

IdM Strategy

Andy Smith MSc FBCS CEng CITP FSI M.Inst.ISP

andy@aisinfosec.com

AIS InfoSec Ltd



The Questions?

🔍 The threats?

🔍 Who are you - Identification?

- 🔍 Ford Prefect problem



🔍 Are you really who you claim to be?

- 🔍 Verification / Authentication
- 🔍 Sidney Bristow problem

🔍 How can I establish an identity and verify it easily?

🔍 How can I be sure you are you?

- 🔍 Unsupervised
- 🔍 No trusted infrastructure



Authentication - Where are the threats from

● Mainly from people

- Muppets
- Pranksters (siblings etc)
- Inadvertency (error, stupidity)
- Opportunists / Journalists
- Malicious people (e.g. revenge)
- Militants & Terrorists
- Criminals
- Serious & Organised Crime
- Foreign Intelligence Services



● Also beyond reasonable control

- Force majeure (e.g. Major incident, Natural disaster)
- Automated, untargeted attacks (e.g. Malicious code)



Threats – People & Process

Humans

- Human Error / Accidents / Stupidity
- Social Engineering / Phishing
- Technophobia
- Apathy / Complacency

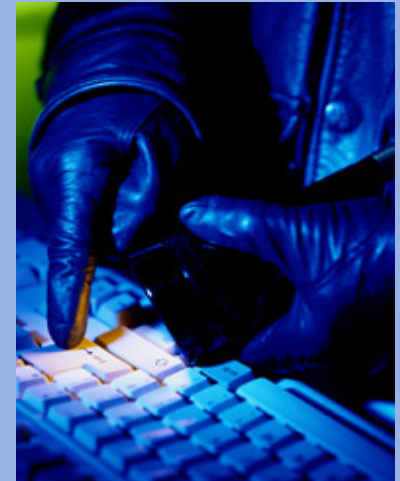
Credentials

- Easily guessed or written down
- Forgotten credentials (support overhead)

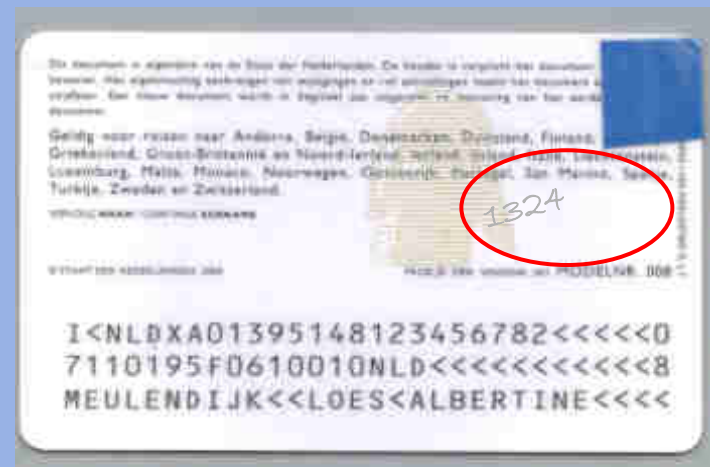
Lack of assurance

- No supervision or oversight
- No trusted infrastructure
- No proof of actions (non-repudiation)

- Theft
- Copying credentials
- Coercion / Duress



e.g. Writing PIN on card



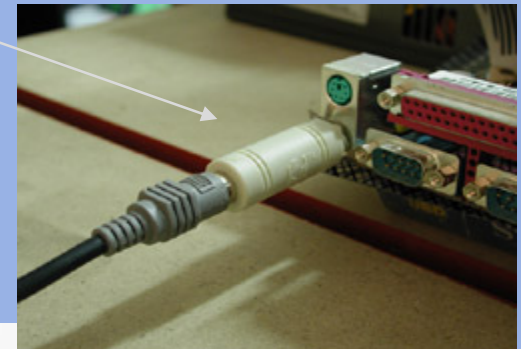
Threats - Technology

Computer based

- Viruses & Malicious mobile code (Java, ActiveX)
- Keyboard loggers (software & hardware)
- Replacement / Trojan software
 - SSL libraries that log all encrypted data
- Hijacking computer (remote control)

