TADIM SP – REPORT OVERVIEW

TRUST ANCHORS FOR DECENTRALISED IDENTITY MANAGEMENT

JOINING FORCES FOR BLOCKCHAIN STANDARDISATION

SHAPING EUROPE'S DIGITAL FUTURE, 17 JUNE 2020

Dr. Ignacio Alamillo Domingo (ES)

Mr. Patrick Curry (UK)

Introduction & ToR (approved in Dublin 2019)

Consider the nature of trust anchors and how they can now, or could in the future, support new and evolving models for decentralised and distributed identity management.

- 1. To form a new JWG4 Study with the purpose of producing:
  - a. A study report;
  - b. Recommendations for further work(s) including, if relevant, for the development of formal documents and international standards;
  - c. If one or more NWIPs are proposed, to provide in each case:
    - i. A draft NWIP;
    - ii. A preliminary working draft.
- 2. To assess whether work with other TC307 and SC27 projects, and a liaison with other bodies, would be helpful in pursuing the respective recommendations.

Scope

Identify, explore and evaluate trust anchors for decentralised and distributed identity management systems. At a minimum:

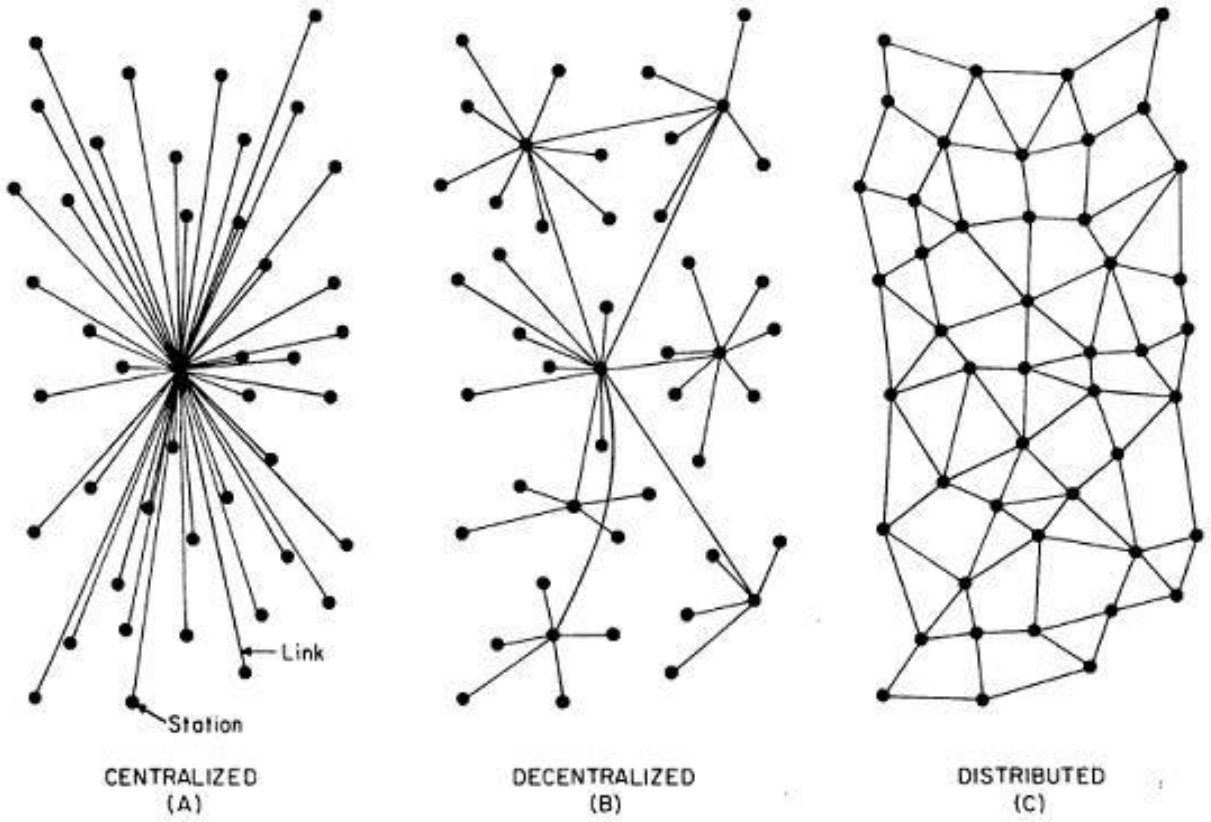
1. Capture information about existing models and practices;
2. Identify primary use cases and communities for each category;
3. Categorise the models and practices according to the trust anchoring techniques and the legal considerations;
4. Assess models for interoperability and federation;
5. Categorise the policies and governance frameworks;
6. Identify anomalies and issues that hinder progress;
7. Include other relevant characteristics.

