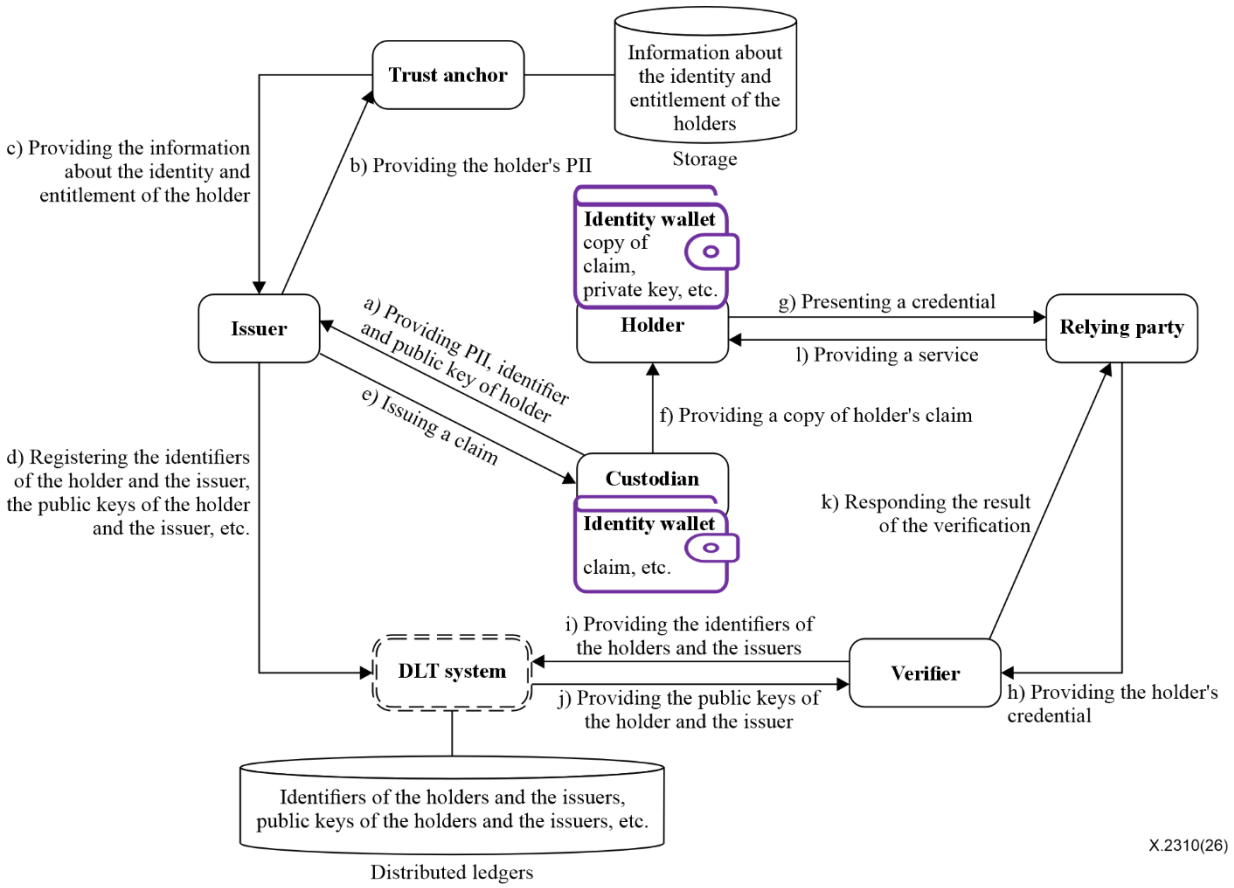


Figure 6-7 – First service scenario and data flow in the custody and delegation model-2

a) The custodian provides the issuer with the PII, identifier and public key of the holder.

b) The issuer provides the trust anchor with the holder's PII.

c) The trust anchor provides the issuer with information about the identity and/or entitlement of the holder.

d) The issuer registers the identifiers of the holder and issuer, the public keys of the holder and issuer, plus other information to verify the claims.

e) The issuer issues the holder's claims to a custodian. The claims include the digital signature of the issuer.

f) The custodian provides a copy of the holder's claim to the holder.

g) The holder presents credentials to a relying party. The credentials include the digital signatures of the issuer and holder. Either a QR code or a PAN (e.g., Bluetooth, WiFi direct, etc.) could be utilized to present the credentials. Utilizing a PAN instead of a QR code could make it easier to simultaneously present multiple credentials (e.g., a digital passport and a

vaccination certificate, etc.) to the relying party. The holder should remove the copy of the holder's claim after presenting the credentials.

h) The relying party provides a verifier with the credentials received from the holder.

i) The verifier provides a DLT system with the identifiers of the holder and issuer.

j) The DLT system provides the verifier with the public keys paired with the identifiers of the holder and issuer.

k) The verifier verifies the authenticity and validity of the credentials, the authenticity of the issuer and the authenticity of the holder (i.e., prover) and then returns the results of the verification to the relying party.

l) The relying party provides the holder with services in accordance with the results of the verification.

In Figure 6-8, the second service scenario and data flow in the custody and delegation model-2 are described as follows:

