A UNIVERSAL MEMORY CARD SERVER

P. Durant[1], P. Ardouin[2], M.-J. Papillon[1], A. Gamache[2], G. Lavoie[1], J. Bérubé[3], and J.-P. Fortin[1;4]

ABSTRACT

This paper describes a memory card server called SCAM (in French: "Serveur de Carte À Mémoire") [2] which has been designed to facilitate the development of smart card applications and their integration into larger information systems. SCAM is a generic software server that can manage smart cards as well as other memory cards including laser cards. The server has been used in the implementation of a portable medical record (PMR) within the Québec Patient Smart Card Project [1;2;3]. This software architecture provides a flexible and evolutive way to manage the PMR and allows its optimization on differents points of view. The PMR is viewed as an object that can be manipulated only by the SCAM's services. This paper presents the concepts and techniques used to provide a generic environment to deal with smart cards (and more generally with memory cards), to obtain a dynamic and evolutive portable record, to raise the system global security level and the data integrity and to significantly optimize the management of the portable record.

RÉSUMÉ

Cet article présente un serveur logiciel de cartes à mémoire (SCAM) [2] conçu pour faciliter le développement et l'intégration d'application utilisant la technologie des cartes à microprocesseur dans les systèmes d'information. Par définition, SCAM est un serveur universel de cartes à mémoire permettant l'accès et la manupulation des cartes à microprocesseur, des cartes optiques (laser) ou d'autres types de cartes à mémoire. Ce serveur est utilisé dans le cadre du Projet de la Carte Santé pour la mise en oeuvre d'un dossier médical portable (DMP) sur carte à microprocesseur [1;2;3]. Cette architecture logicielle offre une flexibilité évolutive appréciable et permet d'optimiser la gestion du dossier portable à plusieurs points de vues. Dans cette optique, le dossier portable est perçu comme un objet pouvant être manipulé uniquement à partir des services spécifiquement offerts par SCAM. Cet article présente les concepts et techniques, mis en application à travers le serveur logiciel de cartes à mémoire, permettant de rendre générique l'utilisation de la technologie des cartes à microprocesseur, d'obtenir un DMP évolutif et dynamique, d'augmenter les niveaux de securité globale du système ainsi que l'intégrité des données et d'optimiser de façon significative la gestion et la manipulation du DMP.

---

1 Projet Carte Santé, Département de Médecine sociale et préventive, Université Laval, Québec (QC), Canada
2 Département d'informatique, Université Laval (QC), Québec, Canada
3 Projet Carte Santé, Direction de la santé publique de Rimouski, Centre hospitalier régional de Rimouski, Rimouski (QC), Canada
4 Head of the research team.

INTRODUCTION

Many smart card technologies are presently avalaible and the domain is in continuous evolution. Futhermore, many software applications, specialized in an area of data management such as medical information, will have to access portable records stored on smart cards, such as portable medical record (PMR). It is important to insure independence between the different components of the system: software application, portable records and microprocessor card technology.

The universal software memory card server described in this paper, SCAM [1], is a generic software tool that provides services required to manage different types of memory cards: smart cards, laser cards and others types. In the case of a smart card application, all specific and technical characteristics of smart card technologies or smart card constructors can be managed by the server. SCAM provides a high level command language in order to manipulate and access data in the portable record. The command language is generic, easy to use and can increase developers' productivity, because they are not required to master all the technicalities of the specific card to be used.

The governments of many countries are presently reviewing the organization of their health care services, in order to simplify administrative procedures. To that effect, smart card appears to be an efficient way for improving communication of clinical information between health care providers. In this context, the Québec Patient Smart Card Project [1;2;3] has been undertaken by the "Régie de l'assurance-maladie du Québec" with the collaboration of Université Laval and the "Centre hospitalier régional de Rimouski" (Rimouski Regional Hospital Center) (Rimouski is a city of 35 000 inhabitants located 300 kilometers east from Québec). One of the main objective of this project is to experiment smart card technology to support a portable medical record, as long as there is already another card for the identification and the administrative procedures.

The research activities that resulted in SCAM have started a few years ago [1;2]. This paper describes the general characteristics of SCAM, including component's independence, architecture, language, multi-task approach, data integrity management, memory management, security management and the logical and physical data zone concepts. To illustrate the characteristics of SCAM, the paper also describes their application in the context of the PMR developed and implemented in the Québec Patient Smart Card Project.

