Integrating Biometric Techniques with an Electronic Signature for Remote Authentication

by Luca Bechelli, Stefano Bistarelli, Fabio Martinelli, Marinella Petrocchi and Anna Vaccarelli

Biometric technologies are currently used for physical access controls. Scientists at CNR aim to integrate this technology with certificates, signatures and smartcards to handle remote authentication.

A project is currently under way at IIT-CNR, in collaboration with two industrial partners, which aims at the integration of biometric devices with digital signature technology (in conformity with current Italian standards). The results of the activity are being tested periodically by other CNR Institutes interested in this technology. The main objective of the project is the definition of standards that guarantee:

- confidentiality of non-public information
- authentication of the entities involved in the protocol (smartcard, biometric device and the user)
- integrity of the messages.

All these steps will be necessary to guarantee non-repudiation between authenticated users.

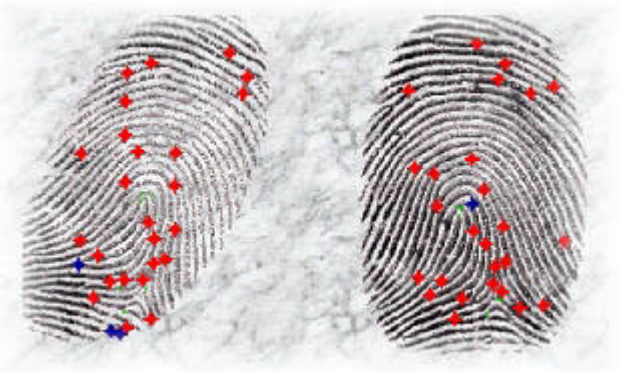
User authentication with biometric techniques does not require 'knowledge' of a secret piece of information, such as the traditional PIN, but requests that the user performs specific 'actions', necessary for a live acquisition of public biometric information.

This is why biometric techniques are used today for physical access controls or for other activities that require the presence of the user. The effective presence of the user during authentication guarantees that the biometric information is not intercepted, stolen or improperly used. Our aim is to perform remote authentication (eg logon to a remote system or unlock of a smart card to sign a document) and to guarantee the presence of the user by using special communication protocols between the biometric device and the smartcard.

The main problems with the use of biometric techniques are:

- the need to ensure that the only way to authenticate the user is the 'action' and not the 'knowledge' of the biometric information
- the association between biometric information and user identity has to be certified.

If these two constraints are not realised, a malicious user could use his own biometric details together with a third party identity (responsibility attack), or attach his identity to third party biometric information (credit attack).



A fingerprint template.

In our work, the biometric information is represented by a fingerprint. During the enrolment phase, a fingerprint template of the user is stored in a secure environment (in our solution inside the smartcard). For integrity and authenticity purposes, the (hashed) fingerprint is then inserted in an 'attribute certificate' signed by an Attribute Authority. In the same smartcard we also store an X.509 certificate of the user, which will be used to digitally sign documents.
In order to validate the fingerprint-identity pair, two important pieces of information are added to the attribute certificate:

- the serial number of the smartcard (in this way the fingerprint can only be used with that smartcard)
- the serial number of the X.509 user digital certificate (in this way, the fingerprint can only be used together with its owner).

This type of solution guarantees:

- that the user can perform classical authentication (with a secret PIN) and use only his X.509 certificate
- the possibility of biometric authentication, and the use of the X.509 certificate for remote authentication and digital signature
- the possibility of only handling the biometric information locally and privately.

In conclusion, biometric techniques work well if the verifier can check two things:

- that the biometric information was supplied at the time of verification (livescan)
- that the biometric information matches the template on file.

If the system cannot do this, then it fails. In fact, biometrics data provide unique identifiers, but are not secret.

We intend to implement the specification described above using the hardware and software products of our industrial partners with template-on-card technologies.

We plan to extend the implementation employing Match-On-Card (where the extraction of the certificate is performed on the card and the match on the system) and System-On-Card technologies (where match, extraction and storage of the template are performed inside the card).

This work has been carried out within a scientific cooperation between IIT-CNR and BiometriKa, an Italian company.

Link:

http://www.iat.cnr.it/attivita/progetti/progetti.html

Please contact:

Stefano Bistarelli, IIT-CNR

Tel: +39 050 315 3438

E-mail: stefano.bistarelli@iit.cnr.it