Entitlement; And Why Identity Needs to be About More Than Just People

PANELISTS:

Andrew Yeomans
Commerzbank

Paul Simmonds
Jericho Forum

Adrian Seccombe
Leading Edge Forum & University of Surrey

MODERATOR:

Dr. Guy Bunker
GB&A

Session ID: IAM-210

Session Classification: General Interest

An Introduction to Identity, Entitlement & Access Management

Paul Simmonds

RSA CONFERENCE EUROPE 2012

The Holy Grail

Entitlement Management

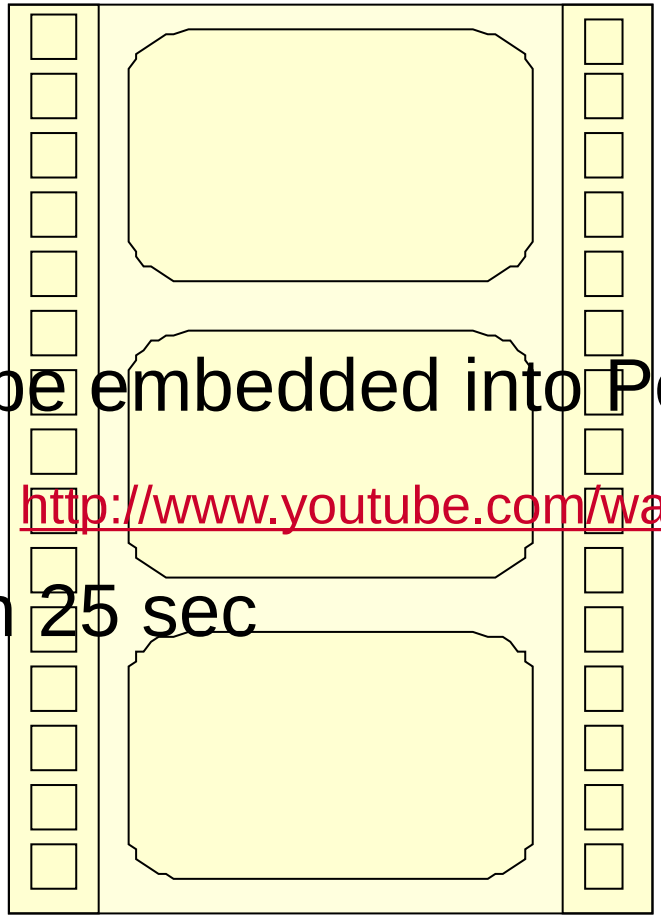
- Making a *risk-based decision*
- About access to data and/or systems
- Based on the trusted identity and attributes
- Of all the entities and components in the transaction chain.

Entities

- Users
- Devices
- Organizations
- Code
- Agents

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

An introduction to Core Identity



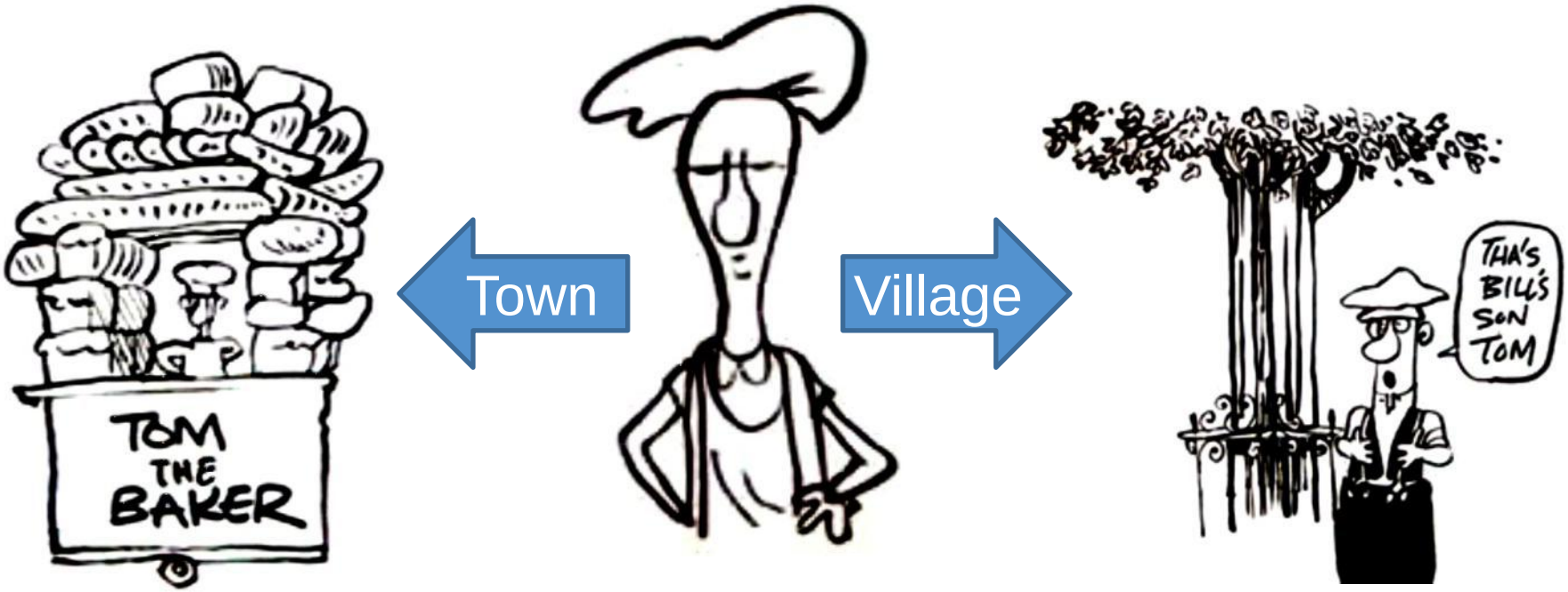
- Video: will be embedded into PowerPoint
- Preview at: http://www.youtube.com/watch?v=lryQ4WfjsVs
- Time: 3 min 25 sec