Describing trust anchors

No single definition of trust anchor. Different categories:

- Legal trust anchors, which set the policy baseline for the trust framework and underpin the operating rules. These operating rules and rulesets can be standardised for use across organisations in support of Common Policy.
- Data trust anchors, which relate to the entities and attributes to be processed, where very high data quality is vitally important.
- Cryptographic trust anchors, which provide the roots of cryptographic trust and enable cryptographic binding, revocation, authentication, signing, encryption and other trust functions.
- Cybersecurity trust anchors, which monitor, detect and respond to policy violations, and enforce policy compliance. This includes assurance, testing and certification regimes, possibly augmented by blue/red teaming.

Distributed and decentralised identity management systems are not equivalent

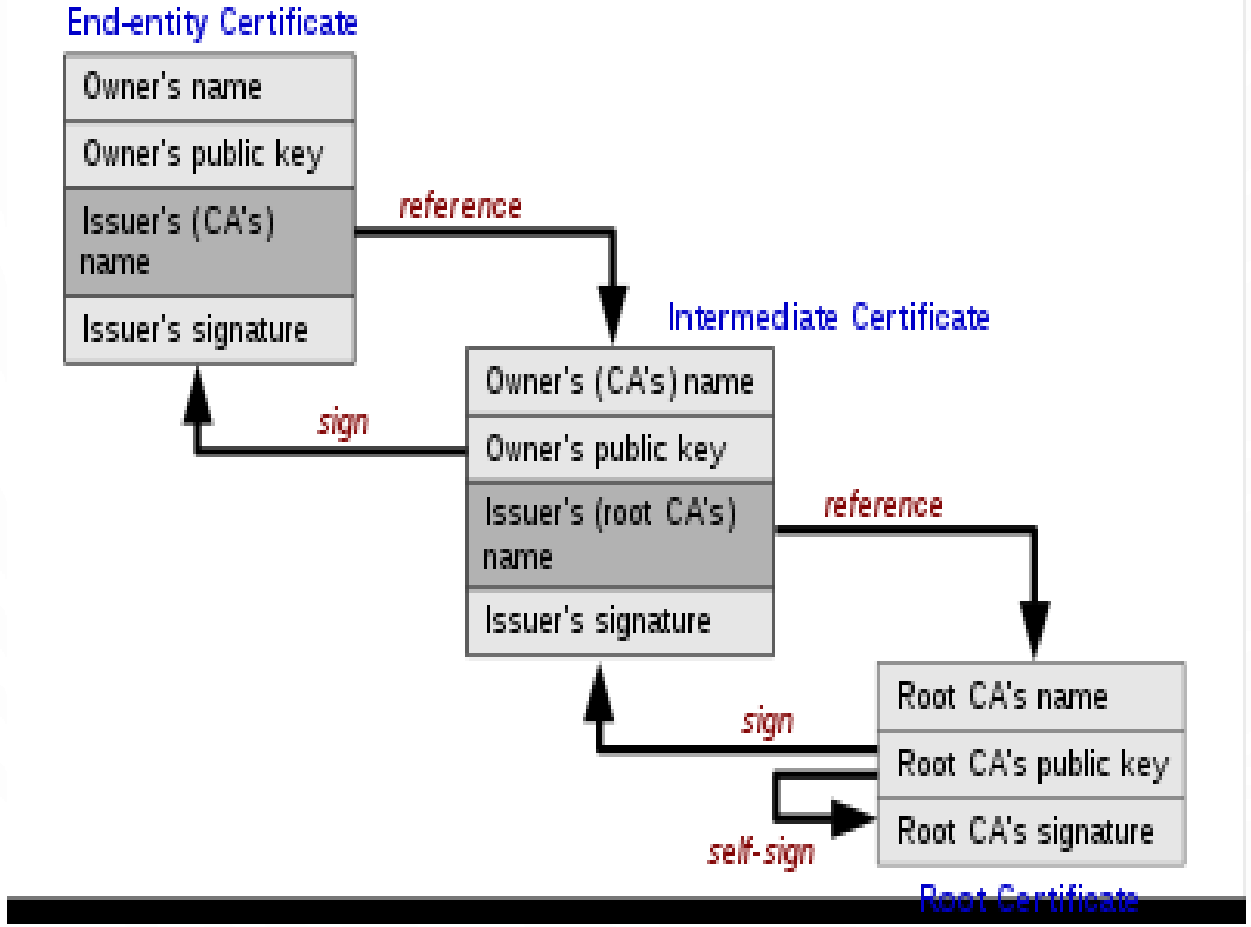


Decentralised networks contain single points of failure and distributed networks do not. Distributed networks operate in a mesh.

Beware of Blockchain based in distributed networks used for partially centralised identity processes and functions.

Federation and inter-federation policies and practices must be considered.

