The Global Identity Foundation
A single global identity for humanity

Global Identity
Challenges, pitfalls and solutions

White Paper

This document has not been verified for avoidance of possible third-party proprietary rights. In implementing this document, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed.

Global Identity - Challenges, pitfalls and solutions (White Paper)

Published by The Global Identity Foundation, September 2019.

Comments relating to the material contained in this document may be submitted to:

e-mail to: info@globalidentityfoundation.org

Index

Figures

Preface

The Global Identity Foundation is a not-for profit foundation; constituted to first oversee the development of a single global identity solution and ecosystem and then maintain the core technology for any solution developed together with the management of its evolution.

For more information see www.globalidentityfoundation.org

Trademarks

The Global Identity Foundation acknowledges that there may be other brand, company, and product names used in this document that may be covered by trademark protection and advises the reader to verify them independently.

- The Jericho Forum® is a registered trademark of The Open Group
- CSA is a service mark of the Cloud Security Alliance
- IBM is a registered trademark of International Business Machines Corp.

Acknowledgements

The Global Identity Foundation gratefully acknowledges the contribution of members of the Jericho Forum to the thinking behind this paper, as well as Jericho Forum's work on the Identity Entitlement & Access Management Commandments.

Patents

The following patens have been granted;

- US Patent US 9,977,886 "Methods, Apparatus and Computer Programs for Entity Authentication"
- European Patent EP2959420 "Methods, Apparatus and Computer Programs for Entity Authentication"

This page intentionally left blank

1. Executive Summary

The Internet is a very untrustworthy place to do businesses, or for people to interact with others. This lack of trust is the root cause of Spam, Scams and Viruses with criminals making profits that some estimates say exceed the global drugs trade, while fraudulent losses on credit cards exceeds the GDP of 80% of African Countries.

Businesses are affected, not only through losses, but also by the inability to make higher value transaction with less risk, or through systems that are hampered by cumbersome (and often ineffective) security trying to compensate for a lack of being able to prove who they are interacting with.

People are affected, as there is no such thing as a global digital (or electronic) identity for people; let alone one that is truly universal, works with everything, and is based on the premise of privacy for the person it identifies, leading to having multiple, disparate accounts, usernames and passwords resulting in their identity being stolen and their privacy being eroded.

The root-cause of these problems is an inability to identify and have trust in whom or what you are interacting with; or more correctly identify, have trust in, and understand the context of all the entities in the transaction chain.

Attempts to date to solve this have failed, because we are not addressing the problems and the failings of current attempts to deliver a solution, and without understanding the history and pitfalls are simply doomed to repeat it.

If we are to solve this problem, then the “do differently” is to “turn identity on its head” and come at it from the point of an entity-centric (person-centric) solution, starting from a simple assertion that “I am who I am” (I am the same person I was when I set up my digital identity, am today, and will be tomorrow) and then layering upon that base, personas of my identity with varying levels of trust (depending on whom signs the individual personas).

From work initially performed by the Jericho Forum, this paper proposes that there is a viable solution waiting to be developed and refined, and one that will work identically for all entities (People, Devices, Organizations, Code and Agents); as well as one capable of being globally acceptable and deployable.

While there are a number of projects, solutions and products available today, these are all limited in their scope; addressing only a limited market, one of the entity types or only a segment of the global population. In contrast this is a project aimed at bringing the key players together to develop a global solution for the future, building on existing good work, and defining a holistic solution that will provide a single electronic identity for all entities.

Delivering on such a goal will deliver a level of trust about the people, devices, organizations code and agents we interact with on a daily basis and bring a global return-on-investment as existing services can be delivered with less risk and new services and opportunities become viable.

2. Introduction

2.1. What is the problem?

Identity in the digital world is broken and has been for some time. Passwords are well beyond their sell-by date, yet for most systems are still the only realistic solution. Meanwhile Spam, Fraud, Phishing and Cyber Crime succeed by being able to steal identities and impersonate individuals, with Credit Card fraud alone hitting an estimated thirty billion US dollars per annum[i].

Some 416 billion e-mails / day are Spam; 85.58% of all email[ii], with 0.22% of that Spam containing malicious content[iii], meanwhile other scams are becoming harder for the individual to spot – the bottom line is the Internet and the digital world is now a harder place for the individual person to trust.

A lack of secure (standard) cryptographic identity means that if you want your e-mail to be reliably readable by the recipient you must send it unencrypted (a postcard sent over the Internet) – although some 92% of email is now secure between servers[iv], with less than 2% of global e-mail is sent person-to-person encrypted.

Identity theft & fraud costs the UK alone around £70bn / annum[v], while globally 1 in every 40 individuals per year are victim to some form of identity theft.

A strong digital linkage to the individual has the ability to reduce or eliminate many forms of Cyber Crime.

Password resets are costing companies millions to manage and the automated systems for password resets to mitigate this cost are often weak and easily subverted, especially for systems that interact with the general public.

More importantly, the lack of good, strong, global standards for Identity of all entities[1] is inhibiting the growth of new goods and services, and perpetuating slow, cumbersome and insecure methods of operating, or the use of weak security as a compromise to bringing products to market quickly.

3. The scale of the problem

3.1. Passwords

According to the Gartner Group between 20% to 50% of all help desk calls are for password resets[vi] and Forrester Research states that the average help desk labour cost for a single password reset ranges from $70[vii] to $18 if using a self-help system[viii]. The move to automate password resets for public facing services, usually driven by this high cost, is enabling an easy back-door for criminals to take over accounts[ix].

It is universally accepted that passwords have had their day[x], however passwords are the default mechanism on nearly every computer system and application.

> The big lie of computer security is that security improves by imposing complex passwords on users.
> In real life, people write down anything they can't remember.
> Security is increased by designing for the way humans actually behave.
> *Jakob Nielsen*

3.2. The rise of the self-asserted identity

Nearly all the accounts that an entity has will be self-asserted, with at best, a closed-loop to validate the e-mail address as being genuine (but critically not the Entity) – and often the account will use the same e-mail address as the unique username (causing all sorts of problems should that e-mail account be abandoned, or compromised).

With these accounts, the attributes provided are also self-asserted, meaning that even when a web site allows a person to use their authentication credential from another service (such as Facebook or Google) this is generally limited to authentication, leaving the user confused as to why this new site is still requesting a plethora of attributes; however the passing of self-asserted attributes could well leave the authenticating site with a large liability. Also, in some parts of the world, particularly Europe under GDPR, passing attributes without the consent of the entity could well be illegal.

Single-sign-on (SSO) services similarly are usually limited to authentication but not the sharing of attributes. External (cloud based) services are generally limited to web-based services. Many SSO solutions utilise a One-Time-Password (OTP) solutions using their own token[xi] usable only with the hub service which then passes authentication credentials only to sites supported by that solution.

Most of these accounts are password-based with sites augmenting log-in with an authentication “app” or with a one-time code sent through SMS; in higher value transactions the use of unique tokens or card readers issued specifically for that account, typically this higher level of authentication is found securing financial accounts.

There are federation “clubs” for identity, when industry partners come together to put in a common identity solution for joint access, examples are SAFE BioPharma[xii] and the Transglobal Secure Collaboration Program (TSCP)[xiii] that serves the Military/Aerospace community; but in both these examples, users still retain separate identities within their parent organizations.

3.3. Lack of authoritative sources for attributes

Like most current identities, the attributes associated with them are also self-asserted. Many are incorrect, deliberately due to security concerns or deliberately so the person can access goods and services; such as a Facebook with a minimum age of 13, or adult content requiring a minimum age 18 or 21.

Few attributes are checked, even if it was technically possible, leading to a high level of fraud (false delivery addresses) or the changing of attributes and other information when accounts are hacked.

[1] Entity types: People, Devices, Organizations, Code & Agents – Source: Jericho Forum Identity Commandments

When paying by credit card, a physical delivery address can be required to use the same address as the card is registered to (in some parts of the world), but this inhibits the ability to send a gift, or to send to a hotel when travelling abroad – and of course is limited only to transactions resulting in a physical delivery.

The ability to provide strong identity proofing is expensive and assertion of attributes from other than the authoritative source carries the risk of financial liability should that assertion prove to be false.

