Estonian Electronic Identity Card: Security Flaws in Key Management

Arnis Parsovs, *Software Technology and Applications Competence Center and University of Tartu*

https://www.usenix.org/conference/usenixsecurity20/presentation/parsovs

This paper is included in the Proceedings of the 29th USENIX Security Symposium.

August 12–14, 2020

978-1-939133-17-5

Open access to the Proceedings of the 29th USENIX Security Symposium is sponsored by USENIX.

Estonian Electronic Identity Card: Security Flaws in Key Management

Arnis Parsovs[1,2]
[1]*Software Technology and Applications Competence Center, Estonia*
[2]*University of Tartu, Estonia*

Abstract

The Estonian electronic identity card (ID card) is considered to be one of the most successful deployments of smart card-based national ID card systems in the world. The public-key cryptography and private keys stored on the card enable Estonian ID card holders to access e-services, give legally binding digital signatures and even cast an i-vote in national elections.

In this paper, we describe several security flaws found in the ID card manufacturing process. The flaws have been discovered by analyzing public-key certificates that have been collected from the public ID card certificate repository. In particular, we find that in some cases, contrary to the security requirements, the ID card manufacturer has generated private keys outside the chip. In several cases, copies of the same private key have been imported in the ID cards of different cardholders, allowing them to impersonate each other. In addition, as a result of a separate flaw in the manufacturing process, corrupted RSA public key moduli have been included in the certificates, which in one case led to the full recovery of the corresponding private key. This paper describes the discovery process of these findings and the incident response taken by the authorities.

1 Introduction

Estonia issues several types of credit card-sized identity documents (hereinafter – ID cards) that contain a smart card chip. The cryptographic functionality embedded in the chip enables secure authentication over the Internet and creation of legally binding digital signatures. The Estonian ID card roll-out started in 2002 and is considered to be one of the most successful in the world in respect to dissemination and active use. From the 1.3 million Estonian residents, 67% have used the ID card electronically at least once in the second half of 2018 [1].

The security of this electronic identity scheme depends on the secrecy of a cardholder's private keys. It is crucial for private keys to be generated in a secure manner and to be accessible only to the corresponding cardholder. In the Estonian ID card scheme, similarly as in many other countries, the key management (key generation, certificate issuance) is delegated to the ID card manufacturer. It is therefore essential to ensure that the manufacturer generates keys of good quality and does not store copies of the generated keys. Unfortunately, there are no effective controls to verify that the manufacturer is trustworthy and handles the key management correctly. The industry response to these concerns has been that manufacturers are in the business of trust and therefore they would never risk their reputation by engaging in sloppy security practices or malicious behavior.

Our contribution in this work is to show, by example of the Estonian ID card, that this trust model does not always work. We show that the ID card manufacturer has engaged in sloppy security practices, ignoring repeated signs of faults in the key management process, and has intentionally breached the ID card manufacturing contract in some cases creating copies of cardholders' private keys. While these findings have resulted in open litigation against ID card manufacturer Gemalto [2], there is no evidence that this loss of trust would have an impact on Gemalto's reputation or its business value and hence would have served as a deterring factor for such misbehavior.

Our findings are based on the analysis of the ID card public-key certificates collected over the years from the public ID card certificate repository. The findings are presented as three separate studies performed over different periods of time. For each study we present the context and describe the process of how the flaws were identified and handled.

First, we discovered that several ID card certificates shared the same RSA public keys. After further investigation we found that the affected ID cards also shared the same private keys. The discovery of duplicate private keys suggested that contrary to the security requirements, the ID card manufacturer had generated keys outside of the card. We obtained convincing evidence that most of the ID card keys had been generated in the card, while a specific set of keys produced in the ID card renewal process had been generated outside the card. Our conclusion is that this violation was likely motivated by performance reasons.

We also found a separate fault in the ID card manufacturing process that resulted in corrupted RSA public key moduli being included in the certificates. In one instance we were able to fully factorize the affected key demonstrating the security impact of the fault. We analyzed the possible causes for the corruption and discussed prevention and detection measures.

The rest of the paper is organized as follows. Section 2 introduces the Estonian ID card ecosystem and smart card chip platforms used over the years. Section 3 gives an overview of related security flaws the Estonian ID card has experienced. The next three sections describe the main findings of this paper. Finally, Section 7 concludes the paper.

2 Estonian ID card

2.1 Cryptographic functionality

From its introduction in 2002 until now, the core cryptographic functionality provided by the Estonian ID card has stayed the same. The ID card contains two asymmetric (RSA or ECC) keys with the corresponding X.509 public-key certificates, and symmetric keys to perform card management operations with the card.