Core Identity

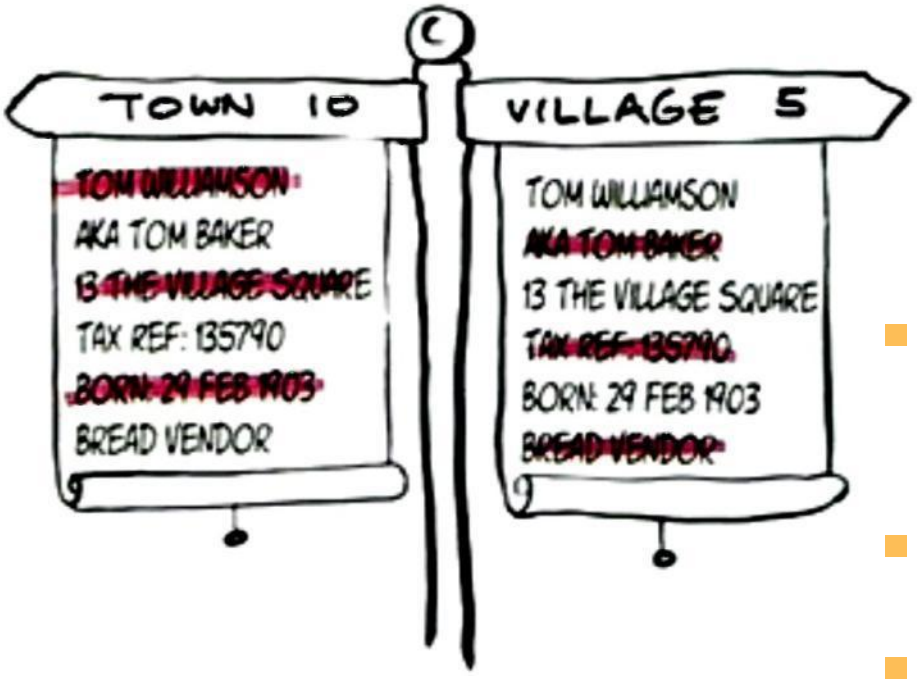
- We all have a core identity
- We are who we are;
- Each of us is a unique entity!

Core Identity

- We operate different facets of our lives with personas tailored to those interactions.
- This limits the number of attributes about ourselves exposed by each persona.



Core Identity

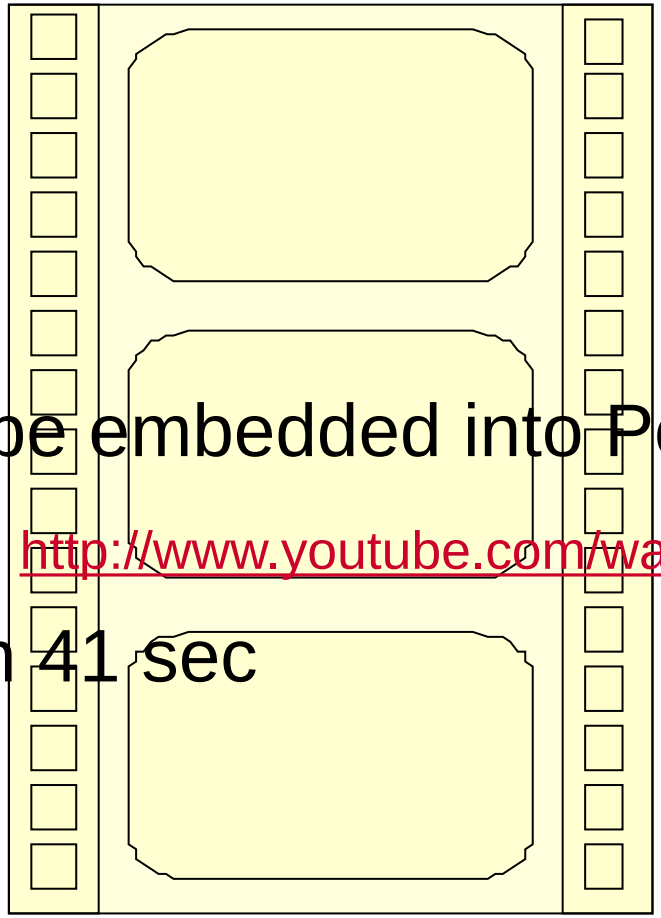


- Limiting attributes in each persona minimises the risk of connecting our different personas.
- Reduces the chance of “Attribute Aggregation”
- Is “privacy enhancing”
- Retains control (primacy) over our personas and related attributes.

Core Identity

- The information we reveal about ourselves in a particular persona
- Is directly related to the trust we have in the people we interact with
- And the value of the transaction.

