J. Lopez, A. Mana, P. Merino, and J. M. Troya, "The Role of Smartcards in Practial Information Security", *ERCIM News*, vol. 49, pp. 38-40, 2002.
NICS Lab. Publications: https://www.nics.uma.es/publications

model. In trust management the core aspect of authorisation is to answer the following question: Does the set of credentials C prove that the request r complies with the set of local policies P? The local policies are the policies of a server that controls access to some resources, and a client provides – directly or indirectly – some credentials to support its request. These credentials will typically take the form of attribute certificates, digitally signed by trusted parties or empowered authorities.

A good delegation logic is a key component in such a framework, since delegation is the central mechanism by which administrative tasks and procedures are broken down into manageable parts. It is also in our opinion crucially important that a clear separation be made between administrative and executive powers. It is very easy to conceive of situations where a power to manage some administrative attributes of a given resource should be granted, but direct access to that resource should be denied. An example is outsourced management.

The main focus of the work at SICS has been the development of a delegation logic which is based on the idea of delegation as the explicit yet constrained creation of new privileges. We have examined the basic principles of such a model, considered the problem of revocation in this context, and produced a number of prototype implementations including adaptations to the ongoing work on SPKI/SDSI at IETF.

Links:
SICS Intelligent Systems Lab:
http://www.sics.se/isl/pbr
Amanda project:
http://www.sics.se/fdt/amanda

Please contact:
Babak Sadighi Firozabadi, SICS
Tel: +46 8 633 1582
E-mail: babak@sics.se

The Role of Smart Cards in Practical Information Security

by Javier López, Antonio Maña, Pedro Merino and José M. Troya

The GISUM research group at the University of Málaga is looking at the use of smart cards to increase security in different scenarios. The work is supported by the EU and the Spanish Ministry of Science. Some interesting results are represented by two recent projects. These are the eTicket project, which has defined and implemented a secure electronic ticketing procedure including related protocols and support services, and the Alcance project, which has developed a secure electronic forms framework for secure communication between citizens and the public administration.

The transition from traditional commerce to electronic and mobile commerce is fostered by aspects like convenience, speed and ease of use. However, security issues remain unsolved. Smart cards open new possibilities for the development of security schemes and protocols that can provide security in applications such as electronic payments or software protection where traditional cryptographic tools are not useful. The GISUM group is involved in several research projects that make use of smart cards. Current applications include a secure electronic forms framework for government-citizen relations, electronic ticketing systems for GMS phones and Internet, a PDA-based digital signature environment, public transport, access control systems, software protection and banking applications. This report focuses on two recent projects: the eTicket electronic ticketing project (1FD97 1269 C02 02 (TAP)), a coordinated project with the Carlos III University of Madrid; and the Alcance project, consisting of the development of a secure electronic forms framework for secure Internet-based communication between citizens and the public administration (1FD97 0850 (TIC)).

Electronic Ticketing

Ticketing services represent an attractive application that is both useful and convenient for the user. However, security features and greater flexibility are needed in order to foster their extensive use and popularity. Most of these services use a single value (usually a numeric code) to represent the ticket. In consequence, tickets can easily be copied or forged, it is impossible to represent different types of tickets, no delegation is supported and finally, the verifier needs to receive a database of tickets emitted before allowing clients to access the service. Our project therefore focuses on the following two points: the development of a representation for the tickets and the development of protocols and mechanisms for the use of the tickets.

After a careful analysis of the electronic ticketing requirements, the following goals were defined: versatility, compactness, security, payment, fast offline ticket verification, minimal number of messages emitted by users and ticket delegation. Our system is based on cryptographic smart cards which contain a key pair generated inside the card and which ensure that the private key never leaves the card. Each card will also contain a certificate of the public key

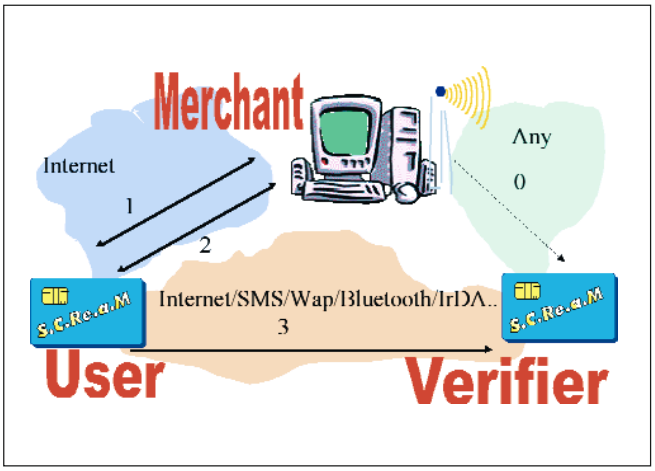


Figure 1: eTicket system architecture.

