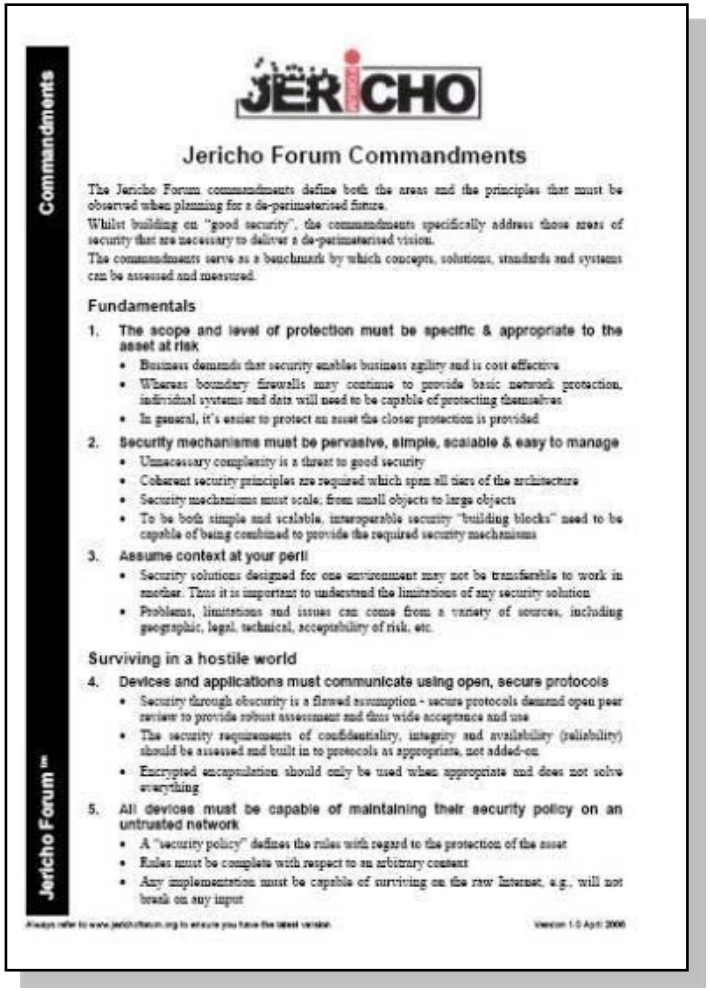
Jericho Forum®

Identity Webinar



Commandments

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterised future.

Whilst building on "good security", the commandments specifically address those areas of security that are necessary to deliver a de-perimeterised vision.

The commandments serve as a benchmark by which concepts, solutions, standards and systems can be assessed and measured.

Fundamentals

1. The scope and level of protection must be specific & appropriate to the asset at risk
   - Business demands that security enables business agility and is cost effective
   - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
   - In general, it's easier to protect an asset the closer protection is provided
2. Security mechanisms must be pervasive, simple, scalable & easy to manage
   - Unnecessary complexity is a threat to good security
   - Coherent security principles are required which span all tiers of the architecture
   - Security mechanisms must scale; from small objects to large objects
   - To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms
3. Assume context at your peril
   - Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
   - Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a hostile world

4. Devices and applications must communicate using open, secure protocols
   - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
   - The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added-on
   - Encrypted encapsulation should only be used when appropriate and does not solve everything
5. All devices must be capable of maintaining their security policy on an untrusted network
   - A "security policy" defines the rules with regard to the protection of the asset
   - Rules must be complete with respect to an arbitrary context
   - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

Always refer to www.jerichoforum.org to ensure you have the latest version. Version 1.0 April 2006

Jericho Forum™

Jericho Forum Commandments

Identity Commandments

"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) personas 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[4]) 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 personas can develop contextual trust, for example linkage to government issued attributes / identifiers.
3. The authoritative source of identity will be the unique identifier[5] 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 Personas (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 #6 apply to ensuring open, secure and interoperable standards
2 A core identifier may refer to a physical, biological or digital entity
3 Derived 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®