SYSTEM COMPONENT INDEPENDENCE

The main system components are microprocessor cards that store the data, the software applications that manage the data, and the portable record. A major role of SCAM is to insure that applications will be independent of the characteristics of the other components, and can go on working even if these other components change.

The architecture based on the use of the server offers flexibility with regards to evolution. With this approach, it is possible to use different smart card technologies. Smart card technology is evolving and manufacturers will aim at integrating new functions or ways to manage memory. In this evolutive context, the type of memory, its management and its security features must be 7taken into account. Either for economic or technical reasons, it is important that the system be sufficiently open in order to interface with other storage media such as optical cards or other types of memory cards. All these elements, associated with memory technology, are taken into account by SCAM, which is responsible for integrating changes.

Similarly, applications would normally be called upon to change over time in order to adapt to legal, functional or ethical needs. Moreover, evolution or adaptation of the applications will become more complex and expensive if different applications are involved, generally with different partners from

different organizations. To deal with this situation, a generic language is used to access and manipulate data in the card memory; this high level langage is independent of the technologies involved. In this way, software applications are totally independant from the storage medium and the portable record is manage as an object.

Features, were guarantee evolution and independence, are extended to the modelisation of the PMR, in order to have a structure dynamically evolving. Thus, the PMR structure is defined at two levels: the logical level and the physical level. A concept of physical data zones has been used to represent the physical structure of the PMR. At a higher abstraction level, applications apply a logical data zone concept that correspond to a logical view of data. The two level PMR structure implement the evolution and independence concepts. Software applications only know the logical data struture. This allows great flexibility for SCAM to manage physical data and change the physical structure without need to change applications using the PMR.

One question remains: How the PMR can evolve without updating the server? In fact, the server needs to know the logical and physical structure in order to be able to make a structural mapping. Specification matrices are used to obtain the required flexibility; these numerical matrices define both structures and their association in order to make SCAM able to manage the data segmentation and physical formating. Construction and maintenance of the matrices are simple. The structure is taken into account when the server is loaded, and can be adjusted and modified as needed.

SCAM ARCHITECTURE

The software server includes two management levels: a logical level and a physical level. The logical level is specifically in charge of the aspects associated with the applications. At this level, SCAM uses a command processor that translates the commands of a high level language into low level instructions (physical commands). At the physical level, SCAM use a low level processor that translates the physical commands received from the logical level into smart card language commands for the specific card being used.

The logical level management of SCAM also encapsulates and enriches the card functionalities and tools, by implementing many concepts and mecanisms essential to get flexibility, security and integrity for the portable record. This software layers are embedding the portable record that is only accessible through SCAM services.

GENERIC HIGH LEVEL COMMAND LANGUAGE

In order to allow applications to interact with smart cards regardless of specific technologies, a generic high level language has been developed. This language corresponds to the implementation of the services of SCAM; its commands are available in a dynamic link library (DLL) of user-friendly functions named Protocolar Library. This library is technically independent of SCAM; it communicates with SCAM using a protocol based on messages.

Each command is a generic macro-command that performs a set of sub-commands in order to provide the level of abstraction required by the application with regards to the specific technicity of the smart card used. These high level commands simplify the use of smart cards and increase the productivity of developers who are not required to know all the technical details of smart cards.

The commands of the language are based upon file manipulation instructions available in several programming languages. To begin a session with a card, it has to be opened by an *Open Card Command*. The portable record can be accessed and processed through a set of *Transactionnal*

Operations. In order to terminate the session, an explicit *Close Card Command* must be used. Some characteristics of these commands are described in the following paragraphs.

Open Card Command

The Open Card command includes all instructions specific to the smart card being used and the communication interface with the user in order to prepare the card for accessing the data. In the context of the Québec Smart Card Project, which uses an IBM microprocessor card, SCAM will ask the user to insert the card in the reader and then put the power on. At this step, a sequence of identification is started in order to recognize the technology being used (the IBM card uses an EEPROM memory for data storage). After this, SCAM will make sure that the card is really a card associated with the Project, and determine the type of card being used, either a health care provider access card or a patient card, and perform the authentification of the card with an asymetric public key algorithm, if the card is an health care provider access card. SCAM will also verify the card version number that specifies the logical and physical structure of the PMR.

