



CPNI Conference
8th Feb. 2007

Identity and Civil Contingencies -

"When the balloon goes up,
will you know who's in it?"

Robin Wilton

Corporate Architect (Federated Identity)

Sun Microsystems

robin.wilton@sun.com

+44 705 005 2931

<http://blogs.sun.com/racingsnake>



Introduction

- The following slides describe a hypothetical scenario and some of the identity-management consequences which might flow from it.
- The first two 'headlines' reflect real BBC news reports.
- The rest are purely imaginary, and do not represent an intent to portray any of the hypothetical participants in an unfavourable light.

Jan. 2007: H5N1 outbreak in UK poultry farm. 160,000 birds culled.
No spread to humans.

Feb. 2007: Indonesia (with the highest H5N1 mortality) declines to
contribute virus material to the international medical community,
amid rumours that they may have done an 'exclusivity' deal with a
pharmaceutical company.

...

Feb. 200x: Further H5N1 outbreak in UK poultry farm. Infection
spreads to several hundred humans, of whom a percentage die.

June 200x: Prophylactic UK vaccination programme for infants,
elderly and 'at risk' categories (poultry workers, asthmatics...)

March 201x: NHS 'Single Patient Record' database populated and
online.

Sept. 201x: H5N1 aerosol released over three UK cities from light
aircraft; millions of humans infected, with proportionate death
rate. Indonesian Jemaah Islamiyah extremists implicated.

Sept. 201x: Emergency containment/quarantine area established.

Sept. 201x: At height of patient triage volumes, access controls to
SPR database lifted 'as one-time emergency response'

... ..

- 1 - Where are those patient records, when the access controls are reinstated?
- 2 - What signs might there be if a mass data compromise had taken place?
- 3 - What if that mass data compromise had actually been planned, as part of the aftermath of the H5N1 release?
- 4 - Suppose that, rather than Patient Records, the data in question had been NIR records (including biometrics)...
- 5 - Does this kind of potential risk suggest mitigations which ought to be designed in now?

Now let's look at what happened next in the aftermath of this hypothetical attack:

Oct.-Dec 201x: The 'flu-like nature of the epidemic results in massive demand for respiratory care, far exceeding the UK 'flu outbreaks of the mid-90s.

Private healthcare schemes decline treatment on the grounds that acts of terrorism are excluded from the terms of healthcare insurance.

As the epidemic outstrips the NHS' ability to cope, the Government gives in to massive pressure and issues vouchers for treatment under private sector schemes.

The over-stretched administrative system for these vouchers, coupled with the massive demand, make it easy to defraud.

Post-epidemic analysis suggests that up to 40% of claims were fraudulent, and that a high proportion of this fraud was organised.

Aim of this presentation

- To look at CNI and emergency response from the perspective of a self-confessed 'identity bigot';
 - To give some simple 'identity lifecycle' models;
 - To indicate some areas of systemic risk.
-
- It is *not* my aim to propose a definitive solution for all cases;
 - I do hope to set out some key strategy and design points.

Topics

- Identity lifecycle – elements, and possible points of failure
- Context, Opportunism, Malice: thinking about risk
- Policy issues: flexibility, roles and privacy

Topics

- Identity lifecycle – elements, and possible points of failure
- Context, Opportunism, Malice: thinking about risk
- Policy issues: flexibility, roles and privacy

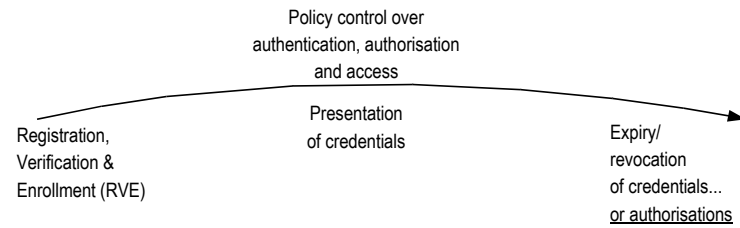
1 - What does Identity consist of?

