Issuer Requirements Guide for Governance Frameworks of Verifiable Credentials

Governance Metamodel Compliant

Governance Stack Working Group

APPROVED DOCUMENT

Version .01

30 January 2024

This publicly available guide was approved by the ToIP Governance Stack Working Group on 30 January 2024. The ToIP permalink for this document is:

https://trustoverip.org/permalink/Issuer-Requirements-Guide-V0.01-2024-01-30.pdf

The mission of the Trust over IP (ToIP) Foundation is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. Founded in May 2020 as a non-profit hosted by the Linux Foundation, the ToIP Foundation has over 400 organisational and 100 individual members from around the world.

Please see the end page for licensing information and how to get involved with the Trust Over IP Foundation.

Table of Contents

Document Information

Authors

- Scott Perry — Schellman

Contributors

- Phil Feairheller – GLEIF
- Neil Thomson - QueryVision
- Steven Milstein - Collab.Ventures
- John Phillips - Sezoo
- Kyle Robinson

Revision History

Version	Date Approved	Revisions
0.1	11 Jan 2024	Draft approved by the Governance Stack Working Group
1.0		Approved by ToIP Steering Committee

Terms of Use

THESE MATERIALS ARE PROVIDED “AS IS.” The Trust Over IP Foundation, established as the Joint Development Foundation Projects, LLC, Trust Over IP Foundation Series ("ToIP"), and its members and contributors (each of ToIP, its members and contributors, a "ToIP Party") expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the materials. The entire risk as to implementing or otherwise using the materials is assumed by the implementer and user.

IN NO EVENT WILL ANY ToIP PARTY BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THESE MATERIALS, ANY DELIVERABLE OR THE ToIP GOVERNING AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RFC 2119

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and to ensure maximal efficiency in operation. IETF has been operating since the advent of the Internet using a Request for Comments (RFC) to convey "current best practice" to those organizations seeking its guidance for conformance purposes.

The IETF uses RFC 2119 to define keywords for use in RFC documents; these keywords are used to signify applicability requirements. ToIP has adapted the IETF RFC 2119 for use in the ToIP Issuer Requirements Guide, and therefore its applicable use in ToIP-compliant **governance frameworks**.

The RFC 2119[1] keyword definitions and interpretation have been adopted. Those users who follow these guidelines SHOULD incorporate the following phrase near the beginning of their document:

> **The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.**

RFC 2119 defines these keywords as follows:

- **MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.**
- **MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.**
- **SHOULD: This word, or the adjective "RECOMMENDED", means that there MAY exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.**
- **SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there MAY exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood, and the case carefully weighed before implementing any behavior described with this label.**
- **MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor MAY choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor MAY omit the same item.**

Requirements include any combination of Machine-Testable Requirements and Human-Auditable Requirements. Unless otherwise stated, all Requirements MUST be expressed as defined in RFC 2119.

- **Mandatories** are Requirements that use a MUST, MUST NOT, SHALL, SHALL NOT or REQUIRED keyword**.**
- **Recommendations** are Requirements that use a SHOULD, SHOULD NOT, or RECOMMENDED keyword.
- **Options** are Requirements that use a MAY or OPTIONAL keyword.

An implementation which does not include a particular option MUST be prepared to interoperate with other implementations which include the option, recognizing the potential for reduced functionality. As

[1] https://datatracker.ietf.org/doc/html/rfc2119. Accessed June, 2021.

well, implementations which include a particular option MUST be prepared to interoperate with implementations which do not include the option and the subsequent lack of function the feature provides.

Executive Summary

In a verifiable credential ecosystem, issuers play a crucial role in the issuance and validity of digital credentials. Verifiable credentials are a type of digital representation of claims or attributes about a subject, which can be an individual, organization, or thing. These credentials are tamper-evident, cryptographically secure, and can be verified by relying parties without the need for a central **authority**.

The responsibilities of an issuer in this ecosystem can be summarized as follows:

1. Issuance of Credentials: The issuer is responsible for creating and issuing verifiable credentials to subjects based on certain claims or attributes. These credentials are digitally signed by the issuer using their private key, ensuring the authenticity and integrity of the information.
2. Trust and Reputation: The issuer's reputation and trustworthiness are crucial in the verifiable credential ecosystem. **Relying parties** (such as service providers or verifiers) rely on the credentials issued by reputable and trusted issuers. The credibility of the issuer is established through various mechanisms, such as being a well-known organization, being part of a recognized **authority**, or holding themselves accountable to the requirements of a **governing authority**.
3. Validation of Claims: Before issuing credentials, the issuer does its due diligence to validate the claims made in the credential. This validation process ensures that the information presented in the credential is accurate and can be trusted by relying parties.
4. Verification of Issuer and Holder: Credentials that contain links to the issuer and/or holder must be built so they can be cryptographically verified.
5. Privacy Considerations: Issuers need to handle personal data responsibly and in compliance with privacy regulations. They should only collect and use the minimum necessary data required to issue the credentials and should obtain explicit consent from the subjects.
6. Revocation and Expiry: Issuers must have mechanisms in place to revoke or expire credentials if the claims become invalid or if the credentials are compromised. This is essential to maintain the trustworthiness of the digital trust ecosystem.
7. Interoperability: Issuers need to follow standardized formats and protocols to ensure that the issued credentials are interoperable and can be easily understood and verified by different relying parties.
8. Auditability and Accountability: Issuers should keep records of issued credentials for audit purposes, lifecycle maintenance, including updates to claims, or re-issuance for any reason and revocation. This enables traceability and accountability in case of disputes or issues with the credentials.
9. **Transparency:** Public disclosure about how an issuer verifies claims, sources of claims, makes decisions, how and why it revokes and how it supports validation of authority (as an issuer), authenticity of the supporting claims and other data is core to establishing trust, including (at some later evolution) being able to support run-time, on demand proofs.

The ToIP Issuer Requirements Guide is intended to provide ToIP Governance Metamodel-compliant requirements for issuers of verifiable credentials within an ecosystem governed by a **governance framework** that conforms to the ToIP Governance Metamodel Specification.

Purpose and Usage of this Document

This document is to be used as a guide for including ToIP recommended issuer requirements within a **governance framework**. This guide assumes that issuers exist within a governed ecosystem that supports verifiable credentials. While most material in this document should be appropriate for a wide range of **governance frameworks**, each **governing authority** will need to tailor the specific content. This may involve adding and removing material from this guide as needed to accommodate the needs and constraints for their particular **governance framework**.

This guide is intended to be used by governance architects that are devising a **governance framework** that conforms with the Trust Over IP governance metamodel. Completed documents using this guide will be used by all stakeholders of a **governance framework** to establish rules, policies, procedures and accountability measures for governance framework requirements.

As this document is intended to provide Issuer-related content to a **governance framework**, the structure of this document will follow the Governance Metamodel Specification.

1. Primary Document

Issuer requirements SHOULD be conveyed within the scope of **governance framework** (GF) and not under a separate document.

Issuer requirements MAY be consolidated within a **controlled document** but that document MUST be tied to a **governance framework**.

Issuers that are addressing requirements from multiple **governance frameworks** MAY create their own issuer policy document for their own purposes. If this is created, it MUST have a **DID** (decentralized identifier) that serves as an identifier of the entire GF and MUST have a unique **DID URL** (as defined in the W3C Decentralized Identifiers 1.0 **specification**) to identify each specific version of the **primary document**.

1.1 Introduction

No stipulation

1.2 Terminology and Notation

All referenceable terms SHOULD be aligned with the ToIP Reference Glossary. Terms that are bolded are referenced within the Glossary.

1.3 Governing Authority

Issuer requirements derived from this document SHOULD be under the legal **authority** of a **governing authority**.

1.4 Administering Authority

If an **administering authority** acts to administer a governance framework, issuer requirements derived from this document SHOULD be under the legal **authority** of an **administering authority**.

1.5 Purpose

If the issuer role is critical to the operation of a **governance framework**, then their role MAY be described in this section of the GF.

1.6 Scope

If issuers are a primary governed role in the **trust community** of a GF, their role SHOULD be included in the scope section of a GF.

