

Online Security: So Who AM I Really Connected To?

InfoSec 27th April 2010

Andy Smith MSc FBCS CEng CITP FSyl

Me in 60 Seconds

- Chartered Fellow of the BCS
- Member of the BCS Security Strategic Panel
- Fellow of the Security Institute
- Masters in Information Security from Royal Holloway
- Started working with the Internet in 1986
- Developing websites and installing firewalls 1992
- Worked in Information Security all over the world
- Currently on contract to Cabinet Office and IPS
- Spent the last 6 years concentrating on
Identity Management and Assurance

The next 2 hours

Aims

- Knowledge Transfer
- Interactive – Ask questions

Agenda

- What is Identity?
- Establishing Identity
- Security issues with Remote Authentication
- Viable options for Remote Authentication

The Questions?

- What is Identity?
- Who are you - Identification?

- Ford Prefect problem



- Are you really who you claim to be?

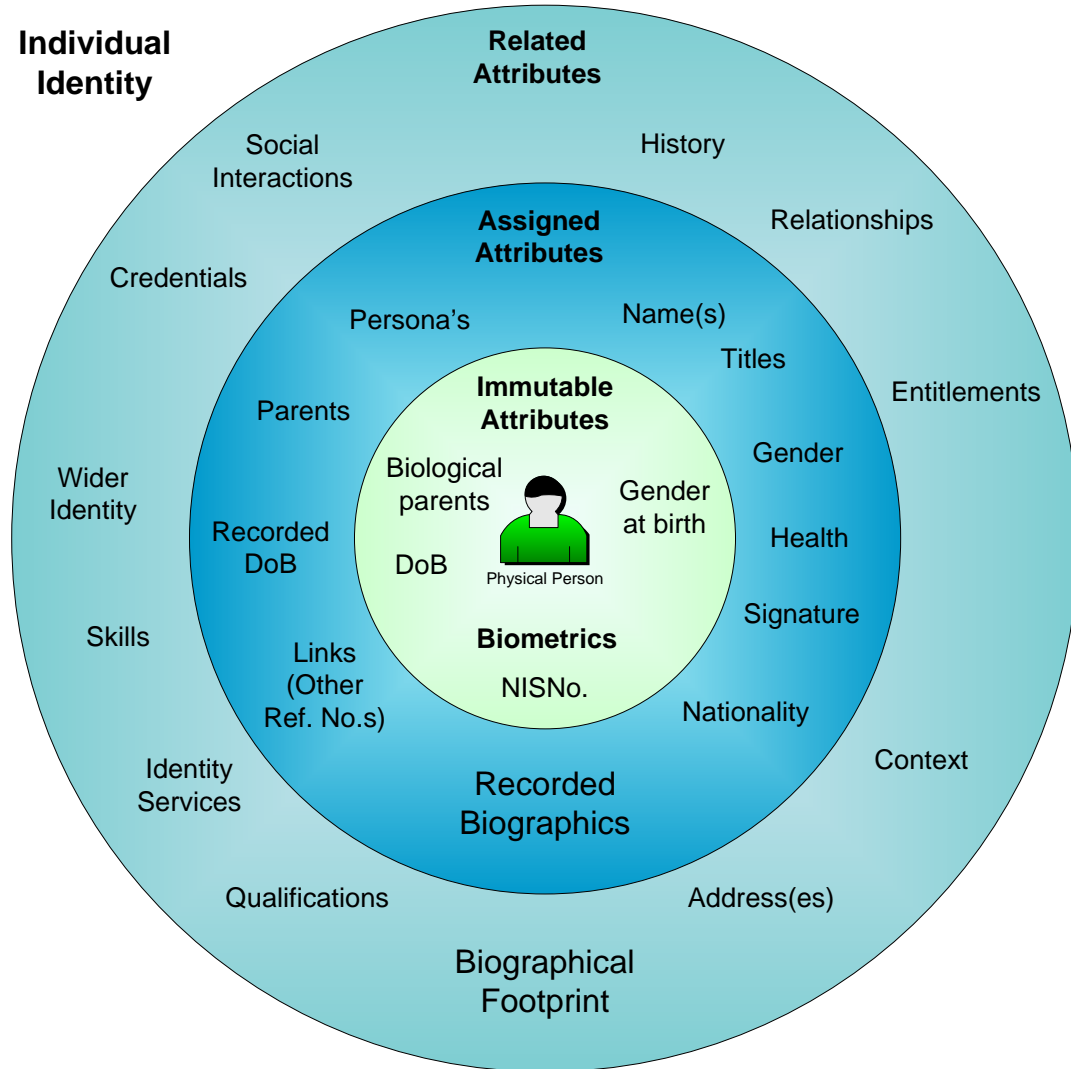
- Verification / Authentication
- Sidney Bristow problem



- How can I establish an identity and verify it easily?
- How can I be sure you are you online?
 - Unsupervised
 - No trusted infrastructure

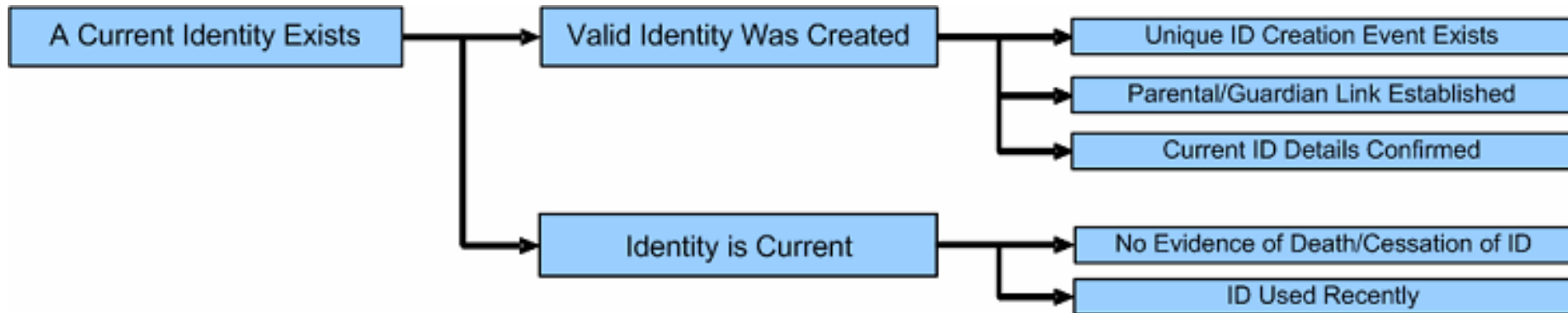
Identity - Fundamentals

- 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:



