White Paper
The Trust Framework Series

A Global Inventory of Trust Lists, Trust Schemes and Trust Frameworks

In Collaboration with the LIGHTest Project

Rachelle Sellung – University of Stuttgart
Mike Leszcz - Open Identity Exchange
Michelle Parks – Open Identity Exchange
Sue Dawes - Open Identity Exchange

November 2017

Contents

Executive Summary

This whitepaper has been developed to share the work that is being undertaken by the LIGHTest project; in particular, work completed on trust inventories and the potential use cases.

The objective of the LIGHTest project is to create a global cross-domain trust infrastructure that renders it transparent and easy for verifiers to evaluate electronic transactions. By querying different trust authorities world-wide and combining trust aspects related to identity, business, reputation etc. it will become possible to conduct domain-specific trust decisions.

This is achieved by reusing existing governance, organization, infrastructure, standards, software, community, and know-how of the existing Domain Name System, combined with new innovative building blocks. This approach allows an efficient global rollout of a solution that assists decision makers in their trust decisions. By integrating mobile identities into the scheme, LIGHTest also enables domain-specific assessments on Levels of Assurance for these identities.

The Open Identity Exchange's UK chapter, OIX UK, is a partner in the LIGHTest project with a focus on informing the trust systems inventory work as well as leading outreach efforts to inform the global identity community on the project's work. This OIX White Paper is one in a series of OIX papers focused on trust framework development, governance, liability management as well as this inventory amplifying the work being done in the LIGHTest project.

OIX's involvement and role in the LIGHTest project is a natural extension of the work done by member organizations, a team of competitors, over the last 7 years. In March 2010, a number of OIX members published "The Open Identity Trust Framework (OITF) Model" white paper.

> *"This paper proposes the Open Identity Trust Framework (OITF) model as a way to achieve the confidence needed to support the exchanges of identity information. The goal is to define a trust framework that reduces barriers and promotes trust so that individuals can conduct trusted transactions."*

Those were the early days of trying to define trust frameworks. Three years later in July 2013 a large group of members came together and formed a working group to develop "OIX Attribute Exchange (AX) Trust Framework Specification".

> *"The intent of the OIX Attribute Exchange (AX) Trust Framework specification is to enable what some call the "Identity Information Exchange Ecosystem." This is an ecosystem or marketplace that is interoperable, secure, and allows users to share reliable identity information with service providers who wish to utilize them. The objective is to provide a starting point from which a Community of Interest (COI) can organize participation from their constituency to customize and implement the business, legal, technical, privacy, certification and audit components of their AX Trust Framework specification."*

OIX then published a white paper "The Vocabulary of Identity Systems Liability" that seeks to explain the concept of liability, and to develop a common understanding of what it means for participants in an identity system to incur liability.

These and other relevant papers are published and available for download at www.openidentityexchange.org. This latest series of OIX white papers focused on trust systems, The Trust Framework Series, builds on the earlier work previously highlighted, all of it informing the LIGHTest project. OIX published the first paper in the series, "Trust Frameworks for Identity Systems" in June 2017.

In addition to the white papers, OIX launched the OIXnet Registry of identity systems in April 2015 that includes trust frameworks, trust schemes, certifications of conformance and other identity systems. It is the first registry developed by global leaders across industry sectors to better enable trusted online transactions at greater volumes and velocity. The trust frameworks and other identity systems registered at OIXnet informed the early inventory work within the LIGHTest project.

The goal of this OIX white paper is to continue to develop the early work done within OIX while amplifying the work being done within the LIGHTest project and its many partners.

What is the LIGHTest Project?

LIGHTest project to build a global trust infrastructure that enables electronic transactions in a wide variety of applications

An ever-increasing number of transactions are conducted virtually over the Internet. How can you be sure that the person making the transaction is who they say they are? The EU-funded project LIGHTest addresses this issue by creating a global trust infrastructure. It will provide a solution that allows one to distinguish legitimate identities from frauds. This is key in being able to bring an efficiency of electronic transactions to a wide application field ranging from simple verification of electronic signatures, over eProcurement, eJustice, eHealth, and law enforcement, up to the verification of trust in sensors and devices in the Internet of Things.

Traditionally, we often knew our business partners personally, which meant that impersonation and fraud were uncommon. Whether regarding the single European market place or on a Global scale, there is an increasing amount of electronic transactions that are becoming a part of peoples everyday lives, where decisions on establishing who is on the other end of the transaction is important. Clearly, it is necessary to have assistance from authorities to certify trustworthy electronic identities. This has already been done. For example, the EC and Member States have legally binding electronic signatures. But how can we query such authorities in a secure manner? With the current lack of a worldwide standard for publishing and querying trust information, this would be a prohibitively complex leading to verifiers having to deal with a high number of formats and protocols.

The EU-funded LIGHTest project attempts to solve this problem by building a global trust infrastructure where arbitrary authorities can publish their trust information. Setting up a global infrastructure is an ambitious objective; however, given the already existing infrastructure, organization, governance and security standards of the Internet Domain Name System, it is with confidence that this is possible. The EC and Member States can use this to publish lists of qualified trust services, as business registrars and authorities can in health, law enforcement and justice. In the private sector, this can be used to establish trust in inter-banking, international trade, shipping, business reputation and credit rating. Companies, administrations, and citizens can then use LIGHTest open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The three-year LIGHTest project started on September 1st, 2016, and has an estimated cost of almost 9 Million Euros. It is partially funded by the European Union's Horizon 2020 research and innovation programme under

G.A. No. 700321. The LIGHTest consortium consists of 14 partners from 9 European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond Europe, LIGHTest attempts to build up a global community based on international standards and open source software.

The partners are ATOS (ES), Time Lex (BE), Technische Universität Graz (AU),EEMA (BE), G&D (DE), Danmarks tekniske Universitet (DK), TUBITAK (TR), Universität Stuttgart (DE), Open Identity Exchange (GB), NLNet Labs (NL), CORREOS (ES), IBM Danmark (DK) and Globalsign (FI). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.

This white paper includes work that was contributed by the LIGHTest Consortium from D2.1, D2.2 and D2.3.

Definitions

For the purposes of this whitepaper, it is helpful to define key terms, as defined by the LIGHTest project, used in more detail in this paper.

Trust Lists: A trust list is defined as providing relevant attributes of enrolled entities and usually signed by an issuing authority with an electronic signature to prove their trustworthiness. Two main types of lists exist, Boolean and Ordinal: Boolean trust lists provide a value for each entity whereas an Ordinal trust list provides a level of assurance for each entity.

Trust Schemes: A trust scheme defines the organizational, regulatory, legal and technical measures to assert trust relevant attributes about enrolled entities in a given domain of trust. The two major trust schemes are authority and reputation based trust schemes.

Trust Frameworks: A “trust framework” is a term used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a group of participants bound by a contractual set of requirements.

Introduction to Trust Lists

Trust lists exist in a number of forms; from government trust lists to industry specific such as tScheme; trusts lists created by companies or even trust lists created by an individual. In its most simple form, a trust list is a list that contains all information that will allow for a verification to be deemed trusted. For trust to be built in a system, a trust path from a trusted root to the destination system is required. This usually happens by listing all trusted systems on a single list and requires a digital signature to trust the list. This signature will usually come from a key certificate that all other parties will trust.