Cryptographic trust anchors in Public Key Infrastructures

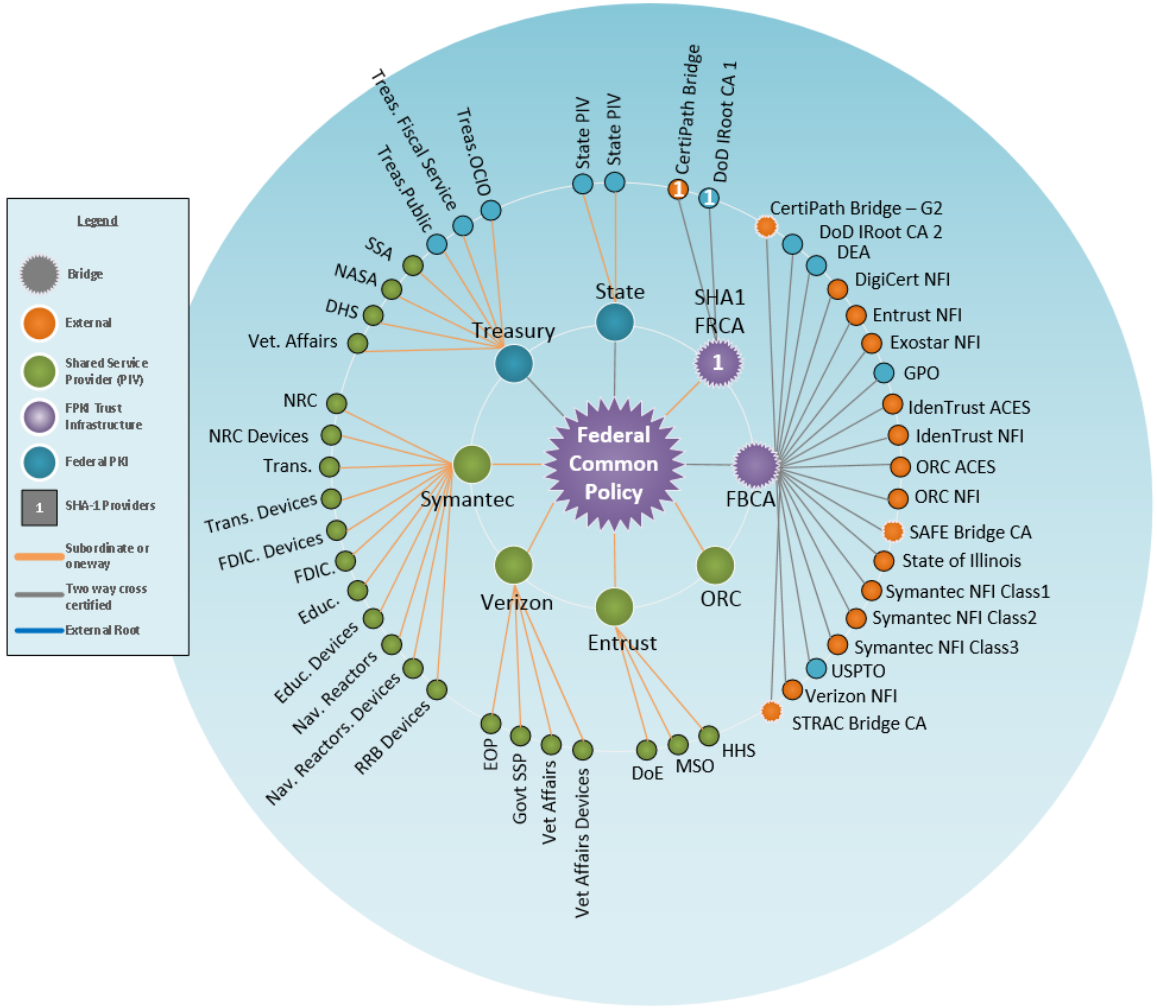


Useful for the validation of digital signatures using certification paths.

A trust anchor represents an authoritative entity via a public key and associated data.