Suggested language for issuer scope:

1. **Trust and Reputation**: The issuer's **reputation** and **trustworthiness** are crucial in the verifiable credential ecosystem. **Relying parties** (such as service providers or verifiers) rely on the **credentials** issued by reputable and trusted issuers. The credibility of the issuer is established through various

mechanisms, such as being a well-known organization, being part of a recognized **authority**, or holding themselves accountable to the requirements of a **governing authority**.

2. **Validation of Claims**: Before issuing credentials, the issuer validates the claims made within the credential. This validation process ensures that the information presented in the credential is accurate and can be trusted by relying parties.
3. **Issuance of Credentials**: The issuer is responsible for creating and issuing verifiable credentials based on certain claims or attributes contained within. These credentials are digitally signed by the issuer using their private key, ensuring the authenticity and integrity of the information.
4. **Verification of Issuer and Holder**: Credentials that contain links to the issuer and/or holder must be built so they can be cryptographically verified.
5. **Privacy Considerations**: Issuers need to handle personal data responsibly and in compliance with privacy regulations. They should only collect and use the minimum necessary data required to issue the credentials and should obtain explicit consent from the subjects.
6. **Revocation**: Issuers SHOULD have mechanisms in place to revoke if the claims become invalid or if the credentials are compromised. This is essential to maintain the trustworthiness of the digital trust ecosystem.
7. **Expiry**: Issuers MAY include expiration dates within the verifiable credential based on whether the claims made within the verifiable credential have a defined lifetime.
8. **Renewal:** Issuers may use processes to renew claims made within a verifiable credential after an elapsed period of time.
9. **Interoperability**: Issuers need to follow standardized formats and protocols to ensure that the issued credentials are interoperable and can be easily understood and verified by different relying parties.
10. **Auditability and Accountability**: Issuers SHOULD keep records of issued credentials for audit purposes, lifecycle maintenance, including updates to claims, or re-issuance for any reason and revocation. This enables traceability and accountability in case of disputes or issues with the credentials.
11. **Transparency:** Public disclosure about how an issuer verifies sources of claims, how and why it revokes and how it supports validation of authority (as an issuer), authenticity of the supporting claims and other data is core to establishing trust, including (at some later evolution) being able to support run-time, on demand proofs.

1.7 Objectives

Issuer high-level outcomes desired by the **trust community** SHOULD be conveyed in the Objectives section of the GF.

placeholder for suggested objectives.

1.8 Principles

Principles stated in a GF SHOULD serve as a guide to the development of issuer policies, rules and requirements.

placeholder for suggested Issuer -related principles.

1.9 General Requirements

No stipulation

NOTE: General requirements in a GF typically apply to the community as a whole and not to specific roles. Therefore, issuer requirements are typically not found in this section:

1.10 Revisions

No stipulation.

1.11 Extensions

No stipulation

1.12 Schedule of Controlled Documents

No stipulation

2. Issuer Requirements in Controlled Documents

2.1 Glossary

Unique issuer terminology needed to form a common reference SHOULD be included in the glossary section of a GF

2.2 Risk Assessment

Issuer related risks SHOULD be considered as part of an ecosystem-wide **risk assessment** and documented in the risk assessment section of a GF

Risk assessments SHOULD consider the following issuer **risks**:

- Credential Issued without issuer control of its private key
- Credential Issued before appropriate proofing of basis
- Credential Issued in the wrong format or structure
- Credential issued to impostors
- Credential issued to wrong holder
- Credential issued to wrong subject
- Credential lacking uniqueness
- Credential becoming obsolete
- There is no or effective means to communicate a revoked status of a credential.
- Identity proofing practices inadequate for **level of assurance**
- Issuer practices not accepted by ecosystem
- Issuer operations unavailable

2.3 Trust Assurance and Certification

Trust assurance and **certification** of issuers SHOULD be included in a **trust assurance framework** that defines a scheme in which they assert compliance with the **policies** of the GF and the mechanisms of assurance over those assertions.

For more information regarding a template that MAY be used to create a **trust assurance framework**, please see Trust Assurance and Certification Controlled Document Template V1.0 (PDF) For guidance in writing such a framework, see Trust Assurance and Certification Companion Guide V1.0 (PDF).

2.4 Governance Requirements

2.4.1 Issuer Identification

For the issuer, this section:

a) MUST state the full legal identity including **jurisdiction**(s).
b) MUST state the **D**ecentralized **ID**entifier (**DID)**.
c) SHOULD include a unique identifier for the **governing authority** such as the Legal Entity Identifier (LEI) as defined by the Global Legal Entity Foundation (GLEIF) or other jurisdictionally recognized identifier..
d) MAY include reference to the vLEI (by DID) associated with the LEI
e) MUST provide contact information for official communication with the issuer
f) SHOULD provide contact information for official persons acting on behalf of the issuer.

2.4.2 Trust Registry

An issuer SHOULD be registered within a **trust registry** governed by an **governance framework**.

2.4.3 Registration Agents

If implemented as part of issuer roles, **registration agents** (RAs), the part of the issuer's infrastructure that performs proper due diligence about claims and their data sources prior to verifiable credential issuance, MUST have a significant control structure that enables reliability of high value verifiable credentials. An issuer or (RA) SHOULD develop **"levels of assurance**" to indicate their confidence level with respect to the level of due diligence and/or the "quality" of the claim/sources.

An issuer MAY elect to use a third-party to perform registration agent duties as long as the issuer takes complete responsibility for the RAs actions.

2.4.4 Credential Usage

An issuer MAY state the appropriate usage of the credentials it issues.

An issuer SHOULD state when there are prohibited usages of credentials it issues.

2.4.5 Repositories

Issuers MUST store or distribute all credentials issued by the issuer in a manner that it is readily verifiable by all verifiers identified in an ecosystem. If this storage is beyond the issuer's control, it SHOULD be stored in a holder-controlled GF compliant **digital wallet** or verifiable data registry.

Public keys needed for verifiable credential verification SHOULD be stored in a publicly accessible repository system that shall be designed and implemented to provide <99%> availability overall and limit scheduled down-time to <0.5%> annually.

2.4.6 **Governance Framework** or Credential Policy

The requirements that guide the issuance and life-cycle management of verifiable credentials MUST be documented in a publicly available **governance framework** that details issuer requirements for that role within a specific ecosystem. Issuers MAY subscribe to multiple ecosystems and follow multiple **governance frameworks**. Therefore, an issuer MAY create an issuer-centric credential policy to document its policies and requirements in the marketplace. An updated version of this policy SHOULD be made publicly available within thirty days of the incorporation of changes. A **governance framework** SHOULD define clear roles and contacts for members of the **governance authority** as well as the issuers.

3 Business Requirements

3.1 Identification, Authorization and Validation

3.1.1 Identifiers

The issuer MUST comply with an ecosystem **governance framework** VC data model specification – adding a compliant field for itself as the issuer and, if required, for the subject of a credential.

Issuer and subject identifiers, if used in credentials, MUST represent unambiguous identifiers.

Identifiers SHOULD be meaningful enough for a human to identify, irrespective of whether the identifier represents a person, machine, or process.

Issuer and subject identifiers MUST be derived from authoritative sources as defined in an ecosystem **governance framework**.

Issuers SHOULD notify holders, upon credential receipt, of their responsibility regarding personally identifiable data.

Issuers SHOULD adhere to jurisdictionally enforceable privacy laws regarding personally identifiable information throughout the credential issuance process. .

Issuers MUST use mechanisms while storing and transporting verifiable credentials that protect the data from those who SHOULD NOT access it.

Issuers SHOULD use rules for **identifiers** that are specified in the W3C data model. Rules for interpreting e-mail addresses are specified in [RFC 2822].

To create uniqueness of credentials, an issuer SHOULD use the *id* property as outlined in the W3C data model specification.

3.1.2 Issuer Identification and Authority

The issuer SHOULD use a Legal Entity Identifier to define itself in verifiable credentials as required by a ecosystem **governance framework**.

The identity of an issuer MUST be verifiable within the content of a credential to a publicly accessible source such as a DID record.

