White Paper
The Trust Framework Series

Trust Frameworks for Identity Systems

Esther Makaay - SIDN
Tom Smedinghoff - Locke Lord LLP
Don Thibeau - Open Identity Exchange

June 2017

Contents

1 Introduction

What do we mean when we talk about a trust framework? Current literature often refers to a broad array of varying and sometimes conflicting descriptions and definitions. This adds complexity to the already complicated task of developing a new trust framework, as well as assessing and comparing existing trust frameworks.

> *What is a trust framework? What is it used for? Why is it important? And what goes into a trust framework?*

This paper sets out a clear description of a trust framework and its role in governing an identity system, addressing questions such as: What is a trust framework? What is it used for? Why is it important? And what goes into a trust framework?

Trust frameworks are not a new concept. They are commonly used outside of the world of digital identities, to govern a variety of multi-party systems where participants desire the ability to engage in a common type of transaction with any of the other participants, and to do so in a consistent and predictable manner. In such cases, they are proven to work and scale. Common examples include credit card systems, electronic payment systems, and the internet domain name registration system, which all rely on a set of interdependent specifications, rules, and agreements. This set of specifications, rules and agreements is referred to by various names, such as "operating regulations," "scheme rules," or "operating policies." In the world of identity systems they are commonly referred to as a "trust framework."

With the growing need for digital transactions and online interactions of ever-increasing significance or value, identity systems are growing, spreading and maturing. Traditional identity systems have often been based on bilateral agreements or loosely-coupled SLAs. But these prove difficult to scale, may be problematic from a liability perspective, and lack transparency needed for trust by all stakeholders. A trust framework provides an efficient and scalable alternate approach that is critical to the functioning of large multi-party identity systems. It allows both participants and end users to rely on assurances for identities, verification, and authentication through a multi-party collaboration facilitated by the trust framework that governs the operation of the identity system.

2 The Basic Concept of a Trust Framework

"Trust framework" is a generic term often 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 community of participants, and bound by a common set of requirements. Examples of multi-party systems that employ trust frameworks include credit card systems (such as Visa or MasterCard), electronic payment systems (such as SWIFT or NACHA), the domain name registration system (ICANN), and identity systems. They all share a

variety of common characteristics, including the fact that each participant needs assurances that each other participant will follow the same set of rules applicable to its particular role.

The set of specifications, rules, and agreements that govern such multi-party systems are referred to by various names. For example, the Visa payment card system refers to them as "Operating Regulations"; the NACHA electronic funds transfer system calls them "Operating Rules"; some identity systems deployed in the U.S. refer to them as a "Trust Framework", whereas identity systems in the UK (e.g., the GOV.UK Verify program) refer to them as "Scheme Rules." Other identity systems call them "Common Operating Rules" or "Operating Policies." All of these various terms, however, define the same thing. This paper will use the term "trust framework," as that is the term most commonly used in the field of digital identity management. But the term "trust framework" should be read as synonymous with terms such as "system rules," "scheme rules," "operating regulations," or "common operating rules."

There is a great deal of literature referencing trust frameworks, which tends to utilize a broad and often conflicting variety of descriptions and definitions.[1] But reduced to its essence a trust framework is simply a legally enforceable set of specifications, rules, and agreements governing the operation of a specific multi-party system.

In this paper we focus on trust frameworks for identity systems, using the definition of an identity system from UNCITRAL[2] to capture a broad variety of the transactions and collaborations encountered in the real world:

> "Identity system" means an online environment for identity management transactions governed by a set of system rules (also referred to as a trust framework) where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their identities. An identity system involves:
>
> a) a set of rules, methods, procedures and routines, technology, standards, policies, and processes,
> b) applicable to a group of participating entities,
> c) governing the collection, verification, storage, exchange, authentication, and reliance on identity attribute information about an individual person, a legal entity, device, or digital object,
> d) for the purpose of facilitating identity transactions.

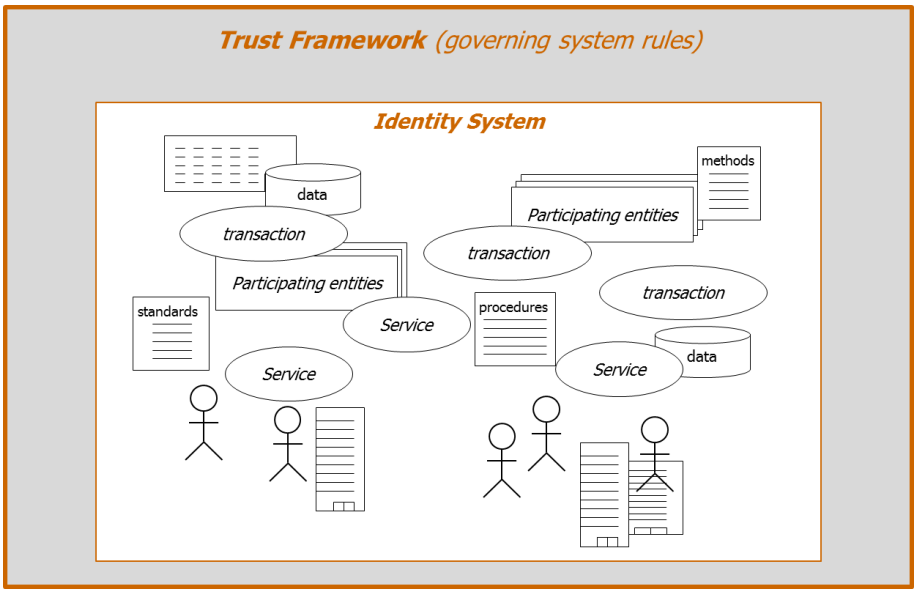
[1] Thomas J. Smedinghoff offers a nice collection of varying definitions on identity trust frameworks in this presentation for the American Bar Association: http://apps.americanbar.org/dch/thedl.cfm?filename=/CL320041/newsletterpubs/4-Trust-Framework-and-Liability-Overview.ppt

