OIX – GUIDE TO TRUSTMARKS

April 2021

Version 1.2

Authors: ID Crowd, Nick Mothershaw

DOCUMENT HISTORY

Version	Date	Key Changes	Author
1.1	February 2021	Initial Issue	ID Crowd
1.2	April 2021	Additional guide contents produced as a result of discussing Trustmark implementation with OIX members in the context of the UK Trust Framework	Nick Mothershaw

TABLE OF CONTENTS

1. SUMMARY

This paper considers the use of a Trustmark[1] in the context of an identity Trust Framework that has been designed to facilitate the creation and ongoing use of trusted identities and attributes amongst the participating entities within it.

It explores the emerging assumptions from previous OIX working groups:

- a Trustmark must clearly identify the Trust Framework or scheme that underpins it
- it must be clear who provides which products or services and where they can be used
- it must be clear how to get help when there are problems
- it must be clear how to escalate complaints if required

And considers recommendations for how Trustmarks could be used across two main user groups:

- **end users** need to both be and feel safe and secure when transacting with organisations
- **participating organisations** must clearly define liability when working with other organisations

[1] https://openidentityexchange.org/networks/87/item.html?id=92 builds on the 2014 OIX white paper: Trustmarks in the identity ecosystem - definitions, use and governance, Dr Gilad L. Rosner.

2. WHAT IS A TRUSTMARK?

A Trustmark is a recognizable signal that a Trust Framework is in operation. The signal could be a phrase or word but is typically a symbol or logo that is easily recognizable.

A Trust Framework is a common set of agreed requirements, activities and responsibilities for participating entities, underpinned by law. It facilitates trust within a robust, secure, scalable and privacy-enhancing ecosystem enabled by entities that are certified to conform to these requirements.

It's in the name - a Trustmark indicates that a product or service can be trusted :

- it provides a human visible record that can help to convey confidence, reliability and / or safety to both individuals and organisations
- It can be an effective way of informing and empowering people, whilst promoting transparency, accountability and responsible practice
- it could potentially provide access to additional information about what the Trustmark offers each party in the transaction including which systems are in place to reassure users that they will be protected when entering personal information and completing transactions.

However, as the definition and use of Trustmarks can be varied and many, trust in a specific Trustmark is engendered through certification against a set of requirements, covering a multitude of criteria including privacy, technical, operational and business policies, that are specific to that Trust Framework. Both the type of assessment and certification, of participating organisations, can vary between self-assessment and assessment by an independent third party as can the overarching governance of both the initial certification and the ongoing compliance.

So, what should be considered when designing and implementing a Trustmark? Identifying trustworthy products or services is a significant challenge and a Trustmark could help organisations to better inform and protect users and facilitate transparency, accountability and best practice. Trustmarks can help users make more informed decisions about what they buy e.g. the Gas Safe Register is a legal requirement for all gas engineers[2]; McAfee Secure[3] indicates a website is free from viruses or malware. The Fairtrade certification label[4] requires "companies to pay sustainable prices (which must never fall lower than the market price)." This helps to ensure fair and sustainable terms for workers in the developing world. These Trustmarks enable consumers to make informed choices about which products or services they choose to buy or use.

---

[2] The official list of UK gas businesses registered to work safely and legally. https://www.gassaferegister.co.uk/

[3] https://www.mcafeesecure.com/

[4] https://www.fairtrade.org.uk/what-is-fairtrade/

The eIDAS EU trust mark[5] indicates to users they can use their national ID to access public sector services across borders within those EU member countries that have been successfully peer reviewed.

- it identifies clearly qualified services provided by qualified trust service providers (QTSPs)
- it guarantees a service meets the requirements of eIDAS Regulation (EU) No 910/2014
- it assures users online transactions will be safe, convenient and secure
- it must be published, by QTSPs, via a link on their website to the relevant trusted list

[5] https://ec.europa.eu/digital-single-market/en/eu-trust-mark

3. TRUSTMARKS - WHO ARE THEY FOR?

3.1 Individuals (users)

For individuals a Trustmark MAY help:

- with understanding of what a Trust Framework enables them to do
- facilitate recognition of which services they can use
- build trust in organisations[6] they transact with, knowing they have undergone rigorous checks
- address concerns around security, safety and privacy
- provide confidence that there is a method of redress

3.2 Organisations

It is important for relying parties to know that organisations providing products and services:

- can be easily shown to conform to initial requirements (certification of onboarding)
- can be easily shown to conform to ongoing requirements (operational conformance)
- can be easily shown to be liable if they do not meet the requirements (non-conformance)
- have undergone a series of rigorous checks and there is a process for redress
- are all part of a level playing field and can be distinguished from other suppliers - knowing what "good looks like" in order to decide from whom to buy services
- can more easily achieve certification by creating a standards based service marketplace and enabling more frictionless and cheaper trade through organisations being compliant "at cost"