Communications

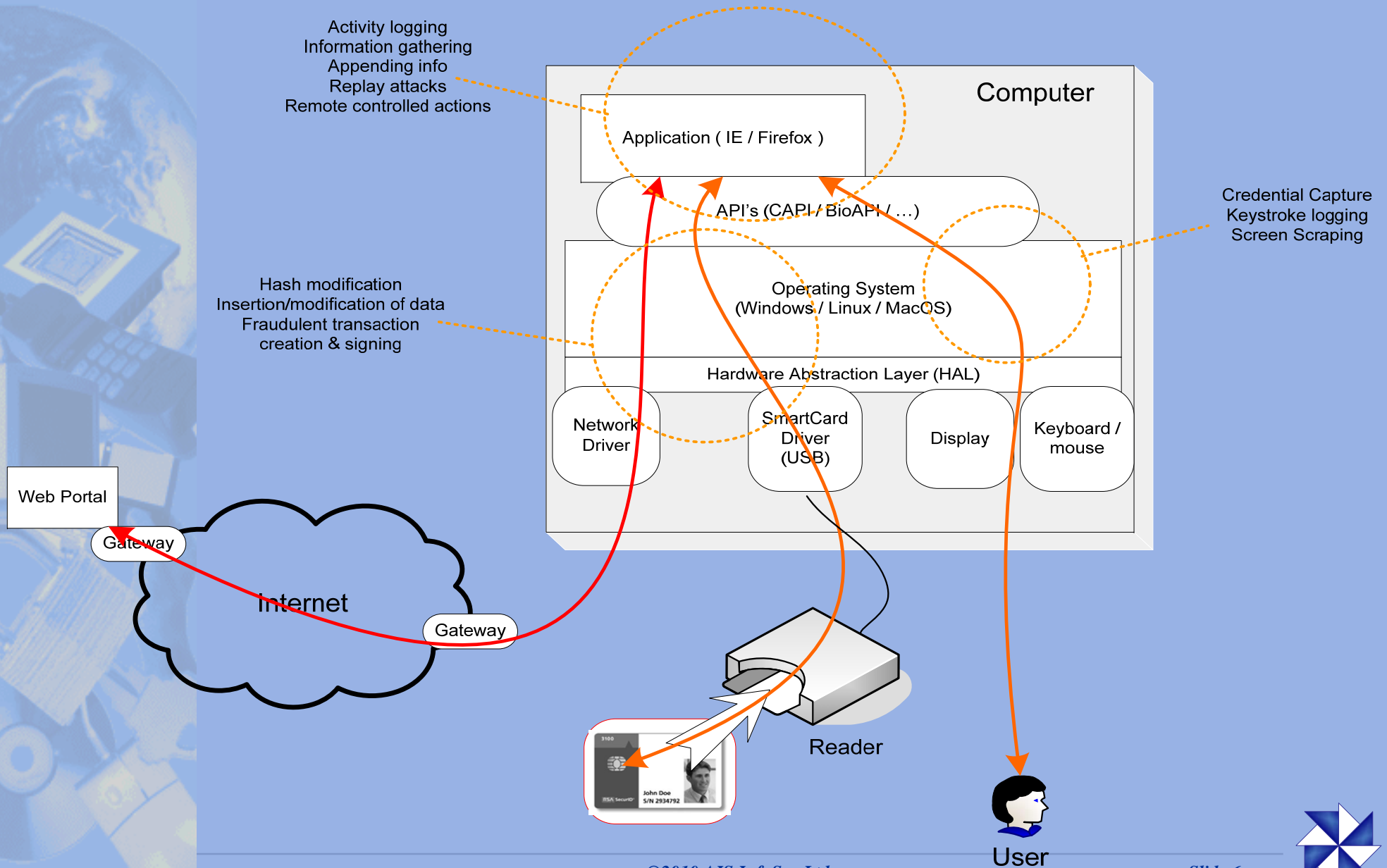
- Network sniffers / probes / recorders
- Listening in (scanners, phone taps)
- Redirection (fake web sites)
- Email / file capture



Scanner for listening to wireless phone conversations



Vulnerabilities - Computers



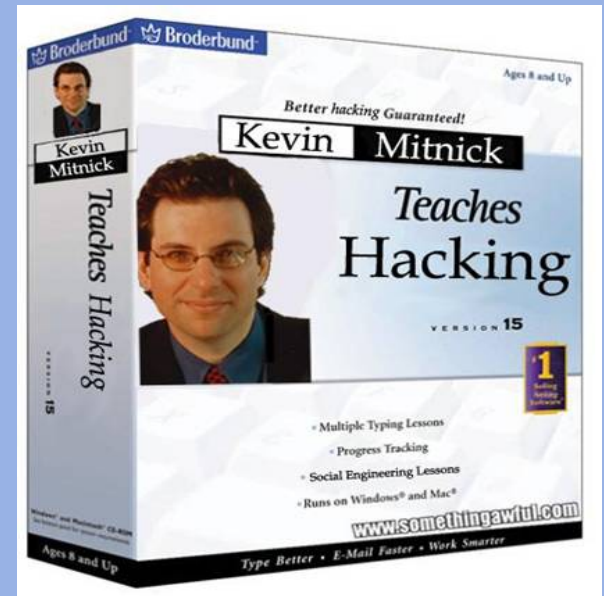
Vulnerabilities often exploited

Computer based

- Office documents via email
- Pdf documents via email
- Web browsers via compromised web servers
- Web browsers via email or other mobile code routes
- Operating system vulnerabilities via malicious code
- Exception handling routine weaknesses

Humans

- Social Engineering and Psychological manipulation
- Apathy, Complacency, Stupidity (e.g. phishing)
- Greed (bribery and corruption of insiders)
- Dumpster Diving (rubbish trawling)
- Putting common identifiers on products (e.g. NINo.)