[2] United Nations Commission on International Trade Law (UNCITRAL), Working Group IV, Document A/CN.9/WG.IV/WP.143, at paragraph 33 (10 February 2017), available at: http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html

There are numerous identity systems in existence, and many more will likely be established. They are established for a variety of different purposes, include a variety of different categories of participants, and employ a variety of different structures.

But while each identity system itself may consist of numerous and varying elements, as the UNCITRAL definition notes, it is "*governed by a set of system rules (also referred to as a trust framework) where […the participating entities…] can trust each other.*" This set of system rules -- the trust framework -- governs the collection, verification, storage exchange, authentication, and reliance on identity information within the context of the identity system.

> *Governed by a set of system rules (also referred to as a trust framework) where [...the participating entities...] can trust each*



A trust framework governs an identity system

3 Defining a Trust Framework for Identity Systems

A trust framework is a legally enforceable set of specifications, rules, and agreements that governs an identity system.

It generally possesses the following characteristics:

- **Scope:** A trust framework governs a specific identity system.
- **Purpose:** A trust framework defines and governs the operation of that specific identity system and the obligations of its participants in order to ensure both the functionality and trustworthiness of the system.
- **Form:** A trust framework can take almost any form, comprise one or several documents, be self-contained or incorporate other documents, and be short or long in length, as necessary to define and govern the specific identity system it addresses;

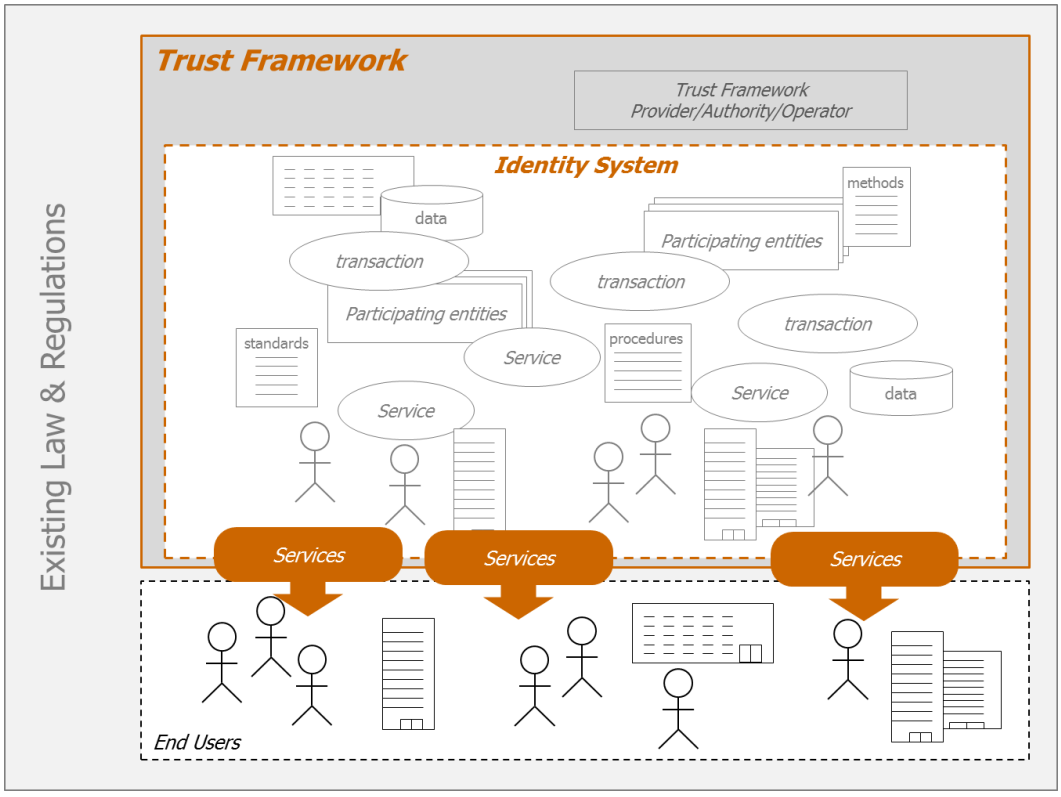
- **Content:** Generally, a trust framework will define the roles and functions required for the operation of the governed identity system, and address numerous issues of importance for the identity system across four categories of requirements.