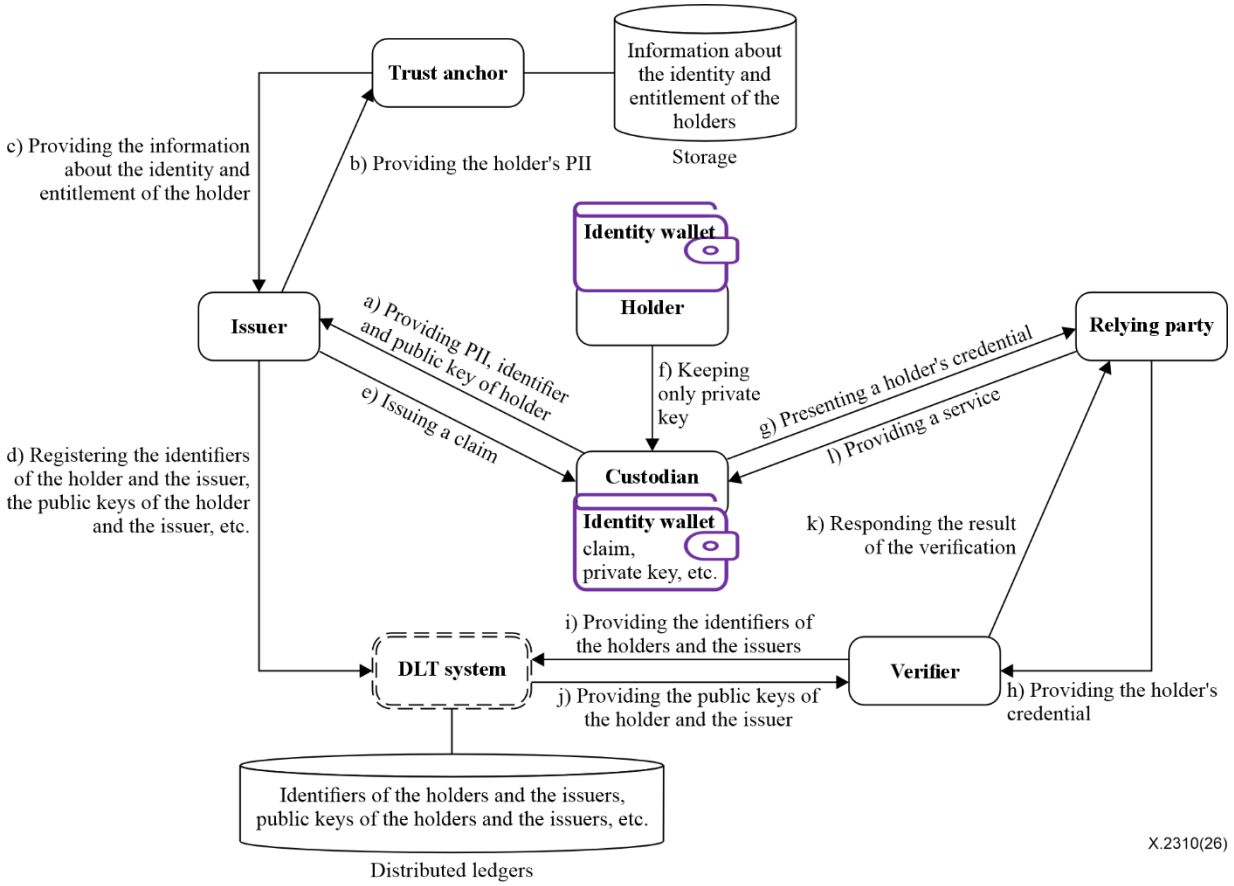


Figure 6-8 – Second service scenario and data flow in the custody and delegation model-2

a) The custodian provides the issuer with the PII, identifier and public key of the holder.

b) The issuer provides a trust anchor with the holder's PII.

c) The trust anchor provides the issuer with information about the identity and/or entitlement of the holder.

d) The issuer registers the identifiers of the holder and issuer, the public keys of the holder and issuer, plus other information to verify the claims.

e) The issuer issues the holder's claims to the custodian. The claims include the digital signature of the issuer.

f) The holder entrusts only the private key to the custodian.

g) The custodian, on behalf of the holder, presents the holder's credentials to a relying party. The credentials include the digital signatures of the issuer and holder. Either a QR code or a PAN (e.g., Bluetooth, WiFi direct, etc.) could be utilized to present the credentials. Utilizing a PAN instead of a QR code could make it easier to simultaneously present multiple credentials (e.g., a digital passport and a vaccination certificate, etc.) to the relying party.

h) The relying party provides a verifier with the credentials received from the custodian.

i) The verifier provides a DLT system with the identifiers of the holder and issuer.

j) The DLT system provides the verifier with the public keys paired with the identifiers of the holder and issuer.

k) The verifier verifies the authenticity and validity of the credentials, the authenticity of the issuer and the authenticity of the holder (i.e., prover) and then returns the results of the verification to the relying party.

l) The relying party provides the custodian with services in accordance with the results of the verification.

6.2.3 Self-issue model

The self-issue model consists of issuers, holders, relying parties, verifiers and registries. These are role-based components. The issuer and the holder should be the same entity. The relying party and the verifier could be the same entity. A relying party could be a service provider. A registry is implemented as either a DLT system or a non-DLT system (e.g., cloud system, storage system, database management system (DBMS), etc.).

Figure 6-9 shows the architecture of the self-issue model.

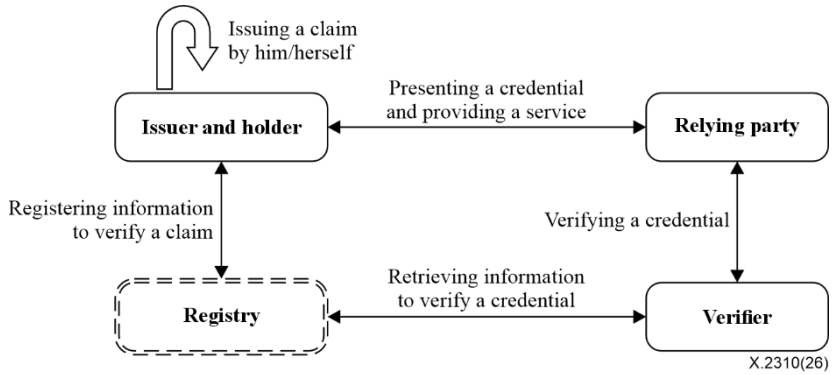


Figure 6-9 – Architecture of the self-issue model

In Figure 6-9, the roles of components in the self-issue model are described as follows:

- The issuer issues claims to the holder and registers information in the registry to verify those claims.
- The holder requests that the issuer issues claims and then receives the claims from the issuer. The holder presents credentials to a relying party in order to be provided with the services.
- The relying party provides services to the holder after verifying the credentials received from the holder. The relying party verifies the holder's credentials through a verifier.
- The verifier verifies the credentials received from the relying party through the registry and then responds to the relying party with the results of the verification.
- The registry stores and maintains information to verify the claim of the holder using distributed ledgers or storage and provides the verifier with the information. If the registry is implemented as a non-DLT system instead of a DLT system, the registry should reinforce the integrity of the information (e.g., prevent forgery of the information, etc.).

