The Global Identity Foundation
A single global identity for humanity

Identity is the new Currency

Paul Simmonds
CEO
The Global Identity Foundation

uk.linkedin.com/in/psimmonds/
www.globalidentityfoundation.org
info@globalidentityfoundation.org

Agenda

Background to the problem(s)

- Externalisation of Data
- The Identity problem(s)

Design requirements

- Entitlement
- Entities
- Trusted Attributes

Examples

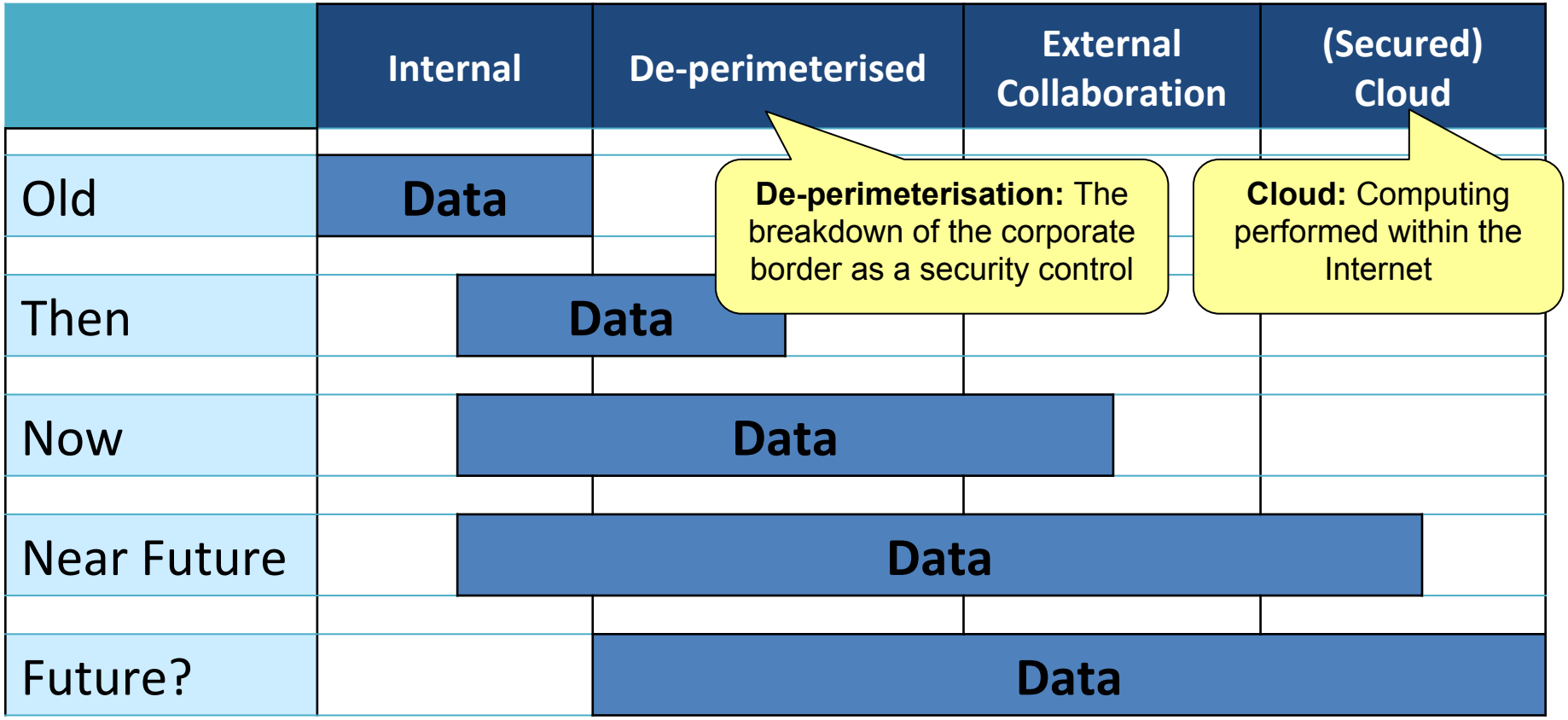
Personas and future states

Challenges

Summary

Q&A

Data is being externalised



The security of the network becomes increasingly irrelevant, and the security and integrity of the data becomes everything.

Question?

66%

2013 Mobile Consumer Insights, Jumio, Inc

Given a choice;

★

When faced with a request for user-name and other information

★

How many people abandon the transaction?

Question?

39%

Ukash research,
Sept 2013

How many people shop with an existing supplier

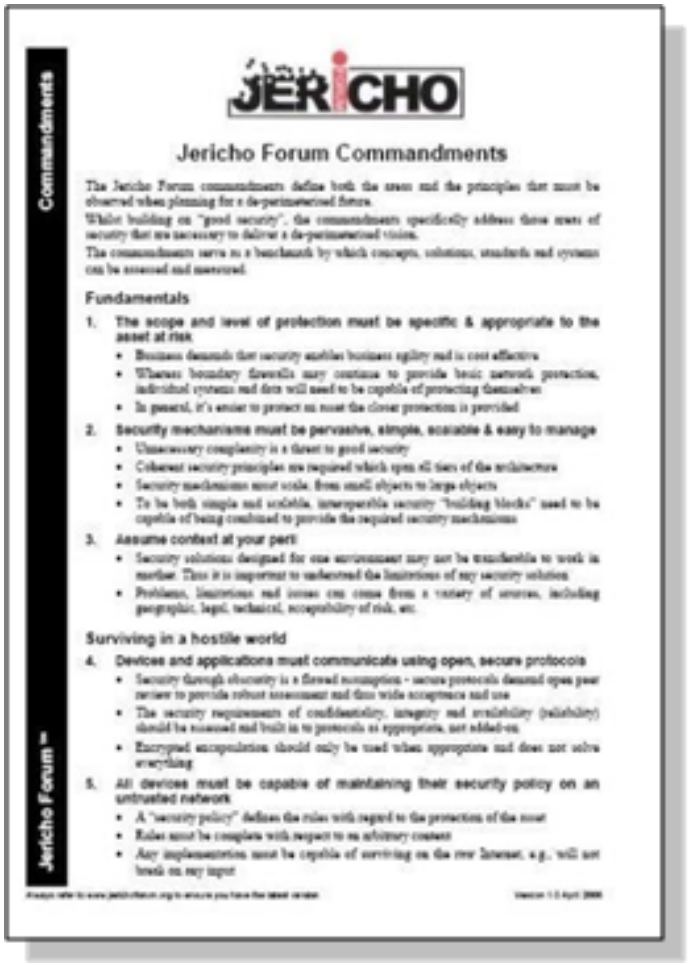
Even when it's more expensive

Rather than create a new account elsewhere?