[6] Relying Parties, IDPs and Brokers and Evidence Verifiers

4. TRUSTMARKS - CONSIDERATIONS

4.1 Purpose and legitimacy

What is the mandate that is indicated by the Trustmark? It is important to clearly explain whether the purpose of the Trustmark is quantitative or qualitative. For example, the European CE mark[7] is an indicator that a product, service or company meets environmental, health and safety standards of the European Economic Area (EEA), however it does not indicate where it was made. Conversely a *"Made in the UK"* product shows where it was manufactured but does not provide any indication of quality[8].

4.2 Digital products and services are complex and certification is costly

Compared to products or services that have a single use, no moving parts like a screwdriver, solutions using identity are multi-faceted and complex. As Trust Frameworks are comprised of requirements across many different areas,[9] assurance and certification for participating organisations is a comprehensive process that can be commercially prohibitive, even for larger companies, unless there is a clear business case to prove the return on investment.

- The proper creation and operation of Trust Frameworks ensures that all participating organisations must conform to the requirements set by a scheme.
- Conformance is performed and assessed throughout all processes from the onboarding of an organisation, through its operation and ultimately offboarding should it become non-conformant.
- Governance is typically provided by both operators of a scheme and independent third parties with the opportunity for redress if required, with clear liabilities and potential penalties that are enshrined in law.

And as the overhead of creating and maintaining a Trustmark can be additionally onerous and expensive it begs the question: are Trustmarks needed?

4.3 Do Trustmarks make more sense for end users than organisations?

Do Trustmarks offer some form of reassurance, a tangible cue, to first time users to build initial trust or when trying to build a new market with nascent services and less well-known providers, such as micro businesses or intermediaries like brokers and aggregators? Has research shown this requirement changes over time? Are Trustmarks only necessary for new or less well known products or services? Could a single, good customer experience also help convince consumers to make further purchases, and can this be achieved without a specific Trustmark? There is evidence to suggest that end users are more likely to continue with a transaction if they recognise a Trustmark, which is explored later in this paper.

---

7 https://ec.europa.eu/growth/single-market/ce-marking_en

8 Requirements for MakeitBritish focus on what percentage of a product has to be manufactured in the UK https://makeitbritish.co.uk/member-verification/

9 OIX Guide to Trust Frameworks - https://openidentityexchange.org/networks/87/item.html?id=365

What benefit do participating organisations derive from a Trustmark that isn't already inherent in the Trust Framework that underpins it? Is there a danger that a Trustmark would mean more time spent on branding when certification and compliance is what all participants actually benefit from? Isn't it worth more to the identity ecosystem to ensure organisations focus on meeting the requirements of the Trust Framework?

The need for legitimacy, limitation of liability and commercial realities indicate that this is less of a requirement for organisations. This is particularly relevant in the private sector where organisations additional overheads are typically engineered out of a proposition to minimise investment, operational expenses and maximise profit. The Georgia Technical Research Institute, sponsored by NIST[10], created a technical framework for Trustmarks[11] that uses machine-readable, cryptographically signed digital Trustmarks, that are an "official attestation by a Trustmark Provider of conformance". However, again the added complexity and cost are likely to be an inhibitor for organisations, especially if they are already participants in a Trust Framework that already supports these needs.

4.4 Perceived reduction of risk but recognition and brand confusion

Recognition plays a large part in the effectiveness of Trustmarks. One eCommerce study[12] found the majority of users sampled indicated they would not continue with a transaction if they did not recognise the logo or if there was none. Research from Actual Insights[13] showed that while Trustmarks can help build perceived trust, only a few are instantly recognisable. A further study on recognition and understanding of Trustmarks, found that online shoppers trust Trustmarks even if they don't recognise them, and a fake Trustmark, created for the study, was actually recognised above ones that actually existed[14].

Recognition can also help to answer some key questions that users have such as "do I feel safe continuing with this transaction?", or "can I use the identity 'thing' I already have, to complete this transaction quickly and easily?" Users really just care about "getting something done", everything else is a minor consideration for most transactions. The first question is often satisfied by a positive result to the second question.

Care should be taken not to introduce too many *Trustmarks* or brands that support them to avoid confusion. The UK public sector digital identity scheme GOV.UK Verify is a case in point, when at its peak, there were eight private sector IdPs with either their own brand identity or one specifically created for GOV.UK Verify, a Verify logo, a certified company logo and the logos associated with the service an end user was trying to use. Clarity of purpose is critical and as the old adage goes, "too many cooks spoil the broth."