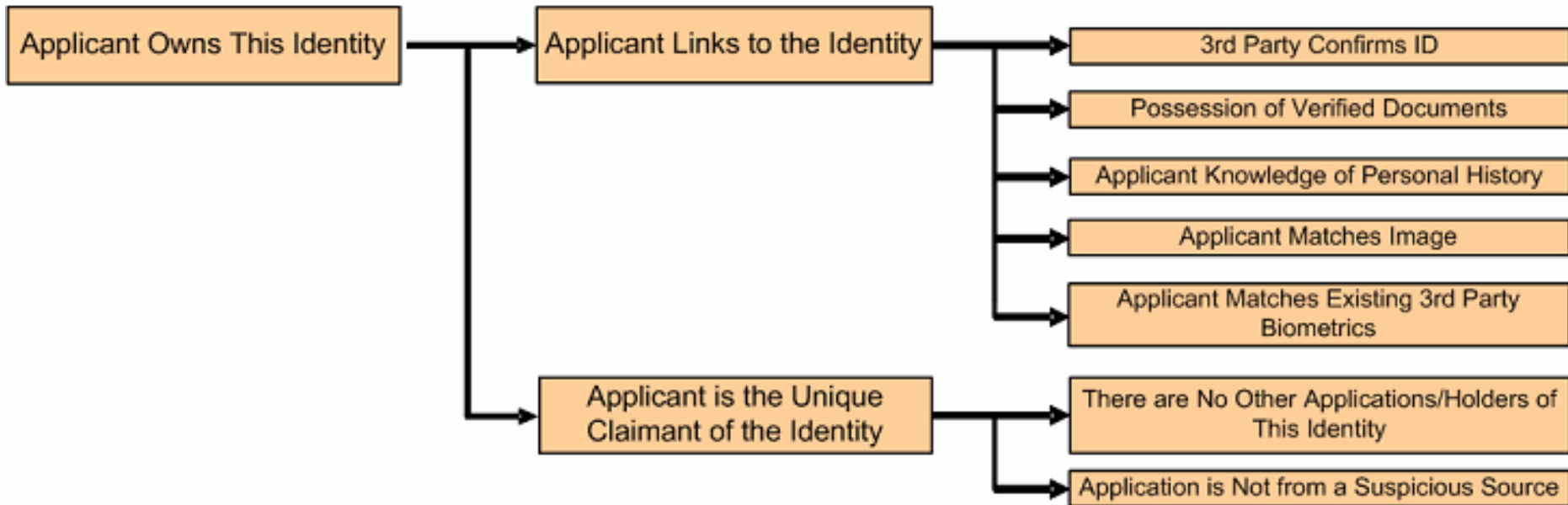
Establishment - Existence

- 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?



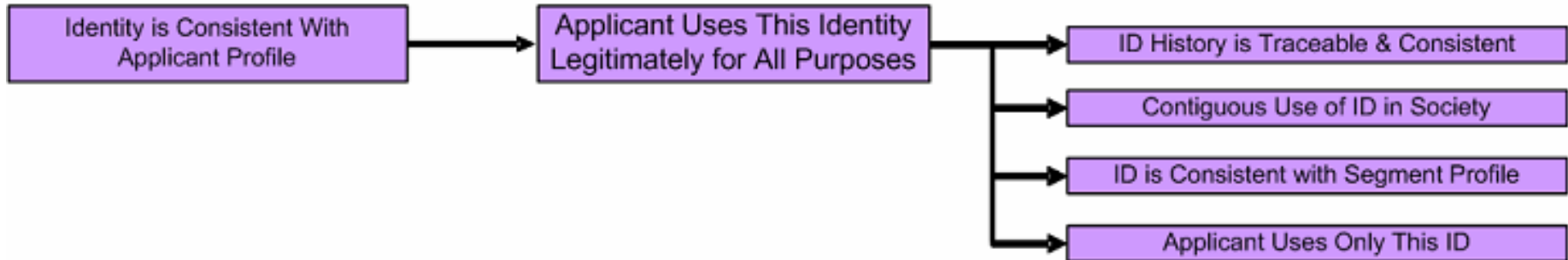
Establishment - Provenance

- 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.
- Look at a real case - Me



A quick look at ME?

- Who can corroborate I am me?

Andrew Ian Smith
Andrew Smith
Andy Smith
Andrew
Andy
A I Smith
A Smith
Smiffy
Smitty
Daddy
Uncle Andy
Mr Smith



Can anyone be sure?