Authentication key. The authentication key is used to log into e-services by providing a signature in the TLS client certificate authentication process [3]. This key can also be used to decrypt documents encrypted for the cardholder [4]. Signature and decryption operations with this key have to be authorized using the 4-digit PIN1 code.

Digital signature key. The digital signature key is used to give legally binding digital signatures that under eIDAS [5] are recognized as qualified electronic signatures. Each signature operation with the key has to be authorized using the 5-digit PIN2 code.

Card management operations. The cards are preloaded with symmetric keys that can be used by the manufacturer to perform various card management operations in the post-issuance phase. This allows to reset PIN codes in case the cardholder forgets them, generate new keys, write new certificates, and even reinstall the whole smart card applet if needed.

2.2 Parties involved

ID cards are identity documents issued by the state. The Police and Border Guard Board (Politsei- ja Piirivalveamet – PPA) is the authority responsible for procurement of ID card manufacturing services and the issuance of identity documents.

From the introduction of ID cards in 2002, the manufacturing and personalization of cards was performed by Trüb Baltic AS. In February 2015, Trüb Baltic AS with their parent company Trüb AG was acquired by Gemalto. As of the end of 2018, the ID cards have been manufactured by Oberthur (now known as IDEMIA).

The ID card certificates are issued by the privately-owned Estonian Certificate Authority (CA) SK ID Solutions AS (hereinafter – SK). According to eIDAS terminology, SK is a qualified trust service provider issuing qualified certificates. SK is a subcontractor of the card manufacturer.

The Estonian Information System Authority (Riigi Infosüsteemi Amet – RIA) is the state agency responsible for coordination and development of electronic identity and cyber security. Among other tasks, RIA organizes the development of ID card client-side software.

2.3 Chip platforms and document types

In this section, we chronologically introduce smart card platforms used over the years and the corresponding identity document types. We use the generic term ID card to refer to all identity document types covered. The SIM card-based digital identity card, in a Mobile-ID format, is not covered in this work.

2.3.1 MICARDO

In 2002, Estonia introduced the *identity card*, a mandatory identity document for all Estonian residents aged 15 and above. The electronic functionality of the card was implemented on top of smart card operating system MICARDO Public 2.1 [6]. The smart card interface is documented in the EstEID specification [7], which later became a national standard [8]. MICARDO-powered ID cards were issued from 2002 to 2011 (Figure 1). The platform is limited to 1024-bit RSA keys.

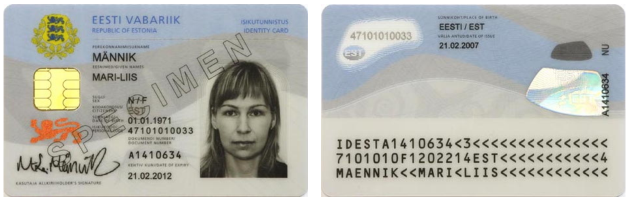

Figure 1: MICARDO-powered *identity card* issued from 2002-01-01 to 2010-12-31 [9]

2.3.2 MULTOS

In October 2010, a *digital identity card* was introduced. Since this document can only be used electronically, it can be personalized in PPA customer service points and issued instantly. The purpose of the *digital identity card* is to provide a backup solution in the event the cardholder's *identity card* cannot be used. The card is powered by MULTOS I4E platform by KeyCorp [10]. The MULTOS applet has been developed to mimic the MICARDO interface described in the EstEID specification. MULTOS-powered cards were issued until December 2014 (Figure 2). The platform is limited to 1024-bit RSA keys.

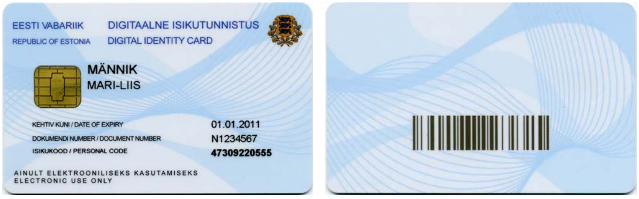
EESTI VABARIIK
REPUBLIC OF ESTONIA
DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD
MÄNNIK
MARI-LIIS
KEHTIV KUNI / DATE OF EXPIRY
01.01.2011
DOKUMENDI NUMBER / DOCUMENT NUMBER
N1234567
ISIKUKOOD / PERSONAL CODE
47309220555
AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY

Figure 2: MULTOS-powered *digital identity card* issued from 2010-10-01 to 2014-11-30 [9]

2.3.3 jTOP SLE66

In 2011, the manufacturing of *identity cards* switched to a new chip platform implemented on top of Infineon's product JCLX80jTOP20ID masked on a SLE66CX800PE chip [11] (Figure 3). The card runs jTOP (Java Trusted Open Platform) JavaCard operating system developed by Trusted Logic. The EstEID functionality is implemented in the JavaCard applet. The platform uses 2048-bit RSA keys. With the introduction of the jTOP SLE66 platform, the *residence permit card* was introduced (Figure 4). This card is issued to non-EU third-country nationals residing in Estonia. The jTOP SLE66-powered ID cards were issued until the end of 2014.

