



...from PKI to Identity Assurance

Richard Trevorah

Technical Manager

tScheme Ltd

Tel: +44 (0)7818 094728

richard.trevorah@tScheme.org



What is tScheme?

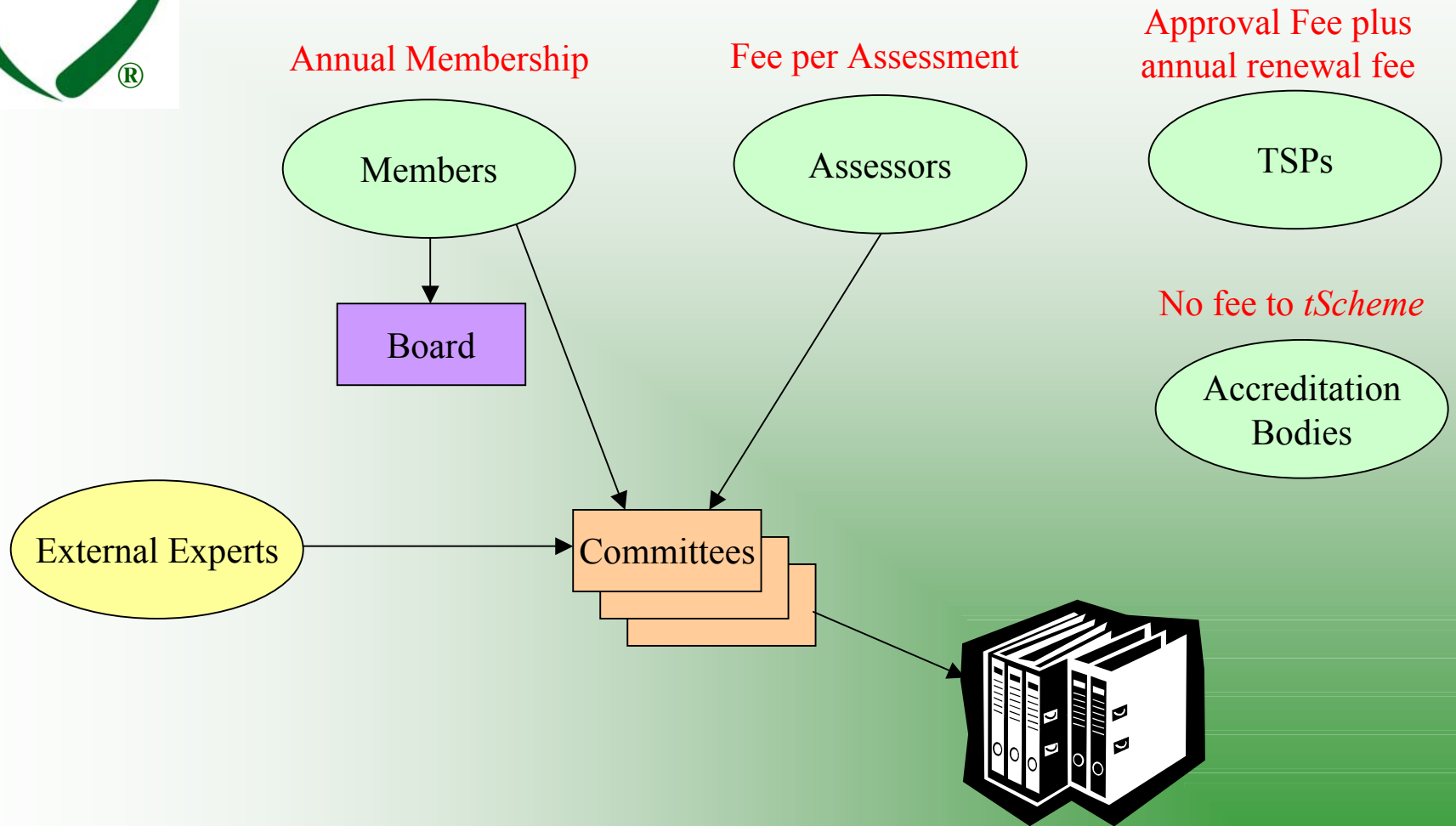
tScheme is a not-for-profit membership organisation chartered by the Electronic Communications Act 2000 and established following successful advocacy by its founder members in persuading HM Government not to invoke direct regulation on the electronic trust services market.

tScheme develops and publishes best practice technical, business and operational criteria for the independent assessment of electronic trust services, and grants approval to services that continue to meet those criteria.