Google search:

Andy Smith ~24,700,000

Andrew Smith ~36,000,000

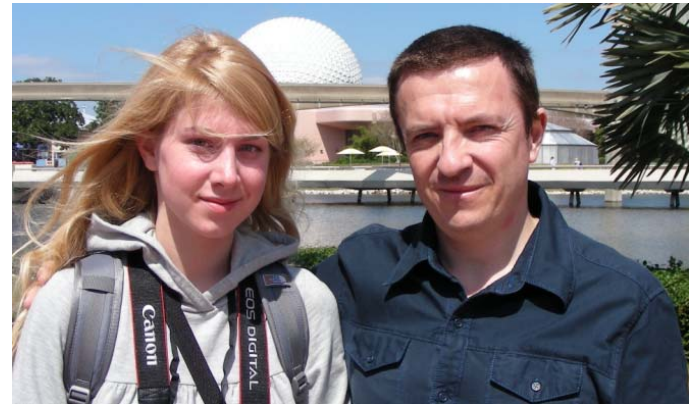
CLAS 276 members

2 Andrew Smith's

School ~2000 students

6 Andrew Smith's

Linda Knows ME



Fred Knows ME



Mum Knows ME



Athena Knows ME



Friends Know ME



Infact lots of people Know ME



Establishing my identity – People

- Family, friends, colleagues, can corroborate my existence
- A good start, but what else?



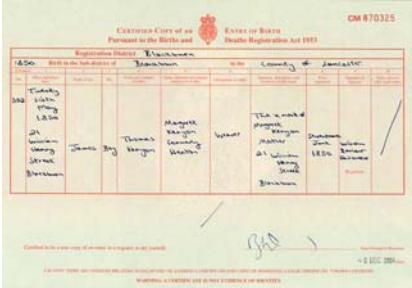
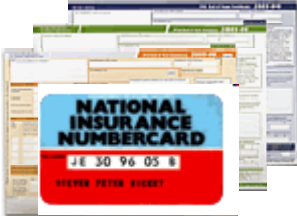
Establishing my identity – Records

A historical document titled "CERTIFICATE OF an Entry to Birth" from the Registrar General, London, dated 1893. The document is a form with a grid for recording birth details. The grid has columns for "Date of Birth", "Place of Birth", "Sex", "Age of Mother", "Name of Child", "Name of Father", "Name of Mother", "Name of Registrar", "Signature of Registrar", and "Signature of Parent". The form is filled with handwritten text. The name of the child is "John William". The name of the father is "John William". The name of the mother is "Mary". The date of birth is "1893". The place of birth is "London". The sex is "Male". The age of the mother is "25". The name of the registrar is "John William". The signature of the registrar is "John William". The signature of the parent is "John William". The document is numbered "CM 870325" in the top right corner.

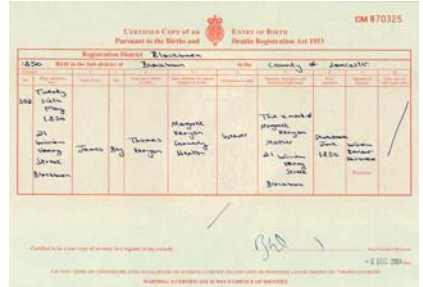
Establishing my identity – School

A birth certificate form from the Registrar General, London, dated 1983. The form is filled out with handwritten information, including the name 'Margaret Margaret' and the date '12th March 1983'. The form is titled 'CERTIFICATE OF AN ENTRY TO BIRTH' and 'Particulars of the Birth and Details Registration Act 1953'. The registration number is CM 870325.

