# Critical Information Systems Authentication Based on PKC and Biometrics

Carlos Costa, José Luís Oliveira, and Augusto Silva

DET/IEETA, Aveiro University, 3810-193 Aveiro, Portugal
ccosta@ieeta.pt, {jlo, asilva}@det.ua.pt

**Abstract.** This paper presents an access control model that dynamically combines biometrics with PKC technology to assure a stronger authentication mechanism to healthcare professional that can be used indistinctly in Internet and Intranets access scenario.

## 1 Introduction

Access control mechanisms are mostly related with the username and password association or with Public Key Cryptography (PKC). Despite these techniques are broadly used, the storage and handling of secrets, like PKC private keys, is yet a hard-worked problem. One solution can be provided by the usage of smart cards to store digital certificates and respective private keys with access provided by means of PIN code verification. However, when we are dealing with very sensible data it is mandatory to guarantee that the user is in fact who he claims to be, preventing the delegation of access to third persons. Our model proposes a new vision to integrate smart cards, digital credential, biometric fingerprint and user password, contemplating the indoor/outdoor access provenience. The main goal was the achievement of a flexible and robust security access system to verify and ensure that the users are in fact who they claim. The deployment scenario to this implementation was a mission-critical Healthcare Information Systems (HIS).

## 2 Developed Model

The first outcome of this system was the development of a web-based interface module to the HIS [1]. The *XML/XSL* technology was used to assure dynamic content creation and formatting, according to the user terminal and to the access privileges of different user profiles. Aspects of interface usability have also been matter of study in the implementation phase, aiming to create a flexible interface to distinct client terminals. The developed multi-platform interface integrates, in run time, the patient information retrieved from the HIS system with its images from the PACS [2], making these alphanumeric and multimedia data available in a unique Internet browser.

Because we are dealing with very sensitive information, the confidentiality, the users authentication and the log of events are crucial requisites. The data communication privacy is ensured with the adoption of protocols, like the HTTPS, to encrypt the data transferred between server and client. However, concerning access control the prob-

J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 543–544, 2003.

lem is a bit more complex. To cope with this we developed a dynamic access policy that contemplates the access source as well the type of authentication and identification provided. The core element of this system is an innovative Healthcare Professional Card (HPC) based in java cards (smart card) and PKC authentication.

In a PKC authentication, the user must sign the server challenge with their private key to prove the identity. This key must be kept in a secure place and the smart card appears as the best and flexible device to securely store these keys. In the proposed model, the smart card PIN results from the inside card processing of distinct elements and from a secret calculus formula that combines the user password with the biometric fingerprint template (a byte stream sequence). The fingerprint template used in the PIN calculus is securely stored inside the card and never leaves this device. The eventual attempt to use a live scan fingerprint capture does not result on a bit string exactly equally to the stored on the card [3] and consequently provides an erroneous PIN.

We realized that inside the institution the professional is authenticated through an HPC-Password pair, but to obtain a similar access level from a remote access our system contemplates and demands the use of the HPC-Password and fingerprint recognizing mechanisms. This idea is based on the assumption that inside de institution other persons and access control devices establish the necessary physical user identity control. Because this situation is not identical in an outdoor access, biometric recognition appears as fundamental element to enforce the identity of HPC owner.

The bypass to the biometric matching process dependents from the access provenience. The evaluation of indoor/outdoor situation is made by the server side, which will check the IP address of client workstation in the indoor access list. If the client, for instance, is not in the private departmental network, the server sends the encrypted information (date + provenience-flag + challenge) demanding the fingerprint match to the java card routine. At the end, the java routine just returns the signed challenge that will be sent to the server to provide user authentication.

## 3 Conclusion

In this paper we have presented an integrated access control model specially designed to information systems that handle sensitive data. The system provides a universal and robust PKC-based authentication, implements a flexible identification model including biometry as second authentication factor, allows high user mobility and copes well with the diverse kind of user interfaces.

## References

[1] Bexiga, A., F. Augusto: IWBDC - Interface para Base de Dados Clínica, in Revista do DETUA. (2003) vol. 3 (8): p. 827–841. (in Portuguese)

[2] Silva, A., et al.: A Cardiology Oriented PACS. in Proceedings of SPIE. (1998). San Diego - USA.

[3] Riha, J., V. Matyas: Biometric Authentication Systems. Masaryk University Brno. (2000)