3.1.3 Organizational Subject Authentication

Before issuing credentials that recognise a delegated authority such as **organizational authority** or a **guardianship arrangement**, the issuer SHOULD validate the subject's authority to act in the name of the organization.

If organizational identity is used as a key trust component of a verifiable credential, before issuing the credential, the **registration agent** (RA) for the issuer MUST verify the subject's organizational information in addition to the authenticity of the requesting organizational representative and their authorization to act in the name of the organization.

The issuer SHOULD use a **legal entity identifier** for organizational subjects as required by a ecosystem **governance framework**.

The RA MUST verify the identity and address of the subject using documentation provided by, or through communication with, at least one of the following:

- Official communication with the organization.
- A third-party database that is periodically updated and considered a reliable data source.
- A site visit by the issuer or a third party who is acting as an agent for the issuer.

3.1.4 Individual Subject Authentication

If human identity is a key trust component in a verifiable credential, the issuer SHOULD ensure that the subject's identity information is verified based on the **level of identity assurance** asserted.

Identity SHOULD be verified before a set time (e.g. no more than 30 days) before initial credential issuance to ensure integrity of the subject's identity.

Issuers MAY accept authentication of a subject's identity attested to and documented by a registration agent proxy to support identity proofing of subjects. Authentication by a registration agent proxy does not relieve the Issuer of its responsibility to authorize the issuance of a credential.

Authentication procedures SHOULD conform to NIST SP 800-63 Digital Identity Guidelines or equivalent.

If the recipient of a verifiable credential is not the subject, (e.g guardian, proxy, etc.), then the recipient's identity MUST be verified and their basis to act on behalf of the subject MUST be validated to the same degree as the recipient of a verifiiable credential.

3.1.5 Device Subject Authentication

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as credential subjects. In such cases, an Authorized Organizational Representative (AOR), or in certain cases the device itself MUST provide identifying information for the device. The AOR/device is responsible for providing registration information which MAY include:

- Equipment identification (e.g., serial number)
- Equipment authorizations and attributes (if any are to be included in the credential)
- Contact information to enable the issuer to communicate with the AOR when required.

The registration information provided by the AOR/device SHOULD be verified. The identity of the AOR/device SHOULD be authenticated.

3.1.6 Application or Service Authentication

Some software applications or services will be named as credential **subjects**. In such cases, an **Authorized Organizational Representative** (AOR) MUST provide identifying information for the device. The AOR is responsible for providing registration information which MAY include:

- Unique software application or service name (e.g., DNS name)

- Specific identifiable version of the software (e.g. version number)
- Software application or service authorizations and attributes (if any are to be included in the credential
- Contact information to enable the issuer to communicate with the AOR when required.

The registration information provided by the AOR SHOULD be verified. The identity of the AOR shall be authenticated. The issuer MUST validate that the AOR is the owner of the application or service by checking the appropriate and reliable 3rd party database.

3.1.7 Role Credential Authentication

For **role credentials** that identify subjects by their organizational roles, the issuer SHOULD validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

A **role credential** MAY identify a specific role on behalf of which the subject is authorized to act rather than the subject's name. A role credential MUST NOT be a substitute for an individual subject credential. Multiple individuals MAY be assigned to a role at the same time.

Holders issued **role credentials** SHOULD protect the corresponding role credentials to the same security level as individual credentials.

The procedures for issuing **role credentials** SHOULD comply with all other stipulations of this Specification (e.g., subject identity proofing, validation of organization affiliation, key generation, private key protection, holder obligations). The AOR MAY act on behalf of the credential subject for credential lifecycle activities such as issuance, renewal, re-key, modification, and revocation.

The issuer SHOULD record the information identified for an AOR associated with the role before issuing a **role credential**. The AOR SHOULD hold an individual credential in the subject's own name issued by the same issuer at the same or higher assurance level as the role credential. The issuer SHOULD receive a signed validation from the AOR that the subject has been approved for the role credential.

AORs shall be responsible for:

- Authorizing subjects for a **role credential**.
- Recovery of the private key.
- Revocation of subject's **role credentials**.
- Always maintaining a current up-to-date list of individuals who are assigned the role; and
- Always maintaining a current up-to-date list of individuals who have been provided the private keys for the role.

3.1.8 Validation of Other Claims within a Verifiable Credential

An issuer SHOULD disclose the level of validation for all claims made within a verifiable credential before issuance.

An issuer SHOULD maintain trustworthy and consistent processes for verification of claims prior to issuance as specified by a **trust assurance framework**.

An issuer MAY tailor the degree of validation measures used for claims made on verifiable credentials subject to a **level of assurance** scheme as defined in a **governance framework**.

3.2 Credential Revocation

Credential revocation requests from the issuer, holder or authorized third party MUST be verified, including verification of the identity of the requesting party.

Requests to revoke a credential MAY be authenticated using an ecosystem **governance framework** -compliant verification process.

A request to revoke a credential SHOULD identify the credential to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally signed). The requirements involved in the process of requesting a certification revocation SHOULD be detailed in a credential policy.

A credential SHOULD be revoked when the claims made using the binding between the issuer and the issuer's public key included within the credential is no longer considered valid. This would also hold true if the subject's public key is included in the credential. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the credential becomes invalid.
- (Role) Privilege attributes asserted in the subject's credential are reduced.
- The subject can be shown to have violated the stipulations of its subject agreement.
- There is reason to believe the private key has been compromised.
- The subject or other authorized party (as defined in a **governance framework** or credential policy) asks for his/her credential to be revoked.

Whenever any of the above circumstances occur, the associated credential SHOULD be revoked, and its status SHOULD be properly updated. Revoked credentials MAY be included on all new publications of the credential status' information until the credentials expire.

Within its span of **authority**, an issuer MAY summarily revoke credentials under its credential policy or a **governance framework**.

A notice and brief explanation for the revocation SHOULD subsequently be provided to the subject or their proxy.

The RA MAY request the revocation of a subject's credential on behalf of any authorized party as specified in a credential policy or **governance framework**.

A subject MAY request that its own credential be revoked.

The AOR of the organization that owns or controls a device MAY request the revocation of the device's credential.

Issuers SHOULD revoke credentials as quickly as practical upon receipt of a proper revocation request.

3.3 Personnel Requirements

3.3.1 Trusted Roles

Trusted role operations include:

- The validation, authentication, and handling of information in credential applications
- The acceptance, rejection, or other processing of credential applications, revocation requests, renewal requests, or enrolment information
- The issuance, or revocation of credentials, including personnel having access to restricted portions of its repository.
- Access to safe combinations and/or keys to security containers that contain materials supporting production services.
- Access to private key protection devices, their associated keying material, and the secret share splits of the access that protect access to the devices.
- Providing enterprise customer support
- Access to any source code for the issuer systems.
- Access to restricted portions of the credential repository
- The ability to grant physical and/or logical access to the issuer equipment.
- The ability to administer the background investigation policy processes.

Mandatory **trusted roles** MUST be defined in an ecosystem **governance framework**. Multiple people MAY hold the same **trusted role**, with collective privileges sufficient to fill the role. Other **trusted roles** MAY be defined in other documents, which describe or impose requirements on the issuer operation as mandated by the **governing authority** overseeing this specification.

The issuer SHOULD maintain lists, including names, organizations, contact information, and organizational for those who act in trusted roles, and MUST make them available during compliance audits (if applicable).

3.3.1.1 System Administrator

The system administrator role SHOULD be responsible for:

- Installation, configuration, and maintenance of the issuer systems.
- Establishing and maintaining issuer system accounts
- Configuring credential profiles or templates
- Configuring issuer audit parameters
- Generating and backing up issuer keys
- Controlling and managing issuer private key container devices
- System backups and recovery
- Changing recording media

System administrators do not issue credentials to subjects.

3.3.1.2 Issuer Operation Staff

The issuer operation staff role SHOULD be responsible for issuing credentials, that is:

- Approving issuer credentials issued to support the operations of the issuer.