Jericho Forum Commandments

Jericho Forum Identity Commandments

Freely available at www.jerichoforum.org/publications.htm


JERICHO
FORUM

Photo © Paul Simmonds

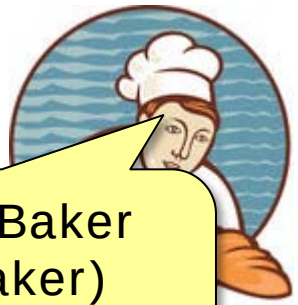
JERICHO FORUM

Q3

15 miles

Parents: David & Mary

Tom David-son (Tom Davidson) Attribute: Son of David & Mary



Tom the Baker (Tom Baker) Reputation: Good Bread

Same Person
or same ***Core Identity***

Facial Biometric
or ***Core Identifier***
Immutably linked

Two ***Personas***

Name: Tom Davidson
Age: 19
Address: Little Plumton
Father: David
Mother: Mary

Village Persona

15 miles

Name: Tom Baker
Occupation: Bread Seller
Reputation: Good
Business Address: Cart
Business Hours: Mon-Fri

Town Persona

Primacy: Yes

Royalty Free Clipart: http://www.clipartof.com/portfolio/patrimonio/

Key aspects for privacy & primacy

- Immutable linking of Core Identity to Core Identifier
  - The only thing we really care about is serial pseudo-anonymity
- Free to set up as many (or as few) Persona's
- The entity must have primacy over all it's personas
- One way trust from unique identifier to a persona
- Thus not able to go "back up the tree"
- Acid test: can you anonymously vote?