Establishing my identity – Government



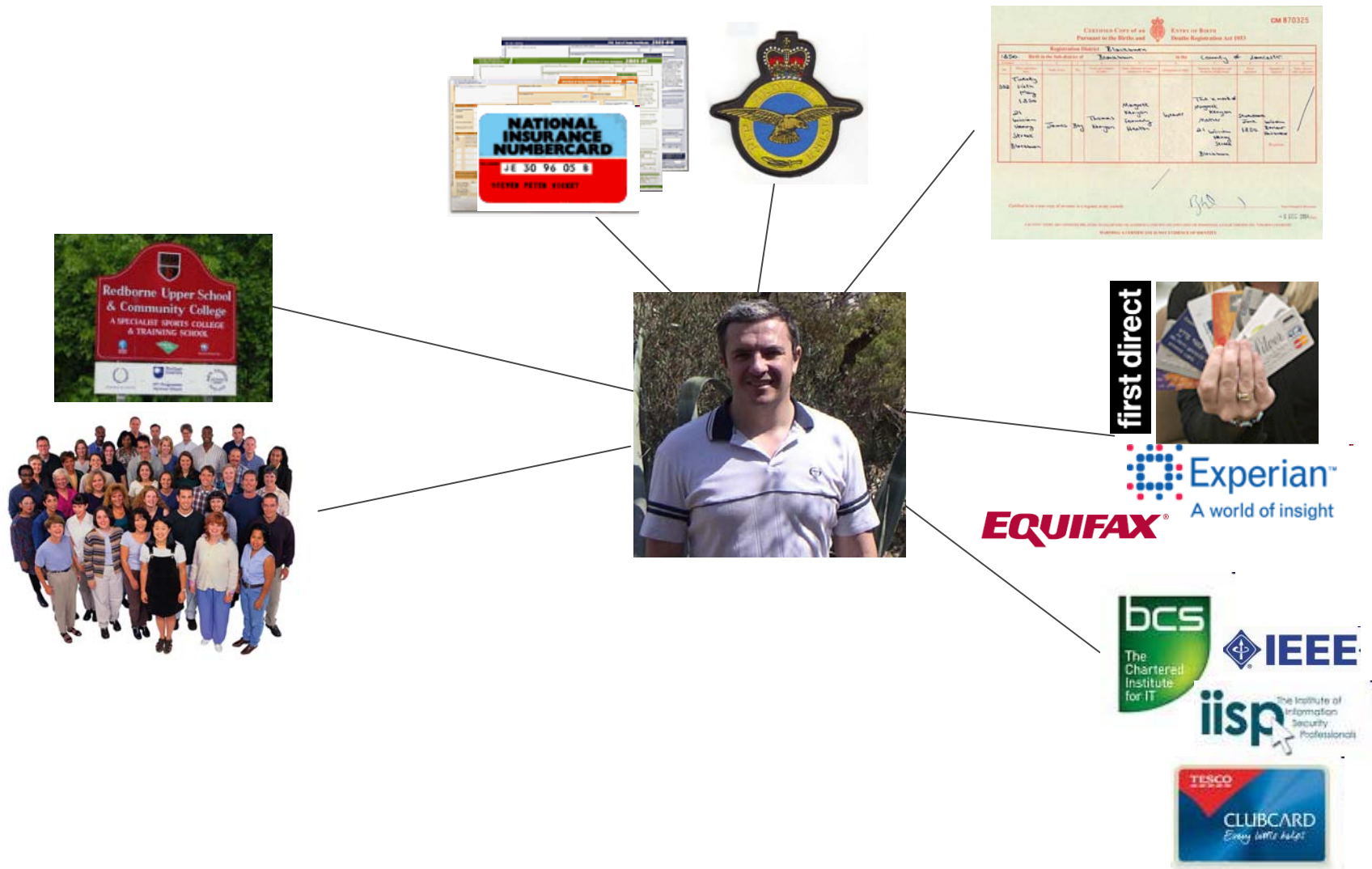
Establishing my identity – Career



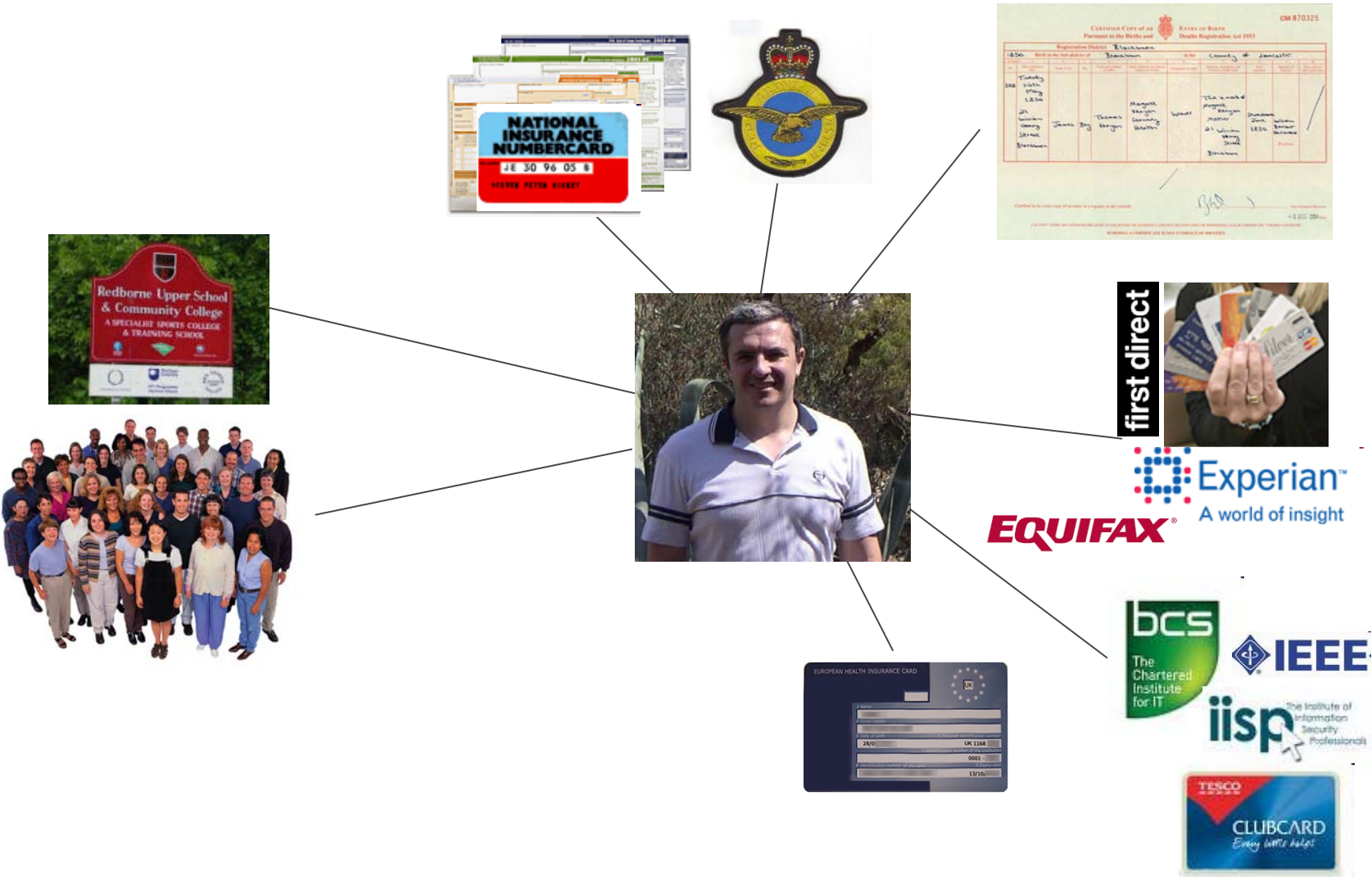
Establishing my identity – Finances