A great example of this would be the eIDAS Regulation which requires EU Member States (MS) to publish a trust list of certain service providers established in their territory. Such service providers offer qualified services, such as issuing (and verifying) qualified signatures, eSeals, timestamping and electronic registered delivery or other services that the member state chooses to include on a voluntary basis.

LIGHTest offers the opportunity to better organize and simplify the process of using disparate trust lists which are located in numerous locations. It will allow someone who is trying to undertake a secure transaction to make a decision about who they are transacting with and whether the source they are using is trustworthy.

Government Trust Lists

Existing EU Trusted Lists and EU Member States Trust Lists

Regulation (EC) No 910/2014/EU Article 22 (eIDAS Regulation) provides the obligation for EU MS to provide trust lists. This includes the processes of establishing, maintaining and publishing trusted lists. The EU MS has to provide information about the qualified Trust Services Provider (TSP) as well as information about the trust services provided by the TSP. Article 22 also provides the obligation that the publication of trust lists happens in a secure manner, which means electronically signed or sealed, and that the trust lists are suitable for automated processing.

This regulation has a constitutive effect. A trust service provider and the services it provides is only qualified if it appears in the trusted list. Consequently, citizens, businesses or public administrations, in general the users, will benefit from the legal effect associated with a given qualified trust service only if it is listed as a qualified service in the trusted lists.

EU MS may add additional trust services other than the qualified ones. This happens on a voluntary basis and on a national level. This entry must clearly indicate that the provider is not qualified according to Regulation (EU) No 910/2014) (Regulation, 2014).

To allow access to the trusted lists of all EU MS, the EC makes trusted lists available for the public as a list of trusted lists. This happens via a secure channel to an authenticated web server. This list of trusted lists is also signed or sealed and suitable for further automated processing.

Industry Trust Lists

There are a number of trust lists that are used by the industry and are interesting for LIGHTest to examine. Below is a description of the trust lists, their purpose and functionality as well as descriptions of the trust schemes that are registered on the trust lists (where available) for the purpose of showing how these trust lists are being used in practice and applied in organizations.

OIXnet

An official online and publicly accessible repository of documents and information relating to identity systems and identity system participants. OIXnet lists worldwide available trust frameworks and registered whitelists and functions as an official and centralized source of documents and information, much like a government-operated recorder of deeds. The purpose of OIXnet is to provide a neutral, authoritative registry of trust information to enable interoperability of identity systems and participants. OIXnet is a registry of registries which differs from other trust lists and aims to provide in one central location, all information related to multiple registrations. Other registries that are in operation generally have limited types of registration with respect to a particular identity.

OIXnet is relevant for trust translation across jurisdiction as a neutral, global platform accessible by anyone at any time with no cost associated; it helps provide the necessary transparency required for trust. It also helps the discovery, authentication and assessment of the trustworthiness of foreign certificates and other artefacts that verifiers need to know when determining which foreign trust schemes to accept and how these map to the trust schemes of a given local jurisdiction.

LIGHTest will be complimentary and not competitive to the Trust Frameworks that are registered at OIXnet. LIGHTest is intended to be cross industry and global, like many of the Trust Frameworks registered, but others are industry and jurisdictionally specific. Communities of interest determine the applicability of a given trust framework and so indicate in its terms of reference.

IDEF Identity Ecosystem Framework Registry

(IDESG, 2016) has been created by the Identity Ecosystem Steering Group (IDESG) for organizations who are interested in independently assisting their own identity management standards against a common set of criteria found in the IDEF. The criteria used are: reliable security, privacy, ease of use, costs savings and user choice. These are taken from the NSTIC Guiding Principles (IDEF, 2016).

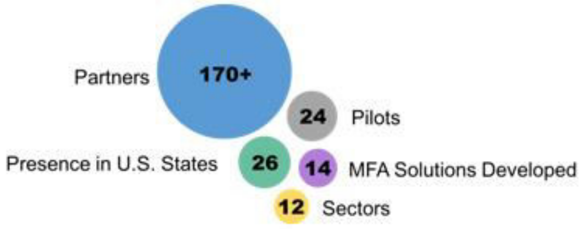


Figure from Imperial Valley website looking at Innovation in the Identity Ecosystem 2016

According to an article in Imperial Valley News (2016 Year in Review: (TIG-ing stock of) Innovation in the Identity Ecosystem, 2016) the introduction of the IDESG's registry has impacted more than 6.7 million individuals across 12 sectors up until September 30 2016.

Kantara Trust Registry

The Kantara Initiative covers: Connected Life (Internet of Things), and Trust Services. Kantara's initiatives include: Identity Relationship Management, User Managed Access, Identities of Things, and Minimum Viable Consent Receipt. This Trust Framework Provider is aligned with the US NSTIC program and looks to approve Credential Service Providers (CSPs) and Accredits Assessors. All those who are approved will be listed on the KTR Trust Status List.

CAB (CA/Browser) Forum

The CAB forum is a voluntary group of Certification Authorities (CAs), vendors of Internet Browser software and suppliers of other applications that use digital certificates for SSL/TLS and code signing. Internet users wanted greater assurance about the websites they were visiting, so the group was formed to leverage the capabilities of SSL/TLS certificates.

As stated on the CAB Forum website, the CAB Forum has adopted version 1.0 of the Extended Validation (EV) Guidelines. EV certificates are issued after extended steps to verify the identity of the entity behind the domain receiving the certificate. Following the publication of the EV Guidelines they have adopted these guidelines for issuing code signing certificates and Baseline Requirements for the Issuance and Management of Publicly-Trusted SSL/TLS Certificates to improve accreditation and approval schemes for all applicants who request that their self-signed root certificates be embedded as trust anchors in software and to extend common standards for issuing SSL/TLS certificates beyond EV to include all Domain-validated (DV) and Organization-Validated (OV) certificates. A list of CAB certification authorities can be found in Appendix Five.

Introduction to Trust Schemes

A trust scheme comprises the organizational, regulatory, legal and technical measures to assert trust relevant attributes about enrolled entities in a given domain of trust. A trust scheme operates in a given trust domain and typically has a declared or implied purpose. The two major types of trust schemes are authority based and reputation based trust schemes.

Authority based trust schemes: An authority issues regulations and conditions that are necessary to certify attributes. A trust scheme may use supervision to ascertain that an entity complies with all conditions and regulations. If the entity complies with the conditions and regulations, it is part of the trust scheme data. Otherwise, the authority can remove it from the trust scheme data.

Reputation based trust schemes: A trusted party collects and publishes reputation data on entities and assembles the data into the trust scheme data.

Current Trust Schemes

tScheme

tScheme is an independent, industry-led and self-regulatory scheme which uses strict assessment criteria to approve trust services. tScheme itself does not run trust schemes or trust frameworks, its role is to define profiles for such schemes against which organizations can be independently assessed by a UKAS assessor.

