OPEN IDENTITY EXCHANGE

TRUSTMARKS IN THE IDENTITY ECOSYSTEM

Definitions, Use, and Governance

White Paper

IDENTITY STEERING GROUP

By Dr. Gilad L. Rosner

Executive Summary

As the identity ecosystem evolves and grows, discussions of trustmarks are becoming more frequent. Trustmarks, privacy seals, certification marks and their like are a common feature of the online landscape, most often seen within an eCommerce context. Policy initiatives such as the US National Strategy for Trusted Identities in Cyberspace (NSTIC) and the Digital Agenda for Europe specifically seek to advance and embed trustmarks for the good of the digital citizenry. The identity ecosystem is not the eCommerce domain, however, and wholesale incorporation of its trustmark concepts is not appropriate. This paper attempts to draw together a broad range of ideas and contexts for trustmark usage so as to distill a set of terms, concepts and considerations that are most useful to the identity management (IDM) community.

Table of Contents

1. Defining trustmarks

The term 'trustmark' is a bit imprecise, made worse by the inclusion of the word 'trust,' which has a highly variable meaning. In a wide range of professional and public discussions, 'trustmark' is often used interchangeably with the following terms:

Certification mark: This is a generic term referring to a mark that indicates a product or service has been certified by a third party to comply with a set of requirements. The US Patent and Trademark Office defines it as

> "any word, phrase, symbol or design, or a combination thereof owned by one party who certifies the goods and services of others when they meet certain standards. The owner of the mark exercises control over the use of the mark…."

The UK Intellectual Property Office (IPO) further states

> "The main feature of a certification mark is that it is used not by the proprietor of the mark but instead by his authorised users for the purpose of guaranteeing to the relevant public that goods or services possess a particular characteristic."

Privacy Seal: This is a specific kind of certification mark, indicating that the bearer has been certified against a set of privacy and/or data protection criteria. A European Commission report states

> "Privacy seals function as privacy and data protection guarantees. They inform consumers about an organisation's privacy policies, operations, practices and adherence to certain privacy and data protection standards. They notify consumers about how an organisation may collect, use or share data." (EU Privacy Seals Project, p. 13)

Similar to these are **security seals**, which attest to adherence to security practices and standards.

Much trustmark literature focuses on their use within eCommerce, where they are sometimes called **web seals**. As such, trustmark definitions are often biased towards an eCommerce context:

> "Trustmarks aim to assure consumers that a particular site or online seller has been validated by a trustmark provider and is found to run a safe sales process. They are designed to increase consumers' trust in the webshop that carries the trustmark." (EU Online Trustmarks, p. 13)

NSTIC definition:

"A trustmark is used to indicate that a product or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority."

However, as will be seen, eCommerce and privacy-oriented definitions for trustmarks are too limiting for a holistic discussion of their use in the identity ecosystem. For the moment, the above definitions for 'certification mark' are sufficiently broad for the identity community. The US NSTIC captures this breadth succinctly:

> **"A trustmark is used to indicate that a product or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority." (p. 22)**

This definition is generic, allowing for a variety of certification requirements: privacy, technical, operational, business policies, etc. It also specifies that these requirements come from an accreditation authority, meaning a body external to the organizations who obtain trustmarks. In line with the UK IPO language above, this means that marks are not used internally by the organizations who manage and license them, only by others. While there are examples of trustmarks that operate in the absence of an accreditation authority, such as some applications of the European CE mark, this paper uses the above NSTIC definition as a baseline.

A trustmark is not always necessary to prove adherence to a set of requirements.

It's important to note that the mark is just that – a symbol. It attests that the organization displaying the mark meets a stated set of requirements. The mark is the visible face of what actually matters: codified requirements and the process by which an entity is certified against them. What follows, therefore, is that **a mark is not necessary to prove adherence to those requirements.** Identity and eCommerce initiatives also use 'trust lists,' 'certification lists,' or, more simply, 'registries' – lists

of entities who have been certified against relevant requirements and standards. One example is the US-EU Safe Harbor Framework. The US Department of Commerce maintains a list of American organizations who have self-certified that they comply with EU data protection principles. The point is that, depending on the use case, it is not a foregone conclusion that the awarding of a visible mark is essential. The choice to use a mark, seal or other visible assertion of certification rests upon a number of factors. In the main, this paper explores the case where use of a trustmark is appropriate and desirable.

"Internet signals can be defined as any computer-mediated actions that firms take in order to project some aspect of their *character*... their *business practices*... or their *output*...."
Aiken et al., p. 258

Visible trustmarks are a **signal** from one party to another. One paper notes:

> "Internet signals can be defined as any computer-mediated actions that firms take in order to project some aspect of their *character* (e.g., their competence, credibility, trustworthiness, etc.), their *business practices* (e.g., their reliability, efficiency, etc.), or their *output* (i.e., their products and services, level of quality, design characteristics, etc.)" (Aiken et al., p. 258)

Trustmarks are a signalling convention to say that something is or is not in conformance with a set of standards. They live within a family of signals, as depicted in the figure on the left.

Family of internet signals

Adapted from Aiken et al., p. 259

A key question, therefore, is **who is signalling whom, and to what end?** This question is explored in the Use Case section below.

Use Cases

Trustmarks fit within two use cases: business-to-business (B2B) and business-to-consumer (B2C). These headings are a shorthand for a more diverse set of relationships that bear further explanation.

