Open Digital Trust Initiative

Principles for Digital Trust Networks

February 15, 2022

Introduction

The Open Digital Trust Initiative is a joint initiative of the Institute of International Finance (IIF) and Open ID Foundation. It is an interoperable and open standards development, aiming to create a vibrant marketplace for digital trust services which would help individuals and entities to confirm identity and other attributes and to understand and manage risk.[1]

The Policy development workstream of the Open Digital Trust Initiative has developed Principles for Digital Trust Networks, identifying at a high level the 'rules of the road' that Digital Trust Networks should adopt in order to incentivize a high level of digital trust, user centricity and low cost, while ensuring that these networks are economically viable and the role of Verification Service Provider is adequately rewarded and realistically protected from a liability perspective.

The broad vision is for Digital Trust Networks to comprise a set of participants, including Users (who are also individual Data Subjects for individual data protection purposes in many cases), Verification Service Providers and Relying Parties. There is also scope for other types of intermediaries to be defined by the Network rules.

Digital Trust Networks are anticipated to have associated Governance Arrangements, which should adhere to certain minimum principles, and may be separate legal entities. The Governance Arrangements will have responsibility for setting out Liability Rules, and other rules and requirements, to be complied with by Network Participants.

While the IIF and Open ID Foundation do not themselves propose to police the Principles, or award or allocate trust marks to particular Digital Trust Networks, they would encourage third-party verifiers, auditors and others to consider offering these services.

A draft of these Principles was publicly released for comment on February 8, 2021, and comments received from commenters have been taken into account in finalizing the Principles.[2]

The IIF has co-published the Global Assured Identity Network (GAIN) White Paper.[3] These Principles are intended to be a framework for many possible digital trust networks, including centralized, federated, and decentralized models, including the GAIN as one example.

[1] This Initiative was described in Episode 73 of the IIF's Finance, Regulation and Technology (FRT) podcast, and discussed in the wider context of digital identity interoperability and inclusion in Episode 78.
[2] Draft Principles for Digital Trust Networks > The Institute of International Finance (iif.com)
[3] Global Assured Identity Network White Paper > The Institute of International Finance (iif.com)

Furthermore, this document is not intended to set a normative standard – it sets out a set of principles that are intended to guide those developing or joining trust schemes. Not all trust schemes are the same or have the same use cases and so there will be justifiable deviations.

Lastly, there are rapid developments across the globe in the market for and ecosystem around digital trust services (including in e-government services), and in adjacent policy spaces including privacy and cyber-resilience. Such developments may mean that the Principles continue to be updated to evolve over time. The IIF will keep the Principles under review as needed, in liaison with its members.

A. Governance Arrangements

Robust governance is at the heart of Digital Trust Networks. [1] *These Principles define the functions of the Governance Arrangements and other principles for the set-up and conduct of those arrangements.*

1. The **Governance Arrangements**, at a minimum, will have the following functions:
    a. Establishing the categories of Network Participant, including categories of participant who may admit other participants in a multi-tiered arrangement.
    b. Establishing criteria (consistently with these Principles) to become, or to cease to be, a Network Participant at any level in the hierarchy, including criteria about contracts (including terms about Liability), or about fees and charges.
    c. Applying those criteria to individual Network Participants or prospective Network Participants at the top level, including by admitting or removing or excluding them (for example, for serious or repeated breach of any applicable requirements, or for misuse of their position as a Network Participant).
    d. Maintaining and operating any infrastructure or property that may be required to be held centrally (such as rules or contracts that apply to Network Participants, trust marks or similar intellectual property, reference data relating to Network Participants, keys to Network Participants, publication of APIs, etc.).
    e. Either determining the scheme management and Technical Standards for the Network or, if another body is the scheme manager or technical standard-setter, liaising with the scheme manager or technical standard-setter to ensure that Network Participants' needs are taken into account by that body and that changes to the scheme and Technical Standards do not cause undue disruption to Network Participants or Network operations.
    f. Delegating any of their functions to a service provider or other body or arranging for them to be carried out by any automated process.
    g. Determining a supervisory function for strategic target alignment/adherence and a conflict resolution mechanism/ function.
    h. Determining any necessary changes to these Principles.
2. **Fit for purpose** – the Governance Arrangements should be able to perform the relevant functions identified in a timely and efficient manner and should have reasonable access to the necessary resources and information to do this.
3. **Economical** – The Governance Arrangements should not be unnecessarily complex or costly.
4. **Consultative** – Changes to the Governance Arrangements and these Principles should be made only after consultation with all affected stakeholders (or, in urgent cases, after consultation with or with appropriate notice to directly affected stakeholders). Changes to the Technical Standards should be notified to all Network Participants with reasonable notice, where possible.
5. **Participant fitness** – a Network Participant should be required to have adequate resources, legal authorities, and reasonable policies and procedures in place designed or adequate to ensure operational viability, system security, and business and system continuity and succession, so as to enable it to operate securely and effectively as a Network Participant.

