

Technical Trust Framework for verifiable credentials



Contents

Technical Trust Framework for verifiable credentials	1
Document Control	3
Version History	3
1. Definitions	4
2. General Requirements	6
2.1 Technical Trust Architecture Overview	6
2.2 Data and Credentials	7
2.3 Metadata	8
2.4 Technical Trust	8
2.5 Interoperability	10
2.6 Protocols and APIs	11
3. Technical and Security Requirements	12
3.1 Protection and Accuracy of Data	12
3.2 Secure Messaging Requirements	12
3.3 Management and security best practice	13
3.4 Security Controls and Technical Infrastructure	13
4. Specific requirements for certain entities	14
4.1 Issuers of credentials	14
4.2 Wallet providers	14
5. Assurance criteria for Issuers	16
C1 – Technical Trust	16
C4 - Specific Entity Requirements	19
6. Assurance criteria for Verifiers	21
C1 – Technical Trust	21
C4 - Specific Entity Requirements	24
7. Common criteria for all providers	26
C2 - Interoperability	26
C3 - Technical and Security Requirements	27
C5 - Compliance with Data Schema	30

Document Control

Key	Name	Role
Authors	ID Crowd	Verifiable credential subject matter experts
Approver	Phil Stradling	Architect, Transformation Directorate
Owner	Ian Townend	Chief Architect, Transformation Directorate
Reviewer	Marcus Appleton	Head of Future Workforce Solutions, Workforce, Training and Education Directorate

Version History

Version	Date	Description
1.0	15/01/2024	First final version
1.1	19/04/2024	Fixed errors in section references

1. Definitions

Digital Staff Passport	A digital service for use by employees within NHS trusts in England to share employment, education and training, and occupational health details as Verifiable Credentials, to support moves between those organisations.
Authoritative Source	An entity that has access to, or verified copies of, accurate information from an issuing source (either itself as the issuer or another such entity). This enables other entities to confirm the validity of evidence supplied e.g., the validity of a credential.
Attribute Provider (AP)	Manages and provides assertions of attributes to other relying parties in the ecosystem.
Credential	A proof of achievement, identity, characteristic, etc.
Disintermediation	The act of bypassing the user/Holder and communication occurring directly between the Issuer and Verifier.
GPG45	Good Practice Guide 45 as published by the Cabinet Office and pertaining to the identity proofing and verification of an individual. This guidance is used as a key element of assurance to trust frameworks such as that proposed by DCMS for digital identity and is aligned with international standards such as NIST 800.63.3.
Holder	The Holder is an entity that holds and can securely share multiple credentials. The Holder may also be the Subject (see definition below).
Identity Provider (IDP)	An entity that can provide proof that an entity is who they claim to be at a recognised [by the relying parties] level of trust.
Information Security Management System (ISMS)	Information Security Management System as described in ISO/IEC 27001. An ISMS is a set of policies and procedures for the systematic management of sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.
Issuer	A participating entity in and compliant with the Trust Framework that is capable of issuing compliant credentials to a verified Subject.

Participating Entity	Any entity (e.g., an Issuer, Wallet Provider, Verifier, User or Relying Party) that operates a service or utilises credentials as part of the Trust Framework
Relying Party (RP)	An entity that relies upon credentials provided by a Holder (or other entity).
Scheme	The set of technical, operational, commercial, and compliance rules that define an identity system.
Selective Disclosure	The ability of a Holder to make fine-grained decisions about what information to share.
Service Provider (SP)	The Relying Party providing a digital service to the Subject through a user agent such as a browser or App (e.g. a Wallet).
Subject	The entity attempting to obtain and/or share credentials with other entities in the Trust Framework. Sometimes referred to as a Holder.
Trust Framework	A set of operational, business, and technical rules and associated governance to enable a group of entities (including schemes) to interoperate with an adequate level of trust.
Trust Framework Implementor	An organisation contracted to provide Digital Staff Passports or contracted specifically by an entity participating in the trust framework (e.g., by an Issuer) to provide Issuer, Holder, or Verifier functionality.
Trust Framework Operator	An entity appointed by NHS England in conjunction with other relevant bodies to manage the operation of the trust framework and to ensure that governance is adhered to by the participating entities.
User	In the context of this technical trust framework, User refers to the entity in control of a digital wallet acting as a Holder of verifiable credentials.
Verifiable Credential (VC)	A digital proof that can be verified independently of the issuer.
Verifier	A logical function of a Relying Party (or Service Provider) that seeks to verify the integrity of a Credential as presented by a Holder.
[Digital] Wallet	A means of holding multiple credentials from multiple Issuers in a secure digital format. Also provides the functionality to securely share credentials with Verifiers.