In Figure 6-10, the service scenario and data flow in the self-issue model are described as follows:

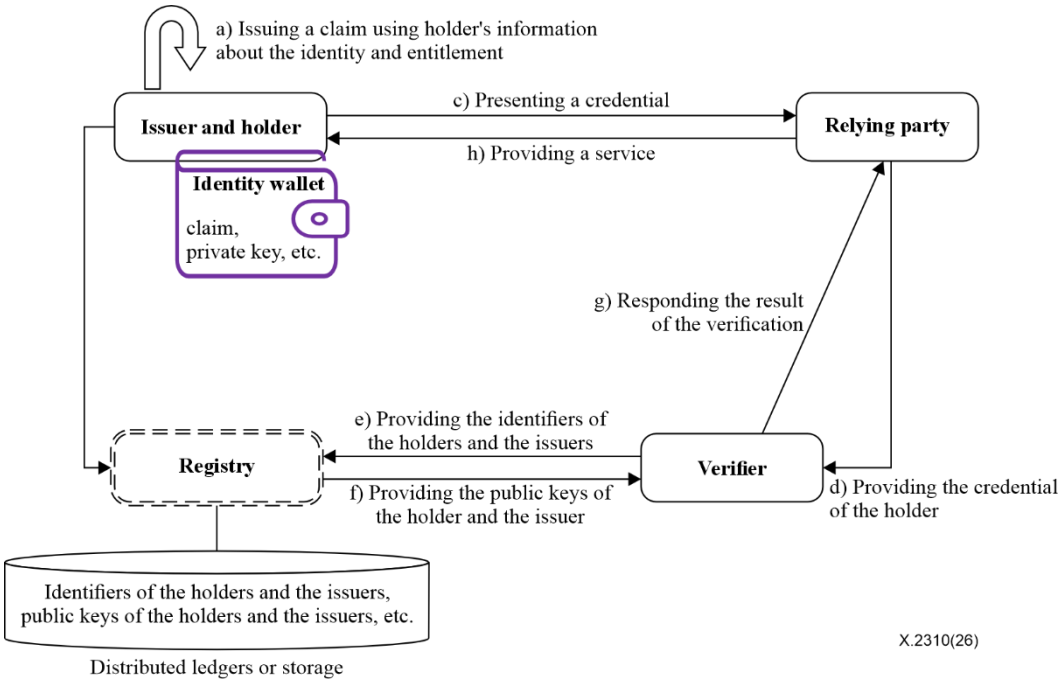


Figure 6-10 – Service scenario and data flow in the self-issue model

In Figure 6-10, the service scenario and data flow in the self-issue model are described as follows:

a) The holder provides the issuer with their information about the identity and/or entitlement and then the issuer issues claims to the holder. The claims include the digital signature of the issuer.

b) The issuer registers the identifiers of the holder and issuer, the public keys of the holder and issuer, plus other information to verify the claims. The identifiers of the holder and issuer could be the same, and the public keys of the holder and issuer could also be the same.

c) The holder presents credentials to a relying party. The credentials include the digital signatures of the issuer and holder. Either a QR code or a PAN (e.g., Bluetooth, WiFi direct, etc.) could be utilized to present the credentials.

d) The relying party provides a verifier with the credentials received from the holder.

e) The verifier provides the registry with the identifiers of the holder and issuer.

f) The registry provides the verifier with the public keys paired with the identifiers of the holder and issuer.

g) The verifier verifies the authenticity and validity of the credentials, the authenticity of the issuer and the authenticity of the holder (i.e., prover), and then returns the results of the verification to the relying party.

h) The relying party provides the holder with services in accordance with the results of the verification.

7 Security threats and security requirements

Potential security threats that could occur in decentralized identity management systems using DLT should be identified. Security requirements (SRs) should be specified to mitigate the identified security threats.

7.1 Security threats

Security threats (STs) to decentralized identity management systems using DLT, including the basic model, the custody and delegation model, and the self-issue model, as mentioned in clause 6, should be identified.

7.1.1 Theft of issuer's identity (ST-1)

An entity that is not authorized to issue a holder's claims could issue the claims by impersonating an issuer that is authorized to issue the claims. For example, a malicious entity seeking financial gain could impersonate a government agency (e.g., centre for disease control and prevention, national police agencies, etc.) to issue holders' digital vaccination certificates and driving licences. This could allow unvaccinated individuals and unlicensed drivers to use unauthorized credentials to falsely prove their qualifications. ST-1 is a security threat to the basic model and the custody and delegation model.

7.1.2 Theft of holder's identity (ST-2)

An entity that is not a real holder of a credential could impersonate the real holder of the credential when proving identity using the credential. For example, holder-2 could use holder-1's digital vaccination certificate and driving licence to prove his/her identity and pretend to be holder-1. These malicious credentials could be used for various crimes. ST-2 is a security threat to the basic model and the custody and delegation model.

7.1.3 Forgery of identity information (ST-3)

- ST-3-1: A holder could generate a fake credential with false and misleading information, without a claim received from the issuer, and present the credential to a relying party. A holder could generate a fake credential by manipulating part or all of the claim received from the issuer with false or misleading information and present the credential to the relying party. For example, a fake credential containing false or forged PII and qualification information (e.g., vaccination status, status of infectious disease testing, status of recovery from infectious disease, etc.) could be used to impersonate others. ST-3-1 is a security threat to the basic model and the custody and delegation model.
- ST-3-2: A holder could receive a fake claim by providing false PII (e.g., name, mobile phone number, email address, etc.) to the issuer and present a fake credential to a relying party. For example, a fake credential containing false PII could be used to impersonate others. ST-3-2 is a security threat to the self-issue model.

7.1.4 Abuse of credentials in QR code form (ST-4)

A holder could copy his/her credentials in QR code form using a screenshot or other method and provide it to others. The recipient of the credentials could impersonate the holder by using the credential. For example, holder-1 copies his/her vaccination certificate in QR code form using a screenshot and provide it to holder-2. Holder-2 can impersonate holder-1 by presenting the vaccination certificate at the airport. Holder-1 can even sell a copy of his/her vaccination certificate in QR code form to holder-2 for a certain amount (e.g., USD 100, EUR 100, etc.). ST-4 is a security threat to the basic model, the custody and delegation model and the self-issue model.