As *tScheme* has such strict criteria, it provides a level of assurance to individuals and businesses who are using or relying upon e-business transactions. Due to this commitment to industry-led self-regulation rather than government-led legislation, tScheme is proving popular across Europe, and their objective is to continue to be the preferred option for fulfilling Part I of the UK's Electronic Communications Act 2000.

tScheme works with a number of different organizations such as:

- Schemes (trust frameworks) Authorities
  - organizations or groups of organizations seeking the development of a specific set of profiles or the addition of an auditable specification to an existing set of profiles to support one or more trust schemes they wish to operate and have any participant independently assessed with approved UKAS tScheme Assessors. For example, GOV.UK Verify
- Applicants
  - organizations who seek to become approved to operate under one or more schemes. They are charged an applicant fee and such organizations need to be assessed by an independent UKAS approved tScheme assessor. Organizations included: Verizon, Experian, Digidentity, BT
- Independent Assessors
  - Organizations who employ assessors to undertake audit and inspection of Applicants under one or more schemes for example KPMG, LRQA.
- tScheme Members

- organizations who are committed to delivering trust based services and see the value in supporting tScheme as an entity, operate and develop an independent approvals body.   Example members of tScheme are Mydex, BT, Experian, Payments UK, Cabinet Office

A Typical tScheme Use-Case:

The Cabinet Office runs a service called GOV.UK Verify that is used by government departments. Those government service providers rely on Identity Providers (IDP) who carry out a process of identity assurance to ensure that the relying party knows that the person visiting their digital front door to access a service is the person they claim to be.

The Identity Providers are subject to approval under the "Verify Scheme" which defines ways they must operate. Within the Verify Scheme organizations are required to get tScheme approval for delivering services against specific Profiles in accordance with a rule book from the scheme called GPG45.

- Base Approval Profile tSd0111 3.00
- Approval Profile for Identity Registration Services tSd0108 2.06
- Approval Profile for an Identity Provider tSd0112 1.00
- Approval Profile for Credential Management Services tSd0113 1.00

To get approved the identity provider must go through the process of being an approved applicant, producing a series of documents and then being independently assessed by a UKAS approved assessor who then writes a report which is submitted to the tScheme approvals The final decision to allow them go live is with the GDS who are the Verify Scheme Authority.

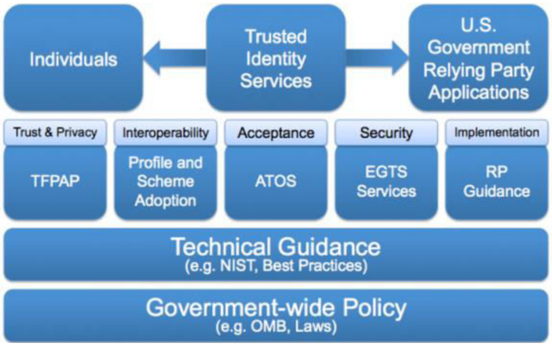
Introduction to Trust Frameworks

A trust framework legally binds participating entities in its identity system with role-specific sets of duties and liabilities. These will apply to the services offered by a participating entity within the context of the trust framework. The articulation typically takes a contractual form when the scope of the trust framework is in the private domain. In other domains such as government, the trust framework could also be in regulatory or statutory form (Esther Makaay, March, 2017).

Government Trust Frameworks

Outside of Europe, the US has a couple of Trust Frameworks, FICAM and National Institute of Standards and Technology (NIST). FICAM Trust Framework Solutions is the federated identity framework for the U.S. federal government and includes processes and supporting infrastructure to enable secure citizen and business facing online service delivery.

The NIST have created the Trust Identities Group (TIG) which is aiming to facilitate a private sector-led implementation approach to trusted digital identity solutions enabling government adoption by evolving risk-based federal guidance.



This diagram highlights the FICAM Trust Framework structure.

Industry Trust Frameworks

Minors Trust Framework

General Description

Working in conjunction with the National Strategy for Trusted Identities in Cyberspace (NSTIC), the MTF (Privo, 2016) is a White House initiative aimed at helping individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice and innovation.

How the framework is being used practically

Under COPPA, every time a child wants to access an online service that they want to interact with, their parent must separately fill in each consent request. This is obviously time consuming and a burden for parents and also the online service provider. Research has shown that less than 1 in 10 consent requests are acted upon, which has obvious knock on effects to the service providers. A big problem is when children lie about their age in order to access online services as this puts children at risk and the service providers could run afoul of COPPA.

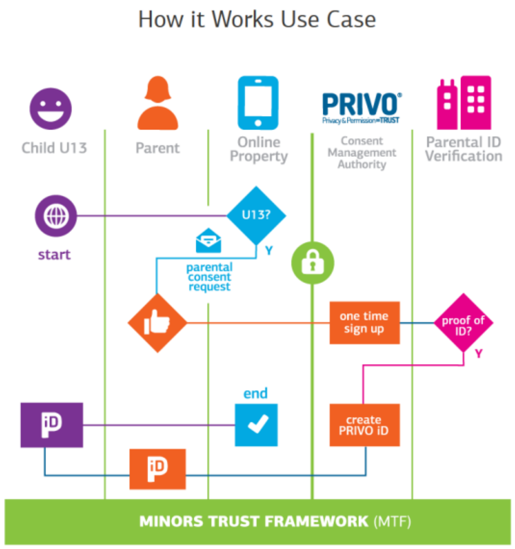


Diagram showing how the Minor's Trust Framework works

The aim of the MTF is to allow credential service providers (CSPs) to create an online credential for parents and children that can be used by other online service providers. All CSPs agree to standards of privacy and security under the Federation. It is free and simple to use and the parents only need to have their identity verified once by an Identity Provider. Once accepted, parents can then pre-consent to their child's access to other Federation approved online services. The children benefit from being able to interact online in a safe and privacy secure manner.

Technical description

The MTF enables Credential Service Providers that issue a Child-unique pseudonymous identifier to interoperate and interact with RPs and other Members.

When someone attempts to access a protected service provider site, an Identity Provider is asked to provide 'identity attributes' to the service provider. Attributes could be a user ID, organizational affiliation status, email address etc. The Federation encourages the support of identity attributes by its participants to improve the COPPA consent process and to help protect personal privacy. The Federation provides the parent with a unique identifier/relationship link and tools to manage multiple consents, notifications, and associations.

Parents can view their child's data and permissions across all the multiple sites and manage this. However, Federation members are prohibited from assisting each other in tracking either Children or Parents by both MTF policy and technical enforcement due to the use of unique globally unique identifier (GUID). Credential holders are encouraged to have unique display names available at the online service level. CSPs and CMAs are permitted to maintain information about a user on multiple venues in order to support the use of federated credentials and consent.

Once the minor reaches an age where they are no longer under COPPA protection, the parent can transfer control of the parent-authorized credential to the minor. Minor's rights to control their credential will be determined by relevant law and the issuing CSP/RP Terms of Service or EULA, and may be viewable from the CMA's parent portal.

Mydex Trust Framework

General Description

The Mydex Trust Framework delivers a trusted digital identity via a secure personal data store and platform where individuals are able to connect to each other and organizations, allowing for and exchange of information in a secure and verified manner.

How the framework is being used practically

The Mydex Trust Framework gives individuals a trusted identity and digital letterbox that they can use online. For organizations, they can operate with large savings in distribution and identity verification costs. Individuals have more control over their data and can share and transact easily online without having to remember multiple usernames and passwords which creates higher levels of risk.

