

An Evaluated Certification Services System for the German National Root CA — Legally binding and trustworthy Transactions in E-Business and E-Government

A. Wiesmaier, M. Lippert, V. Karatsiolis, G. Raptis
Technische Universität Darmstadt, Department of Computer Science
Hochschulstr. 10, 64289 Darmstadt, Germany
[wiesmaie|mal|karatsio|raptis]@cdc.informatik.tu-darmstadt.de
Tel: +49 6151 164889, Fax: +49 6151 166036

This is a draft and will at least be subject to the following changes:
eliminate narrative description
more systematic analysis of the problem
more systematic description of the given case
inference to how to solve such problems in general
improve (merge?) chapters result and impact

This is a submission to IEEE'05. The presenting author is A. Wiesmaier.

Abstract: National Root CAs enable legally binding E-Business and E-Government transactions. This is a report about the development, the evaluation and the certification of the new certification services system for the German National Root CA. We illustrate why a new certification services system was necessary, respective which requirements to the new system existed. Then we derive the tasks to be done from the mentioned requirements. After that we introduce the initial situation at the beginning of the project. We report about the very process and talk about some unfamiliar situations, special approaches and remarkable experiences. Finally we present the ready IT system and its impact to E-Business and E-Government.

Keywords: CC-Evaluation, E-Commerce, E-Government, Global PKI, National Root CA

1 Introduction

The directive 1999/93/EC [Eur99] of the European Union obligates each member to operate a National Root CA (NRC). This spans national public key infrastructures (PKI) and enables legally binding digital signatures within the countries. Thereby it allows legally binding E-Business and E-Government transactions and thus raises trust in those transactions. By cross certifying the individual NRCs the E-Transactions become legally binding (and trustworthy) in an international context. If other continents follow, this will be the step to world wide legally binding E-Transactions.

According to §3 of the German digital signature act (SigG) [GFG01a] the German Regulatory Authority for Telecommunications and Posts (RegTP) is responsible for operating the NRC of Germany. On the first quarter of 2003 the RegTP launched a tender procedure to obtain a new IT system for its certification services. This was necessary to be prepared for new requirements that will occur.

Some of these requirements are related to the proceeding developments in cryptology. To reflect these developments the German Federal IT Security Agency (BSI) regularly suggests suitable cryptographic algorithms and associated parameters. According to the tender procedure, the new IT system must be able to adapt to these directives.

In parallel, the ISIS–MTT [TT04a] SigG–Profile [TT04b] was advanced to version 1.1. It addresses all technical requirements of the SigG and the respective ordinance (SigV) [GFG01b] based on the X.509 [IT97] and the corresponding PKIX [HPFS02] specifications. Conformance to these standards was another demand.

The compliance of the system with the SigG and SigV clearly was another requirement of the tender procedure. Therefore, the security concept of the overall system has to be certified. This includes the evaluation of parts of the system according to Common Criteria (CC) [Com99a] or the Information Technology Security Evaluation Criteria (ITSEC) [FGNU98].

A joint venture of FlexSecure GmbH¹, T-Systems² and Technische Universität Darmstadt³ won the tender. This paper reports on this project from the developer's point of view.

2 Our Tasks

We had to develop a suitable design for the overall system. To be able to do this we had to find out which requirements the SigG, the SigV and the ISIS–MTT profiles implied to our case. The overall design had to include the workflow, the software, the hardware, the environmental and the organizational issues.

We had to implement and prepare the software for a successful accreditation. As discussed in Section 4 this meant for us to evaluate the software to the required CC security level. This was a twofold task. On the one hand we had to produce software that can reach this level of evaluation. On the other hand we had to produce a lot of documentation that describes the system according to the CC.

Testing the system was another task of ours. Clearly, we had to test the software on correct functionality. In addition, we had to test it on security and robustness in order to prevent both intended and unintended misuse of the system. Changing the software after the evaluation point enforces a reevaluation. Thus, the testing had to be remarkable extensive. All tests were part of the evaluation procedure.