3.4. Single device, multiple users

Many computing devices are used by multiple users, especially in the consumer market, and even more when it comes to tablets. Devices owned by parents are then used by the entire family and friends; with the result that the "adult" account can be used by the entire family, often with passwords cached for on-line accounts and credit cards associated with on-line stores that can be accessed by whoever is using that device.

This has led to a series of high-profile problems; like the 13-year old who ran up a £3,700 bill playing games on his iPad[xiv], and Apple agreeing $100m in compensation to US parents whose children racked up huge bills by buying extra content for 'free' iPad games[xv].

The users of smart-phones, especially those used by businesses, want to be able to use a single device for both business and personal (dual-persona); usually resulting in personal e-mail co-mingled with corporate e-mail, or corporate e-mail being sent to personal devices.

3.5. Managing people / users / access for entities that you don't employ

It is common in business to use a mixture of staff and non-staff; such as contractors, outsourced roles or joint-venture staff. However nearly every organization has to manage user accounts for people they do not employ, which results in problems in effectively applying the joiners / changes / leavers process.

In addition, many non-staff want, or are required, to use their own computing equipment, connecting that equipment to the corporate network and accessing corporate resources and data.

3.6. Account apathy

People (in the developed world) have in excess of 100 accounts, each consuming attributes of their identity. Many are used only occasionally and either require resetting when used due to the user forgetting the password, or the person simply creates a new account.

The need for easy (not necessarily secure) automated account recovery is now so critical to stop this account abandonment that weaker methods are being used to deliver ease and convenience over security. This leads to the account reset process being abused to hi-jack accounts.

Old accounts are rarely closed or disposed of, many lying dormant and forgotten. Many accounts are tied to an old forgotten e-mail account, meaning that when that e-mail account becomes lost, so does a whole tranche of accounts that used e-mail to send reset information.

3.7. Inability to consume someone else's (strong) identity

Currently, access to systems by an entity outside that organization (public, partners, JV's etc.) means creating a "dummy" identity for that entity to allow access; with that access often granting unrestricted network access once through the corporate border.

Many companies are using the (public) cloud computing to allow access to shared information thus negating the need for physical access inside an organization (and its firewalls).

However, in both scenarios the impossible challenge is to manage and maintain people and devices outside of your control; while a better solution would be to consume and trust their own identity information, they bring with them.

3.8. Consumerisation is driving less security

The lack of easy identity of entities, particularly people, is causing vendors to trade convenience and speed to market for identity and security. Examples are the introduction of payWave enabled credit cards, NFC enabled phones, direct access to banking via smart phones etc.

4. Areas of applicability (Who should be interested?)

4.1. Internet of Things - IPv6 Direct Access

IPv6 and the "Internet of Things" (IoT) are driving a deperimeterised world, where all devices are directly addressable from anywhere, with many early devices being insecure and trivially hackable. Such ubiquitous access needs secure standards based around the identity of all entity types. In the case of IoT the identity of all entity types in the transaction being attempted are critical to making robust decisions about access and control of such devices.

4.2. Digital access to Citizen e-Services

Governments need to be able to consume the identity of its citizens; the Government should also be the authoritative source (and digital signatory to) the attributes for a "citizen persona"; containing such attributes as "birth name", "date-of-birth", "place of birth", "right of abode". Being able to consume Identity not only from its own citizens but also those issued by other governments allows a single "universal" interface to computer systems as well as not having to maintain pseudo-citizen records for non-citizens simply so all residents in the country can access the tax, benefits, health, border and voting systems.

4.3. Physical access

Utilising a cryptographically secure device allows it to be used in a variety of situation where a physical key may traditionally be used. Home door locks can simply be programmed with temporary access being granted without the worry that keys can be copied. Cars already use a much less secure proximity key, but can be enhanced with the car understanding and allowing different driving profiles for different people, or organizations (for example the local auto-shop who maintains the car).

4.4. Phone and mobile devices

Having a phone or mobile device able to understand who has picked the device up, enables the device to unlock a richer set of functionalities;

Companies will be able to use a BYO-Device; as the corporate e-mail, calendar, contacts and data can be securely locked to a defined corporate persona (and cryptographic keys associated with that persona).

Higher value transactions can be made via the device when the appropriate bank or credit card persona is present.

The use of the device by multiple people can be enabled with access to areas (data stores and apps) restricted dependant on who is holding the device (Android 4.3 onwards supports restricted profiles, and Blackberry 10 supports persona) thus ensuring for example; at a basic level the device auto-locks, and children playing games have no access to in-game payment or inappropriate content.

Utilising the secure capability of the processor (such as ARM's "TrustZone"), cryptographic "blobs" of cached persona assertions can be held locally using the smart phone as an intermediary device, or can be used to securely re-mix assertions.

4.5. Credit Cards / Banks / Financial

Customers using an ATM can verify themselves using their own BYOID identifier registered with the bank. Or use that same identifier to authenticate to a standard identity app inside the smartphone with banking or credit card persona stored within that app. Having such an app allows the financial organisation to identify the type of device being used and use its inherent features to request further verification (or re-verification) when the transaction risk-profile demands it.

For contactless payments using a phone app, device authentication assures that the person paying is actually the owner of the account, reducing risk and allowing significantly higher transaction values to be permitted, and allows additional verification to be requested should the risk-profile demand it.

When paying for a web-based transaction, use that same identifier to make the transaction but assert a one-time signed payment for the amount rather than the need to hand over your credit card number.

With no PIN[2] and no passwords to remember there is nothing to steal, and no password resets required as it's the user's device (not the Bank's or Credit Card companies). Organizations can make the risk decision about whether to proceed with a transaction based on understanding the risk-profile of all the entities and attributes in the transaction chain, not just a few of them – significantly reducing and in many cases eliminating the opportunity for user error, fraud and criminal activity.

4.6. Agents, with access to our lives

Increasingly, we will use "agents" to run our lives; pseudo-intelligent software that understands our routines and the linkages within our lives to perform tasks for us automatically.

The need to be able to rely on the security and integrity of such agents is critical, and in turn the need for a single global standard for identifying all entity types and the trusted attributes is essential for such agents to work across all aspects of our lives.

4.7. Corporate

On boarding a new employee should be simply a case of utilising that new employees existing digital identifier and creating a "Corporate Persona" containing only those attributes owned (and signed by) the corporation.

Computer access is then simply a question of walk-up and log-in to a suitable RF-enabled computer with no username and password required, with features such as auto-screen lock when the user walks away from their computer and auto-unlock when they return.

Physical access to buildings and areas can also be achieved with door locks being programmed with a set of "entitlement rules" pertinent to the organization, and activated by the employee's corporate persona being able to make the relevant assertions.

4.8. Cloud

One of the key area for cloud vendors, whether SASS, IASS or PASS, is how to consume the identity from multiple competing standards, but also how to consume trusted identity attributes into the application in such a way that rich, risk-based entitlement decisions can be easily and simply implemented by their customers, either as part of a IASS / PASS service, or integrated into the application as part of a SASS service.

One of the key advantages of a cloud-based service is the ability to access such a service from anywhere, by users, partners, JV clients, or the general public, without the constraint of needing to first connect to a corporate gateway to validate identity; and ideally without the need to manage those users individually.

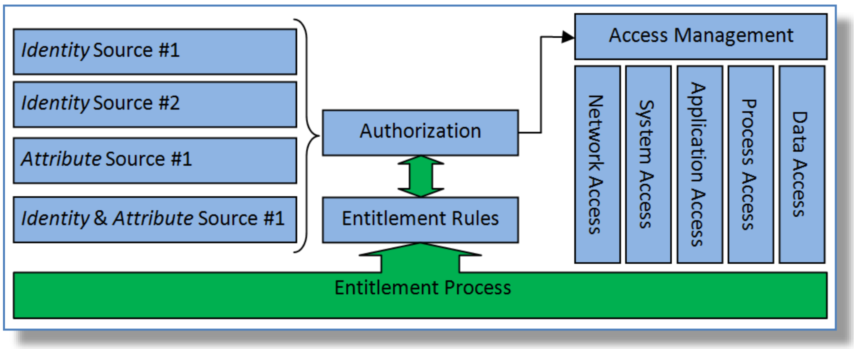


Figure 1: Entitlement Process

Taken from Cloud Security Alliance – "Security Guidance for Critical Areas of Focus in Cloud Computing" v3.0; Domain 12 (Identity, Entitlement, & Access Management)

Cloud vendors rarely want to get involved with managing users, and instead management using entitlement rules[xvi], using a single standard for global identity and trusted attributes, will enable maximum flexibility together with security.

