Summary of the Bachelor thesis:

Possibilities and restrictions related to implementing SPOC for EAC

Author: Joakim Kävrestad

In cooperation with Tomas Gustavsson and Anders Rundgren at PrimeKey Solutions AB.

About this document

This document provides an English summary of a Swedish bachelor degree thesis that examined how the standard of SPOC for EAC, provides support for interoperability between different implementations of SPOC. The work has been done by the author with much appreciated help from Primekey Solutions AB. All results presented in this summary, are results of the original study unless otherwise noted, and the contents are intended for readers with a basic understanding of concepts and protocols associated with electronic passports in general, and EAC and SPOC in particular.

The work covered in this document has been conducted at the University of Skövde and at PrimeKey's offices in Solna.

The full text thesis (written in Swedish) can be found as a downloadable PDF at the following URL: http://kavrestad.se/resourses/. For further questions about the thesis please contact the author at Joakim@kavrestad.se.
Table of Contents

Introduction and background................................................................................................................... 3
Related work............................................................................................................................................. 3
Research questions and method............................................................................................................... 3
  Research questions............................................................................................................................... 3
  Method................................................................................................................................................... 4
Specification analysis............................................................................................................................. 4
Interviews................................................................................................................................................ 4
Case study................................................................................................................................................ 5
Analysis of results................................................................................................................................... 5
Future work.............................................................................................................................................. 6
  Developing the SPOC standard............................................................................................................. 6
  Academic.............................................................................................................................................. 6
Introduction and background

This study analyzes possibilities and restrictions related to implementing SPOC for EAC so that different implementations can communicate with each other. This provides a system where multiple nations under different legislation have to cooperate in order for the system to work, bringing about several issues discussed by Tambouris et al. (2008). The study takes off in previous studies made on areas central to SPOC, as well as observations from a SPOC developer.

Conducted in three steps, the study begins with an analysis of the SPOC standard. The results of that analysis were used as input to the next step in which several people involved in developing SPOC were interviewed. Finally a case study, where an attempt to see whether or not it was possible to use elliptic curve cryptography in an interoperable environment, was made.

Related work

A professional working as a SPOC developer has observed several potential shortcomings in the specification of SPOC. Those shortcomings are believed to potentially cause lack of interoperability between implementations of SPOC and include that the standard is unclear on how some parts of SPOC is to be implemented. Several researchers including Vintila (2010), Kopajtic & Lusa (2003) and Egyedi & Dahanayaue (2003) address the fact that clarity is a very important property of a standard, in order to achieve interoperability between different implementations of that standard. In fact, Egyedi & Dahanayaue (2003) states that lack of clarity will likely cause different developers to interpret the standard in different ways, which in turn probably leads to lack of interoperability.

The developer also observed two technical aspects that may cause issues when implementing SPOC. Firstly, the standard does not specify what happens if a system sends a message to another system that is currently unavailable. Secondly, the standard requires that elliptic curve cryptography (ECC) is implemented in SPOC. In an article by Morales-Sandoval et al. (2011) ECC is described as an algorithm that can cause interoperability issues. Morales-Sandoval states that international standards provide unclear instructions on what parameters to use when implementing ECC. The topic is also discussed by Gutmann (2011) who describes that ECC for TLS is complex, since there are many different options to choose from when implementing.

Research questions and method

This chapter states the research questions and briefly describes the methods used in this study.

Research questions

The aim of this study is to answer the following question:

What possibilities and restrictions have to be considered when implementing SPOC for EAC? In order to clarify the research question, it is broken down into the following goals that will be achieved during the process of this study:
Show how the specification of the standard for SPOC affects the possibility to achieve interoperability between implementations of the specification.

Show which deficiencies concerning interoperability that can be expected between implementations of SPOC for EAC, and analyze the cause of those deficiencies, and how they can be prohibited.

Show possibilities and issues with the use of ECC in a SPOC environment.

**Method**

This study has been conducted in three steps. The first two goals were achieved by conducting an analysis of the specification itself and using the results from that study to perform interviews with individuals who work with SPOC development.

To achieve the last goal, a case study was performed with a single implementation of SPOC. Two instances of the implementation were used, and they were configured to use RSA and ECC for encryption in different scenarios. The goal was to show whether or not the use of ECC was at all possible in a SPOC environment. ECC was analyzed since the previous analysis and interviews indicated that ECC could cause interoperability issues.