    - **Define Roles and Functions:** It typically defines the functions and addresses both the operational roles (if any) necessary to maintain the identity system and the participant roles of those that engage in identity transactions within the identity system.
    - **Address Key Issues:** Its specifications, rules, and agreements address the key business, technical, operational, and legal issues of importance for the governed identity system and as necessary to ensure both the functionality and trustworthiness of the system.

- **Authorship and Control:** A trust framework can be written by any one of a number of entities or organizations, including an entity established for the express purpose of operating or managing the identity system, a controlling entity in the identity system, a committee of participants in the identity system, a government agency or legislative body, or others.

- **Enforceable:** A trust framework legally binds participating entities in its identity system with role-specific sets of duties and liabilities. It is implemented and made legally binding on entities participating in the identity system, usually by contract, although in the case of some government-operated identity systems it can be implemented by statute or regulation.

Each of these characteristics is further described in the following sections.



A trust framework governs an identity system that provides end-user services

4 Characteristics of a Trust Framework

4.1 Scope of a Trust Framework

Each trust framework is typically written for a particular identity system. It sets the rules and regulations for processing[3] of identity information[4] within the context of the identity system it governs. Thus, its scope is limited to the parameters of that specific identity system. It defines and governs the operation of that identity system, the services provided under that system, and the obligations of its participants. Accordingly, each identity system will likely have its own unique trust framework.

4.2 Purpose of a Trust Framework

The purpose of a trust framework is to ensure both the functionality and trustworthiness of the identity system. Ensuring that the identity system functions properly is, of course, a fundamental goal. But because a merely functional identity system is not necessarily a trustworthy system, the specifications, rules, and agreements that comprise the trust framework are usually also written to help ensure the level of trustworthiness required by the entities participating in the identity system and the community relying on the services offered by the identity system.

> *Two primary purposes of a trust framework – functionality & trustworthiness*

These two primary purposes of a trust framework – functionality and trustworthiness -- may be further subdivided and explained as follows:

- **Functionality:** The trust framework facilitates the functionalities of the identity system it governs through the use of specifications, rules, and agreements designed to ensure that it operates properly in two respects:
    - **Proper Operation:** it governs the identity system in a manner designed to ensure that the system functions properly for its intended purpose – i.e., that it works;

[3] Under the EU General Data Protection Regulation (GDPR), "processing" is defined to mean: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[4] In the Open Identity Trust Framework (OITF) Model, the term "identity information" here includes both authentication information for establishing that a legal person or an entity is who he, she, or it claims to be (which may or may not include an identifier), as well as attribute information (details about that person or entity). Such identity information is sometimes referred to as "claims" http://openidentityexchange.org/wp-content/uploads/the-open-identity-trust-framework-model-2010-03.pdf

- **Compliance:** it is also designed to ensure that the system and its participants operate in accordance with the requirements of any applicable law.

- **Trustworthiness:** The trust framework facilitates the trustworthiness of the identity system it governs through the use of specifications, rules, and agreements designed to ensure that it functions in a way that is (and is perceived by the participants to be) sufficiently trustworthy to meet the needs of the community participating in the identity system (i.e., so the various parties are willing to participate and rely). To that end:

  - **Risk Management:** it addresses and manages the various risks inherent in participating in the identity system, and imposes requirements designed to address those risks;
  - **Legal Certainty and Predictability:** it addresses the legal rights, responsibilities, and liabilities of the participants, and eliminates the uncertainty of the application of existing law not written for identity systems;
  - **Transparency:** by making the terms of the specifications, rules, and agreements comprising the trust framework accessible to all participants, it also facilitates trust.

Trust frameworks may also serve other purposes. In some situations enhancing the business case for participation in the identity system is another important goal. To that end, a trust framework might be designed to make it attractive for potential participants to join the identity system by:

- Creating a transparent and equally-applied foundation for core identity-related services which allows for participants to uniquely profile their end-user services instead of competing on aspects such as trustworthiness and security;
- Broadening market adoption of a specialised brand and/or trustmark, and support for related marketing efforts which may facilitate broader market penetration and adoption;
- Standardizing technical or functional operations to allow for reusability and more efficient certification, lowering cost burdens not just for participants but also for end users.

4.3 Form of a Trust Framework

There is no standard form or length for a trust framework. Identity systems can take many different forms and the governing trust frameworks consequently vary greatly in structure and content. The specifications, rules, and agreements comprising the trust framework can take shape in contractual, statutory or regulatory form, and can be structured in many ways. For example, a trust framework may comprise one document or several. It may define its own specifications, or incorporate existing specifications or other policies or procedures developed by third parties. And it may take the form of a master set of rules made binding by separate contract, may itself be a contract, or may take some other form.