Trustmark use cases:

B2B: business-to-business, government-to-business, vendor-to-relying party…

B2C: business-to-consumer, government-to-citizen, vendor-to-customer, relying party-to-customer…

- **B2B**: The B2B use case encompasses business-to-business, government-to-business, vendor-to-relying party – any combination where the essence of the relationship is **organization-to-organization.**
- **B2C**: This use case encompasses business-to-consumer, government-to-citizen, vendor-to-customer, relying party-to-customer – any combination where the essence of the relationship is **organization-to-individual.**

These use cases point to some of the most important questions in considering the use of trustmarks in the identity ecosystem: **Who is the audience of a trustmark?** Who is signalling whom? The answer to those questions, which will invariably fall within one or both of the two use cases, yields great variation in how a trustmark should function, how it is governed, and what form it takes. The Key Considerations section at the end of the paper further explores these and other questions.

Trustmarks and Brands

The family of internet signals above and the preceding discussion defining trustmarks show that several concepts overlap, adding to the imprecision of the term. Moreover, many interview respondents note the difficulty in separating trustmarks from brands. A trustmark is a form of brand, after all – it's a recognizable symbol that relates to a product, service or organization. In the signalling sense, it communicates something about an entity's affiliation and its underlying characteristics. However, while the relationship between trustmarks and more traditional brands is complex, there is a key distinction: **brands relate to origins and trustmarks relate to processes.** The IBM logo indicates the source of a product, whereas a mark from the British tScheme organization indicates that a service has undergone a certification process. **In order for something to be called a trustmark, there must be a process or mechanism that allows someone to trust it.** Furthermore, since marks are intended to be

Brands relate to *origins* and trustmarks relate to *processes*.

Trustmark usage implies membership in a community.

used by more than one entity, **mark usage implies membership in a community.**

The distinction becomes blurrier, however, when brands are used to communicate character. The Rolex watch brand is used to communicate quality, trustworthiness and an aspirational sense of value and class. Now consider the Better Business Bureau OnLine seal, meant to communicate reliability and trustworthiness. With respect to customer evaluation of the two logos, the conceptual distance may not be so great. Both literature and interviewed stakeholders observe that **brands and trustmarks interrelate when presented together.** Users draw inferences, rightly or wrongly, about the relationship between a 'host' brand (e.g., an identity service vendor) and the trustmark or seal. Those inferences may be positive or negative, justified or unjustified. One implication is that a trustmark may not have the desired effect of increasing citizen confidence in an identity service if the perceived interrelationship is negative. These ideas are explored more fully in the Value of Trustmarks section below, but it suffices to say here that some considerations of traditional branding apply to identity ecosystem trustmarks:

Brands and trustmarks interrelate when presented together. Rightly or wrongly, users will draw inferences about the relationship.

- brand confusion is possible; a screen covered in many vendors' logos (the "NASCAR screen") is to be avoided
- recognition is vital, and takes time to achieve
- branding takes up valuable real estate on sites

Trustmarks as Standardization

Trustmarks are an element of standardization. They signal conformance with a set of standards, indicating that an organization is part of a community. These standards address a common set of stakeholder needs. The identity ecosystem can be conceived of as a supply chain: authoritative sources and credential service providers (suppliers), data brokerage hubs (transport), credentials (products), users (consumers), and so on. In trying

The identity ecosystem can be viewed as a supply chain. The stakeholders in the chain share common risks and needs.

to supply identity credentials to the public, this heterogeneous group of stakeholders shares common risks and needs:

- Privacy risks
- Security risks
- Data integrity
- Liability mitigation
- Reliability
- Usability
- Technical interoperability
- Transparency and auditability
- National or international reach
- Conformance with public policies, best practices or international standards

Certification schemes and their visible representations address these needs. Marks and seals are a method of encouraging 'supply chain discipline' to enhance the integrity of an identity system. Scott David, an identity management legal expert, explains:

"Supply chain discipline is enhanced through the use of certification marks that enable instant recognition of conformity to mutually-agreed-upon supply chain participant requirements."

Scott David, University of Washington

> "In supply chains there is a sufficient natural affinity among stakeholders for supply chain integrity and risk reduction through participant discipline. Supply chain discipline is enhanced through the use of certification marks that enable instant recognition of conformity to mutually-agreed-upon supply chain participant requirements."

Trustmarks in this sense are a community 'banner' to rally around, potentially benefitting organizations and individual citizens. Anchoring a trustmark in specific criteria, such as reliability or technical interoperability, reduces ambiguity in both the substance and value of a mark.

Consider the Visa logo. Displaying it indicates the following:

- Technical interoperability – all merchants can accept all cards that display the logo
- Security – data transport systems operate according to a set of security guidelines
- Liability – participating in the VISA scheme requires adherence to a liability framework
- Usability – card use occurs in a familiar way with very limited variation

Using the Visa logo indicates technical interoperability, adherence to a liability framework, familiar usability and known consumer protections.

- Consumer protection – card users are protected in accordance with, at a minimum, national consumer protection laws in cases of fraud

In the case of Visa, the products supplied are credit and a payment mechanism rather than identity assertions, but the goals are the same: system integrity, consumer recognition and trust, and a high rate of transaction success. The Visa logo symbolizes and participates in a disciplined supply chain. Scott David observes:

> "Marking conventions are reaffirmations that promises are being made and kept in the supply chain so everything can keep moving along."