1 Capitalized terms are defined in section F.

6. **Conflicts of interest** – participants in the Network and in the Governance Arrangements must deploy appropriate mechanisms to ensure any information they gain in that capacity is not misused.
7. **Accountable** – the Governance Arrangements should maintain one or more appropriate processes for taking feedback, handling complaints, and dealing with appeals.

B. Economic model

A Digital Trust Network must be economically sustainable while allowing Users ready access to the Network and the Trust it provides.

1. **Fee fairness** – Any fees charged to Network Participants should be allocated among stakeholders fairly and in an inclusive manner. The Network should avoid charging monopoly rents.
2. **Economic sustainability** – Any fees should be consistent with the need to help ensure the economic sustainability of the Network over time.
3. **Adequate incentives** – Network Participants should be entitled to expect fair reward so as to provide adequate incentives for participation.
4. **Inexpensive/free for Users** – The goal is to make verification of Identity as close to free for the individual User as is practicable, consistent with the Principles above.
5. **Transparency** – Any fees charged to a Network Participant should be made transparent to it. Other services associated with or enabled by the verification of Credentials should not be priced in such a way as to undermine this Principle.
6. **Intellectual property** – The Network should license all intellectual property it owns royalty-free, or on fair, reasonable and non-discriminatory commercial terms, to the extent this is necessary to allow other Networks to interoperate with it.
7. **Market based mechanism for service pricing and clearing** — The system should allow for vendors to help connect Relying Parties and Verification Service Providers.
8. **Capable of supporting tiering** — A verification fee should be able to be broken down according to the different services provided. For example: Relying Party —> Aggregator —> Dispute Resolution Provider —> Verification Service Provider —> (Re)insurance Provider.

C. Technical Principles

The technical Principles set out the key technical requirements for the technical system or substrate that underlies each Digital Trust Network, to enable it to comply with these Principles.

1. **Digital** — The Network should be capable of operating 100% digitally. Users, Relying Parties, Verification Service Providers and others should all be able to transact in the digital space. Subject to applicable law, all Network Participants should be able to be onboarded fully digitally. The wholly digital experience can be supported by offline elements where appropriate or necessary (e.g. to ensure access for the digitally or financially excluded).
2. **Open** — The Network should be based on open standards and on a legal framework that does not create undue barriers to entry to the market. The implementation of open standards should be subject to ongoing certification of technical conformance to those standards.
3. **Inclusive** — The Network should be designed so that all people can in principle establish Trust, subject to fulfilling requirements designed to prove Credentials, and specified eligibility requirements such as sanctions.
4. **Interoperable** — No system can expect to be truly global, covering all geographies, sectors and devices, so the Network should be designed to function both on its own and in conjunction with other Networks, including regional and local Networks, single- and multi-purpose Networks (across sectors such as finance, employment, health care, education, and e-government), and Networks giving access through a range of devices.
5. **Probative** — The Network should be capable of generating/supporting binding transactions and enabling proof of Credentials to the standard that is reasonably required by Relying Parties or other Network Participants.
6. **Resilient** — The Network should be technically and operationally resilient, with no single point of failure, and maintain high levels of availability and fast recovery.
7. **Simple / Seamless / Thin layer** — All Network Participants should be able to join and leverage the capabilities of the Network without significant cost or difficulty.
8. **Extensible** — The technical system underlying the Network should be extensible, allowing for a range of storage options (e.g. wallets, vaults), a range of legal contracts, a range of payment terms and a range of types of verification services.
9. **Confidential** – The Network should be protected by confidentiality measures designed to protect against unauthorized access to or disclosure of information.
10. **Integrity** – Data processed by the Network should be protected from corruption or unauthorized modification.