Lastly, the evaluated system had to be installed on the target platforms. Clearly this in-

¹<http://www.flexsecure.de/ojava/home.en.html>

²www.t-systems.com

³<http://www.tu-darmstadt.de/index.en.html>

cluded setting up the software on the computers. Furthermore, we had to configure the runtime environment to meet its special security requirements.

3 Initial Situation

When we started the project we already had a Trust Center (TC) software called FlexiTRUST. It is a component based system which supports all necessary tasks of a TC as registration, certification, key generation and publication of the respective products. FlexiTRUST was developed as a part of our academic work and thus had some experimental characteristics. The main design goals were the flexibility in changing the cryptographic algorithms and parameters, the flexibility to easily integrate it into existing workflows and the flexibility to scale to ongoing load demands.

FlexiTRUST was already successfully used in a variety of projects both in academic and business environments. Each project had different characteristics and requirements. However, none of the projects was comparable to the project described here. This project had a lot of entirely new aspects which were not covered by the original design.

FlexiTRUST neither had passed a certification process as demanded for an accredited certification services provider (CSP) nor an evaluation process according to the CC. Its security features never had to be at such a high level and had not been monitored in such a systematic way. Also its documentation was far from being sufficient for such a process. The evaluation and the certification processes themselves were entirely new and unknown to us.

FlexiTRUST already was compatible with the respective parts of the X.509 and PKIX standards families. It supported all necessary and commonly used optional extensions of these standards. But FlexiTRUST did not produce products conforming to ISIS-MTT respective its SigG profile.

The project schedule was extremely tight. The system had to be designed, implemented, tested, documented, evaluated, installed and certified within 6 months. Nevertheless we were confident to succeed as all parties (the developers, the evaluators, the certifiers and the customer) announced a high level of motivation and willingness for cooperation.

4 Process

The most difficult task of the project was to make FlexiTRUST fulfill the security requirements of the SigG and SigV within the given time. This became even more complex as we decided to evaluate the whole software to be able to benefit from the evaluation in other projects. The approach was to take the security concept as demanded by the SigG as the basis for deriving a security target (ST) for the evaluation process according to the CC. The FlexiTRUST system then was adapted accordingly and the necessary documentation was produced. As far as FlexiTRUST was concerned, the certification of the security con-

cept amounts to certifying the evaluation results. It soon became clear, that this approach would not succeed if we would take these steps sequentially as it is common practice.

The idea was to solve these tasks in parallel and in close cooperation with all parties. While the security target was developed together with the evaluating and the certifying authority, we already began to adapt our system to those requirements which seemed to be stable in the ST. In parallel to changing the software we also started to develop the high- and low level design documents. Whenever we finished a document, we immediately consulted the evaluator. Thereby we obtained three major advantages. Firstly, the evaluating authority very early gained an outline as well as detailed information about the structure of our system. Secondly, we could take their responses into account for the development of the other documents. Thirdly, by linking the requirements of the security target very early to our implementation, we got a better understanding of them. The last two points were especially valuable since we did not have any experience in evaluation processes.

Another challenge was to be conforming to the ISIS–MTT specification. Up to then we had no experience with it. In addition we had to adapt our software to the upcoming version 1.1 which was not yet stable. Furthermore, we had no client applications available to test against them. Our only aid was the ISIS–MTT test bed implemented by Secorvo Security Consulting GmbH. We had close contact to the ISIS–MTT group and our feedback even influenced the final specification.

We modeled the internal processes of this very high security IT system. Thereby it turned out that we had to adapt our system far more than we expected to. Besides implementing the new functionality we had to adjust the security of the internal communication, the access control management and the logging. Furthermore, we needed to adapt to already evaluated components as the key generator and the required type of smart cards. Also, the tailoring of the front–end components to the requirements of the RegTP caused some additional effort.

The development process did not resemble what we had faced so far. Usually we work at our office or at home most of the time being connected to the internet. According to CC the sources of FlexiTRUST had to be protected against unauthorized access. Now, we had to work in a dedicated access controlled area and on dedicated machines. The source code repository was off-line and each change to it was monitored and had to be signed by the developer and the responsible officer for the respective module.

