

Security of Identity Management

Professor Brian Collins

Headline issues

- Purpose of ID management and ID security
- Practical process and technology issues
 - Enrolment processes
 - Identity verification
 - Limitations of Biometrics
 - Usability and acceptability
 - Social Issues
 - Trials
- Aspects of Technological solutions
 - System architecture
 - Functionality
 - Cards and Tokens
 - Challenge processes
 - Registry data management
 - Security and data sharing
- Programme management

Defence College of Management and Technology

Purpose: “Reliable and secure proof of
identity”

- Allowing citizens to prove their identity
- Preventing terrorism and criminal activity, or at least making it harder
- Preventing illegal immigration and work
- Preventing access to services and payments from those not entitled (health, social security)
- Facilitating business transactions
- Etc.

Enrolment processes

- Secure enrolment, and secure storage of enrolment data, is crucial to validity of ID management
- Secure process of establishing ID at enrolment
 - What documents or information is used?
 - How can staff tell whether documents are genuine?
 - What checking is done?
 - How will inconsistencies in existing databases be dealt with?
 - How long will it take to issue ID card or token?
 - Enrolment staff have to be trustworthy and reliable – how will they be vetted?

Verification processes

- Wide range of usage scenarios:
 - Policeman on the beat
 - Airport security
 - Hospitals
 - Doctor's surgery
 - Bank
 - Library
 - Video hire
 - On-line
- Subsequent use of verified information

Technology solutions for tokens

- Card technologies are rapidly changing
- Memory devices are becoming cheaper and widely available in a wide range of formats – why use cards?
- Wireless access gives less intrusive reading capability – proximity devices - RFID
- Network security is vital for high level of confidence in transfer of personal data
- Integrity of systems implementation and operation vital for good user experience

Biometrics

- No single biometric on which whole population can enrol
 - Permanent and temporary problems with finger and iris recognition
 - What to do with people who have problem with both?
 - Some groups do not have to show face on photos?
- Face recognition has close to 100% enrolment, but low performance in field
 - Personal and environment factors
 - False rejection could lead to refusal of service, or slow down service to unacceptable level

Functionality

- Primary functionality is to record identity information at the point of enrolment and to re-verify identity when challenged.
- Other potential functions are:
 - Prove rights for entitlement to services (identity not essential for that at the point of service delivery, only at point of rights enrolment)
 - Proof of personal attributes (age, sex, address)
 - Proof of nationality
- Card information and Registry information may be necessary for all or some of these functions, depending upon data and system architecture

System and Data architecture

- Is the register one database on one machine or is it distributed across many machines – security impact
- What availability of service is required when:
 - A large number of concurrent users are using the system (what number is expected?)
 - System upgrades are necessary
 - Failures of components occur
- What range of user terminals are expected to be able to access the system – PC, Mobile phone, PDA, Internet café, Bespoke system – access controls
- How will the design avoid the system becoming a legacy of the future
- Why is a national system better than a set of interconnected regional systems (cf Germany)
- How is data held and how will formats be kept up to date and data re-verified in case of systems failures

Security and data sharing

- Quality of data – who assesses relevance
- Benefits and risks – to the citizen or the government departments concerned
- Who sets standards for security – national authority?
- How are these aspects audited and by whom and how often
- How is the system protected against denial of service attack

Data checking

- Who does this and against what standards
- When biographical footprints are in another language than English, and maybe only in handwritten form, are there enough cleared people to carry out the work to the required standard
- How are illiteracy and lack of biographical footprints to be dealt with

Conclusions

- Ownership and security of information that supports identity is still a subject for debate
- Technology of biometrics still not good enough for reliable verification
- Systems issues are complex and unresolved
- Expected benefits are yet to be supported by evidence
- And yet – some way of improving identification of people is vital