D. Privacy and data protection

The User should be at the center of the Digital Trust Network, so data privacy and security should be accorded high priority and built in by design, consistent with the business purpose of the Network, while limiting fraud requires a high degree of auditability and traceability.

1. **User centric** — The User should drive the movement and sharing of Trust. Users should own the right over the use of raw data about themselves and have conscious and active control over sharing of such data including, unless they opt-in to a time-limited persistent consent for one or more use cases, each instance of data sharing.
2. **Private** — The User should be in control of what information about the User is shared and when. (This Principle is subject to applicable law, which may specify bases other than consent for the sharing of information. However, these derogations should be made transparent to the User to the extent lawful.)

   > ***Comment:*** *Data within the Network should be handled and all interactions on the Network should be conducted with an expectation of privacy, within the limits of compliance with applicable law and regulations (including those relating to public health).*

3. **Data minimization** – The technical system that underlies the Network should be designed to minimize the exchange and retention of information and data, consistently with applicable regulatory requirements of the Network Participants, and with the desirability of reducing the vulnerability to cyber attack of the Network.
4. **Transparent** — Within each jurisdiction and across jurisdictions, Users should be made aware in clear terms of the legal basis of their participation in the Network, including limits to their privacy arising under applicable law. Settings relating to privacy and consent should be fully transparent to the User and the User should be prompted to review them periodically.
5. **Consent based** – Consent with regard to data sharing and use within the Network (where required) should be given and obtained on an informed basis and with appropriate protections for minors and vulnerable individuals, and fully respecting applicable laws that define consent for data protection purposes.
6. **Portable** — Users should have the right to make use of Verification Service Providers of their choice. In case Users want to store their data with third parties (i.e. not with the Credential Issuer or on their own device) they should have the right to move their Credentials from one Verification Service Provider to another. Network Participants should at all times act consistently with their roles as data custodians on behalf of Users.
7. **Revocable** — Users should be able to request a Revocation of data, which could be implemented by actions by Network Participants or by technical means. Network Participants may need to retain some records for contractual or regulatory purposes.
8. **Highly secure** —Technical, legal and operational measures should be maintained to make the Network highly secure in view of the attractiveness of information contained in Credentials to identity thieves, fraudsters and potentially hostile state actors.
9. **Anti-fraud by design** – the Network should be designed in such a way as to minimize or prevent, within reasonable tolerances, possibilities for fraud. Network Participants should deploy all reasonable measures to ensure they are not impersonated in the Network by malicious actors, having regard to the potentially damaging effect on Network Participants, and the credibility of the Network, of such events, as well as the desirability of Network Participants transitioning from less efficient paper-based methods which may also be insecure.

10. **Supports providing protections as a service** – Network Participants should be enabled to offer services to Users or other Network Participants that prevent facilitation of fraud (for example by reducing or preventing exploitative "dark nudges" that trick Users into sharing data that are not needed to complete relevant transactions).
11. **Auditable** — The Network should be auditable. What information was shared, when, with whom, with what approval and with what tracing technology should be logged. Logging should be consistent with the Private, Highly secure and Data minimization Principles. One specific audit path required for certain use cases is the traceability of a verification back to the Identity of a User.
12. **Compatible with official Identity** — To be compliant with regulations derived from FATF guidelines, Credentials in financial services settings may be required to be based on Credentials issued by official sources. The Network should facilitate the use of officially issued Credentials where required.
13. **Compatible with unofficial identities**: There should be a mechanism, aimed at financial inclusion, that should facilitate the participation of Users who do not have an officially issued Identity, where permitted by regulations derived from FATF guidelines, or in settings where such regulations do not apply.