Transactionnal Operations

Once a card has been opened, the application can access and process the data in the card. It can read a logical data zone, write records into a logical data zone, make a correction to a record, read all the corrected records on the card or get information about the status of the card. All these operations are performed according to the access rights of the user.

Close Card Command

The Close Card command terminates the operations on the card. The access rights are disabled and SCAM will automatically eject the card from the reader, if the specific reader in use can perform such a function.

MULTITASK APPROACH

The performance of any computer based system may be expressed in terms of processing capacity, speed and exchange rate of information flow. In this regard, a smart card may be viewed as a low performance level component that constitutes a bottleneck that slows global system performance and that prevents higher performance components from reaching their full potential. In order to avoid such a situation and allow a sufficient performance level for all system components, the microprocessor card server uses a multitask approach, where read and write operations to the card can be executed in background when the CPU is not in use.

The use of such a multitask approach is an essential contribution towards the acceptance of microprocessor card technology for data storage in applications where the access time requirements are severe. At the Rimouski experimental site, this was an important dimension of the project, because introduction of the smart card could not result in slowing down current medical practice.

MEMORY MANAGEMENT

In order to solve the problems associated with the limited capacity of the microprocessor card memory some technics have been applied. Applications view the memory as a set of logical data zones and transmit data according to a logical format comprising chains of alphanumeric characters. From the type and the domain of each variable, SCAM can translate data expressed in the logical format to a physical

format to optimize the use of memory. Codification tables and logical compression algorithms are applied and result in a binary expression for each data element which is minimized to the nearest bit.

This approach results in the equivalent of allocating virtual memory to applications. In the case of the Québec Patient Smart Card Project, which has an 8 k byte memory card capacity, the use of SCAM enabled the storage of data which would otherwise have required approximately a storage capacity of 15 k bytes. However, the amount of available virtual memory depends upon the data compression rate, which varies according to the data stored in the card. Logical compression is not always possible, for example in the case of free text whose character domain spans upon all the 8 bits of the ASCII table.

DATA INTEGRITY MANAGEMENT

The infrastructure of a PMR system based upon the use of a microprocessor card must insure data integrity, especially because it involves a portable medium that can easily be disconnected from communication with requesting systems. Because of this, mechanisms have been included in the software server for insuring the completeness (or atomicity) of transactions written in the card, detecting incomplete transactions and other data anomalies, and taking appropriate corrective measures; these mechanisms operate both at the logical and physical levels.

At the logical level, the mechanism used for insuring transaction completeness is triggered in two specific cases: 1) when writing records in a logical data zone involves the writing of transactions in different physical zones; 2) when processing a correction transaction for a record in a logical zone. However, the mechanism that validates integrity of written data performs data verification during each access to a logical zone. At the physical level, the server uses writing semaphore to insure the completeness of physical transactions. It also updates an integrity table and the information required to perform physical recovery of data. Verification of the status of a card is performed automatically as soon as the card is opened.

SECURITY MANAGEMENT

The security of a smart card system is based upon security mechanisms inherent to smart cards. However, SCAM provides global security organized at two specific management levels, respecting, on one hand, the independence of the logical aspects relatively to the characteristics and tools of the hardware and, on the other hand, to enrich the global system security.

Management of all keys used for the security of the system is performed within the SCAM software server. Applications do not process any key, except for the session key used for the identification of each user when transaction processing is required. SCAM handles input and transfer or presentation of the keys to the card.

Using SCAM requires the use of two types of card: one card that formally identifies the provider of services and one card that stores the portable record to be processed. In the context of the Québec Patient Smart Card Project, an access card is issued to all health care providers involved: physicians, pharmacists, nurses and ambulance personnel, in order to specifiy their profile of access rights to the portable record.

There are specifically three types of profiles implemented in the system: physical, logical and virtual. The first one defines the access rights to the physical data zones, for read and write operations, and must be controlled through the use of a key. The logical profile defines the logical access rights of a provider of services, either individually or as a member of a class, to its own access card or to the portable record. The rights are expressed as vectors of bits that specify the logical zones accessible either

in reading or in writing; this information is used by the server to control access to the cards. The virtual access profile combines different profiles thus enabling provider of services to have a broader view on data than what their regular profile would allow. However, activation of the virtual profile requires autorisation of the patient card bearer, through the use of a specific key.