2. Trustmark Categories and Types

Trustmark providers

Trustmarks, lists and registries originate from five different sources:

Trustmark provider types:

Industry organizations
Government bodies
Public/Private bodies
Private organizations

- **Industry organizations:** These are bodies made up of private for- and non-profit member organizations. Examples include ETSI, SAFE-BioPharma, the Kantara Initiative and the InCommon Federation.
- **Government bodies:** Accrediting authorities who are created or led by government institutions. Examples are the NIST Cryptographic Module Validation Program and Germany's EuroPriSe Privacy Seal.
- **Public/Private bodies:** These are bodies where a clear distinction cannot be drawn between public and private governance of the trustmark certification process. Examples are ISO, IEC and tScheme.
- **Private organizations:** These are single, private for- or non-profit entities who oversee a trustmark. Examples include the Better Business Bureau, TüvSüd, TRUSTe, and Symantec's Norton checkmark.
- **Marks without a traditional accreditation authority:** Some marks exist that do not have an accrediting body. Rather, use of

the mark is mandated by law for certain product categories, though there is not an accrediting authority in the traditional sense. For example, various European legal instruments specify which products require a CE mark to indicate conformance as well as the acceptable methods of certification (self, third party assessment, etc.); there is no single authority responsible for the CE mark's use.

Certification Methods

There are two methods of certifying that a product, service or organization is conformant with requirements, leading to a trustmark: self-assessment and third-party assessment.

Certification methods:

Self-assessment and certification

Third-party assessment and certification, which includes peer-to-peer, independent, and direct assessment by certifying bodies

- **Self-assessment and certification:** An organization conducts a review of its own products, services, processes, policies or any other business characteristic and then asserts its conformance to standards, regulations, laws, practices or other external requirements through documentary assertion, legal attestation and/or use of a visible trustmark. Assessment criteria potentially originate from within an organization or derive from external sources.

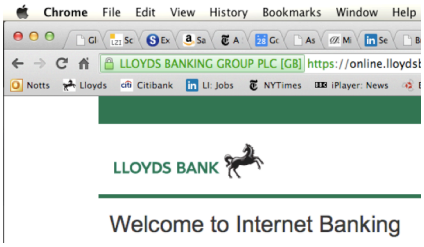
- **Third-party assessment and certification:** An independent third party assesses an applicant organization and certifies that it is conformant with a given set of standards, regulations, laws, practices or other external requirements. This arrangement breaks down into three categories.
    - Peer-to-peer: Organizations are assessed by other organizations participating in a certification scheme.
    - Independent assessors: Organizations are assessed for compliance by entities specifically tasked with independent assessment. These entities are separate from, but work on behalf of, certifying bodies.
    - Certifying body assessment: Assessment is conducted by people or entities who have a direct relationship with a certifying body.

Mark Types

Passive vs. 'active' or 'dynamic' marks: A trustmark can be a simple image, appearing with little variation across multiple organizations and contexts. Alternatively, a mark can change based on some criteria. An example is a security seal from the company McAfee, who scans its customers' sites for malware. In key locations, such as a shopping cart screen, the site displays a McAfee badge that shows today's date, indicating the site has been scanned that day. McAfee claims on its testimonials page that the appearance of the badge has a significant impact on its customers' sales conversions. Justin Basini, Chief Product & Marketing Officer of mobile payments company Zapp, notes that active elements such as dates and scores give consumers a "reason to believe" that a site can be trusted.

An example of an 'active' mark: the McAfee badge indicating that a site has been scanned for malware that day

Self-authenticating marks: It's technically possible for a mark to only display when some or all of the underlying certification criteria are met. These marks are 'self-authenticating' – they prove their authenticity without external assistance. Compare this with a simple trustmark graphic that does not employ any technical measures to help determine its validity. An example of a self-authenticating mark is the Extended Validation SSL Certificate. A special green box appears in a browser's address bar, indicating that a site is operating with one.



An example of a self-authenticating mark: the green portion of the address bar indicates the use of an EV SSL certificate

Machine-readable marks: Recently, there has been research and development into the idea of trustmarks that are intended for use in automated processes. The Georgia Tech Research Institute (GTRI) and others have begun work on treating trustmarks as a set of modular components that could be understood by computers rather than humans. This would require common structure and syntax for trustmark definitions and the development of metadata schema and software tools to allow interoperability. A benefit of this work would be the opportunity to re-use certification components across multiple communities of interest.

GTRI is investigating the idea of machine-readable trustmarks

Certification Categories

Trustmarks in the identity ecosystem can attest to the following certification categories:

- Technical interoperability and adherence to technical standards
- Identity assurance standards
- Data security standards and requirements
- Customer experience or usability criteria
- Privacy requirements
- System performance requirements
- Dispute resolution
- Transparency requirements
- Audit requirements
- Legal compliance
- Business structure, suitability and quality
- Organization and system operational policy compliance

This is not an exhaustive list, though it attempts to capture the most important building blocks of identity-oriented certification schemes. While this kind of granularity may be far too much detail for an individual user, it is essential for the management of a certification scheme and for business relations among participants. These categories can be viewed as modular components, which theoretically could be reused across different trustmarks in differing communities – a form of 'trustmark component interoperability'. One goal of GTRI's machine-readable trustmarks research is to enhance the utility of granular components through increased standardization and automation[1]. A more exhaustive list of certification and trustmark components has been collected into a 'periodic table of trust elements' as part of discussions within the NSTIC Identity Ecosystem Steering Group[2].

Trustmark Certification Categories:

Technical interoperability and adherence to technical standards

Identity assurance standards

Data security standards and requirements

Customer experience or usability criteria

Privacy requirements

System performance requirements

Dispute resolution

Transparency requirements

Audit requirements

Legal compliance

Business structure, suitability and quality

Organization and system operational policy compliance

[1] See https://nstic.blogs.govdelivery.com/2014/01/13/creating-trustmark-compounds-from-trust-elements/

[2] Available at https://www.idecosystem.org/filedepot_download/240/931

3. The Value of Trustmarks

Trustmarks are symbols that attest that a product or service has been certified to a set of standards or requirements. One organization signals another, or an organization signals an individual. This section examines the various intentions, goals and values of these signals.