---

10 https://Trustmark.gtri.gatech.edu/

11 https://Trustmarkinitiative.org/specifications/Trustmark-framework/1.4/tfts-1.4.pdf

12 survey conducted by eBusiness Guru

13 https://web.archive.org/web/20111009234446/http://www.actualinsights.com/2011/trust-logo-recognition-precedes-presence

14 https://idw-online.de/de/news714155

4.5 The need for variability in Trustmarks

It is important to design a Trustmark that is simple enough for users to understand, while still conveying meaningful information about dynamic and complex digital technologies. Conveying the necessary detail has to be balanced with user simplicity and understandability.

The dynamic nature of digital products and services means that they will inevitably evolve over time, not in the least due to ever changing requirements to mitigate risks and threats and streamline user experience and interaction. A Trust Framework provides the necessary assurance that any changes fulfil the underlying requirements.

But how can more nuanced or variable differences be reflected? As the products and services in the identity ecosystem are constantly changing and evolving to both mitigate risks and threats and improve the user experience it might be difficult to convey a real-time status of certification. And as this status can also potentially be more nuanced, for example if more information is being included and communicated (i.e. LOA or sector applicability) perhaps the additional details and complexity of real-time certification status, LOA or sector applicability may result in more confusion for users.

Simplicity in messaging is perhaps the best approach - just enough information for users to recognise the signal but not too much that could inhibit understanding of what is being conveyed. Let's explore some examples of where simplicity has been effective:

No Trustmark but messaging to convey certification to a particular level of assurance - in the US IdPs must conform to national requirements originally created by the US FICAM15 committee, where there are different variants of certification. However, although assessment of IdP conformance is performed by independent assessors[16] no Trustmark is issued but successful organisations can indicate that they are certified to a particular level of assurance as defined by NIST special publication 800-6317.

Visible display of issuer, scheme and type of payment card - while all three signals could be the same depending on the scheme there are clear differences when this is not the case. For example, some schemes offer both credit and debit cards and clearly indicate which is which. This provides an unambiguous signal to the consumer that either debit payments will be taken directly from an account or credit payments will be borrowed with payment, and potentially interest, intended to be made at a later date. Other information about payment protection using credit cards is not obvious without explanation which emphasises the need for comprehensive user education essential to ensure that this information is clearly understood.

A single Trustmark displaying a certified service by a trusted service provide - TrustMark[18] is a UK Government Endorsed Quality Scheme, underpinned by BEIS[19], that gives consumers

---

15 https://arch.idmanagement.gov/

16 who themselves have been accredited by the Kantara Initiative (https://kantarainitiative.org/)h

17 https://pages.nist.gov/800-63-3/sp800-63-3.html

18 https://www.trustmark.org.uk/aboutus/what-is-trustmark

19 The UK Department for Business, Energy and Industrial Strategy

increased confidence and choice in the trades they choose to complete building work around their home. The TrustMark scheme provides an overarching, light touch framework to allow existing government trusted schemes e.g. Fensa to enable registered businesses in their schemes to be thoroughly vetted in order to meet both their own and the TrustMark framework operating rules and thus become “trusted service providers”.

4.6 Proactive marketing or organic adoption

As with all nascent services, adoption is a key fact that must be considered. How can it be made as easy as possible for users to be made aware of the possibilities and potential of any service without proactive advertising and marketing of what the service is capable of, where and how it can be used. The old adage of build a service and users will come does not apply. There must be a compelling reason for a user to use a product either an essential need or a burning desire. If there is no motivation or driving need then users will follow the path of least resistance.

Organic growth can sometimes be achieved but only if the proposition is compelling enough. This can transform users into advocates[20] who tell their friends and spread the word via social media. Of course if there are issues with the service or support thereof, then the same advocates could equally become detractors.

As the use of a Trustmark will necessitate certification to the requirements of a Trust Framework by potentially both the operator of the scheme as well as an independent assessor there exists a mutual interest between all parties to ensure that both the messaging and more importantly the operation is performed well. This in turn means that in addition to a provider advertising their own ability to provide services using a Trustmark there is also benefit to be gained in a mutually advantageous coopetitive[21] strategy to provide a joint marketing campaign so that a marketplace can be developed and to avoid one or more participants providing a poor service and ruining the opportunity for all.

Marketing is essential to ensure that people are aware - I don’t know what I don’t know. But the best strategy is to ensure this activity involves all stakeholders: providers to advertise the service potential perhaps with some bespoke differentiation to encourage users to choose them over others; relying parties consuming these intermediary enabling services and the users themselves by offering compelling services and encouraging users to become proactive advocates.