2. General Requirements

2.1 Technical Trust Architecture Overview

The Technical Trust Framework (TTF) forms one layer of the NHS Trusted Framework and describes the interoperability and security building blocks required to establish trust across multiple parties as required by NHS employers when managing staff movements and interaction with digital healthcare systems.

The TTF describes baseline requirements for interoperability, security, and integrity in the support of technical trust. Providers are at liberty to provide additional functionality to users (of Digital Wallets) although to operate within the trust framework they must provide evidence of compliance with the baseline requirements described in this document.

The TTF must ensure that:

- Digital credentials have an equivalent or greater level of trust compared with paper-based norms.
- Employers have the opportunity to utilise this digital trust to increase efficiency and reduce duplication in the onboarding of staff.
- End-to-end trust is provided (from Issuer, via Holder, to Verifier) without the need for direct communication between Issuer and Verifier.
- Holders of credentials are able to more easily move between employers in the knowledge that their personal data is secure, and their privacy protected.

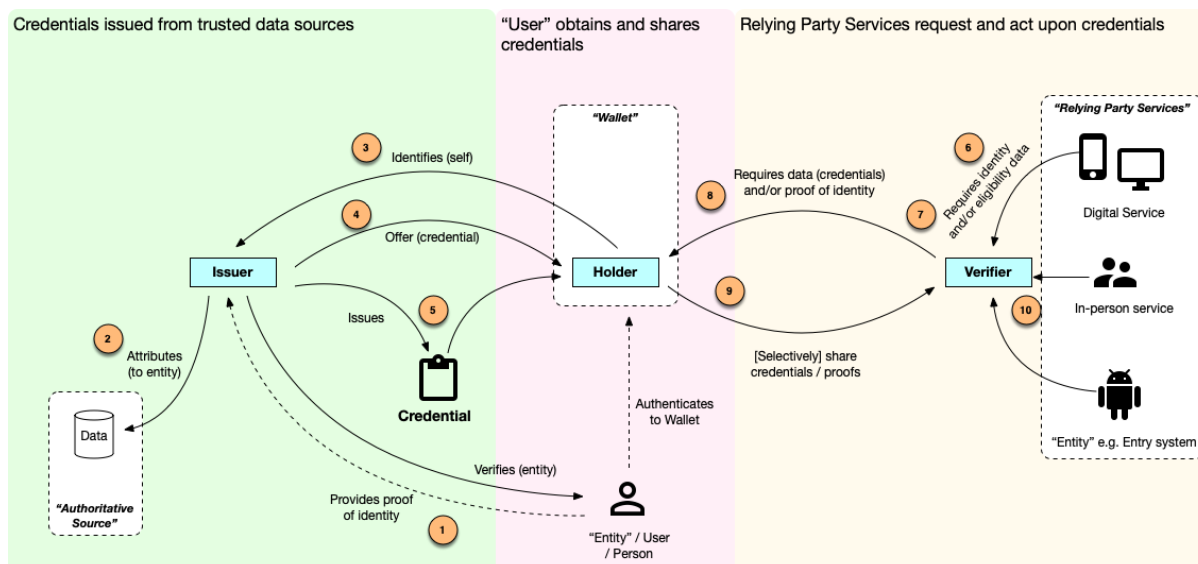


Figure 1: Overview of the proposed technical trust architecture

Step	Description	Notes
1	User onboards with a data provider.	User goes through an identity verification (IDV) process.
2	The data provider attributes data to the User as part of or following onboarding.	For example: the user registers with the General Medical Council (GMC).
3	If not already done the Holder identifies herself with the Issuer as part of a request for a credential.	This could also be an authentication to an online service from which the user wishes to retrieve a credential.
4	If the request is valid the Issuer makes an offer of a credential to the Holder.	
5	A credential is issued by the Issuer to the Holder (in response to a corresponding offer).	And securely transferred to the User
6	When accessing a service, the User [Holder] will be prompted to provide identity and / or eligibility data.	The service could be fully digital, an in-person scenario (e.g., attending an appointment) or accessing a system or physical location (e.g. a building entry system).
7	The Verifier will make a request to the Holder for one or more credentials.	This could be via a QR code or an interaction with a browser-based wallet.
8	The Holder will receive the Verification request and will prompt the User for consent to share information.	In the full solution a User would be able to selectively disclose information held within a credential to satisfy the Verification Request. For alpha, selective disclosure is out of scope.
9	The Holder prepares a Verifiable Presentation and shares the relevant credentials with the Verifier.	
10	The Verifier checks the credentials and retrieves the data for completion of the transaction or for access to a service.	This should involve checks for validity and also for revocation.