Trust

Who is trusting whom?

What is the 'trust threat?'

A central theme of trustmarks is, unsurprisingly, trust. Many interview respondents and much literature cite trust as vital to electronic transactions. It's viewed as necessary for consumers to be willing to engage with online services; for eCommerce and identity services to reach their full potential. But, what is trust? The answers that are most useful to the identity ecosystem have to do with who is the trust 'target': who is trusting whom? What is the 'trust threat' that a mark would address? The delineation of B2B and B2C use cases is useful here.

In the case of citizens interacting with public and private institutions and their identity systems, the key trust issues revolve around unfamiliarity with identity management concepts and the perceived privacy and security risks of sharing sensitive personal data. Research into trust on the internet yields some salient definitions. Trust can be viewed as:

- "a benevolent expectation of fairness" (Aiken et al., p. 255)
- surpassing "perceptions of vulnerability" (Aiken et al., p. 255)
- "perceptions that the trustee has worthy attributes" (McKnight et al., p. 253)

"Trustmarks work powerfully in spaces of unfamiliar territory."

Justin Basini, Zapp

Justin Basini of Zapp notes that "trustmarks work powerfully in spaces of unfamiliar territory." In this way, trust is a form of comfort in the face of ambiguity. Identity systems involve both unfamiliar processes and organizations. A trustmark is a way for an organization to 'rent the reputation' of another to encourage context-specific trust.

It's important to note that both literature and interviewed stakeholders argue that users are often unsophisticated in their appraisal of the trustworthiness of online services. Pete Gale, a user researcher with the UK's Government Digital Service (GDS), observes,

> "Trust is more of an emotional decision than an analytical process."

"Trust is more of an emotional decision than an analytical process."

Pete Gale, GDS

A 2012 research paper on trustmarks and seals had the following to say:

> "The creators of trust seals and website owners who use them expect consumers to search for trust seals, check their authenticity, and understand what protection they offer…[W]e argue that these expectations are unrealistic." (Kirlappos et al., p. 9)

"The creators of trust seals and website owners who use them expect consumers to search for trust seals, check their authenticity, and understand what protection they offer… [W]e argue that these expectations are unrealistic."
(Kirlappos et al., p. 9)

This is not to say that trustmarks are ineffective – that is an open question, one that needs to be answered on a context-by-context basis. Rather, that trustmarks may do the intended job, but not necessarily because users check to see what they represent.

Trust in the B2B case is somewhat different. Businesses need to trust that their partners are performing in an expected and/or agreed-upon way, conformant with legal and community standards. Trust here relates to reliability, consistency, and adherence to agreements. It could be argued that contracts are a better way of securing such trust rather than trustmarks.

Risk Reduction

Relationships between two or more organizations or between organizations and individuals entail risk. When two organizations enter into contractual relations, or especially when they rely on one another in a lightweight fashion without contracts, there is always risk that one partner will not fulfill its obligations, or that it has misrepresented itself. Organizations are subject to unpredictable shocks, or weaknesses in their economic position.

In relationships between organizations and individuals, similar risks appear. Individuals can be at a disadvantage to organizations because of

informational asymmetries – individuals may know less about a company than the company knows about them. Organizations will almost certainly understand their own services and products better than their customers. This is undoubtedly true in the world of identity management. Research and experience show that the general citizenry often struggles with identity and credentialing system designs. No less confusing are online privacy and security concepts. These conceptual difficulties amplify risk – both its perception and reality – for users in the identity ecosystem.

Trustmarks can assist with:
Trust
Risk reduction
Search cost reduction
User performance
Lightweight business negotiations

Trustmarks help to reduce the perception of risk by signalling individuals and organizations that an entity has been assessed against a set of relevant risk-reducing criteria. While self-assessment is certainly a valid method of managing trustmark awards, risk is potentially better mitigated by external assessment from an organization whose reputation is based on sound and thorough methods. For the identity community, B2B risks include weak security, poor privacy and operational policy compliance, incomplete technical interoperability, and brand damage from errant partners. B2C risks include inadequate stewardship of personal data, poor usability and poor problem resolution. Many of these risks can be addressed by certification regime components: interoperability testing, security evaluations, privacy and operational audits, user-centric design requirements, and customer support requirements. External assessments add an additional layer of confidence that certain risks have been addressed by a competent body. Trustmarks signal this confidence in a simple visual way.

Search Cost Reduction

Selecting a business partner or, in the B2C case, an identity provider (IDP), entails search costs. Citizens invest time and business representatives invest time, corporate resources and money. Most discussions of the identity ecosystem envision a plurality of players, so the field of possible choices in a given market may be large. As such, search costs are not trivial. Furthermore, given the information asymmetries noted above, consumers may need

assistance in selecting identity providers from a group that could appear undifferentiated or otherwise opaque.

Trustmarks are a strategy to reduce the cost and time of searching for a service provider or partner. By signalling conformance with standards, requirements or privacy norms, citizens and business representatives can quickly reduce the search space of possible organizations. Consider the B2B case where internal or external requirements force the need to contract with a partner who meets particular legal or technical standards. Trustmarks reduce the list of possible partners through visual shortcuts. In the B2C case, citizens can assuage some of their privacy concerns by quickly identifying identity providers that have been certified to handle personal data responsibly.