Jericho Forum Commandment #8
Identity, Management and Federation

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
- Multiple loci (areas) of control must be supported



Commandments

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

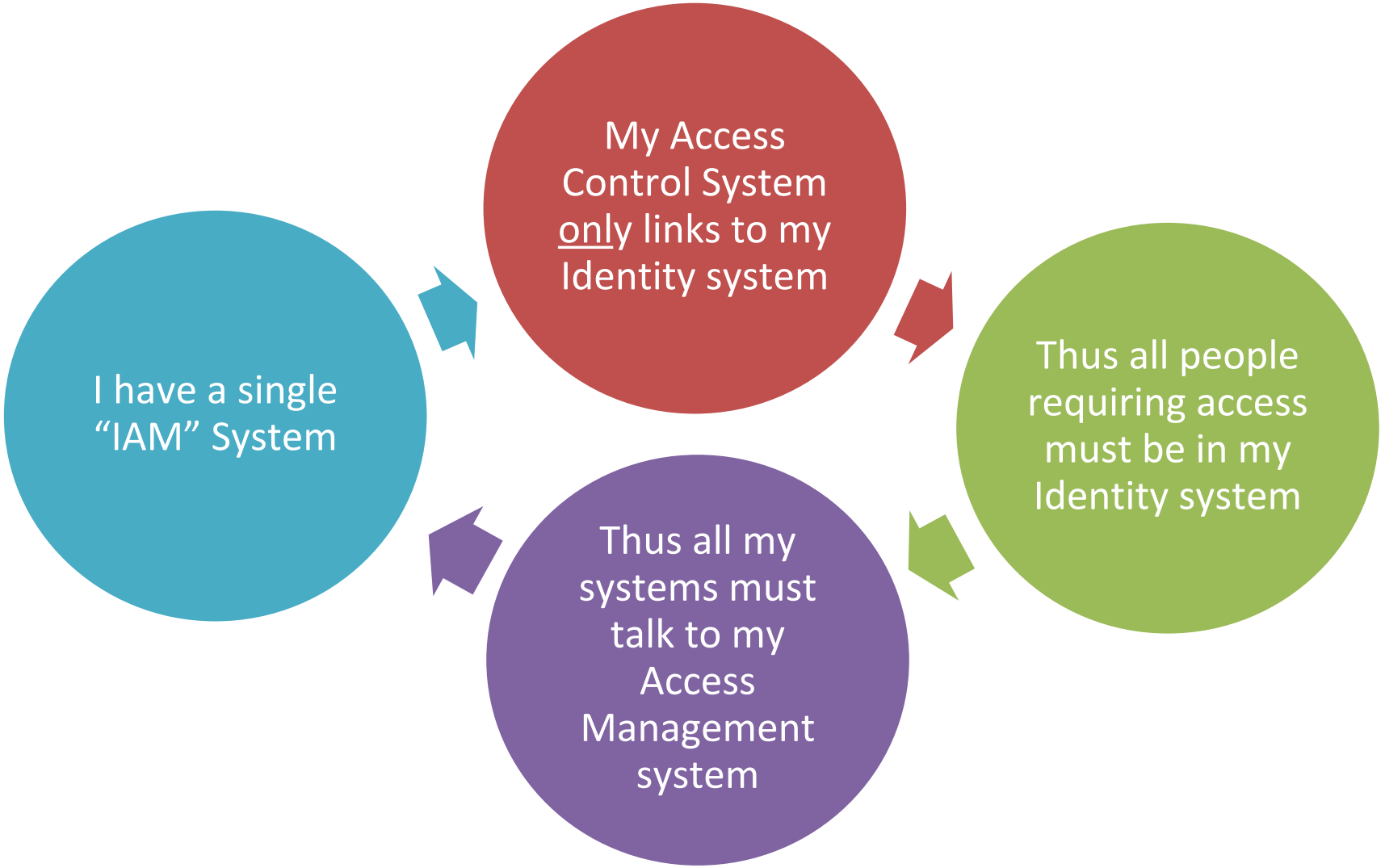
1. **The scope and level of protection must be specific & appropriate to the asset at risk**
   - Business demands that security enables business agility and is cost effective
   - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
   - In general, it's easier to protect as most 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

Jericho Forum™

“IAM” Vicious Cycle



Passwords are dead

1 Identity must be separated from Access Management

- An Identity solution must provide identity to multiple, disparate, Entitlement and Access Management solutions
- Access Management must consume identity and entitlement from multiple sources.

