The Stepwise CNP fraud solution: Technical details

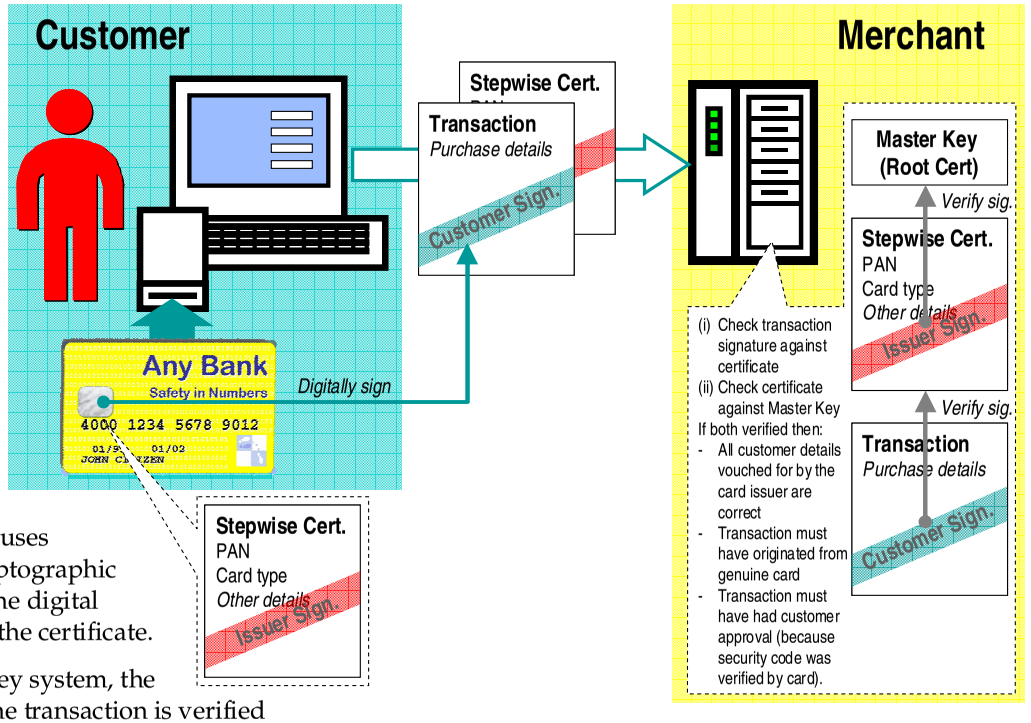
Lockstep Technical Note 2 explains that *Stepwise* uses a "capsule" that contains cardholder details and identifies the issuer, and which is loaded onto a smartcard. The capsule is in fact a standard digital certificate customised to carry all pertinent details about the cardholder account needed by a merchant to authenticate a card transaction. These details will generally be the PAN plus perhaps the expiry date, the card type and so on. *Stepwise* certificates can be configured to contain different details as befits the payment scheme in which they are deployed.

The *Stepwise* certificate is digitally signed by the issuer, and corresponds to a private key held securely inside the smart chip. Ideally, *Stepwise* enabled smartcards will have onboard cryptographic processing to create digital signatures internally. Thus, any digital signature that is verified as corresponding to a given *Stepwise* certificate must have been generated by the indicated smartcard, because there will be no other way to invoke the matching private key.

Transactions are 'sealed' with customer details by way of a digital signature, created in the smartcard under command from the merchant server, which communicates through the browser over XMLsignatures and Microsoft CAPI or the like. A simple Java or similar web page control is used to create the security code prompt.

With reference to the diagram, *Stepwise* operates as follows (note that the same core functionality applies whether *Stepwise* is implemented standalone, or integrated with 3D Secure):

1. The customer creates a transaction, is prompted for their security code, and the chip generates a digital signature.
2. The transaction plus signature code are sent from the browser to the merchant server, along with a copy of the *Stepwise* certificate.
3. The merchant server uses standard built-in cryptographic modules to process the digital signature and verify the certificate.
4. As with any public key system, the user's signature on the transaction is verified against the user's certificate as signed by a bank, and the bank's signature on the certificate is verified against a "master key" (Root Certificate) loaded in the server.
5. If the transaction digital signature and the *Stepwise* certificate are verified, then the merchant is assured:
   - — that all details in the *Stepwise* certificate avowed by the issuing bank are correct for the cardholder
   - — that the transaction must have originated from a genuine bank-issued smartcard, because the unique private key that matches the certificate is held secure within the smartcard, and
   - — that the customer must have consented to the transaction by entering the correct security code to cause the smartcard to create the signature.



Thus it is not feasible for an attacker to falsify the transaction, nor steal and replay a customer's details, because their smartcard is necessary to create the signature.

What happens next depends on how *Stepwise* is implemented. If standalone, the merchant passes to the acquiring bank as per orthodox CNP processing. If *Stepwise* is integrated into 3D Secure, the Merchant Plug-in can copy the signature to the Issuer via the PAReq message, relieving them from extra user authentication.

"Safety in Numbers"

www.lockstep.com.au/technologies