E. Legal framework and liability

To enable adoption and use of any Digital Trust Network, the rules and consequences of participation must be clear and supportive of the intended use. The Principles set out in this section set out the key components that need to be combined to achieve this outcome.

1. **Compliant** – The Network and all Network Participants should comply with applicable law and regulations and with the reasonable expectations of other Network Participants. For example, warrants should be respected, and AML/CTF regulations should be followed by those that are subject to those regulations.
2. **Foundation of Trust** – To establish Trust and acceptance, a Network should have controls that are designed to ensure that it is appropriately reliable for its intended uses, and that Network Participants understand the consequences of proper and improper behavior.
3. **Transparent –** To build this foundation, the policies and practices of a Network regarding topics such as standards / duties, Covered Liability, use benefits and proportionate controls (including on access) should be clear and accessible to Network Participants.
4. **Contract-based –** So that the Transparent Principle is achieved, subject to minimum requirements of applicable law, the items mentioned in that Principle should be explicitly addressed through one or more contracts.
5. **Compliant** – Requirements and restrictions arising from applicable law on, among other things, the ability of Network Participants to exclude or allocate Covered Liability (for example in consumer-facing settings, including regarding the protection of data), or on choice of venue for resolution of disputes, should be respected.

   Comment: *One source of such laws may be open banking/open finance/consumer data right regimes.*
6. **Standardized –** Within a Network and across Networks, contracts among Network Participants should be standardized as much as possible to support Trust and transparency, and reduce the cost and complexity of use.

   Comment: *The form of contract will often be specific to a Network, but there would be benefit in using common language or structures across Networks (akin to open source software licensing, or PKI certificate policies).*
7. **Digital contracts –** To enable 'straight through processing', wherever possible under applicable law, a Network's contracts should be capable of being executed digitally. Additionally, contracts should be structured to minimize bilateral processes between Network Participants (e.g., by being multilateral where required to support the Network operating at scale).
8. **Rules governed –** The Network should set out rules to govern: (i) the allocation of Covered Liability between (categories of) Network Participants (**Liability Rules**); (ii) the terms on which other Networks that wish to federate or interconnect with the Network may do so; and, (iii) on-boarding arrangements that should be consistent with those rules. In framing the Liability Rules, a Network should take account of the factors set out in **Annex 1**.

   Comment: *The Liability Rules or other rules, Technical Standards or protocols governing a Network should also set out clearly the consequences and expected mitigation actions should a Network Participant acquire knowledge that Credentials it supports as a Network Participant have been stolen or compromised.*

9. **User Liability –** The Liability Rules should provide that Users, acting in their capacity as such, will not be subject to direct or indirect Liability for accidental false, misleading or missing information about themselves. This is distinct from:

    a. knowingly providing false or misleading information, or knowingly failing to correct false or misleading information;

    b. withholding information when under a legal obligation to provide it (e.g. in insurance contracts, where obligations of utmost good faith may apply); or

    c. other intentional fault or contravention of the Network rules (such as by facilitating the use of their identity data by unauthorized persons / supporting identity fraud).

    Comment: *The Liability Rules should not protect Users (or those purporting to be Users) that undertake abusive, fraudulent, or criminal behavior.*

10. **Liability approach –** The Liability Rules should clarify the Liability standards that are to apply to Network Participants, at least for the use case where a Verification Service Provider issues, at the request and for the benefit of a Relying Party, an attestation regarding Credentials of a User.

    In recognition of the fact that Verification Service Providers may apply different practices, and Relying Parties may have different needs regarding the exercise of recourse with respect to Credentials attested to by Verification Service Providers, an approach to liability as per the table of **Annex 2** should be considered by Networks.