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

Entitlement

Making a risk-based decision

★

About access to data and/or systems

★

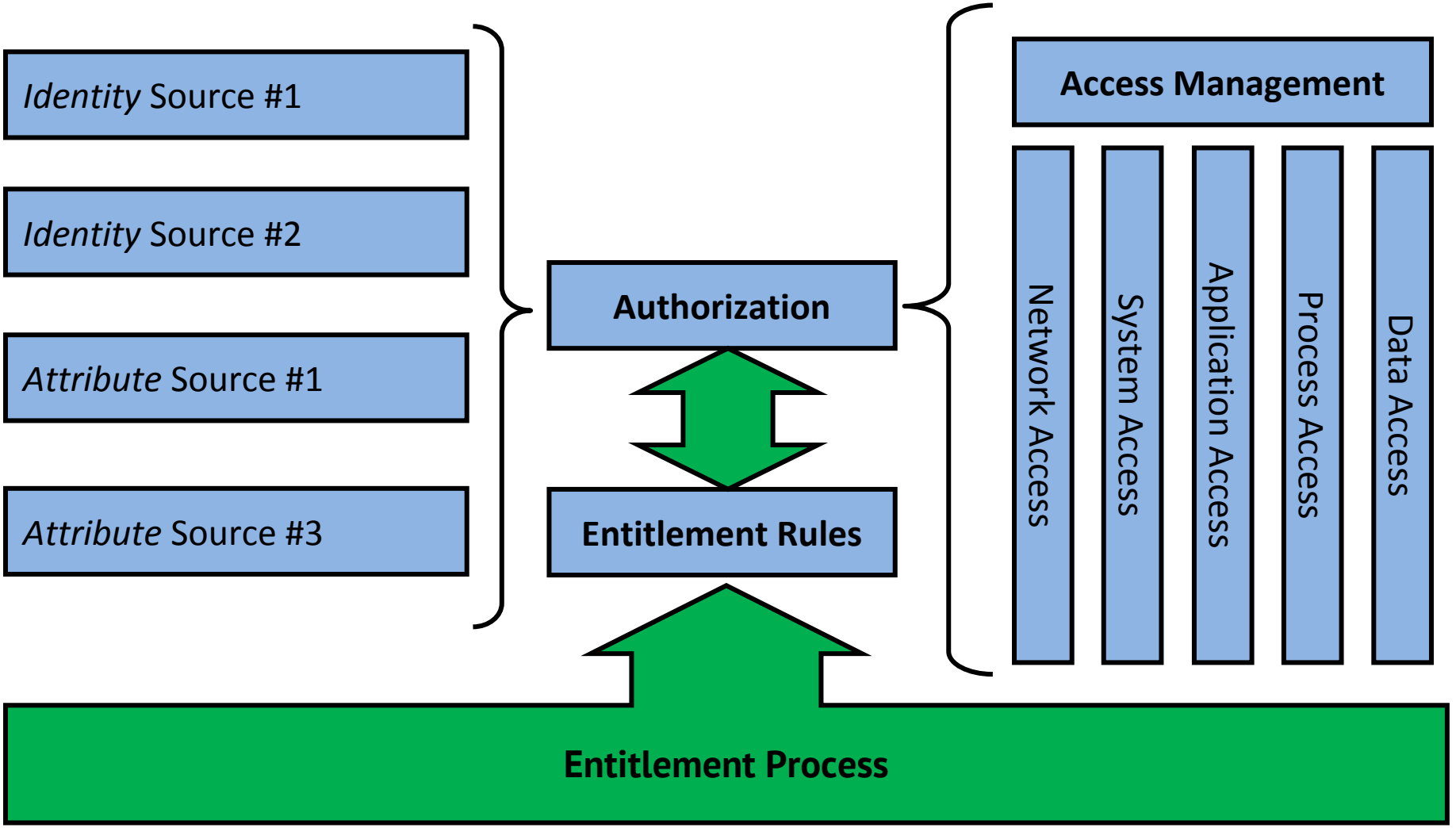
Based on the trusted identity and attributes

★

Of all the entities and components in the transaction chain

CSA Security Guidelines 3.0

Entitlement



Source: Cloud Security Alliance: Guidance v3.0

Entitlement

Table 1— Simple Entitlement Matrix for a Cloud HR Application

Claim / Attribute	Corporate HR Managers Access	User Corporate Access	Corporate HR Managers Home Access (Corp. Laptop)	User Home Access (Own Device)
ID: Organization Id	Valid	Valid	Valid	No
ID: User Identifier	Valid	Valid	Valid	Valid
ID: Device	Valid	Valid	Valid	No
Attrib: Device is clean	Valid	Valid	Valid	Unknown
Attrib: Device is patched	Valid	Valid	Valid	Unknown
Attrib: Device IP (is on corp. net. ?)	Valid	Valid	No	No
Attrib: User is HR manager	Valid	No	Valid	No
Access Result	Read/write access to all HR accounts	Read/write access to users HR account only	Read/write access to users HR account only	Read-only access to users HR account only

Source: Cloud Security Alliance: Guidance v3.0

2

Identity is not just about people

- Identity needs to encompass all objects that need to identify themselves
- This includes;
  - People
  - Devices
  - Code
  - Organisations
  - Agents.

IdEA: Identity, Entitlement, Access
Access granted dependent on assertions and rules & risk, not binary on Username

Martini model[1]: Any IP, any device, any time, anywhere

Entitlement
(Risk Based Access)

Logical / Data Access

Rules Based Access

Physical Access

Resource
-
Data
and/or
System

Resource Attributes:
- Location
- Classification
- AD Group
- etc.