Trustmarks show users where they can use their existing credentials

The above discussion relates to an initial contact with service providers or partners. Trustmarks serve an important function, though, after enrollment or first time engagement. **They enable users to rapidly identify where they can use their existing credentials.** A simple example of this is the VISA logo: it signals to consumers that a merchant will accept their existing credit cards. In the identity ecosystem, citizens already face a great deal of information and challenging concepts. Trustmarks help move the authentication process along by quickly pairing users with service providers who accept their credentials. An example of this is eHerkenning, the Dutch authentication system for employees of private sector organizations that do business with the government. An eHerkenning logo indicating a required level of assurance appears on identity provider and relying party sites, signalling both the general ability to log in plus a more granular requirement.

The Dutch eHerkenning logo and possible levels of assurance

User performance

The complexity of identity interactions and their underlying user experience design are a well-known challenge for the identity ecosystem. Usability is of prime concern because if users become confused or scared by identity systems, they will use them incorrectly or not at all. User research experts measure users' 'performance' – how effectively they complete a given task.

The conceptual complexity of online identities and the perception of privacy and security risks have an effect on user performance. Trustmarks can play a role in improving performance when users interact with authentication systems.

Users struggle with IDM concepts leading to stress and poor performance when interacting with ID systems.

According to Pete Gale of GDS, citizens struggle with the "alien" concepts of identity management:

> "ID concepts are coming thick and fast; users are on the backfoot. People know that they have to protect their identity, but here we're asking them to share personal information with companies to do so. Further, they don't understand private companies' roles in this context."

A key consequence of this struggle is stress, which translates into poor performance. **Recognition and understanding about how something works reduce stress and improve performance.** Moreover, some eGovernment interactions may be inherently more stressful, such as those that involve benefits or unemployment payments. A trustmark is a recognizable landmark in an otherwise complicated landscape. Here, the orthodoxy of the need for trust in online interactions is borne out by empirical research and experience. Pete Gale notes:

Trustmarks can help improve user performance.

> "Users thinking 'I've been through this before' helps to reduce stress. **With the trustmark comes consistency of interaction and behavior.**"

This insight not only adds another dimension to the utility of trustmarks, but it also implies the vital need for user testing of identity management systems. Too often, user design needs are assumed rather than researched. Citizen IDM systems tend to begin life as policy or commercial initiatives, but the final product is a system intended for use by people of a wide range of technical aptitudes. Trustmarks are but one potential answer within a large set of questions concerning the effective design of identity and attribute management systems.

User design needs are often assumed rather than researched.

Lightweight Business Negotiations

Trustmarks enable organizations to enter into lightweight business negotiations. They shortcut the compliance and risk management components of due diligence and contracting. Trust frameworks (explained further below) exist in part to ensure compliance with a community's requirements but avoid bilateral agreements and compliance between the players. Trustmarks, lists and registries are evidence that an organization has been assessed against criteria that another organization requires to do business with them. For example, US federal agencies have been ordered to accept credentials from identity providers external to the government. The Federal Identity Credential and Access Management (FICAM) committee works with trust framework providers to assess identity providers against federal technical, operational and privacy requirements, resulting in a trustmark and/or being placed on a trust list. Federal agencies can then enter into business arrangements without concerning themselves with the requirements or assessments.

4. Governance

Key Governance roles:

Origin of requirements
Certification authority
Trust framework
Mark user / Licensee
Assessor
Enforcement body
Audience for the mark
Marketing

Governance is the beating heart of trustmarks. The following roles are central to the governance and use of trustmarks. In existing mark schemes, these roles overlap and often one entity serves in multiple roles. The roles reflect the major constituent parts of a complete mark scheme.

Origin of requirements

Marks and seals are awarded when an entity is determined to meet a set of requirements. These requirements can originate from various sources: certification bodies, legislatures, regulatory authorities and administrative bodies, and others. These sources can be closely or loosely coupled with other roles within a mark scheme.

Certification authority

This entity has primary responsibility for certifying that an applicant entity conforms to a set of requirements. The authority may be the origin of the

requirements or may only be responsible for promulgating them. They may assess applicants directly, retain assessors, or oversee assessment criteria for third-party or self-assessment. The certification authority may perform or facilitate enforcement; they may monitor compliance or manage the complaint process.

Trust framework

A trust framework is a flexible concept whose definition is not fully agreed upon by the IDM community. It has been used to refer to group of stakeholders who collaborate under a single banner to create, manage and certify against a set of requirements pertinent to a community of interest. More restrictive definitions hold that a trust framework is just the set of requirements that applicants are certified against; certification is then managed by 'trust framework providers.' A 'trust framework operator' has an infrastructural component – providing the technology (e.g., metadata) to connect various certified players and services. The broadest definition of a trust framework is that it is a set of 'rules and tools' for a given set of relationships.

The Kantara Initiative certifies IDPs via independent assessors. Certified companies are placed in a trust registry.

A key example of the first definition is the Kantara Initiative, who, among other things, facilitates the certification of companies who wish to supply identity services. In American IDM policy, IDPs must conform to national requirements created by the US FICAM committee. Kantara ingested the FICAM rules and created a set of criteria for applicants to be assessed against. Independent assessors use these criteria to determine an applicant's conformance. Successful applicants are placed on Kantara's 'trust status list,' a registry of approved providers. A trustmark is not awarded per se, but applicants can indicate that they are certified to a particular level of assurance. For example, a webpage for Verizon Universal Identity Service displays, "Certified to meet Identity, Credential and Access Management (ICAM) Level 3 requirements."