Establishing my identity – Organisations



Establishing my identity – Health



Establishing my identity – Qualifications



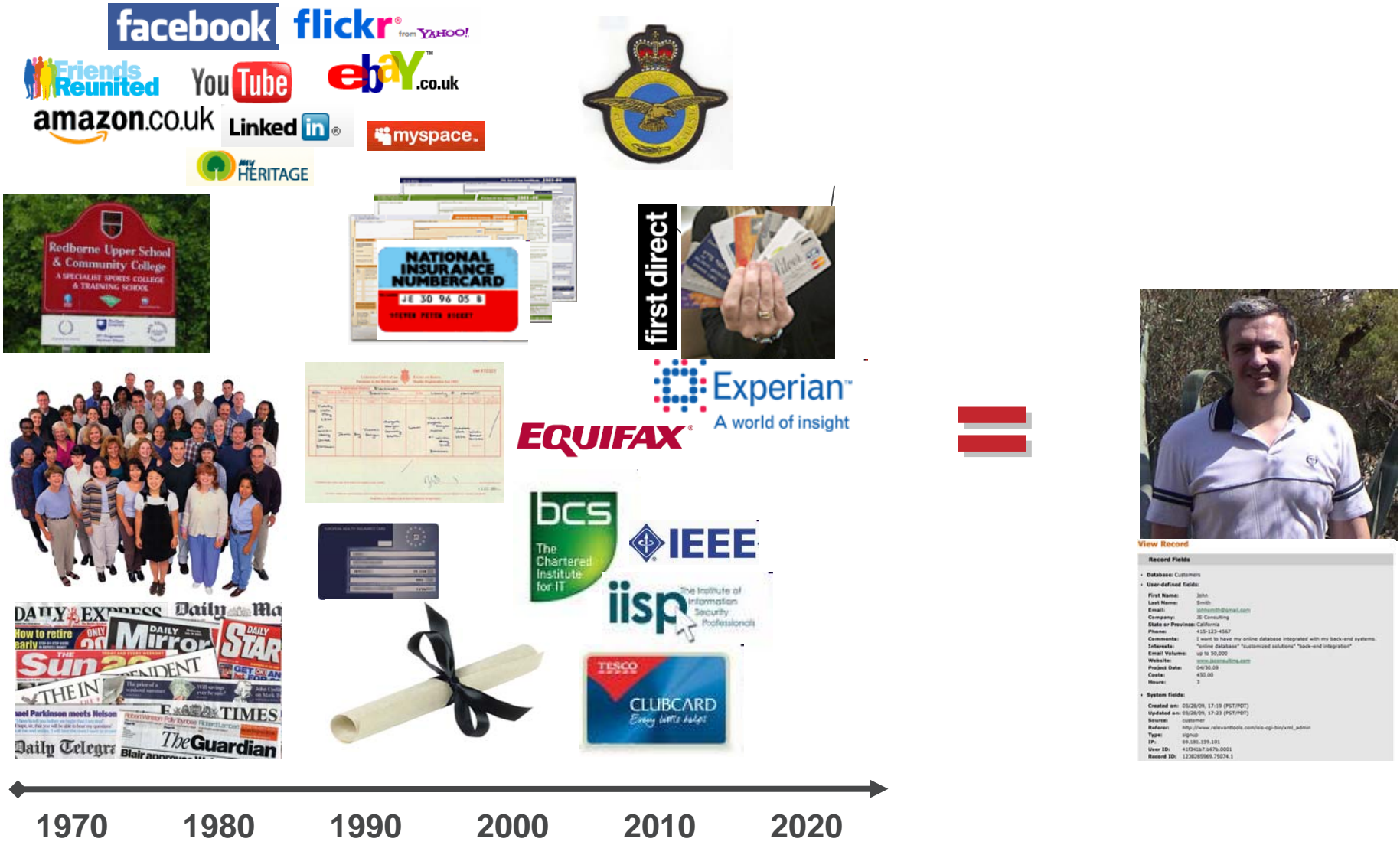
Establishing my identity – Pubic profile