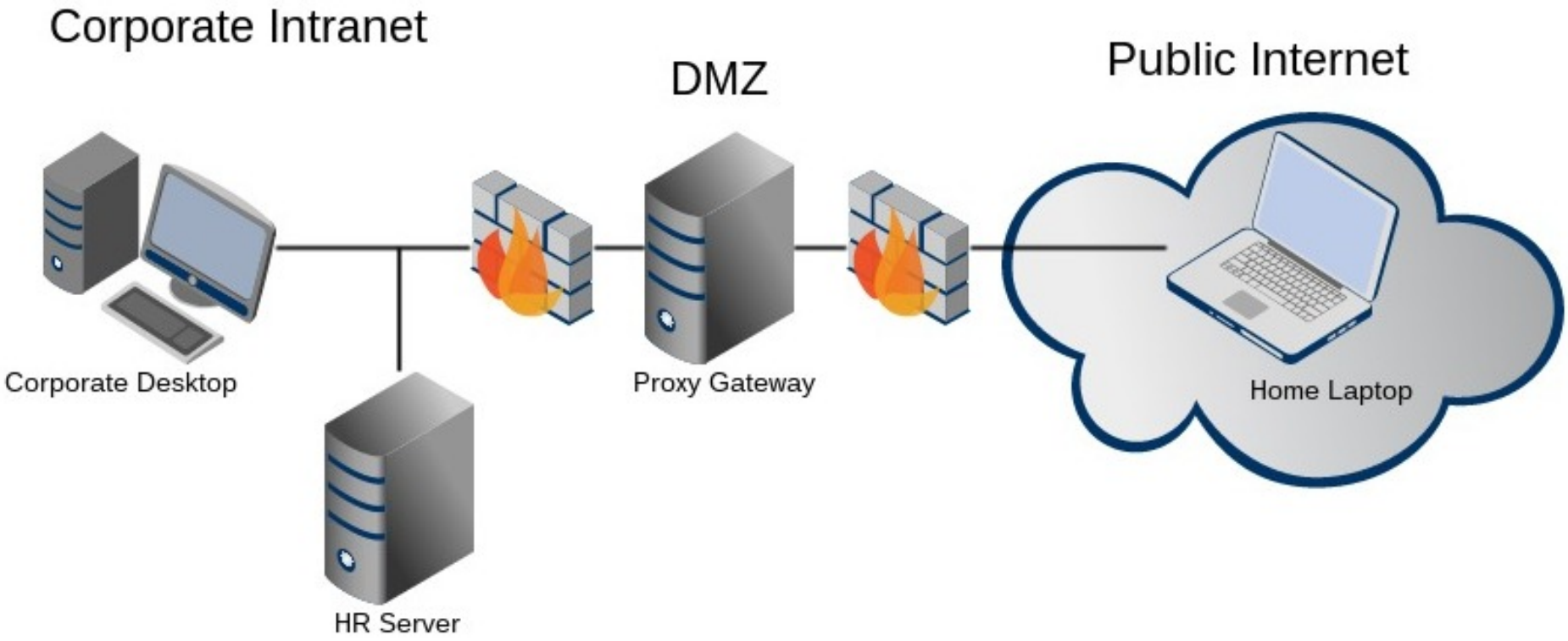
Rules based access:
Using a mix of attributes, based on risk assessment

Bi-directional Trust[2]

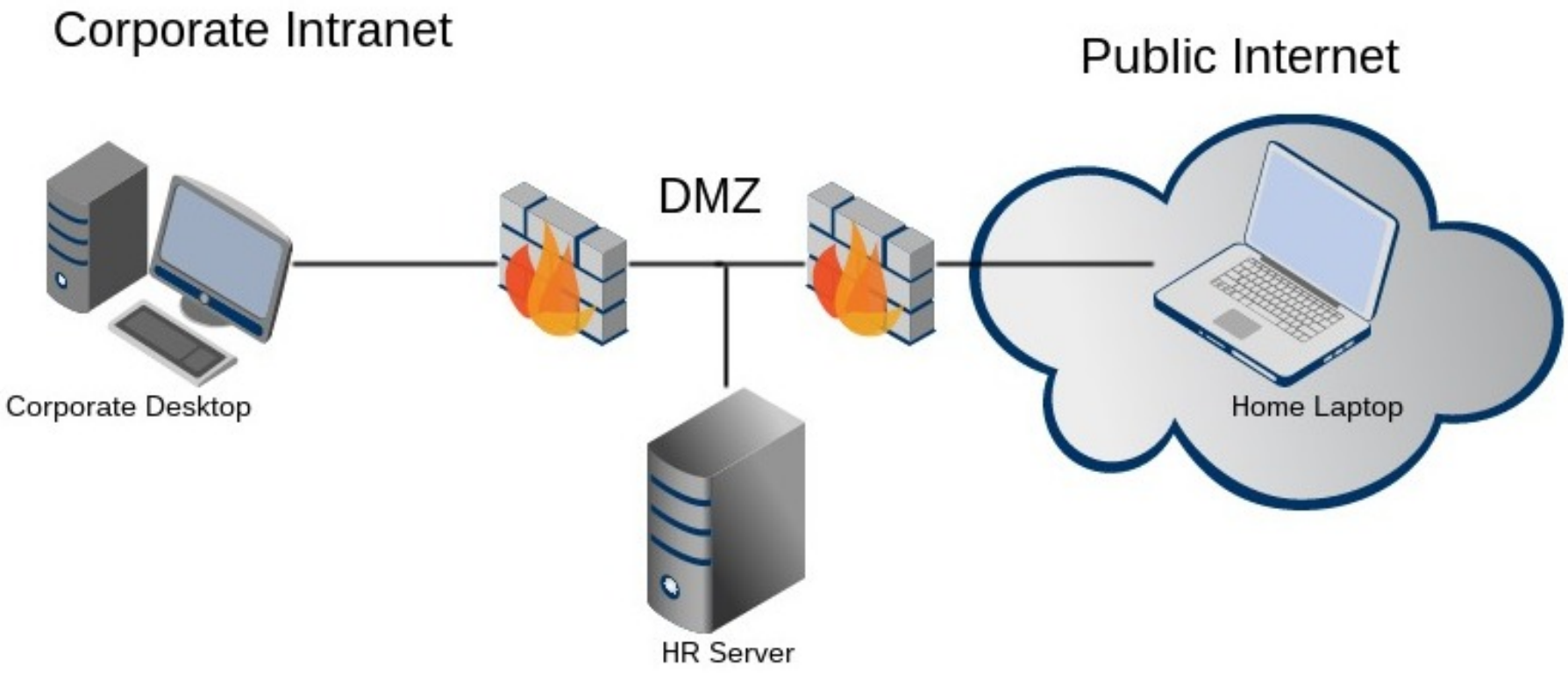
Id / Attributes Asserted
- User Identity
- User Assertions
- Credential strength / trust
- Location Assertions
  - IP-Address
  - Geo-location
  - GPS / GPRS
- Organisation Identity
- Organisation Assertions
- Device Identity
- Device Assertions
  - Functionality Required
  - Functionality Offered
  - Sandbox
  - Secure container
  - Cleanliness of device
- Code Identity
- Code Assertions