By doing this, tScheme enables the UK Government to meet certain obligations under the EU Electronic Signatures Directive [1999/93/EC].



Structure of tScheme





What do Approval Profiles Measure?

- Is the service provider properly established and resourced?
- Is the service sufficiently defined?
- Is the service fair and reasonable?
- Is the service being delivered according to its definition?
- Is it secure enough?



What do Approval Profiles Not Measure?

tScheme does not attempt to test:

- that the service is fit for any particular purpose
- interoperability



tScheme *current status*

- 4 current ‘tScheme-Approved Service’ Grants
 - full details at http://www.tScheme.org/directory/index_appserv.html
- 3 current ‘tScheme Registered Applicant’ Status
 - full details at http://www.tScheme.org/directory/index_regapps.html
- 9 Approval Profiles - consolidation of industry best practice
 - future Profiles anticipated as services evolve
- 300+ individually-tagged assessment criteria
 - also enabling ‘tScheme-Ready’ component service assessment



PKI Bridges

Cross Certified:

D of Defense*
 D of Energy
 D of Homeland Security
 D of Justice
 D of Treasury
 D of State
 NASA
 DST (ACES)
 Illinois

Pending:

Gov of Canada
 ACES
 ECA
 DHS
 MoD UK
 D of Interior
 Patent & Trademark Office
 Educause (HE Bridge)

**Certipath
(Aero)**

**SAFE
(Pharma)**

**Higher
Education**

Tech Interoperability Testing

?

Participants:

BAE
 Boeing
 CAE
 EADS/Airbus
 General Dynamics
 Lockheed Martin
 Northrop Grumman
 Raytheon
 Rolls Royce
 Smiths
 Westland

Participants:

Johnson & Johnson
 Amgen
 Aventis
 Abbott Labs
 Bristol Myers-Squibb
 GlaxoSmithKline
 Pfizer
 Procter & Gamble
 Eli Lilly
 Novartis
 AstraZeneca

Participants:

Dartmouth College
 University of Alabama - Birmingham
 University of California - Office of President
 University of Wisconsin - Madison
 Duke University



Identity – what’s in a name?