2.2 Data and Credentials

The creation, issuance, and use of Credentials will be based on the W3C Verifiable Credentials Data Model 1.1¹ and associated technical specifications provided by the W3C.

The wider trust framework will include a Data Schema. Issuers must conform to both the underlying W3C Verifiable Credentials Data Model and the Data Schema when creating and issuing credentials under the trust framework.

¹ W3C Verifiable Credentials Data Model 1.1 - <https://www.w3.org/TR/vc-data-model/>

2.3 Metadata

Credentials must include metadata that will describe the provenance, quality, and scope of data items presented.

2.4 Technical Trust

Technical trust in the context of this trust framework is the means of communicating that a Credential held by a Subject is valid, has not been tampered with, and was issued by an authoritative source. Accompanying metadata may convey additional information such as the provenance of the credential payload and the level of trust attributed to a Subject.

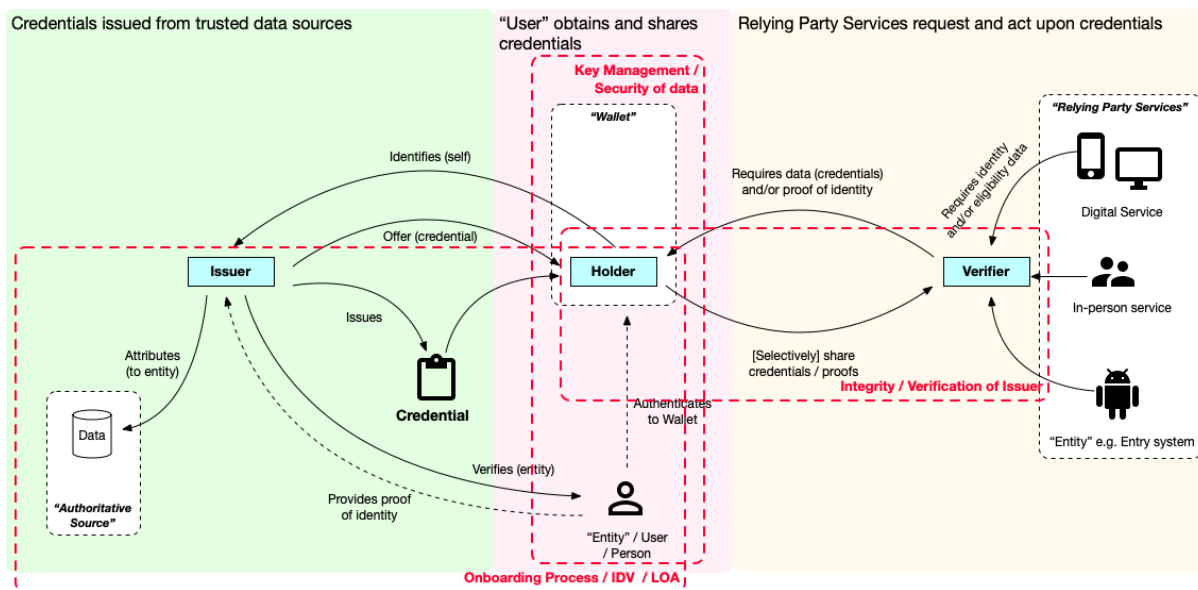


Figure 2: Technical trust requirements overview

There are 4 key areas in the architecture that enable technical trust.

1. Onboarding Processes
2. Key Management and the Security of Data
3. Integrity and Verification of credentials and their issuance
4. Integrity and Verification of credentials when presented by Holders to Verifiers

2.4.1 Onboarding Process

The onboarding process includes the entire issuance lifecycle including correct identification of Subjects and the attribution of data items (credentials) to those Subjects.

Issuers must:

1. Ensure that the identity of each Subject is verified to a baseline of GPG45² (either by the Issuer or by another trusted entity).
2. Verify the data being presented and reliably attribute this data to a Subject.
3. Provide Subjects with the ability to securely update inaccurate or incomplete information held by the Issuer.
4. Protect Subject data and issued credentials throughout the credential lifecycle.