Operating with Personas



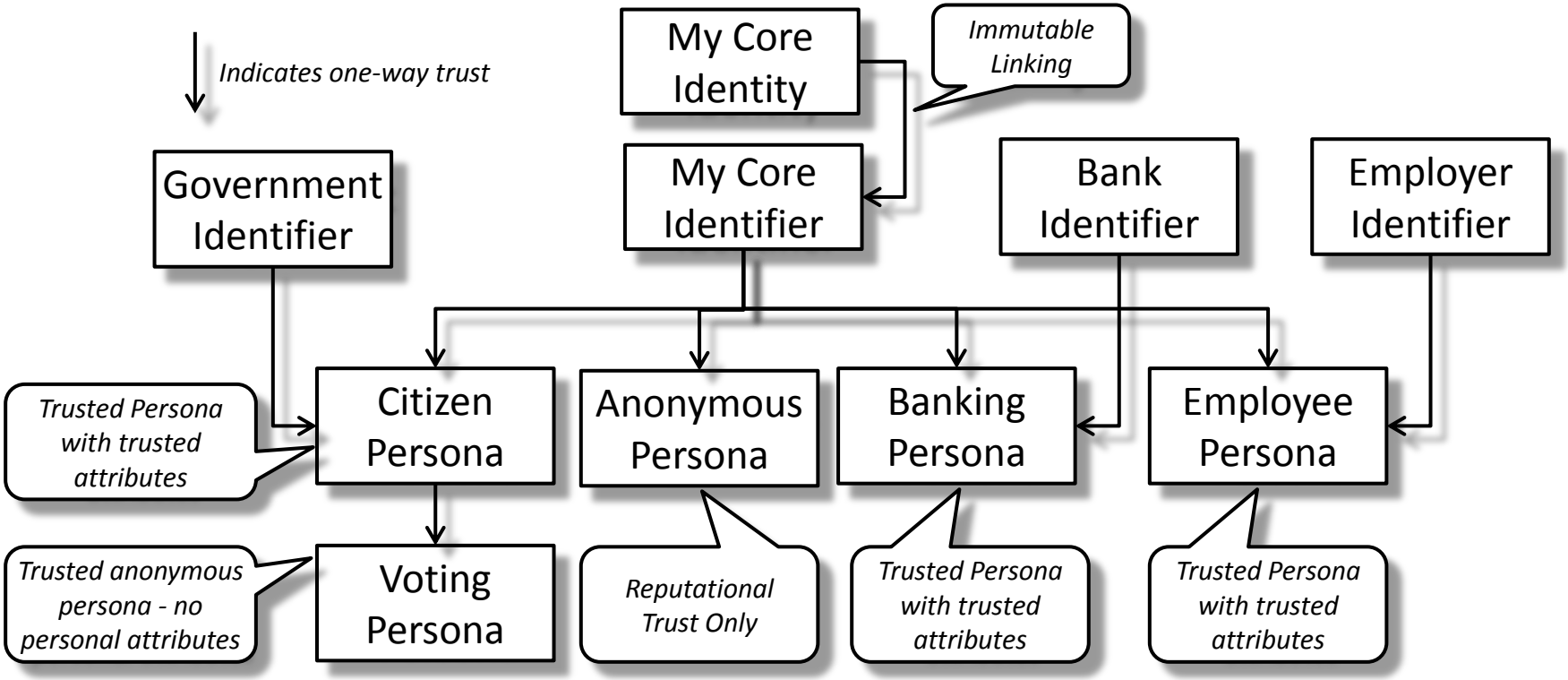
- Video: will be embedded into PowerPoint
- Preview at: http://www.youtube.com/watch?v=X5SdVX7cF00
- Time: 2 min 41 sec

Operating with Personas

- Persona identifiers can be created by joining two identifiers
- For example;
  - A core identifier, and;
  - An organisational identifier.

Operating with Personas

- There can be as many or as few levels in an identity tree as required.



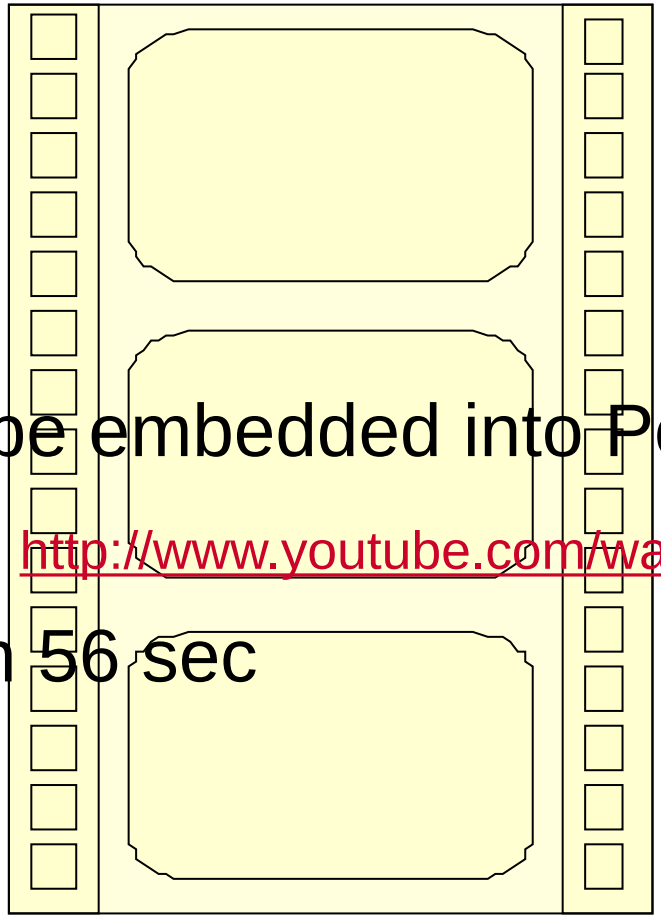
Operating with Personas

- Trust in the persona is the combination of;
  - The trust in the relationship to the Core Identity
  - The organisation identity, and;
  - The attribute provider
- Ranging from high-trust, to;
- No-trust