4.7 Interoperability

While interoperability between entities in a Trust Framework is implicit in the requirements that organisations must meet in order to participate, the aspiration for interoperability across borders and / or sectors is complex and in the short to medium term any future reality is therefore likely to consist of many Trust Frameworks, schemes and Trustmarks.

---

[20] Net Promoter score (https://en.wikipedia.org/wiki/Net_Promoter)

[21] Coopetition - a cooperative strategy with the competition https://en.wikipedia.org/wiki/Coopetition

While a single Trustmark already exists across nations in the eiDAS Trust Framework, which enables the use of Government created identities to be used across the public sector, it is essentially underpinned and supported by individual Governments.

In the private sector this level of liability is unlikely to be achieved, in the near term, across either individual or all sectors. It is more likely that commercial realities will mean that the sector specific dominant Trust Frameworks or schemes will emerge to become the recognisable brand in a sector. This is to be expected as the cost of creating a Trustmark is expensive and could become a burden in a competitive marketplace.

4.8 One or more Trustmarks

It is perhaps inevitable that, across the private sector, different schemes, brands and Trustmarks will emerge specific to individual sectors. Commercial realities will mean that some schemes will prevail and ultimately, we may see different schemes or even companies and brands merging.

Future mergers of competing schemes are likely to follow similar developments to the Payment Card Industry Data Security Standard[22] (PCI DSS) that was formed by the five major payment card companies who enforce the standard[23]. The capital expenditure and ongoing operating costs to support a single scheme are high therefore it made sense to create a common set of standards that provide the appropriate level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data. This trust framework is enabled by ongoing compliance assessments that vary in terms of complexity and rigour according to the number of annual transactions. This allows merchants of different sizes to provide compliant services to consumers.

Mergers could well be within specific sectors as well as across different sectors. For example, it may be relatively straightforward to standardise schemes in one sector i.e. a strictly regulated sector such as financial services while it may be more complex to create equivalence across sectors with very different regulations or requirements. This aspiration has been an ongoing challenge in the UK public sector with much discussion, exploration and moves to influence change with the JMLSG[24] to achieve equivalence between GOV.UK Verify[25] in the public sector and TISA[26] in the financial services sector.

However, the need to meet different requirements, whether this be to align with sector specific regulations or to meet commercial pressures may be difficult. So there may be a period of time where many, potentially competing or overlapping schemes exist. Unfortunately this scenario could cause confusion and distrust among both end users and organisations that are consumers of identity.

---

22 https://www.pcisecuritystandards.org/

23 American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc

24 https://jmlsg.org.uk/

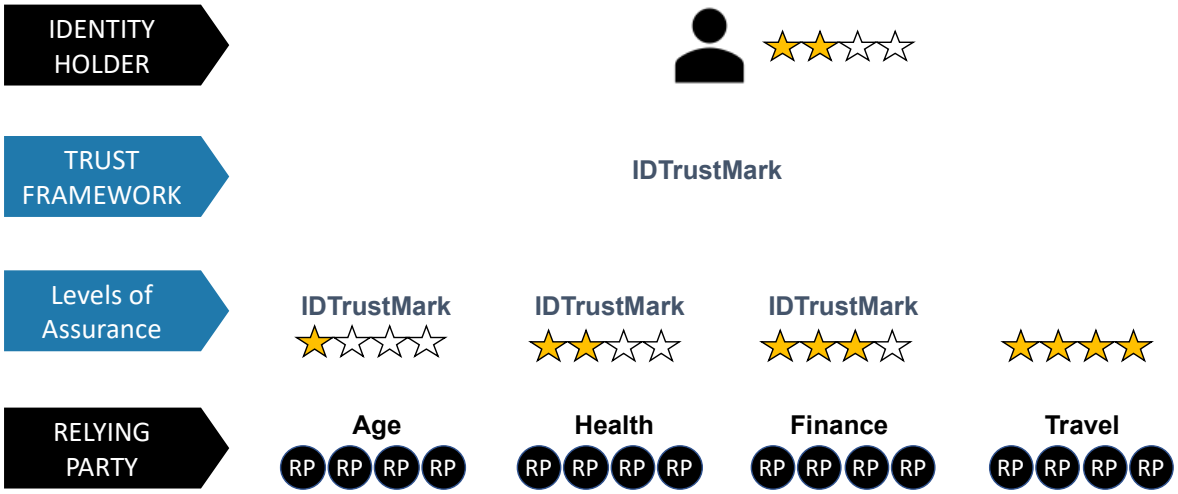
25 https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

26 https://www.tisa.uk.com/

As with the previously described UK Government TrustMark scheme for accredited building services a single, 'umbrella' Trustmark across diverse services in a sector could potentially be enabled by creating an overarching Trust Framework for existing schemes each of which would be required to meet the specific requirements in order for their own participating organisations to be able to display the 'umbrella' Trustmark. Any overarching Trustmark Framework would have to be explored, designed and implemented on a case by case basis. However, this would make it easier for participating organisations to reach wider demographics and allow for easier promotion of a single Trustmark which would enable end users to easily recognise where they could use their digital identity.