    Comment: *Liability transfer between Network Participants should be considered purposefully (and not as an insurance policy that assumes that all Identities should be 'perfect'). This would assist the Network to achieve commercial viability and scale, enable the standardization of Attestation Requests, and offer visibility on Liability implications. No identity proving process is perfect, and different Levels of Assurance can apply in the case of each Credential.*

    Comment: *Different roles within the Network will give rise to different responsibilities and the Liability attaching to those roles may in consequence differ.*

11. **Market freedom –** Subject to these Principles and the Network's Liability Rules, all Verification Service Providers should be free (but not obliged) to offer more beneficial terms (than the default under the Liability Rules) on a bilateral or multilateral basis, including:

    a. different prices or rates at which they are willing to provide services at different Levels of Assurance or to different standards of Liability (e.g. increased liability for premium use cases);

    b. categories of Covered Liability excluded (such as strict or fault-based liability options); and

    c. limitations of Covered Liability accepted (such as per-claim or aggregate limits).

12. **Auditability –** To support Liability Rules, and Trust in the Network, the Network should require and support a proportionate level of data retention that protects the privacy of Users while enabling auditability and traceability, the collection of evidence to enable investigations or other mitigation actions (such as in case of errors, incorrect Credentials, or fraud), or the actioning of Revocation requests (where applicable).

    Comment: *This protects the Network by being able to identify and reduce fraud and errors.*

13. **Objectively testable –** Conformity of Network Participants with the Liability Rules (e.g. conformance to standards that enable Trust and that may provide a defense where fault-based Liability applies) should as far as practicable be objectively testable so as to enable low-cost audit and third-party verification at large scales. The Liability Rules should specify the objective criteria to be applied to determine Liability in each use case and to each Level of Assurance / standard of Liability dealt with.

14. **Principles of engagement –** In making and enforcing Liability Rules, Network Participants should not engage in behavior that contravenes competition law, and should act in a proportionate and consultative matter consistent with the Consultative Principle in Section A: Governance Arrangements.

15. **Other liability arrangements –** Nothing in these Principles should prevent any Network Participant from entering into arrangements (e.g., insurance or derivative contracts) with non-Network Participants to further transfer, share, spread or mitigate Covered Liability. Such arrangements may also operate on a Network-wide basis if the risks are sufficiently understood and a risk pool considered proportionate. However, no such arrangement should alter the application of these Principles, or the Liability Rules.

F. Definitions

1. **Aggregator** – an entity that aggregates Credentials or other information relating to a User or to a Network Participant acting as such.
2. **AML / CFT –** anti-money laundering and countering the financing of terrorism.
3. **API** – application programming interface.
4. **Attestation Request –** a message addressed to a Verification Service Provider requesting the confirmation, to a specified Level of Assurance and/or subject to a specified Liability standard, of certain Credentials.
5. **Covered Liability –** Liability (or category of Liability) arising between Network Participants from their relationship as such.
6. **Credential –** Identity or status information about a User (for example, that may qualify the User for certain benefits or status, such as an attestation that a User is of a particular age or nationality, has gained a certain educational attainment, or has a certain form of legal incorporation or has a specified relationship with another person, entity or thing).
7. **Digital Trust Network** (or **Network**) – a network for the establishment and/or promulgation, through digital means, of Trust.
8. **Dispute Resolution Provider** – a service provider that resolves or seeks to resolve disputes between Network Participants and/or Users.
9. **FATF** – Financial Action Task Force.
10. **Governance Arrangements** – the individuals, entities or algorithms that collectively are empowered to determine the Rules for a Network.
11. **Identity** – means of identification of a User, issued by an authoritative source such as a registry, which may be composed of a set of Credentials, with or without a unique identifier.
12. **(Re)insurance Provider** – a provider of (re)insurance services to Network Participants acting as such.
13. **Issuer** – an entity that issues Credentials.
14. **Level of Assurance** – an indicator of the extent to which Trust may be placed in one or more related Credentials (for example, as a result of the quality of the source or processes surrounding the same); each Level of Assurance in a given Network may correspond with a different Liability standard.