For example:
Your "Citizen" Persona

For example:
A Self-asserted Persona

Trust & Privacy

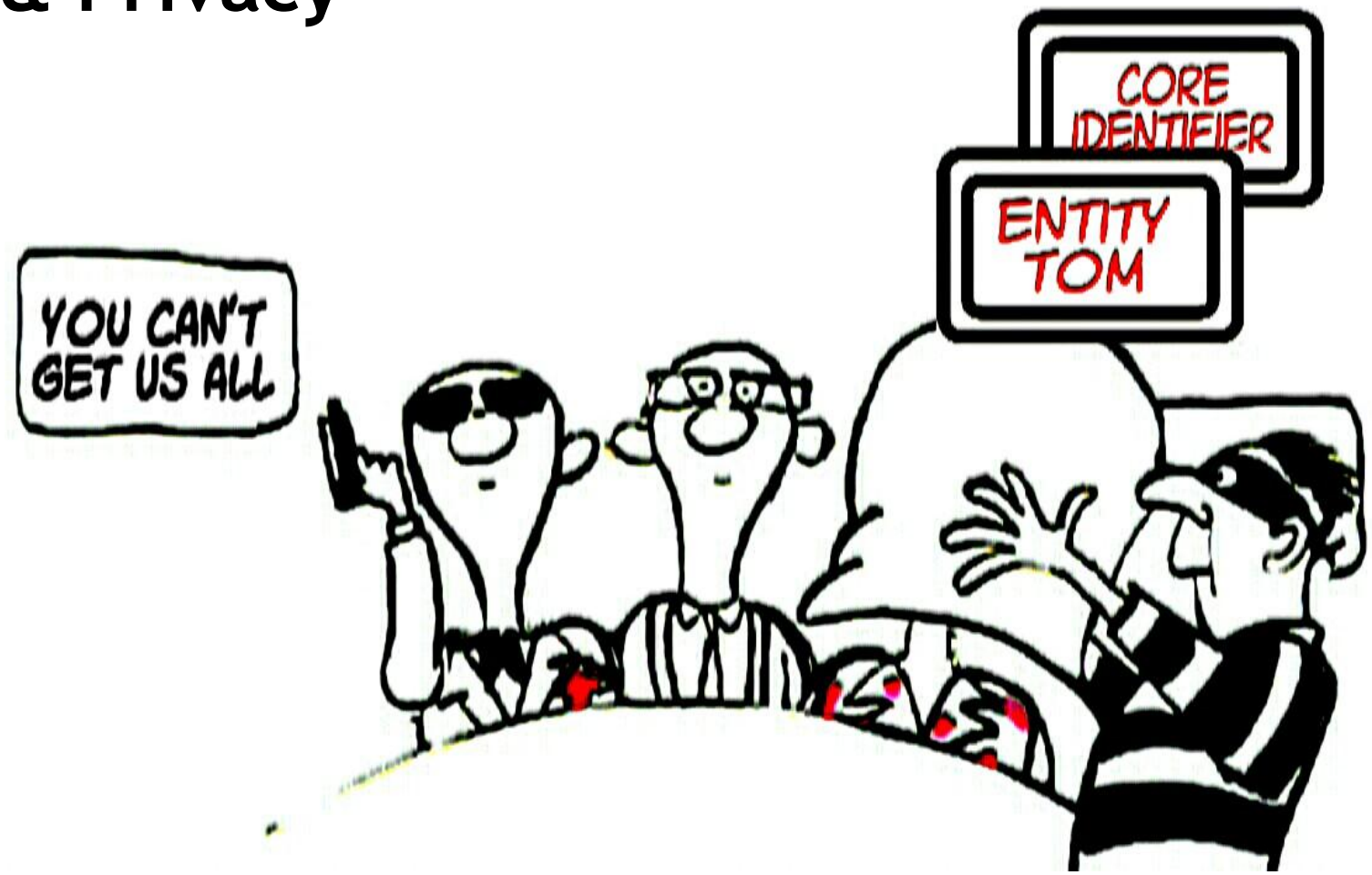


- Video: will be embedded into PowerPoint
- Preview at: http://www.youtube.com/watch?v=kZwKDWIL7vs
- Time: 2 min 56 sec

Trust & Privacy

- Having different personas allows each persona to operate with different levels of trust
- Personal choice to associate attributes to different personas with different levels of trust

Trust & Privacy

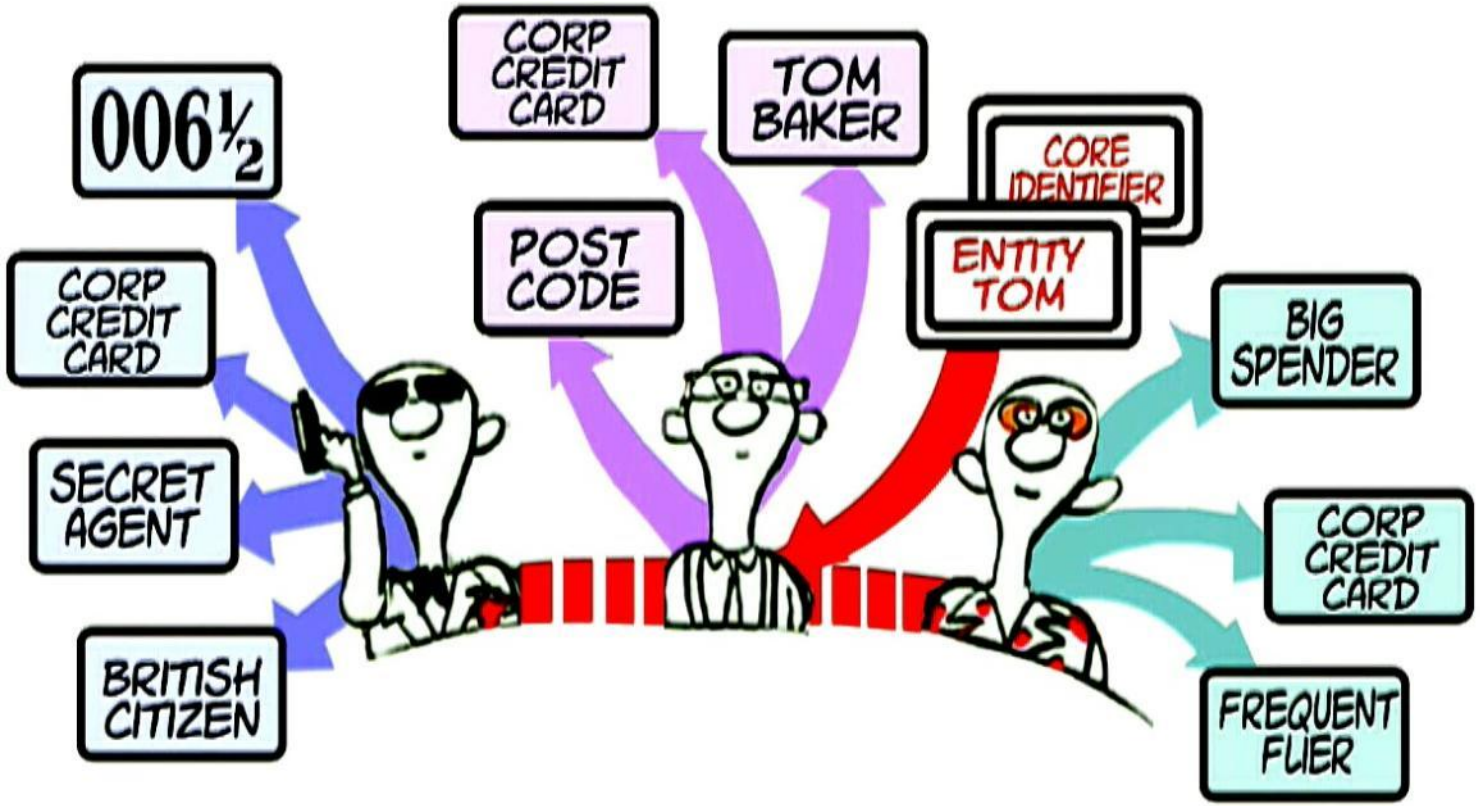


- Distributed personas will minimise the damage and loss of attributes if they are compromised.