In the examples below, a single cross-sector Trustmark – "IDTrustMark" - is used within a Trust Framework. This enables the user to easily understand they can use an ID that has been accredited to the framework. But can their ID always be used for every use case?

The example below show the use of "level ratings" system to show the user where their ID can be used, for example based on a level of assurance:



Displaying "level ratings" to users based on levels of confidence are generally a bad experience bad for users and relying parties.

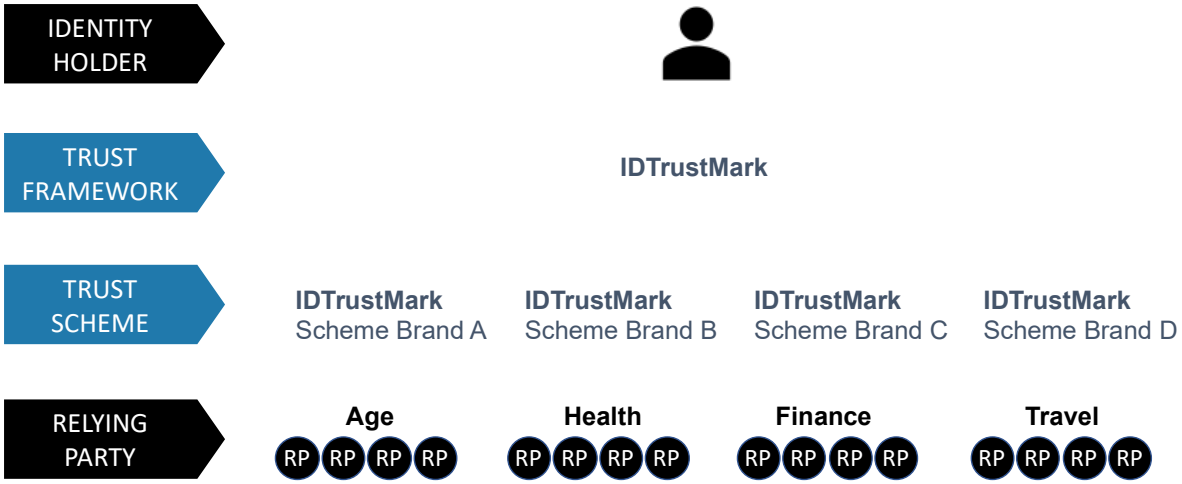
Users with low ratings may think they are underrated, replying parties think users with low ratings cannot meet their ID needs.

Also, for an Identity and Attributes trust framework, the ratings system does not help convey whether the user has the attributes needed for a particular use case, introducing the potential for further confusion.

However, from the point of view of relying parties, Trust Schemes implement specific rules applicable to that relying party's sector, such as required levels of identity assurance, or specific types of identity or eligibility evidence, or levels of fraud control.

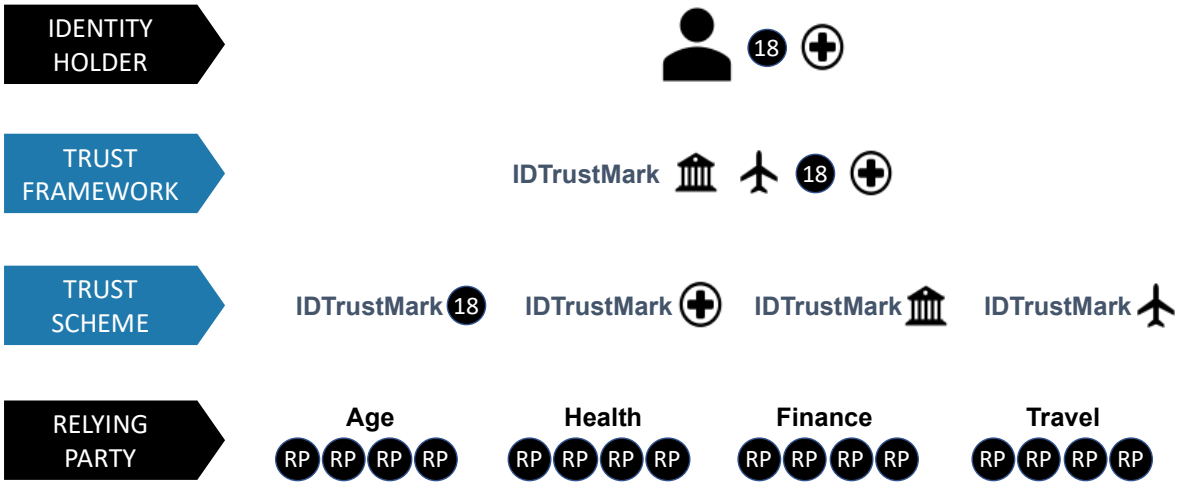
Each sector-based Trust Scheme would have a Trustmark, or Brand that contains the overarching Trust Framework Trustmark but shows that it is applied within the context of that sector, for example “IDTrustMark for Finance”