Establishing my identity – Online profile

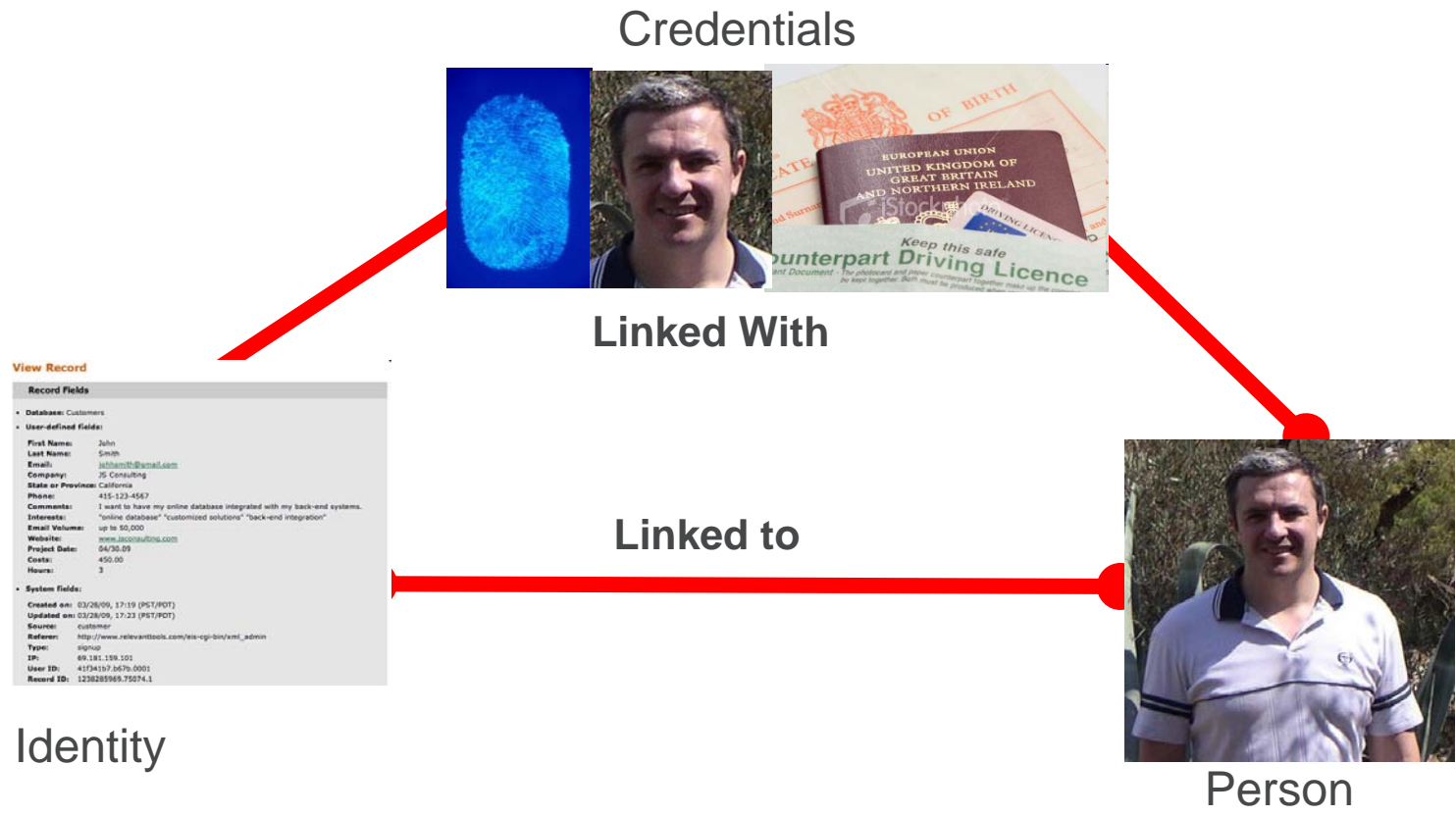


Establishing my identity – Me



High Assurance Link

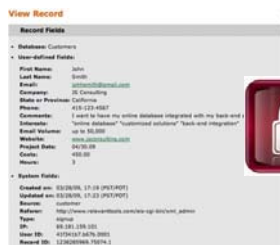
Now we know who I am - with some assurance ID has to be immutably linked to physical person



So what is Identity? My view

- An Identity is who the person is perceived to be by others
 - That the bit of wet carbon and associated attributes
 - Is known by others and has interacted with society
 - Established a biographical footprint in time
 - Consistently used the same personas (maybe more than one)
 - Has a set of personas that remain consistent
- Its all the attributes and relationships that a person has and how they interplay with each other throughout their life

Identity



Person



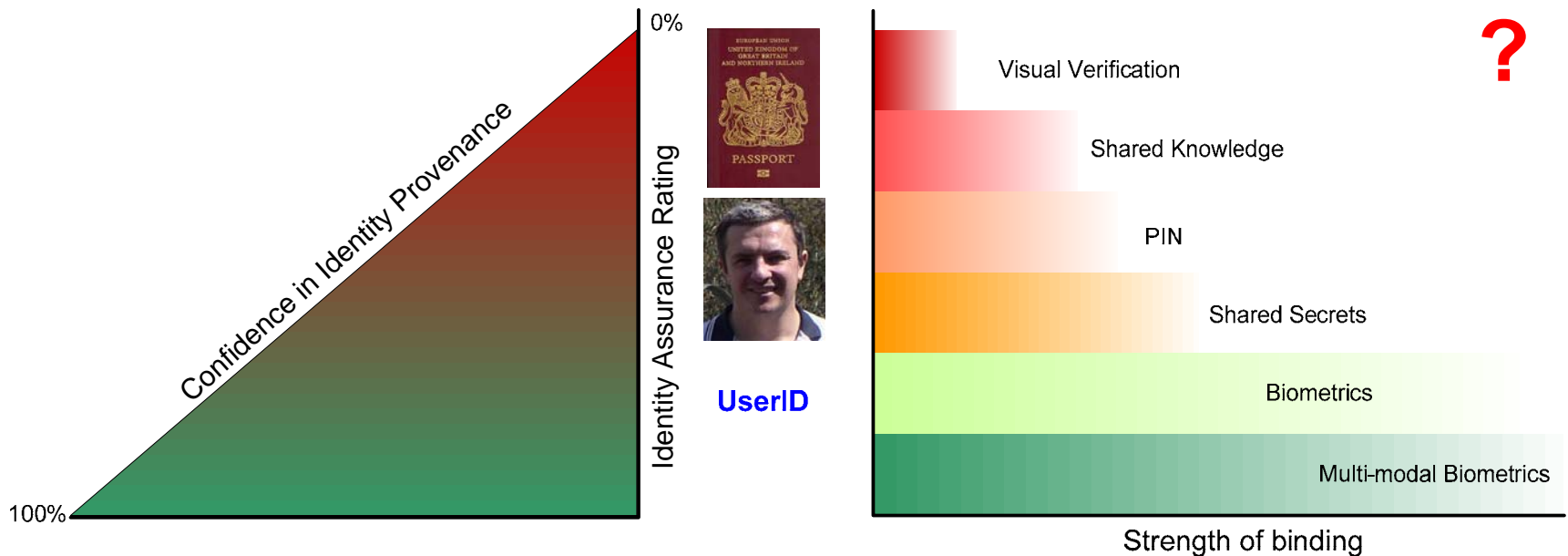
Personas



Assured Identity

- Assurance = level of confidence obtained while establishing the identity
- Sliding scale ranging from illegal immigrant with no papers to royalty with centuries of heritage
- Link to the identity can be locked in using various credentials
 - Can then be reconfirmed at a later date using those credentials

Confidence + Index Credential X 2nd Factor Credential = Assurance level



Summary - Identity Assurance

- Identity Assurance (IdA) covers the provenance and integrity of the identity including its ongoing maintenance.
- It gives you a measure of confidence:
 - That the provenance of the identity has been established as far as practicable
 - That the identity is complete and the integrity of the information cannot be degraded
 - That the asserted attributes are verified accurate as far as practicable
 - That any change of circumstances to attributes are corroborated or validated before being changed
 - That the confirmed identity is linked to the person with high assurance credentials (biometrics); and
 - That the individual and any personas (also known as "identities") they may have are bound to that unique root identity.