There is a standard data sharing agreement which takes into account the specific types of data that will be shared and how it will be used, with the individual being in control of the permission process. This allows individuals to engage with organizations in a more secure, flexible and convenient manner.

Technical Description

The Mydex Trust Framework works with an open API allowing all service providers and application developers signed up to the framework, to offer value. This way of working creates an environment of innovation and allows for new forms of engagement to develop between organizations and individuals.

The Respect Trust Framework

General Description

This was the first digital trust framework that was designed to create a mutual trust network for sharing private data safely between businesses and individuals online.

The Respect Trust Framework is designed to be self-reinforcing through use of a peer-to-peer reputation system called the Respect Reputation System™. The Respect Reputation System is based on peer-to-peer connections between Respect Network members and includes both positive reputation, called Vouching, and negative reputation, called Complaints.

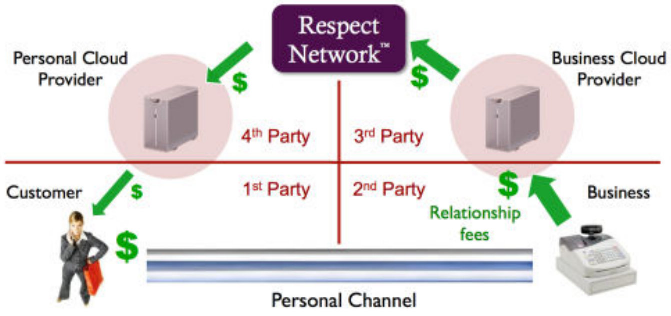


Diagram showing the Personal Channel of the Respect Network.

How the framework is being used in practice

The Respect Trust Framework has a set of five universal principles that govern the protection of identity and personal data: a promise of permission, protection, portability, and proof.

The framework has a network-wide reputation system with four levels of trust as the enforcement mechanism for compliance with the trust framework. This form of self-regulation is intended to ensure that members 'do the right thing' with regards personal data and communications.

Any sub community that requires more specific trust rules can use all the benefits of the Respect Trust Framework and the Respect Reputation System and add their own rules and regulations which apply to their own subnetwork. These communities could include a financial services network, a health information exchange or a social network.

Technical Description

The Respect Network uses the same four-party business model as the credit card networks. Instead of money, it is an exchange of information controlled by the customer. The exchange is directly between the customer's own personal cloud and the business's cloud over a customer controlled communications connection called a personal channel.

Businesses on the Respect Network pay relationship fees which are based on the value of a customer relationship facilitated by the network. According to the Respect Network site, value components include:

- The value of the intimate customer profile, preference, and intention data that a customer is willing to share over a trusted, customer-controlled channel.
- The value of the bi-directional trusted messaging that can flow over the personal channel.
- The value of the automated event processing handled by the channel
- The customer acquisition and retention value of the channel.

This model is called "Relationship-as-a-Service" because a business is outsourcing an extension of its own CRM system directly to the customer. This form of customer-managed relationships is called VRM (Vendor Relationship Management).

SecureKey Concierge™ Canada Trust Framework

General Description

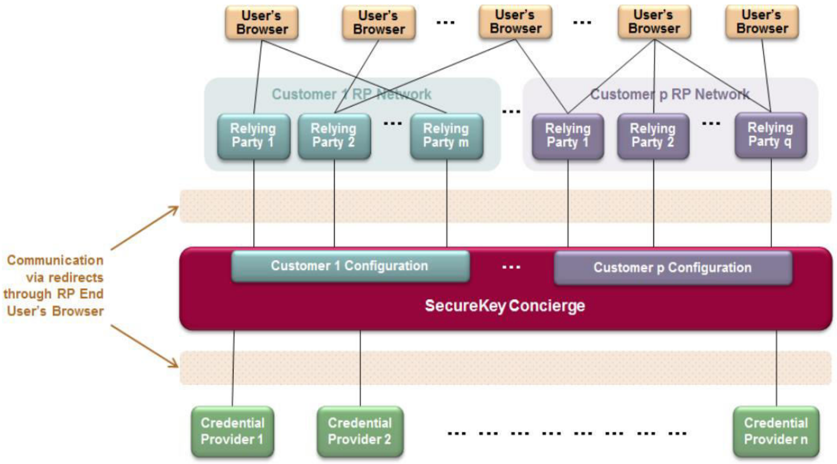


Diagram of the SecureKey Concierge architecture.

The SecureKey Concierge (SecureKey, SecureKey Concierge, 2016) service is a cloud-based, Relying Party (RP) and Credential Provider (CP) neutral, online authentication service that enhances the security of online authentication transactions between Users and Relying Parties (RPs) through a network of trusted Credential Providers (CPs).

How the framework is being used practically

SecureKey Concierge uses a set of standards and technology to formalize the participation of its users through contractual relationships. The governance structure ensures that the ecosystem continually develops and enhances.

Users are able to sign in to Government of Canada services using their profile from their financial institution, bank or credit card instead of a username and password.

Technical description

Of particular importance to this scheme was that the underlying platform would have privacy built in. Therefore, they have developed Meaningless But Unique Identifiers and Persistent Anonymous Identifiers. The SecureKey Concierge also uses a triple-blind privacy model where RPs are blind to the user's selected CP, CPs are blind to the RP the user is accessing and SecureKey has no access to the user's personal identifiable information.

Nate Blue Button for Consumers Trust Bundle (NBB4C)

General Description

The NBB4C works by using trust anchors of consumer-facing applications (CFAs) that securely move data from one application to another. Patients benefit from having access to their health information whilst relying parties can identify CFAs that meet or exceed the criteria of a trustworthy steward of consumer health information.

How the framework is being used practically

The NBB4C website (NATE, 2016) states that those who participate in NBB4C have a secure exchange of health information from provider-controlled applications to consumer-controlled applications. This could include personal health records and will use direct secure messaging protocols. If a provider organization wishes to send messages to consumers using one of the recognized applications, they can load this bundle into their trust stores. In most cases, CFAs that are on boarded to the NBB4C have loaded publicly recognized trust bundles of provider facing applications and Direct Secure messaging should be enabled.

Technical Description

NATE uses trust bundles as a way to establish trust among the participating organizations and enables sharing of health information securely. On the NATE website (NATE, 2016) it states "Each Trust Bundle includes the trust anchors of organizations that have elected to adopt a common set of policies and practices corresponding to a specific health information exchange or purpose".

According to the NBB4C website consumer facing organizations that have completed the NBB4C onboarding include: Carebox Healthcare Solutions, GetRealHealth, Humetrix, iShare Medical, Medical Informatics Engineering, MedYear, Microsoft and Omedix.

ID.me

General description

The ID.me service provides end-to-end identity proofing and credential management service for veterans across North America, first responders, and members of other designated groups. The digital ID card allows for a single sign-on technical to verify their identities remotely, for online transactions, which doesn't expose their personal identifiable information.

This service allows individuals to bind specific characteristic attributes to their primary identity, enabling them to gain a broad range of customized services and benefits across multiple sectors.