1. Multiple Access Real Time IP Network Implementation 2. Jericho Forum Commandments #6 & #7

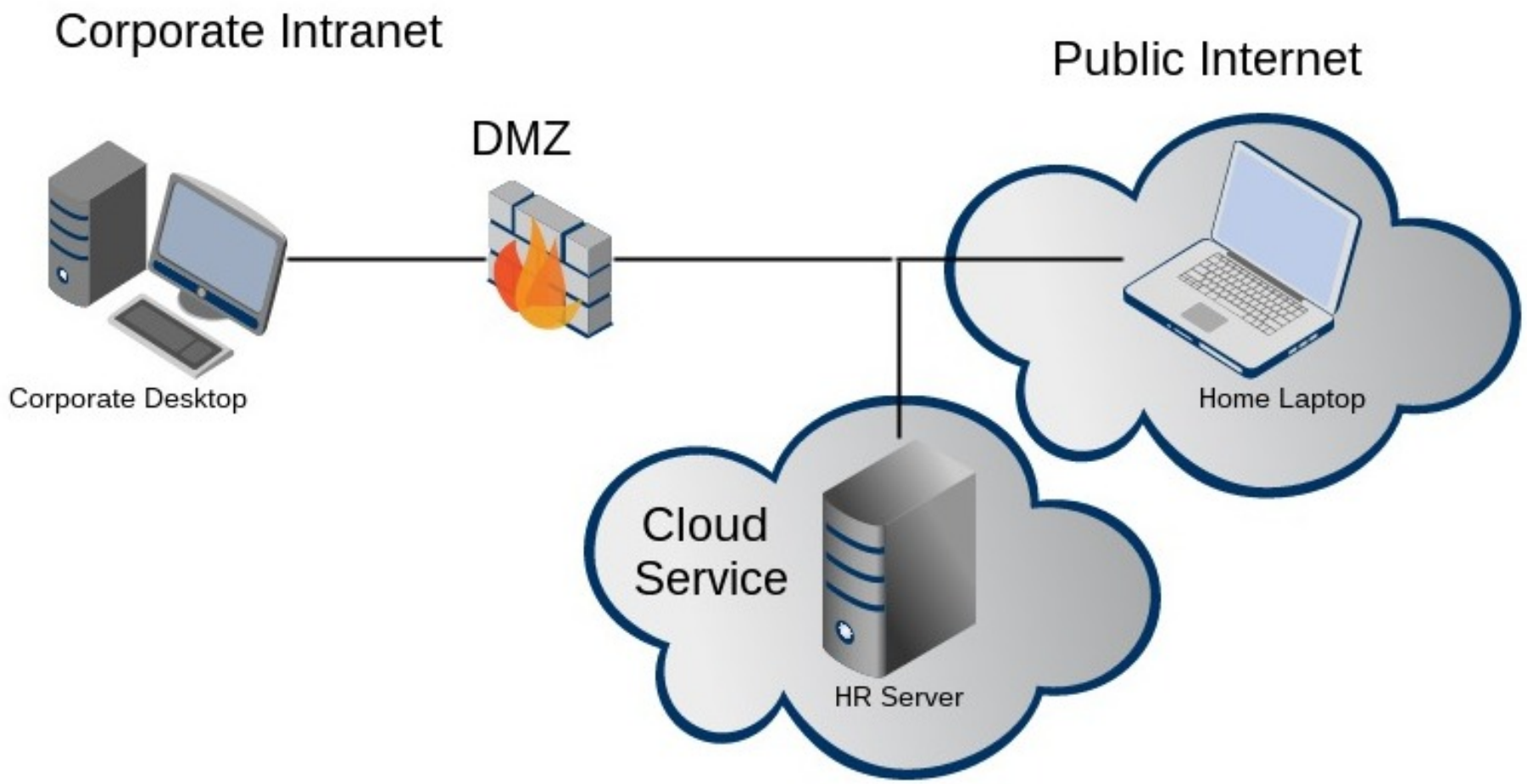
HR Example - The old state



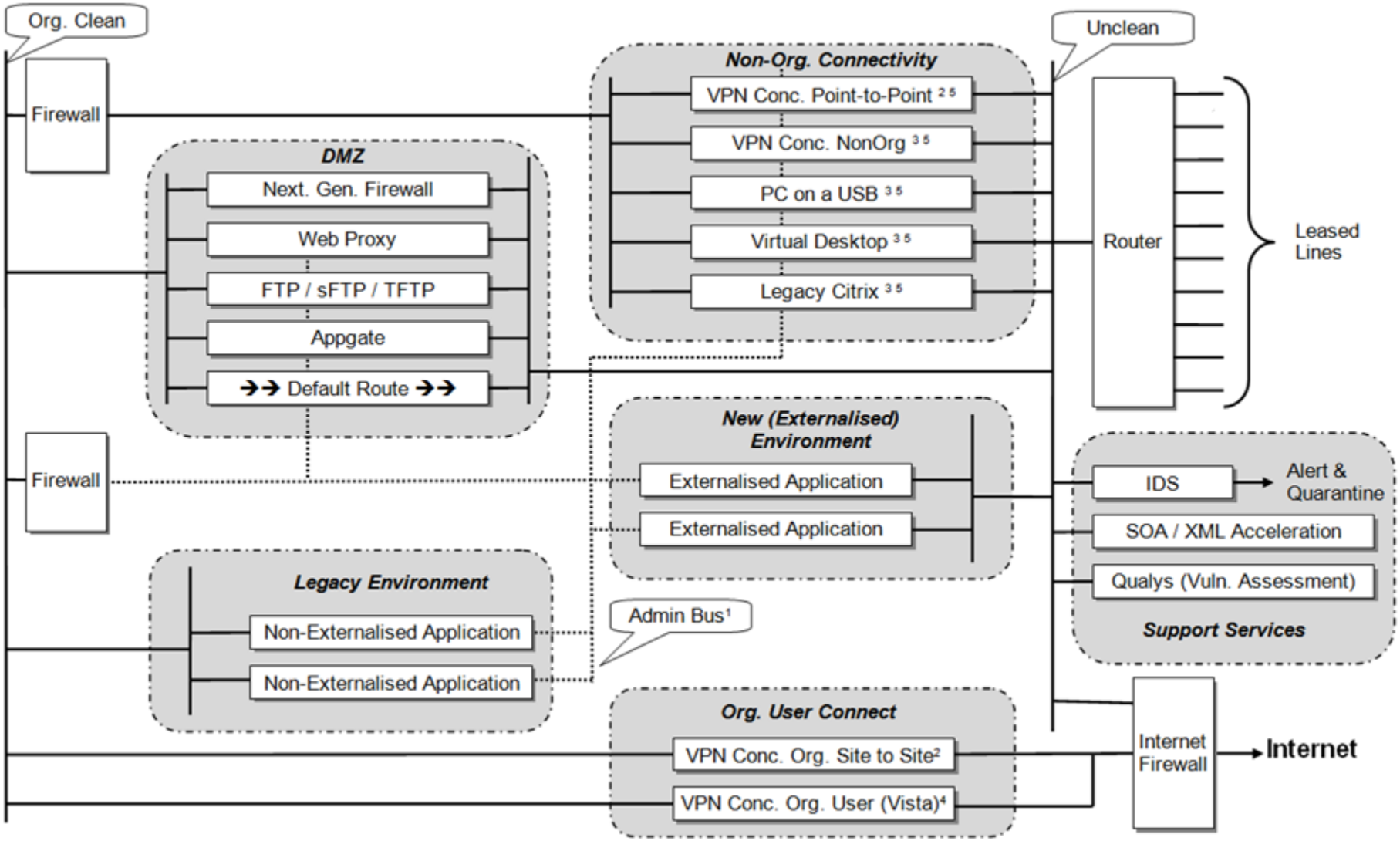
HR Example - The new state



HR Example - The cloud state



The new DMZ (Externalised Applications)



Architecture Summary

- No differentiation between “internal” and “external”
- Data is the new perimeter
- Solution based on designing for an entitlement based solution
- Internal = External = Private Cloud = Public Cloud

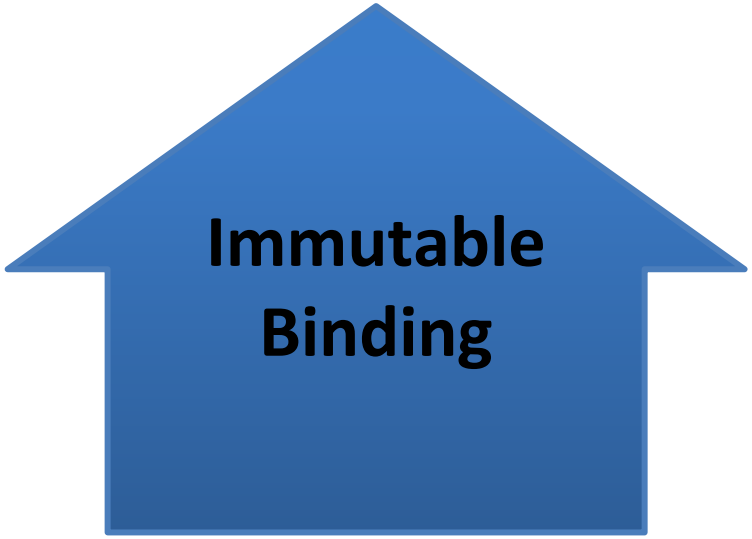
