Conveying the pedigree of identifiers using digital certificates

The problem of identity takeover

The root cause of much identity theft and fraud today is the unfortunate fact that customer reference numbers and personal identifiers are so easy to copy. Simple numerical data like bank account numbers can be stolen from many different sources, and replayed in bogus transactions. In some cases, identifiers like credit card numbers can be simply made up, without merchants being readily able to tell the difference.

Our personal data nowadays is leaking more or less constantly, through websites, online forms, call centres and so on, to such an extent that customer reference numbers on their own are no longer trustworthy. Privacy then suffers badly when customers need to assert their identity by supplementing their numbers with personal details, like name and address, birthdates, mother's maiden name and other pseudo secrets.

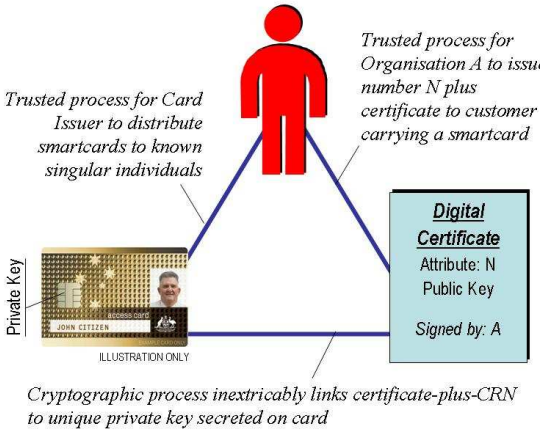
To restore trust in personal identifiers, we need to know their *pedigree*. We need to know when a number is presented that it is genuine, that it originated from a trusted authority, it's been stored safely in the meanwhile, and it has been presented with the owner's consent.

"Notarising" personal data in smartcards

There are ways of issuing personal data to a smartcard that prevent those data from being 'claimed' by anyone else, copied from one card to another, or simply made up.

One way to do so is to encapsulate and notarise personal data in a unique digital certificate issued to a smartcard. Consider an individual named Smith to whom Organisation A has issued a unique customer reference number N. If N is saved in ordinary memory in a smartcard or any other portable device, then it has no pedigree – once N is presented by the cardholder in a transaction, it looks like any other number. To better safeguard N in a smartcard, it can be sealed into a digital certificate, as follows:

1. generate a fresh private-public key pair inside Smith's smartcard
2. export the public key
3. create a digital certificate around the public key, with an attribute corresponding to N
4. have the certificate signed by (or on behalf of) A.



The result is a logical triangle that inextricably binds cardholder Smith to their reference number N and to a specific smartcard. The certificate signed by A attests to Smith's ownership of both N and a particular key unique to Smith's smartcard. Keys generated inside a smartcard are retained internally, never divulged to outsiders. It is impossible to copy the private key to another card, so the triangle cannot be cloned, reproduced or counterfeited.

Restoring privacy and consumer control

When Smith wants to present their personal number in an electronic transaction, instead of simply copying N out of memory (at which point it would lose its pedigree), Smith's software would digitally sign the transaction using the certificate containing N. With standard security software, any third party can then verify that the transaction originated from a genuine smartcard holding the unique key certified by A as matching the number N.

Note that N doesn't have to be a customer number or numeric identifier; it could be any personal data, including a biometric template or a package of medical information.