- Approving revocation of credentials issued to the issuer or to support the operations of the issuer.
- Approving access rights or credentials issued to RAs.
- MAY be a **registration agent**
- Authorizing RAs
- Approving revocation of credentials issued to RAs.
- Providing credential revocation status information
- Posting credentials

3.3.1.3 Registration Agents

Registration Agents are the individuals holding trusted roles that register, issue, and revoke subject credential, that is:

1. Registering new credentials
2. Verifying the identity of subjects (if applicable)
3. Verifying the accuracy of information included in credentials.
4. Approving and executing the issuance of credentials
5. Approving, and executing the suspension, restoration, and revocation of credentials
6. MAY be a member of the issuer operations staff

3.3.1.4 Internal Auditor

Internal auditors are responsible for auditing issuer systems and processes. This sensitive role MUST NOT be combined with any other sensitive role (e.g., the internal auditor MUST NOT also be a system administrator, **registration agent**, or a member of the issuer operations staff).

Internal auditors are responsible for reviewing, maintaining, and archiving issuer activity such as application and security audit logs, and for performing or overseeing internal audits (independent of external compliance audits) to ensure that the issuer is operating in accordance with these requirements or **governance framework** requirements.

3.3.2 Qualifications and Training Requirements

Personnel seeking to become a **trusted role** MUST present proof of the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any **trusted role** MUST meet the following:

- Be employees of or contractor/vendor of the issuer and bound by terms of employment or contract.
- Have successfully completed an appropriate training program.
- Have demonstrated the ability to perform their duties.
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 3.1

3.3.3 Background Check Procedures

Persons fulfilling **trusted roles** SHOULD pass a standard employment background check. The level of background check SHOULD be commensurately increased with the **level of assurance** of the credentials being issued. Background checks SHOULD be renewed every 5-15 years depending on the **level of assurance** of the credentials being issued.

Prior to commencement of employment in a **trusted role**, the issuer shall conduct background checks (in accordance with local privacy laws) which include the following:

- Confirmation of previous employment
- Confirmation of the highest or most relevant educational degree obtained.
- Search of criminal records (local, state, or provincial, and national)
- Identification verification via foundational identity credentials, as applicable

Factors revealed in a background check that SHOULD be considered grounds for rejecting candidates for **trusted roles** or for taking action against an existing trusted person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or trusted person
- Certain criminal convictions

3.3.4 Training Requirements

All personnel performing duties with respect to the operation of the issuer SHOULD receive comprehensive training. Training SHOULD be conducted in the following areas:

- Issuer security principles and mechanisms
- All issuer software in use
- All issuer duties they are expected to perform.
- Disaster recovery and business continuity procedures
- Stipulations of this policy

All individuals responsible for issuer **trusted roles** SHOULD be made aware of changes in the issuer operation. Any significant change to the operations SHOULD be supported with applicable training. Examples of such changes are issuer software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation SHOULD be maintained identifying all personnel who received training and the level of training completed.

3.3.5 Number of Persons Required per Task

Where **multi-party control** is required, all participants MUST hold a **trusted role**. **Multi-party control** shall not be achieved using personnel that serve in an internal or external auditor role except for audit functions. The following tasks SHOULD require two or more persons:

- Generation, activation, and backup of issuer private keys

- Performance of issuer systems administration or maintenance tasks
- Archiving or deleting issuer system audit logs. At least one of the participants shall serve in an Internal or External Auditor role.
- Physical access to issuer equipment (servers, private key protection devices)
- Access to any copy of the issuer private key protection device
- Processing of third party private key recovery requests

3.3.6 Identification and Authentication for Each Role

Individuals holding **trusted roles** MUST identify themselves and be authenticated by the issuer systems before being permitted to perform any actions set forth above for that role or identity. Issuer operations staff MUST authenticate using a credential that is distinct from any credential they use to perform non-trusted role functions. This credential MUST be generated and stored in a system that is protected to the same level as the issuer signing credential.

Issuer equipment SHOULD require, at a minimum, strong authenticated access control for remote access using the most stringent Class credentials as those being issued by the issuer.

Individuals holding **trusted roles** SHOULD be appointed to the **trusted role** by an appropriate approving **authority**. The approval SHOULD be recorded in a secure and auditable fashion. Individuals holding **trusted roles** SHOULD accept the responsibilities of the **trusted role**, and this acceptance shall be recorded in a secure and auditable fashion.

Users MUST authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, and so on) before they can access that resource.

3.3.7 Authentication: Activation Data and Accounts

When the authentication mechanism uses activation data to allow access to private keys for operation, this data MUST use **biometrics** or **complex passwords**. The definition of this data shall be employed, as defined in its credential policy or **governance framework**. If passwords are used for issuer system authentication, they MUST be different from non-issuer systems.

The issuer SHOULD have the minimum number of accounts that are necessary to its operation. Account access SHOULD be locked after 3 to 5 unsuccessful login attempts. Restoration of access MUST be performed by a different person who holds a **trusted role**.

3.3.8 Roles Requiring Separation of Duties

Individuals serving as internal auditors MUST not perform or hold any other **trusted role**. An individual that holds a systems administrator or issuer operations role SHOULD NOT be an RA.

An individual serving in an internal auditor MUST only perform internal auditing functions, except for those internal audit functions (e.g., configuring, archiving, deleting) that require multi- person control.

An individual that performs any trusted role MUST only have one unique identity when accessing issuer equipment for tracking purposes.

3.4 Audit Logging Procedures

Audit log files MUST be generated for all events relating to the security of the issuer systems. Where possible, the security audit logs SHOULD be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism SHOULD be used. All security audit logs, both digital and paper based, SHOULD be retained and made available during compliance audits.

3.4.1 Timestamping

All issuer activities MUST be correlated within five minutes of an atomic clock source. atomic clock. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments SHOULD be considered auditable events.

3.4.2 Types of Events Recorded

All security auditing capabilities of an issuer operating system and applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event.
- The date and time the event occurred.
- Success or failure where appropriate, and
- The identity of the entity and/or operator that caused the event.

A message from any source requesting an action by the issuer SHOULD be considered an auditable event; the corresponding audit record MUST also include message date and time, source, destination, and contents.

The issuer SHOULD record the events identified in the list below. Where these events cannot be digitally electronically logged, the issuer SHOULD supplement digital audit logs with paper-based logs, as necessary.

- AUDIT LOGS:
  - Any changes to the audit parameters, e.g., audit frequency, type of event audited.
  - Any attempt to delete or modify the audit logs.
  - Obtaining a third-party timestamp
- IDENTIFICATION AND AUTHENTICATION:
  - Successful and unsuccessful attempts to assume a role.
  - The value of maximum authentication attempts is changed.
  - Maximum unsuccessful authentication attempts occur during user login.
  - An administrator unlocks an account that has been locked because of unsuccessful authentication attempts.
  - Attempts to set passwords.
  - Attempts to modify passwords.
  - Logon attempts to issuer applications.
  - Escalation of access privilege/rights
- KEY GENERATION:

  - Whenever the issuer generates a key. (Not mandatory for single session or one-time use symmetric keys)
- ISSUER PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - All changes to issuer public keys
- CREDENTIAL REGISTRATION:
  - All credential requests.
- CREDENTIAL VALIDATION
  - All source evidence used to validate the claim(s) made on a credential
- CREDENTIAL REVOCATION:
  - All credential revocation requests and revocation actions.
- ACCOUNT ADMINISTRATION:
  - Issuer **trusted roles** and users are added or deleted.
  - The access control privileges of a **trusted role** account or a role are modified.
  - Appointment of an individual to a **trusted role**
  - Configuration of a multi-party control scheme
- CERTIFICATE PROFILE MANAGEMENT:
  - All changes to the credential profile/template
- PHYSICAL ACCESS / SITE SECURITY:
  - Personnel access to room housing issuer systems
  - Physical access to the issuer server
  - Any removal or addition of equipment to/from the issuer systems cage (Equipment sign-out and return)
- PROCESSING INCIDENTS:
  - System incidents.

3.4.3 Frequency of Processing Log

Audit logs SHOULD be reviewed at least once every 90 days. All significant events SHOULD be reviewed, and actions taken because of these reviews SHOULD be documented.