    > ***Comment****: Various means of indicating the Level of Assurance can be adopted, including confidence scoring, Network specific measures, and/or legally recognized standards such as those under the European Union eIDAS Regulation (Regulation (EU) 910/2014).*
    >
    > ***Comment****: The Liability model does not necessarily limit the Level of Assurance associated with Credentials. It can however provide commercial or financial assurance in relation to a given Level of Assurance.*

15. **Liability –** criminal, civil, administrative or regulatory liability, order or sanction (whether monetary or not) under the laws of any jurisdiction arising in respect of any fault, failure, breach, state of affairs or circumstance (other than a liability in the nature of taxation).
16. **Liability Rules –** the Liability allocation rules determined for a Network as mentioned in the **"Rules governed"** Principle.

17. **Network Participants –** (i) entities or individuals making use of the Network to establish and/or promulgate Trust, including Users, Relying Parties, and Verification Service Providers; and (ii) entities or individuals which have significant influence over, or the right to appoint or elect representatives in, the Governance Arrangements for a Network.
18. **PKI** – Public Key Infrastructure.
19. **Principle** – one of these Principles for Digital Trust Networks.
20. **Relying Party –** a Network Participant issuing an Attestation Request requesting the confirmation by a Verification Service Provider of certain Credentials to a specified Level of Assurance and/or subject to a specified Liability standard.
21. **Revocation** of data – an implementation of a request of a User to be forgotten, or of a mandate or request to delete or deidentify data about a User that is no longer needed.
22. **User** – the individual, legal entity (e.g. private company) or other thing that is, or claims to be, the subject of Credentials.
23. **Technical Standards –** standards (such as technical protocols or APIs) that relate to technical aspects of the operation of a Network or of the technical system that underlies a Network.
24. **Trust –** trust in Credentials relating to Users.
25. **Verification Service Provider –** a Network Participant that agrees, upon receipt of an Attestation Request, to confirm certain Credentials to a specified Level of Assurance and/or Liability standard.

    Comment: *A Verification Service Provider can be either the Issuer itself or a reliable independent third party such as a bank, credit bureau, data provider, or specialist service provider. In some Networks this role may be referred to as an "assurance provider".*

Further definitions for Annex 2

26. **Basic Credential Custody Representations –** all of the following representations in relation to a Credential that are given by a Verification Service Provider, in line with the specific requirements of the Network's processing standards or rules (e.g. the features of the relevant Level of Assurance):
    1. The Credential is **obtained from a source** that is viewed as reliable and using customary identity-proofing or verification processes meeting relevant requirements (e.g. AML / CFT, if the Network is focused on this activity) – specifics on such standards are likely to be set out within the Network's processing standards or rules as part of transparency and ensuring Trust;
    2. The Credential is **maintained** by the Verification Service Provider in compliance with relevant requirements and consistent with the risk profile of the relevant Level of Assurance;
    3. The Credential is **consistent** with other Credentials about the User provided by the Verification Service Provider at the same time, if such checks are part of the processing standards of the Network.
27. **Error**, with regard to a Credential or an attestation relating to a Credential – the Credential or attestation being false or misleading in a material particular, or containing a material omission, whether or not as a result of fault of a Verification Service Provider.
28. **Fraud**, with regard to any Credential – issuing an attestation which contains an Error relating to any Credential, knowing of the Error and intending that the recipient be misled thereby in order to gain a financial or other advantage for the issuer of the

attestation or for another, or to cause the recipient a loss or deprive the recipient of an expected benefit.

29. **GDPR** – General Data Protection Regulation of the European Union (Regulation (EU) 2016/679).

30. **Recklessness or Gross Negligence** – issuing an attestation which contains an Error relating to any Credential, while being reckless or grossly negligent as to the Error or whether the recipient would be misled thereby; this shall include willful default and other equivalent action in breach of the Network's processing standards or rules (e.g. the features of the relevant Level of Assurance).

Annex 1: Factors to Be Taken into Account in Framing Liability Rules

A Network should take account of the following Principles when framing its Liability Rules.

