

FASME – A STEP TOWARDS EUROPEAN E-GOVERNMENT SOLUTIONS

Niklas Auerbach

Department of Information Technology,
University of Zurich, Winterthurerstr. 190, CH - 8057 Zurich
Phone: +41 1 635 43 26 - Fax: +41 1 635 68 09
auerbach@ifi.unizh.ch

Nico Maibaum¹

Department of Computer Science,
Chair for Information and Communication Services, University of Rostock
Albert-Einstein-Straße 21, D-18059 Rostock
Phone: +49 381 498 3430 - Fax: +49 381 498 3440
maibaum@informatik.uni-rostock.de

ABSTRACT

The ongoing European integration on a political and economic level leads to an increasing mobility of European citizens. In this paper we describe the generic problems addressed by the European Research Project FASME (Facilitating Administrative Services for Mobile Europeans). We propose a citizen-centric civil registration process based on JavaCards and discuss cultural and technical problems that need to be addressed in interstate e-government solutions. The status quo of administrative processes in Europe, the electronic document handling concept and research implications of the FASME system architecture are considered.

1. INTRODUCTION

The ongoing European integration on a political and economic level leads to an increasing mobility of European citizens. More and more people live outside their home country and become migrants within Europe. Whereas high mobility of the workforce is a desirable property for a single European market, the mobile citizens have to face complex and time consuming administrative processes when moving from one member state to another. Addressing this problem necessitates creating an interstate e-government solution in the domain of citizen to authority e-government (Gisler and Spahni 2000).

A lot of countries have introduced national ID or citizen cards or will do so in the next years in order to give the citizen a digital communication channel with public authorities. These cards are mostly restricted smart cards in which data from a paper based ID card were transferred to its digital counterpart. They are not interoperable on a European level and often lack the flexibility to enlarge the functionality of the cards after the card has been issued. Furthermore, cardholder verification (CHV) keys, for example a four up to eight digits personal identification number (PIN), are the only access restrictions protecting the card's data.

¹ Supported by a grant of the Heinz Nixdorf Foundation and by the EU Fifth Framework Project FASME, IST-1999-10882, <http://www.fasme.org>

The European research project FASME – an acronym for Facilitating Administrative Services for Mobile Europeans – aimed at creating a user-friendly JavaCard based prototype system to help mobile citizens perform administrative tasks when migrating. The project was conducted within the Information Society Technology (IST) track of the 5th Framework Research program of the European Union.

The project consortium comprised researchers from different fields like computer science, social science, industry partners and six European municipalities. Requirements were collected from communal authorities in Belgium, Denmark, Germany, Great Britain, Ireland, Italy, and the Netherlands. The current status of the project is that a prototype has been implemented and an evaluation has been conducted. The FASME JavaCard as a component within an administration network serves as a profile bearing entity enabling an individual service support and also serves as a storage device for digital documents. Personal profiles are stored on the card in a secure manner and are used to provide a situation-guided and a life-episode-based service selection. The FASME services and the document handling and management system are based on the currently implemented systems in the corresponding cities.

In this paper we present generic problems addressed by the FASME system. We first explore the status quo of today's administrative processes and propose a citizen-centric civil registration process based on JavaCards. After that we present the architecture of the FASME prototype with special focus on the FASME JavaCard, the biometric fingerprint sensor, and the secure card extension. Based on this infrastructure we discuss electronic document handling and concepts for cross-border information transfers. Section 5 concludes the paper and gives an outlook on further research issues.

2. STATUS QUO: ADMINISTRATIVE PROCESSES IN EUROPE

When collecting the requirements for a cross-national and user-friendly administration system we had to face the problem of highly heterogeneous administrative cultures in different member states (Riedl, 2001a). Considerable differences are encountered in laws, cultural aspects and administrative procedures. In this section we point out some noteworthy differences between EU member states and describe the civil registration process in three European countries. Although other communal processes such as applications for parking permits were also researched we will focus in this paper on civil registration. This process exhibits features common to all administrative processes and constitutes a prime example of European diversity.

2.1. Civil Registration in Italy

The first administrative contact for mobile Europeans moving to Italy is usually the Anagrafe. The Anagrafe is a registry of inhabitants that is maintained on a municipal level. Currently around 8100 Anagrafes exist in Italy. Citizens moving to Italy have to report to this office and fill in a standardized form to declare their new place of living. This form is available in Italian only and can usually not be completed without the assistance of a clerk given that it contains questions on education, the economical sector of activity and other questions requiring the entry of dedicated codes. The new address is communicated to the local police office, which then sends an officer to check the given address. Upon address confirmation the entry in the Anagrafe can be finalized.