Such reviews SHOULD involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

Real-time automated analysis tools SHOULD be used. All alerts generated by such a system SHOULD be analyzed.

3.4.4 Retention Period for Audit Log

Audit logs SHOULD be retained on-site for at least one month. in addition to being archived as described in section 4.3. The individual who removes audit logs from the Issuer system SHOULD be a **trusted role**.

3.4.5 Protection of Audit Log

Audit data SHOULD not be open for modification by any human, or by any automated process, other than those that perform audit processing.

Digital logs MUST be protected to prevent alteration and detect tampering. Examples include digitally signing audit records or the transfer of logs to a separate system to prevent modification after the log is written to media.

Audit data SHOULD be moved to a safe, secure storage location separate from the location where the data was generated.

Trusted roles MUST archive or delete audit data. Procedures SHOULD be implemented to protect archived data from deletion or destruction before the end of the data retention period.

3.5 Records Archival

3.5.1 Types of Events Archived

Archive records SHOULD be sufficiently detailed to determine the proper operation of the issuer and the validity of any credential (including those revoked or expired) issued by the issuer.

The following data SHOULD be recorded for archive:

- Issuer accreditation (if applicable)
- Credential policy
- Credential practices or process documents
- Credential schema(s) used for all issued credentials
- Contractual obligations (users, service providers, registrations, etc.)
- Credential due diligence evidence
- All Audit logs (per section 4.2.2)
- Audit log exception or audit summary reports
- All changes to the trusted public keys, including additions and deletions.
- Incident reports relevant to issuer operations

3.5.2 Retention Period for Archive

Archive records MUST be kept for the time that issued credentials are active or by a stated term documented in a **governance framework** or stipulated by jurisdictional law.

3.5.3 Protection of Archive

No unauthorized user SHOULD be permitted to write to, modify, or delete the archive. For the issuer, the authorized individuals are Internal Auditors.

Archived records MAY be moved to another medium. Records of individual transactions MAY be released upon request of any subjects involved in the transaction or their legally recognized agents. The contents of the archives maintained by issuers operating under this policy MUST not be released except as required by law.

Archive media SHOULD be stored in a safe, secure storage facility separate from the issuer equipment with physical and procedural security controls equivalent to or better than those of the issuer. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media SHOULD be defined by the archive site.

3.6 Key Rotation

To minimize **risk** from compromise of an issuer's private signing key, that key SHOULD be changed often. From that time on, only the new key will be used to sign subject credentials.

The issuer's signing key shall have a validity period as described below

1. Issuer private keys SHOULD be rotated no more often than once every six months and no less often once every two years or in accordance to the risk mitigation strategy of the ecosystem.
2. Issuer private keys MUST be rotated whenever there is an indication or a declaration of key compromise.
3. Key rotation MAY involve multiples parties for split knowledge of private keys.
4. The details of a key rotation ceremony MUST be kept confidential among the key holders until

after the rotation has been completed.

5. Pre-rotation mechanisms MAY be used to provide a higher level of protection for issuer private keys if needed.
6. Any key change MUST be published to relying parties.

3.7 Compromise and Disaster Recovery

Issuer organizations SHOULD have an incident response plan and a disaster recovery plan.

If compromise of an issuer is suspected, an independent, third-party investigation SHOULD be performed to determine the nature and the degree of damage.

Credentials issued off that issuer SHOULD be stopped immediately upon detection of a compromise.

If an issuer private signing key is suspected of compromise, the procedures outlined in section 3.7.2 Key Compromise Procedures SHOULD be followed. Otherwise, the scope of potential damage SHOULD be assessed to determine if the issuer needs to be rebuilt, only some credentials need to be revoked, and/or the issuer private key needs to be declared compromised. The independent, third-party investigating party SHOULD make the determination that an issuer private key has been compromised.

3.7.1 Corrupted Issuer Systems or Data

When Issuer system computing resources, software, and/or data are corrupted, issuers SHOULD respond as follows:

- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.
- If the issuer signing keys are not destroyed, the integrity of the system has been restored, and the **risk** is deemed negligible, reestablish issuer operations, giving priority to the ability to generate credential status information within the CRL issuance schedule.

- If the issuer signing keys are destroyed, the integrity of the system cannot be restored, or the **risk** is deemed substantial, reestablish issuer operations as quickly as possible, giving priority to the generation of a new issuer signing key pair.

3.7.2 Issuer Private Key Compromise Procedures

In the case of the issuer private key compromise, the issuer SHOULD notify relying parties via public announcement, any utility ledgers holding DIDs, all subjects and **relying parties** to reject verifications of its public key.

Notification SHOULD be made in an authenticated and trusted manner. Initiation of notification to relying parties and subjects MAY be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is determined that the issuer operations can be securely re-established, the issuer SHOULD then generate a new set of signing keys, solicit requests and issue new credentials.

3.7.3 Business Continuity Capabilities after a Disaster

Issuers SHOULD maintain a disaster recovery plan.

In the case of a disaster in which the issuer equipment is damaged and inoperative, the issuer operations shall be re-established as quickly as possible, giving priority to the ability to revoke subject's credentials.

In the case of a disaster whereby an issuer installation is physically damaged, and all copies of the issuer signature key are destroyed as a result, the issuer MUST request that its credentials be revoked. The issuer installation SHOULD then be completely rebuilt by re-establishing the issuer equipment and generating new private and public keys. Subsequently all subject credentials MAY be re-issued. In such events, any **relying parties** who continue to use credentials signed with the destroyed private key do so at their own **risk**, and the **risk** of others to whom the data is forwarded, as no revocation information will be available.

3.8 Issuer Termination

When an issuer operating under this Specification terminates operations before all credentials have expired, Entities SHOULD be given as much advance notice as circumstances permit. In addition:

- The issuer MUST revoke all unexpired credentials prior to termination.
- The issuer MUST archive all audit logs and other records prior to termination.
- The issuer MUST destroy all its private keys upon termination.
- The issuer archive records MAY be transferred to an appropriate authority specified in credential policy or **governance framework**.

4. Technical Requirements

4.1 Issuer Private Key Management

Issuer private keys MUST be managed as part of a GF compliant key management system.

Any duplication of issuer private keys MUST be protected at no less than the level of security in which they are generated, delivered, and protected by the issuer.

Issuer private keys MUST NOT be held in trust by a third party.

Issuers SHOULD document their specific practices in their Credential Practice Statement that is conformant to its Credential Policy.

4.1.1 Private Key Delivery to Subject

If issuers generate subject's private keys for them, the delivery of that private key MUST not allow the key to be transmitted or stored in the clear except within a **hardware secure device** or within a GF-compliant **digital wallet**.

4.1.2 Public Key Delivery to Credential Issuer

Where key pairs are generated by the subject or their project that will be included in verifiable credentials, the public key MUST be delivered securely to the issuer for credential issuance. The delivery mechanism MUST bind the subject's verified identity to the public key. If cryptography is used to achieve this binding, it MUST be at least as strong as the issuer keys used to sign the credential.

4.1.3 Issuer Public Key Access to Relying Parties

The public key of an issuer included on verifiable credentials MUST be stored and made available to the subjects, their proxies and verifiers acting as relying parties in a secure manner so that it is not vulnerable to modification or substitution.

Issuer public keys MUST be made available whenever and wherever verification is required.

All instances of rotated keys MUST be secure and made available using requirements specified in this section.

4.2 Key Size and Complexity

The determination of cryptographic key size and the complexity within a hashing algorithm SHOULD consider the **risk** of determining the private key from a brute force attack. With the advent of quantum computing, governing authorities establishing these requirements MUST consider the value of encrypted material and the actions that can occur if private keys are compromised. Governing bodies SHOULD complete a formal **risk assessment** and consider key size and hashing algorithms from standards bodies such as the National Institute of Standards and Technology (NIST) to establish the requirements for its governance framework.

4.2.1 Credential Validity Periods

Depending on the nature of the credential and its use, verifiable credentials MAY have a validity period.

Credentials that have a specific validity period SHOULD conform to usage of validFrom and validUntil specifications in the W3C Verifiable Credentials Data Model.