The relying party would show that it accepts IDs accredited to its sector-based Trust Scheme by showing the scheme level Trustmark or Brand. The use of the overarching framework Trustmark allows the user to see that an interoperable ID can be used across schemes:



Importantly it also allows any scheme specific rules to be explained to the user by the Relying Party, ID Provider or the Scheme. For example, a user may need to add a passport to their ID to be compliant with a Trust Scheme for Air Travel. It’s still the same ID, but until the passport is added the ID is not accredited to allow the user to board a plane.

Communication of Scheme / Sector certification IDs could be an iconised add on to the Trustmark by a Scheme. For example, like the laundry instruction icons on garment labels we are all familiar with:



These examples show several ways that a hierarchical framework / scheme relationship might be positioned.

However, the Trustmark LOGO may not need to communicate where the ID can be used to the user at all. A single Trustmark should be displayed everywhere and the user given the appropriate information and assistance as to where and how their ID will work:

Trust Framework should explain to users:

- Where they can use their ID: sectors / schemes.

Scheme Website should explain to users:

- The attributes required for the supported use cases
- The type of proofing and authenticators required the use case.

The **Identity Provider** should explain this to users, in specific terms:

- Why they need to add these attributes to their ID for particular use cases
- Why they need to go through more proofing, add more attributes or add new authenticators for a particular use case.

The Relying Party should explain that it needs an ID that is certified to a Scheme, or the framework generically.

Relying Parties are principally interested in whether an ID will meet their data and regulatory requirements. If this is achieved by the trust framework alone, then only the Trustmark is required for Identity Providers to communicate this to relying parties. However, where a Scheme is ensuring specific data and regulatory requirements for a relying party needs are met, the Scheme brand associated with the trust framework will also be important for the relying party.

This is a complex area, combining communication of a layered ecosystem on the one hand with an explanation of where a user can use their ID on the other. OIX recommends that significant user research is undertaken to determine the best way address this for each particular framework implementation.

4.9 Governance and enforcement

Use of the Trustmark

Deciding how, where and when to show a Trustmark is important. How much information can be shown within a Trustmark itself or how much more could be provided at a user's request must be considered carefully. Should there be a single central location or should each participating entity provide more detail according to a strict set of brand identity design guidelines?

Strict requirements for the use of a Trustmark including how it can be displayed across different mediums and channels i.e. print vs online and how, where and when it can be presented will be defined within legally enforceable contracts as part of a Trust Framework. If there are variants that provide more detail on level of assurance or service type then the requirements for how this additional detail will be presented must also be included.

To mitigate against the spoofing of websites or other collateral a combined approach of user education must be made available to ensure that users know how to establish that an entity presenting a Trustmark is certified to do so. This could be instructions on how to query a trusted registry of all certified providers within a scheme as per the requirements defined within the eIDas regulation. Or a definitive record might be included in another authoritative source such as a published directory with frequent publications and the ability to provide ad hoc notifications if a provider has been removed from a scheme. It is important that there is an independent means of validating an entity displaying the Trustmark rather than trusting links on a website or notifications from a provider, on face value.

Governance of the Trustmark

Along with education about how a Trustmark may be presented, the certification of providers against the requirements of a Trust Framework, both initial and ongoing, is essential before they can be entitled to display a Trustmark. Ongoing assessment as part of the provider assurance process is imperative to ensure that only organisations that have been assessed and certified present a Trustmark and are able to offer legitimate services.

The presentation of a Trustmark will provide transparency for both relying parties and users. Understanding how to get help and support; how to escalate and potentially get compensation; the certification both and authority that provides the overarching governance; potentially a list of the participating entities by role profile; capabilities of use for users i.e. where they can do what; additional in depth guidance of variations in service or product ie levels of assurance and how they are achieved and what happens when things don't work i.e. the need for assurance up-lift and some explanations as to why it sometimes fails.

Enforcement of incorrect or illicit use of the Trustmark by providers must be able to be enforced with penalties. This must also be accompanied with the ability for any incursions to be reported and potentially even with a proactive enforcement function to be always on the lookout for misuse or misrepresentation by fraudulent parties.