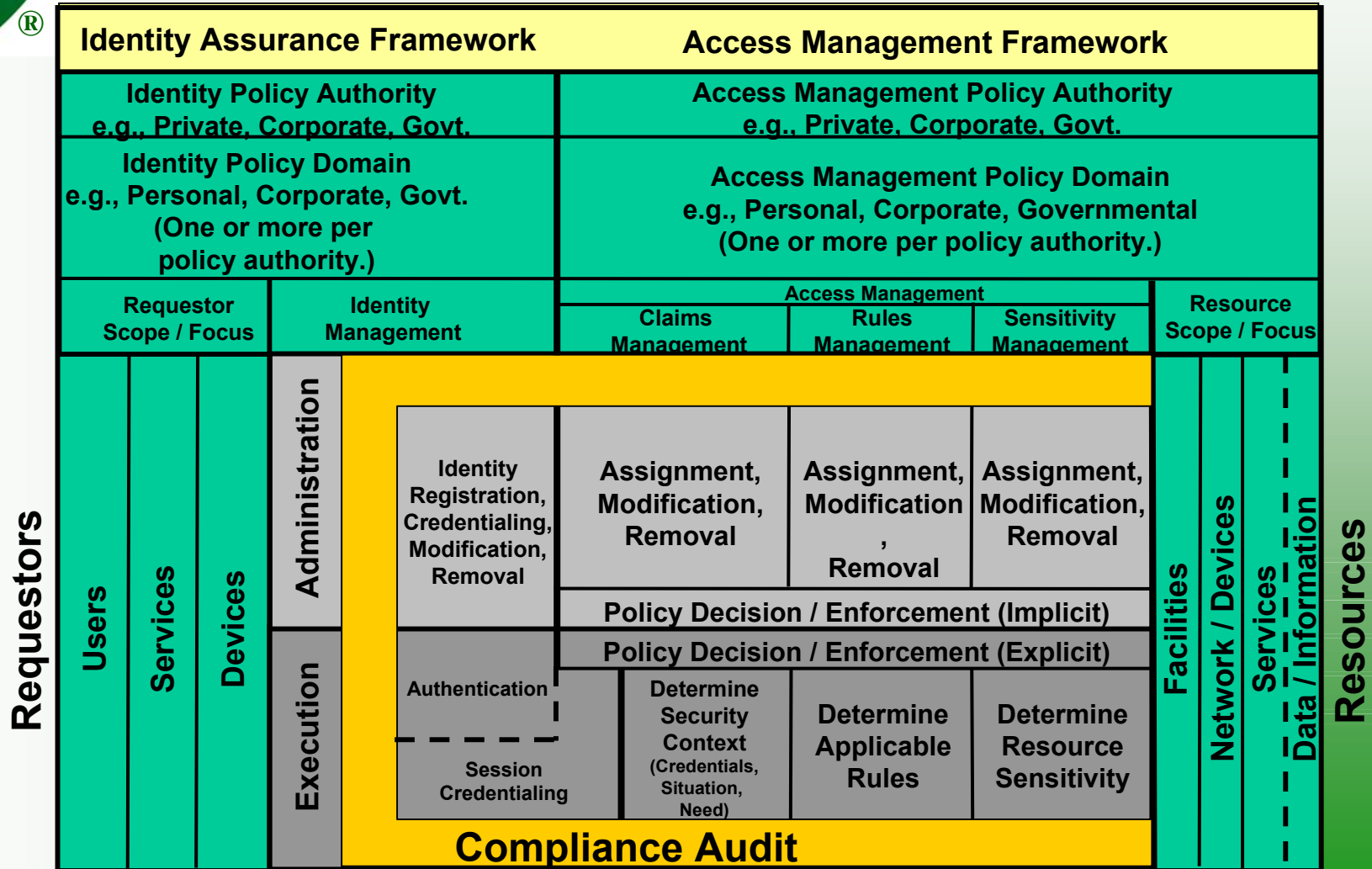
“A rose, by any other name, would smell as sweet.”

William Shakespeare, who never had to attempt to provide single sign-on across multiple platforms with highly-distributed resource managers consuming non-uniform APIs using inconsistent authorization names; with directory services that are not globally visible; supporting multiple, inconsistent authentication protocols.