The form used will likely vary significantly depending upon the nature of the identity system to which the trust framework applies.[5] Most private and public-private trust frameworks are based on

[5] See the OIXnet Registry at www.oixnet.org for examples of different trust frameworks.

contractual agreements, which constitute private (i.e., contract-based) law. In the case of government-operated identity system, the trust framework may take the form of a statute or regulation adopted by the jurisdiction.

4.4 Contents of a Trust Framework

The contents of a trust framework will vary greatly, depending upon the nature of the identity system it governs, the level of trust it seeks to achieve, and the level of detail the parties desire to address. Generally, however, the content of a trust framework will define the roles and functions required for operation of the governed identity system (described in 4.4.1 below), and address numerous issues of importance for the identity system across four categories of requirements (described in 4.4.2 below).

4.4.1 Definition of Roles and Functions

An identity system may consist of many different roles providing or consuming a variety of services, and require the performance of many different functions to achieve the desired results. The specifications, rules and agreements in a trust framework will typically identify and define those roles and functions, the individuals and organizations eligible to participate in each of those roles, the rights and responsibilities assigned to each of those roles, and the requirements for each of the functions. For entities interested in participating in one or more of its defined roles, the trust framework may also specify any requirements that must be satisfied before the entity is allowed to participate in such role.

A 'role' does not refer to a specific individual, organisation, or entity: a role is a set of functions and obligations that are assigned to a particular defined position within the context of the trust framework, such as "identity provider" or "relying party." Depending on the requirements associated with a particular role, the role can be fulfilled by any number of individuals, organisations, or entities. In many cases, a single organisation can perform multiple roles. The terms of a trust framework that apply to a specified role will usually apply equally to all participants who fill that role.

The scope, purpose, and structure of an identify system, as defined by the trust framework that governs it, determines which roles are required and the functions assigned to each such role. Not all roles and functions mentioned in this paper need to be present in a trust framework. Likewise not all possible roles and functions that can exist are described here. Specific needs and requirements of a trust framework may call for specific solutions.

Generally, the functions defined by a trust framework may be grouped into two general categories:

- **Operational functions:** Functions relating to defining, governing, and operating the identity system itself, which are assigned to one or more roles within the trust framework, and
- **Participating functions:** Functions concerning the participating entities within the identity system and the transactions and services involved, which are assigned to one or more participant roles.

Operational Functions

The need for one or more operational roles depends on the required functions and maturity of the governed identity system. At a minimum, someone must be responsible for developing and maintaining the trust framework itself, and amending it when changes are required or new issues arise. In more complex identity systems, with a large network and many types of participating entities offering many different services, there may also be a need to provide for additional governing roles to address a variety of other governing functions, such as:

- **Governance and Policy Development:** Developing and amending policies; decision-making; stakeholder-facilitation; managing standards and procedures; accountability mechanisms.
- **Policy Enforcement:** Ensuring compliance with existing policies; enforcement mechanisms; performing assessments or audits; managing changes and releases.
- **Participating Entity Management:** Administration and enrolment of participating entities; certification and trust marks; support; dispute resolution; billing.
- **Network Evolvement:** Growing and supporting the network; marketing; communication and; developing strategy.
- **Trust Framework Operations:** Offering central services to the participating entities and/or public, e.g. information and discovery services.

In many cases these functions can be addressed by a designated separate legal entity (like Visa, Inc. does for the Visa credit card system). In other cases, a cooperative consortium might fill one or more of the governing roles or a committee established by the participating entities.

The roles tasked with performing these functions are sometimes referred to as a Trust Framework Provider, Trust Framework Authority, Policy Authority, or Trust Framework Operator (depending on their specific functions).