4.2.2 Issuer Private Key Usage Period

Given the efficacy of the issuer's private key over time, the issuer's key pairs SHOULD be changed periodically. The change cycle SHOULD be determined by a risk assessment.

4.3 Private Key Protection Controls

4.3.1 Private Key Protection Device Controls

Issuers MUST use a GF compliant **digital wallet** or commensurate device or FIPS 140 Level 3 or higher validated hardware cryptographic module for signing operations.

Subjects or their proxies MUST use a GF compliant **digital wallet** or commensurate device for all cryptographic operations.

A single person MUST NOT be permitted to activate or access any cryptographic module that contains the complete issuer signing key. Issuer signing keys MAY be backed up only under two-person control. Access to issuer signing keys backed up for disaster recovery MUST be under at least two-person control. The names of the parties used for two-person control SHOULD be maintained on a list that shall be made available for inspection during compliance audits.

Issuer private keys MUST NOT be escrowed.

Issuer private signature keys and subject private signature keys SHOULD not be archived.

4.3.2 Private Key Backup

4.3.2.1 Backup of Issuer Private Signature Key

The issuer private signature keys MUST be backed up under the same multi-party control as the original signature key. At least one copy of the private signature key SHOULD be stored off-site. All copies of the issuer private signature key MUST be accounted for and protected in the same manner as the original. Backup procedures shall be included in the issuer's credential policy.

4.3.2.2 Backup of Human Subject Private Keys

Backed up human subject private keys MUST not be stored in plaintext form outside the private key protection device (**digital wallet** or **HSM**) storage procedures MUST ensure security controls consistent with the protection provided by the subject's private key protection device.

4.3.2.3 Backup of Device Private Keys

Device private keys MAY be backed up or copied but MUST be held under the control of the device's AOR. Backed up device private keys MUST NOT be stored in plaintext form outside the private key protection device or cryptographic module.

Backup copies shall be controlled at the same security level as the original.

4.3.3 Private Key Transfer into or from a Private Key Protection Device or Cryptographic Module

Issuer private keys MAY be exported from the cryptographic secure module or secure **digital wallet** only to perform issuer key backup procedures. The issuer private key MUST NOT exist in plaintext outside the private key protection device or **hardware secure module**.

All other keys MUST be generated by a GF compliant **digital wallet** or cryptographic module. If a private key is to be transported from one **digital wallet**/cryptographic module to another, the private key MUST be encrypted during transport; private keys MUST NOT exist in plaintext from outside the **digital wallet**/cryptographic module boundary.

Symmetric keys used to encrypt other private keys for transport MUST be protected from disclosure.

4.3.4 Method of Activating Private Key

The Issuer MUST be authenticated to the private key protection device before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs, or biometrics. Entry of activation data MUST be protected from disclosure (i.e., the data SHOULD not be displayed while it is entered).

A device MAY be configured to activate its private key without requiring activation data, provided that appropriate physical and logical access controls are implemented for the device. The AOR is responsible for ensuring that the system has security controls commensurate with the level of threat in the device's environment. These controls MUST protect the device's hardware, software, and the private key protection device and its activation data from compromise.

4.3.5 Method of Deactivating Private Key

Private key protection devices that have been activated MUST NOT be available to unauthorized access. After use, the private key protection devices MUST be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable credential policy or **governance framework**. Single-purpose portable private key protection devices MUST be removed and stored in a secure container when not in use.

4.3.6 Method of Destroying Private Key

Individuals in **trusted roles** MUST destroy issuer private signature keys when they are no longer needed.

4.3.7 Issuer Private Key Activation Data Generation and Installation

Issuer activation data MAY be user-selected (by each of the multiple parties holding that activation data). IF the activation data MUST be transmitted, it MUST be via an appropriately protected channel, and distinct in time and place from the associated private key protection device.

4.3.8 Issuer Private Key Activation Data Protection

Data used to unlock private keys MUST be protected from disclosure by a combination of biometric, cryptographic, and physical access control mechanisms. Activation data MUST be either:

- memorized.
- biometric in nature; or
- recorded and secured at the credential class level associated with the activation of the private key protection device.

5. Information Trust Requirements

5.1 Facility and Environmental Requirements for Issuer Systems

5.1.1 Physical Security

The location and construction of the facility housing the issuer equipment, as well as sites housing remote workstations used to administer the issuer systems, MUST be consistent with facilities used to generate credentials at their stated **level of assurance** indicated in a credential policy or **governance framework**.

The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, SHOULD provide robust protection against unauthorized access to the issuer equipment and records.

At a minimum, computing site location and construction for issuer equipment and all portable secure private key protection container devices MUST be located in a dedicated cabinet within a computer room dedicated to information processing.

Physical access to issuer equipment MUST be limited to issuer operations staff and internal auditors. The security mechanisms shall be commensurate with the **level of assurance** of credentials being issued by the issuer.

At a minimum, physical access controls for issuer equipment and all private key protection devices MUST meet the following requirements:

- Ensure that no unauthorized access to the hardware is permitted.
- Be manually or electronically monitored for unauthorized intrusion at all times.

For higher **level of assurance** credentials physical security controls SHOULD also include the following requirement:

- Ensure an access log is maintained and inspected periodically.
- Mandate at least two-person access requirements. At least one individual MUST be a member of the issuer operations staff.
- Technical or mechanical mechanisms (e.g., dual locks) MUST be used to enforce the two-person physical access control. Other individuals MUST be escorted by two persons. This includes maintenance personnel. All individuals MUST be recorded in the access log.

When not in use, removable private key protection devices, removable media, and any activation information used to access or enable issuer private key protection devices or issuer equipment, or paper containing sensitive plain-text information MUST be placed in locked containers sufficient for housing equipment and information commensurate with the sensitivity, or value of the information being protected by the credentials issued by the issuer. Access to the contents of the locked containers shall be restricted to individuals holding Issuer trusted roles as defined in Section 3.1.

For higher levels of assurance, these containers SHOULD utilize two-person access controls, and two-person integrity while the container is unlocked. Private key protection devices held within the work area for intermittent use throughout the day MAY be kept under one lock, as long as they are stored in an area where there are at least two persons physically present at all times.   Knowledge of the combination or access to the key used to secure the lock MUST be restricted to authorized individuals only.   When in active use, the private key protection device MUST be locked into the system or container (rack, reader, server, etc.) using a physical lock under the control of the issuer operations staff to prevent unauthorized removal.

5.1.2 Environmental Support Requirements

Issuer systems SHOULD have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing credentials and any revocation lists) SHOULD be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

Issuer equipment SHOULD be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

Adequate fire suppression, prevention and protection controls protecting issuer equipment SHOULD be in place such as temperature and smoke alarms, and fire suppression devices.

Media SHOULD be stored to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media not required for daily operation or not required by policy to remain with the issuer that contains audit, archive, or backup information SHOULD be stored securely in a location separate from the issuer equipment.

Media containing private key material SHOULD be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or provides access. Storage protection of issuer private key material shall be consistent with stipulations in Section 6.1.1.

Destruction of media and documentation containing sensitive information such as private key material SHOULD comply with stipulations for destroying sensitive information.

A system backup SHOULD be made when an issuer system is activated. If the issuer system is operational for more than a week, backups SHOULD be made at least once per week. Backups SHOULD be stored offsite either in a physical location or stored in a secure cloud repository. Only the latest backup SHOULD be retained. The backup SHOULD be stored at a site with physical and procedural controls commensurate to that of the operational Issuer system.

The data backup media SHOULD be stored in a facility approved for storage of information of the same value of the information that will be protected by the credentials and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material identified in Section 6.2.4.1.

5.2 Access Control

Access to information such as sensitive details about customer accounts, passwords, and ultimately, issuer related private keys SHOULD be carefully guarded, along with the devices housing such information.

The issuer SHOULD create and document roles and responsibilities for each employee job function in the credential policy or **governance framework**. The issuer SHOULD create and maintain a mapping of these roles and their associated responsibilities to specific employees and their accounts on issuer systems.