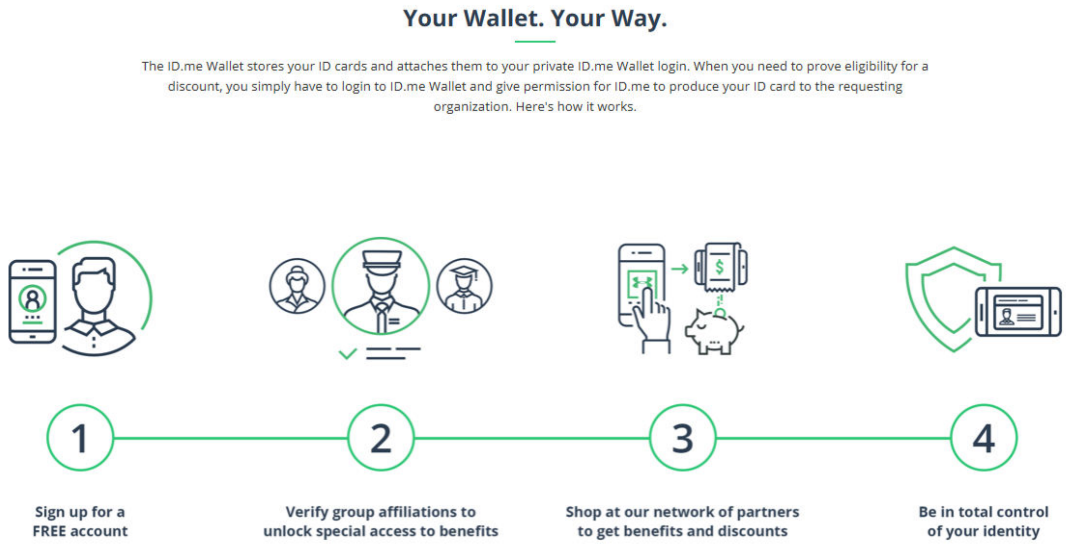
How this framework is being used practically

As an example, this scheme is being used by military personal, both active and veterans, to allow them to verify their military credentials at a number of retail partners and government agencies. This allows them to get discounts at various retailers without having to show their social security number.

Technical description

ID.me issues password-based single and multi-factor credentials across Assurance Levels 1, 2 and 3. To enroll, consumers apply through the ID.me website, fill in some of their personal information such as name and zip code, and then fill in a secret field that varies according to the organization and benefit value. For example, in a military context this could be a full or partial social security number. In the back-end, ID.me then compares the applicant's information with authoritative databases such as a bank or university. Any organization that uses the technology to prevent fraud is charged up to $1 for the verification response.

ID.me uses SAML protocol to return a response from government agencies. To ensure the security of all sensitive information, ID.me uses RSA 2048 encryption for data in transit and AES 256-bit encryption for data at rest.



Your Wallet. Your Way.

The ID.me Wallet stores your ID cards and attaches them to your private ID.me Wallet login. When you need to prove eligibility for a discount, you simply have to login to ID.me Wallet and give permission for ID.me to produce your ID card to the requesting organization. Here's how it works.

1 Sign up for a FREE account

2 Verify group affiliations to unlock special access to benefits

3 Shop at our network of partners to get benefits and discounts

4 Be in total control of your identity

Diagram demonstrating the ID.me process.

Pan Canadian Trust Framework (PCTF)

General Description

The PCTF launched in September 2016 and is not yet operational, however there are lessons that can be learnt from their policy frameworks and as of January 2017, the private and public sector in Canada are heavily involved.

The PCTF is a collaborative initiative of the public and private sectors and has been developed through collaborating with the Digital ID and Authentication Council of Canada (DIACC) and the Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada. The PCTF will be applied across industries and subject to the laws and regulations of Canada. The idea is to allow PCTF to enable an ecosystem of trusted services as a foundation for digital interactions.

How the framework will be used practically

The PCTF is designed to allow digital identification, online credential, electronic authentication and authorization systems to provide services to government, citizens and businesses. Stakeholders will include: federal and provincial governments, financial institutions, telecoms and identity networks.

TeX from Tax Incentivised Savings Association (TISA)

TeX is a contract club with a single agreed set of SLAs that is backed and funded by all major platforms, asset managers and service managers. Their membership covers over 95% of all UK Platform AUA and 90% of all UK Fund Manager AUM.

Background

In 2010, the Retail Distribution Review stated that platforms had to allow re-registration of their platform. This was a challenge as at that time, re-registrations were manual and paper-based which meant it was slow, people-heavy as well as expensive and prone to error.

The Solution

It was agreed that if there was one central contract that laid out all the various liabilities and responsibilities of each party, established a dispute resolution and a set of service level agreements, then all firms could sign up to that one set of contract terms. TeX was therefore established to manage that contract and maintain a register of firms who had signed up it and control the compliance issues.

Example Use-Cases of LIGHTest Across Public Sector, Private Sector and Government

Globally there are a wide variety of different certifications available. These could be training certificates, other forms of non-government education, government certificates (birth certificates, tax certificates). These wide varying certifications may be country specific, or even specific to a certain domain. With an abundance of fake certificates, and also fake certification authorities, it can pose difficult to determine which is real and which isn't. LIGHTest could prove valuable to not only ensure trust in those certifications but also translate those certifications between different countries and domains. While there are a wide variety of different use cases that LIGHTest could be applied to, the LIGHTest project will be implementing two pilots within the duration of the project; the eProcurement Pilot led by IBM and a Trustworthy Communications Pilot led by Correos.

The following section provides prospective use cases that could be implemented in future versions of the LIGHTest infrastructure.

Public Sector Cross-Government Official Communications

A general use case that could affect many expats or travellers, would be the optimization of being able to conduct stronger cross-government official communications. For instance, the LIGHTest Infrastructure could provide a tool that could be used to verify international communications sent within the EU, across state borders in the USA, or across general country borders in a global scale. Examples of what official communications could be included are: traffic violations, health notifications, etc.

Public Sector Trusted Open (Government) Data

Governments are increasingly publishing data collected and/or processed in open formats, to be used by industry, communities or other government entities. LIGHTest could be used to ensure the integrity (and authenticity) of the published data, even across borders. The LIGHTest tool could be used in the sense of verifying different Governmental Data, such as, a valid driver's license, health insurance, a university diploma, etc.

Public Sector LIGHTest-eSENS-e-Health Use Cases

A specific use case to how LIGHTest could optimize e-Health, would be to work with the e-SENS e-Confirmation domain use case. The e-SENS e-Confirmation domain use case consists of the cross-border issuance and verification of a Provisional Replacement Certificate for a patient who applies to a medical facility in need of medical treatment. For instance, there could be a check of what is covered by the Health Insurance from Germany for a certain procedure that is done in the France. Further, e-SENS has another use case for e-Health that regards e-Prescription, which would allow the process of executing a prescription that was given in Germany in Spain, where Spain could decide the translation of the prescription and the verification process of the Prescription. The translation and verification process, could be conducted with the LIGHTest Infrastructure.

Shipping Insurance and Other Shipping Documentation

With regards to the shipping industry, LIGHTest could assist in the process verifying shipping insurance. Specifically when it comes to container insurance, which needs a variety of different insurances and other forms of documentation in order to ship to different ports worldwide. For instance, one could check each container and see who it was insured by, where it is shipping from, when, and other information. It could make use of lists, such as, Lloyds List of Intelligence service and others.

