

Facilitating Administrative Services for Mobile Europeans with secure Multi-Application Smartcards

Reinhard RIEDL¹

Department of Computer Science, University of Zurich,
CH-8057 Zurich, Switzerland,

Tel: +41-1 635 43 31; Fax: +44-1 635 68 09; Email: riedl@ifi.unizh.ch

Abstract. We discuss how JavaCard technology may be exploited for facilitating better administrative services for a broad class of inter-organizational and brokerage processes. Particular emphasis is given to the required interdisciplinarity of the engineering process.

1 Introduction

In this paper we discuss, how JavaCards may be used for the coupling of inter-organizational administrative processes, which respects existing local solutions and supports the exchange of data and workflows between them nevertheless. The paper relies on the work done in the current IST-project “FASME – Facilitating Administrative Services for Mobile Europeans”. on Smartcard-based identity Cards for the ‘citizen to civil services access’.

If a European citizen migrates from one European country to another, she has to interact with various authorities. In particular, she has to obtain personal documents from authorities in her former place of residence and to deliver them to authorities in her future place of residence. Due to the incompatibility of administrative procedures, authorities further have to interact with foreign authorities or the embassy in order to obtain information not provided on foreign personal documents. This creates a lot efforts for both the citizen and the involved civil servants. FASME intends to reduce these efforts significantly by digitalizing administrative procedures. It is a joint project of industrial and academic partners and various European municipalities and heads for generic solutions. Smartcards enable the citizens to obtain, store, transport and deliver personal documents in digital form. They can use them to apply for administrative services and to control the access of authorities to data, whether these data are stored on the card or in a remote data repository. Thus, Smartcards provide an electronic support for the interaction between citizens and authorities, which releases citizens from the burden of physically visiting different authorities and collecting and delivering personal documents in paper form to the authorities.

FASME pursues scientific, technological, and political objectives. Primary objectives are supra-organizational interoperability, exploitation of JavaCard & CORBA technology, and reduction of European border-barriers. Secondary objectives are gaining practical experience with state-of-the-art social engineering, visual prototyping for a better integration of users in the specification process, identification of social constraints, rapid prototyping including end-user testing, documentation with formal models, and quality management in international, interdisciplinary projects. FASME heads for a specification of generic JavaCard services with respect to inter-organizational administration procedures and the demonstration of the feasibility of these services by means of a prototypical implementation of JavaCard-based identity Cards for three European cities and three applications: change of place of residence,

¹ Partially supported by Swiss grant BBW 99.0045 FASME

change of car licence, and customized user portals. The overall evaluation of the project will focus on the quality of the resulting 27 uni-directional communication channels, where each channel corresponds to one application, one source and one target city for the migration process. Hereby, quality is evaluated with respect to security, usability, performance, choice of the degree of transparency, and on the overall resulting trust and confidence.

2 Why JavaCards?

JavaCards are more flexible than common Smartcards and provide scalpel-like security control on data access. On the one hand, they provide a straightforward, fine-grained tunable security management on the basis of access control. This enables a joint usage of the JavaCard infrastructure by different public or commercial providers of services. If the JavaCard is properly designed, the user is guaranteed, that applications, which she is interacting with by means of JavaCard can only read those data they are entitled to, and two different applications from possibly different providers cannot interfere with each other. On the other hand, applications on JavaCards may be easily uploaded, removed, or updated by the Card holder herself. Built-in security mechanisms to prevent unfriendly activities are easy to handle and difficult to break as long as the basic infrastructure is coded correctly. Thus, JavaCards may be used to keep different, individually chosen applications on one Card without additional risks for the owner and at very low management overhead costs. Furthermore, updates create no additional costs on the user side and little dissemination costs on the provider side. Moreover, JavaCard applications are coded with the JavaCard language subset of Java, and there are millions of SW-developers writing code in Java. Therefore, no Smartcard specialists are needed for the development of new JavaCard applications, once a framework – such as it is to be provided by FASME – is available. SMEs will not necessarily have to write their own framework, but can join an existing infrastructure. The flexibility of the JavaCard itself transfers to the flexibility of its economic usage and incurred implementation costs for JavaCard-systems are reduced likewise. Consequently, JavaCards offer new, very promising opportunities for SMEs in the Smartcard business sector.

3 Multi-Application Smartcards

Smartcards and in particular JavaCards offer the possibility that their owners control the access to their personal data. This creates new possibilities for the internetworking of different organizations on the level of processes. Personal data stay protected, when access to them is controlled by means of a JavaCard, and nevertheless, remote applications may access them upon a granting confirmation issued by the owner of the data. An integration of biosensors and cryptographic coprocessors further increases the quality of security control service provided by the Card. The Card then provides the following basic services: identification of the physical identity of the Card holder, transport of personal data and personal profiles on the Card, secure communication of personal data based on a public key scheme, and authorization of applications to access data based on digitally signed, time-stamped credentials. This is exactly what Card holders need to control access to their data, as long as they can trust the data management system, where data are stored. The latter is a *conditio sine qua non*, without which no data protection can be guaranteed.