Various documents have to be presented by the citizen at the Anagrafe. Usually a passport, a residence permit (obtained from the police foreign office) and documents proving the civil status have to be presented. The current process does not seem to be citizen friendly and involves visits to several authorities and filling in forms that are not available in the citizen's mother tongue.

2.2 Civil Registration in The UK

Legislation in the United Kingdom does not know mandatory civil registration. Citizens do not have to register with the municipality they live in because the common point of view is that any citizen moving to the UK should have the right to stay anonymous. Therefore a civil registry, as it is known in continental Europe, does not exist. Only an Electoral Roll is maintained and a register of birth, deaths and marriages. This example shows that a wide range of administrative cultures exist in Europe, which poses an additional challenge to trans-European e-government solutions.

2.3 Civil Registration in Germany

The civil registration in Germany has most characteristics in common with its Italian counterpart. Registration is handled at community level and a permit from the Foreign Citizen Authority is a prerequisite. As in Italy, a passport and proof of civil status have to be presented. Again some cultural differences have to be considered: The police is not involved in the process and a German registration form does not ask for as many details. A further difference is that the form requires the citizen to declare the religious affiliation and we discovered that many Europeans find these questions objectionable, if not unacceptable. This example again illustrates the diversity in administrative cultures.

2.4 A JavaCard-based civil registration process

Because any scenario of moving from one member state to another involves presenting documents to an authority, a concept for handling digital documents and communication with local authorities had to be implemented. In FASME, a JavaCard serves as mobile access token to municipal services and guides the citizen through the administrative tasks. This section gives an overview of a redesigned smart card-driven civil registration process.

From a citizen's perspective the first step is to collect information on a particular process from the FASME kiosk – which is the administrative contact point for mobile citizens in the FASME system. The information available from the kiosk also comprises which documents have to be presented in order to successfully perform the administrative task. When moving to Italy this may be a birth certificate and proof of last place of living. After obtaining this information the citizen can now use the JavaCard to create a document request and to obtain a trustworthy digital copy of the required document in case the document is not stored on the JavaCard yet. The smart card in combination with biometrics guarantees secure access to digital personal documents.

As an example, for a citizen taking residence in a foreign country this may encompass a document request for a birth certificate to the registry of births, deaths and marriages. The citizen receives the document at the kiosk in digital form and may now store this document on the FASME card to use it in a registration process. Subsequently the citizen enters all necessary data into a form on the kiosk whereby situated guidance is given and context-sensitive help is provided. The multilingual graphical user interface of the kiosk enables the citizen to interact with the local authority in their mother tongue.

After submitting the digitally signed registration form and the required digital documents the task is routed to the civil servant. For the local authority there are no changes in the local processes – except that citizens submit their registration documents electronically. The civil servant decides on the registration case and informs the citizen of the outcome of the process.

3. ARCHITECTURAL OVERVIEW OF THE FASME SYSTEM

In this section we present a simplified framework of the complete FASME system infrastructure. It contains a structural description of the FASME system architecture which comprises hardware and software components and which includes middleware services. Furthermore, some selected components of the FASME system are briefly explained. This includes the citizen authentication, the FASME JavaCard, the biometric fingerprint sensor and the concept for the Secure Card Extension.

Technical as well as user requirements, constraints from data protection laws and discussions with specialists from European municipalities formed the fundamentals for the technical design. The FASME architecture contains an application server, a kiosk including a citizen terminal, a civil servant