Private Sector: Trust Services for the Credit Card Industry

The credit cards industry was built up on a contractual basis by the banking industry, which also built its global infrastructure for it. LIGHTest can be effectively promoted as a flexible infrastructure to validate the communications between the business partners in a cross-border environment and validate trust in credit card transactions. The various trust services involved in this use case would be the eID, eSignature, eSeal, eTimestamp, Web certificates.

Opening a Bank Account in a Country that You are Moving to for Work

Delivery of services that require data flows across multiple legal jurisdictions can be difficult for private sector companies. People today live international lives, often working or being educated across national borders. Opening a bank account in another country can be difficult and slow and users would need to assert trustworthy data about themselves to support an application for a new financial service. Where additional data is required by the financial institute, with the users consent and control to enable an account to be opened in line with regulatory obligations, LIGHTest may be able to help with this cross border verification. This fits into the 'Supporting Trust Services' scope of the project.

Conclusion

This whitepaper is just a subset of the many trust schemes and lists from the LIGHTest deliverable, of which we have selected just a few to use as examples. The full deliverable produced by LIGHTest has a more extensive list and also covers existing device attestation schemes, relevant delegation schemes, trust policies and policy languages as well as best practices of interaction design. The LIGHTest full deliverable can be found here: http://lightest.eu/downloads/pub_deliverables/

The use cases have also been added to show how LIGHTest could potentially be applied in real life scenarios. A wider spectrum of use cases for the LIGHTest Infrastructure was established in a project deliverable, the spectrum ranges across private, public, and non-governmental sectors. It provides use cases on other trending topics of Internet of things and Predictive Maintenance.

OIX UK's involvement in the LIGHTest project along with the development of this white paper highlights that the syncing of definitions and concepts across global identity initiatives continues to be a challenge. Without a common vocabulary, interoperability is a challenge. OIX sees this challenge as an opportunity and is planning a white paper in 2018 that will map definitions and concepts in an effort to form a consensus.

Appendices

Appendix One: Introduction to LIGHTest

The central objective of LIGHTest is to create the tools to use a global trusted communications mechanism – the DNS – for the discovery, validation and translation of certain trust information. This trust information in the context of LIGHTest principally relates to trust policies, i.e., a recipe that takes an electronic transaction and potentially multiple trust schemes, trust translation schemes and delegation schemes as input and creates a single Boolean value (trusted [y/n]) and optionally an explanation (e.g., why not trusted) as output (source: D2.1 – Inventories). Broken down to the simplest terms, a trust policy contains the rules to make a decision on whether a transaction can be trusted or not.

Trust schemes and trust decisions can take many forms and cover many topics, and the legal framework that applies to these – including the liberty that parties have for making a trust decision – can vary from case to case. To give a few examples:

- A relatively simple trust decision that LIGHTest will support is validating whether a trust service provider (i.e. the provider of services in relation to electronic signatures, electronic seals, time stamps, electronic registered delivery services, or website authentication) complies with the legal rules of the eIDAS Regulation, and more specifically whether the service providers are qualified or not. The rules (and indeed the entire trust scheme) in relation to this decision are captured in law, notably in the eIDAS Regulation (EU) No 910/2014[1]. The trust policy is therefore simple, and consists of the rules of the eIDAS Regulation which act as the trust scheme. The trust decision is correspondingly simple, and consists of an assessment whether the provider complies with the requirements of the eIDAS Regulation (which are explained in D2.10 in greater detail). The law (namely the eIDAS Regulation) is relatively comprehensive on this point, and the decision is a relatively straightforward yes/no decision: a provider complies or it does not. No notable margin of appreciation exists.
- In realistic cases, business decisions can be much more complex. If a company receives an electronically signed document – e.g., an order for a product or service – it can create its own rules (its own trust scheme) on how it will assess the validity of these orders. These rules constitute the trust scheme, and the resulting decision – do I accept the order or not? – is the trust decision. The presence of an electronic signature and whether it complies with the eIDAS Regulation can be a factor. Other elements may be whether the customer is known, the size of the order, its place of establishment, etc. Laws do not answer all of these questions: while there are rules on what constitutes a lawful order, individual preferences and choices can play a role. Indeed, a company may simply have a rule that it doesn't accept electronic orders at all, for whatever reason, or that it only accepts electronic orders which are signed using signatures from a local trust service provider. Such policies (and the resulting trust decisions) may be objectively irrational or illogical, but none the less they can exist.
- Finally, there are cases where trust policies and trust decisions are entirely determined by the participants in a transaction or business relationship, without any significant impact from legislation. By way of example, a European trade association may have its own internal rules on which companies are

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

permitted to join. These are likely to include rules on business activities, place of establishment or business, membership fees, and adherence to codes of conduct. The trade association may decide to publish membership, so that its members can make trust decisions on that basis (do I know that this company is indeed a member of this trade association)? The rules of membership are then the relevant trust policy, and the members can take their own trust decisions on the basis of the information made available by the trade association – which may or may not be covered by any legal assurances from the trade association, depending on its own trust policies.

The examples above serve to make a central challenge clear: LIGHTest is a technology that can be applied to a nearly unlimited range of use cases, with vastly diverging legal and policy challenges. In these situations, there is no 'one-size-fits-all' approach that ensures that the technology is automatically compliant with legal requirements and with the trust policies that parties may have defined on a case-by-case basis.

The same observation applies also to the topic of delegation, which can exist in many shapes and forms, which are subject to different legal requirements. One need only consider a contractual delegation to go shopping for groceries on behalf of a person, to buy a house on behalf of that person, or to vote in national elections on behalf of that person. Depending on the context and country, the delegation may be simple and straightforward – an oral agreement suffices – or highly complicated, requiring signatures from both parties which are certified and registered by a trusted third party. In other contexts, it may not even be possible to issue a legally valid delegation at all (e.g. giving a mandate to vote to a person who is not qualified).

LIGHTest aims to use the same infrastructure as a model for the discovery and validation of all such delegations. This implies that LIGHTest cannot ensure that trust decisions made using LIGHTest technology are automatically legally valid without any further customisation or tailoring to the challenges of each use case, in the same way that a word processor also cannot ensure that a contract written through the software is legally valid. The technology itself cannot ensure legal validity; it must be used in a way that complies with legal constraints. The technology can support this, but ultimately a broader legal superstructure is needed, in the form of contracts and policies that are tailored to each specific use case.

LIGHTest's approach to legal compliance and legal validity is therefore based on ensuring transparency to its users (i.e. those that publish trust schemes, those that conduct trust translations or verify delegations, and those that make trust decisions on the basis of the policies), and providing a set of standardised legal tools to ensure that LIGHTest can indeed be deployed in specific use cases with appropriate consideration for their individual specificities.

To find out more about LIGHTest and join the community, please visit www.lightest-community.org

Appendix Two: Digital Signatures vs. Electronic Signatures

Digital signatures are a sub-group of electronic signatures providing the highest level of security and universal acceptance so they cannot be copied or tampered with. Digital signatures are based on Public Key Infrastructure technology and the only signature standard which is accepted by governments around the world. The use of cryptographic operations mean that a digital signature creates a ‘fingerprint’ unique to both the signer and the content. To verify a digital signature, a trust anchor will be used which acts as authoritative entry via public key and associated data and uses a public key to verify the signature. A trust anchor needs to be transparent, independent, provide basic management operations and security measures.