7.1.5 Leakage of critical information during the presentation of credentials (ST-5)

- ST-5-1: When presenting a holder's credentials in the form of a QR code to a relying party, the holder's critical information (e.g., PII, qualification information, financial information, medical information, etc.) contained in the credentials could be leaked when the QR code is scanned. For example, the individual's critical information (e.g., name, date of birth, name of infectious disease, etc.) contained in a vaccination certificate in the form of a QR code can be read when the QR code is scanned by others. ST-5-1 is a security threat to the basic model, the custody and delegation model and the self-issue model.

- ST-5-2: When presenting a holder's credentials to a relying party by PAN (e.g., Bluetooth, WiFi direct, etc.), the holder's critical information (e.g., PII, qualification information, financial information, medical information, etc.) contained in the credentials could be leaked during the transmission of the credential. For example, the critical information could be leaked during transmission between a holder's mobile device and a mobile device of a relying party connected by PAN. ST-5-2 is a security threat to the basic model, the custody and delegation model and the self-issue model.

7.1.6 Leakage of critical information when storing credentials and claims (ST-6)

- ST-6-1: When storing credentials in the storage of relying parties and verifiers, the large amount of critical information (e.g., PII, qualification information, financial information, medical information, etc.) of holders contained in the credentials could be leaked by unauthorized entities (e.g., malicious code, malware, etc.). ST-6-1 is a security threat to the basic model, the custody and delegation model and the self-issue model.
- ST-6-2: When storing claims in the storage of custodians, the large amount of critical information (e.g., PII, qualification information, financial information, medical information, etc.) of holders contained in the claims could be leaked by unauthorized entities (e.g., malicious code, malware, etc.). ST-6-2 is a security threat to the custody and delegation model.

7.1.7 Loss of private keys (ST-7)

A holder's private keys stored on his/her device could be lost. For example, if a holder's private key stored in his/her mobile device could be lost due to the device failure or loss, the holder should generate a new key pair (private key and public key) and register the new public key in a registry implemented as either a DLT system or a non-DLT system for the verification of the holder's credentials. ST-7 is a security threat to the basic model, the custody and delegation model and the self-issue model.

7.1.8 Unauthorized receipt of credentials by impersonating a relying party (ST-8)

When presenting a holder's credentials to a relying party by PAN (e.g., Bluetooth, WiFi direct, etc.), an entity impersonating the relying party could receive the credentials from the holder. For example, an entity impersonating a quarantine officer at the airport could receive the massive vaccination certificates from passengers by PAN. ST-8 is a security threat to the basic model, the custody and delegation model and the self-issue model.

7.1.9 Abuse of custodian's authority (ST-9)

If a holder entrusts a custodian with his/her key pair (private key and public key), the custodian could abuse the holder's public key to issue the holder's claim, and the custodian could abuse the holder's private key to present the holder's credentials to a relying party. For example, the custodian could make money by abusing the holder's claims and credentials. ST-9 is a security threat to the custody and delegation model.

7.2 Security requirements

Security requirements (SRs) should be specified to mitigate the identified security threats to decentralized identity management systems using DLT as described in clause 7.1

7.2.1 Verification of an issuer's identity (SR-1)

When issuing a claim to either a holder or a custodian, a digital signature using the issuer's private key should be provided and the issuer's public key should be stored in the DLT system. When verifying a holder's credentials, the identity of the issuer should be confirmed by verifying the issuer's digital signature using the issuer's public key stored in the DLT system. SR-1 mitigates ST-1 and ST-3-1.

7.2.2 Verification of a holder's identity (SR-2)

When issuing a claim to either a holder or a custodian, the issuer should store the holder's public key in the DLT system. When either the holder or custodian presents the holder's credentials to a relying party, they should provide a digital signature using the holder's private key. The verifier should confirm the identity of the holder by verifying the digital signature of the credentials using the holder's public key stored in the DLT system. SR-2 mitigates ST-2.

7.2.3 Verification of minimum PII (SR-3)

When issuing a claim to a holder, the issuer should verify the authenticity of the minimum PII received from the holder. For example, an issuer could verify the authenticity of a name and mobile phone number received from a holder through mobile phone authentication and could verify the authenticity of an email address received from a holder through email authentication. SR-3 mitigates ST-3-2.

7.2.4 Prevention from the copy of QR codes and the usage of copied QR codes (SR-4)

When generating a credential in QR code form, the QR code should be a dynamic QR code, not a static QR code. The dynamic QR code should be generated automatically at regular intervals (e.g., every 15 seconds, etc.). The dynamic QR code prevents a copied QR code from being used by checking the expiration date. The mobile device that generated the dynamic QR code should have an anti-screenshot function enabled. SR-4 mitigates ST-4.

7.2.5 Data encryption (SR-5)

- SR-5-1: A holder's critical information (e.g., PII, qualification information, financial information, medical information, etc.) contained in a credential in the form of a QR code should be encrypted using a secure cryptography algorithm (e.g., the advanced encryption standard AES-128, SEED-128, the Rivest Shamir Adleman RSA-2048, etc.). SR-5-1 mitigates ST-5-1.
- SR-5-2: A holder's critical information (e.g., PII, qualification information, financial information, medical information, etc.) contained in a credential should be encrypted using a secure cryptography algorithm (e.g., AES-128, SEED-128, RSA-2048, etc.) during the transmission of the credential by PAN (e.g., Bluetooth, WiFi direct, etc.). For example, the critical information should be encrypted during transmission between a holder's mobile device and a mobile device of a relying party connected by PAN. SR-5-2 mitigates ST-5-2.
- SR-5-3: The critical information (e.g., PII, qualification information, financial information, medical information, etc.) of holders contained in credentials that relying parties and verifiers retain should be encrypted using a secure cryptography algorithm (e.g., AES-128, SEED-128, etc.), if the information should be kept for a certain period. SR-5-3 mitigates ST-6-1.
- SR-5-4: The critical information (e.g., PII, qualification information, financial information, medical information, etc.) of holders contained in claims that custodians retain should be encrypted using a secure cryptography algorithm (e.g., AES-128, SEED-128, etc.), if the information should be kept for a certain period. SR-5-4 mitigates ST-6-2.

