



Protection of Identity in E-Borders Programme

Back to Basics

Tony Collings OBE, FBCS, IISP, CLAS

Achieving Integrity





Significance of E-Borders

- **First duty of a state is to safeguard its citizens**
- **One mechanism is to protect its borders**
- **A vital prerequisite is surely an assured identity**
- **‘I counted them all out and I counted them all back’**
- **The USA has a similar problem**



The Denial Syndrome

- **Good intentions to meet challenging political objectives invariably founder on the rock of practical implementation**
- **An assumption that existing processes, products and mechanisms meet the core requirements of identity management**
- **Integrity is rarely a requirement yet it is pivotal to public acceptance & success**



Process Integrity

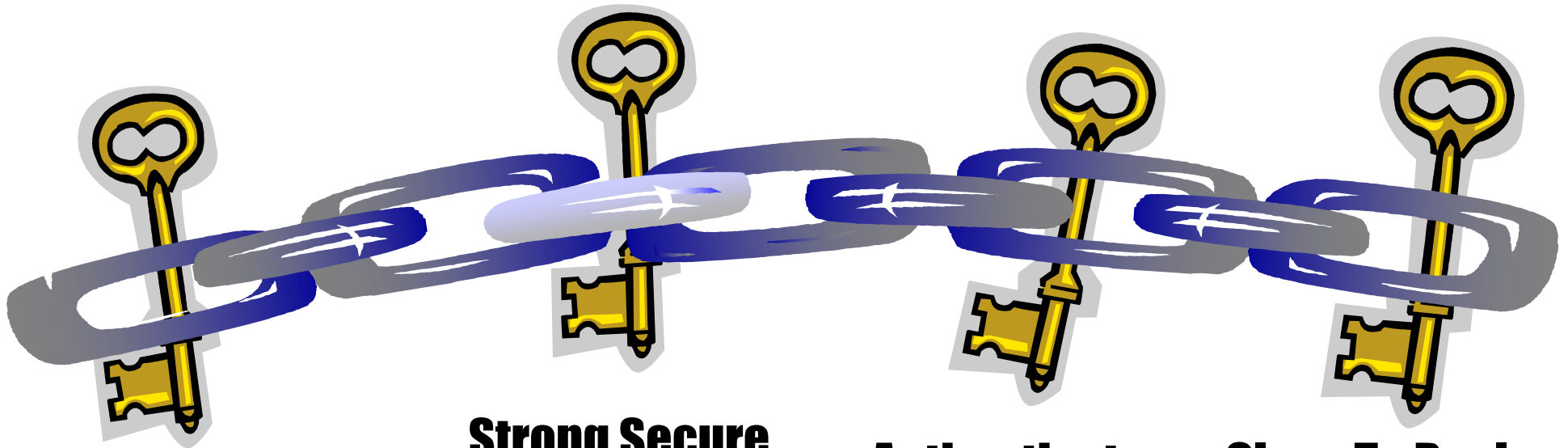
- **The whole is only as good as the sum of its parts (ie its weakest part)**
- **The law of unintended consequences can deliver a significant vulnerability**
- **Is the process and product appropriate for onward use and re-use within government under the shared services agenda ?**
- **Is the challenge of storing biographical and biometric data together understood?**



Why Identity Management?

- Identity impersonation is hardly new
- What makes Identity Management important today is the significance and impact of electronic transactions globally
- These assume ‘trust’ in identity attributes either self declared or awarded by ‘trusted’ organisations, commercial or government. **The chain of Trust**

The Chain of Trust



**Strong Identity
Proofing and Vetting**

**Strong Secure
Issuance Process**

**Authenticate
Authenticate
Authenticate
Every Time**

**Close To Real
Time Revocation**



Starting at the beginning

- **Establish your Identity**
 - This should be to an accepted, recognised level of assurance (beyond reasonable doubt).
 - This is sometimes easier stated than achieved, as standards of recorded documentation and evidence vary widely
- **Only then you can consider adding additional information (i.e. log the ‘biometric record’ of the individual)**
 - This can be used to link that recording with the “assured identity” to **bind** an electronic record of an identity