**Specification analysis**

The analysis is based on the literature in the section “Related work” and resulted in a few areas that could potentially cause lack of interoperability between implementations of SPOC. Those areas were:

- The specification does not state what will happen if a message is sent to a system that is currently unavailable.
- The specification demands that all implementations of SPOC implement unclearly defined ECC.
- The specification demands that SPOC systems must be registered to each other in order to communicate, but does not specify how they should become registered.
- For SPOC to be useful, communication between SPOC and EAC must work, but the specification of SPOC does not describe how this communication should work.

**Interviews**

Using the results from the previous step, an interview was conducted with three individuals who work with development of SPOC systems. During the interviews the following questions were asked to all participants:

- The SPOC-standard declares that TLS must be used for communication between SPOC-systems. The standard also declares a number of cipher suites that can be used for
communication. In your professional opinion, does the choice of cipher suite propose interoperability issues? If you think it does, how do you suggest those issues can be counter measured?

• The SPOC-standard declares that all SPOC-servers must be registered to each other in order to communicate. However, the standard does not describe how the registration should happen. In your professional opinion, does this affect the possibility for SPOC-systems from different vendors to communicate, and if so, why? How do you think that the registration should be carried out?

• The SPOC-standard does not specify the internal communication between SPOC and the EAC-system that the SPOC-server supports. Does this affect the costumer’s possibility to choose SPOC and EAC-systems from different vendors?

• The SPOC-standard does not specify how to handle retries/resends of messages if the receiving server is unavailable. Do you think that this can cause interoperability issues and in that case what can be done to remove those issues?

In the answers to the first question, all participants said that the use of ECC could create interoperability issues, and one participant suggested the specification should provide a more precise guideline on how to implement ECC.

Based on the answers to the second question, the participants did not believe that the lack of a specified registration process could lead to interoperability issues.

Based on the answers to the third question, the participants stated that it is currently hard to use EAC and SPOC from different vendors, but that is not in fact a problem, since customers in practice uses SPOC and EAC from the same vendor.

Based on the answers to the fourth and last question, two out of three participants viewed the lack of retry/resend semantics, a huge issue concerning interoperability.

Case study

Finally a case study was conducted where two instances of a single implementation of SPOC was used to analyze if it was at all possible to use ECC in a SPOC environment. In this study the two instances were configured to use RSA and ECC for encryption in the following scenarios:

• System A: RSA, System B: RSA

• System A: ECC, System B: ECC

• System A: RSA, System B: ECC

• System A: ECC, System B: RSA
Communication were successful in all scenarios and therefore this case study generated a proof of concept for the use of ECC in SPOC.

Analysis of results

The aim of this study was to point out issues and possibilities in the specification of SPOC, that could cause lack of interoperability between different SPOC implementations. Based on the analysis of the specification itself and interviews with SPOC developers, it is clear that the specification does not define all the error handling needed to ensure interoperability over all implementations of SPOC. Also, it is indicated that the requirement of support for ECC could pose a problem, since it is not clear what options ECC should be implemented with.

However, as shown in the case study, it is evident that it is possible to use ECC in a SPOC environment, given that ECC is implemented in the same way on all of the communicating systems.

Finally the analysis indicated that the specification is not describing all vital parts of a SPOC environment, such as SPOC to EAC communication and SPOC to SPOC registration. However the interviews indicate that this is of minor concern.

Future work

This chapter is divided into two parts; future academic work including future studies that could be made, and what could be done in order to remove the issues that were identified in this study.

Developing the SPOC standard

In order to address the two issues that were discovered in this study the SPOC standard should be updated with:

- Clear specifications on how to implement ECC, so that all implementations of SPOC can use ECC that has been implemented using the same options.
- Rules for what should happen if data is sent to a system that is currently unavailable.

Academic

This work is, to the best of my knowledge, the first academic study to analyze interoperability between implementations of SPOC. Therefore this study could be seen as an overview of the subject, and more detailed future studies could be conducted to find technical issues that might cause interoperability issues. Also, the effects of having multiple nations trying to agree on a common system, could be investigated.
Reference list

Note that this list only covers a subset of the references used in the thesis.