7.2.6 Data deletion (SR-6)

- SR-6-1: A relying party and a verifier should delete the critical information (e.g., PII, qualification information, financial information, medical information, etc.) of a holder contained in credentials after the verification of the credentials is complete, if the information does not need to be stored. SR-6-1 mitigates ST-6-1.
- SR-6-2: A custodian should delete the critical information (e.g., PII, qualification information, financial information, medical information, etc.) of a holder contained in claims

after the delegated authority from the holder has expired, if the information does not need to be kept. SR-6-2 mitigates ST-6-2.

7.2.7 Private key backup and recovery (SR-7)

A holder's private keys stored on his/her device should be backed up from the holder's device to external storage (e.g., universal serial bus (USB) memory, cloud system, etc.), and the holder's private keys should be recovered from the external storage to the holder's device. For example, a holder's private keys stored on his/her mobile device should be backed up from the holder's mobile device to a cloud system, and the holder's private keys should be recovered from the cloud system to the holder's mobile device. SR-7 mitigates ST-7.

7.2.8 Access control in wireless communication (SR-8)

When presenting a holder's credential to a relying party by PAN (e.g., Bluetooth, WiFi direct, etc.), the wireless communication radius between the holder's device and the relying party's device should be narrowed to minimize the possibility of an unauthorized third party connecting to the holder's device from a distance, and mutual authentication between the holder's device and the relying party's device should prevent an unauthorized third party from receiving the credential. For example, the distance between mobile devices could be measured using Bluetooth. SR-8 mitigates ST-8.

7.2.9 Security audit for custodians (SR-9)

The history for access to a holder's claim and key pair (private key and public key) entrusted to a custodian should be logged and should be reviewed regularly (e.g., at least once a month, etc.). The history for the issuance of a holder's claim and the presentation of the holder's credentials delegated to a custodian should be logged and should be reviewed regularly (e.g., at least once a month, etc.). SR-9 mitigates ST-9.

8 Governance considerations for protecting holders

Governance considerations for protecting holders of decentralized identity management services, including the basic model, the custody and delegation model and the self-issue model in clause 6, should be identified. These considerations are helpful for the development of countermeasures against potential security threats to the services.

8.1 Lifecycle management for credentials

Lifecycle management for credentials should be considered to prevent the theft of a holder's identity.

In Figure 8-1, the issuance, storage, migration, usage, suspension, reactivation and revocation phases of a lifecycle management model for credentials are described as follows:

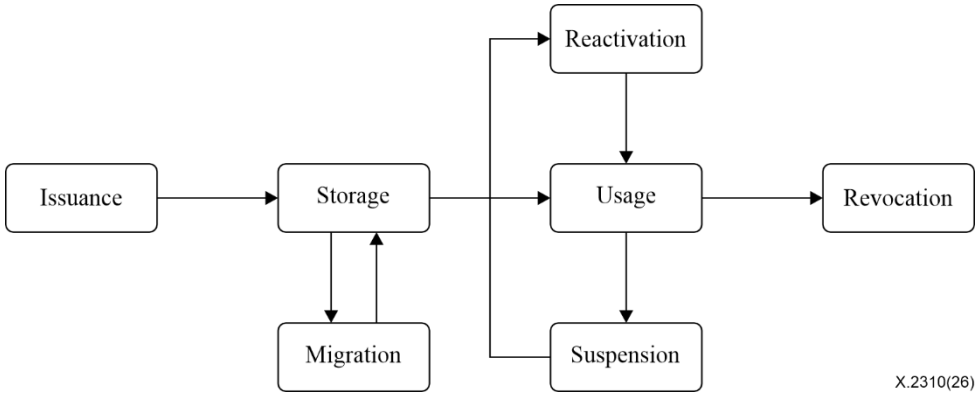


Figure 8-1 – A lifecycle management model for credentials

- Issuance: An issuer issues a holder's claim to the holder or to a custodian with authority delegated by the holder. The issuer should identify and authenticate the custodian. The issuer should verify the holder's PII received from the holder or the custodian. The information for verifying the issued claim should be stored in a DLT system.
- Storage: A holder's claim issued by an issuer is stored in an identity wallet running on the holder's device or a custodian's device, such as a smart phone. The claim could be stored in a cloud system.
- Migration: A claim in an identity wallet running on a holder's device is moved to an identity wallet running on a custodian's device. A holder's claim in an identity wallet running on a custodian's device is moved to an identity wallet running on the holder's device. A claim in an identity wallet running on a holder's device is moved to an identity wallet running on another device of the holder. During the movement of a credential, any data contained in the credential should not be tampered with.
- Usage: A holder presents his/her credentials to a relying party. The credentials are provided to a verifier, who then verifies the credentials using a DLT system.
- Suspension: A holder suspends the use of his/her credentials for a certain period. For example, a holder could suspend his/her driving licence until he/she purchases a vehicle.
- Reactivation: A holder resumes the use of their credentials that have been suspended. For example, a holder could reactivate their driving licence as soon as they purchase a vehicle.
- Revocation: A holder's claim is revoked after the expiration date. For example, a driving licence could be revoked after three years from the date of issue. The holder should receive a new claim issued by an issuer after the claim is revoked.

8.2 Lifecycle management for identity wallets

Lifecycle management for identity wallets should be considered for preventing the theft of a holder's identity.