Trust & Privacy

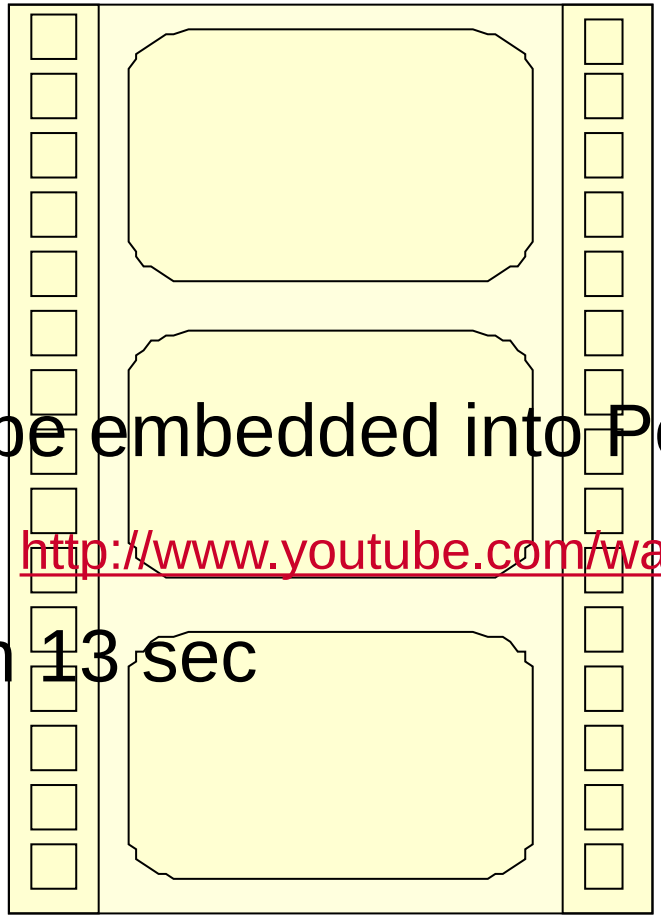
- Fundamental difference to a super-repository of attributes
- Total compromise if successfully hacked
- Or accessed by a corrupt government.

Trust & Privacy



- Distributed personas and ability to assert attributes from multiple personas minimises attribute exposure
- Reduces ability for identity aggregation another privacy enhancing feature