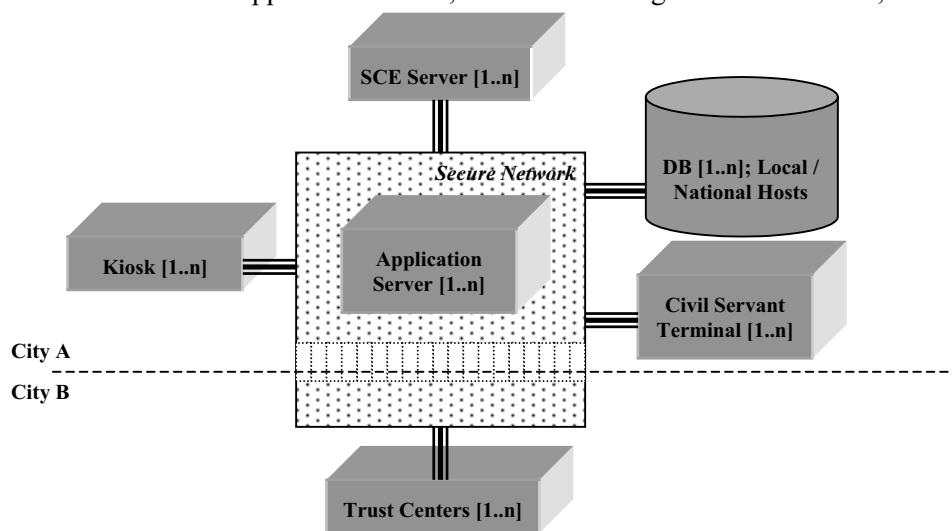


Figure 1: FASME Architecture

terminal, and the local or national legacy database(s). The FASME system is based on a public key infrastructure (PKI) where security including authentication, integrity, data confidentiality and non-repudiation is required. Furthermore, it includes a secure network and a network of Trust Centers, both being used to guarantee secure transactions between different locally or geographically distributed elements. An architectural overview of the FASME system is shown in Figure 1.

3.1 Citizen authentication

E-Government strongly requires authentication, and in contrast to human authentication in face-to-face government the whole authentication process has changed (Joshi et al. 2001). FASME uses biometric authentication instead of the usage of PINs or passwords. The FASME card will include a biometric fingerprint sensor in the future. The authentication takes place via something that “*I am*” (the fingerprint) and something that “*I own*” (the FASME card), and not something that “*I know*” (e.g. a PIN). The verification of the minutiae (patterns of the finger) will be done within the FASME card. The biometric data of the citizen will be enrolled on-card, will be stored within the card and will be verified by the card. Biometric information will never leave the card, and cannot be misused. Central databases with large sets of biometric information are prevented.

FASME supports different levels of authentication. If no authentication is required, the FASME card is more or less a simple key. If a low level of security is required, only an authentication between the card and the kiosk takes place. If this is not enough and a high level of security is required, the authentication takes place between the citizen and the FASME card and between the card and the kiosk.

3.2 The FASME JavaCard

The FASME card, which is in our case a JavaCard (Fünfroeken 1999), is a small, low-priced device, which everyone can carry in their pocket as a useful token for accessing administrative services. The card includes a Java capable processor in order to run Java cardlets (applets on a JavaCard), and a cryptographic co-processor for security issues. The JavaCard was selected as access token because of its flexible structure (re-engineering) and its support for a variety of strong security mechanisms. The JavaCard makes use of an object oriented software technology allowing reuse of existing components and state of the art engineering concepts. This leads to a reduced “time to market” for new applications. The JavaCard is the medium for the simple, secure, and safe transport of personal data.

The FASME card uses the cryptographic co-processor in combination with public and private keys for encryption and decryption of data and documents. This helps to ensure protection of privacy. Furthermore, a private key for electronic signature in combination with the fingerprint sensor enables qualified electronic signatures. This guarantees non-repudiation and authenticated data. Security algorithms used are based on the recommendations from the BSI². This includes among others 1024 Bit RSA public key encryption and decryption, 160 Bit support for the hash algorithm SHA-1 and signature services (Schneier 1996).

Within FASME different types of data exists:

- a.) Lasting information - partly to be updated during the card’s life cycle (persistent data).
- b.) Passing information (transient data).
- c.) Profiled information - a combination of lasting and passing information.

The FASME card contains user related information stored in the so-called FASME Data Set (FDS). This FDS is divided into three subgroups called public, private and secret FDS. The *public FDS* contains publicly accessible information data that is also visible on the cover of the JavaCard (e.g. names and expiry information). The *private FDS* contains additional data, partly stored on the cover, that are only available after a successful authentication of the cardholder. The *secret FDS* contains all data that must never be accessible from outside the card. Security-critical data such as private keys and biometric minutiae belong to this category.

3.3 The Biometric fingerprint sensor

In order to implement authentication three different models of authentication can be considered. First of all the authentication by something that “*I own*”. This can be a key, a magnetic card, a passport or a smart card. The second possibility can be achieved via authentication by something that “*I know*”. Examples are passwords, PIN codes or answers to personal questions. Authentication by something that “*I am*” is the last possibility. This is a biometric feature like fingerprints, iris scan, face and voice recognition and so on (Ashbourn 2000).