(signed by the card issuer), the public key of the card manufacturer and some support software.

Ticket merchants are assumed to have access to the public keys of all card issuers whom they wish to accept for the sale of the tickets (usually a small number). When the user requests a ticket from the merchant, an 'open' ticket (ie, one that is not associated with any user) is sent to him. Once the open ticket is received, the smart card verifies that it is correct, extracts the service identifier and authorisation components and stores them in its memory. The authorisation component includes, among other values, the number of closed tickets that the smart card is allowed to produce from that open ticket. To spend an open ticket the user must first close it, which is achieved by including some identification information for the spending of the ticket. This process must be done in the card of the user who bought the ticket from the merchant. Where the user and buyer of the ticket are different entities, we say that the ticket is delegated. Ticket delegation is possible because the software contained in the smart card is trustworthy. For the same reason, there is no possibility for the card to produce more closed tickets than are authorised.

The trustworthiness and the authenticity of the card software is guaranteed because the card issuer signs the public keys of the cards it sells.

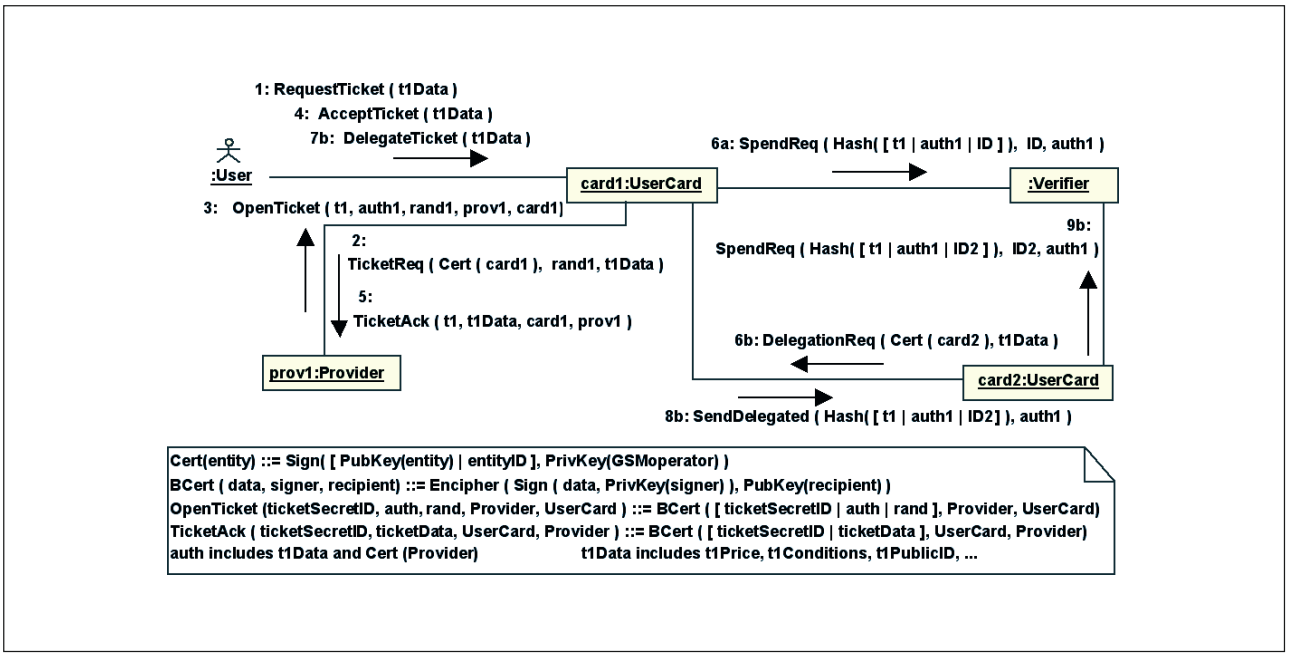
To spend the ticket the user presents the closed ticket to the verifier, providing evidence that he has received the secret service identifier. This is both a fast proof - the only operation involved is a hash - and a secure one, because it is not feasible for a dishonest user to produce the result of the hash operation without knowledge of the secret service identifier.

Secure Software Framework

For public organisations, a telematic version of administrative procedures would bring meaningful benefits concerning accessibility and availability of documents and services, regardless of time, location and quantity. While some implementations exist, a number of technological deficiencies hinder a higher degree of communication between administrations and citizens/companies through the Internet.

It is convenient to define models to include security properties into applications as well as components that have been already developed, and this must be fulfilled making small changes to the code.

The area of application of this project was determined by the computerisation of the Junta de Andalusia Sanction Procedures, which are associated with



Scenarios for ticket spending and delegation.

the Ground Transport Arrangement Law. More specifically, Alcance is being developed inside the Strategia Project, associated with the Works and Transport Council of Junta de Andalusia. The project involves several independent systems, with the Sanction System being one of the most important. Inside the Sanction System, the main task related to our research project is the design of a module which, by using Web browsers, will allow over fifty thousand private organisations and companies to track and transact the sanction files assigned to them in one or more sanction procedures. The module developed allows private organisations and companies, whose access is controlled by Web digital certificates, to monitor their files independently of location and time. Certificates on smart cards support the authenticity necessary for the communication between companies and the Council, and allow the exchange of signed official documents.

We have designed and developed a Form Description Language, called LDF, which is based on XML, and more precisely on XFDL. The use of LDF and related tools introduces many advantages in comparison with traditional use of HTML. Regarding forms status, it is easy to add new components not included in HTML. These new components can be useful for avoiding invalid inputs in the electronic forms, thus achieving a more dynamic management. Additionally, automatic data validation can be done without programming specific code for that operation, as the form specification includes the check itself. Regarding forms management, LDF includes the possibility of forms visualisation by using a traditional browser (for on-line operations) or an independent application (for any off-line ones). Signed forms management is easier, as signers can store in their own hard disk a copy of a partially filled document, which can be opened later for completion using a browser. Moreover, one or more users can sign forms that can be encrypted using unconstrained implementations of algorithms.

Regarding communication, a specialised format ensures the context of the signature is not lost, so that the authenticity of the data is never compromised. Besides this, the document is audited (persons involved, date of the agreement, etc) on its own. In contrast to HTML, LDF provides a data structure and separates application, presentation and logic levels.

Link:
GISUM research group:
http://www.lcc.uma.es/~gisum/

Please contact:
Javier López, Antonio Maña, Pedro Merino, José M. Troya, University of Málaga, Spain
E-mail: {jlm,amg,pedro,troya}@lcc.uma.es

Realizing Trust through Smart Cards

by István Mezgár and Zoltán Kincses

Trust from users is a fundamental element in network-based services. Building blocks of trust are different security mechanisms. A smart card (SC) is a device that can integrate different security mechanisms in a handy form, but interoperability problems can decrease its wide usability. Software reconfiguration can be a way to overcome this problem. A project has been started at SZTAKI to develop an ontology-based reference architecture that supports SC reconfiguration.

Trust and confidence are essential for the users of networked systems, as for all members of the Information Society. The lack of trustworthy security services is the main reason of not using the electronic and mobile technologies in private, business or in public services.

The basic term of trust means reliability in some person or thing, or to allow to do something without fear of the outcome. Trust is of different categories, eg, Impersonal/Structural trust, Dispositional trust, Personal /Interpersonal trust.

In order to motivate individuals to use a certain information system, users have to be convinced that it is safe to use the system, their data will not be modified, lost, used in other way as defined previously, etc. In case the individual has been convinced, one will trust the system and will use it.

Access control (identification), authentication, privacy, and confidentiality are services forming the sense of trust for a human being. To achieve these services three basic building blocks of security mechanisms are applied: encryption (for providing confidentiality, authentication and integrity protection), digital signatures (for authentication, integrity protection and non-repudiation), checksums/hash algorithms (for integrity protection and authentication).

Smart cards can become essential trust elements in a security infrastructure as they are able to integrate different security mechanisms besides the current application. They are efficient devices to execute security functions, such as digital signatures. The workable interoperability of technical and organizational frameworks and supporting infrastructures is a big problem, as the lack of them can decrease SC usability. Overcoming this problem can help the software reconfiguration.

In the close future smart cards will have a role more important than today. Multifunctional cards can integrate different applications; identity card, bank-card,