IRMA Assurer

Securely storing identity document chip data onto IRMA cards

Geert Smelt*

March 7, 2014

Kerckhoffs Institute
Supervisor: Bart Jacobs

When purchasing a restricted product or a service people are generally required to show a form of identification. Ideally you would like to share only the information that is required in order to be allowed purchase of the product or service. Showing an identification document generally reveals more information than is necessary. The IRMA card is a solution to this problem, as it allows revealing the bare minimum of information and keeping the rest a secret. Before this IRMA card can be used to share this information however, it needs to contain attributes that describe what you are. Copying the information that is already present on the chip embedded in identity documents is a good starting point for obtaining these attributes. This research aims to perform this process securely by applying strong cryptography.

*gasmelt@student.ru.nl

1 Introduction

IRMA, short for I Reveal My Attributes, is a project in which properties about you are stored on a smart card and can be verified by authorized parties. These properties are essentially pieces of information about what you are, such as your age, your social security number, your relatives; anything you can think of that applies to you. These properties, from here on called attributes, are stored on the smart card in such a way that you only have to reveal the attributes that are required to be known by the other party before receiving a service or purchasing a product. A classical example of this is the age verification before you are allowed to buy alcoholic beverages. Should you use a passport for age verification, the liquor store owner learns all attributes that apply to you and are printed on the passport. Should you instead present your IRMA card to a reader, only the attribute that states whether you are of legal drinking age is revealed to the store owner, who then allows you to buy liquor without ever learning your actual age. The IRMA project can be a solution to many such problems. For more information about the IRMA project, please see `https://www.irmacard.org/`.

2 Problem

One of the problems of passports and other identity documents is the fact that using them for identification generally means the identifier will have access to all information on the document, rather than only to the minimal required information. It is therefore benificial in terms of privacy to store these attributes on the IRMA card instead.

Document holders would not be able to store the attributes on the IRMA card themselves. For that they would need to go to a designated location, such as a town hall, where a notary would read out the chip in the identity document and store the information on the chip as attributes onto the IRMA card.

The goal of this research will be to create an application that can be used on NFC enabled tablets by these notaries to read out the chip embedded in people's identity document(s), verify the attributes learned from it and finally store the attributes securely onto the IRMA card.

The major challenge will be to design a communication protocol for verifying the attributes read from the identity documents. It is undesirable to have each notary's tablet contain a copy of the private key used for signing the verified attributes. The ideal scenario would be to have a centralized private key, held by the government, that is used for signing verified attributes and the notaries send verification requests. The research question therefore will be: "What is the most secure method to copy the information on the chip in identity documents as attributes onto the IRMA card?"

3 Motivation

Research on this topic is relevant because people are becoming more and more aware that their privacy is (almost) never guaranteed. Often one is required to submit a print copy of an

identity document with an application for a service, which in turn sometimes leads to identity fraud. The IRMA project is focused on privacy and therefore solves some of these problems. Before the IRMA card can be used to reveal attributes however, it first needs to contain some attributes. The information on the chip in identity documents is a good starting point for initializing ones IRMA card with attributes.

4 Theoretical Scope

The first objective of this research is to read the data on the chip in the identity document. For this the JMRTD application has been developed as a research project of the Digital Security group at Radboud University in Nijmegen [3]. There is also already functionality available to store credentials onto IRMA cards.

Gergely Alpár and Jaap-Henk Hoepman present a security model that includes mutual authentication using attributes [1].

Gergely Alpár and supervisor Jacobs provide the most important credential design principles [2].

Pim Vullers and Gergely Alpár present a method for efficient selective disclosure of attributes [4].

5 Strategy

My strategy is to first design a sound and secure protocol for the communication between a notary and the government's verification server. After that is complete, I am going to use the JMRTD project for retrieval of data from the chip on the identity document and use the new protocol to verify the data and sign it. Once I have the signed and verified data, I am going to store it as attributes onto the IRMA card.

6 Time Schedule

Table 1: Time Schedule

Week	**Activity**	**Deliverables** (submit-by date)
9	Meeting with supervisor	
10	Write research proposal Meeting with Ronny Meeting with IRMA project members	
11	Write research proposal	Research proposal

Continued on next page

Table 1 – *Continued from previous page*

Week	Activity	Deliverables
12	Meeting with supervisor Set up required programming environment	
13	Start designing a communication protocol	
14	Meeting with supervisor	Communication protocol
15	Start implementing protocol	
17	Meeting with supervisor	
21	Finish implementing protocol	Code
22	Meeting with supervisor	
23	Start writing paper	
25	Meeting with supervisor	Draft paper
26	Finish writing paper	Paper
27	Meeting with supervisor	
29	Start writing presentation	
30	Finish presentation	Presentation
31	Meeting with supervisor	

References

[1] Gergely Alpár and Jaap-Henk Hoepman. A secure channel for attribute-based credentials. In *Proceedings of the 2013 ACM Workshop on Digital Identity Management (DIM 2013), Berlin, Germany*, pages 13–18, November 2013.

[2] Gergely Alpár and Bart Jacobs. Credential design in attribute-based identity management. In Ronald Leenes and Eleni Kosta, editors, *Bridging distances in technology and regulation, 3rd TILTing Perspectives Conference, Tilburg, NL*, pages 189–204, April 2013.

[3] ICIS SoSGroup. Radboud University Nijmegen. JMRTD project, 2007.

[4] Pim Vullers and Gergely Alpár. Efficient Selective Disclosure on Smart Cards using Idemix. In Chris Mitchell et al., editor, *IFIP IDMAN. Springer Science and Business Media*, 2013.