We planned to adapt our software to third party cryptographic hardware with independent evaluations. We designed the respective interfaces in a way that allows the transparent substitution of those components. This prevents a reevaluation of the whole system in case of changing cryptographic algorithms or parameters. This was possible for the key generator. For the smart card and the card reader this plan had to be dropped, because the driver software was not deliverable in an evaluated version within the given time. Thus, the driver was evaluated together with our software. This is going to result in additional effort, when adapting to longer keys or different algorithms.

A crucial point was the decision, which security requirements to achieve solely with the FlexiTRUST system and which to delegate to the environment. A trade-of needed to be found between the time necessary to adapt FlexiTRUST and the flexibility gained or lost by

delegating them to the environment. We succeeded in keeping the effort for development and evaluation minor and gaining a high flexible system which can be used in other projects without reevaluation.

We needed to find, read and understand the important parts of the CC. It was very useful to be guided by the evaluating and the certifying parties. The first developer who had to write a certain kind of document took the hard way and learned it from the standards. The hints and the fast feedback of the evaluator as well as taking the common evaluation methodology (CEM) [Com99b] documents into account, helped to avoid mistakes, misinterpretations and dead ends. Now having the know how this developer was able to support the next team member in the same task. By this, knowledge spread quickly in the whole team. This speeded up the evaluation process considerably.

5 Result

The resulting system consists of three main components. One for certification, one for revocation and one for directory services.

The software is able to utilize arbitrary algorithms and algorithm parameters (e.g. the key length). All existing ones and even those who will be invented in future. Thus it is ensured to be able to always meet the cryptographic demands.

It is possible to host other Root CAs in parallel with the German NRC. Moreover the software is able to take over the directory services of closed certification service providers.

Its design allows FlexiTRUST to be embedded in existing workflows. It is based on components with each component being highly modularized. This allows the integration of the TC into arbitrary environments and the configuration to any special needs. The components can run together or being distributed over a network. The same is true for the modules of each component.

The flexibility in distribution leads also to a high scalability of the system. For low load applications it is suitable to run one instance of all necessary modules on the same computer. For high load applications it is possible to have many instances of the same modules run concurrently in the network sharing the load. All steps between really low load configuration and really high load configuration are possible.

There are two possibilities to run the system in a fault tolerant mode. One is distributing the modules like it is done for high load situations. If a computer in the network crashes the work of the dropped out modules can be done by the remaining modules of the same type. Another is installing the full set of modules two times in two different networks. This is done at RegTP. They have two full instances of the TC in different towns. They are connected and stay synchronized automatically. While the backup certification component is in cold standby the backup revocation and information services are in hot standby.

Even the level of security is adaptable. There are modules for high security applications (e.g. a NRC) which make use of evaluated cryptographic hardware and require strong operator authentication. But there are also modules for low security applications which

implement all features in software. There is a variety of reasonable combinations to reach different security levels.

The generated products and offered services are fully standards compliant. The Certificates (CRT) and Certificate Revocation Lists (CRL) are following the PKIX standard respective the ISIS-MTT SigG profile. The offered services use standard protocols as Lightweight Directory Access Protocol (LDAP) or Online Certificate Status Protocol (OCSP).

In November 2003 FlexiTRUST 3.0 Release 0347 was evaluated according to CC EAL3 augmented. The strength of the established security mechanisms is high. The CC certification report is [ccCa], the certificate can be found in [ccCb]. In December 2003 the software was attested to conform to SigG and SigV. The respective certificate can be found in [sig03].

6 Impact

The introduced certification service system enables global legally binding and therefore trustworthy transactions in E-Commerce and E-Government.

FlexiTRUST is installed as a NRC. It can be installed as NRC for other countries, too. Further it is possible to host foreign NRC within existing installations. Thus, FlexiTRUST enables international legally binding digital signatures. This is the basic requirement for legally binding E-Transactions.

FlexiTRUST is able to be used with arbitrary cryptographic algorithms and parameters. Thus it can always be adjusted to the ongoing cryptographic efforts. In addition this makes the TC suitable to be used with the Fail-Save-Concepts proposed by Maseberg [Mas02]. Due to these two points it is possible to ensure long term security. Thus long term non-repudiation for E-Transactions is possible.

