An electronic "Medic Alert" model using smartcards

Digital certificates are an ideal means for encapsulating packages of personal data, including emergency medical data, so as to convey their pedigree and integrity (see Babystep 11). This paper builds on that idea to show in some detail how medical information could be managed in ways that very closely reflect the trusted Medic Alert process. A cornerstone of Medic Alert is a form specifying the clinical conditions of interest, which is completed by the patient's doctor – who must be a registered medical professional – and signed by both the doctor and the patient.

In an electronic scheme, standard clinical software as commonly used in general practice would be enabled to interface with a smartcard in the possession of (or issued to) the patient, as well as a PKI-enabled professional smartcard (such as the Medicare Australian "HeSA" card). A new screen would be added to the software for the task of creating what we will call here an "Emergency Health Record" (Record) and loading it to the patient card, as follows:

1. The Record would comprise the same sorts of data currently catered for by Medic Alert, known by the doctor about their patient. The software screen would likely provide pull down menus of common options, such as allergies, to help construct the Record. Other data such as current medications would be imported automatically from the local database. Once assembled, the doctor and the patient would review the Record, discuss the implications of loading it to the patient's smartcard, and agree to do so. The patient's formal consent would be recorded (and perhaps sealed using keys in their chip).
2. After the contents of the Record have been signed off, the actual data that will comprise the Record as stored in the chip would be formatted by software, to comply with relevant standards (e.g. SNOMED, HL7 etc.).
3. To securely bind the Record to the patient smartcard, the software would create a special digital certificate, where the Record is included as a custom attribute, as follows:
   i. the software instructs the patient smartcard to generate a fresh public-private key pair (an action which would likely require patient PIN entry, to signify consent)
   ii. the public key is exported from the smartcard to the application
   iii. a certificate is generated, including the patient's public key and the Record data
   iv. the certificate is signed by the doctor's HeSA private key or some other key[1] under the doctor's control, and
   v. the certificate is loaded to the patient card.

In effect, this special certificate has the doctor to digitally notarise the Emergency Health Record.

Benefits of the electronic Medic Alert

Anyone retrieving such an Emergency Health Record from an individual's smartcard can be assured that the Record:

- was created (and notarised) by an authorised medical doctor
- was created with the cardholder's consent
- had been carried on a genuine smartcard of a type approved by the Medic Alert scheme
- cannot have been tampered with after being notarised by the doctor
- cannot have been copied from another card, or otherwise made up.

The integrity and authenticity of emergency health information sealed within a digital certificate can be verified anytime offline in a wide variety of settings, *with no need to revert to a central smartcard management system*. While the patient's PIN would probably be necessary to create the Record initially, no PIN would be needed to retrieve it. Privacy could be enhanced if the smartcard were to only reveal the Record to specially authorised readers.

[1] Using the HeSA private key would be elegant, but using a different scheme-specific key might better convey the doctor's specific authorisation under Medic Alert. These details are unimportant.