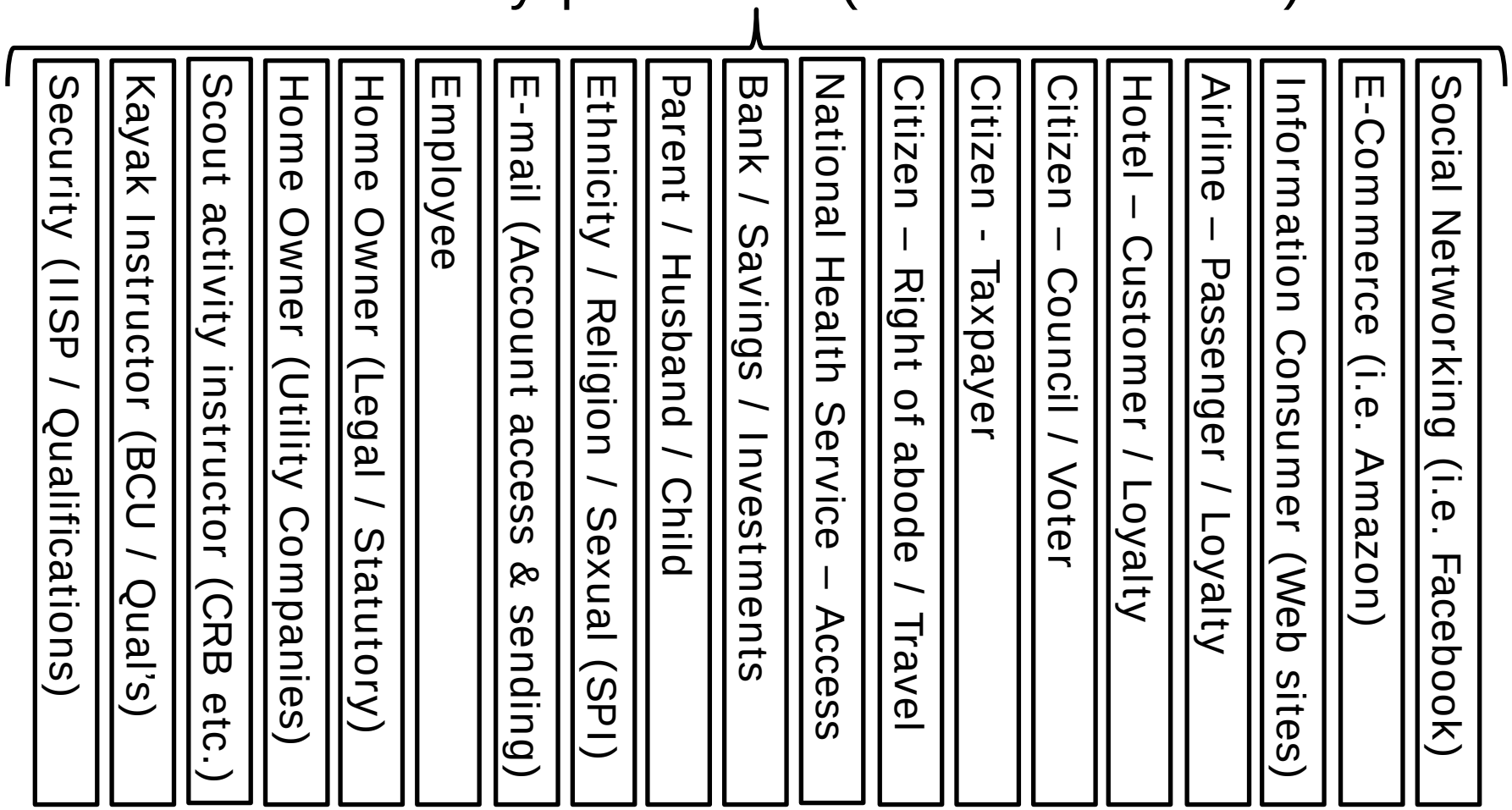
Entities

- Users
- Devices
- Organizations
- Code
- Agents

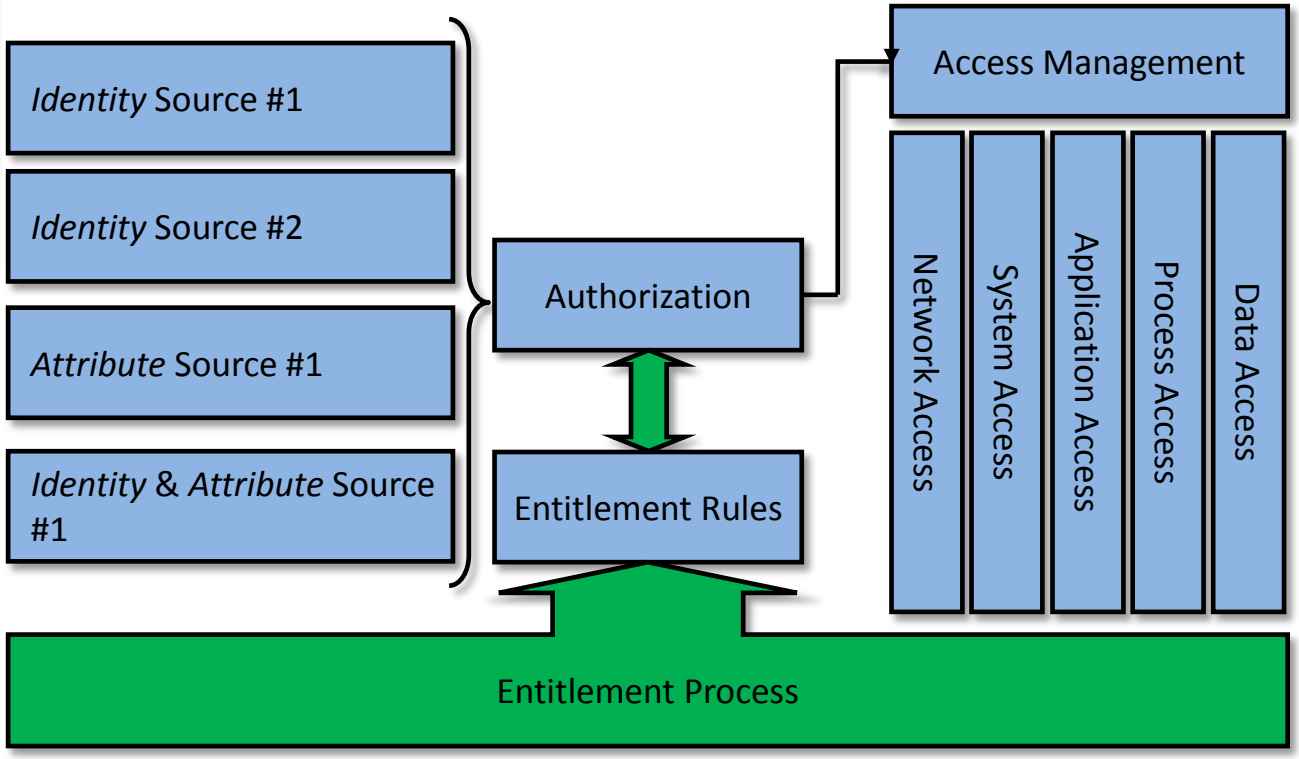
Note:
Data is not an entity unless self-protecting – then it's code!