A. **Objectives**: The objective(s) of the allocation of Covered Liability should be clearly defined.

Default objectives: In the absence of other defined objective(s), the objectives of the Liability Rules should be to:

a. incentivize the Network Participants to collectively undertake an efficient level of investment in ensuring the accuracy, integrity and security of Identities and Credentials (i.e., the level of investment at which the marginal social cost of higher investment is greater than the marginal social benefit);

b. incentivize the Network Participants to act so as to maintain a high degree of Trust while ensuring that different categories of Network Participant are not subject to Liability that is disproportionate to the rewards they may derive from participation in the Network;

c. recognize and clearly define the different kinds of Network Participant, such as Relying Party, Verification Service Provider, and other participants including User and any intermediaries such as wallet or vault providers;

d. clearly recognize that Credentials are not 'perfect' and that a level of error is inherent. The Liability Rules can (if appropriate for the Network's activity) distinguish between various Levels of Assurance and/or standards of Liability, or similar criterion, but this should focus on fault related to an Attestation Request unless a commercially viable alternative is desirable to achieve the objectives of the Network; and

e. place low or negligible Liability on Users, where those Users do not engage in abusive, fraudulent, or criminal behavior.

B. **Covered Liability definition**: the Liability Rules should clearly define the Covered Liability within their scope. This could be done by reference to:

a. the sources of Covered Liability (e.g. treaty, supranational law or regulation, national law or regulation, judge-made/case law, contract, administrative action, rules, etc.);

b. the type of Liability (e.g. criminal/civil/administrative) and the type of sanction that may be imposed; and

c. the duty, breach, relationship and conduct or other circumstances giving rise to Covered Liability.

Where different allocation rules or principles apply to different categories of Liability, the Liability Rules should also clearly define them by reference to the same factors.

C. **Scenarios under which Liability is imposed under the Liability Rules:** Where Liability is imposed under the Liability Rules (in particular, around Attestation Requests), that approach should be justified. As such, the Liability Rules should clearly specify:

a. the scenarios in which Liability will be additional to the position that would obtain in the absence of the Liability Rules (i.e. under applicable law);

b. the categories of Network Participant to be made subject to such additional Liability; and

c. the justification for, and any limits around, such departure.

Annex 2 – Illustrative Liability Approaches

A Network should take account of the following possible approaches when framing its Liability Rules

LIABILITY STANDARD	**1. BASELINE FAULT BASED LIABILITY**	**2. GREATER FAULT BASED LIABILITY**	**3. STRICT LIABILITY**
Purpose & contemplated use case	The Baseline Fault Based Liability model offers minimal recourse and protection regarding information attested by the Verification Service Provider but may be considered for data viewed as less critical by the Relying Party or in relation to which a higher degree of assurance is more difficult to obtain.	Subject to any cap arrangement agreed upon between the participants and where the commercials / pricing are capable of supporting it, the Greater Fault Based Liability model offers financial recourse and protection regarding information attested by the Verification Service Provider. In a finance context, this Level of Assurance may be viewed as commensurate with collated data for generally accepted customer due diligence (CDD) recommendations as defined by the FATF.[1] The Greater Fault Based Liability model implies that the Verification Service Provider may be held responsible when required processes are not complied with.	Subject to any cap arrangement agreed upon between the participants and where the commercials / pricing are capable of supporting it, the Strict Liability model offers recourse and protection regarding information attested by the Verification Service Provider and may be considered for data viewed as needing to be highly reliable, or critical.
General meaning	The Verification Service Provider assumes no responsibility for any Error in any attestation relating to any Credential transmitted to the Relying Party except to the extent of any of the following on the part of the Verification Service Provider in relation to the Error: - Gross Negligence / Recklessness; or - Fraud.	Same as for Baseline Fault Based Liability save that, in addition, the Verification Service Provider assumes liability in case of a Basic Credential Custody Representation (BCCR) being false in any material respect. The Verification Service Provider is deemed for these purposes to have made the BCCRs on each occasion.	The Verification Service Provider assumes responsibility for any Error in any attestation about any Credential transmitted to the Relying Party (regardless of fault). This is likely to be rare as a model (unless Liability is fixed or capped at a low level) given the absence of fault as a prerequisite for such Liability to be imposed.