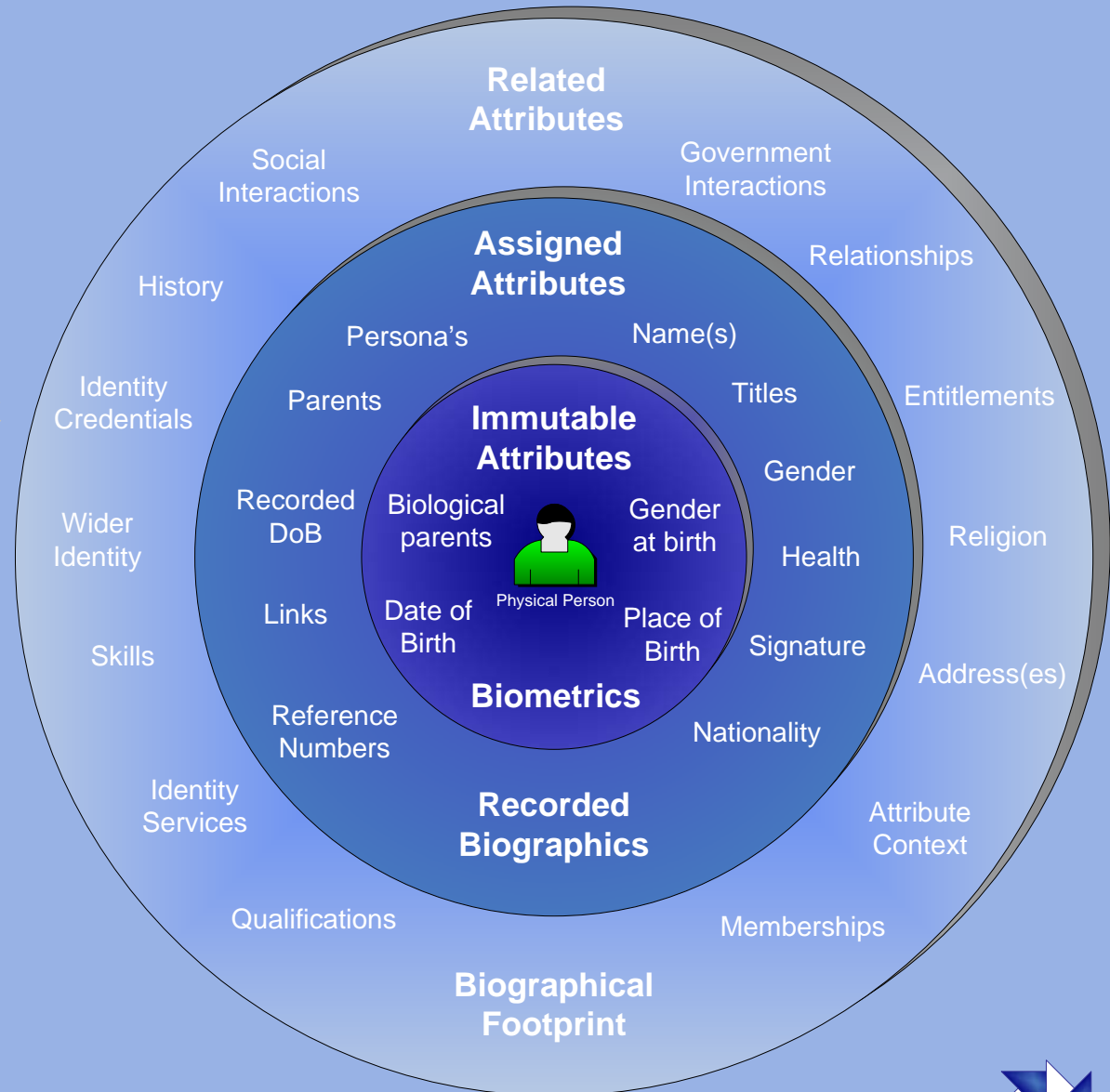


Identity - Fundamentals

3 Main sets of data

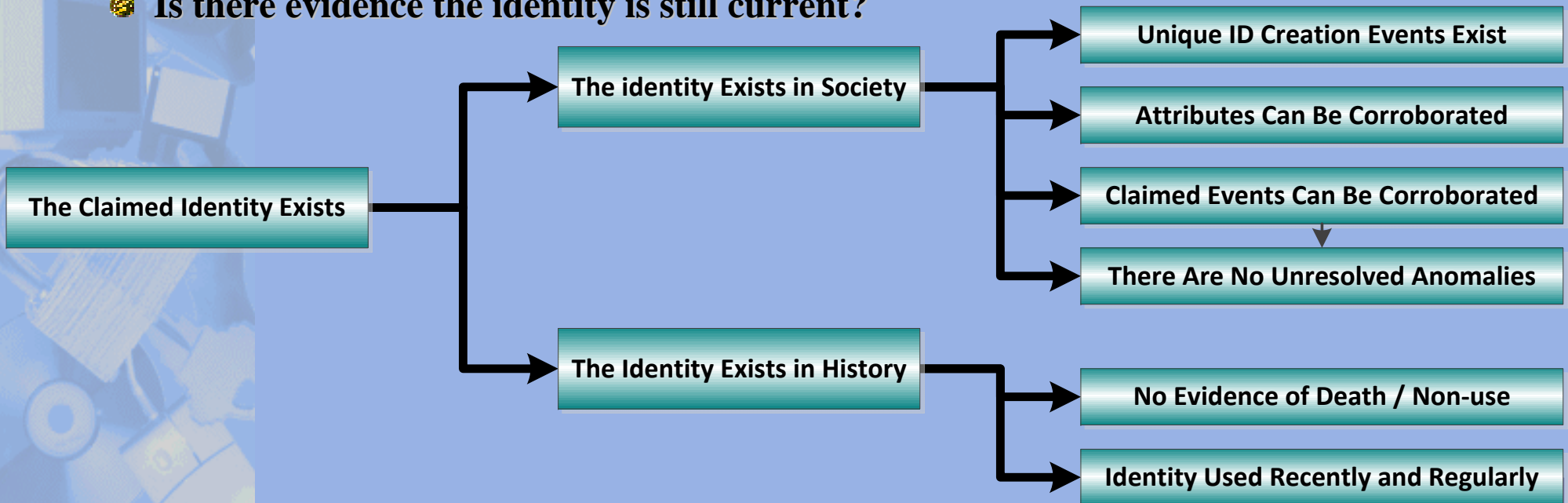
- Those intrinsic to you when you are born
- Those assigned to you by others
- Those you get as you interact with the world

Establishing identity looks at all of these in 3 steps:



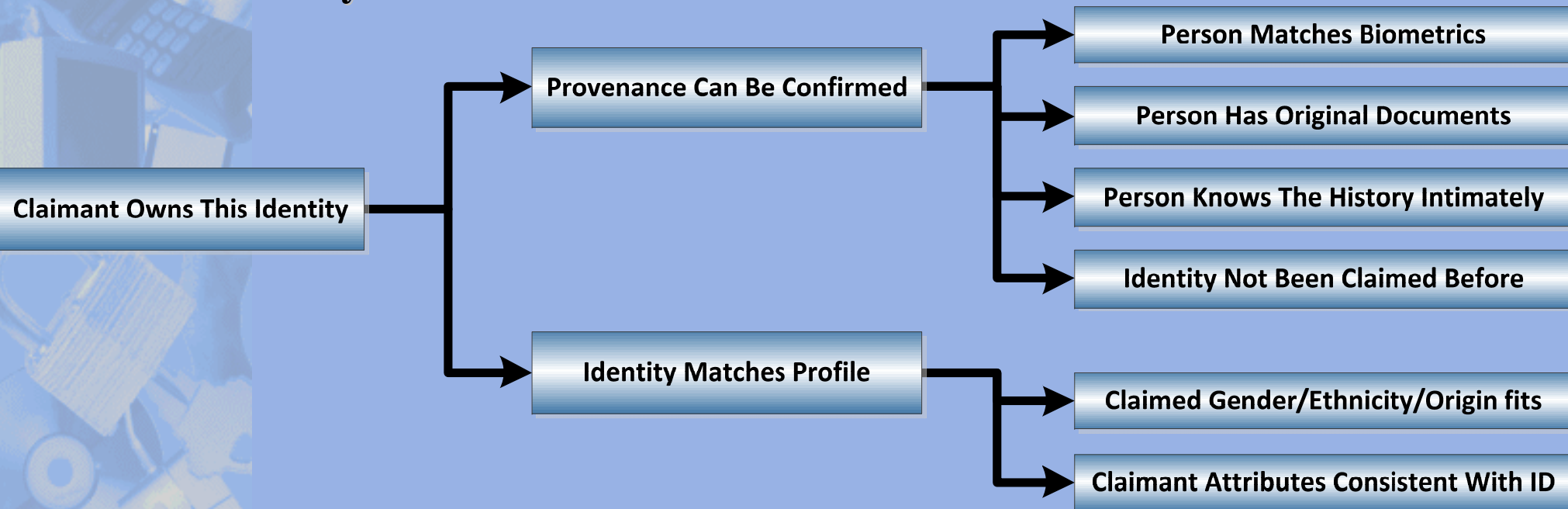
Establishment - Existence

- Is the asserted identity real?
- Can all of the claims be corroborated?
 - are there anomalies?
- What is the strength of the corroboration?
 - A biographical check of the identity across various data sets
 - Is there a footprint of use in society?
 - Is there a historical record of use?
 - Is there evidence the identity is still current?



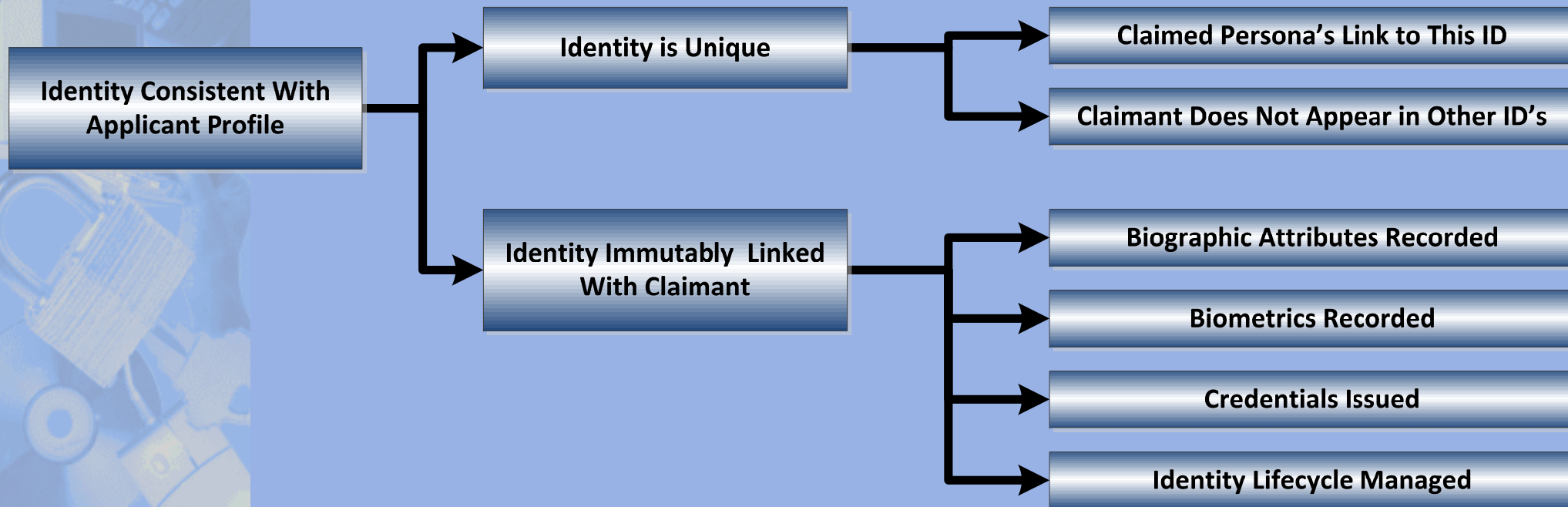
Establishment - Provenance

- Is this really your Identity?
- Can provenance be established?
 - Detailed knowledge of the identity
 - Original documents
 - Interview if appropriate
 - Resolve any anomalies

