Electronic Patient Record Virtually Unique Based on a Crypto Smart Card

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 a Multi-Service Patient Data Card (MS-PDC) based on a crypto smart card and Web technology that integrates a new set of functionalities that allow handling well patient mobility.

1 Introduction

The world globalization process is increasingly promoting peoples' mobility, creating a higher dispersion of patient clinical records and forcing even more the healthcare providers to take measures to promote the share and the remote access to patient clinical data over the Internet. It is recognized today that Web-based technologies are a fundamental piece in the access to database and medical image systems. In this scenario, it is proposed and described a MS-PDC based on Web technology, Public Key Cryptography (PKC) and crypto Smart Cards that is unequivocally providing a way to store and transport patient's administrative and clinical data, handling well patient mobility and implementing an innovator vision of a virtual unique Electronic Patient Record (EPR).

2 Proposed Model

The patient administrative data and the emergency data are stored inside the card EPROM and structured following the G-8-Netlink specifications to ensure the PDC international interoperability [1]. On the Hyperlink area it is possible to store Web EPR locations [2]. We can see this feature as a mobile clinical patient homepage portal. This is achieved through a structured implementation of hyperlinks associated to remote clinical patient data, creating, by one side, a truly distributed EPR system and promoting, by the other, the idea of a virtual unique and universal EPR. When a patient goes to a healthcare provider and clinic data is produced, the institution can write on the card a digitally signed hyperlink referencing the local EPR information. The hyperlink dataset was defined in ASN.1 [3] and follows an ISO8825 data encoding implementation. Every pointer includes, beyond other fields, an electronic record address (URL), the issuer institution identification and digital credentials references, a relevancy factor indicator, as well important coded clinical details. They work as structured bookmarks that objectively provide the indexing, sorting, location and ac-

J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 545–546, 2003.

cess mechanisms to a distributed electronic patient record. Associated to every link it is appended the respective digital signature made using the institution private key. Due the smart card memory limitations many of the hyperlink fields are stored in a coded way and interpreted in run time by the browser API engine that converts and presents the card hexadecimal bit stream in a human legible form.

The remote access to distributed EPR locations and respective information systems is grounded on the presupposition that the system must proof, in a strong way, that patient is in fact on the remote place. The MS-PDC is supported by a cryptographic token, allowing the store and management of patient digital credentials. The confidence on security issues depends strongly on the trust we have on digital certificates, on private key storage and how it is verified that the correct person is the owner of the private key. Contemplating these demands, the PDC (hosted by a crypto smart card) implements card owner verification procedures. The first identity proof is related with the patient physical card possession. However, to access to local and remote patient data the authentication is made through the patient private key that signs a host-side challenge and proof the user identity. The user private key is unique and securely stored on the card protected by a PIN and/or biometric device. The PDC supports PIN verification but it is also prepared to acquire and store two distinct card owner fingerprint templates.

The system is supported by a Web portal that ensures the entire tasks related with the PDC issuing/revocation, patient digital credentials management and support, update of protected data and backup of information like the Hyperlink MS-PDC zone contents. Moreover, the URL of this PDC portal service is stamped on smart card front side and any institution or practitioner with the necessary credentials and a web browser client and a smart card reader can navigate inside the card contents making use of the API available in this portal.

3 Conclusions

The presented product represents a cost-efficient solution that enables high patient data mobility, implements a flexible and trustable model to index and access to distributed EPR information over open and heterogeneous environments as the Internet. Strong authentication enforcements, completely scalable and integrated utilization are other achievements of the proposal.

References

1. G-8-Netlink-Consortium: Netlink Requirements for Interoperability", v2.2, http://www.sesam-vitale.fr/html/projects/netlink
2. Costa, C., et al.: *New Model to Provide a Universal Access Mechanism to Clinical Data.* Technology and Health Care - IOS Press, (2001) vol. **9**(6): p. 459–460.
3. ITUT02: ASN.1 encoding rules Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER),ITU-T Rec. X.690 (2002) ISO/IEC 8825-1:2002 (2002)