Electronic signatures are based on proprietary formats that may use a digitized image of a handwritten signature, symbol or voiceprint to identify the author of an electronic document. They are legally enforceable but they are vulnerable to copying and tampering and require proprietary software for validation. Hence the law below requiring electronic validation services. Electronic

To enroll in a trust scheme, the digital signature must meet certain requirements otherwise it will not be as legally valid in the same way a handwritten signature would be. Globally there are a number of laws related to digital and electronic signatures such as the Electronic Signature Law of the People’s Republic of China (LINK). For a full list of all countries and their Digital and Electronic Signature Laws, please visit DocuSign’s eSignature Legality guide.

Appendix Three: Definitions

Entity	An entity is a person, organization, or thing enrolled in a trust scheme.
Trust Domain	A trust domain defines a set of entities that are eligible to enroll in a scheme and describes the trust relevant aspects of the enrolled entities. A typical way to define such a set for a trust domain is the use of constraints.
Trust Scheme Authority	A trust scheme authority manages multiple trust schemes. The trust scheme authority may delegate the management to sub authorities.
Trust List	Provides relevant attributes of enrolled entities. A trust list provides relevant attributes of enrolled entities. A trust lists is usually signed by an issuing authority with an electronic signature to prove their trustworthiness. Different types of trust lists do exist. For example, a boolean trust list provides a boolean value for each entity. An entity can either be trusted or not trusted. As another example, an ordinal trust list provides an ordinal value for each entity. Typically, typical value for an ordinal value is a Level of Assurance (LoA).
Trust Scheme	A trust scheme comprises the organizational, regulatory, legal and technical measures to assert trust relevant attributes about enrolled entities in a given domain of trust. A trust scheme operates in a given trust domain and typically has a declared or implied purpose. The two major types of trust schemes are authority based and reputation based trust schemes. • Authority based trust schemes: An authority issues regulations and conditions that are necessary to certify attributes. A trust scheme may use supervision to ascertain that an entity complies with all conditions and regulations. If the entity complies with the conditions and regulations, it is part of the trust scheme data. Otherwise, it the authority can remove it from the trust scheme data.

	• Reputation based trust schemes: A trusted party collects and publishes reputation data on entities and assembles the data into the trust scheme data.
Trust Scheme Data	Trust scheme data represents the current content of a trust scheme. It is a data set managed by the trust scheme authority and contains information on the status of an entity.
Trust Scheme Publication	A trust scheme publication makes the trust scheme data available to verifiers either as complete or a subset of the trust scheme data. A trust scheme publication may contain different aspects of the trust scheme data including (from least to most accurate trust scheme publication mechanism) • Historical publications: Include the full set of change events and make it possible to determine the status of the trust scheme data at different positions in time. • Snapshot publications: Report the status of the trust scheme data at a given point in time. • Sampled publications: Report the state of the trust scheme data at the point of time when it was last queried. • Real time publications: Report the state of the trust scheme data at the point of time of a query. The LIGHTest infrastructure supports two trust scheme publications: Sampled and real time publications.
Boolean Trust Scheme Publications	Boolean trust scheme publications are defined as: • entityID -> Boolean Instead of explicitly stating the boolean value, every entity listed in a publication has the same boolean value. Trusted (true) in the case of white lists and untrusted (false) in case of black lists.
Ordinal Trust Scheme Publications	Ordinal trust scheme publication are defined as • entityID -> Ordinal value An ordinal value describes a certain Level of Assurance. It is seen as a reputation rating for the entity. Examples for ordinal values are [low, medium, high], [level1, level2, level3, level4], or [0-stars, 1-star, 2-stars, 3-stars, 4-stars, 5-stars]. Every entity listed in a publication is assigned to an ordinal value. Entities listed in a publication may have different ordinal values. Note that boolean turst scheme publications are a special case of ordinal trust scheme publications.
Generic Trust Scheme Publications	Generic trust scheme publication is defined as • entityID -> tuple of attributes A generic trust scheme contains a tuple of attributes for an entity. An attribute can be an LoA, date of foundation, legal form, social capital, etc. Note that boolean and ordinal trust scheme publications are a special case of generic trust scheme publications.

Appendix Four: Table of Acronyms

AVANTSSAR	(EU project) Automated Validation of Trust and Security of Service oriented Architectures
A2A	Administration to Administration
A2B	Administration to Business
A2C	Administration to Citizen
AdESeal	Advanced Electronic Seal
AdESig	Advanced Electronic Signature
AdES	Advanced Electronic Signature covers AdESig, AdESeal, and AdEStamp
AdESQC	Advanced Electronic Signature supported by a Qualified Certificate
AdEStamp	Advanced Electronic Stamp
AES	Advanced Encryption Standard
ANSSI	*Agence nationale de la sécurité des ystems d'information* (in English: National Cybersecurity Agency of France
AQAA	Attribute Quality Authentication Assurance
BMBF	Bundesministerium für Bildung und Forschung (German Federal Ministry for Eductation and Research)
BAN-logic	Burrows Abadi Needham
B2A	Business to Administration
CA	Certification Authority
CEHRT	Certified Electronic Health Record Technology
COPPA	Children's Online Private Protection Act
C2A	Citizen to Administration
C2C	Citizen to Citizen
CAdES	CMS Advanced Electronic Signature
CID	Commission Implementing Decision
CEF	Connecting Europe Facility
CFA	Consumer Facing Applications
CP	Credential Provider
CSP	Credential Service Provider
CROBIES	Cross-Border Interoperability of eSignatures project
CMS	Crytographic Message Syntax
CRM	Customer Relationship Management
DPC	Derived PIV Credential
DL	Description Logic
DIACC	Digital Identification & Authentication Council of Canada
DAA	Direct Anonymus Attestation
DV	Domain Validated
ESSI	Electronic Exchange of Social Security Information
EHR	Electronic Health Record
eIDAS	Electronic IDentification And Signature
eID	Electronic IDentity
eTS	Electronic Trust Services
EC	European Commission
CEN	European Committee for Standardisation
EN	European Norm

ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
EVCP	Extended Validation Certificate Policy
XACML	eXtensible Access Control Markup Language
FIDO	Fast Identity Online
FBCA	Federal Bridge Certification Authority
FICAM	Federal Identity, Credential and Access
FIPS	Federal Information Processing Standard
FP	Fixedpoint
GSMA	Global System for Mobile Communications Association
HWAT	Hardware Based Device Attestation
HIE	Health Information Exchange
HISP	Health Information Systems Program
ID	Identity
IaaS	Identity as a Service
IDEF	Identity Ecosystem Framework Registry
IMSC	Identity Management Sub-Committee
IdP	Identity Provider
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union (United Nations)
IETF	Internet Engineering Task Force
KTR	Kantara Trust Registry
LoA	Level of Assurance
MTF	Minors Trust Framework
MNO	Mobile Network Operator
MOA	Modules for Online Applications
MS	Member State
NBB4C	Nate Blue Button for Consumers Trust Bundle
NIST	National Institute of Standards and Technology
NSTIC	National Strategy for Trusted Identities in Cyberspace
NFC	Nearfield Communication
nPA	Neuer Personalausweis (German eID card)
NPE	non-person entity
NSL	Norton Secure Login
OIX	Open Identity Exchange
OASIS	Organization for the Advancement of Structured Information Standards
OV	Organization Validated
PCTF	Pan Canadian Trust Framework
PAdES	PDF Advanced Electronic Signature
PHR	Personal Health Records
PIV	Personal Identity Verification
PUF	Physically Unclonable Function
PCR	Platform Configuration Register
PEP	Politically Exposed Person
PDF	Portable Document Format
PRIVO	Privacy Vaults Online