4.9. Application Vendors

The default for most application vendors is to use an identity and access management system built into the application, or to use one provided by the operating system on which the application is residing. This approach is a pragmatic one, based on the multitude of competing identity solutions in use by their customers. In the future; one set of APIs that can leverage a trusted global identifier together with trusted and authoritative attributes allows true "entitlement" based

[2] Device dependant

access to be built into their application; with the ability to consume identity and attributes related to the transaction chain enabling a more granular access to both the data and the application environment.

4.10. Identity Vendors

Vendors involved in any aspect of identity, currently have to deal with a plethora of competing identity standards, tokens, devices, and passwords. The move to a single, global, open standard for identity allows them to concentrate on adding value via their services or as part of the entitlement process.

5. Current problems with identity

5.1. Locus of control

Nearly every current identity ecosystem revolves around the concept of a "locus of control" [xvii]. These work well only when a single body controls the entire Identity Ecosystem. This is typical of a corporate system that uses (for example) Microsoft Active Directory, or a government run "citizen identity" system.

The need to control all identities and attributes in such a system leads to trusting only the one system, and two undesirable behaviours; first, the "fools-quest" to create a single authoritative repository of identity and attributes; and second, the mistrust of all other identity and attribute systems (see Figure 2: Vicious Identity & Attribute Circle).

Federating such systems, suffers from the same trust issues, especially around the problems with transitive trusts (because A trusts B, and B trusts C, should A trust C?), and all federations suffer from the n-factorial problem where multiple trust relationship almost immediately become too large to manage or understand.

Federation clubs can work when groups have common enough aims and agree standards for proofing (TSCP and SAFE-BioPharma are two examples) but in almost all examples separate identities are retained for internal use.

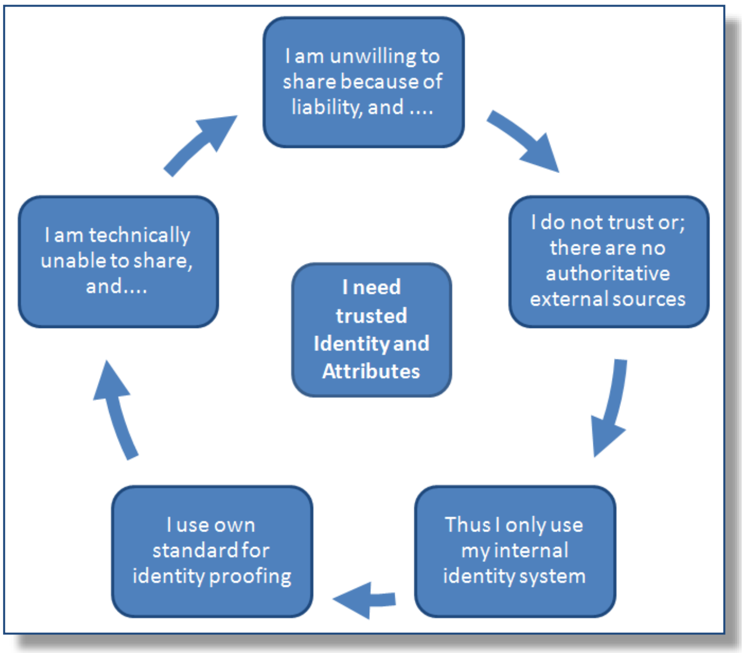

I am unwilling to share because of liability, and ....
I do not trust or; there are no authoritative external sources
Thus I only use my internal identity system
I use own standard for identity proofing
I am technically unable to share, and....
I need trusted Identity and Attributes

Figure 2: Vicious Identity & Attribute Circle

5.2. Linking the entity identity to the digital identity

When the entity type is already digital (Device or Code) then digital identity is feasible. However, when it comes to the other entity types then the trust ecosystem fails when trying to tie the non-digital entity (Person, Organization or Agent) to its digital identity.

Each of us knows how to identify people in the real world; faces, introductions, previous interactions, all allow us to choose who we deal with and in what situations. Yet, when it comes to extending this into a digital identity there is no simple, single, extensible, standard method of putting our identity into the digital realm.

5.3. Identity proofing & liability

Any solution that promises to be a "clearing house" for an individual's various attributes quickly runs into a number of problems. The biggest of these is that they are unlikely to be the authoritative source for any of the attributes. Thus, there is a need to (often blindly) trust the strength and method of proofing, as well as the need to trust the organization performing the proofing (especially if this needs to globally scale).

Where an organization is not the authoritative source for the attributes then the question of liability arises – in the USA the owning of fake ID is considered the norm in those under 21, allowing them to buy and consume alcohol – consider who is liable should an underage drinker with a validated but fake digital identity commits vehicular manslaughter while under the influence. Or that body incorrectly proofing an individual’s fitness to own a weapon, that then goes on to murder another person with it.

5.4. Privacy

Governments are proposing that they, or corporations authorized by them, should be the holder of an individual’s digital identity - taking identity from the control of the citizen and placing it in centralized databases.

To maintain privacy, it is critical that an entity, wherever possible, is in control of its own identity, digital identifier and related attributes; this is the principle of “primacy”.

> "If privacy is outlawed, only outlaws will have privacy!"
> *Philip R. Zimmermann*
> *(creator of PGP)*

Thus, the entity can control with whom and under what circumstances identity and attributes are shared.

5.5. User Experience

The current user experience is abysmal, with disparate user interfaces, arbitrary requests for attributes, and user-name and password rules that are unconnected and difficult to remember.

Users crave a simple, frictionless, standard method of easily proving “I am me” to a remote digital system; with that remote system capable of evaluating that assertion and only when the risk demands it, asking for extra supporting proof.

5.6. BYOiD

Today, the ability to bring-your-own-identity (BYOiD) is limited to using a self-asserted identity (such as Facebook or Google) to replace the authentication component of a log-in.

For BYOiD to be successful it must extend beyond authentication and allow the assertion by the entity of trusted attributes that have been signed by the authoritative source.

6. Six Conundrums of Global Identity

There have been many attempts to implement large-scale identity solutions. All have either failed, or imploded to servicing a sub-set of systems under the locus-of-control of the identity provider – for example most government attempts at citizen identity implode to providing access for a sub-set of government services.

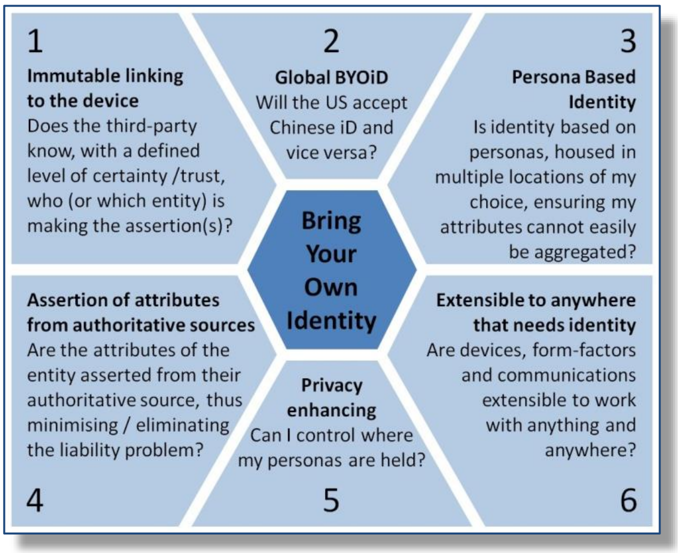
For a truly global identity ecosystem to develop there are six key conundrums that must be addressed for it to stand a chance of being successful.

6.1. Immutable linking to the device

If the other party in the transaction does not know, with a defined level of certainty / trust, who (or which entity) is making the assertion(s) then the entire foundation for the transaction is flawed.

The trust required will come by providing three key assertions about the level and method of connection;

- Immutable linking[xviii]; the method of linking the entity to the device and thus linking the entity to the cryptography.
- The model of the device; which in turn allows the determination of potential exploits, as well as the capability of the device.
- The issuer of the device at the point it was initialised; which determines the chain-of-custody as well as provides guarantees behind the initialisation process.