3 Federation of existing IAM system will not scale

- Technically difficult
- n-factorial problem
- Transitive trusts problem
- A “trusted assertion” based solutions will allow both scalability and flexibility.

How do we fix this?

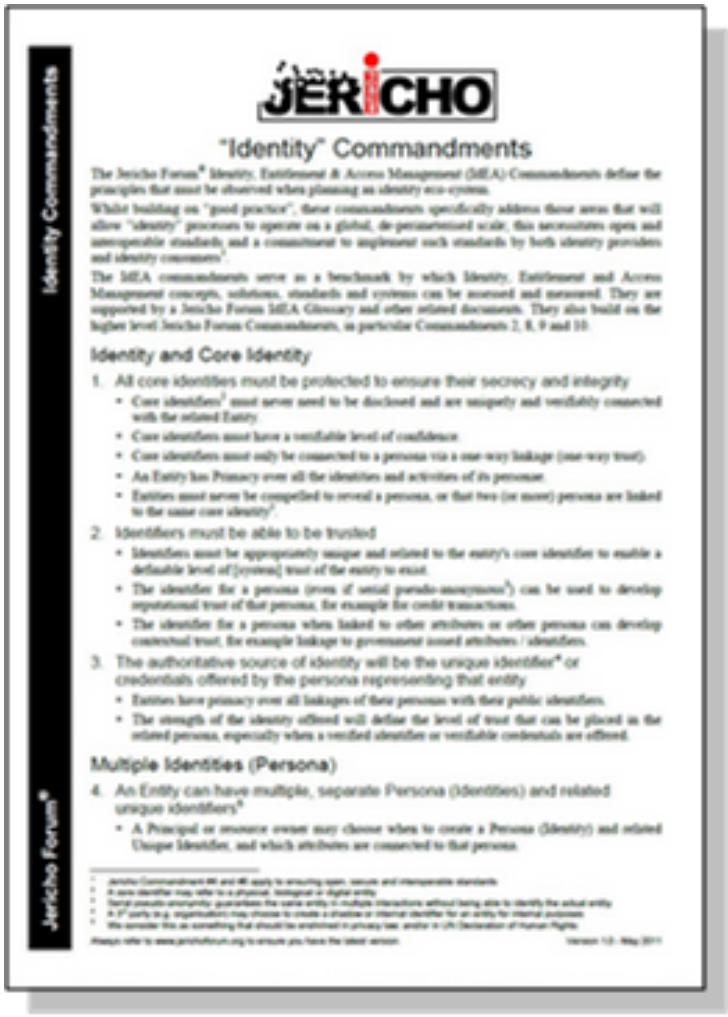
Architect it to operate as people operate

Assert the binding between device and entity



Identity Commandments

- Entity-centric ID
- Core Identity must be secret & protected
- Primacy
- Persona-based
- Immutably linked entity
- Attributes from authoritative sources