Information system account management features MUST ensure that issuers access only that is functionality permitted by their role or function. All account types with access to information systems SHOULD be documented along with the conditions and procedures to follow in creating new accounts. Groups and roles SHOULD have a documented relationship to the business or mission roles involved in operating the issuer.

Section 3.1 of this document defines roles and job functions for personnel that the issuer will use when defining access control mechanisms. The issuer SHOULD employ the principle of least privilege when creating users and assigning them to groups and roles; membership to a group or role is granted shall be justified based upon business need. The issuer SHOULD take appropriate action when a user no longer requires an account, their business role changes, or the user is terminated or transferred. Periodically, the Issuer SHOULD review all active accounts to match active authorized users with accounts, and disable any accounts no longer associated with an active authorized user.

To assist with the management of the information system accounts, automated systems SHOULD assist in maintaining access for only those users who are still authorized to use the information system. After an extended period of inactivity, an account SHOULD be automatically disabled and attempts to access any deactivated account SHOULD be logged.

All account administration activities SHOULD be logged and made available for inspection by appropriate security personnel. Account administration activities that SHOULD be audited include account creation, modification, enabling, disabling, group or role changes, and removal actions.

The issuer MUST NOT use shared/group and guest/anonymous accounts for logon to information systems.

5.2.1 Least Privilege

In granting rights to accounts and groups, the issuer SHOULD employ the principle of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The issuer SHOULD explicitly authorize access to accounts and groups for controlling security functions and security-relevant information. The issuer SHOULD authorize access to privileged commands and features of information systems only for specific, organization-defined compelling operational needs and documents the rationale for such access. The issuer SHOULD require that users of information systems with access to administrative privileges to utilize non-privileged accounts or roles when accessing non-privileged functions (such as reading email).

5.3 Processing Integrity

5.3.1 System Isolation and Partitioning

Issuer systems MUST be configured, operated, and maintained to ensure the continuous logical separation of processes and their assigned resources. This separation SHOULD be enforced by:

- physical and/or logical isolation mechanisms, such as dedicated systems or virtualization
- protecting an active process and any assigned resources from access by or interference from another process
- protecting an inactive process and any assigned resources from access by or interference from an active process
- ensuring that any exception condition raised by one process will have no lasting detrimental effect on the operation or assigned resources of another process.

All issuer system components SHOULD be logically separated from each other and shall be logically separated from any other business system of the issuer.

Security critical processes (e.g., issuer signing activities) MUST be isolated from processes that have public interfaces.

If the issuer uses shared resources (e.g., storage) between issuer systems and other business applications, the underlying system(s) MUST prevent any unauthorized and unintended information transfer between processes via those shared system resources.

The issuer SHOULD develop and document-controlled procedures for transferring software updates, configuration files, credential requests, and other data files between trusted components.

5.3.2 Malicious Code Protection

The issuer system MUST employ malicious code protection mechanisms to mitigate the **risk** of malicious code on issuer system components. Malicious code on trusted issuer components could allow an attacker to issue fraudulent credentials, create a rouge intermediate or signing issuer server, or compromise the availability of the system.

Issuer system components running standard operating systems that are not air-gapped from the Internet MUST employ host-based anti-malware tools to detect and prevent the execution of known malicious code. These tools shall be configured to automatically scan removable media when it is inserted, as well as files received over the network. Introduction of removable media shall not cause automatic execution of any software residing on the media.

Anti-malware tools employed by an issuer MUST be properly maintained and updated by the issuer. Anti- malware tools on networked systems SHOULD be updated automatically as updates become available, or issuer system administrators SHOULD push updates to system components on a monthly basis. Anti-malware tools MAY be employed on air-gapped systems. However, without sufficient technical and procedural controls, the processes for updating these tools could provide an attacker with a means for spreading malicious code to these air-gapped systems. IF anti-malware tools are employed on air-gapped systems, the issuer SHOULD document in its procedures how these tools will be updated, including mitigations intended to reduce the risks of spreading malware and exfiltration of data off of compromised issuer systems.

Anti-malware tools SHOULD alert system administrators of any malware detected by the tools.

5.3.3 Software and Firmware Integrity

The issuer SHOULD employ technical and procedural controls to prevent and detect unauthorized changes to firmware and software on issuer systems. Access control mechanisms and configuration management processes (see Section 6.5.1.1 and 6.6.2) shall ensure that only authorized system administrators are capable of installing or modifying firmware and software on issuer systems.

5.3.4 Information Protection

The issuer MUST protect the confidentiality and integrity of sensitive information stored or processed on issuer systems that could lead to abuse or fraud. For example, the issuer MUST protect customer data that could allow an attacker to impersonate a customer. The issuer MUST employ technical mechanisms to prevent unauthorized changes or accesses to this information, such as access control mechanisms that limit which users are authorized to view or modify files. Sensitive information stored on devices that are not physically protected from potential attackers MUST be stored in an encrypted format, using a NIST approved encryption algorithm and mode of operation.

5.4 System Development Controls

The issuer system MUST be implemented and tested in a non-production environment prior to implementation in a production environment. No change MUST be made to the production environment unless the change has gone through the change control process as defined for the system baseline.

To prevent incorrect or improper changes to the issuer system, the issuer system MUST require multi-party control for access to the issuer system when changes are made.

For any software developed by the issuer, evidence SHOULD be produced relating to the use of a defined software development methodology setting out the various phases of development, as well as implementation techniques intended to avoid common errors to reduce the number of vulnerabilities. Automated software assurance (i.e., static code analysis) tools shall be used to catch common error conditions within developed code. For compiled code, all compiler warnings shall be enabled and addressed or acknowledged to be acceptable. Input validation shall be performed for all inputs into the system.

5.5 Security Management Controls

A list of acceptable products and their versions for each individual issuer system component SHOULD be maintained and kept up to date within a configuration management system. Mechanisms and/or procedures SHOULD be in operation designed to prevent the installation and execution of unauthorized software. A signed whitelist of the acceptable software for the system MAY be one of the ways to control the allowed software. An issuer system SHOULD have automated mechanisms to inventory on at least a monthly basis software installed on a system and alert operators if invalid software is found.

To reduce the available attack surface of an issuer system, only those ports, protocols, and services that are necessary to the issuer system architecture MUST be permitted to be installed or operating. The issuer system SHOULD maintain a list of ports, protocols, and services that are necessary for the correct function of each component within the issuer system. There SHOULD be automated mechanisms to monitor the running processes and open ports against the permitted list.

To validate the integrity of the issuer system, automated tools that validate all static files on a component MAY be in operation to notify operators when a protected file has changed.

The issuer system SHOULD establish and document mandatory configuration settings for all information technology components which comprise the issuer system. All configuration settings capable of automated assessment SHOULD be validated to be set according to the guidance contained within a documented security configuration checklist on at least monthly basis for powered on systems or next power-on for systems which are not left powered-on.

5.5.1 Life Cycle Security Controls

For flaw remediation, the issuer SHOULD scan all issuer systems for vulnerabilities using at least one vulnerability scanner every year.

Each vulnerability found SHOULD be entered into a vulnerability tracking database, along with the date and time of location, and shall be remediated within 72 hours. Remediation SHOULD be entered into the vulnerability database as well (including date and time).

The issuer SHOULD monitor relevant notification channels on a monthly basis for updates to packages installed on issuer systems (including networking hardware). Issuers SHOULD have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption. For critical vulnerabilities, the issuer SHOULD evaluate and install the update within 24 hours. For less critical vulnerabilities, the issuer SHOULD evaluate each package to determine whether an update is required, and if so, that update shall be applied to all affected issuer systems within 48 hours. A log SHOULD be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches.

From time to time, the issuer MAY discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The issuer SHOULD correct such errors within 24 hours of discovery, and shall document the reason for the error, and the associated correction.

5.6 Network Security Controls

5.6.1 Isolation of Networked Systems

Issuers which are connected to networks are, thus, exposed to potential attackers. Communication channels between the network-connected issuer components and the trusted issuer processing components MUST be protected against attack. Furthermore, information flowing into these issuer components from the network-connected issuer components MUST not lead to any compromise or disruption of these components.

