Stepwise – safety in numbers

With Lockstep's award winning Stepwise, you can take better care of your numbers

Lockstep Technologies' ***Stepwise*** radically enhances privacy, security and safety for consumers transacting on the Internet. ***Stepwise*** uses smartcards to de-identify highly sensitive transactions, such as e-health record entries, welfare entitlements and payments instructions, e-voting and so on.

Our numbers are under attack!

We all live and work by our numbers. Account numbers, personal identifiers, policy IDs, licence and membership numbers are all part and parcel of today's world. Each number succinctly represents our status in a community of interest, or our relationship with a service provider.

When we look closely at identity fraud, the fundamental problem is that our numbers are simply too easy to copy! Account IDs and driver license numbers are quoted and copied so often that on their own, they're no longer sufficient to establish a customer's bona fides. And so we have to play 'twenty questions' with call centre operators because they cannot trust a number on its own.

There's a cyber-crime arms race, and customer safety and convenience are losing. Transactions involve more and more layers of secrets, like the CCV numbers printed on our credit cards. They buy us a little more security for a little while longer – until we're tricked into typing the CCV into a fake website, or a corrupt call-centre operator sells off the CCVs of a thousand customers.

The Lockstep solution

Stepwise encapsulates customer reference numbers, identifiers, biometric templates or any other personal ID data, and seals them crypto-graphically into a smartcard. It isolates each identifier, removes all extraneous personal detail and linkages, and puts all identifiers back under the sole control of the consumer. ***Stepwise*** ensures that when any identifier is presented online, we know that it's legitimate, it comes from a genuine smartcard, and that it's been used with consent. ***Stepwise*** makes customer numbers trustworthy again and thereby stems the leakage of personal information.

Stepwise benefits

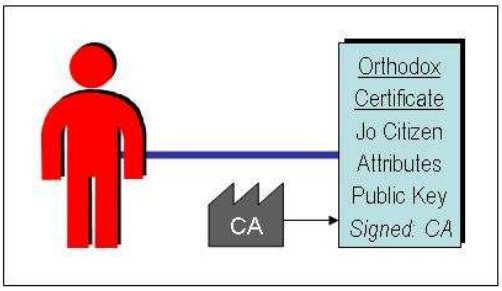
- ***Stepwise*** identifiers cannot be cloned, counterfeited, or illicitly copied from one smartcard to another
- transactions originating from a ***Stepwise*** smartcard are sealed with their respective identifiers, contain the bare minimum personal information, and cannot be cross-linked with each other
- every transaction bears a tamper-proof pedigree, proving it originated from an authentic smartcard carrying a bona fide identifier, used with the consent of the cardholder.

Stepwise – how it works

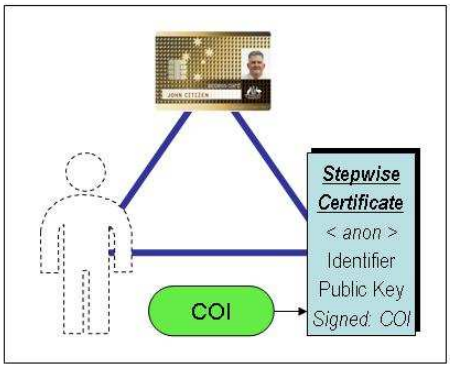
It is well known that smartcards can store multiple personal identifiers in different "containers" or memory "slots". But the conventional approach of treating identifiers as data means that outside the smartcard, they revert to being ordinary numbers, vulnerable to cloning and counterfeiting.

The *Stepwise* innovation

Stepwise applies digital certificates in a brand new way. An orthodox digital certificate is a signed declaration by a Certification Authority (CA) that a named individual, together with certain attributes, is associated with a cryptographic key. The logic was, if you trusted the CA then you trusted the association. But there was no intrinsic privacy in this arrangement, and with most CAs being new start-up businesses, trust was problematic.



Lockstep Technologies' breakthrough has been to insert into the relationship a tamper resistant key store such as a smartcard, allowing the declaration to be de-identified. ***Stepwise*** involves an anonymous but otherwise standard digital certificate, issued to a smartcard by or on behalf of a trusted community of interest (COI) such as a bank, a health body, a licensing authority or a government agency. The ***Stepwise*** certificate declares that *someone* with certain attributes such as an identifier is associated with a public key carried on a smartcard, without revealing who that someone is. The individual remains anonymous to all third parties, unless and until they present their smartcard.



Stepwise thereby triangulates three trusted processes:

1. the issuance of physical cards to singular individuals
2. the assignment of unique reference numbers to known customers, and
3. the binding of digital certificates to keys held on smartcards.

When a transaction is digitally signed using a ***Stepwise*** certificate, the transaction data is indelibly bound to the ***Stepwise*** identifier but contains no other identifying information.

Lockstep intellectual property

Stepwise is protected by Australian patents PCT/AU2005/000364 and PCT/AU2005/000522. Patents are pending in Europe and the USA.

Stepwise system requirements

- Multi-programmable smartcard with cryptographic processing
- EEPROM 64K or higher
- On-chip key generation
- RSA or DSA 1024 bits or higher
- PKCS#10 certificate request interface (or equivalent).