In Figure 8-2, the generation, distribution, usage, migration, deactivation, reactivation and removal phases of a lifecycle management model for identity wallets are described as follows:

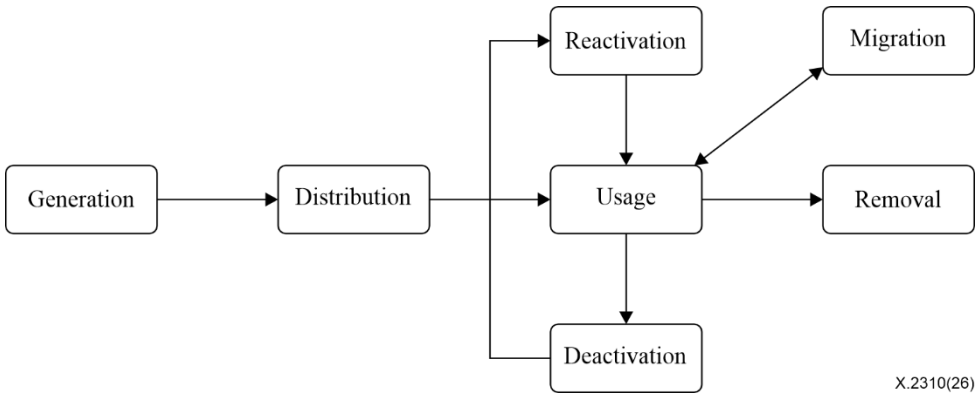


Figure 8-2 – A lifecycle management model for identity wallets

- Generation: A developer develops identity wallets by considering legal, functional and security requirements, and then tests whether these requirements are properly implemented.
- Distribution: A developer registers generated identity wallets on websites or online stores and ensures that the identity wallets cannot be tampered with while users (i.e., holders) download them.
- Usage: An identity wallet is installed on a holder's device (e.g., a smart phone), and a unique private/public key pair should be generated to verify the authenticity of the holder's credentials. The identity wallet should identify and authenticate the holder, and its usage

history should be securely stored and managed. Unauthorized access to the identity wallet by other applications running on the user's device should be prevented.

- Migration: The identity wallet installed on a holder's device is moved on to another device of the holder. During the movement of an identity wallet, any data stored in the identity wallet should not be tampered with.
- Deactivation: A holder suspends the use of their identity wallet for a certain period. Access to all data stored in a deactivated identity wallet should be prevented.
- Reactivation: A holder resumes the use of their identity wallet that has been suspended.
- Removal: A holder removes the identity wallet installed on their device. All data stored in the identity wallet should be deleted.

8.3 Verification of relying parties

The verification of relying parties should be considered for preventing leakage of a holder's identity information and PII. As a malicious entity could impersonate a relying party, holders should identify and authenticate relying parties before presenting their credentials to the relying parties. For example, a malicious entity impersonating a relying party could steal a holder's identity information and PII but could fail to provide any services to the holder.

8.4 History management of credential presentation

History management of credential presentation should be considered for identifying the theft of a holder's identity. An identity wallet running on a holder's device such as a smart phone should store and maintain the history of credential presentation. A relying party should store and maintain the history of credential verification. The holder should identify the theft of their identity by comparing between the history of credential presentation and verification.

8.5 Identity wallet protection

Identity wallet protection should be considered for preventing leakage of a holder's identity information and PII. As an identity wallet is running on a holder's device such as a smart phone, other applications running on the same device can access the identity wallet. Unauthorized applications could steal a holder's identity information and PII from the identity wallet. For example, as smart phones are always connected to the Internet, they are more susceptible to malware infections.

Appendix I

Use cases of decentralized identity management systems using DLT

(This appendix does not form an integral part of this Recommendation.)

I.1 Digital certificate system using QR codes

A certificate system using QR codes (e.g., static QR code, dynamic QR code, etc.) consists of issuers, holders, service providers and DLT systems. An issuer issues a claim requested by a holder who provides their PII to the issuer. The claim issued by the issuer is stored on the holder's mobile device. The issuer stores information to verify the authenticity and validity of the claim in the DLT system. A service provider verifies the authenticity and validity of a certificate presented by the holder using the information stored in the DLT system and provides a service to the holder if the verification is successful. When presenting the holder's credentials to the service provider, the holder generates a QR code containing the credentials on their mobile device, and the service provider scans the QR code with the camera on the service provider's mobile device. The DLT system stores and manages the information used to verify the authenticity and validity of the holder's claim.

Figure I.1 illustrates an example of a digital certificate system using the QR code.

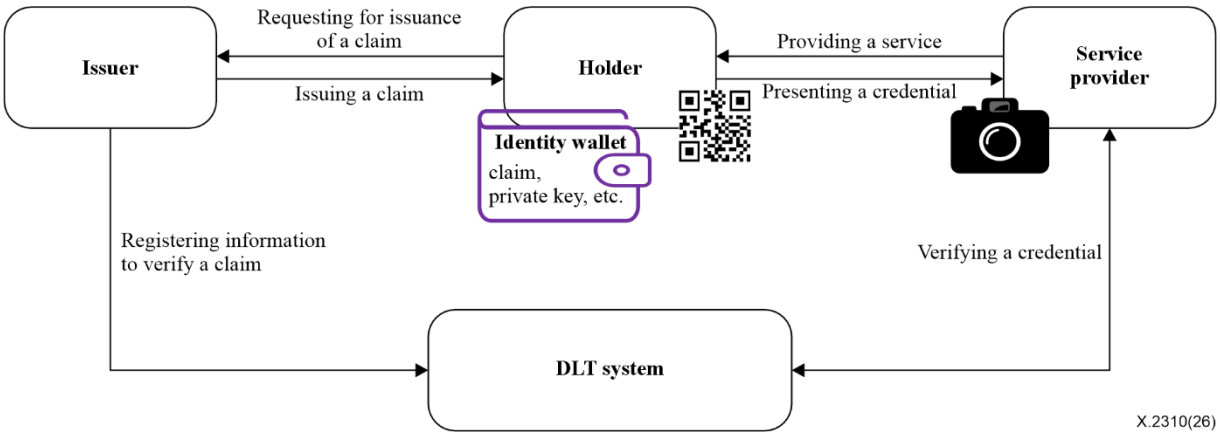


Figure I.1 – Example of a digital certificate system using QR code

I.2 Digital certificate system using PAN

A certificate system using PAN (e.g., Bluetooth, WiFi direct, etc.) consists of issuers, holders, service providers and DLT systems. An issuer issues a claim requested by a holder who provides his/her PII to the issuer. The claim issued by the issuer is stored on the holder's mobile device. The issuer stores information to verify the authenticity and validity of the claim in the DLT system. A service provider verifies the authenticity and validity of a certificate presented by the holder using the information stored in the DLT system and provides a service to the holder if the verification is successful. When presenting the holder's credentials to the service provider, the holder sends the credentials to the service provider by the Bluetooth and WiFi modules on the holder's mobile device, and the service provider receives the credentials by the Bluetooth and WiFi modules on the service provider's mobile device. Utilizing PAN instead of QR codes could make it easier to simultaneously present the holder's multiple credentials (e.g., a digital passport and a vaccination certificate, etc.) to the service provider. The DLT system stores and manages the information used to verify the authenticity and validity of the holder's claim.