Wallet Providers must:

1. Protect credentials, both when stored in a digital wallet solution and in transit, against unauthorised access and malicious attack.
2. Ensure that authentication to access any digital wallet (or equivalent solution) is at a level of trust at least as high as the highest trust credential held within that wallet.
3. Provide recovery mechanisms that meet the highest level of trust supported by the framework.

2.4.2 Key Management / Security of Data

Wallet Providers must:

1. Provide functionality to protect keys, secrets and other private data (such as credentials) from unauthorised access or malicious attack.
2. Include key management functionality to handle the generation, rotation, revocation, storage, signing, and protection of cryptographic keys and associated secrets.
3. Provide for point-to-point trust where a credential is presented to a Verifier

2.4.3 Integrity / Verification of Issuer

Verifiers must:

1. Ensure that received messages / credentials have not been tampered with.
2. Verify the Issuer as a recognised issuer of credentials under the trust framework.
3. Check that received credentials have not been invalidated or revoked by the Issuer.

² Good Practice Guide 45 (GPG45) – <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>

2.5 Interoperability

2.5.1 Support for Multiple Wallet Providers: Verifier

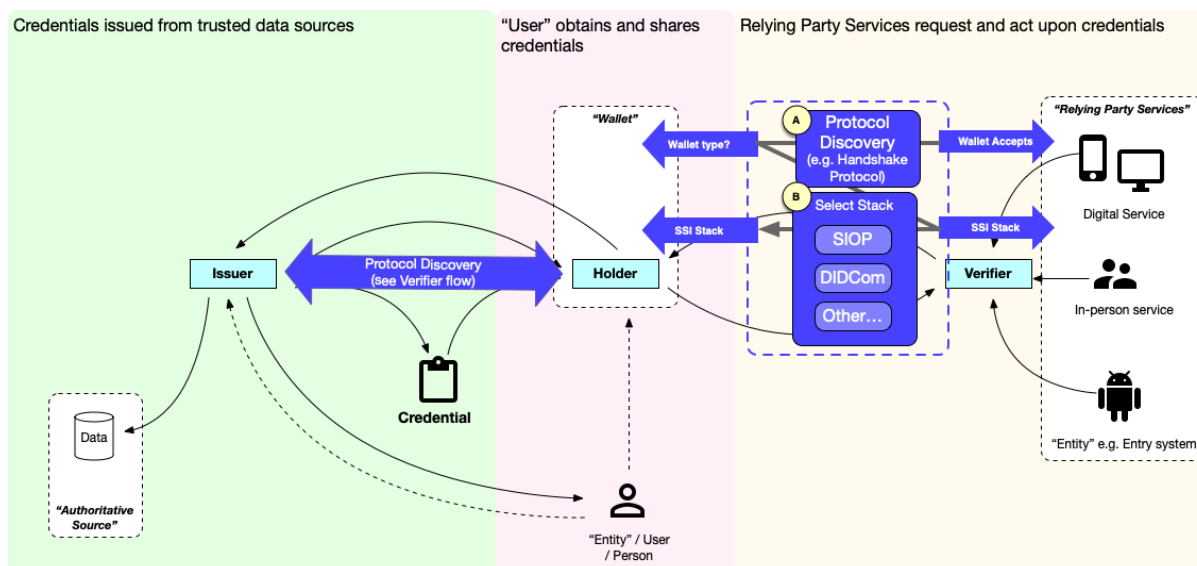


Figure 3: Wallet stack discovery overview

To ensure that multiple wallet providers are supported under the trust framework, implementors are encouraged to support the OpenID family of specifications as the means for a common protocol for the exchange of credentials between an entity and the Subject's Wallet.

2.5.2 Issuer Discovery

An out-of-band list of trusted Issuers and the credentials they provide will be made available to Verifiers. This trusted list will be maintained and published by the Trust Framework Operator.

2.5.3 Trusted Wallet List

An out-of-band list of trusted Wallet products and versions will be made available to Issuers and Verifiers. This trusted list will be maintained and published by the Trust Framework Operator.

Issuers and Verifiers should not trust wallets that do not identify themselves as a product included in this trust list.

2.6 Protocols and APIs

2.6.1 OpenID for Verifiable Credentials

The OpenID Foundation, in liaison with the Decentralised Identity Foundation (DIF) and with relevant working groups in International Organisation for Standardization (ISO), has developed specifications for the use of OpenID Connect, and OAuth 2.0 as a basis for verifiable credential issuance and presentation.

Although still in draft form these specifications have already been specified as part of the European Digital Identity Architecture and Reference Framework³ and are implemented in 18 wallets under the European Commission EBSI project⁴.