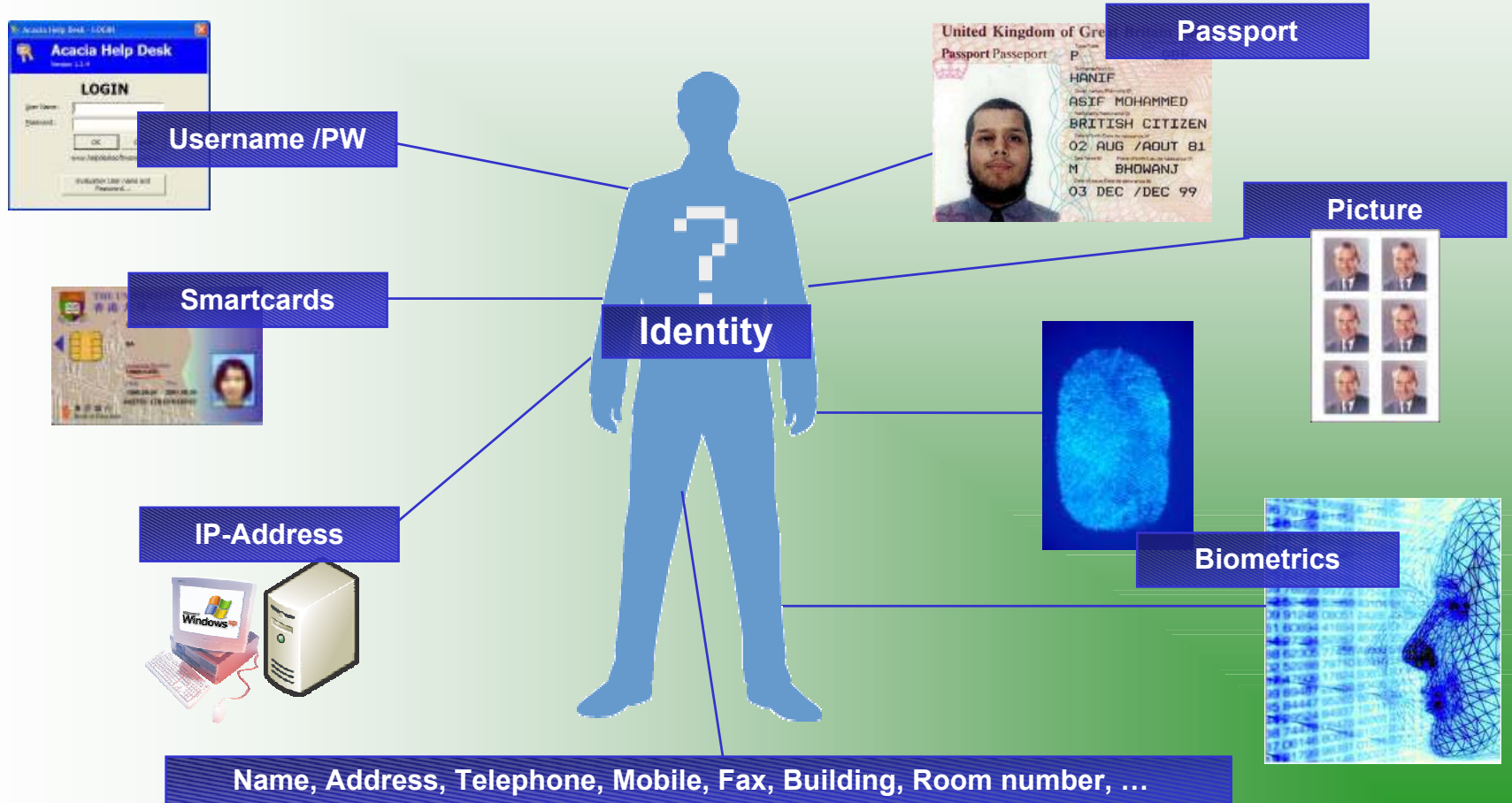
Identity – a Technologist’s View

Identity and Access Management Policy Framework





Need for Identity Management





Identity Management is a Process

- 1. Strong authentication of the individual**
- 2. Binding identity to a management system**
- 3. Binding credential to the individual**
- 4. Authentication of credential at all access points**
- 5. Real-time revocation of the credential**
- 6. Safeguarding identity information from unwarranted disclosure**



The Big Issue is TRUST

- **How much trust should be placed in the other organization's credential?**
- **What level of background vetting does the other organization employ?**
- **What is the strength of the credentialing process?**
- **Is there an effective process for revoking credentials?**
- **What level of access should this credential provide?**
- **Can a minimum level of trust be established?**



Trusted Information Sharing

The Trust Life-Cycle



- Are you who you say you are?
- Are you authorized to access my information?
- Can your organization prove this to me?



Authentication is not trust

- A credential provides
 - Authentication – knowing “with certainty” the name of the counterpart
 - “Proof” of this authentication
- This is not sufficient to trust the counterpart
 - Knowing the name of the crook does not make him honest



Trust Fundamentals

- Business probity and management competence
- Management and security policies and procedures
- Assurance of technical infrastructure
- Suitability of personnel
- Compliance with applicable legislation
- External relationships involved in service delivery
- Service-related policies and procedures
- Financial resources consistent with liabilities
- Procedures for dispute resolution



How to Establish Trust?