Kantara did not originate its certification requirements; FICAM did. However, Kantara (with input and approval from FICAM) originated the actual assessment criteria. Kantara maintains both its trust status list and the infrastructure that allows technical validation of approved entities. This means that Kantara can also act as an enforcement mechanism by removing an entity's visible and technical certification. Kantara is broader however than these activities, and represents other communities besides the identity management sector.

Mark User / Licensee

This is the entity seeking to use a certification mark or trustmark. In the case of self-certification, the user awards itself the mark. In the case of external certification and depending on the legal regime, the user licenses the mark. In the case where no mark is awarded, the user may be placed on a registry.

Assessor

The Assessor is the person or group who examines products, processes or organizations for adherence to a certification scheme's requirements. In the case of self-assessment, this may be an employee of a company intending to apply a trustmark to one of its products. For third-party assessment, this could be a certification body's own inspectors or independent examiners working in service of a body or a law. In the case of peer-to-peer assessment, the assessor is an accredited member of the community in which the trustmarks are awarded.

The Enforcement body has two sub-roles: the complain function and the enforcement action.

Enforcement Body

The enforcement body is the entity or entities responsible for taking corrective action when a mark user has breached some requirement. There are two sub-roles to consider:

Complaint Function

Complaints can flow from several sources, implying multiple layers of administration that lead to an enforcement action. Complaints can originate from the public, assessors, peers, regulators and certification bodies. The

complaint processes is therefore a critical piece to consider in the development of a mark's governance – who has the right to complain, who receives those complaints, how are they reviewed before being proceeding to an enforcement stage? Complaint implies **monitoring** – this could be accomplished in a passive way, relying upon identity system users, business partners, scheme participants or others to raise a complaint. Or it could be active, in form of periodic audits performed after an initial certification, or through technical means. Both cases require a formal process to determine the validity, nature and scope of a complaint.

Enforcement Action

The entity enforcing a sanction against a violator may be the same as the one receiving or generating the complaint. However, other arrangements are common, the key one being the use of courts. In the US and UK, for example, rogue uses of trustmarks can be addressed in the same way as rogue uses of trademarks – by bringing legal action against the rogue user. US and UK trademark law disallow use of a mark by those who have not been licensed, and allow mark licensors to start infringement cases against them.

Audience for the mark

Trustmarks schemes may need to consider Marketing to improve recognizability and for damage control in case of brand injury.

This is the 'consumer' of the mark. As discussed in the Use Cases section above, generally this is an individual citizen or representatives of an organization. In the case of machine-readable trustmarks, one could say that a computer system is the audience for a mark.

Marketing

While not strictly related to the operation of a mark or certification scheme, respondents for this research have cited marketing as a salient consideration for both the long-term confidence in a trustmark and to do damage control when problems arise. Marketing teams help to communicate the value of a mark and increase its recognizability. In some private schemes, such as Symantec's Norton Secure trustmark, the mark issuer has a say in who gets to display the mark after a consideration of an applicant's brand compatibility. In

the case of damage to a trustmark's brand in the wake of a negative event by a mark user, marketing teams may become involved to minimize damage to the rest of the trustmark scheme.

5. Legitimacy and Confidence

Legitimacy and confidence are not naturally occurring - they must be cultivated and maintained over time.

Trustmarks can accomplish their intended tasks only if they are legitimate and people have confidence in them. These two qualities, though, are not naturally occurring – they must be cultivated and maintained over time. One scholar defines legitimacy as follows:

> "Legitimacy is a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions." (Suchman, p. 574)

With respect to certification and trustmarks in the identity ecosystem, these traits can be said to contribute to the legitimacy of a marking scheme:

- it is backed or mandated by law
- it has approval from a public authority
- scheme components are derived from legal or policy principles
- the scheme is based on community standards or codes of conduct
- equitable involvement of stakeholders, including citizens
- accountability of participants
- transparency of governance

Emerging identity systems around the world embrace these traits to greater and lesser degrees. They are a core set of principles that can be incorporated into certification schemes to help ensure willing user participation and overall integrity.

Legitimacy and confidence are not the same thing. Legitimacy emerges from institutional or structural characteristics, while confidence emerges from use.

Confidence is a similar though distinct trait. Legitimacy emerges from institutional or structural characteristics of a marking scheme, such as its basis in law, certification requirements or its governance. Confidence, on the other hand, is a quality that emerges from use of a system. Identity ecosystem stakeholders identified a number of ways to build and maintain confidence in

a trustmark. Some of these strategies are applicable to the mark and its governance while others apply to the organizations who display the mark.

Strategies to build confidence in trustmark schemes:

Consistency
Reliability
Clarity
Recognizability
System integrity
Meaningful enforcement
Problem resolution
Active engagement with the field
Improvement in mark usability

- **Consistency:** Certification assessment must be performed consistently across scheme participants and over time.
- **Reliability:** Scheme participants and their systems must function reliably. User research shows that people heavily bias their evaluation of a company based on their last interaction with it.
- **Clarity:** Information about why a trustmark is displayed, what it means, as well as the explanation of how a service functions must be clear. Particularly in the B2C case, confusing, opaque or overly technical language can hinder confidence.
- **Recognizability:** Marks and/or their originating organization must be recognizable. Identity systems' look and feel should be consistent across providers and contexts.
- **System integrity:** Security measures should be built into the mark to prevent fraudulent use.
- **Meaningful enforcement:** Rogue mark use or scheme members who violate certification criteria must be subject to meaningful enforcement.
- **Problem resolution:** When something goes wrong, there are mechanisms to address it.
- **Active engagement with the field:** The trustmark organization should be actively and visibly engaged in the wider field that its trustmark addresses. Engagement can revolve around communications, such as newsletters and customer education, or can be focused on evolving the space itself, such as through policy advocacy. These types of engagement signal commitment to the field, community investment and longevity.
- **Improvement in mark usability:** Trustmarks may not be perfect when they're first instituted. A mark can be evolved over time to improve its usability and utility.