Attributes of Identity

- **Primary Identifying Documents**
 - Linking a person to an officially recognised and documented **event** (i.e. Birth Certificate etc.)
- **Secondary Identifying Documents**
 - Linking a person to a recorded **place** (i.e. local tax record or utility bill)
- **Identifying Characteristics**
 - **Biometric identifiers** (i.e. digital photograph, fingerprint, iris scan, DNA)



Primary Identity Documents

- These documents vary in style
- Historically completed in manuscript
- They contain errors in spelling or local styles
- They were produced on cheap paper
- They rarely required evidence of “fact” for issue
- They were never intended as “proof of identity”
- Yet they are accepted as “prima facie” evidence of identity that can be, and are, widely falsified, forged or simply obtained by misrepresentation.



Secondary Identity Documents

These vary even more

- The original processes and rules for issue of these secondary documents were never originally intended as “proof of identity”.
- They have been adopted as ‘de facto, proof of ID’ in the absence of other valid proof of ID.
 - Driving Licences
 - Passports
 - Utility Bills



ECA
alliance Through Security

Identity Fundamentals

- **Who do you claim to be?**
- **Whom do you wish to be known as?**
- **How do you prove it?**
- **There will be those who may genuinely not know or have the 'required documents'**
 - Third World Country
 - Parents were not married
 - Birth not registered or Birth Certificates not issued or ambivalent
 - May not know their age etc
 - May have lost or destroyed their documents
 - BUT they exist, are here, claim to be 'X' and are applying.....



What is Good Identity?

- Good isn't always best!
- What is the required standard?
- What is good enough?
- What are the levels of 'Assurance' that we can accept?
 - US PIV Standards (HSPD 12, Fips 201, PIV)
 - UK Biometric Visa, Residence Permit, Passport, ID Card, e-borders.....



Identity Theft

- Is it 'Theft' or 'Impersonation'?
- No common definition in the EU, nor a crime in many parts of the world
- It is misuse of personal data in order to impersonate another individual
- Intent to commit an illicit activity



Staff

- **Staff and process INTEGRITY** in Identity Management are paramount.
- Serious Identity Management demands competent, motivated, trustworthy staff, without whom the entire enterprise and its product is likely to be flawed
- This requires consideration of enhanced levels of pre-employment clearance and appropriate security vetting



Identity has a Value

- **This is well understood commercially, particularly by criminals (and terrorists)**
- **The underlying process that establishes, awards or accepts an identity credential is fundamental to integrity (passports and visas)**



People, Process and Technology

- **Over reliance on leading edge technology (ie biometrics)**
- **Are existing IT systems and security regimes up to the task?**
- **Integrity of the underlying process allied to staff integrity**
- **Outsourcing to local firms especially overseas brings its own challenges**



Criminals and 'Insiders' present significant challenges

- Identity attributes have a value and are targeted by criminals
- Serious, organised crime is well organised and funded
- There is a trade in identity information: (offshore call centres, government departments etc)
- Fraud and Theft cause significant financial loss and consequent restoration work
- And the reputational damage



Does Identity Management matter?

- Yes, of course it does!
- If your organisation has information worth protecting, somebody will try to steal, borrow or share that information.
- If identity attributes are used to authorise transactions of 'value' ie entry rights, those attributes have a value and will be targeted, suborned and misused.
- Unauthorised access, sharing or release of information may have serious implications.



The use of System generated Credential Checks

- Are Biographical Footprint Checks essential toolsets or do they give a false sense of security?
- Re examine the appropriateness of the original design intent (unthinking re use)
- If Credit Reference checks are used, remember that they are predicated on “ability to pay” and not on “assured identity”



In the end Its all a question of Risk Management & Balance Cost - Risk - Assurance



Photo courtesy of SpinSheet Magazine.



We have to commit to a proper process of Identity Management and stay the course

- It must be applied Holistically on:
 - Application and Enrolment
 - Maintenance
 - Biographical and Biometric handling
 - Authorisation for sharing
- This is new territory and we are all too trusting or assume existing process will do
- **Doing bits of it is delusional, a waste of time and money but with a potentially disastrous sting in the tail.**



**And in this business there are no
Absolutes.....**

QUESTIONS?



June 2007

© ECA Limited