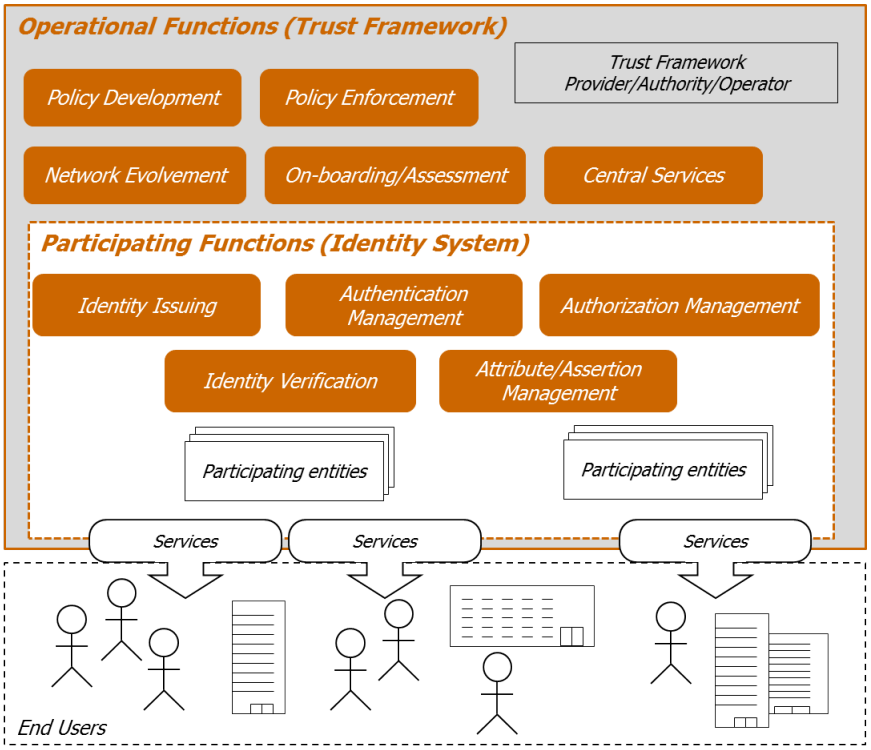
Participating Functions

Trust frameworks for identity systems typically focus on provisioning and verification of identity information. Accordingly, functions that need to be addressed by participating roles often include the following:

- **Identity Issuing:** Registration of identities and related attributes; issuing identity credentials; binding identities and credentials to end-users.
- **Identity Verification:** Verifying identity information and credentials; providing or verifying additional attributes and assertions.
- **Authentication Management:** Requesting verification of credentials; requesting verification of attributes and claims; providing results of verification.
- **Authorisation Management:** Managing delegations and mandates; managing (end user) consent; managing identity verification and authentication policies.
- **Attribute, Claims or Assertion Management:** Registration of attributes and credentials;

binding of attributes and credentials to identities; verification or provisioning of claims based on registered attributes and credentials.

The roles performing some of these functions are commonly referred to by designations such as Identity Provider, Relying Party, Hub/Broker, Authentication Provider, Attribute Provider, and Authorization Manager.



Functions that may be assigned to roles in a trust framework and the identity system

> *The roles performing some of these functions are commonly referred to by designations such as Identity Provider, Relying Party, Hub/Broker, Authentication Provider, Attribute Provider, and Authorization Manager*

4.4.2 Issues Addressed

A trust framework governs a particular identity system and provides the specifications, rules, and agreements that guide, dictate and enforce transactions with and within that identity system. But what issues should be addressed in the document(s) that constitutes the trust framework?

The contents of a trust framework – i.e., the specifications, rules, and agreements that comprise the trust framework -- generally address the key business, technical, operational, and legal requirements of importance for the particular identity system it governs. While these are not rigidly separated categories (and in fact, often overlap significantly), some general descriptions might be useful:

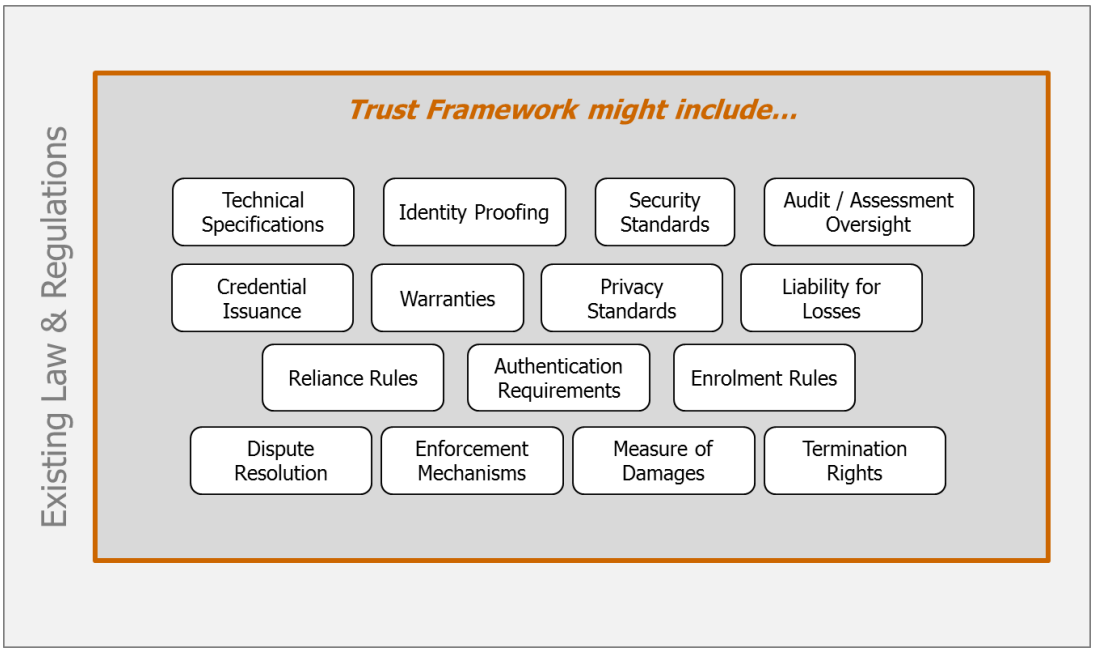
- **Business requirements** focus on high level business issues such as the scope of the identity system, the services it provides, its structure, requirements for participation in the identity system, or rules for branding or use of trust-marks to enhance the trust associated

with its services.