The data security is guaranteed by a contract between the Card holder and the data management system, where the personal data are stored. This contract defines, how the Card holder can authorize an application to request for these data in effigy of the Card holder. Clearly, it must be impossible to guess this contract, not even from the knowledge of given contract. Thus contracts are encrypted authentication messages, which unambiguously identify the sender. The integration of the involved components on the Card ensures, that all processing is down on the Card. The main possible security bottleneck in this architecture is the Card reading

device, which is used not only for the interaction between the Card and an application, but also for the interaction between the Card and its owner via a GUI. One possible solution to overcome related problems is to provide TPEs at the municipalities, i.e. certified Black Boxes, whose internals cannot be read by the applications and which contain a user terminal, whose correct presentation of data is guaranteed. Another possible solution would be the usage of PDAs or mobile phones with equivalent reading functionality.

4 JavaCard Services for inter-organizational administrative processes

As a result of the analysis of user requirements in FASME, we have identified the following generic non-digitalized business scenario: First, a citizen provides evidence of her identity and of personal data with hard copies personal documents. Second, the citizen applies for a service, which comprises a change of personal data - possibly the creation of new data at the place of residence or the deletion of data (or marking of data as invalid) at the old place of residence - and the issuing of a corresponding document. Third, the civil servant checks the lawfulness and legitimacy of the request, possibly interacting with civil servants or services from other department (e.g. in Italy the police will check, whether the citizen actually lives at the stated new place of residence). Fourth, either the civil servant completes the service locally or she creates a document that confirms the correctness of data delivered by the citizen to the office in charge of the requested service.

Any such type of business process may be digitalized in the following way: First, the user is guided through the services according to the user profile stored on the Card. Second, authentication and part of the personal documents are supplied the JavaCard. Third, manual input of additional data is performed through a user interface, which is customized according to user preferences stored on the Card. Fourth, additional personal documents needed are fetched by the JavaCard application (running at the municipality) with an encrypted authorizing stamp issued by the JavaCard upon the citizen's consent and approval. Fifth, the application performs consistency checks and part of the legitimacy checks, while others parts still involve the civil servant. Sixth, the application requests for additional services from other authorities by means of an electronic document and also receives the results of these activities as an electronic document (compliant with the corresponding national standards). Seventh and finally, either the application sends a certified electronic request (for the services requested by the user) to the authority in charge of such services, or it performs the change of the citizen's personal data at the local data repository and possibly informs other authorities of this activity.

The digitalization of this type of administrative business scenario can be realized with an integrated JavaCard (including a JVM, a bio-sensor, and a cryptographic co-processor), a flexible XML standard for data exchange, i.e. an intermediaire data format, and local applications running at the municipalities, which execute the workflow defined by the conventional business process. In FASME, the application design relies on the CORBA technology, and in particular on CORBA services. The application creates context objects (based on the current pseudo-object), which are attributed properties during execution time of the workflow. Authorizing messages issued by the JavaCard are time-stamped in order to prevent misuse. There is no restriction of applicability of the generic services depicted to the public sector, as Commercial application with corresponding tasks may equally be realized that way.

5 The Basic Service Architecture

Our service architecture is based on a global intermediaire personal data representation format in XML for European citizens. In general, global data representations of citizens exist

only in parts and they are stored in physically and logically distributed data repositories. Local data representations of citizens, i.e. stored personal data, are called views if the format they are stored is compatible with the global intermediaire representation format. The latter is the case if and only if the data may be mapped bijectively onto a subset of the virtual global data representation of the citizen. There are three basic services in our service architecture: administrative services (like registration of a new place of residence or issuing of a car licence), the provision of trustworthy data, and the provision of trustworthy requests for trustworthy data. Trust and confidence in data is provided by the digital signature of a trustworthy principal. Further, secure communication is based on public key cryptography and trust in signatures is provided by 3rd party services.

The trustworthy data create a virtual market. The goods “traded” in this market are the signed data, whereby the value of a good is constituted by both the data itself and the signature creating trust and confidence in the data. Signing of data by a trustworthy principal thus creates value, which is determined by the party using these data. This is not only true for the business scenario we are working on in FASME, but for all business scenarios, where trust in data is needed. In our business scenario, however, all signed data are personal data, which are views of the virtual global data representation of the citizen.