OpenID for Verifiable Credentials consists of three specifications:

- OpenID for Verifiable Credential Issuance (OID4VCI) – Defines an API and corresponding OAuth-based authorization mechanisms for issuance of Verifiable Credentials
- OpenID for Verifiable Presentations (OID4VP) – Defines a mechanism on top of OAuth 2.0 to allow presentation of claims in the form of Verifiable Credentials as part of the protocol flow
- Self-Issued OpenID Provider v2 (SIOPv2) – Enables End-Users to use OpenID Providers (OPs) that they control

Issuers, wallet providers, and service providers are recommended to consider these specifications when implementing solutions.

2.6.2 Presentation Requests

Service Providers (Verifiers of verifiable credentials) should use Presentation Requests to define the credentials that Holders will need to provide to satisfy a particular transaction.

Presentation Requests should use the Verifiable Presentation Request Specification⁵.

³ <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline>

⁴ <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Conformant+wallets>

⁵ [OpenID Connect for Verifiable Presentations](#)

3. Technical and Security Requirements

3.1 Protection and Accuracy of Data

3.1.1 Protection of personal data

All entities must have controls against the act by an adversary to access, delete, or modify the personal data or credentials in any form.

Security controls must ensure the confidentiality and integrity of personal data, at rest or in transit, and processes put in place to protect the underlying identity system from unauthorised access or abuse. Baseline standards for data security such as ISO/IEC 27001 and the implementation of an information security management system, or equivalent, should be considered where appropriate.

In the case of a breach at the issuing authority the user(s) and any relying parties must be alerted electronically by a method previously agreed with those parties.

3.1.2 Privacy throughout the identity lifecycle.

Privacy of the Subject must be protected throughout the identity lifecycle. The principles of Privacy by Design and Data Minimisation should be observed as should the spirit of GDPR even if that Regulation is not enforced by law for a particular implementation.

3.1.3 Data accuracy

Data accuracy should be a priority and Subjects should be able to view and amend errors or make required updates. Subjects should be able to update erroneous, out of date, or poor-quality data to reduce identity and attribute data errors.

3.1.4 Data sharing

The sharing of data should be avoided where aggregate computations are sufficient.

Where possible computations on personal data, yielding aggregate answers that reduce or eliminate the possibility of re-identification of an individual through correlation of data should be applied when populating Credentials.

3.2 Secure Messaging Requirements

3.2.1 Message Integrity

The integrity of all messages between entities in the trust framework should be ensured either at the network level or where personal or sensitive data is passed (e.g., in the form of a credential data payload) by digitally signing the data payloads. As all credentials in the

trust framework should conform to the Verifiable Credentials Data Model this will be accomplished by digitally signing the credential payload on issuance of the credential.

Issuers should use the JSON web token signed as a JWS for the credential format.⁶

3.2.2 Eco-system Technical Trust

There shall be a mechanism to ensure that only parties which are participating entities in the trust framework are able to interoperate with the technical components of the scheme (e.g., Credential Providers, RPs / Verifiers, and wallet providers).

3.3 Management and security best practice

Entities should demonstrate acceptable policies and procedures for the management of solution development and security throughout the organisation.

Examples of evidence that could be produced by the applicant are as follows:

1. A documented statement of applicability describing the control measures to be implemented and reasons for their selection to meet the base criteria and any additional specific criteria.
2. Presentation of a documented ISMS and any supporting opinion of a qualified external assessor.
3. Evidence may be offered against widely recognised standards such as ISO/IEC 27001 and ISO/IEC 27002.

3.4 Security Controls and Technical Infrastructure

Issuers, Wallet Providers, and Relying Parties (Verifiers) shall ensure that security controls are built into any technical infrastructure of their solution. These controls, and any physical or administrative security measures, should ensure the maintaining of any level(s) of trust required by the trust framework.

In addition, the following should be considered:

- Security policy
- Security organisation
- Asset classification and control

⁶ [JSON Web Token VC \(JWT-VC\)](#) signed as a JWS ([RFC7515](#))

- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance with legal and security policy requirements.

4. Specific requirements for certain entities

4.1 Issuers of credentials

4.1.1 Revocation checks

A means of checking for the revocation of credentials should be provided by Issuers of those credentials. This will enable Verifiers with the ability to confirm the validity of a credential in addition to any associated expiry data of that credential.

4.1.2 Verification of claims

The system must support verification of claims by the issuer without the risk of disintermediation.

Must be able to prove that credentials are genuine, untampered, pertain to the Subject, and have not been revoked.