- **Technical requirements** focus on details regarding data formatting, communication interfaces, and processing specifications to ensure consistency and interoperability across all identity system transactions, often through use of standards and standardisation of interfaces for transactions.
- **Operational requirements** address identity system functionality issues, such as rules for identity proofing, requirements regarding the dissemination and use of information, authentication procedures, and support procedures that need to be in place.
- **Legal requirements** address the rights and obligations of each of the participant roles, as well as issues such as warranties, liability allocation, governing law, and dispute resolution, and in many cases flow from the other requirements imposed on participants.

Within these four categories there are numerous issues that might be addressed in a trust framework. But ultimately, which issues should be covered, and the level of detail with which they should be addressed, will be determined by the nature and scope of the governed identity system, as well as applicable law and the willingness to defer to such law rather than adopting an alternate approach.

As a general matter, however, a trust framework typically defines the scope and purpose of the identity system, determines what roles are to be included and what duties are assigned to those roles, sets the eligibility requirements for entities seeking to fulfil those roles, and establishes the rules and regulations for processing of identity information within the context of the identity system. Common elements of a trust framework include defining the rights and responsibilities of the participants in the identity system; specifying the policies and standards specific to the identity system; and defining the specific processes and procedures that provide an appropriate level of assurance or trust for the participants and end users. Common issues covered by a trust framework include those identified in the diagram below:



Issues that might be addressed in a trust framework

The rights and responsibilities of the participants in the identity system are typically specified for each role defined by the identity system, and apply to each participating entity filling that role. By specifying rights and responsibilities, the trust framework also provides a basis for determining liability in the event of a problem. That is, by assigning certain rights and responsibilities to each role, the trust framework creates legal duties, which, if breached, can form the basis for potential liability. In some cases the trust framework may address the scope and extent of a role's liability for breach of its obligations under the terms of the trust framework itself. In other cases, that liability can be left to existing law (e.g., for breach of contract).

4.5 Authorship and Control of a Trust Framework

Someone (a person, an entity, a group, or a committee) must be charged with the task of writing the trust framework, and someone (not necessarily the same person or group) should be assigned responsibility thereafter for updating and maintaining it as necessary to meet future needs.

The authorship and control over the content of a trust framework for any particular identity system is often a function of the nature and structure of that identity system. In some cases, this may be assigned to the legal entity that established the identity system, or a separate legal entity charged with the task of managing the trust framework. In other cases, a trust framework may be written by a consortium of participating entities that mutually agree on rules and regulations, or by a committee of participants elected to oversee accountability and governance.

Common examples of possible authors for a trust framework include the following:

- **Independent Governing Entity:** For some identity systems, an independent entity may be formed or designated for the specific purpose of developing, maintaining, and enforcing an appropriate trust framework. This typically occurs in the case of a large-scale identity system that includes numerous identity providers and relying parties. Such an entity is commonly referred to as a *trust framework provider, operator or authority*. An example is the SAFE-BioPharma identity system, which is managed by the SAFE-BioPharma Association.[6]

- **Consortium of Participating Entities:** In other cases, a group consisting of some, but not necessarily all, of the participating entities in an identity system will convene to draft, and update as needed, the appropriate trust framework. An example of this is provided by the CA/Browser Forum, which consists of a group of browser vendors and certification authorities that jointly agrees upon the trust framework for a system focused on recognition of trust roots for website server and related domain name owner identification.[7]

- **Single Participant Governing Entity:** In some cases, a single existing organization (typically an entity acting as either the sole identity provider or the sole relying party) both establishes the identity system and acts as a participant for its own specific purposes. As the

[6] SAFE-BioPharma Association, https://www.safe-biopharma.org

[7] CA/Browser Forum, https://cabforum.org/. This trust framework governs the issuance of EV-SSL server certificates.

strong central entity, it dictates the architecture, policies and contractual structure of the trust framework, and may also manage and operate a technical platform, which supports the interactions among the participants. Examples include single identity provider systems, such as those operated by Google and Facebook, and single relying party systems, such as those operated by the US government's Login.gov program or the UK government's GOV.UK Verify program.

- **Non-Governing Standards or Certification Organization:** In some cases, an independent entity may be established to develop (and update from time-to-time) standard rules for a trust framework, but such entity will not itself actually govern the operation of an identity system. It may, however, certify participants (particularly identity providers) as compliant with its system rules. Examples of this approach include the Identity Assurance Framework issued by the Kantara Initiative[8], and the tScheme Approval profiles issued by tScheme[9].

- **Mutual Agreement Among All Participants:** In smaller scale identity systems, system rules can be jointly negotiated by the participants (or written by a dominant participant), and memorialized in a mutual agreement. In such case there is no separate governing entity, but simply an agreement between and among all of the participants.