1 **Immutable linking to the device** Does the third-party know, with a defined level of certainty /trust, who (or which entity) is making the assertion(s)?

2 **Global BYOiD** Will the US accept Chinese iD and vice versa?

3 **Persona Based Identity** Is identity based on personas, housed in multiple locations of my choice, ensuring my attributes cannot easily be aggregated?

Bring Your Own Identity

4 **Assertion of attributes from authoritative sources** Are the attributes of the entity asserted from their authoritative source, thus minimising / eliminating the liability problem?

5 **Privacy enhancing** Can I control where my personas are held?

6 **Extensible to anywhere that needs identity** Are devices, form-factors and communications extensible to work with anything and anywhere?

Figure 3: Six Conundrums of Global Identity

6.2. Global BYOiD

For any solution to be globally acceptable the root of the device ecosystem must be country. organization and company agnostic. For example: US Companies and the US Government are unlikely to trust an identity issued by a Chinese company and vice versa. For a global identity ecosystem to be a success then an individual holding dual Chinese-US citizenship needs to be able to use their single digital identity to assert their citizenship of both countries; in a form acceptable to both Governments.

6.3. Persona Based Identity

People use personas to segregate attributes about themselves to ensure their privacy, for example an actress may use different personas with her stage name (professional), husband's name (at child's school) and actual name (legal). Mirroring this to the digital world, privacy is enhanced when the personas and the attributes they contain is under the control of the entity they are about (primacy). Those personas also need to be in locations under the control of, or approved by, the entity.

Should an identity provider house multiple personas, or worse still all the personas and attributes for an entity, there is a risk of identity aggregation, and a single point of attack to steal an entities entire identity.

6.4. Assertion of attributes from authoritative sources

For attributes to be truly authoritative, they need to be signed by the authoritative source for that attribute. The need for a US company to understand the level of vetting and identity proofing that was performed by an unknown third-party company in (say) Azerbaijan so they can make the appropriate risk calculation will not scale globally.

Key identity attributes must be asserted from their authoritative source, thus minimising / eliminating the liability problem as well as the need for third parties performing identity vetting.

6.5. Privacy enhancing

As well as the need for an entity to control where personas are held (primacy) there is also a need to incorporate other privacy enhancing technologies to ensure the attributes of a persona are limited in their exposure.

The assertion of attributes and the form they take must be under the direct and primary control of the entity, this includes the ability to re-mix signed attributes. For example; an entity needing to prove they are over 21, the solution is not to assert a government signed attribute of their date of birth (from their "citizen" persona) but to re-mix the signed date-of-birth into an assertion (still signed by the government) that they are over 21.

6.6. Extensible to anywhere that needs identity

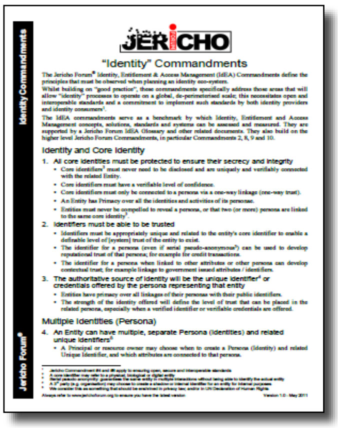
The digital identity ecosystem will need to be developed and the standards, devices, form-factors and communications must be extensible to work today as well as tomorrow. The needs of communities that do not have always-on Internet, or the need for mobile personal identity vs. corporate identity must factor into any developed solution, otherwise identity solutions will fragment to serve those individual markets.

7. Jericho Forum Identity Commandments

First published in 2011, the Jericho Forum® Identity, Entitlement & Access Management (IdEA) Commandments[xix] define the principles that must be observed when planning an identity ecosystem.

Whilst building on "good practice", these commandments specifically address those areas that will allow "identity" processes to operate on a global, deperimeterised scale; this necessitates open and interoperable standards and a commitment to implement such standards by both identity providers and identity consumers.

The IdEA commandments serve as a benchmark by which Identity, Entitlement and Access Management concepts, solutions, standards and systems can be assessed and measured. They also build on the higher level Jericho Forum Commandments[xx], in particular Commandments 2, 8, 9 and 10.



Identity Commandments

JERICHO FORUM

"Identity" Commandments

The Jericho Forum® Identity, Entitlement & Access Management (IdEA) Commandments define the principles that must be observed when planning an identity eco-system.

Whilst building on "good practice", these commandments specifically address those areas that will allow "identity" processes to operate on a global, de-perimeterised scale; this necessitates open and interoperable standards and a commitment to implement such standards by both identity providers and identity consumers[1].

The IdEA commandments serve as a benchmark by which Identity, Entitlement and Access Management concepts, solutions, standards and systems can be assessed and measured. They are supported by a Jericho Forum IdEA Glossary and other related documents. They also build on the higher level Jericho Forum Commandments, in particular Commandments 2, 8, 9 and 10.

Identity and Core Identity

1. All core identities must be protected to ensure their secrecy and integrity
   - Core identifiers[2] must never need to be disclosed and are uniquely and verifiably connected with the related Entity.
   - Core identifiers must have a verifiable level of confidence.
   - Core identifiers must only be connected to a persona via a one-way linkage (one-way trust).
   - An Entity has Primacy over all the identities and activities of its personae.
   - Entities must never be compelled to reveal a persona, or that two (or more) persona are linked to the same core identity[3].
2. Identifiers must be able to be trusted
   - Identifiers must be appropriately unique and related to the entity's core identifier to enable a definable level of [system] trust of the entity to exist.
   - The identifier for a persona (even if serial pseudo-anonymous[3]) can be used to develop reputational trust of that persona; for example for credit transactions.
   - The identifier for a persona when linked to other attributes or other persona can develop contextual trust; for example linkage to government issued attributes / identifiers.
3. The authoritative source of identity will be the unique identifier[4] or credentials offered by the persona representing that entity
   - Entities have primacy over all linkages of their personas with their public identifiers.
   - The strength of the identity offered will define the level of trust that can be placed in the related persona, especially when a verified identifier or verifiable credentials are offered.

Multiple Identities (Persona)

4. An Entity can have multiple, separate Persona (Identities) and related unique identifiers[5]
   - A Principal or resource owner may choose when to create a Persona (Identity) and related Unique Identifier, and which attributes are connected to that persona.

[1] Jericho Commandment #4 and #8 apply to ensuring open, secure and interoperable standards
[2] A core identifier may refer to a physical, biological or digital entity
[3] Serial pseudo anonymity guarantees the same entity in multiple interactions without being able to identify the actual entity
[4] A 3rd party (e.g. organisation) may choose to create a shadow or internal identifier for an entity for internal purposes
[5] We consider this as something that should be enshrined in privacy law, and/or in UN Declaration of Human Rights

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 - May 2011

Jericho Forum®

7.1. Entity-centric ID

The commandments define that the root of an entity's identity must be secret, in effect simply proving "sameness" (I am the same entity I was when I initialised the cryptographic keys, am today and will be tomorrow). This has a number of key benefits when building a global identity ecosystem, among them; No ability to subvert a store of identities and the acceptability to use a single cryptographic root to an entity's identity across multiple countries and organizations.

7.2. Core Identity must be secret & protected

The commandments introduce the concept of a "Core Identity" (I am who I am, a collection of personas; each with a set of specific disparate and often unique attributes) and a "Core Identifier" – the digital cryptographic representation of the entity, from which, using a one-way trust, separate cryptographic personas can be generated by the entity. The one-way trust ensures that knowing about a particular persona does not allow the core identifier (and thus the core identity) to be derived and therefore does not allow other personas to be deduced.

7.3. Primacy

At all times the entity must have primacy (full control) over where they link their core identifier to; the entity is in control of whether to create a new persona, with whom, and what attributes they are happy with that persona having. It is always their choice not to create a persona, or (in extreme cases) to maintain multiple core identifiers.

7.4. Persona-based

The use of cryptographically linked but separate personas is a key privacy enhancing technology. Only the owner of the core identifier can assert the persona and/or the attributes linked to it. A persona and their associated attributes can be signed by the authoritative source (say a "citizen" persona or a "corporate" persona) but can only be asserted by the entity owning the core identifier.