Managed using trust lists and trust anchor stores.

Public Key Infrastructure Federated approaches

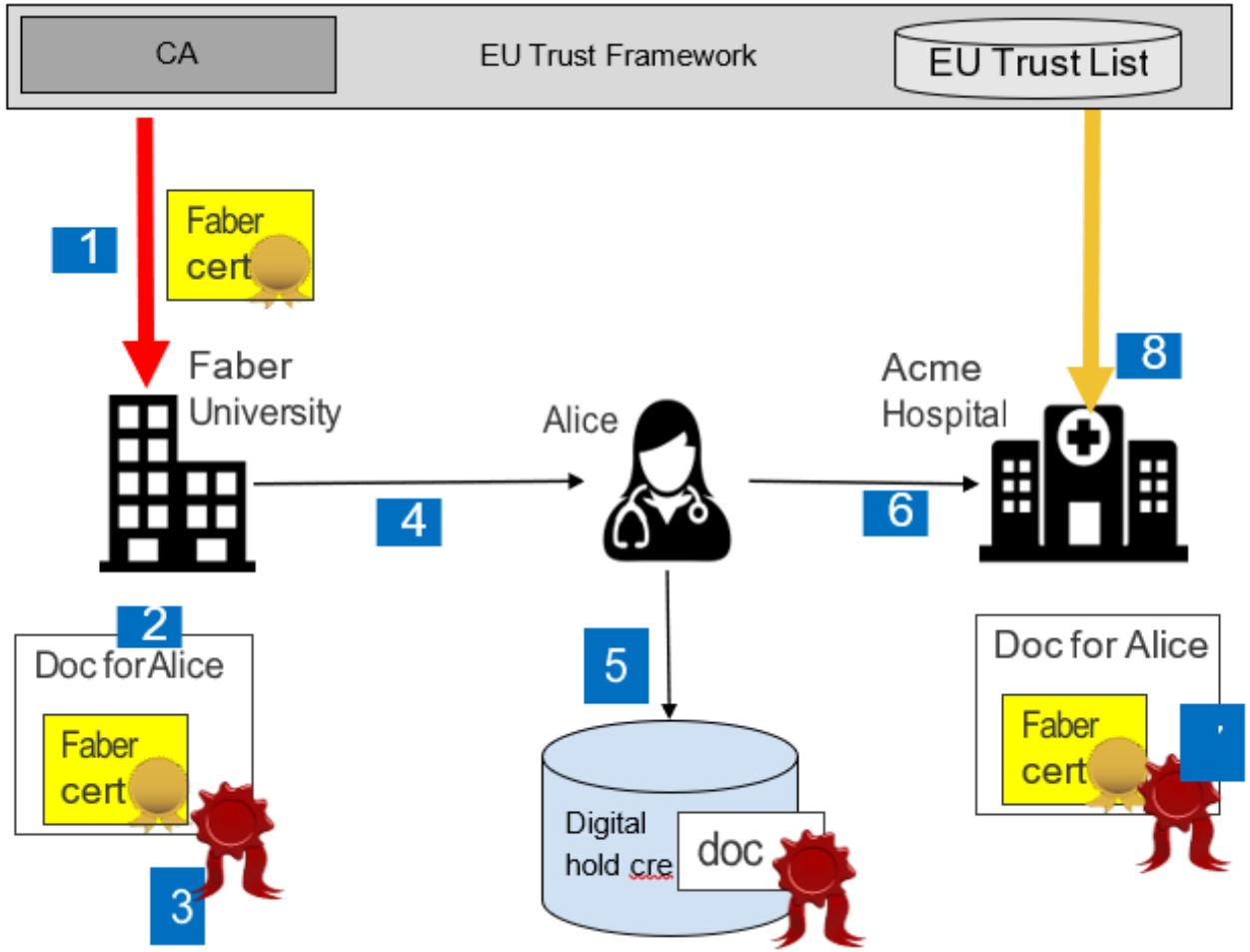


Used in high or very high security scenarios (such as government and industry employees), but no in consumer scenarios.