Figure I.2 illustrates an example of a digital certificate system using a PAN.

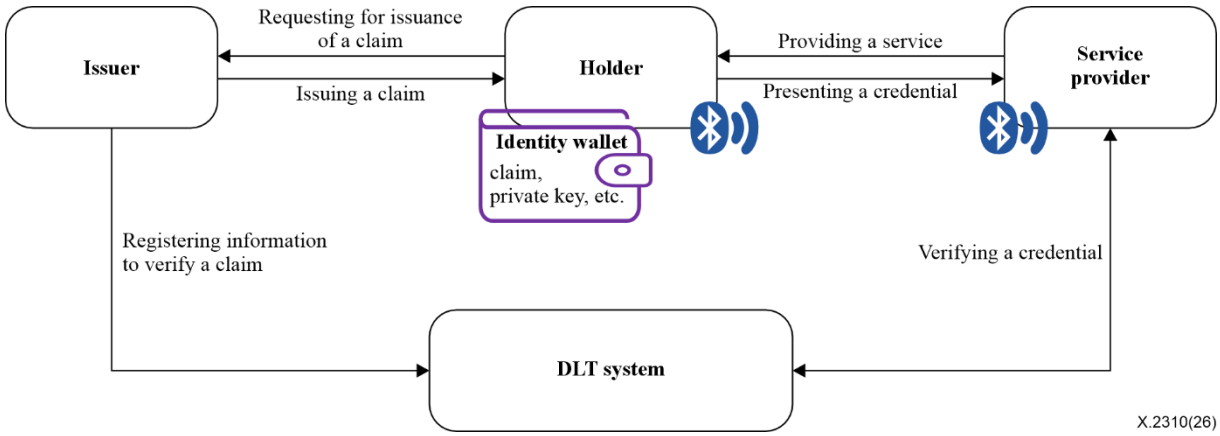


Figure I.2 – Example of a digital certificate system using PAN

I.3 Driving licence

In Figure I.3, the holder (i.e., a driving licence holder) requests the issuer to issue a claim such as a driving licence, which includes a digital signature of the commissioner of the district police agency. The trust anchor (e.g., a national police agency) provides the issuer with the information about the identity and/or entitlement of the holder. The issuer registers information to verify claims in the DLT system. The DLT system stores the information for claim issuance verification and claim status (e.g., validity, revocation). The holder stores the claim issued by the issuer in the identity wallet. The holder presents a credential to the verifier (i.e., service provider). The verifier verifies the authenticity of the credential received from the holder using the DLT system and provides a service to the holder in accordance with the result of the credential verification.

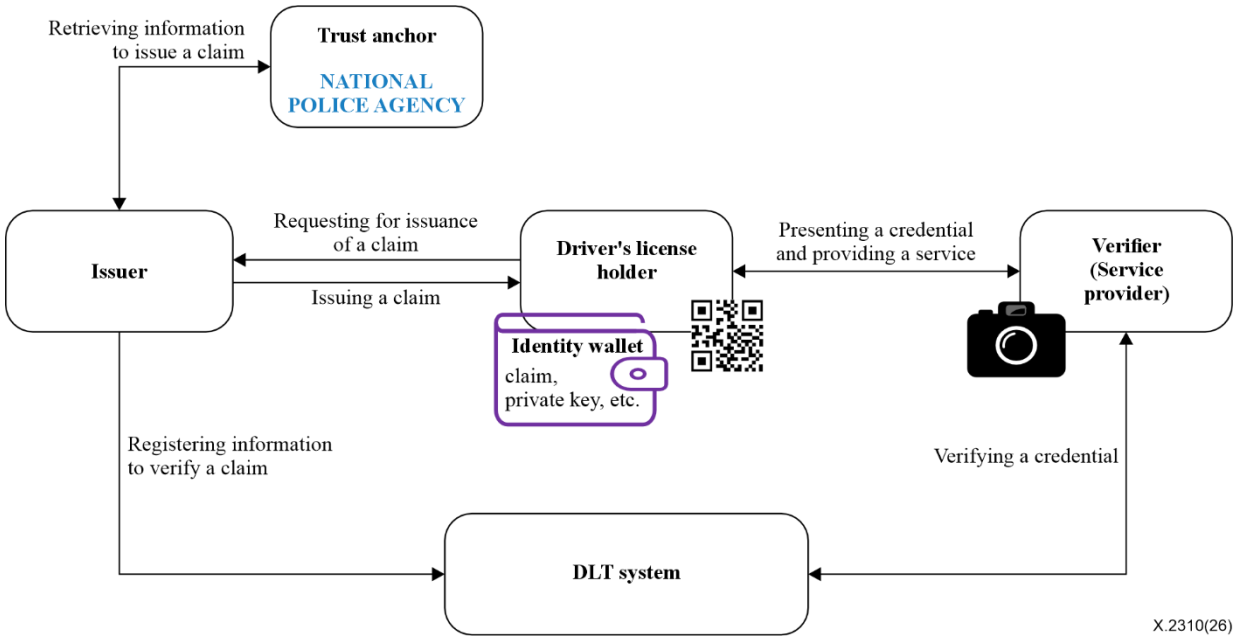


Figure I.3 – Example of a driving licence system using the basic model

I.4 Digital badge

In Figure I.4, the holder (i.e., job seeker) requests the issuer to issue claims such as academic certificates, certificates of qualification, career history, internship history and vocational training history. The issuer registers information to verify claims in the DLT system. The DLT system stores the information for certificate issuance verification, certificate issuance history, certificate verification history and certificate status (e.g., validity, revocation). The holder stores the claims issued by the issuer in an identity wallet. The holder presents credentials to the verifier (i.e., recruiter). The verifier verifies the authenticity of the credentials received from the holder using the DLT system.