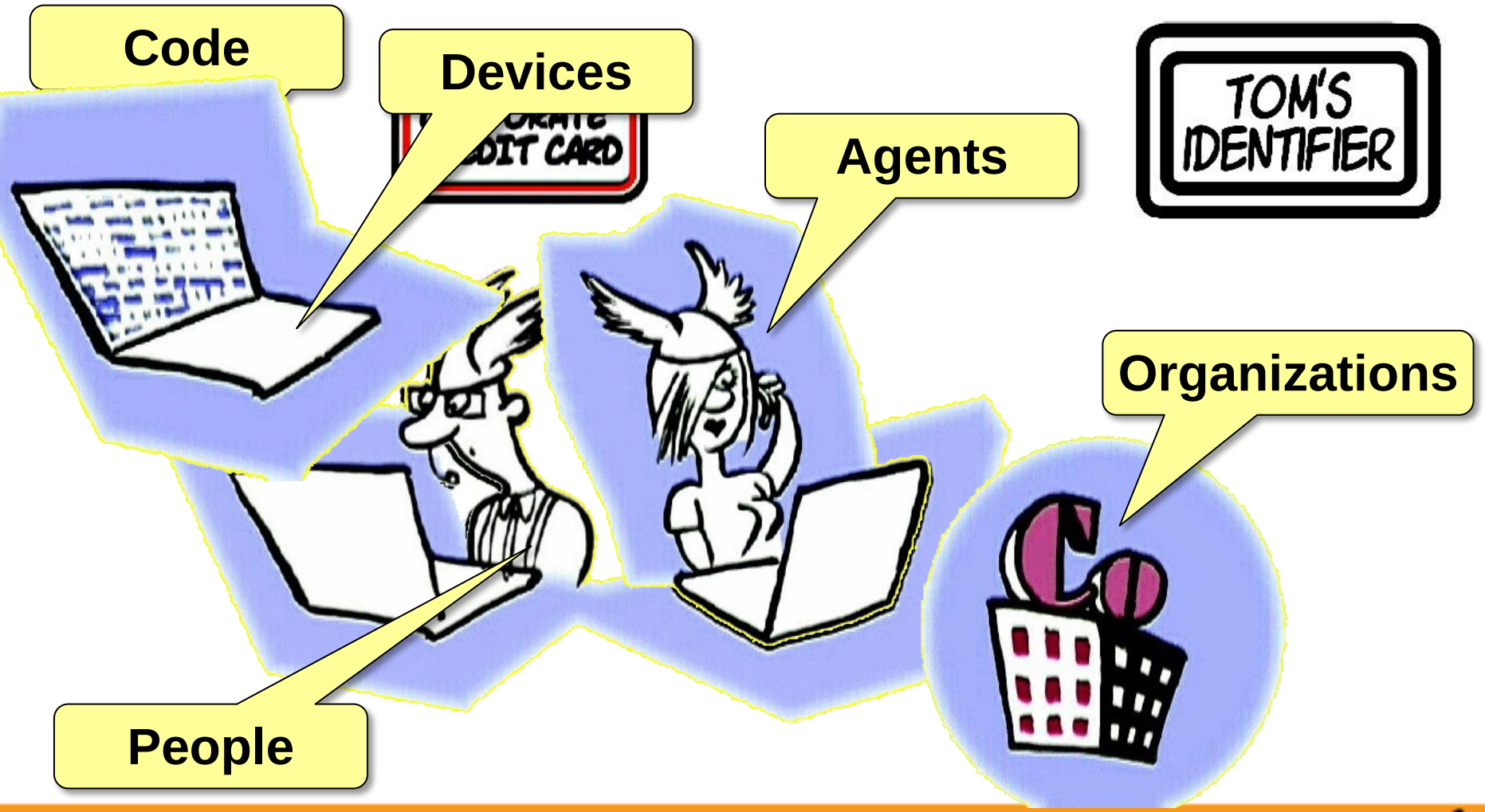
The Bigger Picture

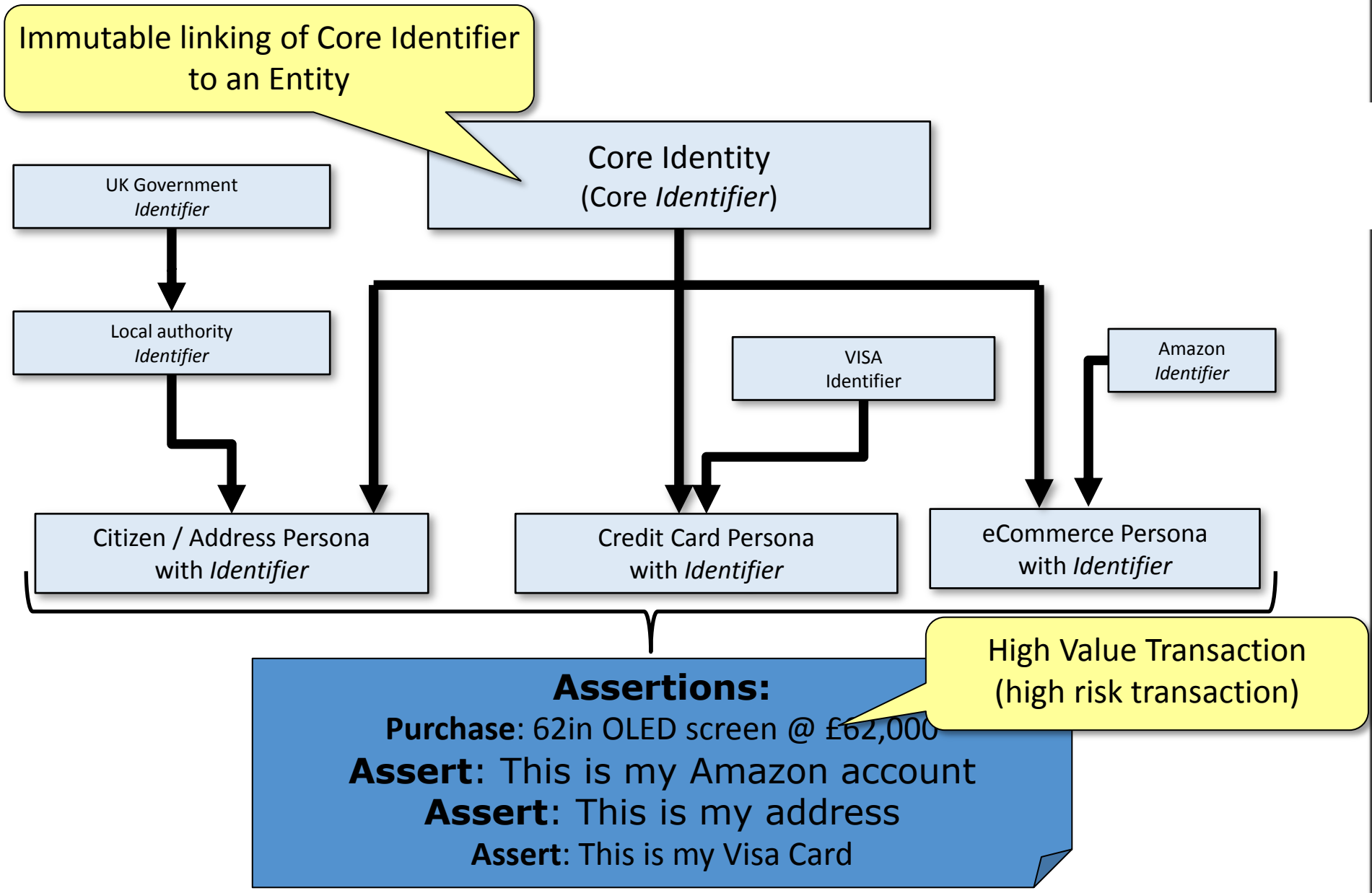


- Video: will be embedded into PowerPoint
- Preview at: http://www.youtube.com/watch?v=1DOYvRmn94E
- Time: 2 min 13 sec