Within FASME a combination of something that “*I own*” (the FASME card) and that “*I am*” (biometric patterns) is used. Human recognition is replaced within our e-government system through biometric authentication (Pankanti 2000). Biometric identification serves the same purpose as a conventional PIN but makes the system more convenient to use and far more secure. Biometric fingerprint sensors eliminate the need to remember several different PIN codes and prevent the unauthorized use of a lost card.

In the FASME project the fingerprint sensor is used as an external device that captures the minutiae of the user and passes them on to the card environment where the matching takes place. In two to four years time the biometric fingerprint sensor will be integrated into the card. Biometric information of

² German Federal Office for Security in the Information Technology (<http://www.bsi.de>)

the citizen will be measured on the card, stored within the card and verified by the card. Secure biometric information will never leave the card. Whether biometrics or a PIN code or both shall be used is up to the decision of the citizen.

3.4 The Secure Card Extension (SCE)

The storage of a large set of electronic documents is often necessary in e-government applications. In the FASME project the citizen's profile information, the biometric information and private keys are kept on the card. Since today's JavaCards provide very limited storage (up to 32 k of EEPROM typically) a secure expansion mechanism was necessary to accommodate a possibly large number of electronic documents on the card. The Secure Card Extension (SCE) expands the normally limited memory of the JavaCard (similar to virtual memory) and provides virtually unlimited data capacities. The FASME card is the enabling device (identity key) to access the SCE and is the only gateway to this extension. Further information on the SCE can be found in (Cap et al. 2001).

4. ELECTRONIC DOCUMENT HANDLING

Analyzing today's civil registration processes, it becomes clear that procuring information and documents are the biggest problems to be handled by an e-government solution. Procuring, accessing and deploying documents must become a user-friendly and transparent process. In this section we discuss the challenges and a possible solution in form of an application system.

In order to facilitate civil registration it is necessary that the citizen can create digitally signed representations of paper-based documents and deploy them at will in an administrative process. Since we deal with mobile Europeans documents generally have to be procured from authorities in other member states thus necessitating a cross-border document transfer. This raises the question of requirements for such a transfer. From a theoretical perspective we concluded that an ad-hoc networking of governmental agencies was required, supporting the secure transfer of trustworthy and therefore time-stamped and signed documents. This view was also underpinned by the experience of administrative experts from the participating municipalities. A question that remained unanswered was the life cycle of administrative documents, i.e. questions relating to relevance and actuality within a given scope and the possible deployment of validation agents in such networks.

Digital documents were implemented using XML (www.w3c.org/xml) as markup language. XML is not only becoming a quasi-industry standard but this approach also enables the issuer of a document to integrate relevant context information into the digital representation. Furthermore, document type definitions (DTD) help all involved authorities to quickly check whether a document is well formed. XML turned out to be a universally accepted choice of technology for inter-administrational data exchange. Our choice was also confirmed by the fact that the UK has launched *Gov-Talk* (<http://www.govtalk.gov.uk>), an initiative aiming at creating XML schemas for all data exchange needs between British authorities.

4.1 Trans-border procurement of Documents

At the Kiosk – which is the administrative contact point for mobile citizens in the FASME system – the citizen collects information on the required documents. In a next step a document request is created. This involves identifying the issuing authority with guidance of the FASME Kiosk and then signing a formal request. The request is time-stamped and digitally signed with the help of the FASME Card that acts in effigy of the citizen. It has to be mentioned that the decision of accepting a request lies in the receiving authority as otherwise national laws may be violated.

Upon verification of the digital signature with the aid of a Trust Center the issuing authority will create a digital version of the required document. Discussions with experts from various authorities

have made clear that this process has to be fully automated not only to ensure scalability but also for economical reasons. Today's public key infrastructures may not always provide the prerequisites for such automation but the concept of unambiguously tying an identity to an ID-like JavaCard offers scope for automatic signature checking.

Any digital document issued by an authority must be delivered to the citizen in encrypted form and the receiver again must be able to establish the authenticity of the document. This is also true for any municipality that receives such a document as part of an administrative task. It is up to the civil servant to decide on the trustworthiness of the information contained in the document. Prototyping yielded the result that any administrative system must support authentication functions and shall therefore possess facilities to communicate with Trust Centers.