Having a set of NRCs alone is not enough. The customers / citizens and the companies / civil services have to be equipped with certificates. This efforts that a small meshed network of PKIs has to be established. Those PKIs have to conform to the respective laws to provide an environment suitable for legally binding signatures. Small companies might be served with a few dozens of certificates. But the TCs of big corporate groups may have to deal with millions of certificates or must answer millions of status requests. And the services have to be guaranteed. FlexiTRUST can easily be installed at companies, civil services and other institutions as it can easily be integrated in the existing workflows. It is certified to fulfill the legal demands. In addition it is possible to install it in the whole range between low load and high load systems. The robustness of the system can be ensured by failover mechanisms. As we see, FlexiTRUST enables the area-wide participation of institutions and people in E-Business and E-Government.

Having all people and institutions participating in law conforming PKIs still is not enough. It must be ensured that each entity is able to communicate with each other entity. FlexiTRUST produces standard compliant products and offers standard compliant services. This guarantees a high interoperability and ensures that using the infrastructure

is easy and efforts only minimal training of the participants. Thereby it is possible to have comfortable E-Transactions between any entities.

By having legally binding long lasting signatures, an area-wide participation, a high interoperability and a comfortable usage the trust in and the acceptance of the infrastructure is raised. This addresses the most important issue on E-Business and E-Government. The people must be willing to execute E-Transactions.

References

- [ccCa] This reference will appear in the full paper.
- [ccCb] This reference will appear in the full paper.
- [Com99a] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation, 1999. <http://www.bsi.de/cc/ccplv21.pdf> (11 Nov 2004).
- [Com99b] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, 1999.
- [Eur99] European Union Parliament and Council. Directive on a Community Framework for digital Signatures; 1999/93/EC, 1999. http://www.e-podpis.sk/laws/eu.ep_dir93_1999.pdf (11 Nov 2004).
- [FGNU98] France, Germany, Netherlands, and United Kingdom. Information Technology Security Evaluation Criteria (ITSEC), V1.2, 1998. <http://www.bsi.de/zertifiz/itkrit/itsec-en.pdf> (11 Nov 2004).
- [GFG01a] German Federal Government. Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften. *Bundesgesetzblatt Jahrgang 2001 Teil I*, Nr. 22:876–884, 2001. <http://bundesrecht.juris.de/bundesrecht/sigg.2001/> (11 Nov 2004).
- [GFG01b] German Federal Government. Verordnung zur elektronischen Signatur (Signaturverordnung-SigV). *Bundesgesetzblatt Jahrgang 2001 Teil I*, Nr. 59:3074–3084, 2001. <http://bundesrecht.juris.de/bundesrecht/sigv.2001/> (11 Nov 2004).
- [HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. *RFC 3280*, 2002. <http://www.ietf.org/rfc/rfc3280.txt> (11 Nov 2004).
- [IT97] ITU-T. Information Technology — Open Systems Interconnection — The Directory: Authentication Framework. 1997. <http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.509> (11 Nov 2004).
- [Mas02] S. Maseberg. Fail-Safe-Konzepte für Public-Key-Infrastrukturen, 2002. <http://www.informatik.tu-darmstadt.de/ftp/pub/TI/reports/maseberg.diss.pdf> (11 Nov 2004).

- [sig03] Bestätigung von Produkten für qualifizierte elektronische Signaturen, 2003. <http://www.t-systems-zert.de/pdf/ein.02.sig.pro/zf.02096.d.pdf> (11 Nov 2004).
- [TT04a] TeleTrusT and T7-Group. Common ISIS-MTT Specifications for Interoperable PKI Applications — Core Specification, 2004. http://www.teletrust.de/Dokumente/ISIS-MTT_Core_Specification.v1.1.pdf (11 Nov 2004).
- [TT04b] TeleTrusT and T7-Group. Common ISIS-MTT Specifications for Interoperable PKI Applications — Optional Profiles, 2004. http://www.teletrust.de/Dokumente/CISIS-MTT_Optional_Profiles.v1.1.pdf (11 Nov 2004).