Strong, policy driven, governance frameworks.

Allow resilience between multiple CAs using cross-signing.

Data trust anchors in eID regulations – eIDAS regulation

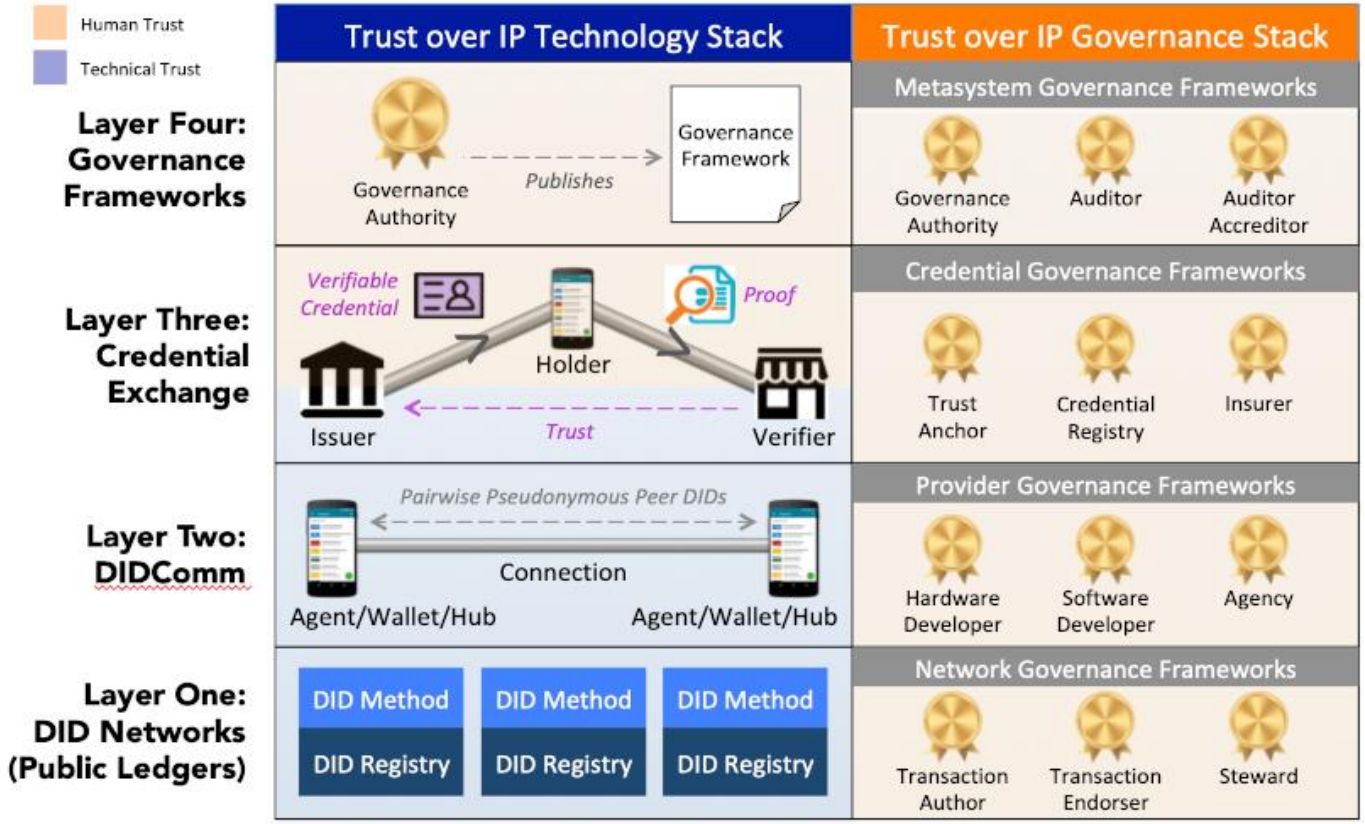


A legal trust anchor, partially based in cryptographic trust anchors, but not necessarily.

