Smartcard transaction privacy

An overview of Lockstep Technologies anonymity R&D

Health & welfare smartcard projects (like the DHS Access Card proposal) aim to control and streamline a range of information flows and transactions using a single card. To protect privacy, we should avoid unnecessary linkages and the swapping of personal data between otherwise unrelated institutions. In particular, financial institutions should not have access to health information or identifiers, and governments should not have sensitive third party transactions pass through their systems.

Lockstep Technologies R&D has led to a unique de-identification solution for smartcards, which could decentralise personal identifiers, account details and so on, and leverage security functions available in many smartcard platforms to quarantine the information flowing to government agencies, banks, healthcare providers and so on. An innovative new type of anonymous certificate can provide receivers of de-identified messages with high levels of assurance that the sender was properly credentialed by a trusted authority, and was using a genuine smartcard of a known type.

Overview

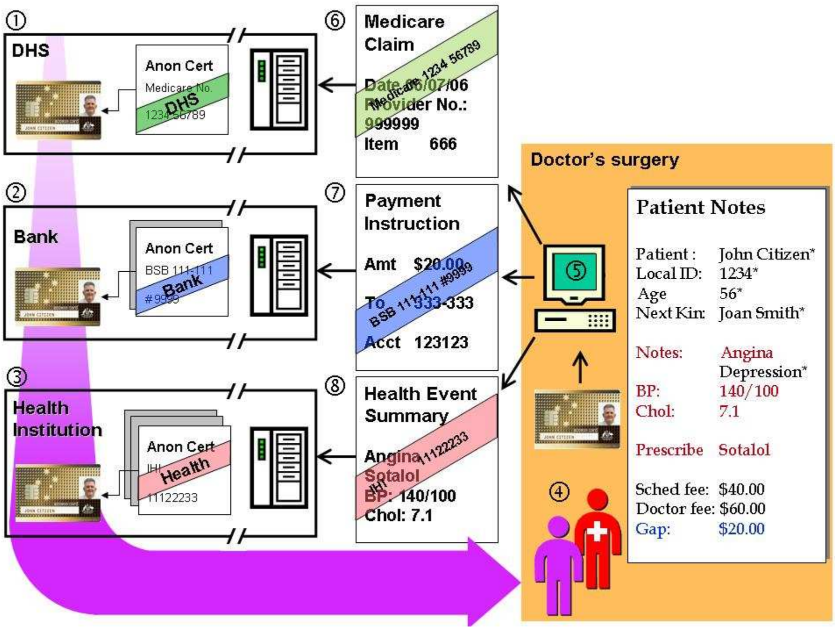
Individuals in the health & welfare environment tend to deal with a number of separate service providers. A typical consumer will have a Medicare number, a health insurance policy, at least one bank account, and may also be known to one or more additional human services agencies. In the near future, many individuals will be issued with a unique health identifier, to help manage electronic health records. Traditionally, each service provider will know an individual according to a unique identifier, account number or the like. Crucial for privacy is the principle that identifiers not be re-used across disparate systems; in fact Australian privacy law expressly forbids the re-use of government identifiers.

Modern secure smartcards can store and manage multiple digital credentials. As plain numbers, it is straightforward for a smartcard to hold different identifiers in different secure "slots". However, for these numbers to be used and trusted in electronic transactions, we must guard against them being manipulated, counterfeited, copied from one card to another, or simply made up. When an identifier is 'quoted' online by a consumer – or by a healthcare professional acting on the consumer's behalf – it is critical to know that the identifier is genuine, current, and is being quoted from a secure medium like a smartcard.

Lockstep Technologies research into these challenges has identified a novel approach, made feasible by security features built in to most modern smartcard platforms. For each service provider that an individual deals with, we would create under carefully controlled circumstances, an anonymous credential which holds their identifier and nothing else. When personal information is exchanged with a particular system, the smartcard is used to "seal" the information together with the credential relevant to the system. Thus, the bare minimum of personal information is transmitted, and the opportunities for unauthorised cross-matching greatly reduced. In greenfields, such as electronic health records and the new Individual Health Identifier, transactions sealed using these anonymous certificates could be totally anonymous.

A workflow scenario

The diagram below illustrates how anonymous banking, Medicare and health records details could be managed using a single smartcard, so as to 'firewall' transactions carried out with different service providers. *The Access Card is used for illustration only.*



An Access Card when first issued could come with one's Medicare number already installed, held inside an anonymous certificate 'sealed' by DHS (step 1). At any later time, and at the card holder's discretion, the Access Card could be topped up with banking details and/or health identifiers, each sealed in their respective anonymous certificates (steps 2 & 3). Other possibilities – such as health insurance numbers, other human services identifiers, and state government or private sector health identifiers – are not shown.

Now consider a typical visit to the consumer's doctor. The doctor's information system routinely generates a record of each patient encounter, including such data as clinical signs and test results, prescribed drugs, the Medicare code for the type of service delivered, the scheduled fee (to be reimbursed by Medicare), and whatever additional gap fee the doctor will charge the patient for the appointment. The doctor's system also holds local administrative data, including their own government-issued Healthcare Provider Number and their banking details.

Increasingly, e-health systems generate multiple online transactions between doctors and diverse service providers, where subsets of the local patient record are extracted and sent outside the doctor's local system. Lockstep Technologies can help de-identify these transactions, 'firewall' them from one another to reduce linkages, and provide strong assurance to receivers of the pedigree of all sensitive data being sent.

In the scenario illustrated above, at the conclusion of the visit, the doctor asks the patient if they'd like these transactions to be launched on their behalf. By handing over their Access Card, the patient consents to having a Medicare claim, a payment instruction and a health event summary each created, sealed and sent out for processing. Note that the highly sensitive personal data marked with an asterisk in the figure is not sent outside the doctor's environment.

Receivers can be sure that the identifiers quoted are genuine, that they were issued by the correct trusted authorities, and that a bona fide Access card was used. Furthermore, they can be assured that while a number of identifiers are being exercised by the one smartcard, none of the various service providers can access identifiable information from any other system or transaction stream.

Benefits of Lockstep Technologies

— Messages sealed with the smartcard contain the bare minimum personal information as required by the receiver; messages are not inter-linked by common identifiers.

— For greenfield deployments (such as Australia's planned Individual Health Identifier scheme), total anonymity is possible.

— Anonymous messages sealed with the smartcard cannot be re-identified without the card and therefore with the cardholder's express consent.

— The combination of on-chip key generation and trusted registration processes mean that the presence of a Lockstep certificate proves the bona fides of the smartcard and of the user. The certificate can also indicate the type of EOI process and thus the trust level of the user without revealing their identity.

— **Thus, each and every message sealed in this way bears a tamper-proof chain-of-trust, assuring receivers of its "pedigree": each message must have originated from an authentic smartcard, topped up with the user's consent, with a legitimate identifier from a legitimate issuer.**

— Identifiers sealed within Lockstep credentials by keys generated in the smartcard, cannot be cloned, counterfeited, or copied from one card to another. Unauthorised creation and loading of identifiers into spare memory in a smartcard is prevented.