7.5. An immutably linked entity

Key to making a risk-based decision about whether to transact with an entity that is making assertions about its identity is understanding the level of immutable binding between the entity (core identity) and the cryptographic root of the assertions (core identifier). The device securely holding the root cryptographic keys must be able to independently assert the binding used, the features of the device as well as the device chain-of-custody, thus enabling the transacting party to have a complete understanding of all entities in the transaction chain.

7.6. Attributes from authoritative sources

Attributes need to come from their truly authoritative source, otherwise questions about liability and the level of trust you can place in the identity proofing arise. Having attributes grouped into a persona is both privacy enhancing, mirroring the way humans maintain their privacy, and leads to the use of disparate personas. As personas are protected via a one-way trust, should a persona be compromised, there is no ability to link this persona to other persona (and that personas attributes) or back to the core identity.

8. Needs from a global identity ecosystem

8.1. What people want

Entitlement

Making a risk-based decision

●

About access to data and/or systems

●

Based on the trusted identity and attributes

●

Of all the entities and components in the transaction chain

Quite simply; people know who they are, and all they want is to be able to re-use that fact repeatedly, securely and in an easy to use manner.

People want privacy; they want to give out attributes only when required and those requested attributes should be applicable to the environment they are interacting with. They want to be known as '*Dave'* to their friends in the Squash club, but '*David*' at work, '*Alphonse David*' when needing their legal/birth name and '*anonymous*' in other interactions; all from a single core identity under their control.

People want convenience, a single digital device that will interoperate with ***everything*** they need to interact with. In a form factor that makes sense for them and they can choose.

If people were offered a "master key" that opened their house, cars, safe-deposit box and the doors to where they work, they would want to ensure it was secure and only operated under their control. People need to be assured that this digital master-key to their identity is similarly secure and only operates under their control.

Any device needs to be extensible to work with any electronic device, either directly or (more probably) via proxy devices such as a smart-phone. As soon as people need to manage a second (or third) "master key" to their identity any advantage is severely diminished.

8.2. What the third-party wants

The third-party wants a set of trusted attributes, authentication (and sometimes portions of an identity) that enable the transaction to be carried out with the risk to all parties minimised and with an ease of use for the interaction that will ensure the transaction is not abandoned due to a burdensome set of information being requested.

They want one set of API's to implement that will allow them to accept Identity information (both authentication and attributes) from any entity, anywhere in the world and they want attributes that can be trusted, or at least come with a known level of trust, to enable them to make an "entitlement" decision.

They want attributes, authentication and identity to function the same, globally, thus ensuring the same entitlement process can be used to make the risk decision, and "specials" to not have to be implemented (and maintained) for each country / region / area.

They want a low cost, and preferably no-cost to using this system and a very low cost of entry; standard API's that can be implemented for their systems that enable entitlement, trusted attributes, authentication and identity to be simply used to enable a lower cost of digital interactions and a lower risk profile than currently exists.

9. Flawed solutions

9.1. Government implemented / sponsored solution

All attempts to date of a government solution have started with grand intentions and then either failed, as the UK National Identity Card scheme, or it has imploded into a method of "citizens" accessing a sub-set of government services, such as the German ID card, generally with work-arounds for non-citizens to be able to access those same services.

Where there have been some more successful state-implemented solutions all have major flaws; India's Aadhaar (Hacked[3]), Norway's BankID (does not work across Scandinavia let alone wider, trust in your Bank does not scale), Estonian ID-kaart (cryptographic key vulnerability, requiring upgrading all ID cards).

[3] https://www.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system

9.2. Solutions that need a “locus of control”

Corporate identity systems fall into this category; “we trust this identity because we personally (corporately) have proofed the entity (usually people, but often devices as well) to our standard”. To extend that system into environments that you don’t control relies on the environment placing complete trust in the proofing someone else has performed; this is typical of traditional federated models. Unfortunately, this does not scale to more than a few tiers of trust, or outside an identity club of like-interested organization that agree to operate a similar proofing standard.

Many [claimed] Single-Sign-On (SSO) solutions suffer from this flaw, whether developed in-house, or now utilising a cloud-based SSO solution, that allows authentication to be extended outside the organization, the flaw still exists; that it is reliant on trusting the proofing organization.

9.3. The solution is limited in its scope

From solutions that replace the multitude of web passwords, to apps on smart-phones that allow similar access to web based services, there are a plethora of offerings that offer to bundle one aspect of people’s lives, often at the compromise of security, unless each receiving service has a specific connector for the authentication service you happen to choose.

Nearly all of these services only deal with people, not entities, and miss both the points; that identity and authentication needs to work identically whether it is a person, a device, an organization, code, or an agent; and in addition, better risk-based transaction can take place when the identity and attributes of all the entity-types can be used to understand context.

There is a reliance on an always-on or always-available solution; without the understanding that using cached credentials should simply change the transaction risk, and in some transactions force revalidation in real-time.

> "The definition of insanity is doing the same thing over and over again and expecting a different result."
> *attributed to Albert Einstein*

9.4. Reliance on a central ecosystem

Most identity ecosystem needs a single (central or distributed) service, leading to a number of issues. From monitoring ingress / egress to those points, to inserting monitoring code (either covertly or as a legal requirement), even if the attributes and identity is protected (even encrypted), many other aspects of what an entity is communicating with (and for what reason) can be inferred through the meta-data.

Central ecosystems are a central point to be hacked, in fact any ecosystem that becomes big enough will be a target, and (given the high-profile hacks of security companies and government) will succumb.

10. Different thinking

In over fifty years of computers needing identity to transact with an entity, has the identity problem been solved in a global, extensible way. Thus, the need to turn identity “on-its-head”; to start from an untrusted, 100% anonymous, root of an entities identity and then layer personas and attributes below that root, each having varying levels of trust.

10.1. Proving “I am me” or “sameness”

At the heart of an identity ecosystem, identity starts with being able to prove “I am me”; I am the same person today as when we were first introduced and also will be tomorrow.

Moving this concept to the digital world, the root of an entity’s identity is simply proving that this is the same entity that you first encountered (and possibly registered), is still the same entity today, and will be tomorrow.

Work from the Jericho Forum identified the root-cause problem with current identity ecosystems as this inability to prove “I am me”; the immutable linkage between a Human Entity and their digital “Core Identity”, and do it in a way that protects the privacy of the individual entity involved.

The solution to this problem needs to balance a strong proof of “sameness” along with the need for the privacy of the entity at the core. The individual needs to be in control, or have “primacy”, over their identity; as well as any solution needing to transcend national or corporate boundaries and work globally.

10.2. Identity Proofing

Strong identity proofing should only be carried out when necessary; and then only for those attributes for which the proofing body is truly the authoritative source. In this way attributes, signed by the authoritative source, can be asserted, negating the liability issues that come with a third-party asserting an attribute for which they are not authoritative.

10.3. Privacy by design

Privacy is achieved by giving the individual full and direct control (primacy) of which personas they choose to create (or to link their identity to), the attributes those personas have, who they choose to interact with and in what situations; yet implemented in a way that provides strong identity to everyone who needs it, including banks, governments, retailers and corporations.

10.4. The entity at the "root" of its own identity

Having an entity at the root of its own identity has a number of fundamental advantages;

- The entity has a vested interest in the primacy of its own identity, personas and attributes.
- The entity can assert disparate attributes from multiple personas as a cryptographically linked set.
- There is no central repository (or system) to hack or subvert.
- Should a persona or attributes be hacked or subverted, without the root cryptographic keys those attributes cannot be asserted by the thief.
- Should attributes become publicly known, without the root cryptographic keys those attributes cannot be asserted to impersonate the entity.
- There is no federation, thus the solution does not suffer from an n-factorial problem, and thus will scale globally.

10.5. Segregation of attributes using personas

Using personas to segregate attributes has a number of advantages;

- It mirrors how humans operate their (analogue) identity to segment their lives and thus manage privacy.
- It allows personas, and their attributes, with different levels of trust to operate as part of a single overall identity.
- It enables the proofing of attributes only when required and to a level appropriate to that persona and/or attributes.
- It allows personas for different functions; such as an anonymous voting persona, a self-asserted persona or a government-signed citizen persona; all linked to the same root identity.