4.2 Inter-cultural Information Exchange

This still leaves the question open of how a civil servant from one country has to interpret a information that was provided by another country possibly using different ontologies (Eder and Missikoff 2001). In the following sections we discuss the open question of how information can be represented in electronic documents and what cultural problems arise in such an information transfer.

Data extracted from a database must be presented as a document in a format that is decoupled from the original system and can be interpreted by the receiver unambiguously. The underlying problem in this domain is that national systems differ widely in their ontologies (Oostveen and Van den Besselaar 2001). Municipalities across Europe often use different names for the same concept. As a consequence a representation has to be found that does not create a standard per se but nevertheless allows the transfer of administrative documents.

4.3 Intermediary Data Representation Format

Fully automated creation of electronic documents also means that data has to be retrieved from a database and converted into a given document format. Since the identity of the citizen can doubtlessly be established through the electronic signature this step is not posing problems. In contrast converting a document into a format that can be interpreted by all involved municipalities brought a number of interesting problems to light.

In the FASME system it was required that all digital documents could be generated automatically from existing databases. This not only necessitates integrating pre-existing database system into the e-government solution. It also creates a need for a data representation format that can be understood by all parties involved i.e. the participating governmental authorities. Although local initiatives like Britain's GovTalk exist we were facing a lack of standards for trans-national information exchange (Riedl, 2001b).

Standardizing datasets in civil registries across Europe is not a feasible solution. Due to the large number of legacy databases and organizational difficulties, standardization would fail. Instead the complex cross-border e-government information flow is implemented in FASME using an intermediary data representation approach. This implies a EU-wide applicable XML data format that can be translated to and from any local database. Adapting legacy systems to read and write this format is the responsibility of the local communities and a small burden compared to data set standardization.

For the actual mapping of the intermediary representation to local databases two approaches can be distinguished. The first approach is the EU-wide Data Representation that was chosen in FASME. For each top-level attribute, a unified data structure is defined which allows capturing attributes of all countries. In this case, for each country a mapping must be defined between the national and the international level, and vice versa. The advantage of this approach is that the number of mappings to

be defined is reduced. However, due to the different semantics (ontologies) of the attributes, each country has a slightly different mapping algorithm requiring n mappings for n participating countries.

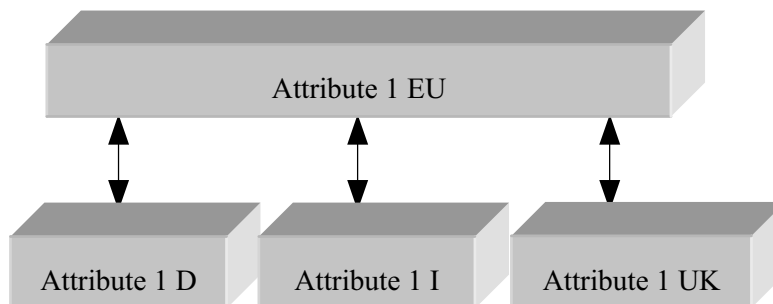


Figure 2: Intermediary data representation

Alternatively, bilateral data mappings can be considered. For each pair of two participating EU countries, an attribute mapping between the two countries is defined manually. In this case, for each member states a data translation scheme must be defined which means that every time a new country joins all countries must create a new mapping. This approach requires n^2 mappings for n participating countries.

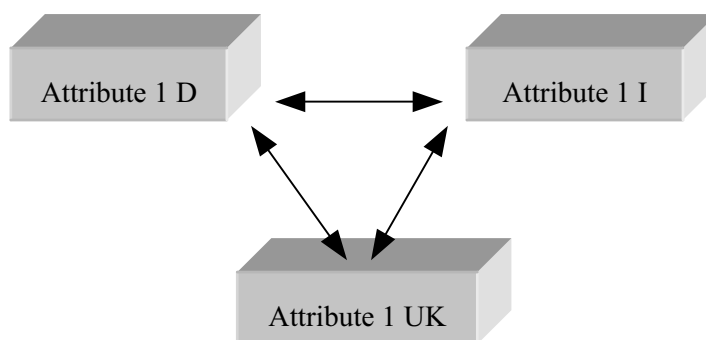


Figure 3: Bilateral Data mapping

The first approach was chosen for the implementation of the FASME prototype. Scalability, maintainability and reliability are easier achieved with a universal data mapping strategy. We perceive the intermediary representation format in conjunction with attribute-wise mapping to be currently the only feasible technical solution to the interoperability problem arising from the different ontologies in European administrative databases. The virtual ontology of a EU-wide namespace for attributes considerably reduces the complexity of the mapping problem. It has to be noted that this approach works in a distributed way and does not necessitate a centralized European data storage. Neither does it require the routing of all documents through a central conversion facility and therefore helps in protecting the citizen's privacy.