Data trust anchoring, based in inheriting trust from eID means.

Trust bridging between digital certificates and verifiable credentials.

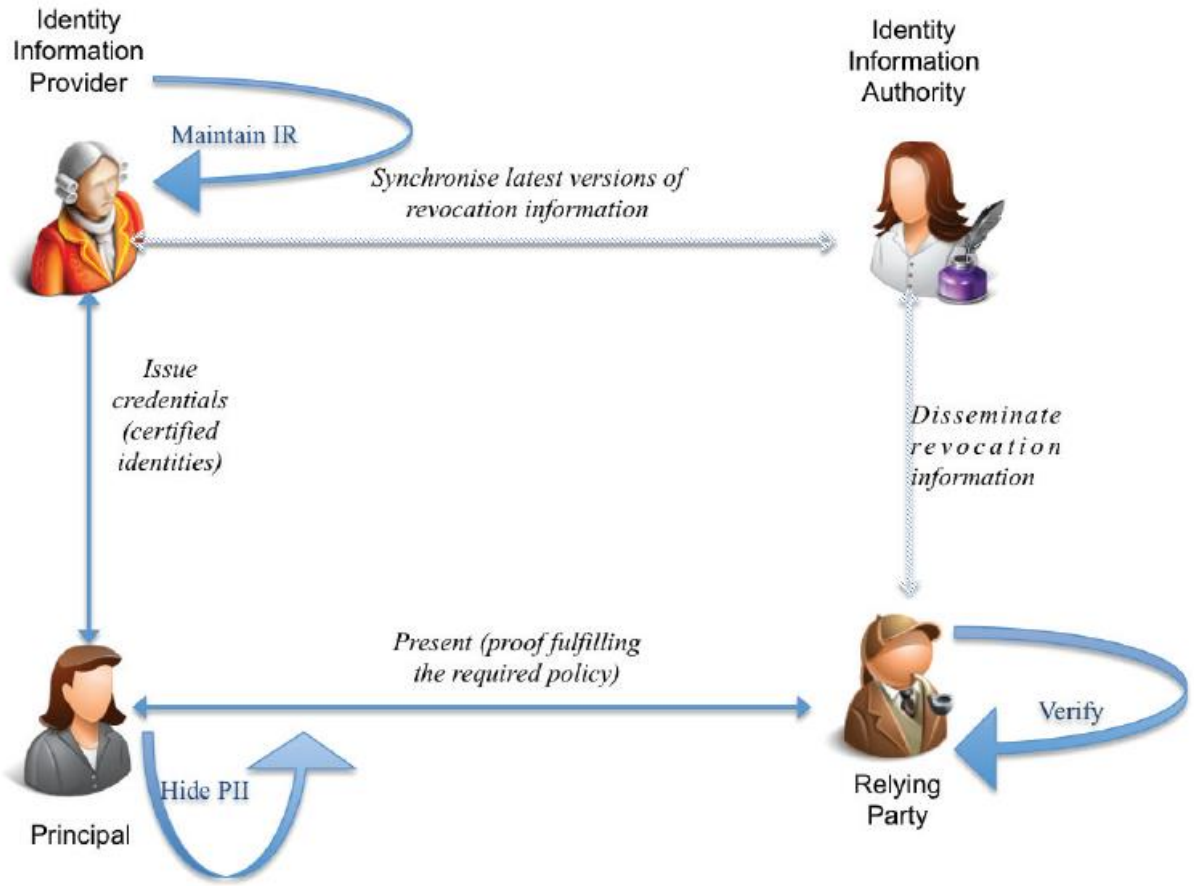
Data trust anchors in non-PKI-based SSI solutions using DIDs



Trust anchor as an authoritative issuer of a credential under a governance framework.

Different mechanisms to designate trust anchors: publishing lists of DIDs, issuing verifiable credentials to issuers, or using credential registries.

Data trust anchors using ZKP



Can provide a privacy preserving, one-time link between on chain integrity and off chain personal data

Avoids the stateful trusted intermediary such as DID and DID document.

Enables authoritative sources to notify changes directly to a Relying Party without user participation.