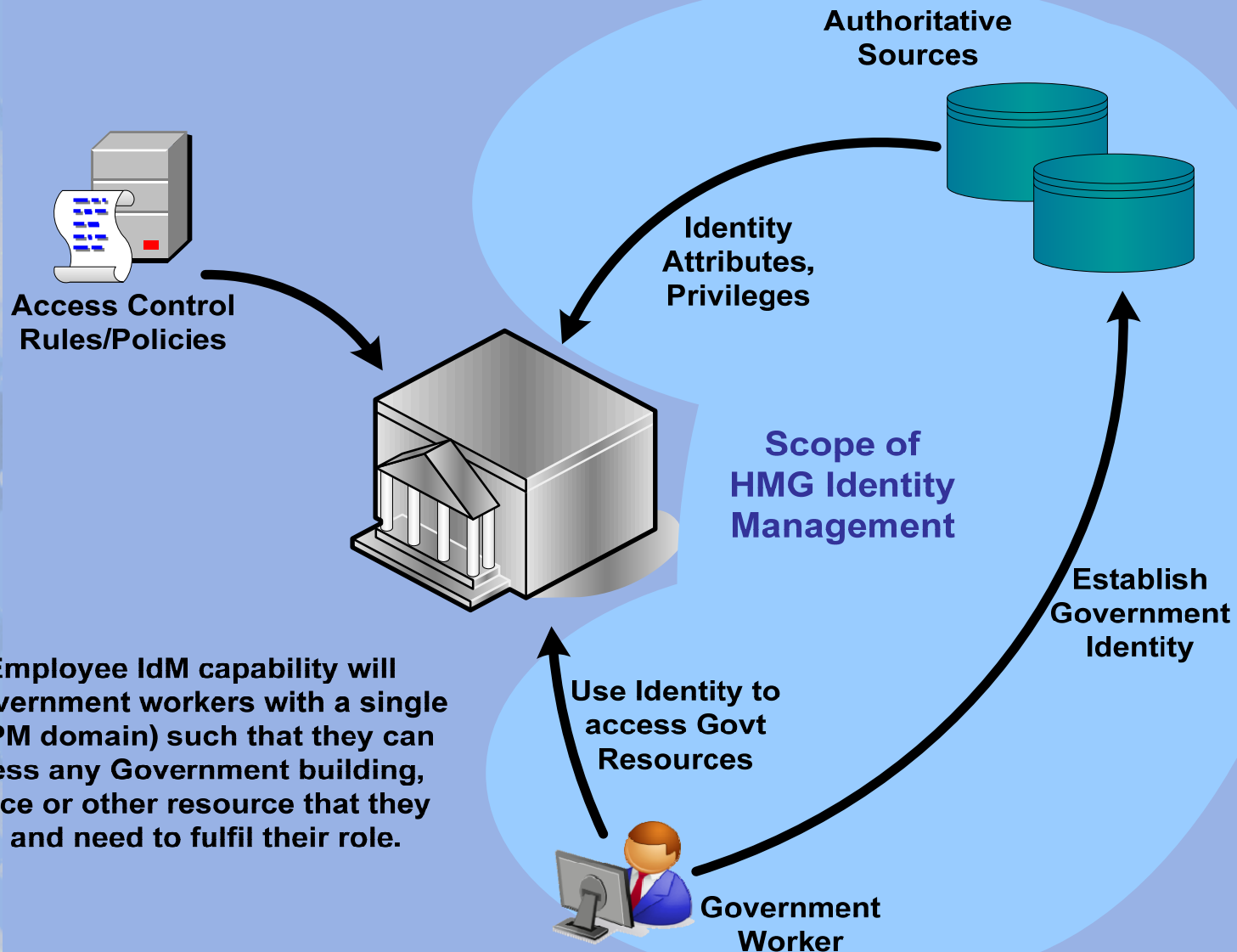


Establishment - Uniqueness

- Is this your primary identity?
- Is it your only identity – is it unique?
 - Are there any other personas linked to the identity e.g. stage name
- The person is then locked into the identity using:
 - Biometrics – Photograph, Fingerprints and signature
 - Credentials – ID Card, Driving licence, Passport, etc.



Cross-Govt Scope Today

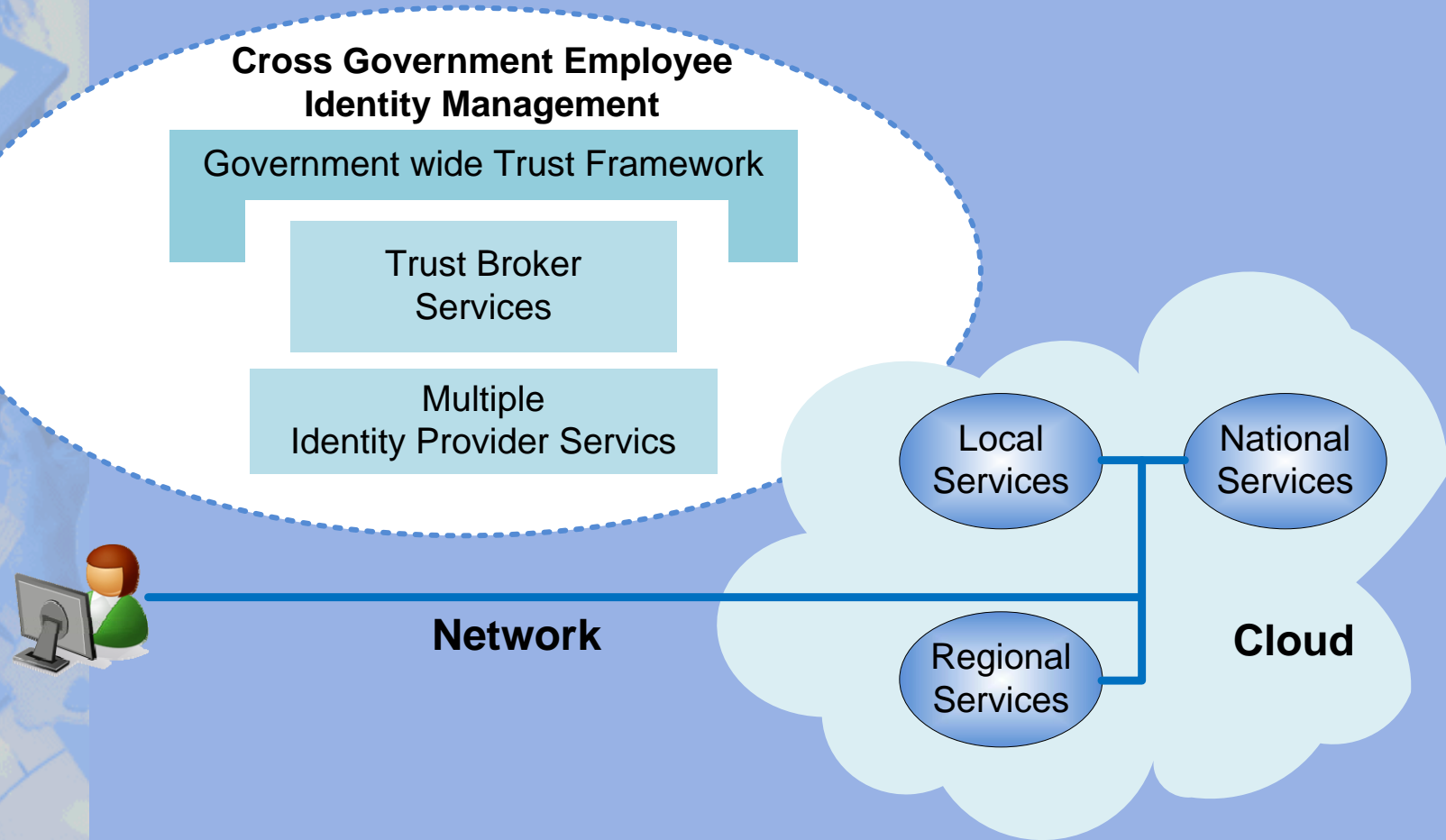


The HMG Employee IdM capability will provide all Government workers with a single identity (per PM domain) such that they can use it to access any Government building, system, service or other resource that they are allowed and need to fulfil their role.