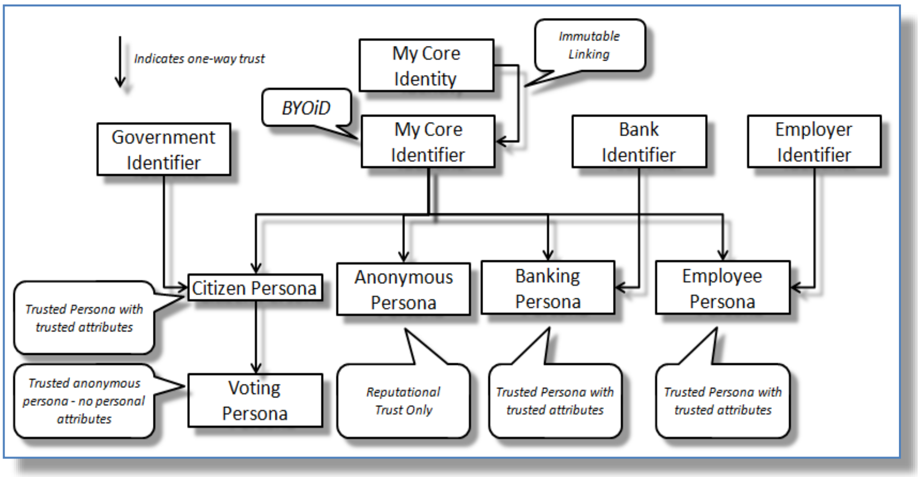


Figure 4: Simplified personas for a citizen

10.6. Minimising attribute collection for privacy

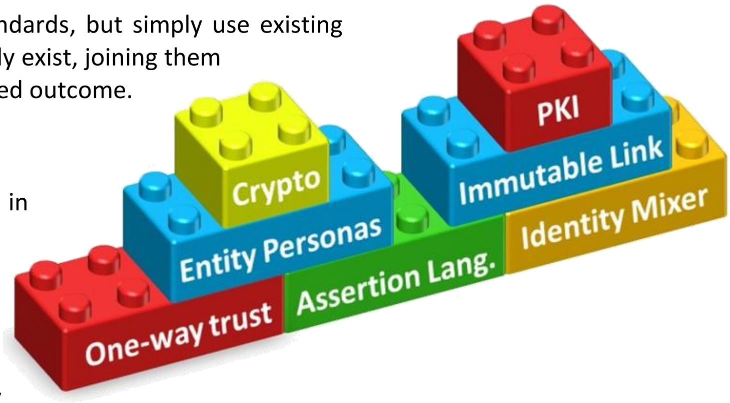
The way we currently use identity needs different thinking; For example, an e-commerce order currently (typically) creates a new account; mandating name, address, e-mail, credit card details, information for account recovery (mother's maiden name, pets name etc.). In our new paradigm, an e-commerce order can be based simply on two assertions; a cryptographically linked assertion of guarantee to pay and delivery address, together with an assertion about the level of immutability of the entity:person to the device they are using. As long as both are signed by the authoritative source, and the level of immutability meets the risk tolerance of the vendor, then no account, log-in or other information should be required.

11. Building blocks

At a fundamental level our work to date suggests that all the basic building blocks for a global solution exist; it is "simply" a question of understanding the business-use models and ensuring that how the "blocks" are arranged address those needs – globally.

11.1. Existing Standards

Where possible, the aim is not to invent new standards, but simply use existing standards, solutions, and building blocks that already exist, joining them together in a standard manner to perform the desired outcome.



11.2. Cryptography

There are two requirements for the cryptography in the ecosystem;

First; It must be secure, and remain secure for the foreseeable future, and;

Second; it must be fully open, fully inspectable, royalty free, and capable of being implemented by anyone who wishes to.

To achieve global acceptability, the ability to inspect and be satisfied that it is truly secure (and not deliberately weakened) and there are no back-doors to the encryption, is critical.

Certain areas of the cryptographic solution, particularly those around public-private key pairs, will probably need to utilise post-quantum (PQ) cryptography.

It is envisaged that the basic concepts behind hashing, data compression, symmetric-key cryptography and finally public-key cryptography form the underlying techniques for a viable solution, are all standard and are well understood.

11.3. Cryptographic one-way trust

The use of a cryptographically secure hash function that provides a one-way linkage between the Core Identifier and persona under it, and in turn the persona below them, provides a one-way trust; an ability for the entity to be able to have a relationship with its subordinate personas, but a third-party in possession of a particular persona is not able to "go back up the identity tree" and derive the core identity.

There are a number of cryptographic hash functions that are fast to compute (like SHA 256) with the strongest versions offering fast, practical solutions for one-way computation.

11.4. Personas

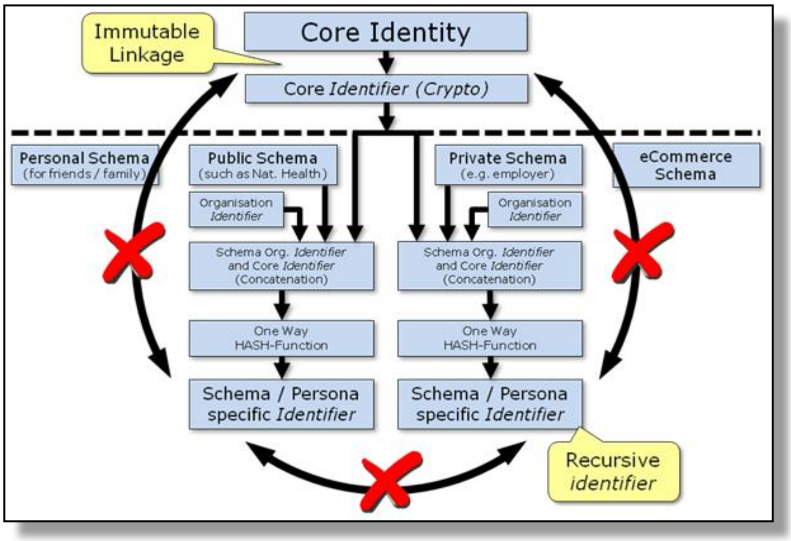

Immutable Linkage
Core Identity
Core Identifier (Crypto)
Personal Schema (for friends / family)
Public Schema (such as Nat. Health)
Private Schema (e.g. employer)
eCommerce Schema
Organisation Identifier
Organisation Identifier
Schema Org. Identifier and Core Identifier (Concatenation)
Schema Org. Identifier and Core Identifier (Concatenation)
One Way HASH-Function
One Way HASH-Function
Schema / Persona specific Identifier
Schema / Persona specific Identifier
Recursive identifier

Figure 5: EGIZ Personas (Jericho Forum variant)

***Credit:** This drawing was originally produced for and internal Jericho Forum discussion, and in turn takes its inspiration from the Austrian "E-Government Innovationszentrum – EGIZ", originally from a presentation by Thomas Gert Rössler showing how a stand-alone Core Identifier can be used to create a distributed set of personas. It is close in concept, but not an exact match, for what is being proposed in this paper.*

The concept of personas is critical an achieving a viable global identity ecosystem. Using personas has a number of key advantages;

- It is how humans operate their identity
- Implemented properly, they are privacy enhancing
- They manage the joins between disparate entities, for example; person and government (citizen persona), person and company (corporate persona), person and bank (credit card persona), laptop and company (corporate laptop persona) etc.
- A single persona can have a number of validated attributes, proofed and signed to an appropriate level, for example a Citizen Persona (a join of person and government) can have proofed and signed attributes for "date of birth", "place of birth", "sex at birth", "legal name", "citizenship rights".
- Personas can be created at will (primacy) by the entity, allowing personas with various trust levels; from high-trust (citizen & banking) to little-trust (self-asserted, reputational – such as e-Bay), or no-trust (anonymous but with sameness[4]).
- Personas can be created with no entity attributes, such as a voting persona.

11.5. Personas with cryptographic recursive self-similarity

For a persona to be unique it needs to have a unique cryptographic identifier (cryptographic keys) connected to the parent via a one-way trust. Entities will have multiple personas that can be as simple or as complex and as deep as desired. Most people will probably have a relatively simple set of personas linked to their (core) identity, while some entities (for example a corporation) will likely have a complex and many-level identity tree.

