Lockstep *Stepwise*

Introduction to de-identification solution

Stephen Wilson
Lockstep Technologies Pty Ltd

Our numbers are under attack!

Good morning Madam. Can I start with your account number please?

Sure, it's 123456

OK, thanks for that.

Now …
What's your full name?
Your date of birth?
Your billing address?
The supplementary card holder?
Your mother's maiden name?
Your credit limit?
What's the CCV number?

Cost of data breach at TJX soars to $256m

The Boston Globe

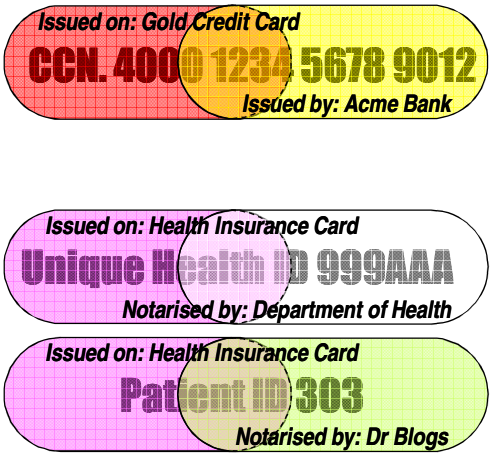
Suits, computer fix add to expenses

By Ross Kerber, Globe Staff | August 15, 2007

TJX Cos. said its costs from the largest computer data breach in corporate history, in which thieves stole more than 45 million customer credit and debit card numbers, have ballooned to $256 million.

The more personal details we divulge to prove our identity, the greater the leakage, and the risk gets worse!

Safety in numbers!



Normally, when a digital identity is quoted on its own, nobody can tell if it's real, or stolen and replayed, or simply made up.

Stepwise encapsulates digital identities – like credit card numbers, health IDs, or any customer reference number – with a two-fold "pedigree". Firstly, *Stepwise* shows who issued the ID in the first place, to prove its bona fides.

Secondly, *Stepwise* names the particular type of personal security device on which the identity has been carried, and thus safeguarded against theft or replay.

If desired, multiple digital identities can be loaded to the one card and have their pedigree similarly assured. For instance, a health smartcard can carry a national unique identifier, and a separate local ID issued by a doctor or service provider. *Stepwise* IDs are exercised independently and verified by receivers locally without any central identity 'broker'. The unique decentralised architecture of *Stepwise* protectsIDs from being linked.

Benefits of Stepwise

In e-government and healthcare:

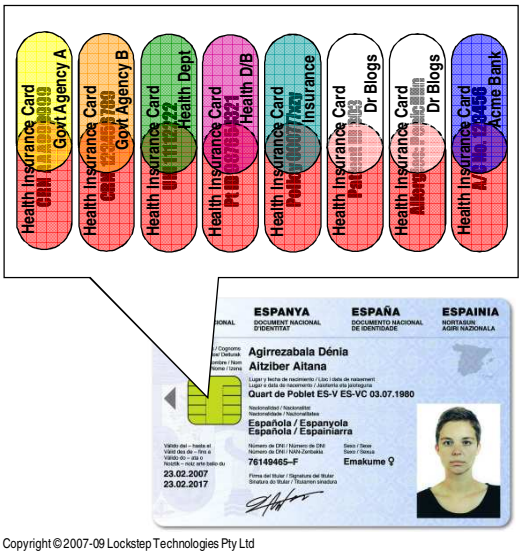
- Dramatically enhances privacy and reduces ID theft
- Eliminates the major political risks associated with privacy fears; transforms ID cards into friends of the citizen, not agents of government
- Creates a potent strategic weapon against identity crime; demonstrates government leadership
- Increases confidence in government online
- Increases smartcard utility with e.g. health identifiers, proof-of-age etc.
- Brings new revenue potential through commercial applications enabled by privacy architecture; enhances ROI on smartcards
- Transparent, decentralised, uncomplicated security model, readily verifiable, and attractive to diverse stakeholders.

Benefits of Stepwise

In e-commerce and payments:

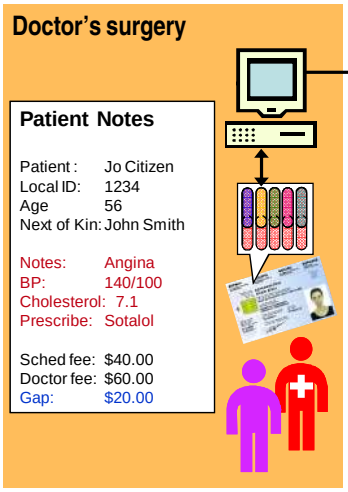
- Vastly improved customer experience: *simpler, faster, ATM-like*
- Greatly reduced risk of Card Not Present payments fraud
- Increased confidence in shopping online
- Radically better privacy protection, reduced disclosure of extraneous personal details; reduced incentive for identity theft
- For e-merchants – better compliance with PCI obligations, lower cost
- For banks – enhanced ROI on Chip-and-PIN (EMV) cards
- For e-merchants & banks – simpler, lower cost implementation; less reliance on centralised authentication servers.