On an abstract level, the administrative services can be described by a workflow, which starts with a signed request by the citizen, which ends with a signed confirmation by the civil servant (and the resulting changes of data in the data repositories of the involved authorities), and which comprises the provision of a defined set of trustworthy views of the citizen’s personal data. Each view is defined by a subset of the virtual, intermediaire, global representation and a trust requirement, which is represented by a list of trustworthy roles. Thus, any principal in a trustworthy role as confirmed by an appropriate 3rd party can fulfil the trust requirement by her digital signature.

The workflow is executed at a civil office in the following way: First, the JavaCard creates a signed request for the service. Then, the views are collected, whereby the trust requirements are fulfilled by the signatures of principals in trustworthy roles and the latter is checked by a 3rd party service. Finally, the application executing the workflow checks data consistency and then the civil servant provides her confirmation. This results either in the change of personal data at the local data repository of the authority (plus possibly messages to involved further authorities to perform the same) or in an electronic request to perform some service at a remote authority. The latter request is signed by the local authority thus creating trust in the correctness of the request plus the included data for the remote authority.

The views to be collected by the application executing the workflow may be provided in a trustworthy way by different instances. Part of them will be fetched from the local data repository of the authority (in which case no signing is needed), part of it will be provided by the JavaCard (either with signatures from other authorities or simply with the signature of the owner), part of it will be provided by the owner manually as input to the Black Box (and signed by putting his finger on the JavaCard, which then creates a digital signature), part of it will be provided by remote authorities. (Note that in our model, the confirmation of the living place by the police is considered as view to be signed by the police department). In case that a remote authority has to provide a view, the application realizing the workflow requests corresponding signed requests from the JavaCard, which are then sent to remote authorities and processed there.

Note, that in all cases indicated above the service pattern is the same. An application provides a trustworthy, signed view of the personal data of a citizen, based on a trustworthy signed

request. Thus, a service is characterized by a data view, the trust requirement for the request – usually the signature of the authority, to which the data are to be delivered and the citizen represented by the data -, and the trust requirements for the data view to be provided (which is the signature of the authority providing the service). In fact, signing of requests for trustworthy data views by the JavaCard realizes the same service pattern, too, since it is based on trust requirements of the JavaCard for its signature. When the JavaCard signs a time-stamped request for the personal data, it delegates its owner's rights to access these data for a certain period of time to the application realizing the workflow and this delegation of rights is based on the discussed contract between the Card holder the keeper of the data.

6 Business Technology

The main problems with ambitions like the one pursued in FASME is that requirements of different local cultures have to be satisfied. Smartcards solutions in scenarios like the ones discussed in this paper are successful only if the design is focused on the needs of the user, her knowledge, her abilities to deal with electronic applications, and her cultural background. Successful, innovative Smartcard projects demand an interdisciplinary engineering approach, which takes into account various different perspectives. In the following we discuss the basic perspectives of an interdisciplinary approach.

The *common user perspective* comprises the modeling of needs and constraints, the design of user user-to-system interaction processes and user interfaces, and the evaluation of results. It is focused on the *citizens* with needs, possibly constrained physical abilities, and a specific cultural, knowledge and life context. It has to be delivered to the project work by sociologists. They have to perform social constraints modeling and they have to contribute to the design of MVC model of the application (in form of constraints, monitoring of experimental interactions of trial persons with prototypes of the application) and to the design of the organizational prototype.

The *expert user perspective* comprises the modeling of the business process and organizational constraints. It is focussed on the *civil servants*, who have a practical knowledge of the actual administrative processes and who are aware of ongoing change activities and planning. It has to be delivered to the project work by civil servants – clerks and IT consultants - and academics and/or consulting experts on administrative business processes, who provide input to the design process in the form of use cases and conceptual UML contributions to the design of MVC model.

The *legal perspective* comprises the modeling of legal demands and constraints. It focuses on *citizens* and *civil servants*, who are involved in the actual execution of administrative processes (with a primary focus on citizens' rights). It has to be delivered to the project work by civil servants – juridical and data protection consultants – and sociologists, who have to provide guidelines to ensure a European-wide usage, with a particular emphasis on the implementation (user interface design!) of digital signatures and data protection.

The *cultural and sociological perspective* comprises the design of bootstrapping activities for the usage of the novel technological solutions. It focuses on the *citizens* and the *society as a whole*. It has to be delivered to the project work by sociologists, who have to identify identify the cultural differences and gaps by comparing new technologically controlled processes with traditional processes and who have to identify possible acceptance problems.