PP	Protection Profile
PKI	Public Key Infrastructure
PSCIOC	Public Sector Chief Information Officer Council
PSSDC	Public Sector Service Delivery Council
QESQC	QES based on Qualified Certificate
QC	Qualified Certificate
QESeal	Qualified Electronic Seal
QESig	Qualified Electronic Signature
QES	qualified electronic signature/seal
QTS	Qualified Timestamp
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate
QAA	Quality Authentication Assurance
QR Code	Quick Response Code
RUP	Rational Unified Process
REM	Registered Electronic Mail
RP	Relying Party
RFC	Request for Comments
SEDA	Scalable Embedded Device Attestation
SCUBA	Secure Code Update By Attestation in Sensor Networks
SMART	Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust
SAML	Secure Assertion Markup Language
SE	Secure Element
STORK	Secure idenTity acrOss boRders linKed
SSL	Secure Socket Layer
SAML	Security Assertion Markup Language
SPM	Self Protecting Modules
SML	Service Metadata Locator
SMP	Service Metadata Publisher
SaaS	Software as a Service
SWAT	SoftWare Based Device ATtestation
SP	Special Publication (NIST)
SIM	Subscriber Identity Module
TS	Technical Specifications
TSA	Time Stamping Authority
TL	Trust List
TLS	Transport Layer Security
TFI	Trust Framework Initiative
TFP	Trust Framework Provider
TSP	Trust Service Provider
TTS	Trust Translation Schemes
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
TTP	Trusted Third Party
US	United States
U2F	Universal 2nd factor

UAF	Universal Authentication Factor
UICC	Universal Integrated Circuit Card
UPU	Universal Postal Union
USB	Universal Serial Bus
VIPER	Verifying the Integrity of PERipherals
XAdES	XML Advanced Electronic Signature Time-Stamp Protocol

Appendix Five: CAB Certification Authorities

Certification Authority	Link
Actalis	https://www.actalis.it/
Amazon	https://www.amazon.com/
ANF Autoridad de Certification	https://anf.es/
Buypass	https://www.buypass.no/
Certinomis	https://www.certinomis.fr/
certSign	http://www.certsign.ro/certsign/
Certum	http://www.certum.eu/certum/cert,eindex_en.xml
China Financial Certification Authority	http://www.cfca.com.cn/
Chunghwa Telecom Co., Ltd.	http://epki.com.tw/
China Internet Network Information Center	http://www1.cnnic.cn/IS/fwqzs/
Cisco	https://www.cisco.com/
Comodo CA Ltd	http://www.comodo.com/
D-TRUST GmbH	http://www.d-trust.net/
DigiCert, Inc.	https://www.digicert.com/
Digidentity	http://www.digidentity.eu/
Disig, a.s.	http://www.disig.sk/
DocuSign (formerly OpenTrust/KEYNECTIS)	https://www.opentrustdtm.com/
E-TUGRA Inc.	http://www.e-tugra.com.tr/
Entrust	http://www.entrust.com/
ESG de Electronische Signatuur B.V.	https://www.de-electronische-signatuur.nl/
Firmaprofesional	http://www.firmaprofesional.com/
Global Digital Cybersecurity Authority Co., Ltd	https://www.gdca.com.cn/
GlobalSign	http://www.globalsign.com/

GoDaddy Inc	http://www.godaddy.com/
Hellenic Academic and Research Institutions Certification Authority (HARICA)	http://www.harica.gr/
Izenpe S.A.	http://www.izenpe.com/
Kamu Sertifikasyon Merkezi	http://www.kamusm.gov.tr/
KPN Corporate Market BV	http://www.kpn.com/
Let’s Encrypt	https://letsencrypt.org/
Logius PKIoverheid	http://www.logius.nl/english/
National Center for Digital Certification	http://www.ncdc.gov.sa/
Network Solutions, LLC	http://www.networksolutions.com/SSL-certificates/index.jsp
Open Access Technology International	http://www.oati.com/
Prvni certifikacni autorita, a.s.	http://www.ica.cz/
QuoVadis Ltd.	http://www.quovadisglobal.com/
Secom Trust Systems	http://www.secomtrust.net/
Shanghai Electronic Certification Authority Center Co. Ltd	http://www.sheca.com/
Skaitmeninio sertifikavimo centras (SSC)	http://www.ssc.lt/
StartCom Certification Authority	http://www.startssl.com/
Swisscom (Switzerland) Ltd	http://www.swisscom.ch/
SwissSign AG	http://www.swisssign.com/
Symantec Corporation	http://www.symantec.com/
TAIWAN-CA Inc.	https://www.twca.com.tw/Portal/Portal.aspx
TrustCor Systems, S. de R.L.	https://www.trustcorsystems.com/
Trustis Limited	http://www.trustis.com/
Trustwave	http://www.trustwave.com/
TURKTRUST	http://www.turktrust.com.tr/

WoSign		http://www.wosign.com/english

Trust Framework	Trust List Member	Website
Minors Trust Framework	OIXnet	https://privo.com/minors-trust-framework/
Mydex Trust Framework	OIXnet	https://mydex.org/prnews/mydex-trust-framework-recognised-by-open-identity-exchange/
Nate Blue Button for Consumers Trust Bundle (NBB4C)	OIXnet	http://nate-trust.org/nbb4c-trust-bundle/
The Respect Trust Framework	OIXnet	https://respectnetwork.wordpress.com/respect-trust-framework/
SAFE-BioPharma FICAM Trust Framework Provider Program	OIXnet	https://www.safe-biopharma.org/SAFE_Trust_Framework.html
SecureKey Concierge™ Canada Trust Framework	OIXnet	http://securekey.com/wp-content/uploads/2015/09/SK-UN117-Trust-Framework-SecureKey-Concierge-Canada.pdf
tScheme	OIXnet	http://www.tscheme.org/
Pan Canadian Trust Framework		https://diacc.ca/2016/08/11/pctf-overview/
Personal Data and Trust Framework		https://pdtn.org/
DigiCert	IDEF	https://www.digicert.com/direct-project/
ID.me	IDEF	https://www.id.me/
MorphoTrust USA	IDEF	http://www.morphotrust.com/eID.aspx
Symantec Corporation	IDEF	https://www.idefregistry.org/registry/listing/norton-secure-login/
PRIVO	IDEF	https://www.idefregistry.org/registry/listing/privo-lock-and-the-privo-id-platform/
MedAllies	Kantara	http://www.medallies.com/productsservices.html