4.6 Enforceability of a Trust Framework

> *A trust framework is of no value unless the participants in the identity system that it purports to govern are legally obligated to follow the rules set out in the trust framework – i.e., it must be enforceable*

Regardless of its form, format, or content, a trust framework is of no value unless the participants in the identity system that it purports to govern are legally obligated to follow the rules set out in the trust framework – i.e., the trust framework must be enforceable. In some cases, the rules of the trust framework can be made binding by law or regulation. Likewise, depending on the technologies and procedures specified by the trust framework, policies may also be enforced by systems, software and applications. But in most cases, the rules of a trust framework are private law that can be made enforceable only by voluntary agreement of the parties.

Thus, once a trust framework is written, a key challenge is establishing a mechanism to ensure that all participants within the scope of its rules are legally bound in a manner that makes the portion of the rules relevant to their role enforceable against them. And ideally, each participant should be legally obligated to follow the rules of the trust framework for the benefit of all other affected participants in

[8] Kantara Initiative, https://kantarainitiative.org

[9] tScheme, www.tscheme.org

the identity system (including the end users) even though each participant will not enter into a separate contract directly with all such other participants. This is usually accomplished as follows:

- In the case of private sector identity systems, the governing trust framework is usually made enforceable by some sort of contractual mechanism. Many approaches can be used, although one of the more common approaches is to develop a master set of trust framework rules (set out in one or more documents), which all parties agree to through the use of a simple form contract that references or incorporates the rules by reference.
- In the case of government sector or government-sponsored identity systems, the governing trust framework may take the form of a statue or regulation. In such cases, the terms of the trust framework are binding on the participants by law.
- Trust frameworks for public-private partnerships might rely on a contract-based approach, or a hybrid form might be used, where the foundation and main principles are based in law, but certain specific role-related requirements are enforceable through agreements.

In some cases, trust frameworks are not made legally binding on certain roles, such as end users or attribute providers, although the trust framework may regulate the conduct and responsibilities of other participants relative to those roles. For example, in some cases users (i.e. the subject of identity credentials) do not contractually agree to the terms of the trust framework itself. However, the trust framework may impose on identity providers an obligation to enter into a contract with such users that contains certain terms or imposes certain requirements.

5 How a Trust Framework Fits in the Overall Legal Framework for Identity

The role of a trust framework in the overall legal framework for identity is much like the role of a sales contract in the overall legal framework governing the sales of goods. That is, it is written to address the specific issues of a particular identity system, but is also subject to, and governed by, more general higher-level law.

Identity systems and identity transactions, like most commercial systems and commercial transactions, are typically governed by up to three levels of different legal rules. These legal rules may be generally described as follows:

- **Level 1 - General Law:** The first (and foundational) level of legal rules applicable to identity management systems and transactions is existing general law. This consists of the rules enacted as statutes by legislatures, adopted as regulations by government agencies, or determined by judicial decision. Such law was not written for identity systems, but is frequently applied to identity systems and identity transactions to the extent it relates generally to the activities of identity systems. General law includes contract law, tort law, privacy law, export control law, warranty law, consumer protection law, antitrust law, and the like. Such law is public law (i.e., written by governments), applies to all identity systems and

identity system participants by the authority of the government, and is enforceable in the courts. Unfortunately, because it is not written for identity systems, it may not be a good fit, or may yield unanticipated or inappropriate results.

- **Level 2 – Identity Management Law:** The second level of legal rules applicable to identity management systems and transactions consists of identity management law. This law (where it exists) is new, is written specifically to govern all identity systems within its scope, and is designed to address one or more of the specific issues that arise in the context of the operation of such identity systems (e.g., participant liability). Very little such law currently exists, but projects are underway in several jurisdictions to develop such Level 2 law for the purpose of encouraging and/or regulating identity systems and identity transactions. The prime example of such Level 2 law is the Virginia Electronic Identity Management Act[10]. Level 2 law is also public law, and applies to all identity systems and identity system participants that operate within its scope by the authority of the government, and is enforceable in the courts.