Complaint and redress process

It is essential there is enforcement of the requirements to ensure that organisations comply. This must also include the opportunity for both users and relying parties to make complaints and seek redress. Thus, it is essential that the requirements include formal processes, timescales and escalation paths.

5. SUMMARY OF FINDINGS

Trustmarks need legitimacy and purpose which is provided by the Trust Frameworks or schemes that underpin them. Developing a Trust Framework is a complex initiative involving many stakeholders that takes considerable time and money to create and the start-up and ongoing costs for organisations to participate and be assessed against framework operating rules along with the time and effort required are considerable. However, once in place a Trust Framework will help to limit liability through structured onboarding and strict governance and can help reduce fraud and error, streamline services and transactions and reduce costs.

A Trustmark can provide organisations and individuals with reassurance that service providers can be trusted as the effort to join ensures that participating organisations have a vested commercial interest in maintaining their compliance with the requirement of the Trust Framework.

The additional expense of creating and maintaining a Trustmark must be balanced with the need to address the perceived and actual reduction of risk and increased end user confidence, in light of the increasing number of data breaches and consumer mistrust in technology, it will offer. The potential value of a Trustmark - to inform and empower end users should not be underestimated.

For nascent providers and new services or where the aspiration is to build a market, Trustmarks can help to provide another route to assist in communicating clear and coherent messaging about a Trust Framework. However, the consumer while individuals are more likely to continue with a transaction if they recognise a Trustmark, the added complexity and costs are likely to be less compelling for organisations that are already or plan to be participants in a Trust Framework.

Recognition plays a large part in the effectiveness of Trustmarks, however care should be taken not to introduce too many *Trustmarks* or brands that support them to avoid confusion. Simplicity in messaging is perhaps the best approach for Trustmarks - just enough information for users to recognise the signal but not too much that could inhibit understanding of what is being conveyed. The need to provide additional detail, for example level of assurance, needs to be balanced with what users are trying to do i.e. complete a task - they don’t care how that is achieved only that it works.

Trustmarks could help to provide a clear signal that a user can complete a task, however awareness of where this can be done should be through a combined set of marketing activities by all participants in a Trust Framework. It should be recognised that while the aspiration to have a single Trustmark is an end-goal, challenges with interoperability between different Trust Frameworks and schemes may well mean this is more of a long term objective. Robust governance with enforcement is imperative to create and maintain trust between all stakeholders.

Creation of a Trustmark should be undertaken through consultation with all relevant stakeholders - including government, regulators, participating organisations and end users.

5.1 Recommendations

1) Trustmarks must be recognizable, understandable and able to be differentiated

    a) Too many Trustmarks or too much detail about a specific Trustmark will add to the confusion and potentially hinder a user's ability to make decisions.

    b) For a Trustmark to be effective and meaningful, it has to be recognised widely and perceived as legitimate and trustworthy.

2) It must be clear that the Trustmark is underpinned by a Trust Framework

    a) As the essence of a Trustmark is to demonstrate trust through a mark - trust must be considered as the essential part of what a Trustmark could convey. The use of a Trustmark must only be allowed once an organisation and it's service has met the requirements of the Trust Framework.

    b) Clear loopback mechanisms can enable access to more detailed or up to date information which will cater for the ever changing functionality of digital identity

3) Trustmarks do not negate the need for careful service design

    a) service design should consider clarity of information and messaging, usability, clear access to help, support and opportunity for redress, if required. And additionally could consider building trust through transparency by exposing user reviews and feedback.

4) Use of the Trustmark requires strict governance and active enforcement for non-compliance

    a) how to assess whether participating companies meet the criteria, and whether these criteria should be supported through legislation outlining minimum standards.

    b) Ongoing operational governance of participating organisations and each product or service they provide must be carefully managed.

5) A single Trustmark, with sector applicability can provide clarity and avoid confusion for users

    a) Fewer Trustmarks will make it easier for end users to understand what it is and where it can be used. For end-users the aspiration should be for a single Trustmark.

    b) It could also provide a means for participating organisations to develop more effective and wide reaching marketing campaigns and differentiate themselves from other organisations in the wider marketplace.

6) A Trustmark is a brand and developing a brand is a multi-year investment[27]

[27] https://doteveryone.org.uk/wp-content/uploads/2018/04/Exploring-a-trustworthy-tech-system-3.pdf

a) The organisation managing the Trustmark must be large enough with sufficient capacity, resources and legitimacy and adequate investment to enable ongoing development and publicity as well as the ability to potentially be transnational.

b) In circumstances where there is compelling evidence to suggest that multiple similar or competing Trust Frameworks or schemes may come into existence it will be important to work across all these different schemes to explore if it might be possible to create an overarching Trustmark similar to the example discussed within this paper about the UK government backed TrustMark scheme for the building sector.