Trusted Identity Schemes

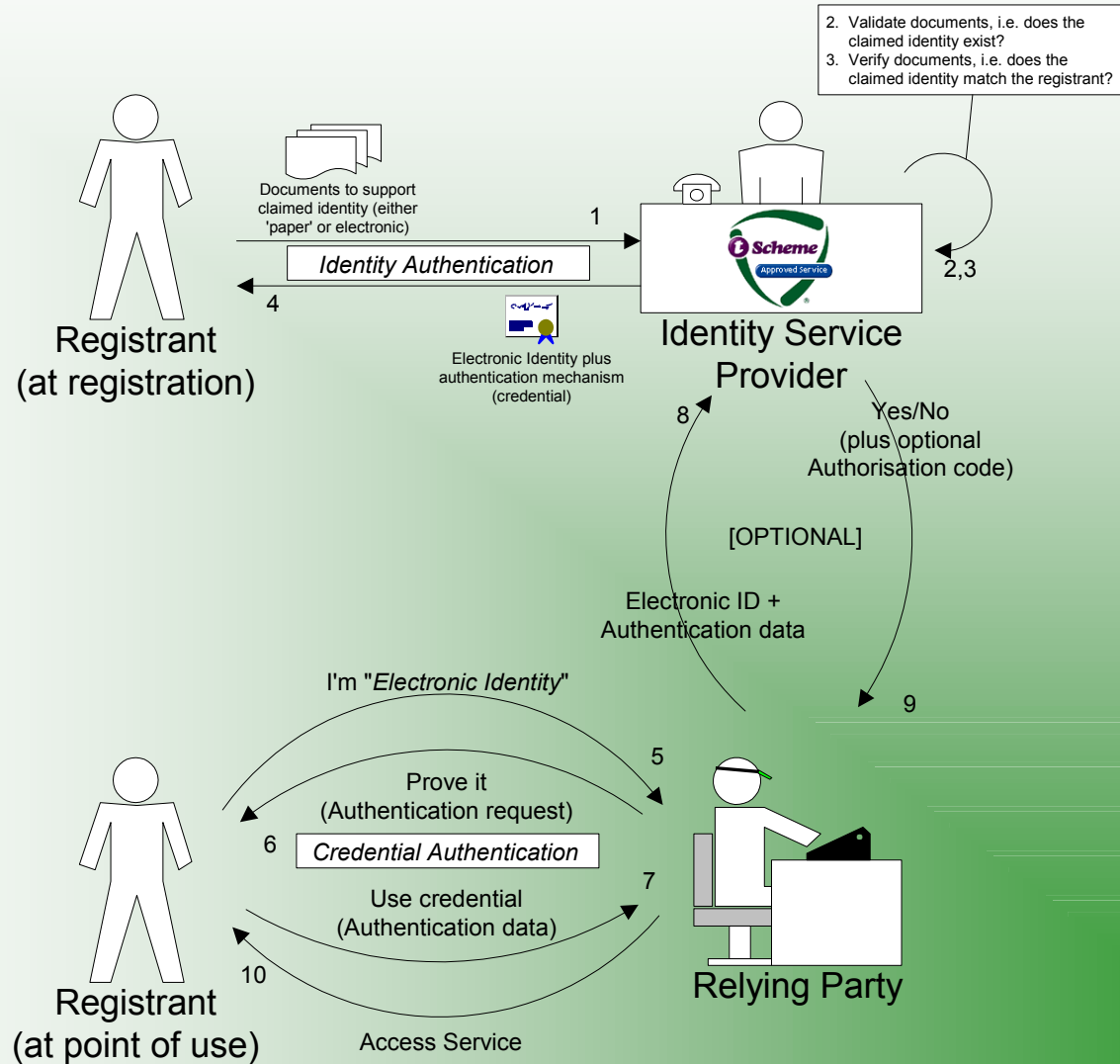


Trusted Identity Schemes

- Example of a Trusted Identity Scheme is *tScheme*
- *tScheme* assessment process based on independent audit
- Existing mechanisms for providing trust & confidence
- Maximum re-use of existing standards
- Profiles contain best-practice criteria
- Enrolment process assessed against current Identity Profile
- New Profile can be added to reflect additional criteria