Identity Commandments

"Identity" Commandments

Identity and Core Identity

1. All core identities must be protected to ensure their secrecy and integrity
2. Identifiers must be able to be trusted
3. The authoritative source of identity will be the unique identifier* or credentials offered by the persona representing that entity

Multiple Identities (Persona)

4. An Entity can have multiple, separate Persona (Identities) and related unique identifiers*

Jericho Forum®

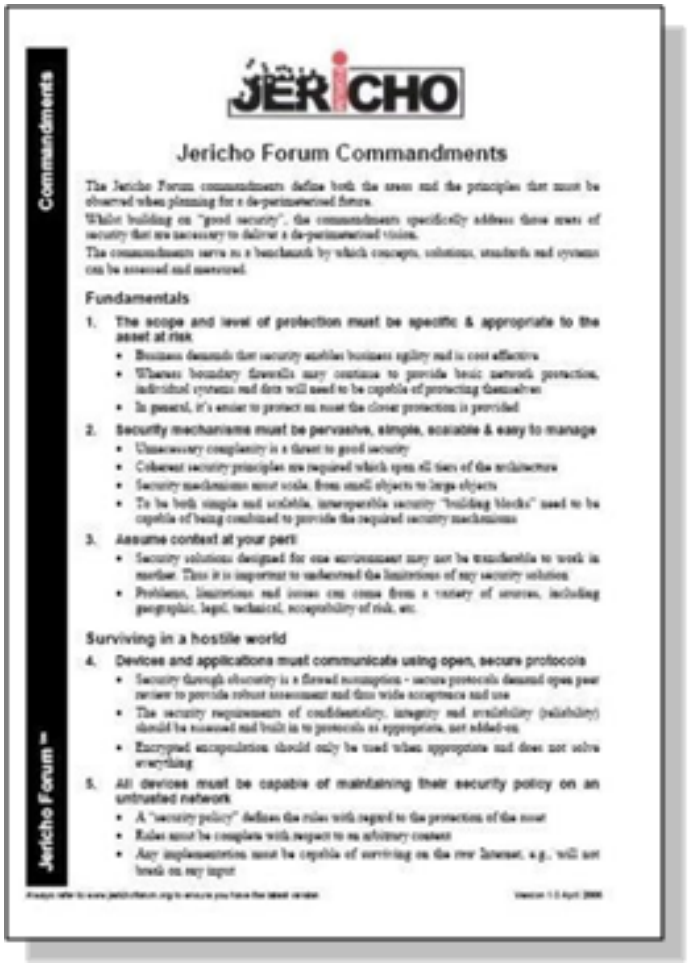
Commandments

#3 Assume context at your peril

- Security solutions designed for one environment may not be transferable to work in another

Solution:

- Understand (as much about) the context in which the transaction is taking place.
- Understand the operating context of the entity



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

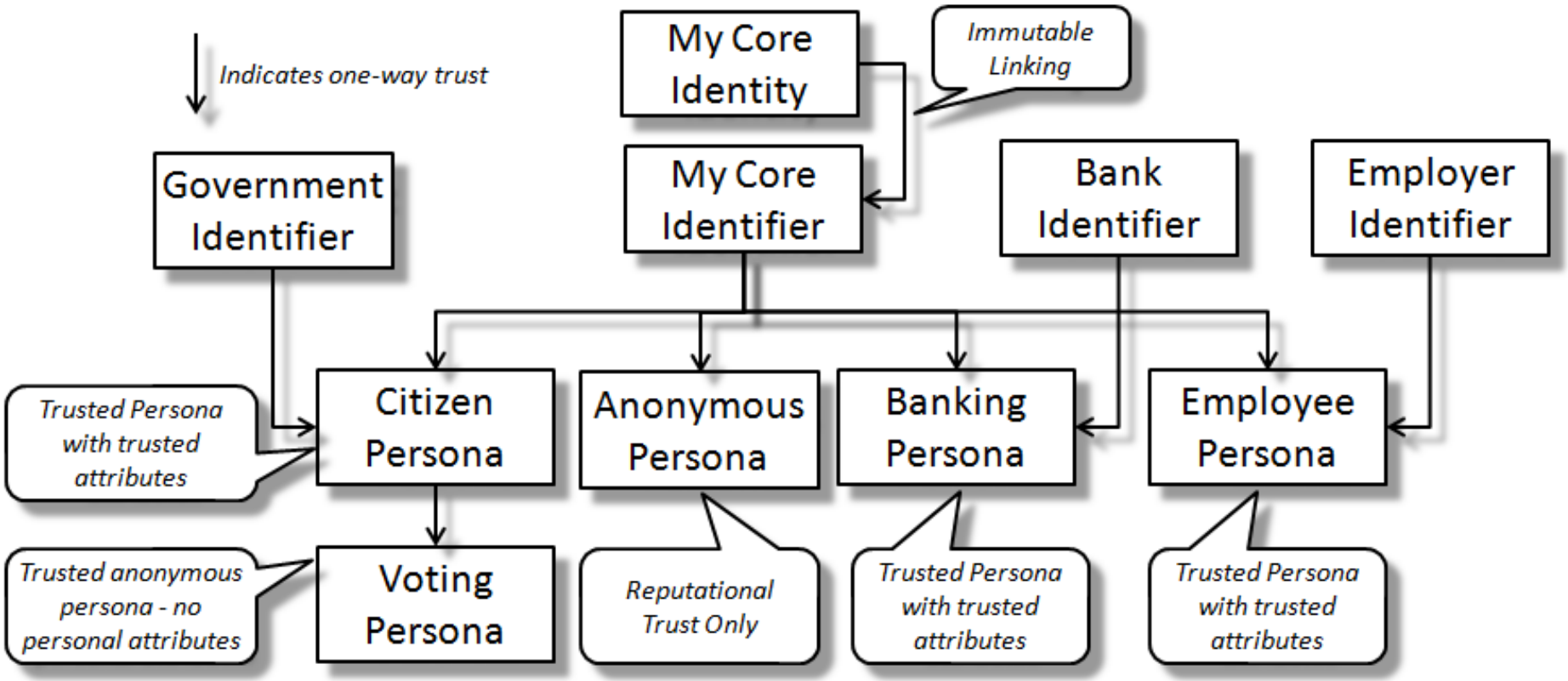
1. The scope and level of protection must be specific & appropriate to the asset at risk
   - Business demands that security enables business agility and is cost effective
   - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
   - In general, it's easier to protect as most 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