7) There must be clear methods to get legitimate information, help and support

8) Any additional information about a Trustmark must be absolutely necessary

   a) Different services or variants e.g. level of assurance must be clearly displayed

6. APPENDIX - COMPARING IDENTITY WITH PAYMENTS

As with any nascent market there are always comparisons with existing similar markets. As an example, the payment cards model is often cited as being analogous with a potential model for identity.

The Payment Card Industry Data Security Standard[28] (PCI DSS) was formed by the five major payment card companies who enforce the standard[29]. The capital expenditure and ongoing operating costs to support a single scheme are high therefore it made sense to create a common set of standards that provide the appropriate level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data. This trust framework is enabled by ongoing compliance assessments that vary in terms of complexity and rigour according to the number of annual transactions. This allows merchants of different sizes to provide compliant services to consumers.

Figure 1 provides illustrative examples of both the payment cards model and a model for a potential identity ecosystem.

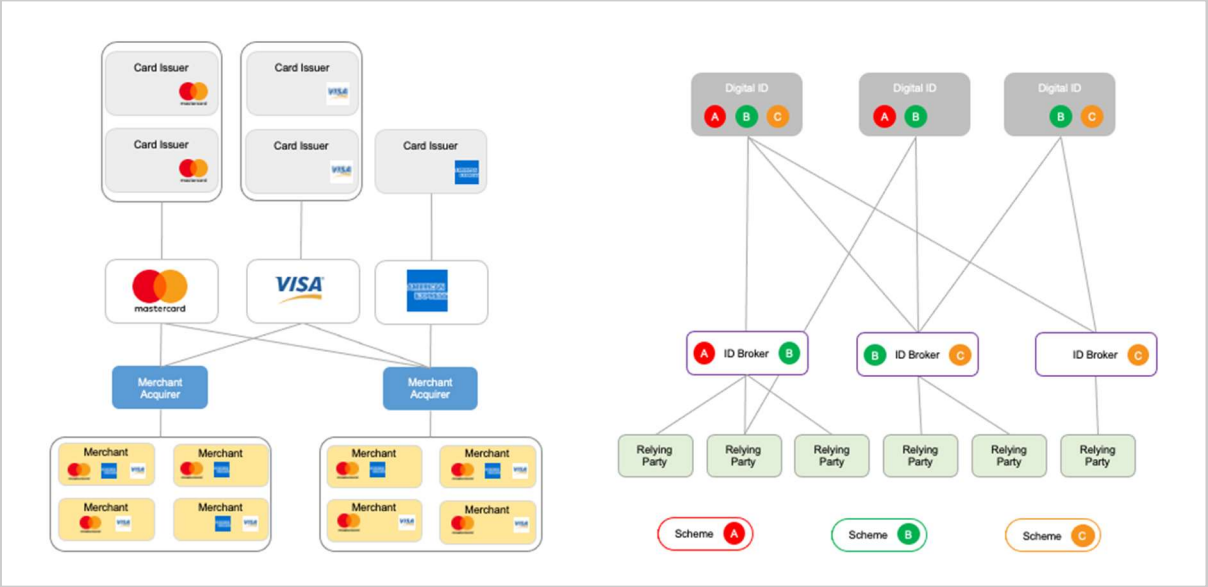


Figure 1: examples of the payment card industry model and a potential model for identity

28 https://www.pcisecuritystandards.org/

29 American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc

Discussions within an OIX working group established that although they are similarities between these models they are not the same. The table below provides a descriptive comparison of the two.

Payment cards	Identity
• Participants include Consumers using cards, merchants accepting cards, acquirers facilitating payment and financial institutions reconciling payment • Each scheme has only one provider • Interoperability between schemes is at the POS[30] terminal for consumers and merchants • Cards are issued by financial institutions supporting one of the PCI DSS scheme members • Consumers can only use their card where a merchant has signed up to a scheme • Merchants and acquirers choose which schemes to support • Availability of a scheme depends on the territory, merchant and acquirer • There are variants in the type of card offered - Credit or Debit cards	*Participants include Individuals, Identity providers / brokers, Evidence issuers and verifiers, relying parties* • Schemes may have many providers and there could potentially be many schemes per Trust Framework • Identities are created by identity providers • Relying parties, identity providers and identity brokers could choose to accept different Identities at different levels of assurance • Interoperability will only be achieved following a comprehensive process that will involve mapping legal, technical and procedural requirements to ensure equivalence and to potentially accept Identities from different schemes and sectors

30 Point of sale terminal