6. Key Findings and Considerations

Interviews with identity ecosystem stakeholders have yielded the following findings:

Recognition of a trustmark is essential for it to have any value. Trustmarks should be anchored within an organization that mark audiences have a previous, positive connection with. Marketing efforts and mark use designed to improve recognizability are critical. The converse of this is that a new trustmark whose originating organization has no history behind it adds no value.

Enforcement is a vital element of a mark scheme. For the mark to have value, it has to be policed. A mark's utility stems from it reliably indicating that a mark user is conformant with given requirements. Operational, policy and best practice compliance are often invisible to citizens and business partners – ongoing proof of compliance can only be maintained by complaint, audit and enforcement processes. They not only maintain participant conformance, but also ensure the integrity of the overall mark scheme.

Too many trustmarks will confuse people. The conceptual challenges of online identity, privacy and security are amplified by an overabundance of trustmarks. Too many marks or too much granularity hinder rather than help users' decision-making processes.

Trustmarks and brands appearing in the same place interrelate. People will draw inferences, rightly or wrongly, about relationships between trustmarks and brands. This could be positive or negative. A relatively unknown brand could positively borrow reputational capital from a known trustmark; a trustmark may become more trusted and recognizable from association with a well-established brand. Similarly, a publicized breach of a trustmark scheme participant may reflect poorly on the scheme as whole; or, an unknown trustmark on a known brand's site may be seen as a cynical attempt to garner trust.

In addition to the findings above, interviews and literature yielded the following considerations and questions regarding the creation and use of a trustmark scheme:

Necessity

- Is the mark actually necessary? The impulse to create a marking scheme – and all the organizational overhead that entails – should not be uncritically embraced. A centrally controlled trust registry may suffice, reducing the need to monitor for rogue use. Or, perhaps no externally-facing scheme is needed at all. Some functions in an identity system may not appear in the absence of an entity's certification. For example, an identity provider would not appear in a citizen IDM system unless several layers of assessment have occurred. Perhaps the fact that an IDP appears at all is sufficient to indicate conformance with the IDM system's various requirements.

- Who is being certified? Does each party need certification? Will they each be subject to the same certification type (self vs. third-party)?
- What problem is being solved by the trustmark? What is the 'trust threat' being addressed? Is it merely assumed to exist, or has that assumption been tested with the intended mark audience?

Audience

- Who is the audience for the mark? Is it a citizen or a business representative? What is her or his technical aptitude? Who receives the value of the trustmark?

Usability

- Where does the mark appear? Does it appear on every page of the user journey, or does it appear at only specific, contextually appropriate places?
- What, if anything, does the mark link to? Is it a dynamic mark, changing its appearance at different times or on different sites?
- Has the mark use undergone user testing? Is the mark doing what was intended? Does it affect user performance?
- Are expectations about users' willingness to learn about what a mark represents realistic?
- How are mark users and mark audiences notified about substantive changes in the marking requirements?
- In the B2C case, is the language used simple, consistent and free of technical jargon?

Culture

- Will a target mark audience respond better to government issuance of a mark, private industry, non-profit organizations, a consumer group, a standards body, a security agency?

Risks

- There is a great deal of evidence that when citizens notice marks they influence their choices. This means that mark schemes must be used cautiously with great attention paid to their long-term legitimacy.
- What happens when something goes wrong? Will user reliance on trustmarks translate into assistance with data and usability issues, questions and problem fixing?
- Trustmarks with poor enforcement or declining confidence render the mark meaningless.

Governance

- Does policy or law exist that requires adherence to or use of a trustmark? If not, should it be proposed?
- How much should a government entity set the operational environment for trustmarks?
- What sustains the governance of a trustmark over time? That is, what keeps the participants coming back year after year to review, augment and adapt the mark scheme? If there are political changes in the environment, will the mark's governance be affected? How is the mark organization funded?

- Is mark conformance governed by technical or non-technical means? Is monitoring automatic or does it require an audit or complaint process?
- Are the marks self-authenticating or do they require additional mechanisms to show validity, such as a trust registry?
- In the case of a hub architecture, how does the trustmark interact with the hub technically, contractually and with respect to governance?
- How will scheme participants be sanctioned if found to violate the certification requirements?
- Is there a conflict of interest between mark issuers and receivers? For example, when trustmark organizations are paid by mark users, those organizations may be loathe to enforce or publicly acknowledge violation of the mark requirements.
- Are there legitimacy or other concerns about the public or private nature of a mark's governance?
- Does the mark raise regulatory costs for private organizations? This may be a source of friction. If a mark scheme is governed in part or whole by private organizations whose costs may rise, questions of independence must be considered.
- Can parts of the governance structure be borrowed from other existing certification schemes?
- What does the 'steady state' of a mark scheme look like? That is, what does a mature mark scheme look like with respect to its governance?

Cost

- What does it cost to administer a mark? What will it cost in five or ten years?
- What does it cost to obtain a mark? In the case of private organizations, where are those costs recovered?

Legitimacy and Confidence

- How are legitimacy and confidence to be maintained over time?
- Are there ongoing outreach or marketing efforts? What is the level of investment required to ensure recognition and positive association?
- How does the certification authority adapt to a changing policy, technical and user awareness landscape?
- How will the mark scheme and its participants recover from damage to the mark's brand?