Conclusions – 1

1. Trust anchors are already being used but more are required, particularly to meet high assurance requirements in any regulated blockchain implementation and operation. These requirements need to be defined.

2. Trust anchors are essential to underpin the implementation and operation of trust frameworks at appropriate Levels of Assurance. Four types of trust anchors exist: Legal, Data, Cryptographic and Cybersecurity trust anchors. There may be more types in the future.

3. Legal trust anchors based in legislation, such as KYC, AML, GDPR, eIDAS, will normally be used to underpin data, cryptographic and cybersecurity trust anchors. It most cases, the legal trust anchor will support the governance framework based on contractual agreements or statutory law.

Conclusions – 2

4. The study shows there's a strong connection between trust anchors and distributed identity management trust frameworks, at different levels of assurance, as trustworthiness depends on the legal conditions regarding the quality and reliability of the identity information, and also the issuer's liability conditions. Ultimately, the authoritative source/issuer will only accept liability for relying parties if all the policy requirements are met. This also includes compliant policy and systems implementation inside the relying party.

5. Data trust anchors are authoritative, according to its related legal trust anchor, for a (distributed) identity provider to issue identity assertions (i.e. a form of a bound credential or a ZKP attribute) to relying parties. There are various proposals for establishing and managing these data trust anchors, but many lack sufficient maturity and best practices, and do not meet relevant standards or assurance criteria.

Conclusions – 3

6. Cryptographic trust anchors play many important roles, including cryptographic validation of digital signatures, when issuing and presenting identity attributes, and when DIDs are derived or associated to PKI schemes. There are various proposals for establishing and managing these cryptographic trust anchors, but many lack sufficient maturity and best practices, and do not meet relevant standards or assurance criteria.

7. Distributed, rather than decentralised (which contains single points of failure), identity management provides resilience, however, there can still be components in the distributed identity management implementation that are centralised.

Conclusions – 4

8. It is possible, even common, for a network to be partially distributed and partially decentralised. Therefore, any further work on TADIM needs to apply to both distributed and decentralised networks because there is so much that is common and because this better reflects reality. This means that TADIM should not be limited to decentralised systems, and its title should be changed from "Decentralised" to "Distributed".

9. Today's PKI federation models can provide a form of distributed identity management and enable multiple communities of trust to interoperate under a Common Policy. The combination of federation and distributed identity management principles is expected to create opportunities for new identity management services.

10. Today, the major technologies that support some form of distributed identity management include PKI, W3C verifiable claims, and ZKP. All of these rely upon the existence of at least four types of trust anchor.

Conclusions – 5

11. Further work is required to go deeper into each type of trust anchor and map them to major business use case scenarios, functional use, risks, different types of distributed identity management technologies and the trust anchors that each need in order to identify best practices and define requirements to be addressed. The result would be a framework.

12. Where possible, these requirements need to be aligned across the different business use case scenarios. Further work is needed to categorise each type of trust anchor with regard to risk and Level of Assurance, and typical use case scenarios. This would extend the framework.

13. Trust anchors and systems cannot operate in isolation; they have external dependencies. Chains of trust have to be an essential component in any framework, to address upstream and downstream dependencies.

Conclusions – 6

14. The study has shown a lack of risk models for in defining and managing trust anchors. The assurance of data and cryptographic trust anchors will be undermined unless the underlying legal and cybersecurity trust anchors exist and are strong.

15. Blockchains and DLT that are operating to provide a distributed identity management service will have additional requirements for trust anchors; these additional requirements need to be defined. They may themselves also be trust anchors to other services, including other blockchains.

16. The study recognises opportunities for blockchains and DLT to support both trust anchors and distributed identity management.

17. Further work is also required to develop new, suitable governance frameworks.

Recommendations to TC307 and JTC1/SC27, Nicosia 2020

1. To rename TADIM as Trust Anchors for DLT-based Identity Management.
2. To create a Technical Report – Overview Trust Anchors for Distributed Identity Management (TADIM) that uses the content from this Study Period.
3. To structure TR - TADIM similarly to TR 23249 – Identity, with similar section headings to enable clarity and to be mutually supporting. A WD0 has been provided.
4. To close the initial TADIM Study Period.

PLEASE CONTRIBUTE! SUCCESSFUL STANDARDISATION NEEDS STRONG COMMITMENT FROM EXPERTS