- SAML implies a useful three-layer model for Identity Data:



- Assertions about Identity are, essentially, assertions that the person presenting *credentials* is the person to whom they were issued at a point in the past.
- This reveals an implicit 'chain of trust', which must be intact if we are to trust an identity assertion.
- Maintaining that 'chain of trust' under emergency conditions introduces some new challenges...

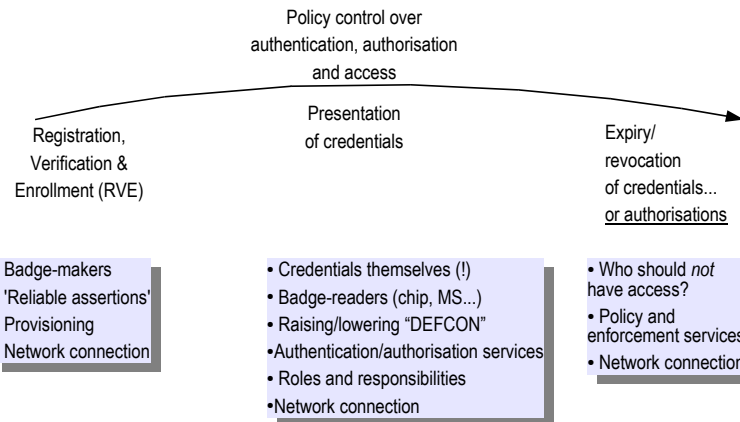
2 – Identity lifecycle and the 'Chain of Trust'



- RVE, credential verification, policy, authorisation, access control... all tend to use discrete components.
- These may be unavailable for a wide range of reasons.
- Does 'fallback security' have to mean 'worse security'?

© Copyright Sun Microsystems February 2007

2 (b)– Identity lifecycle and the 'Chain of Trust'



© Copyright Sun Microsystems February 2007

Topics

- Identity lifecycle – elements, and possible points of failure
- **Context, Opportunism, Malice: thinking about risk**
- Policy issues: flexibility, roles and privacy

Risk: Context, Opportunism, Malice

- Context: are you trying to keep people in, out, or both?
 - > For 'epidemic containment' how do you audit 'escapes' (in the likely absence of credentials...)?
- Opportunism: fallback security often creates openings for abuse. (Intentional disappearances, identity theft...)
 - > What forensic indicators might you look out for?
 - > What assets might you reclassify, given this risk analysis?
 - > One Katrina 'missing/found' BBS has over 28,000 posts, many of which include addresses, names of relatives, and so on.
- Malice: there is [credible evidence](#) that some terrorist organisations cash in on charity disaster donations.
 - > Again, what forensic indicators might there be if this is going on?
 - > It's not a huge leap from this to 'terror attacks as revenue generators'

As with any security measure, the vulnerability is often not along the primary axis of defence.

Topics

- Identity lifecycle – elements, and possible points of failure
- Context, Opportunism, Malice: thinking about risk
- Policy issues: flexibility, roles and privacy

Policy Issues – flexibility, roles and privacy

- Flexibility: can you cope with 'degraded' facilities?
 - > Balance of technology and process;
 - > 'Loose coupling' of policy and technology.
- Roles: 'first response' may have to be based on who is available, not what it says on their badge.
 - > 'Gold/silver/bronze' roles may cut across organisations and hierarchies.
- Privacy:
 - > It may be tempting, at a given point, to say: "Open the data up; we can clean it up later" (for instance, immunisation records);
 - > Disaster missing/found priorities often encourage PII disclosure.

There are good and bad times to be thinking through this kind of policy decision...



CPNI Conference
8th Feb. 2007

THANK YOU

Robin Wilton

Corporate Architect (Federated Identity)

Sun Microsystems

robin.wilton@sun.com

+44 705 005 2931

<http://blogs.sun.com/racingsnake>