The components of an issuer requiring public network connections MUST be minimized. Those networked components MUST be protected from attacks using firewalls to filter unwanted protocols (utilizing access rules, whitelists, blacklists, protocol checkers, etc., as necessary). Similarly, some form of data leak prevention MUST be employed to detect inappropriate leakage of sensitive information.

5.6.2 Availability

Credential request and issuance services SHOULD be available but can tolerate some down time. Revocation services, which include the request for revocation as well as the advertisement of revoked credentials, MUST be highly available. If revocation information is not available, or if revocation information is inaccurate, then a **relying party** could be easily convinced to trust a revoked credential.

5.6.3 Denial of Service Protection

Issuer systems MUST be configured, operated, and maintained to maximize uptime and availability. Scheduled downtime SHOULD be announced to Users.

Issuers SHOULD state acceptable methods to request revocation in their credential policy or **governance framework**. At least one of those methods MAY be out of band (i.e., network connectivity is not required).

Issuers MUST take reasonable measures to protect credential request and issuing services from known DoS attacks.

The availability of revocation status MUST be configured and deployed in such a manner and capacity that overall availability is maintained at a minimum of <99.99% (52 minutes/year)>, with no single outage lasting longer than 5 minutes. If users and relying parties are geographically dispersed, such services SHOULD be homed in a minimum of two geographically independent locations with no single-points of failure (SPOFs – e.g., same backbone provider) which could affect availability.

5.6.4 Communications Security

5.6.4.1 Transmission Integrity

Source authentication and integrity mechanisms MUST be employed to all credential request and issuance communications, including all related services irrespective of whether those services are hosted on the same or different platform than the issuer workstation.

5.6.4.2 Transmission Confidentiality

Communications that cross the physical protection barrier of the credential-signing portion of the issuer system MUST be confidentiality-protected.

Confidentiality of credential source data MUST be maintained.

Connections SHOULD be terminated after a period of inactivity.

Network connections between issuers and subjects MUST be terminated at the end of the session or after a period of inactivity. Keep-alive and quick-reconnect mechanisms SHOULD NOT be employed, so that message replay and session hijacking are avoided.

5.6.4.3 Session Authenticity

For issuer to subject communications, session identifiers MUST not be reused. The parties involved in a session MUST have a clear session termination capability and MUST receive explicit notification that a session has been terminated.

5.6.5 Network Monitoring

The issuer systems MUST be monitored to detect attacks and indicators of potential attacks.

5.6.5.1 Events and Transactions to be Monitored

The issuer SHOULD identify a list of essential information, transaction types and thresholds that indicate potential attacks. These events SHOULD include:

- Bandwidth thresholds
- Inbound and outbound communication events and thresholds
- Unauthorized network services
- CPU usage thresholds
- Certificate request thresholds from a single Registration Agent
- Access Control thresholds

5.6.5.2 Monitoring devices

An issuer SHOULD deploy intrusion detection tools or other monitoring devices to collect intrusion information and at ad hoc locations within the system to track specific types of transactions of interest to the organization. These monitoring devices SHOULD be configurable to react to specific indications of increased **risk** or to comply with law enforcement requests. The devices SHOULD alert security personnel when suspected unauthorized activity is occurring. These devices SHOULD be network-based and SHOULD be also host-based. The devices SHOULD NOT be by passable by non-privileged users. The issuer SHOULD utilize automated tools to support near real-time analysis of events and these tools SHOULD be integrated into access control and flow control mechanisms for rapid response to attacks.

5.6.5.3 Monitoring of Security Alerts, Advisories, and Directives

An issuer SHOULD monitor information system security alerts, advisories, and directives on an ongoing basis. The issuer SHOULD generate and disseminate internal security alerts, advisories, and directives as deemed necessary. The issuer SHOULD employ automated mechanisms to make security alert and advisory information available throughout the organization as needed.

5.6.6 Remote Access

For operational reasons, there MAY be a need to perform remote management of some Issuer resources. The requirements in this section are meant to allow remote management while maintaining the desired security posture.

5.6.6.1 Bastion Host

All access to issuer systems in a restricted communication zone SHOULD be mediated by a bastion host (i.e., a machine that presents a limited interface for interaction with the other elements of the issuer also known as a jump server). No direct access SHOULD be permitted. The bastion host SHOULD be patched regularly, maintained, and SHOULD only run applications required to perform its duties. The Bastion Hosts SHOULD be located between the restricted communication zone where the issuer is located and the zone where the issuer operations staff are located.

No remote access SHOULD be permitted with special access communication zones used for processing and storage of especially high value data such as cryptographic keys.

5.6.6.2 Documentation

The issuer SHOULD document allowed methods of remote access to issuer systems, including usage restrictions and implementation guidance for each allowed remote access method.

5.6.6.3 Logging

Logging SHOULD be performed on the bastion host for each remote access session with the issuer. Logs SHOUD include date and time of the connection, the authenticated identity of the requestor, the IP address of the remote system and the commands sent to the bastion host. Logs shall be maintained on a corporate audit server. Time on the bastion host shall be synchronized with an authoritative time source.

5.6.6.4 Automated Monitoring

Automated monitoring SHOULD be performed on all remote sessions with the bastion host, and on all interactions between the bastion host and other issuer systems. Upon detection of unauthorized access, the issuer SHOULD terminate the connection and log the event.

5.6.6.5 Security of Remote Management System

Machines used for remote access to the issuer system SHOULD be either corporately managed (including patching) or SHOULD be a machine dedicated to that purpose. It SHOULD NOT be used as a personal machine for the remote user. The machine SHOULD be maintained at the same level as the machines that it accesses (i.e., all policies on patching, virus scanning, etc. that are levied on the target systems shall apply to this machine as well). The issuer SHOULD make use of network access control technology to check the security posture of the remote machine prior to connecting it to the network. Remote management of the issuer system SHOULD be the only use of Remote Access.

5.6.6.6 Authentication

Any machine used to access issuer systems remotely MUST require two or more factors of authentication. An identity credential MUST be required. Authentication MUST occur between the remote machine and the bastion host.

5.6.6.7 Communications Security for Remote Access

All communications between the remote access host and the issuer system MUST be protected by [FIPS 140] validated cryptography. Session identifiers SHOULD be invalidated at logout to preserve session authenticity.

5.6.7 Vulnerability and Penetration Testing

The issuer SHOULD perform assessments of system and network vulnerabilities at least annually.

The issuer system SHOULD conduct at least annual external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems. Penetration testing SHOULD occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.

A standard method for penetration testing consists of:

- pretest analysis based on full knowledge of the target system.
- pretest identification of potential vulnerabilities based on pretest analysis.
- testing designed to determine exploitability of identified vulnerabilities.

Detailed rules of engagement SHOULD be agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Vulnerabilities uncovered during penetration testing SHOULD be incorporated into the vulnerability remediation process.

TRUST Over IP FOUNDATION

The Trust Over IP Foundation (ToIP) is hosted by the Linux Foundation under its Joint Development Foundation legal structure. We produce a wide range of tools and deliverables organized into five categories:

- Specifications to be implemented in code
- Recommendations to be followed in practice
- Guides to be executed in operation
- White Papers to assist in decision making
- Glossaries to be incorporated in other documents

ToIP is a membership organization with three classes—Contributor, General, and Steering.

The work of the Foundation all takes place in Working Groups, within which there are Task Forces self-organized around specific interests. All ToIP members regardless of membership class may participate in all ToIP Working Groups and Task Forces.

When you join ToIP, you are joining a community of individuals and organizations committed to solving the toughest technical and human centric problems of digital trust. Your involvement will shape the future of how trust is managed across the Internet, in commerce, and throughout our digital lives. The benefits of joining our collaborative community are that together we can tackle issues that no single organization, governmental jurisdiction, or project ecosystem can solve by themselves. The results are lower costs for security, privacy, and compliance; dramatically improved customer experience, accelerated digital transformation, and simplified cross-system integration.

To learn more about the Trust Over IP Foundation please visit our website, https://trustoverip.org.

Licensing Information: