A Smart XML Access Right Controller for Mobile Applications

Luc Bouganim, François Dang Ngoc, Philippe Pucheral

A Smart XML Access Right Controller for Mobile Applications

Luc Bouganim [**] François Dang Ngoc [*] Philippe Pucheral [*,**]

* University of Versailles
78000 Versailles - France
<Firstname.Lastname>@prism.uvsq.fr

&

** INRIA Rocquencourt
78035 Le Chesnay - France
<Firstname.Lastname>@inria.fr

Abstract: *Chip-Secured XML Access (C-SXA) is a versatile XML-based Access Right Controller embedded in a smart card. C-SXA can be used either to protect the privacy of on-board personal data or to control the flow of data extracted from an external source. C-SXA addresses a broad range of applications, like secure portable folders, Digital Right Management, parental control or exchange of confidential information among a community of users. We illustrate the effectiveness of this technology through a collaborative agenda application embedded in a cellular phone SIM card.*

1 Introduction

Chip-Secured XML Access (C-SXA) is a versatile XML-based Access Right Controller embedded in a smart card. C-SXA evaluates the user's privileges on on-board or external XML data and delivers the authorized subset of these data. The use of XML (the de-facto standard to describe and exchange data) makes C-SXA agnostic about the kind of data to be protected and then participates to its versatility. Indeed, an increasing part of the information accessible through the web (textual documents, datasets, images, video, sounds, services) is now represented or annotated in XML.

The first issue addressed by C-SXA is protecting the privacy of personal data embedded in the smart card. Existing approaches store row data sequentially and propose at best rudimentary mechanisms to regulate the access to these data (e.g., password). C-SXA implements database features to store effectively XML data and to share them among multiple users or certified applications at a much finer granularity (e.g., browser, agenda or address book applications can share parts of a user's profile with different privileges).

The second issue is controlling the access to external resources. Existing approaches, like secure storage services, secure data sharing or Digital Right Management (DRM), implement access control by means of encryption. In these approaches, the sharing scenarios among users are crude and pre-compiled at encryption time. By contrast, C-SXA clearly separates the concern between data encryption and access control. C-SXA processes the card holder's access control rules on an encrypted XML input document and delivers the authorized subset of this document. Several and personalized access control policies can therefore be defined on the same document, reflecting different privileges for different users. These policies can easily evolve by updating the access control rules without impacting the document encryption.

Thanks to these two features, C-SXA addresses important applications emerging in the telecom and banking domains (e.g., portable folders, DRM, secure data sharing among family members, friends or business partners) that cannot be tackled by existing technologies. While powerful, C-SXA accommodates well the strong hardware smart card constraints. This equation has been solved thanks to a long expertise in developing advanced database components embedded in smart cards [ABB01, PBV01, BoP02, BoP04, BDP03].

The sequel of this paper is organized as follows. Section 2 presents the main application domains targeted by C-SXA and discusses the current state of the technology in these domains. Section 3 introduces the C-SXA architecture and illustrates its use through an application's sample, namely a collaborative agenda managed through cellular phones. Finally, section 4 discusses the ease of use and cost-effectiveness of the proposed technology.

2 Target applications and alternatives

Storage and protection of on-board data

The rapid growth of smart card stable storage capacity (from kilobytes to megabytes soon) makes the management of on-board data realistic and more and more attractive for a wide range of applications. The concept of secure portable folder has emerged with the idea of carrying a patient's medical history in a smart card [SCA03]. Since then, the value of smart cards to secure and share in a controlled way personal information has been recognized in several domains like education (scholastic folders), commerce (loyalties), telecommunication (address book) or mobile computing (user's profiles containing licenses, passwords, bookmarks, etc). MasterCard published recently the *MasterCard Open Data Storage (MODS)* Application Programming Interface "*to meet the desire expressed by customers to better control how much information they are willing to share with whom*" [Mas02]. The IBM-Harris report on consumer privacy survey strongly

highlights this same requirement [IBM]. According to MasterCard, MODS gives issuers the market differentiation they want, merchants the marketing tools they need, and consumers the convenience and control they have been asking for.

While the need for on-board data management and sharing facilities is clearly established, few technical solutions have been proposed yet. Existing solutions are generally application specific, store data sequentially, allow basic searches and protect data thanks to passwords. The Structured Card Query Language (SCQL) standard [ISO99] is a first attempt to define database-style storage techniques and privileges. PicoDBMS [PBV01, ABB01], designed by our team, was the first full-fledged relational database system embedded in a smart card, supporting a robust subset of the SQL standard (and then encompassing SCQL). PicoDBMS is however a complex technology primarily designed to manage efficiently huge and well structured embedded folders. The versatility and wide acceptance of XML [XML] makes this standard the best candidate today to describe, organize, store and share the variety of data that appear in the above applications. To the best of our knowledge, C-SXA is the first technology providing a smart card XML data store and access controller.

Protection of external data

Different requirements motivate a secured access to external data from a smart card: (1) the management of personal folders (as above) whose size exceeds the smart card storage capacity; (2) the sharing of personal or professional data (e.g., agenda, address book, bookmarks, etc) among a community of users (family, friends, colleagues, partners); (3) the consumption of information disseminated through a license-based distribution channel or (4) accessed freely through the Internet.

While the internal data are protected by the tamper-resistance of the chip, external data need be protected by encryption. The role of encryption differs depending on the source of threatening. In cases (1) and (2), encryption is required to preserve the confidentiality of the data hosted in untrusted servers, considering the increasing suspicion towards *Database Service Provider* (*DSP*) [HIL02] and the vulnerability of database servers facing external and internal attacks [FBI03]. In case (3), the role of encryption is protecting digital assets from illegal access and copying [Sma]. Finally, case (4) refers to the ever-increasing concern of parents and teachers to protect children by controlling and filtering out what they access on the Internet [PIC]. To meet this last requirement, encryption can take place in the Web server, in the ISP or in the client device communication card while the access control and decryption remains confined in the smart card.

Usually, the data are kept encrypted at the server and a client is granted access to subparts of them according to the decryption keys in its possession. Variations of this basic model have been designed in different context, such as encrypted backups for personal data [Sky], encrypted data hosted by untrusted DSP [HIL02], encrypted relational databases [Ora04, HeW01], lucrative as well as non-profit publishing [MiS03, Sma]. Despite their respective merit, these models have in common a static way of sharing data. Indeed, access control policies are all precompiled by the encryption, so that changing these policies may incur a partial re-encryption of the dataset and/or a potential redistribution of keys [BDP04]. A touch of dynamicity can be introduced by decomposing each data in disjoint encrypted parts and leave clients access subparts of the data according to a license [Sos]. However, decomposing each data and administering the corresponding licenses is a rather tricky and cumbersome task.

Unfortunately, they are many situations where access rules are user specific, dynamic and then difficult to predict. In medical folders, the rules protecting the patient's privacy may suffer exceptions in several situations (e.g., in case of emergency) [ABM03]. In a data-sharing scenario, the sharing policies change as the initial situation evolves (new relationship between users, new partners or friends, new projects with diverging interest, etc.). Access control languages like XrML [XrM] or ODRL [ODR] demonstrates the need for more expressiveness and flexibility in DRM applications (e.g., Alice may listen freely to a piece of music provided she has listened a given amount of commercial before). Finally, neither Web site nor Internet Service Provider can predict the diversity of access control rules that parents/teachers with different sensibility are willing to enforce (e.g., rules may depends on religious beliefs, political opinions, lecture topics, etc.). Again, to the best of our knowledge, C-SXA is the first technology capable of supporting the access control flexibility required by these applications. This flexibility is guaranteed by a clear separation between encryption and access control and by a smart and versatile XML access controller embedded in a secured chip. The resulting benefit is threefold. First, C-SXA provides a very user friendly and powerful way to define access control rules (e.g., Salary[amount>10000] expresses in a single formula the protection of all salaries greater than $10.000 in a complete – group of – document). Second, access control rules are fully dynamic since they are downloaded by the smart card on demand. Third, C-SXA applies to any kind of data described or annotated in XML, a standard flooding every activity sectors.

Market perspectives

To predict the market impact of emerging applications is a rather difficult task. However, elements for this analysis can be delivered. The target applications mentioned above impact primarily the SIM card market and the banking card market. Indeed, digital asset consumption through cellular phones is yet a reality and data sharing among a community of user is well in the spirit of the SMS phenomenon. At the same time, the customer's interest for secure portable folders has been clearly identified by MasterCard. According to Eurosmart, the telecom market alone worth 60% of the

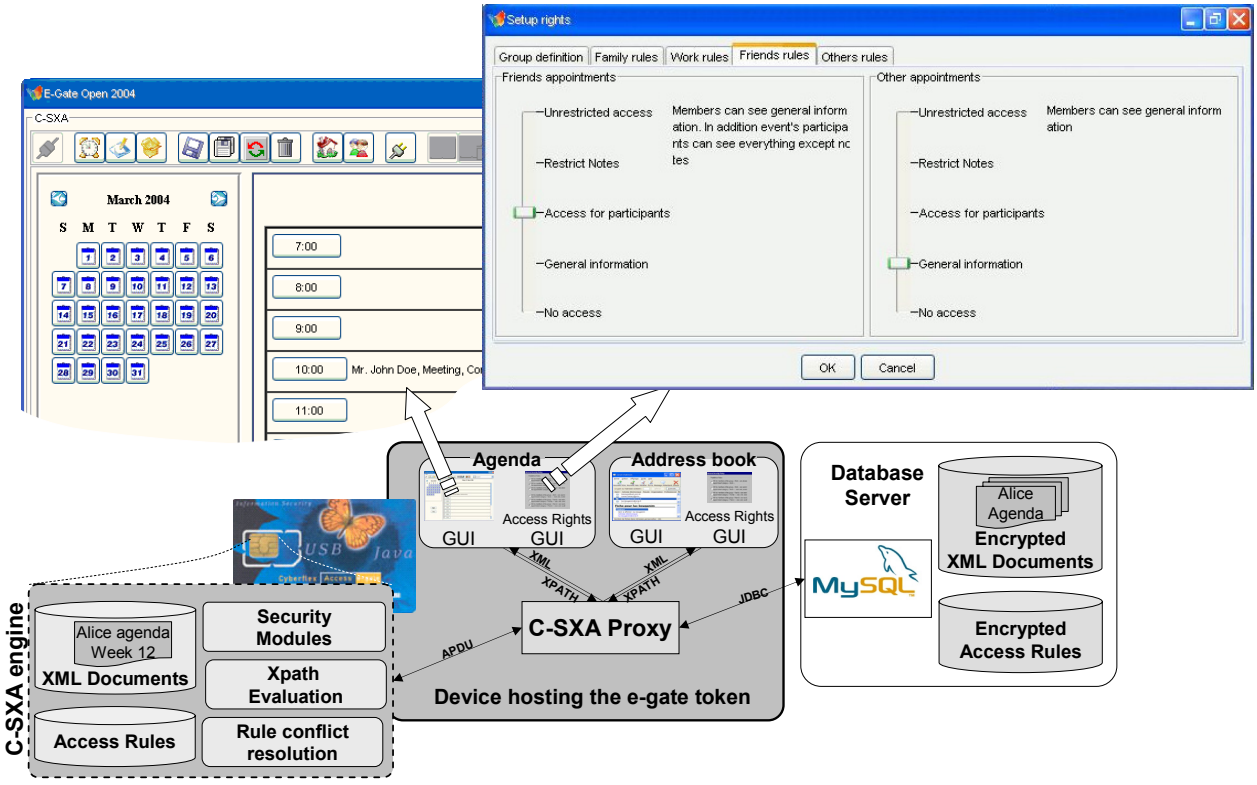

Figure 1: *Target architecture*

smart card market's global sales, estimated at 1.7 billion euros in 2002. ST Microelectronics indicates that 500M of SIM smart cards and 200M of banking smart cards have been sold in 2002 representing roughly 85% of the total market. As Eurosmart confesses, the development of new SIM card services is, however, more difficult to quantify. Anyway, services in relation with DRM will undoubtedly receive a particular attention considering the dramatic impact of worldwide digital piracy for the music industry (loses estimated to $5 billion every year by the RIAA) and the movie industry (loses estimated to $3 billion every year by the MPAA). Also, data privacy (and then secure folders) is becoming a major concern for most citizen and consumers, as stated in the IBM-Harris Multinational Consumer Privacy Survey [IBM].

Parental and teacher control could also generate a new mass market for smart cards. To illustrate this, the French government launched an important educational program to give students and teachers a controlled access to a wide range of digital assets (book extracts, encyclopedia elements, geographical maps, works of art, etc) [Jou04]. As an indication, the number of French students was estimated by INSEE to 14,4M in 2001.

3 Architecture and application's sample

To illustrate how the C-SXA technology works, we use a collaborative agenda application. This application clearly exemplifies the need for dynamicity. Indeed, access control rules are likely to evolve while new partners join or leave the community of users and ad-hoc rules may be defined for some sensitive appointments. Models compiling access control policies in the data encryption cannot tackle these situations.

In this application, the agenda is actually stored in an encrypted form on a remote server to allow the sharing among partners while protecting the data confidentiality. Part of the agenda (e.g., the current week) of a user can also be stored in his own smart card to give him the ability to consult his agenda thanks to his cellular phone in a stand-alone mode (e.g., while being disconnected). Figure 1 pictures the target architecture.

Let assume now that Alice agrees to share part of her agenda with Bob and that both Alice and Bob use a C-SXA enabled SIM card in their cellular phone. Alice will fix Bob's access control policy thanks to a user friendly *rights management GUI* (default rules are proposed to manage the usual cases, as pictured in the figure). These rules are translated in XPath [XPA] expressions by the application and are stored in an encrypted form in the remote server. Later on, Bob connects to the server and asks for Alice's agenda. At that time, C-SXA downloads Bob's access control policy through a secured channel in Bob's SIM card. Bob can then issue a query on Alice's agenda, again thanks to a user friendly GUI (e.g., by clicking on a particular day). The application translates this query in an XPath expression, then C-SXA interprets it, downloads the relevant day of Alice's agenda in a streaming fashion, decrypts it, checks its integrity and evaluates Bob's access control rules to deliver the authorized final result. Bob can issue an update on an authorized part of Alice's agenda (e.g., to notify her from a change in an appointment) exactly in the same way as a query. If Alice is willing to change Bob's access control policy, she uses again the access access right management GUI, the new policy is sent to the server and will become active the next time Bob connects to Alice's agenda.

The C-SXA mechanisms are generic and can be applied to any kinds of XML document. Only the GUI and the application logic are specific. The reader interested by a deeper description of the C-SXA internals is referred to [BDP04].

4 C-SXA ease of use and cost-effectiveness

The ease of use is a primary concern for the end-user. To this respect, the benefits provided by C-SXA are the following. First, any kind of data can be represented in XML and then can be stored inside the smart card for personal use or outside from the smart card for a collaborative use, as easily as saving a file on a PC. Second, the declarative expression of access control policies and the dynamicity of these policies strongly simplify their administration. To simplify further this administration, each application can provide a dedicated GUI allowing the end-user to click on a list of predefined policies, in a way similar to Internet Explorer content advisor or MSN parental controls. The Agenda rights management GUI presented in Figure 1 illustrates this principle. Queries are also automatically generated by clicking on the main application's GUI (e.g., a click on a particular day of the Agenda is translated by the application in an XPath expression).

Ease of use is also a strong argument for the application developer. C-SXA tackles this requirement in two ways. First, all the complexity of the storage, access control, query and security management is confined in the smart card and smart card proxy codes, so that the application developer can concentrate on the application logic. Second, C-SXA complies with the standards. Documents are described in XML and both access control rules and queries are expressed in XPath, two very popular W3C standards.

Finally, the cost-effectiveness for the smart card manufacturer or the C-SXA distributor (if different) comes from the simplicity and the versatility of the C-SXA engine. The same engine will be shared by all applications concerned either with local data storage, access control or query management. Its development and deployment cost can then be amortized on very large-scale markets. In the long term, and depending on the market demand, C-SXA could even be integrated in the smart card OS as a native functionality.

More information can be found on the C-SXA web site: http://www-smis.inria.fr/Eprototype_C-SXA.html

5 References

[ABB01] N. Anciaux, C. Bobineau, L. Bouganim, P. Pucheral, P. Valduriez, "PicoDBMS: Validation and Experience", 27th Int. Conf. on Very Large Data Bases (VLDB), demo session, 2001.

[ABM03] A. El Kalam, S. Benferhat, A. Miege, R. Baida, F. Cuppens, C. Saurel, P. Balbiani, Y. Deswarte, G. Trouessin, "Organization based access control", IEEE 4th Int. Workshop on Policies for Distributed Systems and Networks, 2003.

[BDP03] L. Bouganim, F. Dang Ngoc, P. Pucheral, L. Wu, "Chip-Secured Data Access: Reconciling Access Right with Data Encryption", 29th Int. Conf. on Very Large Data Bases (VLDB), demo session, 2003.

[BDP04] L. Bouganim, F. Dang Ngoc, P. Pucheral, "Client-Based Access Control Management for XML Documents", 30th Int. Conf. on Very Large Data Bases (VLDB), 2004.

[BoP02] L. Bouganim, P. Pucheral, "Chip-Secured Data Access: Confidential Data on Untrusted Servers", 28th Int. Conf. on Very Large Data Bases (VLDB), 2002.

[BoP03] L. Bouganim, P. Pucheral, Procédé de sécurisation de bases de données. Patent deposit by the CNRS in august 2001, request for PCT (USA, Europe, Canada, Japan) in august 2002, end of the examination phase in august 2003.

[FBI03] Computer Security Institute, "CSI/FBI Computer Crime and Security Survey" http://www.gocsi.com/forms /fbi/pdf.html.

[HeW01] J. He, M. Wang, "Cryptography and Relational Database Management Systems", IDEAS, 2001.

[HIL02] H. Hacigumus, B. Iyer, C. Li, S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model", ACM SIGMOD, 2002.

[ISO99] International Standardization Organization (ISO). Integrated Circuit(s) Cards with Contacts – Part 7: Interindustry Commands for Structured Card Query Language (SCQL). ISO/IEC 7816-7, 1999.

[IBM] IBM-Harris Multinational Consumer Privacy Survey: www.pco.org.hk/english/infocentre/files/westin.doc

[Jou04] JournalduNet, 'L'espace numérique des savoirs', http://www.journaldunet.com/0302/030207espacessavoirs.shtml

[Mas02] MasterCard, 'MasterCard Open Data Storage (MODS)', 2002. https://hsm2stl101.mastercard.net/public/login/ebusiness/smart_cards/one_smart_card/biz_opportunity/mods

[MiS03] G. Micklau, D. Suciu, "Controlling Access to Published Data Using Cryptography", 29th Int. Conf. on Very Large Data Bases (VLDB), 2003.

[ODR] The Open Digital Rights Language Initiative, http://odrl.net/.

[Ora04] Oracle Advanced Security Administrator's Guide 10g. http://otn.oracle.com

[PIC] W3C consortium, "PICS: Platform for Internet Content Selection", http://www.w3.org/PICS.

[PBV01] P.Pucheral, L. Bouganim, P. Valduriez, C. Bobineau, "PicoDBMS: Scaling down Database Techniques for the Smart card", Very Large Data Bases Journal (VLDBJ), Vol.10, n°2-3, 2001.

[SCA03] Smart Card Alliance, HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements, 2003.

[Sma] 'The Smartright content protection system'. http://www.smartright.org/

[Sky] SkyDesk : @Backup (Storage Service Provider). http://www.backup.com/index.htm

[Sos] Sospita Secure Web. http://www.sospita.com/files/support/ssw_white_paper.pdf

[XML] www.w3.org/XML

[XPA] www.w3.org/TR/xpath