Meta data should be provided to describe not only how any identity proofing was performed but also the Identity Assurance Level attained as a consequence of that proofing process and the subsequent issuance of credentials.

4.2 Wallet providers

4.2.1 Multiple credentials and granular control

Subjects must be able to store and manage multiple credentials from government, NHS, and other organisations.

The system must support a subject being able to present credentials issued to them without the risk of disintermediation.

Subjects must have granular control over the sharing of credentials. Subjects must have the ability to allow or deny the sharing of personal data at the point of request, as a preference before request, or at a later point in time, by giving their informed consent.

4.2.2 Backup and recovery

Backup and Recovery capability must be provided to protect Subjects in case of loss, corruption, or hacking of the Wallet solution.

4.2.3 Secure Storage

Wallets should provide for the secure storage of the keys, secrets, and other private data that the Subject elects to store in the wallet. The implementation of this secure storage may vary depending on the nature of the wallet but could be satisfied by secure enclaves on mobile phones, secure storage governed by trusted execution environments (TEEs), or hardware security modules (HSMs) as used by cloud-hosted wallets.

5. Assurance criteria for Issuers

Provider solutions for Holders (wallets) will be assured against the following criteria each of which references technical aspects defined in the preceding sections above on the requirements of the technical trust framework.

Providers are requested to respond to all questions unless they do not fulfil a specifically highlighted role (in this case they must respond “Not Applicable”).

When responding providers should include details relating to the specific solutions or products and not generally to an organisation.

C1 – Technical Trust

Establishing that a particular provider solution supports the reliable creation, issuance, and subsequent verification of credentials.

Code	Question	Options	Supporting information	Scoring criteria
C1.1	Onboarding Process		See section 2.4.1	
C1.1.1	Not Applicable			
C1.1.2	Not Applicable			
C1.1.3	Not Applicable			
C1.1.4	Not Applicable			
C1.1.5	Wallet providers: adequate protection of credentials	Provided No evidence available		To pass, Wallet Providers must provide evidence of controls to ensure the protection of credentials, when stored in a digital wallet solution and in

				transit, against unauthorised access and malicious attack
C1.1.6	Wallet providers: appropriate authentication for access to wallets	Provided No evidence available		To pass, providers must provide evidence authentication of an appropriate trust level is utilised when a Subject attempts to access data or functionality of the wallet solution. The level of authentication should be at a level of trust at least as high as the highest trust credential held within that wallet.
C1.1.7	Wallet providers: means of recovery	Provided No evidence available		To pass, providers must provide evidence of recovery mechanisms that meet the highest level of trust supported by the framework.
C1.1.8	Client Authentication	Provided No evidence available		To pass, Wallet providers must provide a means of identifying the wallet as an approved Wallet (according to the underlying trust framework) to an Issuer and/or Verifier. Entitles (e.g., an Issuer) must be able to verify the claim

				made by a wallet cryptographically.
C1.2	Key Management / Security of Data			
C1.2.1	Wallet providers: adequate protection for keys, secrets, and personal data	Provided No evidence available		To pass, providers must provide evidence of implemented controls that protect keys, secrets, and other private data (such as credentials) from unauthorised access or malicious attack.
C1.2.2	Wallet providers: key management capability	Provided No evidence available		To pass, providers must provide evidence of mechanisms for key management functionality to handle the generation, rotation, revocation, storage, signing, and protection of cryptographic keys and associated secrets. Providers should also describe the methods of key management and any scope limitations that may exist.
C1.2.3	Wallet providers: point-to-point trust	Provided No evidence available		To pass, providers must provide evidence of implemented controls that ensure point-to-point trust where a credential is

				presented to a Verifier from the wallet.
C1.3	Integrity / Verification of Issuer			
C1.3.1	Not Applicable			
C1.3.2	Not Applicable			
C1.3.3	Not Applicable			

C4 - Specific Entity Requirements

Establishing that entities (provider solutions) fulfil specific obligations as part of the technical trust framework.

Providers should note that where a question does not apply to their solution scope an explanation must be included in the answer.

Code	Question	Options	Supporting information	Scoring criteria
C4.1	Issuers			
C4.1.1	Revocation mechanism	Provided No evidence available	See section 4.1.1	To pass, providers must provide evidence of a reliable revocation mechanism and associated service to enable Verifiers to confirm that credentials have not been revoked.