Relationship to brand

- How does a trustmark and the 'host' brand of the mark user interrelate? Does the association confuse the user?
- Too many trustmarks hinder rather than help decision-making.
- How does the brand value of a mark increase over time? That is, how can the mark be evolved to do its job better and become more recognized?

Liability

- Does use of the mark and/or compliance with the underlying certification yield a liability shift?
- Could a liability shift be used as an incentive to increase trustmark usage?

Relationship with other trustmark schemes

- Can value be drawn from relationships with other mark schemes? This could help by giving history, context or positive associations from previous successful initiatives. Can trust be 'borrowed' from an existing certification scheme?
- Is there a possibility for re-use or extension of the trustmark as other players enter the ecosystem? For example, some identity management systems only apply to eGovernment but plans exist to extend them into the private sector. Can trustmarks used in the first context be adapted and extended into the second? What additional steps would be needed?
- Can an unrelated regulator rely upon a trustmark? Is the certification scheme robust and transparent enough for an unrelated regulatory authority to easily trust the processes for its own needs? One example is age verification. Identity providers are certified as to the quality of their ID proofing and vetting processes, enabling trust in certain key attributes like age. How can an authority who has no relationship to the certification bodies or processes transitively trust the age assertions of certified identity providers? What bridges the regulatory processes?

7. Further Reading

EHerkenning (in English): https://www.eherkenning.nl//eRecognition

European Consumer Centres' Network, "Trustmarks Report 2013 – 'Can I Trust the Trustmark?'": http://ec.europa.eu/dgs/health_consumer/information_sources/docs/trust_mark_report_2013_en.pdf

European Union Agency for Network and Information Security, "On the security, privacy and usability of online seals: An overview": https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/on-the-security-privacy-and-usability-of-online-seals

GTRI NSTIC Trustmark Pilot, focused on modularity and machine-readable trustmarks: https://trustmark.gtri.gatech.edu/

NSTIC Trust Framework and Trustmark Committee wiki: https://www.idecosystem.org/wiki/Trust_Frameworks

Rodrigues, R., Wright, D. and Wadhwa, K. (2013). Developing a privacy seal scheme (that works). *International Data Privacy Law, 3*(2), 100-116.

Interview Subjects

The following people graciously contributed their time to be interviewed for this paper.

Elinor Hull and Diane Joyce, UK Post Office
Pete Gale, UK Government Digital Service
Zia Hayat, Callsign
Richard Trevorah, tScheme
Justin Basini, Zapp
Richard Hobday, Gov.uk
Marcel Wendt, Digidentity
Jeremy Grant, NIST
Mike Garcia, NIST
Paul Agbabian, Symantec
Scott David, University of Washington
Tom Smedinghoff, Edwards Wildman
Matt Stroud, ee
Brian Moore, Experian

References

Aiken, K., Liu, B., Mackoy, R. and Osland, G. (2004). Building internet trust: signalling through trustmarks. *International Journal of Internet Marketing and Advertising, 1*(3), 251-267.

de Bruin, R., Keuleers, E., Lazaro, C., Poullet, Y. and Viersma, M. (2005). Analysis and Definition of Common Characteristics of Trustmarks and Web Seals in the European Union. Available at http://ec.europa.eu/consumers/cons_int/e-commerce/e-commerce_final_report_en.pdf

European Commission. (2012). EU Online Trustmarks: Building Digital Confidence in Europe. Available at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1815

Intellectual Property Office. (n.d.). Certification and Collective Trade Marks. Available at https://ipo.gov.uk//tmmanual-chap4-certcoll.pdf

Kirlappos, I., Sasse, M. and Harvey, N. (2012). Why Trust Seals Don't Work: A study of user perceptions and behavior. In: S. Katzenbeisser, E. Weippl, L. Camp, M. Volkamer, M. Reiter and X. Zhang (Eds.) *Trust and Trustworthy Computing*, pp. 308-324. Available at http://discovery.ucl.ac.uk/1353955/1/Kirlappos_Trust_2012.pdf

McKnight, D., Kacmar, C and Choudhury, V. (2004). Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business. *Electronic Markets, 14*(3), 252-266.

Rodrigues, R., Barnard-Wills, D., Wright, D., De Hert, P. and Papkonstantinou, V. (2013). EU Privacy seals project: Inventory and analysis of privacy certification schemes: Final Report Study Deliverable 1.4. Available at http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf

Suchman, M. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of Management Review, 20*(3), 571-610.

Temoshok, D. (2014). TFTM 01-06: Conformance Program Discussion [slide deck]. Available at https://www.idecosystem.org/idesgwiki/images/b/b6/TFTM_Conformance_Program.pptx

US Patent and Trademark Office. (2013). What is a certification mark? Available at http://www.uspto.gov/faq/trademarks.jsp#_Toc275426676

Glossary

Attribute provider: (AP): Supplier of verified attributes about a person, such as age or licensure
Credential: A token containing identifying information that can be used to access a service
Data brokerage hub (Hub): A system architecture where a centralized infrastructure brokers identity and attribute interactions between various parties
Government Digital Service (GDS): UK agency responsible for citizen identity initiatives
Identity provider (IDP): Supplier of identity credentials and services
Identity Management (IDM): An operational and technical framework that defines and administers the lifecycle, use and security of digital identities
NSTIC: US National Strategy for Trusted Identities in Cyberspace
Trustmark: A mark used to indicate that a product or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority
Relying party (RP): An organization that relies on the assertions of identity and attribute providers