Multiple *Stepwise* capsules



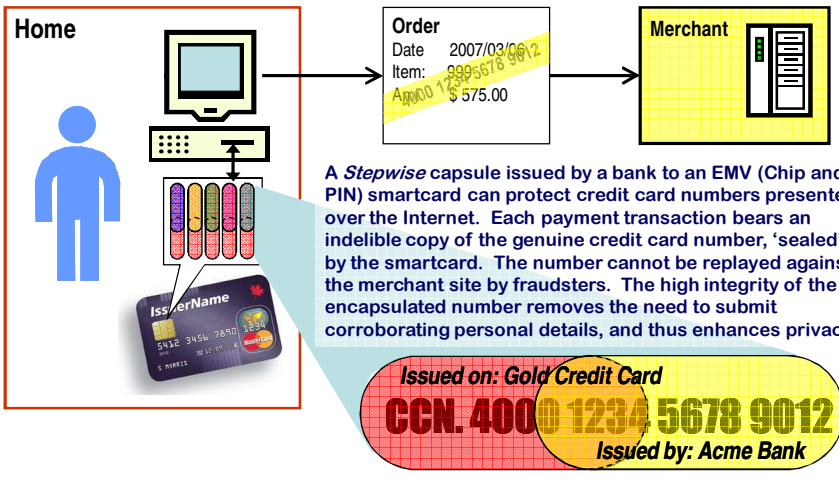
- **Identifiers and personal data encapsulated by *Stepwise* cannot be cloned, faked, or copied**
- **every capsule bears a tamper-proof pedigree, proving its identity data is authentic, was carried in an authentic device, and was presented with the consent of the cardholder**
- **encapsulated data can be verified offline, without the need for central ID brokers**
- **additional capsules can be added at anytime, memory allowing.**

Transaction de-identification



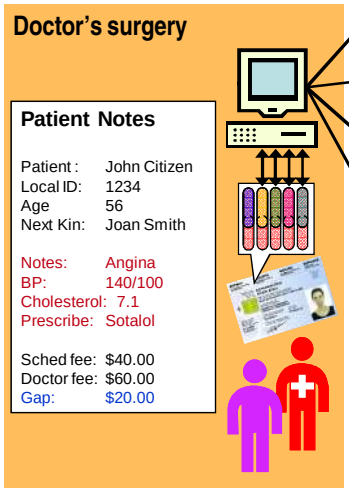
Stepwise capsules are bound to transactions through standard digital signatures. Each transaction is "sealed" with the appropriate capsule, indelibly binding to it the corresponding identity data. Each transaction bears the minimum ID data needed to authorise it, with no extraneous personal details. The contents of each capsule are "baked in"; i.e. digitally signed by the issuer. The capsule's integrity can be verified by the receiver quickly and simply, offline, using standard cryptographic library functions built into almost all server platforms today.

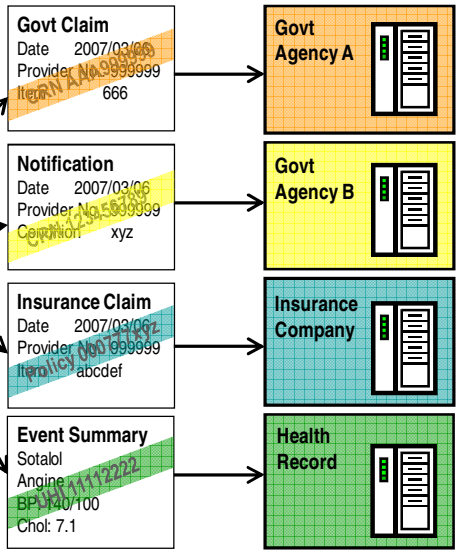
Solving Card Not Present fraud



A *Stepwise* capsule issued by a bank to an EMV (Chip and PIN) smartcard can protect credit card numbers presented over the Internet. Each payment transaction bears an indelible copy of the genuine credit card number, 'sealed' by the smartcard. The number cannot be replayed against the merchant site by fraudsters. The high integrity of the encapsulated number removes the need to submit corroborating personal details, and thus enhances privacy.