When dealing with a particular persona it should be impossible to know where in their identity tree that persona resides; thus, as well as having a single, standard methodology for handling the joins between entities and their personas it is critical that the cryptographic format for the persona identifiers have "recursive self-similarity", that is; they have the same form and function irrespective of position in the identity tree or the entity type.

[4] "pseudo-anonymous sameness" proves that it's the same person repeatedly, even if you do not know who they are.

11.6. Assertions

The linkage down the identity tree allows an entity to make multiple linked assertions from different personas with the relying party able to validate that only one, single entity, could have made that set of linked assertions.

Thus, in the example (Figure 6) shows how a high value and potentially high-risk transaction can be made using a set of linked assertions each signed by the authoritative source for those attributes.

Secure assertion languages are well established, and can be extended to make multiple linked assertions.

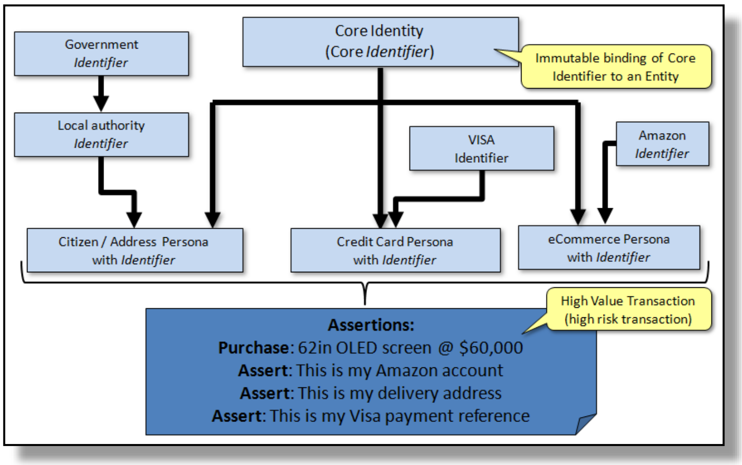

Government Identifier
Core Identity (Core Identifier)
Immutable binding of Core Identifier to an Entity
Local authority Identifier
VISA Identifier
Amazon Identifier
Citizen / Address Persona with Identifier
Credit Card Persona with Identifier
eCommerce Persona with Identifier
High Value Transaction (high risk transaction)
Assertions:
Purchase: 62in OLED screen @ $60,000
Assert: This is my Amazon account
Assert: This is my delivery address
Assert: This is my Visa payment reference

Figure 6: A high-value transaction using personas and signed attributes

Showing how linked assertions from different (linked) persona can be used to make a trusted high-value transaction.

Caching assertions in a secure environment allows assertions to be re-mixed into a format under the entity's control (using a device such as a smart-phone that allows better user interaction). Cached assertions can factor into the third-parties risk equation and could include the third-party requesting that the linkage between attributes, personas and the core identifier is revalidated (via verifying the immutable linkage in real-time) for high value transactions.

11.7. Identity Mixer – Privacy by design

Key to any identity solution is one that has privacy of the entity at the centre of its design. Identity Mixer (idemix) is an anonymous credential system developed at IBM Research that enables strong authentication and privacy at the same time.

This is a suite of cryptographic protocols that allow privacy in identity management to be enhanced and available in an open-source implementation of cryptographic algorithms and protocols to realize an efficient anonymous credential system. This work is partially funded by the PrimeLife[xxi] research project funded by the European Commission's 7th Framework Programme.

11.8. Devices

Currently there is a lack of viable devices that will provide the cryptographic-repository for the Core Identity and that are guaranteed to only be usable by the entity linked to it. Fixing this block is a key enabler to increased trust in a viable, global, identity ecosystem.

The requirement is for a device that has, dependant on the authentication level required, some or all of the following features;

- Is capable of being used stand-alone in a wide variety of circumstances
- Is simple to use (can your Grandmother easily use it?)
- Can provide a definable level (risk) of immutable binding between entity and device
- Is able to assert the standard to which the immutability is guaranteed
- Is able to assert the model (and therefore functionality) of the device
- Is able to assert the chain of custody from manufacture to issue to the entity
- Retains all private key cryptography securely and tamper-proof on-device
- Retains all cryptographic links to paired personas securely and tamper-proof on-device
- Where biometrics are used, any stored biometric does not leave the device
- Can optionally support duress feedback
- Can optionally support both feedback to the user as well as requests for more information / revalidation
- Supports a variety of interfaces, probably a chip-card interface, RFID as well as NFC

- Performs all cryptographic verification, as well as any biometric matching, "on-device"

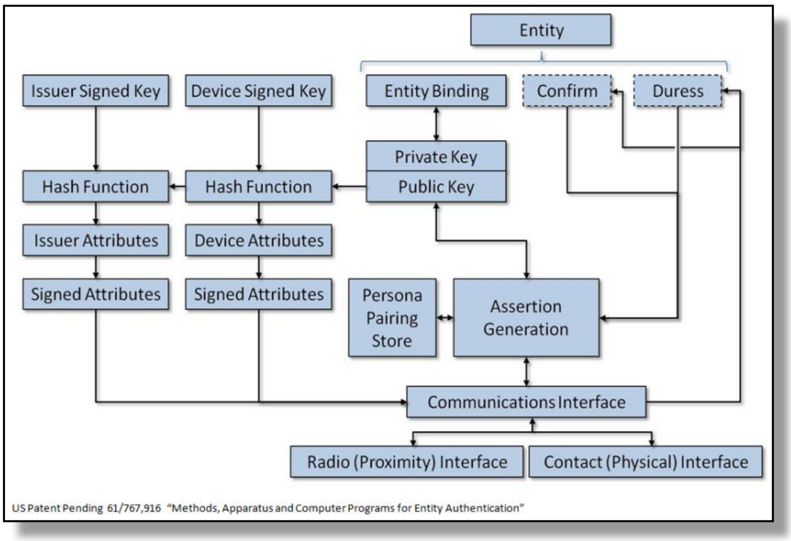


Figure 7: Identity Device block diagram

Block diagram of a proposed core identifier device

As part of a "chain of custody" assertion, it would be feasible for a device model to be validated by governments and then issued by a trusted process, including initialising and immutably linking the entity to the device as well as training the recipient in its use, as well as any duress functions, thus potentially meeting the need for a government grade identity device capable of meeting border-entry requirements.

11.9. Device portability and updates

An area that needs to be addressed is the potential need to migrate to newer hardware during the lifetime of the entity, while maintaining said device as the only place personas and private keys exist.

The need to migrate could be for a number of reasons, among them obsolete hardware, the need to support new physical and RF interfaces, or that a particular device has security flaws or exploits against it which necessitates the need to migrate to a newer, more secure device.

Work done by the Trusted Computing Group (TCG) on the "TPM Key Backup and Recovery for Trusted Platforms[xxii]" seems to provide solutions in this area.

11.10. Trust ecosystem

For trust in identity, personas and attributes outside of your locus-of-control, there needs to be a viable global trust ecosystem which provides a verifiable level of trust and allows the verification of the identities and attributes that are being asserted.

Having identity, persona and attributes proofed, issued and signed by their authoritative source limits the need to have signing authorities thus making a trust ecosystem viable and globally scalable. The current (broken) model of having random businesses that perform proofing to various levels of assurance makes it impossible on a global scale for trust to be established in any current identity ecosystem.

For example; the validation of citizen persona and attributes can be limited to approximately 300 signing authorities[5], a Visa, Mastercard or American Express persona and attributes is potentially just a single point of reference, while corporate persona and attributes are a single point of reference for verifying and ensuring trust in those corporate persona and attributes.

[5] The approximate number of passport issuing authorities

12. Why a global foundation?

12.1. The need to be different

This is about getting the right people, the key global players, into the same neutral environment, sponsored either by their respective companies, or if necessary, specifically invited as recognised industry experts with key expertise.

For this to be successful this needs to be a global initiative, not constrained by the aspirations of national governments, or the aspirations of any one corporation. Anyone should be able to implement the solution, or leverage the Identity from the solution within their products thus prohibiting monopolization of the technology.

The aim is a single solution, acceptable to all individuals, at a cost all citizens can afford.

12.2. Why a global not-for-profit foundation?

For competitors to work together, with no preconceptions or industry bias, there needs to be a neutral and safe environment that operates with a global remit.