Federated Identity Management

- **Improve service and reduce cost**
 - a trusted community for information sharing
 - a 'portable identity' across organisational boundaries

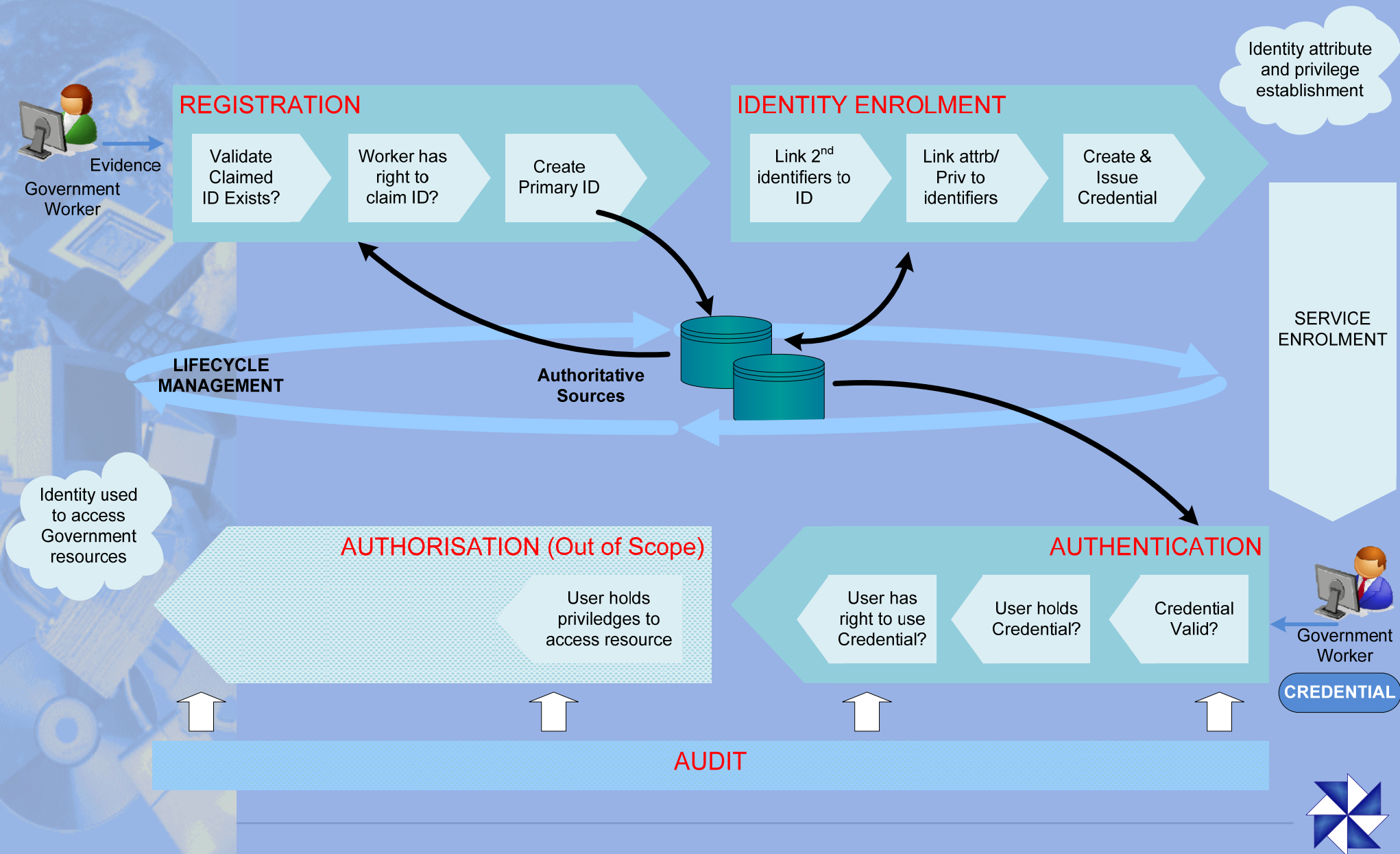


Federated Identity Management - Principles

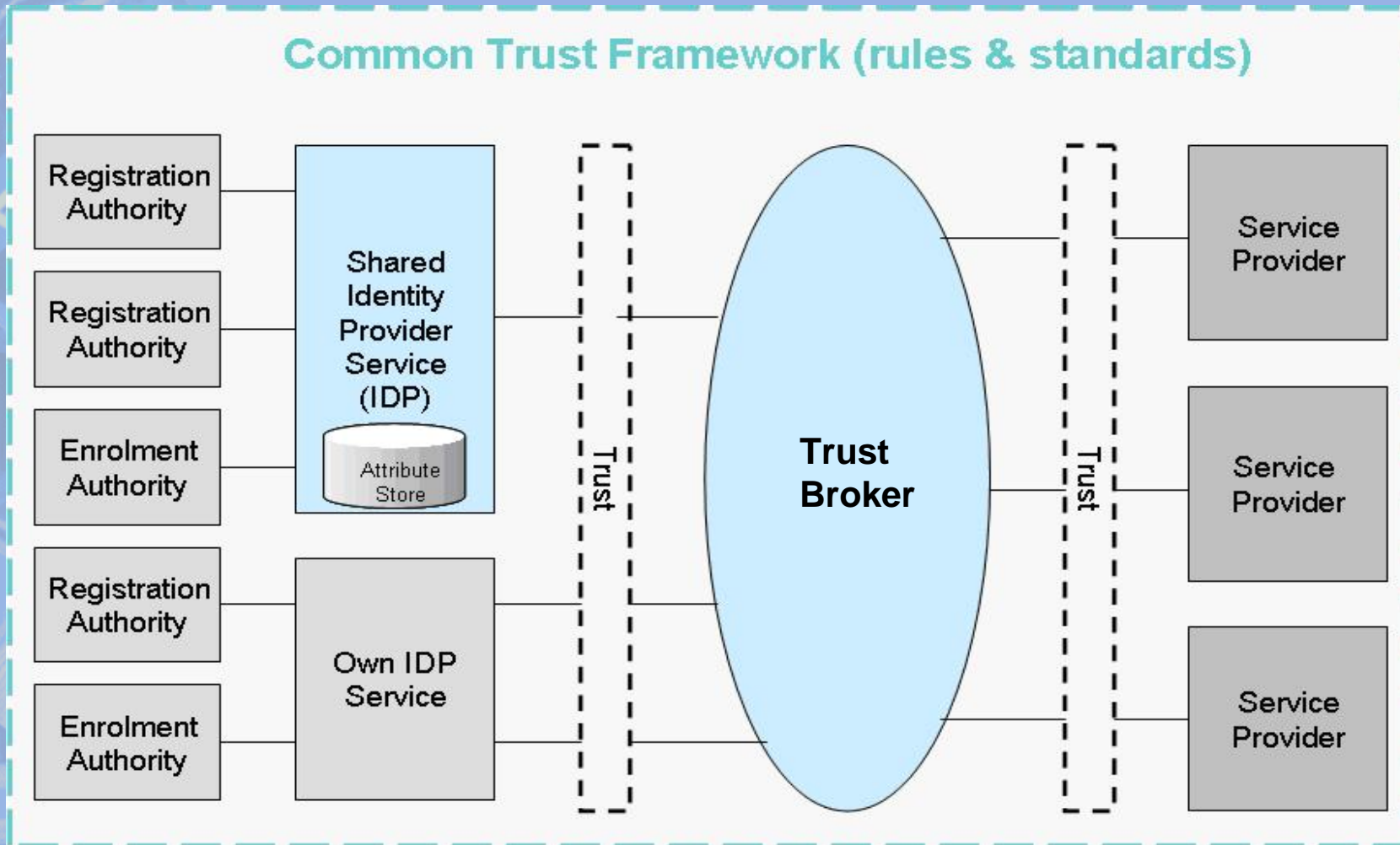
- 1. A federated model will be adopted.**
- 2. One logical record of an individual's identity will be established.**
- 3. The owner organisation shall have responsibility for maintenance of a minimum set of identity data (attributes) about the individual.**