Core Identity

Some of my persona's (Paul Simmonds)

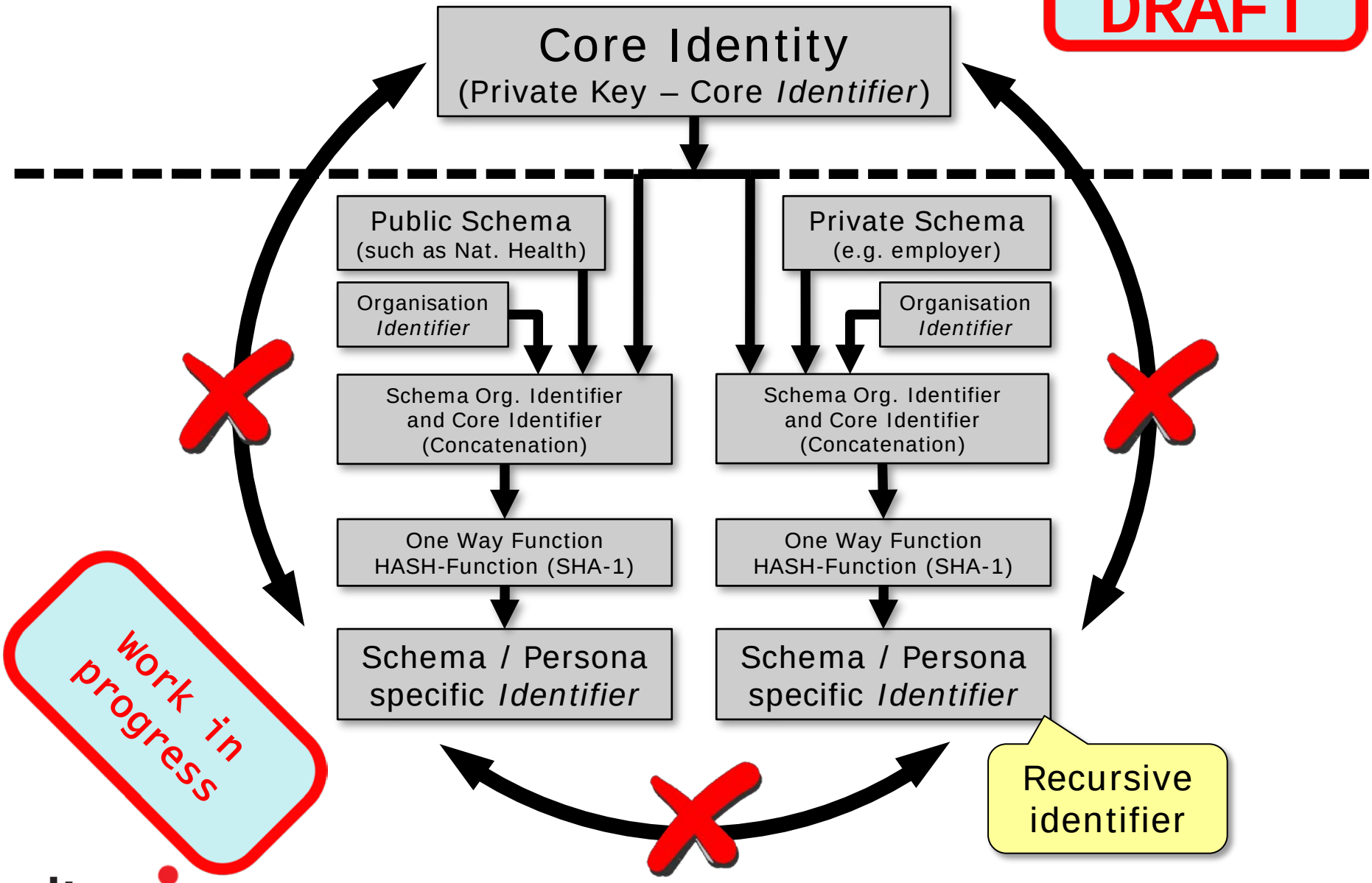


Personas of my *Core Identity*

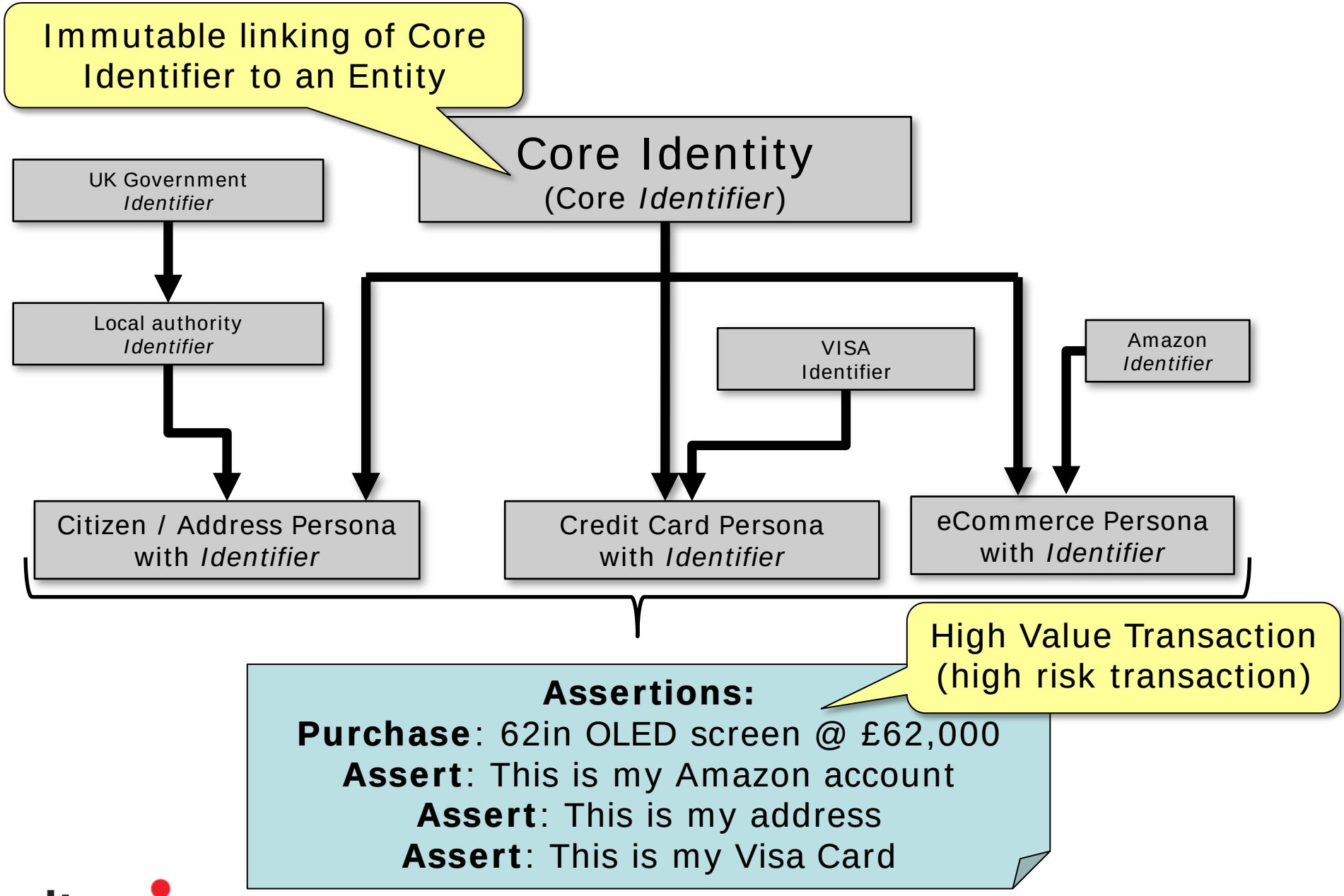


Source: CSA Guidelines v3.0

DRAFT



JERICHO FORUM


Immutable linking of Core Identifier to an Entity
Core Identity
(Core *Identifier*)
UK Government *Identifier*
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 @ £62,000
Assert: This is my Amazon account
Assert: This is my address
Assert: This is my Visa Card

Government Schemes

- UK ID Scheme (failed)
- NSTIC (National Strategy for Trusted Identity in Cyberspace)
- STORK (pan-European recognition of electronic Ids)
- UK Cabinet Office initiatives
- Other Government ID Schemes
  - German “EID card”
  - Austrian “Citizen Card”
  - Estonian “ID Card”
  - Finland “Citizen Certificate”
  - Hong Kong “Smart ID Card”
  - Malaysian “MyCad”
- EURIM

Acid tests for a good Identify Ecosystem

- Secure – open to review by experts
- Trust eco-system – needs to be built on rock
- Open cryptography
- Recursive cryptography
- Open implementation reference model
- Implementable anywhere in the world

Read more in the Jericho Forum response to NSTIC

http://www.nist.gov/nstic/governance-comments/Jericho-Forum_NSTIC-NOI-July2011.pdf

Action List

- Read the JF Identity Commandments
- Implement identity for all entities
- Mobile Device Management to onboard user-owned BYOD
- Implement authentication with attributes and rules (entitlement rules)
- Have good Master Data Management processes
- Develop a good identity strategy
- Perform an Identity risk assessment as it's foundation
- Get involved in NSTIC
- Add a SAML capability (to existing corporate ID solution)
- Adopt Open Authentication (OAuth)

Questions & Comments

Questions & Co
omments
Questions & Comment
Questions & Comments
ions & Comment

Shaping security for tomorrow's world

JERICHO FORUM