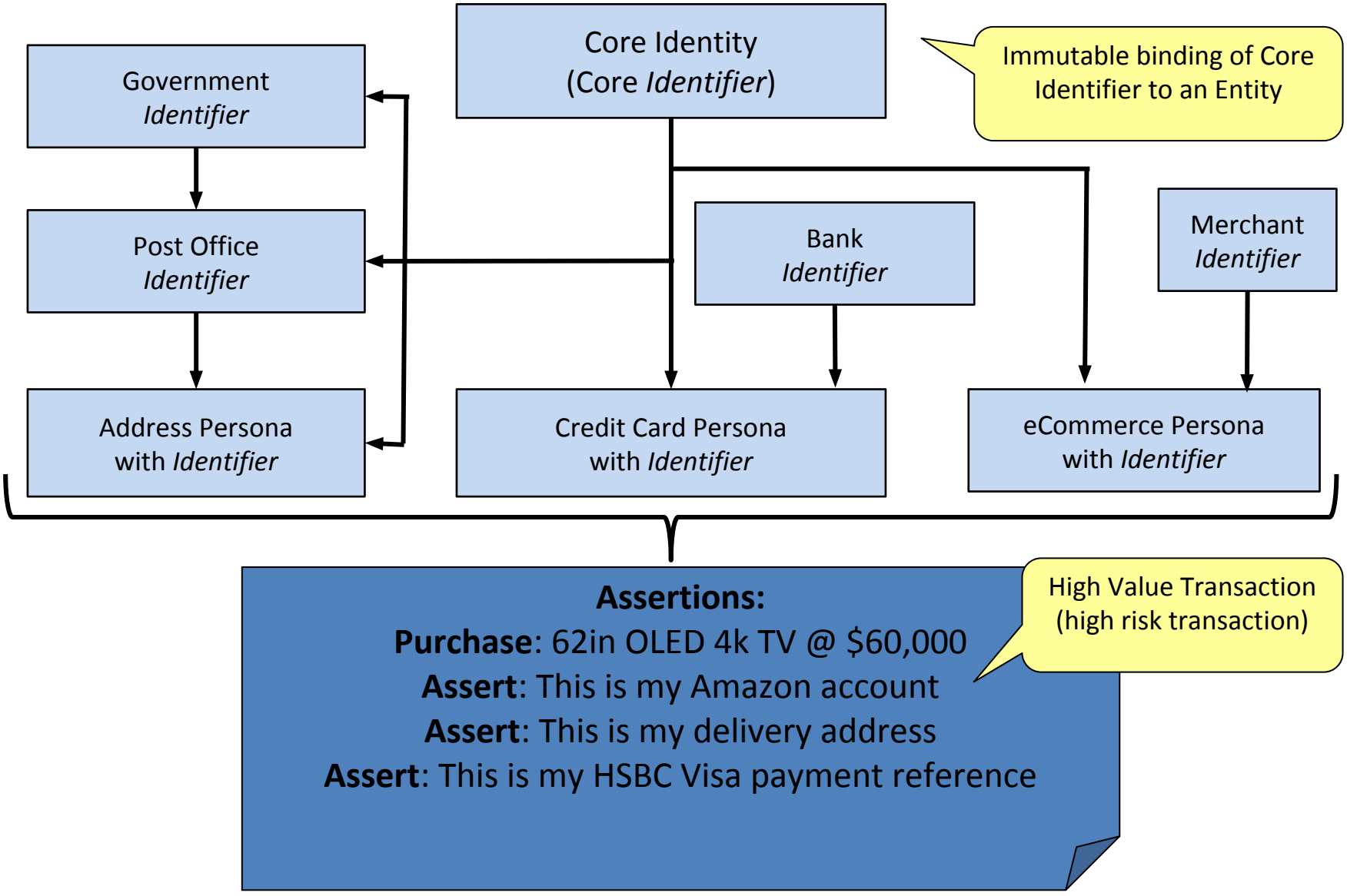
4. Devices and applications must communicate using open, secure protocols
   - Security through obscurity is a flawed assumption – secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
   - The security requirements of confidentiality, integrity and availability (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

Jericho Forum™

Operating with Personas



Multiple (tied) Assertions



4 Strong identity is key to trust and collaboration on the Internet

- The lack of Strong Identity is hindering adoption
- People operate with personas
- A strong, anonymous, core identity is key
- People must own their own core identity
- People must be able to control their identity
- Escalating individual personas to a pseudo-core will fail.

The Challenges (Now)

- Hundreds of personal passwords to manage
- Tens of corporate passwords to manage
- Lack of authoritative sources for attributes
- The rise of the self asserted ID (Weak BYOiD)
- Single device, multiple users (£3700 Apple bill)
- Passwords beyond their “sell-by” date
- Managing people / users / access for entities you don’t employ
- Managing devices you don’t own (or have access to)
- Inability to consume someone else's (strong) identity

The Challenges (Near Future)

- Internet of Things
- Authoritative sources of attributes
- BYOiD
- Better trust required in the eco-system
- Cars, Phones, Houses & Work utilising personas
- Access to government e-Services (inc. anon. voting)
- Agents, with access to our lives
- Urgent need to extend identity to all entities
- Need to make better risk-based decisions

In Summary

Application and services that give granular and flexible access, irrespective of location, will win the business!

Thus, **Data** is the new perimeter;

And, **Entitlement** is how you control access to it;

And, **Identity** is what you use to drive entitlement.

Thus **Identity** is the new currency!

The Global Identity Foundation

A single global identity for humanity

- Primacy
- Global Solution
- Open Standard
- Open Implementation
- Works Universally

Join us on LinkedIn
"Global Identity Foundation"

www.globalidentityfoundation.org