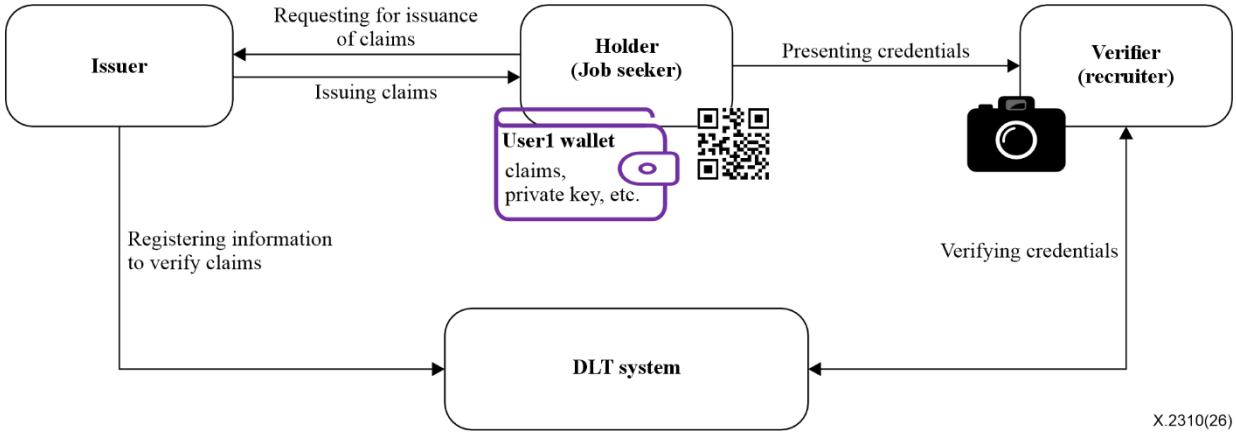


Figure I.4 – Example of a digital badge system using the basic model

I.5 Digital business card

Users can exchange digital business cards with each other using the self-issue model. Users can generate and manage digital business cards by directly entering their company name, their name, company phone number, mobile phone number, email address, company address, etc. on their mobile devices. Users register information to verify their digital business cards in the registry. Users can store and manage digital business cards received from others' mobile devices on their own mobile devices. Users verify digital business cards received from others' mobile devices using the registry. This reduces the costs of producing and storing physical business cards, and users can instantly generate and provide digital business cards to others even if they do not have physical business cards.

In Figure I.5, the users utilizing the proposed system should keep their mobile devices located within a short range (e.g., within a 40-meter radius) to ensure seamless Bluetooth and WiFi direct connections.

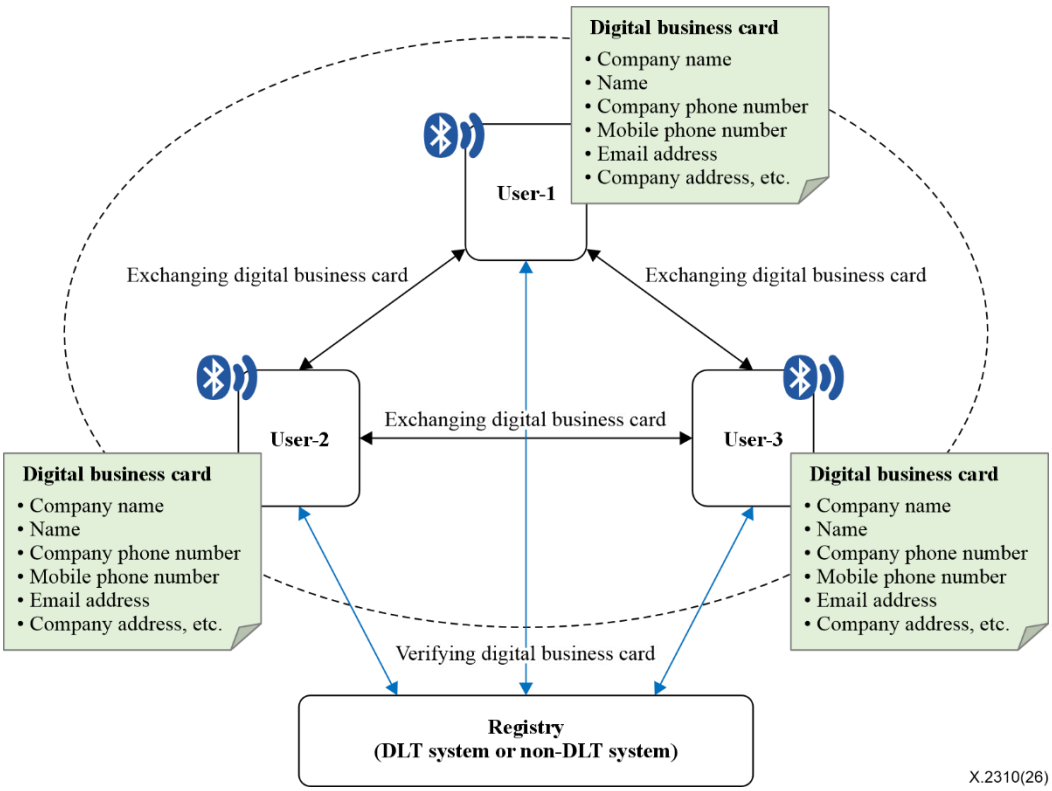


Figure I.5 – Example of a digital business card system using the self-issue model

Bibliography

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions.*

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2020), *Entity authentication assurance framework.*

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2026), *Terms and definitions for distributed ledger technology.*

[b-ITU-T X.1403] Recommendation ITU-T X.1403 (2020), *Security guidelines for using distributed ledger technology for decentralized identity management.*

[b-ISO 13111] ISO 13111-1:2017, *Intelligent transport systems (ITS) – The use of personal ITS station to support ITS service provision for travellers – Part 1: General information and use case definitions.*

[b-ISO 15045] ISO 15045-1:2004, *Information technology – Home Electronic System (HES) gateway – Part 1: A residential gateway model for HES.*

[b-ISO 19784] ISO/IEC 19784-1:2018, *Information technology – Biometric application programming interface – Part 1: BioAPI specification.*

[b-ISO 22453] ISO 22453:2021, *Exchange of information on rare earth elements in industrial wastes and end-of-life cycled products.*

[b-ISO 23644] ISO/TR 23644:2023, *Blockchain and distributed ledger technologies – Overview of trust anchors for DLT-based identity management*.

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information technology – Security techniques – Entity authentication assurance framework*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2026