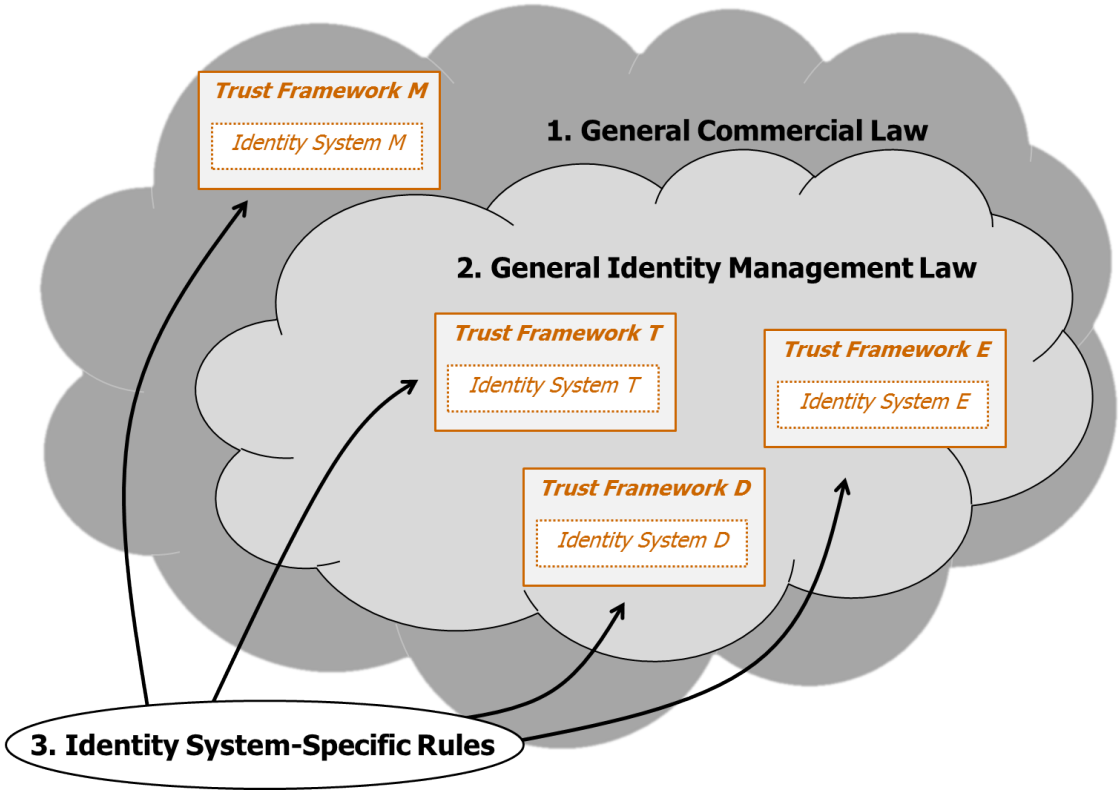
- **Level 3 – Trust Framework -- Identity System-Specific Rules:** The third level of legal rules applicable to identity management systems and transactions consists of the trust framework – *i.e.*, the system-specific rules adopted by (or for) a particular identity system for its own operation. Such system-specific rules are usually necessary in some form regardless of whether that identity system is operated by a government or a private sector entity. In the case of private sector identity systems (and some public-private identity systems) the trust framework typically takes the form of *contract-based rules* (i.e., private law) drafted by one or more participants in, or the governing body of, the specific identity system and voluntarily agreed to by the participants. In the case of government operated identity systems, the trust framework typically takes the form of *statutes or regulations* adopted by the operating government body (most often a country's national ID system, or *e.g.*, the eIDAS Regulation in the EU[11]). In either case, however, these system-specific identity system rules apply only to the specific identity system for which they were written. Thus, there will be many such trust frameworks. Contract-based trust frameworks must, of course, also comply with the governing legal rules in Level 1 and Level 2. In the case of trust frameworks that exist in contract form, they are binding only on those parties that voluntarily agree to the terms of the applicable contracts. If such rules exist as a statute or regulation, they are binding only on those who are expressly within their scope. In either case, such trust frameworks only apply to one particular identity system.

This legal framework is depicted in the diagram below. As this diagram illustrates, portions of the legal framework for any private-sector identity system (i.e., the Level 3 trust framework portion) are under the control of the developers of that identity system, and other portions (i.e., Levels 1 and 2) are outside of their control. That is, the operators of an identity system are free to make up the Level 3 system rules (so long, of course, as the participants contractually agree to be bound by them), but

[10] The Virginia Electronic Identity Management Act: https://lis.virginia.gov/cgi-bin/legp604.exe?151+sum+SB814

[11] EU eIDAS Regulation: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

at the same time, the private contracts that make these system rules binding on the participants are supplemented (and in some cases superceded) by existing laws and regulations. As such, the Level 3 system rules must interface with existing law – a challenge made all the more difficult for identity systems that cross jurisdictional boundaries. Moreover, any issues not addressed by the Level 3 trust framework will be determined by the public law at Level 1 (and Level 2 if it exists).



About OIX

The Open Identity Exchange (OIX) is a technology agnostic, non-profit trade organization of leaders from numerous business sectors focused on building the volume and velocity of trusted transactions online. OIX enables members to expand existing identity services and serve adjacent markets. Members advance their market position through joint research and engaging in pilot projects to test real world use cases. The results of these efforts are published via OIX white papers and shared publically via OIX workshops. OIX members work together to jointly fund and participate in pilot projects (sometimes referred to as alpha projects). These pilots test business, legal, and/or technical concepts or theory and their interoperability in real world use cases. OIX operates the OIXnet trust registry, a global, authoritative registry of business, legal and technical requirements needed to ensure market adoption and global interoperability.

Web: www.openidentityexchange.org

Contact: director@openidentityexchange.org

> *Join and help shape the markets you intend to lead.*