- 4. Each organisation shall have responsibility for access control to their resources.**
- 5. An accreditation and audit regime will be operated, based on agreed standards and policies.**
- 6. Organisations should accept identity data from other organisations that have been accredited and audited to the agreed standards.**
- 7. Transitive Trust.**
- 8. Reuse of authentication results will be supported.**
- 9. Use of identity management processes will be subject to audit.**



Federated Identity Management – Key Processes



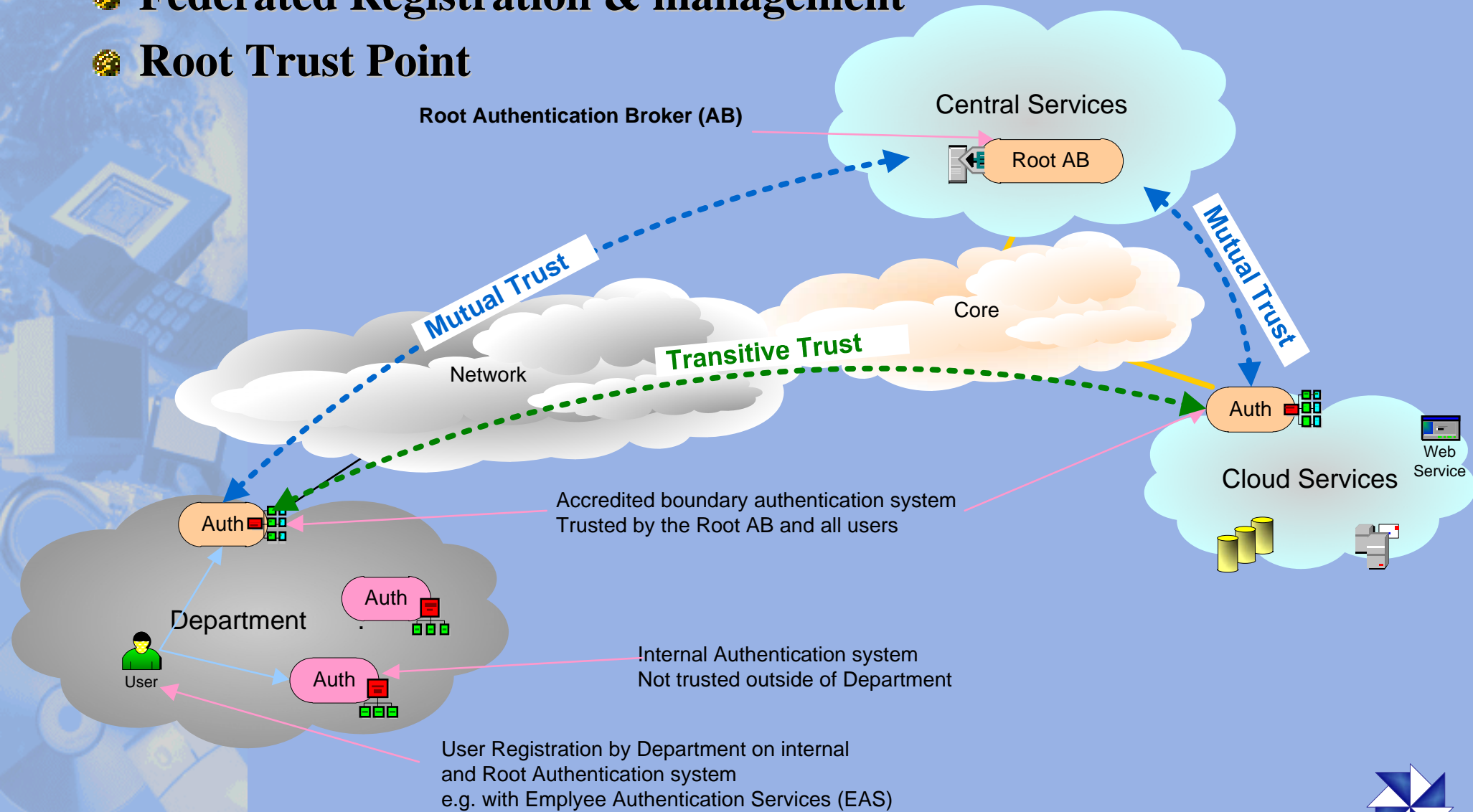
Federated Identity Management – Trust Framework