The provider access card contain the keys required to access the portable record; these keys are encrypted with DES (Data Encryption Standard) and are not accessible by the provider of services. The access card also includes a certificate that enables the server to authenticate the cards; this certificate is generated by an asymetrical algorithm using a public key.

In the context of the Québec Project, the patient cards, containing the portable medical record, are of the same type as the one used as the health providers. Access to the data is controlled by a set of keys, each of which being associated to rights in reading and writing. However, contrary to the health provider card, the bearer of a patient card is not required to provide a PIN to access the data; this is done through the health care provider card.

LOGICAL AND PHYSICAL ZONE CONCEPTS

A smart card system using SCAM would normally favors independence of system components. For that purpose, a two level architecture has been designed for the portable record: the logical level and the physical level. The logical level uses an approach similar to traditionnal data bases, where the portable record data are organized in logical data zones, which are sets of occurences of a type of record, that comprises semantically associated variables which are individually defined according to a specific type that coresponds to its domain.

When designing the logical zones, developpers do not have to take into account the specific user access rights to the variables, because of the two level portable record management; this is done by the server. Thus, the portable record conceptual structure can be directly applied at implemention time.

The physical management level of the portable record is the sole responsibility of the server. This level uses the concept of physical data zones, which may be viewed as sets of memory blocks; comprising sets of contiguous bytes. The access rights to data are taken into account at this level, and in fact, this is one of the main criteria upon which the organization of data in the card is based.

In order to implement the system, the SCAM server must map the logical structure into its corresponding physical structure. This is done through by using the matrices of specification of the portable record. For each logical zone, matrices indicate the number and types of each logical variable and their physical correspondence in terms of physical variables and physical data zone where each physical variable is to be recorded.

The logical-physical mapping is a transparent operation that can be illustrated by two typical examples. In the first simple example, all variables of a logical zone share the same access rights in reading and writing, and in that case, the logical to physical correspondance is of 1-1 type, where the logical variables are written in the same physical zone in the card. In the second case, the variables of a logical data zone can be accessed with different read and write access rights and must be stored in different physical data zones according to the access rights. Thus, the logical to physical correspondence is of 1-n type. This mechanisms allow SCAM to provide the appropriate views of the data according to the access rights.

CONCLUSION

The research activities mentioned in this paper have resulted into a flexible system architecture to implement a portable records on smart cards. The essential element of this architecture is a generic card server called SCAM (in French: "Serveur de Cartes À Mémoire"), involving independence of system components. The server insures the security of the portable record in several manners, and is a success factor for the integration of smart cards into larger information systems. The approach for structuring and managing data is somewhat similar to the use of a conventionnal database management system, and results in secure operations, processing efficiency and satisfactory response times. Finally, SCAM is a generic server that can support different types of memory cards, including existing microprocessor cards and other technologies such as optical cards. Current research activities are oriented towards Open Database Connectivity (ODBC), and the use of an SQL language, by the application, to manage the portable record.

ACKNOWLEDGEMENTS

The research project that resulted in this paper has been financially supported by the Régie de l'assurance-maladie du Québec.

REFERENCES

[1] Gamache A., Ardouin P., Lavoie G. et Fortin J.P., «Caractéristiques systémiques et techniques d'une carte-santé réalisée avec la carte intelligente», Actes d'un Colloque sur l'intégration des cartes intelligentes dans le développement des systèmes, Université Laval, Sainte-Foy (Québec), septembre 1990.

[2] Durant P., «Architecture et fonctionnalités d'un serveur de cartes à microprocesseur dans la mise en oeuvre d'un dossier médical portable», Mémoire de maîtrise en sciences (informatique), Faculté des Sciences et de Génie, Université Laval, février 1992.

[3] Papillon M.-J., Bérubé J., Comeau M., Lavoie G., Kirouac S. and Fortin J.P. «Futuristic Microchip Health Card Experiment in Québec», Canadian Medical Informatics, Volume 1, Number 1, P.16-17, May/June 1994.