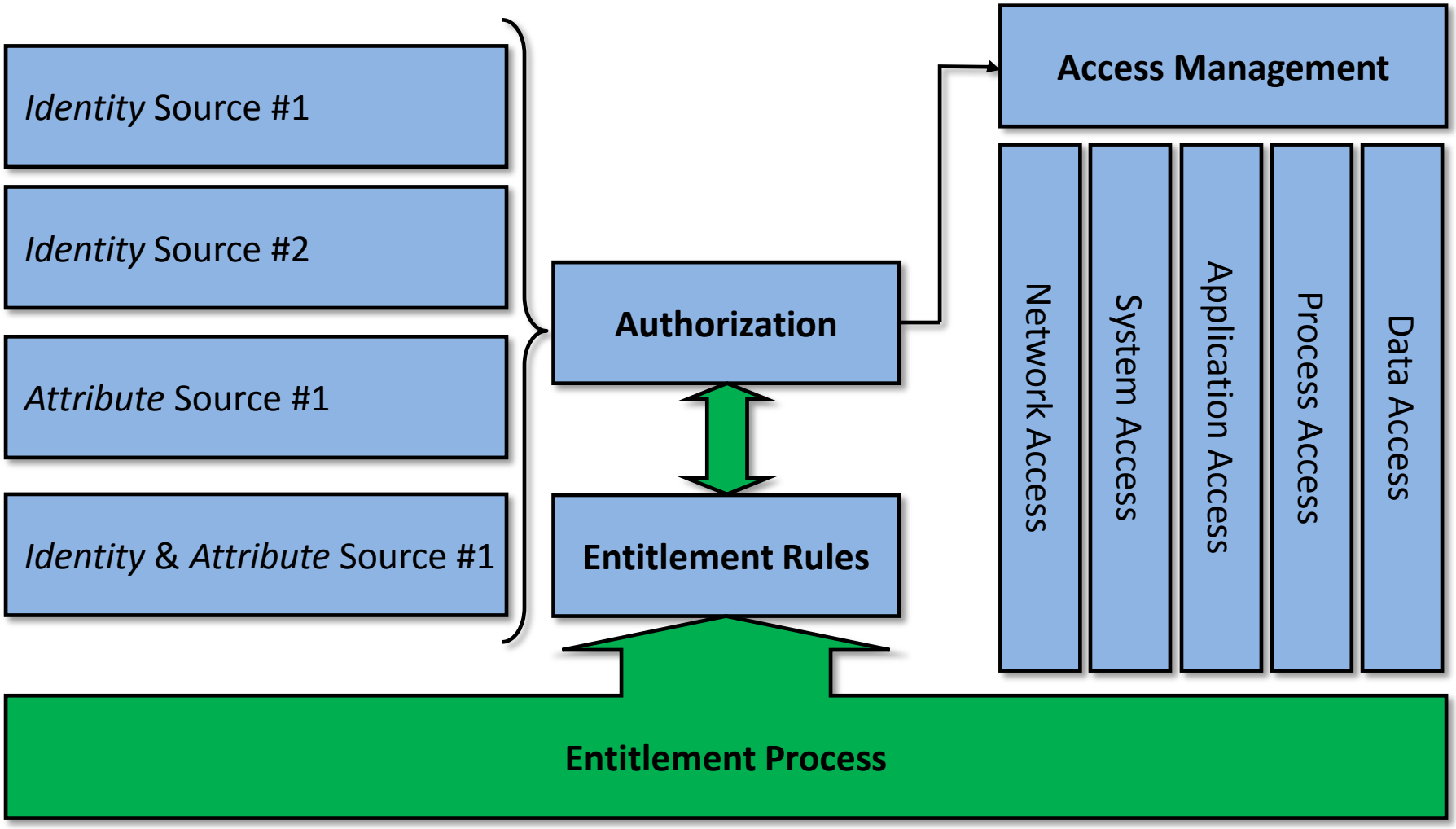
The Bigger Picture

- Identity needs to cover more than just people




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*
Assertions:
Purchase: 62in OLED screen @ £62,000
Assert: This is my Amazon account
Assert: This is my address
Assert: This is my Visa Card
High Value Transaction
(high risk transaction)