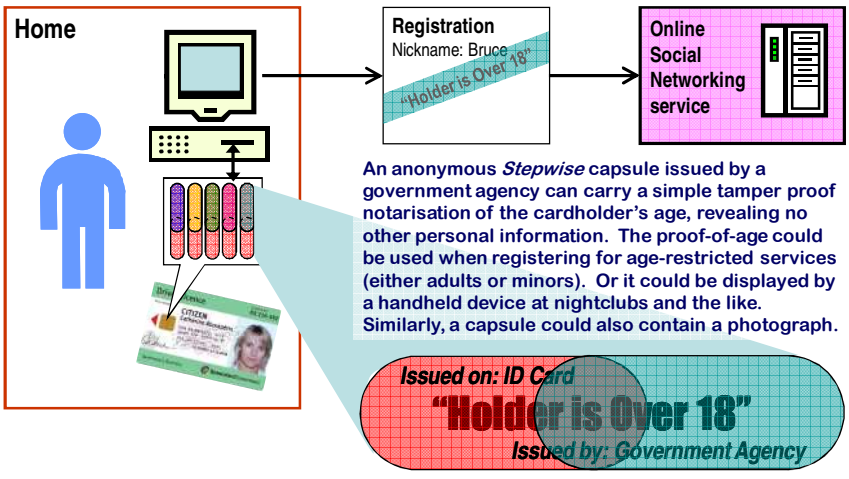
"De-linking"





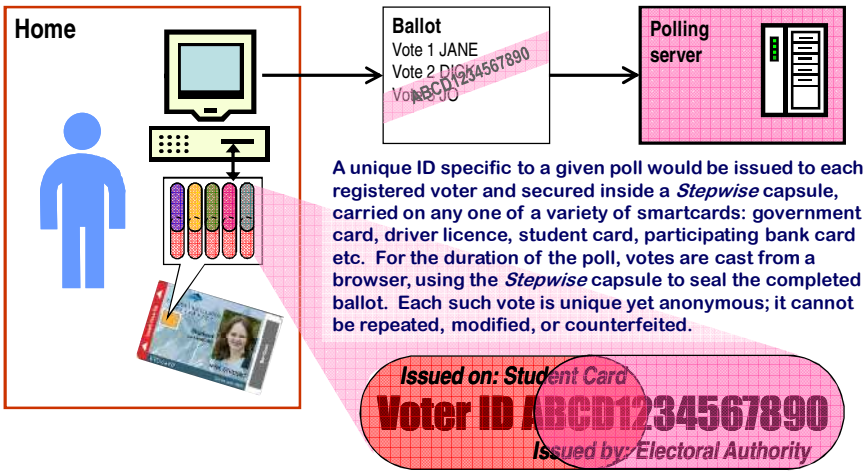
Stepwise secured transactions cannot be cross linked. Each uses a different digital ID or customer reference number, specific to the transaction context. The seals can be verified without a central ID broker. There is no leakage of personal data between transactions or receivers.

Anonymous Proof of Age



An anonymous *Stepwise* capsule issued by a government agency can carry a simple tamper proof notarisation of the cardholder's age, revealing no other personal information. The proof-of-age could be used when registering for age-restricted services (either adults or minors). Or it could be displayed by a handheld device at nightclubs and the like. Similarly, a capsule could also contain a photograph.

Anonymous Internet voting



Under the covers

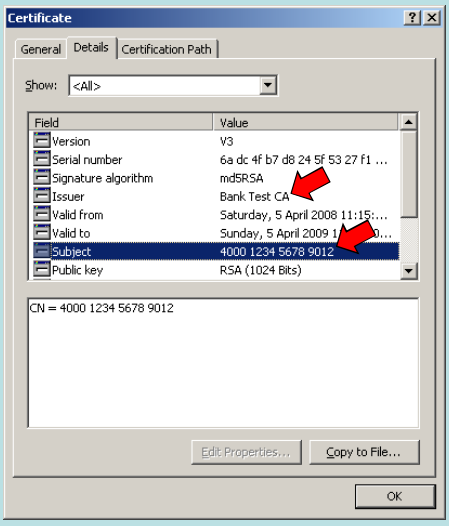
How Stepwise capsules are created using anonymous digital certificates

Technically, the three way binding of a card holder, a piece of personal data, and the issuer or notary of that data, is achieved using anonymous digital certificates. In the example, a bank has issued one of its customer with a digital certificate that identifies only their credit card number *4000 1234 5678 9012*. The Public Key in the certificate is associated with a unique Private Key generated and stored within the customer's EMV smartcard. The certificate is signed by the bank, which will only issue this type of certificates to known customers holding current credit cards.

Thus it is impossible to clone or counterfeit a ***Stepwise*** certificate – because each of them is linked to a different private key secreted inside a smartcard – or to substitute the name of another issuer or notary of the data – because each certificate is digitally signed.

A conventional digital identity certificate will contain a complex "distinguished name" for the Subject, including their full name, nickname, e-mail address, organisation affiliations and so on. The ***Stepwise*** certificate on the other hand holds only a pseudonym, such as the credit card number, or any other Customer Reference Number, identifier, biometric template, or personal data.

Note that the *Certification Path* can be used to create a chain of command from the issuer back to the peak scheme owner, adding an additional level of "branding" to each capsule. For example, the certificate issuer used to create Dr Blogs' medic alerts could itself be signed by DHS, for added security against unauthorised issuers of data to Access Cards.



Stephen Wilson
Lockstep Technologies
swilson@lockstep.com.au
www.lockstep.com.au/technologies