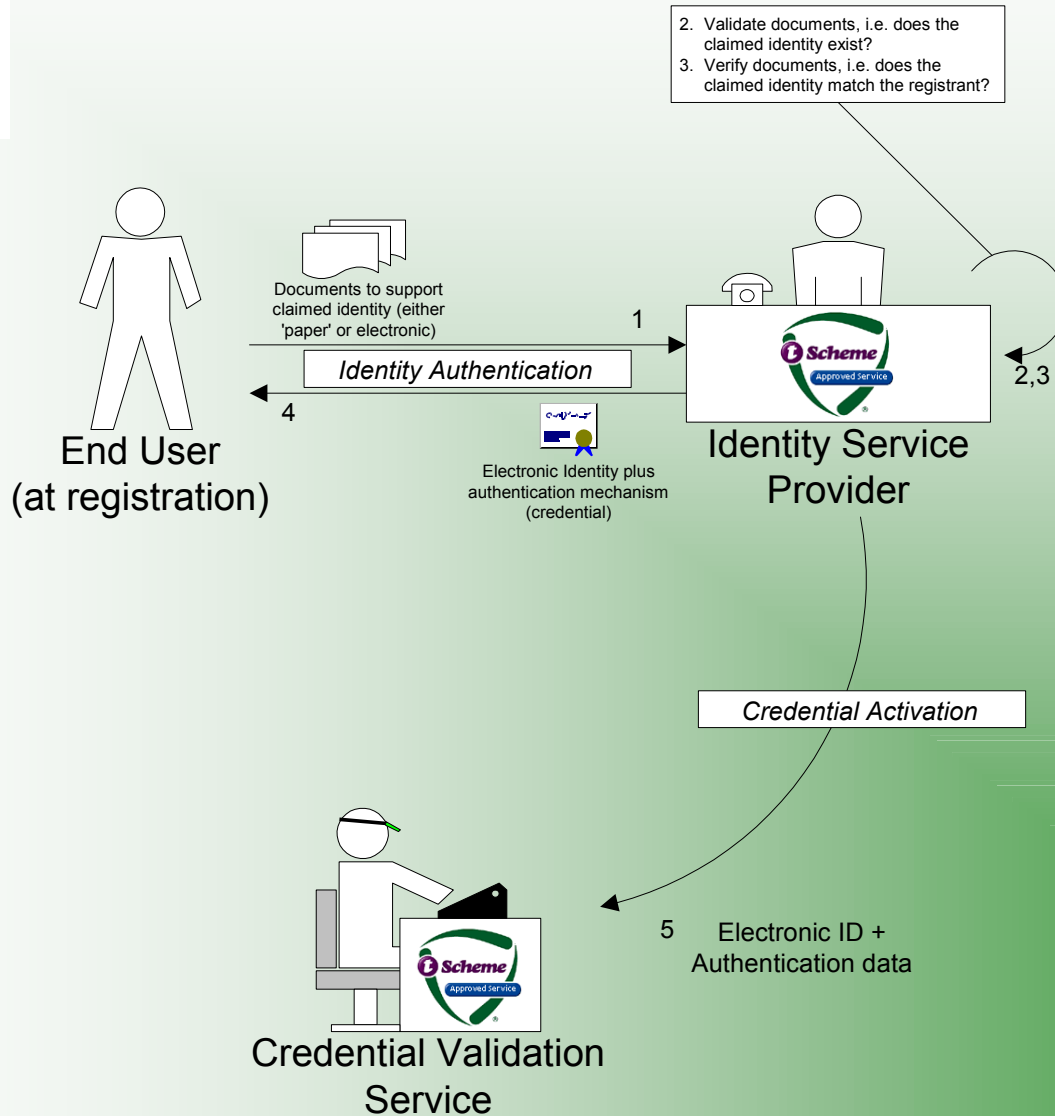


Identity Provider Service Profile



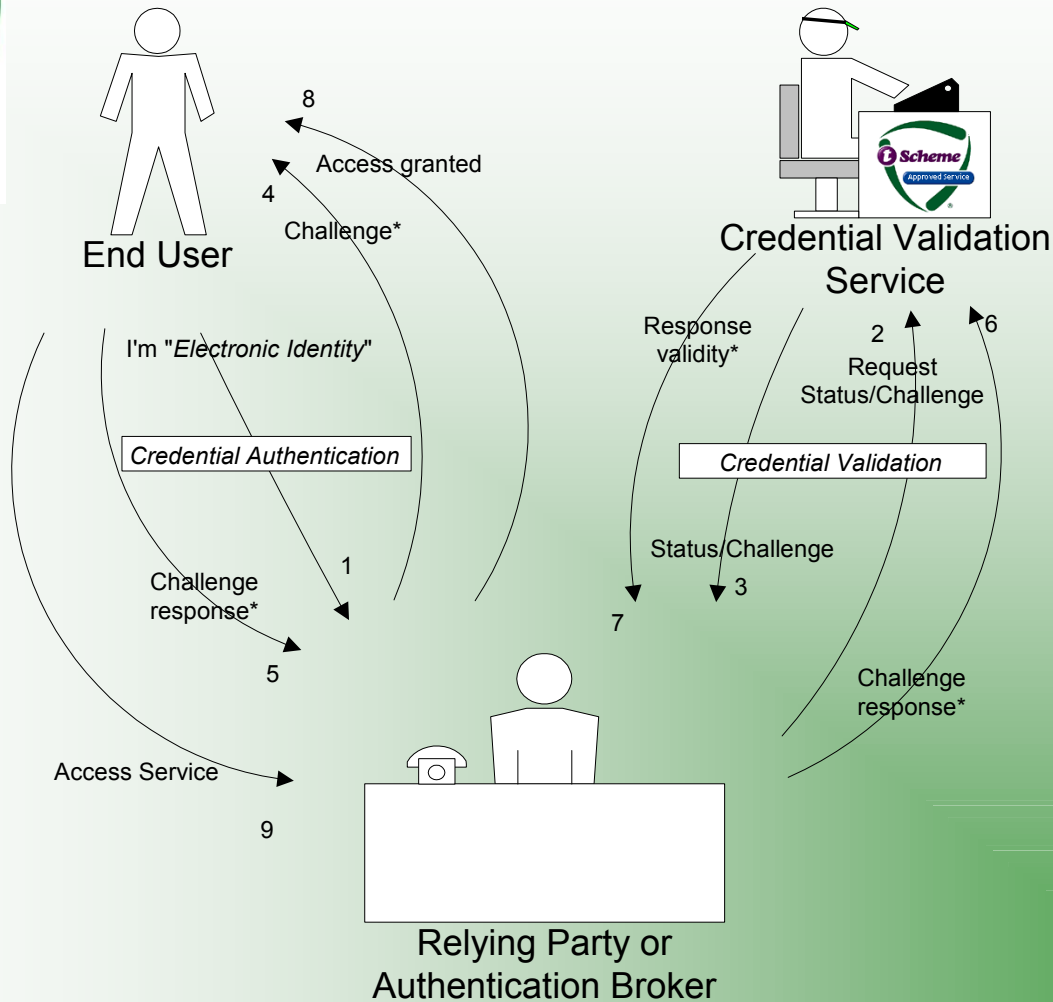


Credential Validation Service Profile (1)





Credential Validation Service Profile (2)



* Steps 4, 6, 6 & 7 are optional if CVS just provides a status and does not require a challenge/response mechanism



Government Gateway view

Trusted Sources of Identity

- There could be several sources of a trusted Identity (Identity Providers).
- The National Identity Scheme (NIS). This will provide the highest level of assurance for an Identity. However there will not be mass adoption for several years.
- Existing Government departments eg: DWP
- The Private Sector
 - A market could be created within the private sector that could provide services to both the public and private sector.
 - This aligns with current Government policy.
 - In order to access pan Government s services the Identity Provider would need to be tScheme accredited.

paye online construction industry scheme corporation tax vat returns
vat returns self-assessment online