4.4 Future Research

We have presented an approach to inter-organizational digital document exchange in the administrative domain that is scalable and respects diversity in local administrative cultures. It might appear that the application logic and document handling described in this section are purely technological artefacts but a comparison with conventional ideas and evaluation with users from different countries have shown acceptance for the concept of a kiosk providing situated guidance through a document-oriented workflow and the entailing document service for remote access to relevant documents. Issues for further research can be frameworks for relevance and classifications for

context information of the involved documents. In the area of JavaCards the life cycle management of the citizen cards seems to be an area posing problems that are currently underestimated.

5. CONCLUSION

In this paper we have presented a framework to support migrating European citizens. We have discussed the central role of a digital document exchange as well as concepts for a possible intercultural information transfer. The FASME research project has shown that from a technical perspective registration processes without paper-based documents are feasible - provided a solution respects and preserves the cultural differences in Europe. JavaCards can provide safe access to personal documents and serve as access key for an ad-hoc networking of European authorities. The trustworthy exchange of digital documents constitutes in our view a core service for flexible e-government solutions and will be subject to further research. Although the social consequences of such a system would be immense they should be further discussed by interdisciplinary teams of researchers.

6. ACKNOWLEDGEMENTS

Part of the work underlying this paper has been funded by the European Commission in the Information Society Technology program under contract number IST-1999-10882. Partners in the project are the University of Amsterdam, the University of Cologne, the University of Rostock, the University of Siena, the University of Zurich, the City of Cologne, the City of Grosseto, Newcastle City Council, City of Den Haag, Telepolis Antwerpen, City of Naestved, Belfast City Council, ICL, Zuendel & Partner Unternehmensberatung GmbH and Zuendel & Partner Systems Consultants GmbH. The authors would like to thank the project partners for many fruitful discussions during the project and at workshops.

REFERENCES

- Ashbourn J.(2000). *Biometrics - Advanced Identity Verification, The Complete Guide*, Springer London, 1st Edition, London.
- Cap C., Maibaum, N. and Heyden, L. (2001). Extending the Data Storage Capabilities of a Java-based Smartcard, in *Proceedings of the Sixth IEEE Symposium on Computers & Communications ISCC 2001*, Tunisia, p. 680 – 685.
- Eder J. and Missikoff M (2001). Ontologies for Managing Knowledge about Forms for Government Processes. In *Knowledge Management in e-Government KMGov-2001*, Universitätsverlag Rudolf Trauner, Linz.
- Fünfroeken, S., Mattern, F. and Moschgath, M.-L. (1999). Die JavaCard als Programmier- und Ausführungsplattform für verteilte Anwendungen, in *Proceedings JIT'99*, 100-109.
- Gisler M. and Spahni D. (2001). *eGovernment – Eine Standortbestimmung*, Haupt Verlag, Bern.
- Joshi J., Ghafor, A., Aref, W.G. and Spafford, E.H. (2001). Digital Government Security Infrastructure Design Challenges, in *IEEE Computer*, 34(2), 66-72.
- Oostveen A. and Van den Besselaar P. (2001). Linking Databases and Linking Cultures, in *Towards the E-Society. Proceedings of the First IFIP Conference on E-Commerce, E-Business and E-Government*, Kluwer Academic Publishers, Boston.
- Pankanti, S., Bolle, R.M. and Jain, A. (2000). Biometrics: The Future of Identification, in *IEEE Computer*, 33(2), 46-49
- Riedl, R. (2001a). Document-based Interorganizational Information Exchange, in *Proceedings of SIGDOC 2001*, Santa Fe, 2001
- Riedl, R. (2001b). Interdisciplinary Engineering of Interstate E-Government Solutions, in *Proceedings of Fourth International Conference on Cognition Technology: Instruments of Mind*, Warwick 2001
- Schneier B.(1996). *Applied Cryptography*, John Wiley and Sons Inc, 2nd edition, New York.