[1] Note that the CDD-Linked Liability model is primarily related to FATF Recommendations 10 (*Customer Due Diligence)* & 17 (*Reliance on third parties)*.

LIABILITY STANDARD	**1. BASELINE FAULT BASED LIABILITY**	**2. GREATER FAULT BASED LIABILITY**	**3. STRICT LIABILITY**
Burden of proof in case of exercise by Relying Party	The Relying Party must show that: - the attestation relating to the Credential issued by the Verification Service Provider contained an Error; **and** - the Verification Service Provider acted with Gross Negligence, Recklessness or Fraud with regard to the Error; **and** - Liability was incurred by the Relying Party as a result of the Error. Other evidence (e.g. as to causation and mitigation) may be relevant.	The Relying Party must show that: - the attestation relating to the Credential issued by the Verification Service Provider contained an Error; **and** - either: o the Verification Service Provider acted with Gross Negligence, Recklessness or Fraud with regard to the Error in issuing the attestation; **or** o a Basic Credential Custody Representation was false in a material respect; **and** - Liability was incurred by the Relying Party as a result of the Error. Other evidence (e.g. as to causation and mitigation) may be relevant.	The Relying Party must show: - That the attestation concerning the Credential issued by the Verification Service Provider contained an Error; **and** - unless Liability is for a fixed sum (e.g. equal to, or a multiple of, the fee paid), the Liability amount that was incurred by the Relying Party as a result. Other evidence (e.g. as to causation and mitigation) may be relevant.
Main use case	This Liability standard is consistent with a use case offering limited protection and recourse to the Relying Party. This may be the case for lower risk use cases, or lower cost Attestation Requests, or in relation to certain categories of Credential.	This Liability standard is consistent with a use case offering protection and recourse to the Relying Party which is limited but consistent with the status of a Verification Service Provider supporting a Level of Assurance in respect of the Credential attested to higher than a low level.	This Liability standard is consistent with a use case offering protection and recourse to the Relying Party regardless of fault – it should not be assumed to offer 'full protection' without limit as this would rarely be commercially viable as a Network model.
Opt-out possible?	**Yes –** If another standard is mandated by the Network's Liability Rules, or agreed to between the relevant parties (e.g. Verification Service Provider and Relying Party), for the (subcategory of) use case concerned. Opt-out would, however, not be normal given the benefits of standardization.		
Basic Credential Custody Representations	Optional	Yes	Yes
Liability Cap	Yes, in line with the Network's Liability Rules or agreed to between the relevant parties (most commonly, Verification Service Provider and Relying Party). There may be areas where no cap applies, such as where imposed under law (for example, aspects of the GDPR).		

Annex 3: Contributor acknowledgements

The Policy workstream of the Open Digital Trust Initiative as a whole has contributed to the development of the Principles, and in particular the two dedicated working groups on **Liability and legal framework** and **Individual (or user) centricity**.

We wish to particularly thank and acknowledge the leading contributions of:

Rod Boothby – Banco Santander (Open Digital Trust Initiative co-chair)

Gena Boutin – Experian

Wendy Callaghan – AIG (Government and academic sector Working Group lead)

Scott David – University of Washington

Gene DiMira – The AML Shop (Interoperability Working Group lead)

David Hardoon – Union Bank of the Philippines (Individual centricity Working Group lead)

Angus McFadyen – Pinsent Masons LLP (Liability and legal framework Working Group lead)

Nick Mothershaw – OIX

Stéphane Mouy – SGM Consulting

Christopher Ngoi – Fnality

Bryn Robinson-Morgan, Mastercard

Tom Smedinghoff – formerly of Locke Lord LLP

Don Thibeau – OpenID Foundation (Open Digital Trust Initiative co-chair)

Eric Wagner – Raiffeisen Bank International AG

Laurence White – IIF

Greg Wolfond - SecureKey