C4.1.2	Verification of claims	Provided No evidence available	See section 4.1.2	To pass, providers must describe how their solution ensures that Verifiers are able to determine that claims are verified without the need for multiple intermediaries as well as providing adequate metadata to support trust.
C4.2	Wallet providers			
C4.2.1	Multiple credentials and granular control	Provided No evidence available	See section 4.2.1	To pass, providers must describe how their solution supports the acquisition of multiple credentials from multiple issuers and that Holders have full control over the subsequent sharing of credentials and attributes.
C4.2.2	Backup and recovery	Provided No evidence available	See section 4.2.2	To pass, providers must provide evidence that backup and recovery facilities are provided to Holders and that this functionality is easy to use, secure, and portable (e.g., for transfer to a new device).

C4.2.3	Secure Storage	Provided No evidence available	See section 4.2.3	To pass, providers must provide evidence that keys, secrets, and sensitive personal data is stored in an appropriate secure storage system. Where on device or hardware solutions are not utilised, the provider must detail how their solution provides an equivalent or superior secure storage function.
--------	----------------	----------------------------------	-------------------	---

6. Assurance criteria for Verifiers

Providers of Verifier solutions will be assured against the following criteria each of which references technical aspects defined in the preceding sections of the technical trust framework.

Providers are requested to respond to all questions unless they do not fulfil a specifically highlighted role (in this case they must respond “Not Applicable”).

When responding providers should include details relating to the specific solutions or products and not generally to an organisation.

C1 – Technical Trust

Establishing that a particular provider solution supports the reliable creation, issuance, and subsequent verification of credentials.

Code	Question	Options	Supporting information	Scoring criteria
C1.1	Onboarding Process		See section 2.4.1	
C1.1.1	Not Applicable			
C1.1.2	Not Applicable			
C1.1.3	Not Applicable			
C1.1.4	Not Applicable			
C1.1.5	Not Applicable			
C1.1.6	Not Applicable			
C1.1.7	Not Applicable			
C1.2	Key Management / Security of Data			
C1.2.1	Adequate protection for keys, secrets, and personal data	Provided No evidence available		To pass, providers must provide evidence of implemented controls that protect keys, secrets, and other private data (such as credentials) from unauthorised access or malicious attack.
C1.2.2	Key management capability	Provided No evidence available		To pass, providers must provide evidence of mechanisms for key management functionality to handle the generation, rotation, revocation, storage, signing,

				and protection of cryptographic keys and associated secrets. Providers should also describe the methods of key management and any scope limitations that may exist.
C1.2.3	Point-to-point trust	Provided No evidence available		To pass, providers must provide evidence of implemented controls that ensure point-to-point trust where a credential is presented to a Verifier from a wallet.
C1.3	Integrity / Verification of Issuer			
C1.3.1	Verifiers: message integrity checking	Provided No evidence available		To pass, Verifiers must provide evidence of controls to ensure that received messages / credentials have not been tampered with.
C1.3.2	Verifiers: issuer verification	Provided No evidence available		To pass, Verifiers must provide evidence of steps taken to verify the Issuer as a recognised issuer of credentials under the trust framework.

C1.3.3	Verifiers: credential validity checking	Provided No evidence available		To pass, Verifiers must provide evidence of steps taken to verify that credentials have not been invalidated or revoked by the Issuer.
--------	---	----------------------------------	--	--

C4 - Specific Entity Requirements

Establishing that entities (provider solutions) fulfil specific obligations as part of the technical trust framework.

Providers should note that where a question does not apply to their solution scope an explanation must be included in the answer.

Code	Question	Options	Supporting information	Scoring criteria
C4.1	Issuers			
C4.1.1	Revocation mechanism	Provided No evidence available	See section 4.1.1	To pass, providers must provide evidence of a reliable revocation mechanism and associated service to enable Verifiers to confirm that credentials have not been revoked.
C4.1.2	Verification of claims	Provided No evidence available	See section 4.1.2	To pass, providers must describe how their solution ensures that Verifiers are able to determine that claims are verified without the need for

				multiple intermediaries as well as providing adequate metadata to support trust.
C4.2	Wallet providers			
C4.2.1	Multiple credentials and granular control	Provided No evidence available	See section 4.2.1	To pass, providers must describe how their solution supports the acquisition of multiple credentials from multiple issuers and that Holders have full control over the subsequent sharing of credentials and attributes.
C4.2.2	Backup and recovery	Provided No evidence available	See section 4.2.2	To pass, providers must provide evidence that backup and recovery facilities are provided to Holders and that this functionality is easy to use, secure, and portable (e.g., for transfer to a new device).
C4.2.3	Secure Storage	Provided No evidence available	See section 4.2.3	To pass, providers must provide evidence that keys, secrets, and sensitive personal data is stored in an appropriate secure storage system. Where on device or hardware solutions are not utilised, the provider

				must detail how their solution provides an equivalent or superior secure storage function.
--	--	--	--	--

7. Common criteria for all providers

All Providers will be assured against the following common criteria each of which references technical aspects defined in the preceding sections of *Part 1: Core Requirements* of the technical trust framework and *Part 2: Data Schema*.