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

RA - Where are the threats from

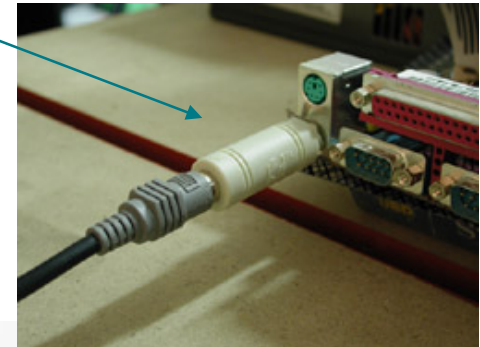
- Mainly from people
 - Pranksters (siblings etc)
 - Inadvertency (error, stupidity)
 - Opportunists / Journalists
 - Malicious people (e.g. revenge)
 - Militants & Terrorists
 - Criminals
 - Serious & Organised Crime
 - Foreign Intelligence Services

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



Threats - 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)



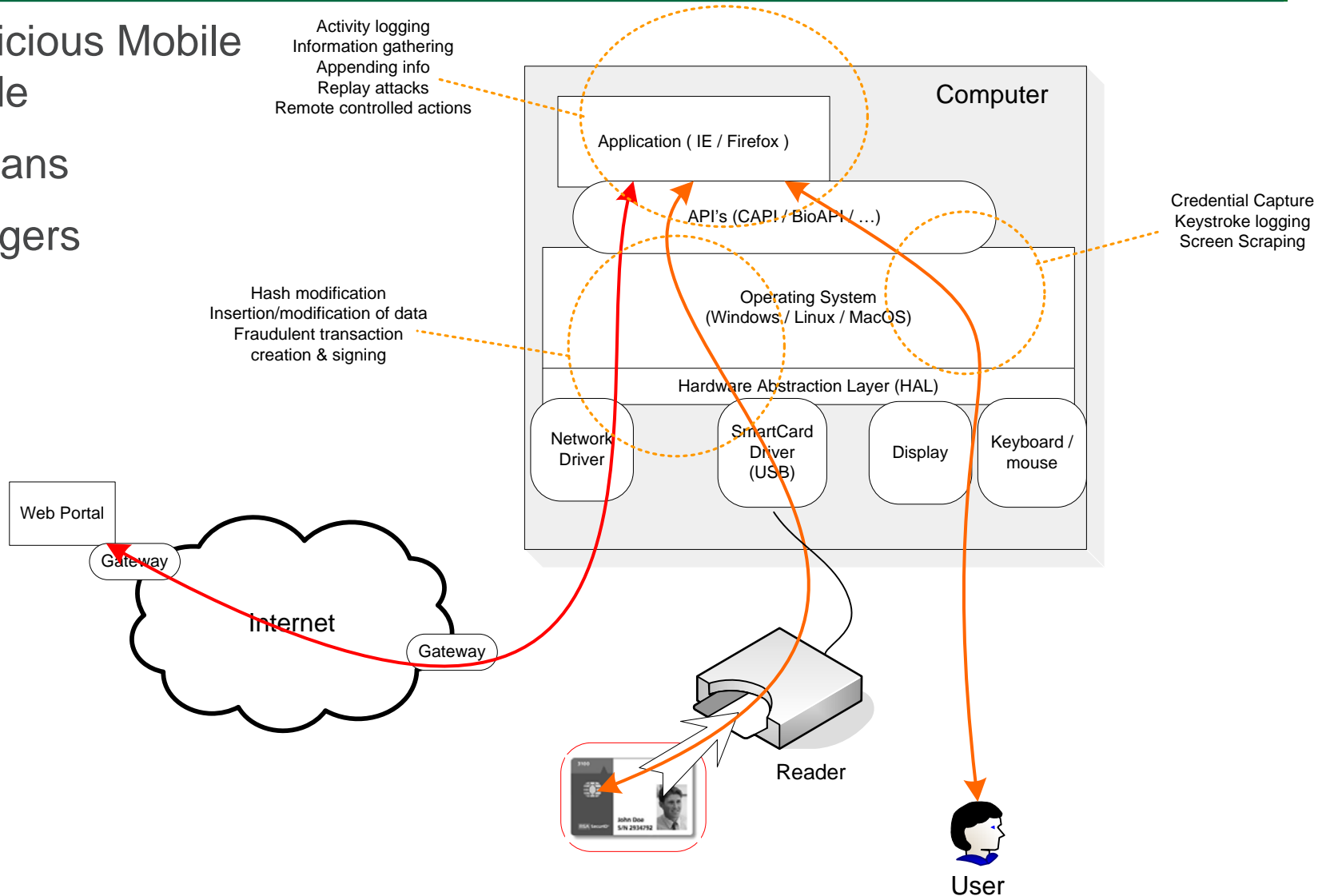
- Communications
 - Network sniffers / probes / recorders
 - Listening in (scanners, phone taps)
 - Redirection (fake web sites)
 - Email / file capture