 HM Government

Government
Gateway



The Role of the Assessors

Quis Custodiet Ipsos Custodes



Accreditation of Assessors

- Performed by National Accreditation Bodies
 - e.g. UKAS in the UK
- International Guidelines
 - International Accreditation Forum MLA signatories
- CIS3 framework document issued
 - Guidance covering EN45012 & EA 7/03 interpretation
 - available as a common standard for Certification Bodies

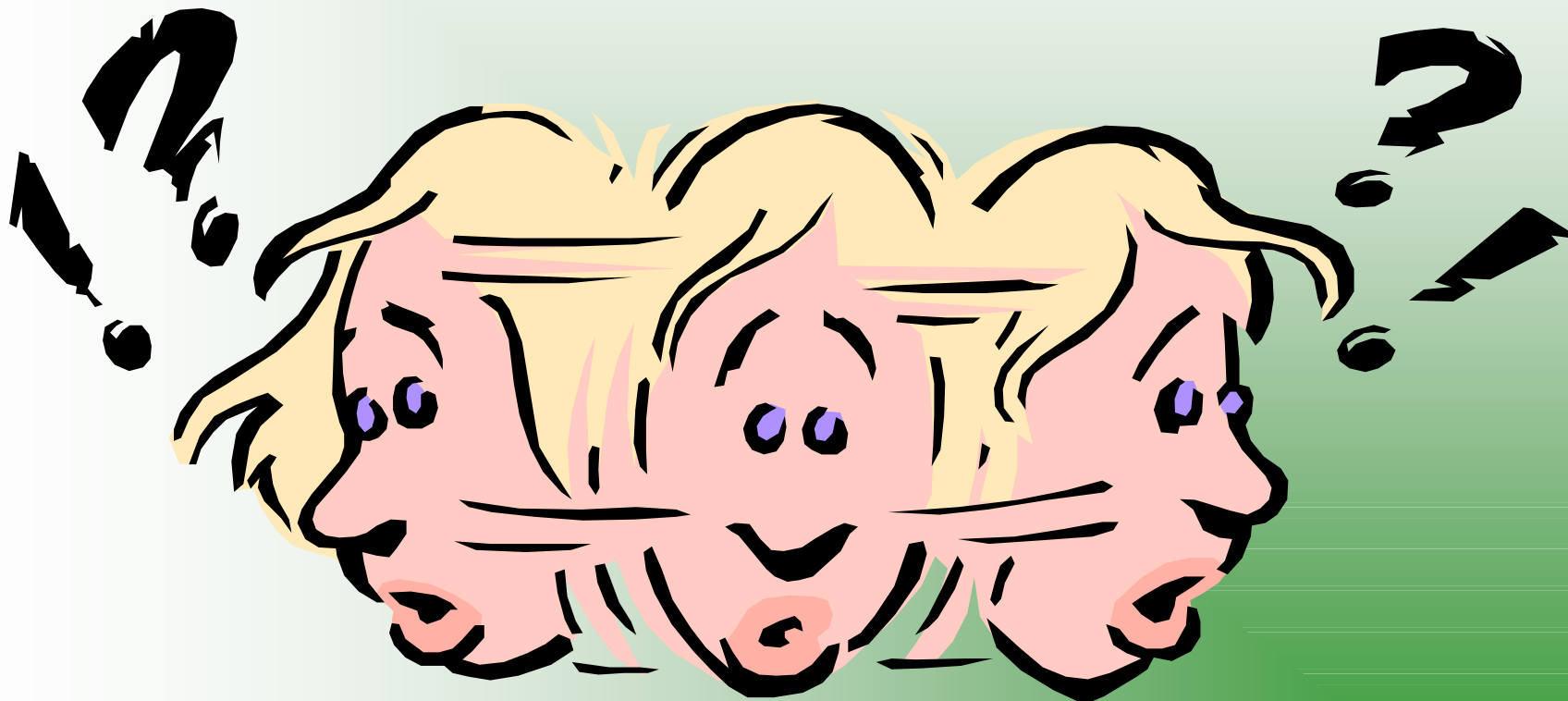


Auditors – a conceptual model





Questions?





look for the Mark:



www.tScheme.org

richard.trevorah@tScheme.org