Providers are requested to respond to all questions unless they do not fulfil a specifically highlighted role (in this case they must respond “Not Applicable”).

When responding providers should include details relating to the specific solutions or products and not generally to an organisation.

C2 - Interoperability

Establishing that provider solutions are able to interoperate despite the use of differing SSI stacks in the ecosystem.

Providers should include details of how their solution supports interoperability directly clearly stating where capability is in production or is planned for future releases.

Code	Question	Options	Supporting information	Scoring criteria
C2.1	Please provide details of how your solution is able to interoperate with a common protocol for credential exchange as described in section 2.5.1 including a list of stacks supported.	Provided No evidence available	See section 2.5.1	To pass, the provider must evidence interoperability capability with OpenID SIOP stack.

C2.3	Please confirm that your solution supports Presentation Requests either as a Verifier or as a Holder (wallet) processing such as request.	Yes No Not applicable		To pass, the provider must confirm that Presentation Requests are supported.
------	---	---------------------------	--	--

C3 - Technical and Security Requirements

Establishing that provider solutions meet baseline requirements for information security and the protection of personal data in any form as it is processed or stored.

Providers should focus responses on the solutions and products directly deployed in the ecosystem rather than more general organisational controls or provisions.

Code	Question	Options	Supporting information	Scoring criteria
C3.1	Protection of personal data	Provided No evidence available	See section 3.1.1	To pass, the provider must provide evidence that controls are in place to ensure the confidentiality and integrity of personal data, at rest or in transit, and processes are put in place to protect the underlying identity system from unauthorised access or abuse.

C3.2	Privacy of the Subject must be protected throughout the identity lifecycle	Provided No evidence available		To pass, providers must provide evidence of controls implemented to ensure that the principles of Privacy by Design and Data Minimisation are observed with regard to Subject data.
C3.3	Data accuracy	Provided No evidence available	Not applicable to Verifiers and/or Relying Parties.	To pass, Issuers and Wallet Providers must provide evidence of process and/or functionality enabling Subjects to view and amend errors or make required updates. Subjects should be able to update erroneous, out of date, or poor-quality data to reduce identity errors.
C3.4	Data sharing	Provided No evidence available	See section 3.1.4	To pass, providers must provide evidence of how data sharing is avoided where excessive and where aggregate computations are used as a sufficient alternative to data sharing.
C3.5	Message integrity	Provided No evidence available		To pass, providers should provide a confirmation that they are compliant with the W3C

				Verifiable Credential Data Model v1.1 with reference to the signing of credential payloads. Providers should also provide evidence of additional provision for message integrity above and beyond the signing of credentials.
C3.6	Ecosystem technical trust	Provided No evidence available		To pass, providers must provide a description of controls implemented to ensure that only parties which are legitimate scheme members are able to interoperate with their solution in the context of the Trust Framework.
C3.7	Management and security best practice	Provided No evidence available		To pass, providers must provide evidence of, and that they have fully implemented, appropriate policies and procedures for the management of solution development and security throughout the organisation.
C3.8	Security Controls and Technical Infrastructure	Provided No evidence available	See section 3.4	To pass, providers must provide evidence that appropriate security controls are built into

				any technical infrastructure of their solution. These controls, and any physical or administrative security measures, should ensure the maintaining of any level(s) of trust required by the trust framework.
--	--	--	--	---

C5 - Compliance with Data Schema

Establishing that data is encoded and shared between entities in a standard format that promotes principles of data minimisation but also interoperability across the ecosystem.

Code	Question	Options	Supporting information	Scoring criteria
C5.1	Compliance with the data schema when utilising credentials as part of the trust framework.	Yes No		To pass, providers should describe how they comply with the data schema when issuing, holding, or verifying credentials.
C5.2	Compliance with the data schema in the management and use of metadata alongside credentials as part of the trust framework.	Yes No		To pass, providers should describe how they comply with the data schema with regards to metadata and how that



				metadata is utilised in their solution.
--	--	--	--	---