Scanner for listening to wireless phone conversations

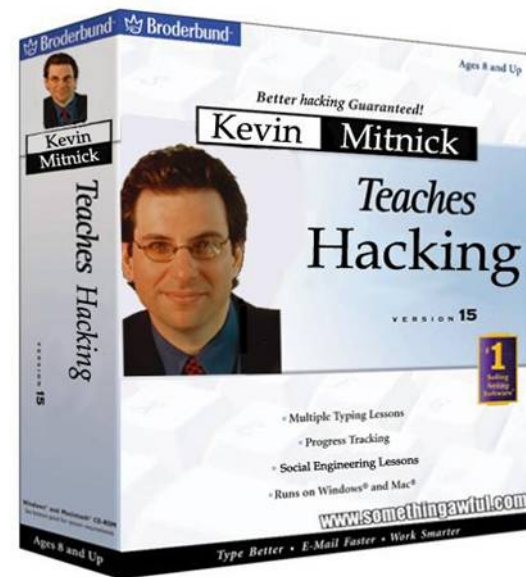
Threats - Computers

- Malicious Mobile Code
- Trojans
- Loggers



RA – 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)



RA – Risks

- Keyboard logging and screen scraping of credentials or personal information that can be used to steal a whole identity or just misuse an identity for gain
 - Insurance/mortgage/loan/passport application forms
 - Online purchases giving credit card details
 - Review of online accounts showing detailed information (e.g. Creditcheck)
- Information can be used to:
 - Apply for bank account or credit cards
 - Transfer of funds from a bank
 - Order goods or services
 - Adopt the identity of someone who has emigrated or recently died
 - Adopt the identity of someone who does not understand computers
 - Commit a serious crime in another persons identity

Risks with current methods

Biggest risk with remote authentication is failure to authenticate a person with any level of assurance over untrusted infrastructure, in an unsupervised environment

- Inability to trust the decision giving access
- Guessable standard questions on voice channels
 - Mothers maiden name shared in family and easy to obtain from birth certificate and marriage certificate
 - Date of birth easy to obtain from birth certificate and various sources such as Friends Reunited, electoral roll, letters, rubbish
- Static credentials (e.g. password, PIN)
 - Can only be sure that remote card-holder knows the credential not that they are the authentic holder of the credential
 - Can easily be recorded and replayed

RA - Solution Requirements

- Not dependent on an untrusted computer
 - No need for a computer (telephone, post, mobile, PDA)
 - Works with shared, office or public computers
- Dependent on what can be given to user e.g. token
 - Provides a high assurance link between person & token
 - Uses capabilities of token that are impracticable to forge
 - Responses unique to that token
- Some level of Trusted Infrastructure
 - Evaluated standalone device – token and reader?
 - Cheap - Free to customer (Given away with Weetabix)
 - Trusted decision, linking user to token
- Non-repudiation
 - Legally admissible evidence

RA - Solution Practicalities

- Remote Authentication does not need to be 100% secure
 - Not used for changes to identity or high value transactions
 - Used to change basic details online (address, contact details)
 - Used to perform transactions based on risk assessment
- But must provide much higher assurance than other credentials
 - Combination of token and Password/PIN (Two-Factor)
 - False accept rate of at least 1 in 1,000,000 preferably higher
 - 4 digit PIN only 1 in 10,000 6 digit PIN gives 1 in 1,000,000
 - Not forgotten, guessed, stolen or copied easily
- Yet needs to be simple to use
 - Consistent interface for all contact channels
 - Support for special needs

RA - Credential options

- Password – The most common option
 - Adequate in limited risk areas, e.g. logging onto a computer in a trusted environment. Fixed passwords are not good over the Internet or when keyboard logging could take place
- Two Factor with simple token and Personal Identity Number (PIN)
 - Adequate with trusted infrastructure and two factor authentication (ATM, EPOS, bank network) or in a supervised environment (bank, office)
 - Can be used remotely with token as part of a business process
 - Cannot be used for high assurance authentication
- Two Factor with secure token and trusted reader
 - Prevents PIN/PW being captured on computer
 - Provides end-to-end mutual authentication of token
 - PIN or Password provides evidence of authorised access to token
 - Provides the best possible assurance in the authentication

Example 1

- Special problem of malicious code on computers
 - Cannot trust operating system or 3rd party software
- Therefore need trusted code
 - Authored by trusted provider and downloaded from trusted site
 - Portable application (e.g. only dependent on Java being available on computer or mobile phone)
- Encryption between Application & Web Server
 - Prevents malicious code capturing or changing information
 - Mutual authentication between end-points
- Reader connected via USB to computer
 - Encryption between application & card
 - Decision making and private keys stay on card
 - Credentials entered via reader, not computer



Example 2

- Use of a completely separate device for:
 - One time password
 - Challenge / Response
 - Electronic Signature
- Prevents malicious code working
- Works with various channels
 - Computer / PDA / Blackberry
 - Phone (voice and SMS)
 - Even post



VeriSign Identity Protection Mobile Center

VIP Access for Mobile

VIP Access for Mobile provides an easy process to download, access, and enable your VIP credential.



Select BlackBerry



Select iPhone



Select Other Phone

VIP Access for Mobile is supported by a variety of mobile brands and models.

Residual Risks

- Coercion / Duress
 - We cannot overcome this remotely
- Trojan loggers
 - Has to run on as standard OS
 - Static credentials easy to capture and reuse
- Theft / capture of PIN if used
 - A PIN should not be used if possible as it is easy to steal, copy, guess or otherwise obtain
- Breaking the private key, if challenge-response too short
 - Possible to attack cryptography using short sets of encrypted responses & unencrypted challenges
- Even good tokens like credit cards can be cloned

Conclusion

- Remote Authentication is obviously possible
 - Need to have a strong registration process or rely on others
 - Need some method to implement trusted infrastructure
 - Token – prevent cloning and provide mutual authentication
 - Reader – not dependent on untrusted infrastructure
 - Credentials need to:
 - Be two-factor
 - Implement one-time authentication
 - Level of access needs to be determined by risk assessment
- Residual risks remain
 - Coercion / Duress
 - Theft or compromise of credentials
 - Misuse of credentials (e.g. sharing them with a friend)

Questions



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