Cross Government approach

Federated Registration & management

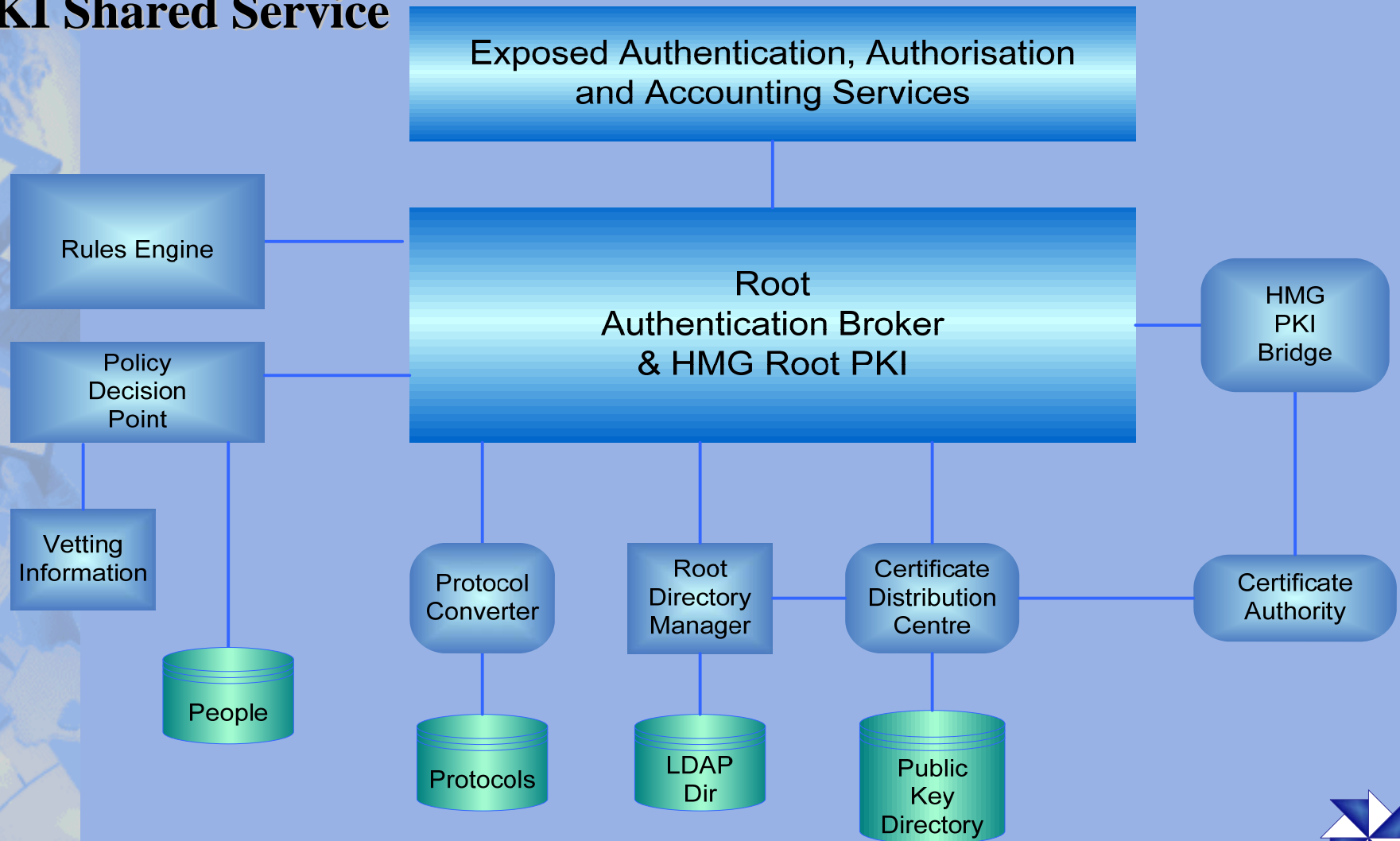
Root Trust Point



Migration & Transition

Multi-tier Authentication

PKI Shared Service



Summary - Identity Management

- **Identity Management (IdM) covers the whole lifecycle of an identity from initial enrolment into the IDMS through to archiving.**
- **It includes the governance, processes, data, technology and standards concerned with:**
 - Application to register an identity
 - Authenticating the identity and its claimed attributes
 - Establishing ownership and provenance of the identity
 - Enrolling that identity into the IDMS and linking it to the individual
 - Maintaining that identity and its attributes
 - Ensuring integrity of the information and improving its assurance
 - Providing credentials & services to authenticate that identity to third parties
 - Minimising theft or misuse of an identity and
 - Managing identity restitution and redress



Questions



"On the Internet, nobody knows you're a dog."