The perspective of *infrastructure engineering* comprises the prototypical development of basic components, namely

- ❖ *JavaCards* = integrated system of JavaCard VM, biometric sensor and cryptographic processor
- ❖ *Secure end user devices* = reading devices including a monitor, alternatively PDAs or TPEs; i.e. personally own HW/SW or publicly provided secure, certified Black Boxes with a user monitor, which take care of the communication between the JavaCard and the application.
- ❖ *JavaCard Middleware* = all communication facilities and protocols of the JavaCard covering in particular cryptographic issues.
- ❖ *General computing and communication infrastructure*

In the FASME project, the Card engineering relies on the support from industry (JavaCards and biosensors), consulting experts on system integration, and academic computer scientists, providing the infrastructure and its integration. The engineering of the secure end-user devices is based on available industrial products and the collaboration between academic computer scientists and industrial partners. The output of FASME will be Black Box model and its prototypical implementation. And the JavaCard Middleware is supplied by academic computer scientists and again supported by industry. The output of FASME will be a model and its prototypical implementations of a secure, lightweight communication between the JavaCard and the application.

The perspective of *SW-engineering* comprises the prototypical development of the application. It focuses on the *generic service model*, the *prototypical implementation* of the application, and the *integration with legacy systems*. The first has to be delivered to the project work by modeling experts (process and architecture modeling, data engineering, performance modeling), relying on the input of business experts and the feedback from SW-engineers. They have to come up with a joint, generic model (both informal and formalized) for the services, an intermediary data representation format, and the architectures implementing the services. In addition, a scalability analysis is needed. The second has to be provided by SW-engineers, who ought to rely on

- ❖ visual prototyping based on the conceptual business process models
- ❖ rapid prototyping (in the development of the 3-tier architecture from the first to the third tier) based on extensive tests including end-user tests, and
- ❖ a posteriori (sic!) state machine documentation

The integration with existing systems has to be done by database experts, who have to dock the applications to existing data management systems at the municipalities.

The perspective of *quality management* concerns the quality of the project as an engineering process and it comprises joint activity of all partners. This includes an a priori design and an updating of evaluation criteria (driven by user experiments), a final evaluation with respect to the evaluation criteria, and regular evaluations of the development process with respect to design, implementations, and formal models (specification and documentation).

Finally, the *economic* perspective comprises the analysis of the project risks, permanent market observation, the design of value chains, and the evaluation of the potential economic success and impact. It focuses on the *project in the market*. In FASME it is performed by the project management and an industrial partner in collaboration with all partners. Apart from conventional project risk analysis and market monitoring, risk analysis is also performed by way of the comparison of the results of the application requirement engineering with the business process requirements for four additional European municipalities.

As a consequence of the above considerations on the different perspectives of work, in FASME we have split the work into concurrent processes with well-defined interdependencies. The workplan neither reflects the different perspectives nor the

contributing expertise in a one-to-one manner, but combines them with traditional steps in an engineering cycle, as they would appear in a waterfall model. In principal, there are two different possible implementations of such a workplan: glueing all different experts needed to a working group together, or creating independent work-groups, which cooperate on the basis of well-defined interfaces. Due to the geographic distribution of project partners, there was no choice in FASME but the distributed engineering approach. Moreover, such an approach has also the major advantage that views are not unified, but exchanged on the basis of equality. This results in a broader horizon of the engineering then it would result in the case of the first choice.

Project success needs a quality management, but by the very definition of interdisciplinary work, there are no quality standards. (Emerging of quality standards would create a new discipline.) In order to tackle this intrinsic problem, first, a considerable amount of work has to be spent on the further development of evaluation criteria, and second, serialization of work has to be avoided. The final evaluation criteria will constitute a major outcome of FASME, as they are reusable know-how, which can be used to steer future projects in a similar area more successfully. And a true concurrency of work can guarantee a permanent interest of all participating parties in the project, which is needed for the evaluation of project results. Therefore, we have defined clear interfaces between the different work-packages and we have identified important information flow events across these interfaces as milestones. It is of essential importance, that the complexity of the internal interactions is located at these interfaces, and that information flows across these interfaces is documented persistently in a way which is accessible for all project partners. In FASME, the latter is realized with a web-based documentation procedure in the internal part of the FASME Web-site.

7 Conclusions

We have discussed the capabilities of JavaCard technology with respect to inter-organizational administrative processes. It is essential to understand the role signed, trustworthy data play in this process and how JavaCards enable citizens to control a secure data transfer. It results from our discussion that there is a very simple generic type of service which enables us to digitalize the administrative processes and that this type of service is not restricted to administrative applications, but it can be applied whenever trust in digital data constitutes a value. Any generic SW-solution for this service type is thus widely applicable. The true problem for the development of a SW/organizational solution are the cultural differences among different organizations. We have given a survey of a multi-disciplinary approach, which is capable of dealing with these cultural differences. Still, this remains a hard practical problem.

8 References

[1] www.fasme.org