



Stepwise – safety in numbers

With Lockstep's award winning Stepwise, you take better care of your online identifiers

Lockstep Technologies' Stepwise radically enhances privacy and security for consumers on the Internet. Stepwise uses smartcards and similar personal security devices to de-identify sensitive transactions, such as credit card payments, e-health record entries, government services, and online social networking. Stepwise prevents ID theft, increases convenience and speed, and enhances privacy by dispensing with extraneous personal details.

Our numbers are under attack!

We all live and work by our numbers. Credit cards, account numbers, personal identifiers, policy IDs, licence and membership numbers are all part and parcel of today's world. Each number succinctly represents our standing in a community of interest, or our business 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 any number alone.

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 the backs of our credit cards. They bought us a little more security for a little while longer but now organised cyber criminals buy and sell CCVs in the millions, along with other personal details of credit card holders.

The Lockstep solution

Stepwise encapsulates customer reference numbers, identifiers, biometrics or any other personal ID, and seals them cryptographically into a chip. It might be a smartcard or a SIM, or it can be a dedicated USB key.

Each identifier is isolated, stripped of all extraneous personal detail and linkages, and placed under the sole control of its owner. *Stepwise* ensures that when any identifier is presented online, the receiver knows that it's legitimate, it came from a genuine security device, and that it was used with consent. *Stepwise* makes customer numbers trustworthy again and in the process, can stem the leakage of personal information.

Stepwise benefits

- *Stepwise* identifiers cannot be cloned, counterfeited, or illicitly copied
- each transaction originating from a *Stepwise* enabled chip is sealed with its respective identifier, contains the bare minimum personal information, and cannot be cross-linked with other transactions
- every *Stepwise* 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 for Card Not Present payments

One of the most pressing problems in Internet security today is Card Not Present (CNP) fraud. Now the most common type of payment card fraud, CNP fraud for FY08 totalled AU\$63M in Australia and exceeded £320m in the UK.

Now *Stepwise* offers a quantum jump in CNP security, by providing merchants the means to trust credit card details presented online. *Stepwise* can be integrated with the credit card associations' *3D Secure* protocol, or deployed standalone, to dramatically cut fraud and create a more user friendly EFTPOS-like experience in the customer's browser. At the same time, *Stepwise* protects consumer privacy, dramatically streamlines payment processing, and reduces merchant risks in safeguarding cardholder data.



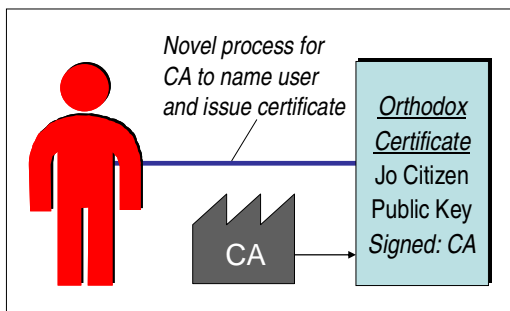


Stepwise – how it works

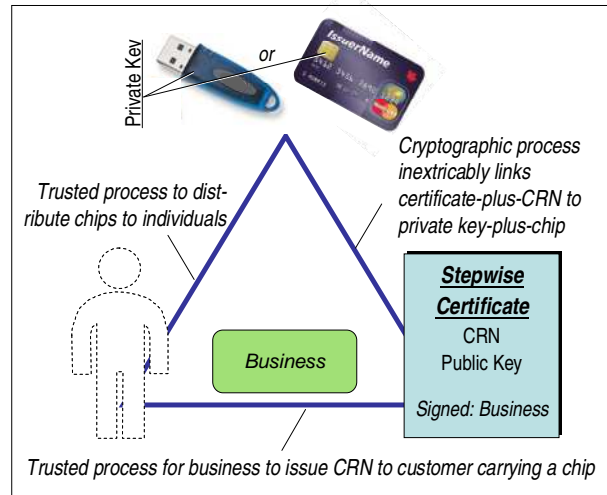
It is well known that smartcards can store multiple personal identifiers in different “containers” or memory “slots”. But the conventional approach means that outside the smartcard, identifiers revert to being ordinary numbers, and become vulnerable to theft, replay attack, and counterfeiting.

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 a standard digital certificate, issued to a chip held by the user and signed by a business with whom the user has a trusted relationship, such as a bank, a health body, a licensing authority or a government agency. The Stepwise certificate declares that *someone* with a certain identifier is associated with a public key carried on a particular chip device, without revealing who that someone is. The individual remains anonymous to all third parties, unless and until they present their chip.



Stepwise thereby triangulates three trusted processes:

1. the issuance of chips to individuals
2. the assignment of customer reference numbers to known customers, and
3. the binding of digital certificates to keys held on chips.

When a transaction is digitally signed using a Stepwise certificate, the transaction data is indelibly bound to the Stepwise encapsulated 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 chip (e.g. smartcard, USB key or 2.5G SIM) with cryptographic co-processor
- EEPROM 64K or higher
- RSA or DSA 1024+ bits with on chip key gen
- PKCS#10 certificate request interface or equivalent.