This is not a research project, taking years and publishing papers, the aim is to push towards a viable solution designed to work globally, and that will equally be accepted by Governments, corporations and the citizens of the globe.

The foundation needs to be the legal entity for the intellectual property (IP) that is developed and hold any core patent(s) and/or IP such that it can have unrestricted use by anyone that follows those agreed standards.

The foundation has no interest or intention to build anything, or sell any identity services. Clearly the foundation is not authoritative for any part of the identity chain (notwithstanding the standards themselves) and thus has no part to play in any operational or service capacity.

12.3. Standards?

A single global specification / standard and interoperability criteria allowing the solution to be implemented anywhere, by anyone, usable by every entity on the planet. The aim is to use (re-use) as many open standards as possible. Where new standards are required then they will be submitted to the appropriate body at the appropriate time.

12.4. Cost?

The target for a stand-alone identity device is an end-user price below US$25 (ideally sub-$15), which is individually affordable and/or capable of subsidy.

There will be many areas where a company will buy and provide such a device to its customers for free; Banking, Credit Cards and high-value Cellular Phones all have an obvious return-on-investment.

However, as this is a BYOiD device, a person only requires a single device, thus very quickly a critical mass can be achieved.

Downstream, no cost is envisaged in using the device or the API's.

12.5. Licensing

By licensing the IP to the device manufacturers, subject to a small royalty payment (estimated at sub-$1) allows the funding of ongoing research, maintenance of the API's and codebase that system developers require as well as interoperability testing and if required conformance testing.

12.6. What will we do differently?

Be inclusive and gather global experts together, funding their involvement if it is required to ensure global applicability and global involvement.

Be a single, independent organization, looking to maintain the purity of a clearly and concisely articulated goal, and delivering a pragmatic solution, while operating by consensus to ensure no one person nor organization can dominate.

Ensure an open solution/standard is produced that can be used anywhere and by anyone.

13. Outcomes

13.1. Building a viable solution

For a global identity solution to be viable and global then it needs to meet the following criteria;

- Be identical for all entity types
- Be based on open standards and fully peer-reviewed
- Ensure the privacy of the entities using the solution
- Work globally
- Have a low-cost or no-cost of entry

13.2. Adoption (code base, samples)

It is a fact of life these days that most programming is performed with high-level tools and with sample blocks of code and/or API's taken from manufactures or providers of services.

For any global deployment and adoption to be successful then we would aim to deliver;

- A set of securely-coded modules that serve as a demonstration for their incorporation into all operating systems, applications and web-servers
- A set of sample API's and clear guidance on how vendors can incorporate code into their commercial products and offerings.
- Clear guidance on how to validate Identity, Persona and Attributes from their authoritative sources
- Clear guidance on how to validate attributes and minimise transaction risk while consuming attributes in a privacy enhancing manner
- Clear guidance and examples on how to enhance security by offering access using an "entitlement" decision based on all (or as many as possible) identity, persona and attributes in the transaction chain

14. Why should I be interested?

14.1. Why should I get involved?

The Global Identity Foundation is a not-for-profit, vendor neutral organization, combining the identity requirements of numerous sectors of industry as well as other interested parties to define a consistent set of use cases for identity and from that a single set of requirements.

Building on the work of the Jericho Forum and many others, the aim is to expand a draft identity ecosystem to a viable solution set of capabilities that would be implemented by the many members, using global open-standards as the core foundational principles.

In this way, vendors can implement their piece of the identity puzzle, being able to rely on others to play their part, saving both money and time, with users able to bring their own single global identity (BYOiD) to all aspects of their digital lives. While users can be assured that using this single standard all the components will interact correctly while protecting their privacy and leaving them in control.

14.2. What can I contribute, and what do I get back in return?

Corporate members of the Global Identity Foundation will;

- Have access to all aspects of the process
- Be involved in scenario workshops
- Help refine the generic use cases (and define new use cases)
- Be involved in the distillation of those use cases into a set of identity ecosystem design requirements based around the concept of an entity being able to have a single global identity (and identifier).

Companies will want their experts in the areas relevant to them to be actively involved;

- To influence the global ecosystem design
- Have advanced knowledge of how their products may want to evolve in the future
- Understand new products or offerings that they may want to develop

14.3. Process timelines

An initial high-level process timeline envisages a duration of two years to reach the end of phase-three and the go/no-go decision point. The block diagram details a rough outline of the major activities.

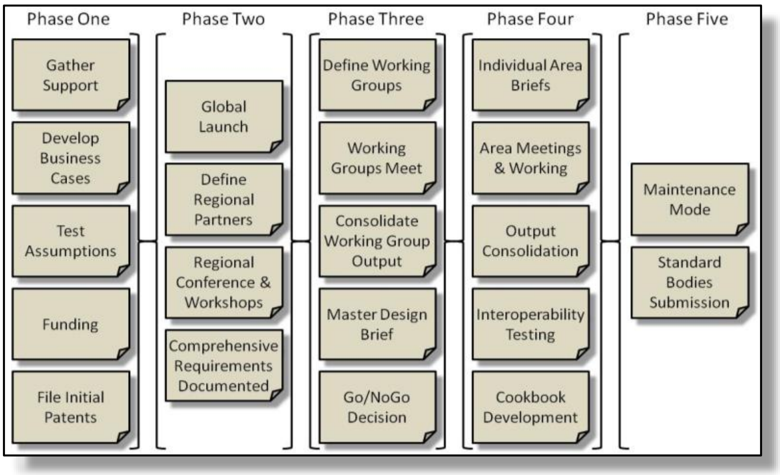


Figure 8: High-level plan

Block diagram of high-level activity

14.4. What does a future with global identity look like?

For people; accessing a site, application or item of hardware with the GiD Logo on it will let them know that they can interface safely and securely, and most importantly, simply and easily with that entity.

For other entities; they can add the GiD interface into products, web-sites, apps, and devices in the knowledge that it will enable a standard set of interfaces, allowing a more informed transactional risk decision to be made, interfacing with other entities in a standard manner, using code and methods maintained by an industry-neutral body.

15. References

[i] 2012 Estimates, Source: www.executiveboard.com/towergroup-blog/card-not-present-fraud-rising-problem-lagging-solution/

[ii] https://www.talosintelligence.com/reputation_center/email_rep (August 2019)

[iii] 2012 Figures, Source: royal.pingdom.com/2013/01/16/internet-2012-in-numbers/

[iv] https://www.cloudwards.net/email-security/

[v] https://www.bbc.co.uk/news/uk-47016671

[vi] "Addressing IT Self-Service Myths and Realities for Successful Implementations" www.gartner.com/resId=1409913.

[vii] www.mandylionlabs.com/PRCCalc/PRCCalc.htm

[viii] blogs.forrester.com/stephen_mann/12-06-21-it_service_management_and_automation_now_thats_a_double_whammy_of_business_enabling_goodness

[ix] www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/

[x] www.forbes.com/sites/kashmirhill/2011/04/15/the-password-is-dead-time-for-better-online-security/

[xi] www.wwpass.com

[xii] www.safe-biopharma.org

[xiii] www.tscp.org

[xiv] www.dailymail.co.uk/news/article-2298771/Policeman-Doug-Crossan-reports-13-year-old-son-Cameron-FRAUD-running-3-700-iPad.html

[xv] www.dailymail.co.uk/sciencetech/article-2284743/Apple-agrees-66m-compensation-US-parents-children-racked-huge-bills-buying-extra-content-free-iPad-games.html

[xvi] www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf - Domain 10 & Domain 12

[xvii] Commandment # 8 – Jericho Forum Commandments

[xviii] US Patent Pending 61/767,916 “Methods, Apparatus and Computer Programs for Entity Authentication”

[xix] www.opengroup.org/jericho/Jericho%20Forum%20Identity%20Commandments%20v1.0.pdf

[xx] www.opengroup.org/jericho/commandments_v1.2.pdf

[xxi] PrimeLife: A research project funded by the European Commission’s 7th Framework Programme

[xxii] http://www.trustedcomputinggroup.org/files/resource_files/ABEDDF95-1D09-3519-AD65431FC12992B4/Kazmierczak20Greg20-20TPM_Key_Management_KMS2008_v003.pdf