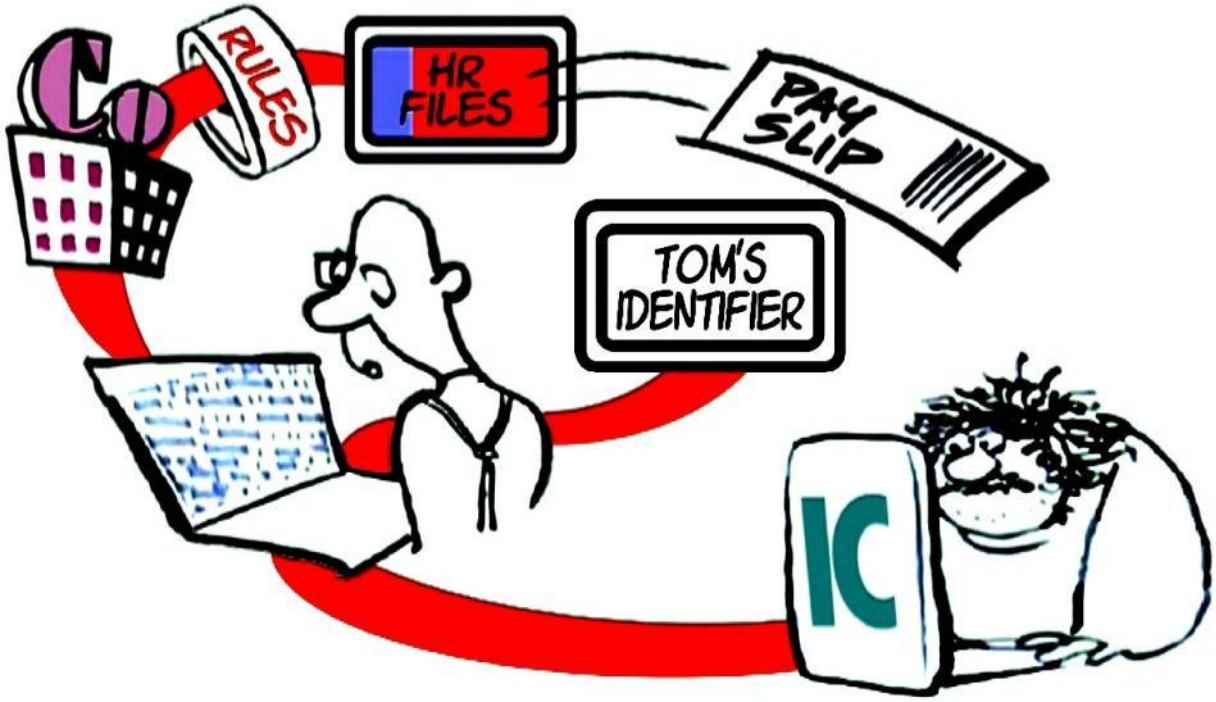
The Bigger Picture



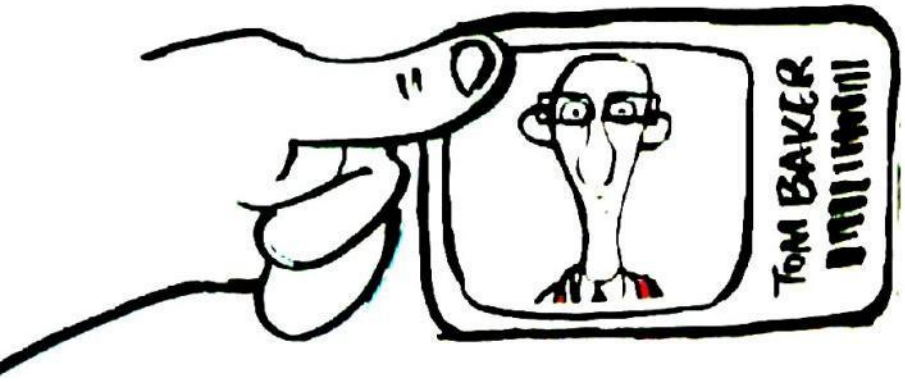
Source: CSA Guidelines v3.0

The Bigger Picture

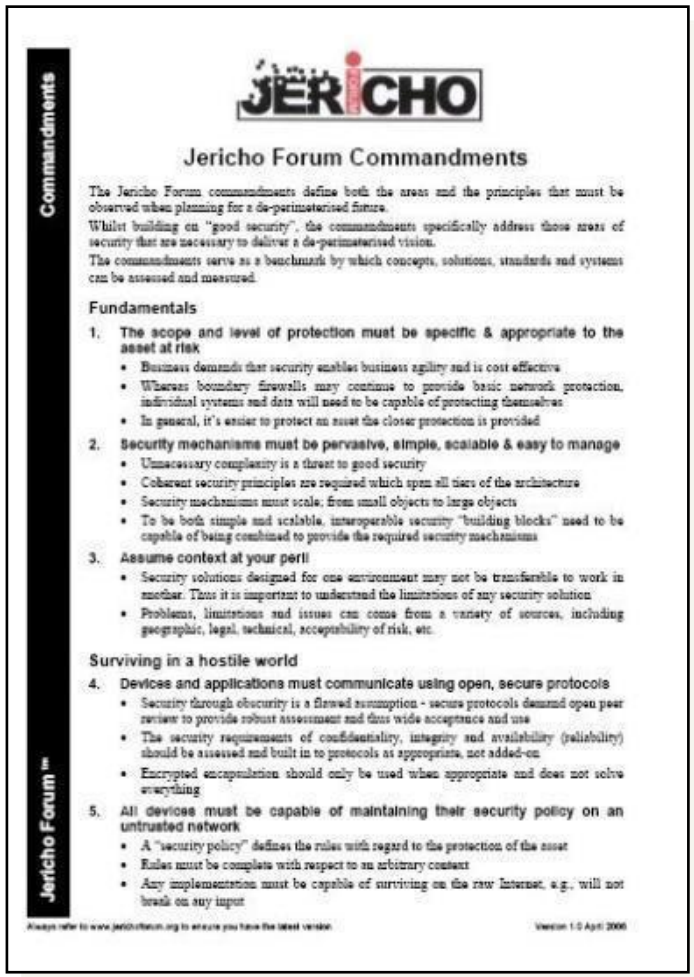
- Properly implemented entitlement rules;
  - Minimise the identity (persona) exposed
  - Minimise the attributes required to be exposed
  - Are privacy enhancing
  - Are Compliance enhancing



Putting it all together



- Key to the trust is the immutable linking of Entity to the digital Core Identifier
- This needs to happen in a form factor that;
  - Guarantees the binding
  - Is usable by Joe Public
  - Provides the interfaces necessary to connect with the digital world



Commandments

Jericho Forum™

JERICHO

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 Commandments

Identity Commandments

Jericho Forum®

JERICHO

"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[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 #6 apply to ensuring open, secure and interoperable standards

2 A core identifier may refer to a physical, biological or digital entity

3 Denial pseudo-anonymity guarantees the same entity in multiple interactions without being able to identify the actual entity

4 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 Identity Commandments

Freely available at www.jerichoforum.org

Entitlement; And Why Identity Needs to be About More Than Just People

PANELISTS:

Andrew Yeomans
Commerzbank

Paul Simmonds
Jericho Forum

Adrian Seccombe
Leading Edge Forum & University of Surrey

MODERATOR:

Dr. Guy Bunker
GB&A

Take Away & Apply

- Entitlement is part of the ID solution needed for global collaboration
- Solutions exist today and answer part of the question
- We need to build additional demand to make this ‘a global standard’
- When looking to the cloud, think and plan for the bigger picture

Shaping security for tomorrow's world

Panel Discussion Questions & Points to cover

- Standards are great..... Everyone has one – are there too many standards?
- What other ID schemes are being developed?
  - [Andrew] 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

Panel Discussion Questions & Points to cover

- Why do government ID schemes historically fail?
  - [Andrew] JF#8 - Authentication, authorisation and accountability must interoperate / exchange outside of your locus / area of control
    - People/systems must be able to manage permissions of resources and rights of users they don't control
    - There must be capability of trusting an organisation, which can authenticate individuals or groups, thus eliminating the need to create separate identities
  - [Paul] Government only considers citizens – Internet, commerce, business all global thus - to-date all Gov schemes "implode" to a sub-set of Gov services
  - [Adrian] Mindset (Set by Spooks) but also ingrained in IT thinking, that Government MUST own the root of a persons identity
  - [Andrew] Lack of global or critical mass adoption (historically default to lowest-common-denominator standards, SMTP E-mail, HTTP, Telnet, FTP, Facebook for Identity)
- Is the "One ring to rule them all" a good idea?
  - [Adrian] Anonymous Core Identifier and binding personas to it YES
  - [Paul] Putting all identities in a super-repository – NO (Theft, Impersonation)

Panel Discussion Questions & Points to cover

- Are we deluding ourselves that a global “identity eco-system” is possible?
  - [Andrew] Facebook demonstrates that a critical mass ID eco-system can work (but Low Grade / Self Asserted) and business / government will use it
  - [Paul] Challenge is to add Core ID / Immutably Bound / Digital ID above it to give it a high grade assertion “that I am who I say I am”
- What will it take to build this?
  - [Adrian] Monetising the transactions, credit cards, lottery tickets, high grade identity reduces fraud - $2.4Bn (Global Card Fraud)
  - [Andrew] Needs global agreement – standards, NSTIC, governments particularly (as potential roots of trust) needs to agree no a non-country specific solution
- How long for this to become ubiquitous?
  - [Paul] Facebook to 1Bn users in 8 years
    With serious benefits, and savings to the financial industry critial mass could be sooner.

Panel Discussion Questions & Points to cover

- Will the liability issue scupper the development of a global system.
  - [Paul]
    Hopefully it will kill off the “super-repository”
    Key flaw in current thinking, that IDP going hold secondary data
    Attributes must come from authoritative source
    Employment records (bank details), clean driving licence (DVLA),

- What would it take for Commerce Bank / Surry Uni to enrol new users with an external ID.
  - [Adrian] In 2008 Boston collage stopped offering e-mail addresses – BYO-E-Mail, how long before BYO-Id?
  - [Andrew] ??