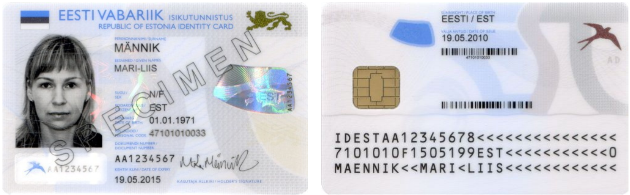
EESTI VABARIIK
ISIKUTUNNISTUS
REPUBLIC OF ESTONIA IDENTITY CARD
MÄNNIK
MARI-LIIS
SPECIMEN
N/F
EST
01.01.1971
47101010033
AA1234567
19.05.2015
EESTI / EST
19.05.2010
IDESTAA12345678<<<<<<<<<<<<<<<
7101010F1505199EST<<<<<<<<<<<0
MAENNIK<<MARI<LIIS<<<<<<<<<<<<

Figure 3: jTOP SLE66/SLE78-powered *identity card* issued from 2011-01-01 [9]

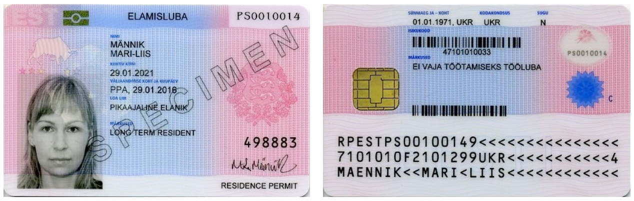

Figure 4: jTOP SLE66/SLE78-powered *residence permit card* issued from 2011-01-01 [9]

2.3.4 jTOP SLE78

At the end of 2014, the production of *identity cards*, *residence permit cards* and *digital identity cards* switched to jTOP SLE78 platform. The visual design of *identity cards* and *residence permit cards* stayed the same (Figure 3 and 4), however, the visual appearance of *digital identity cards* became a bit more colorful (see Figure 5). The EstEID functionality was implemented in a JavaCard applet on top of Infineon's product SLJ52GCA080CL [12] masked on the SLE78CLX800P chip [13] that runs the jTOP JavaCard operating system developed by Trusted Logic. With the switch to jTOP SLE78 platform, the *e-resident's digital identity card* was introduced (Figure 5). This card is issued through the e-Residency program [14] to persons who are not residents of Estonia. In the beginning of 2017, the *diplomatic identity card* was introduced (Figure 6). This card is issued to persons with diplomatic status. Initially, the jTOP SLE78 platform used 2048-bit RSA keys, but due to the ROCA flaw (see Section 3), at the end of 2017, the switch to ECC keys using curve P-384 was made. The jTOP SLE78-powered ID cards were issued until the end of 2018. ID cards manufactured currently are powered by the chip platform supplied by IDEMIA (not covered in this work).

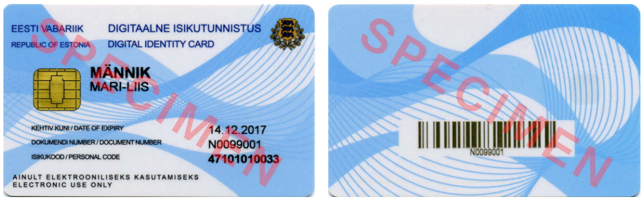
EESTI VABARIIK
REPUBLIC OF ESTONIA
DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD
SPECIMEN
MÄNNIK
MARI-LIIS
KEHTIV KUNI / DATE OF EXPIRY
14.12.2017
DOKUMENDI NUMBER / DOCUMENT NUMBER
N0099001
ISIKUKOOD / PERSONAL CODE
47101010033
AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY
SPECIMEN
N0099001

Figure 5: jTOP SLE78-powered *digital identity card* and *e-resident's digital identity card* issued from 2014-12-01 [9]

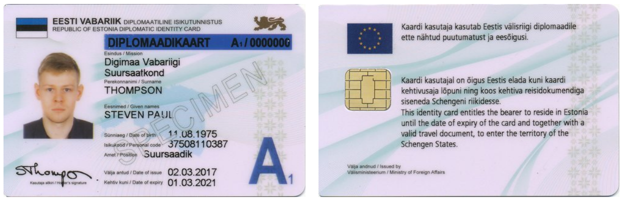
EESTI VABARIIK
DIPLOMAATILINE ISIKUTUNNISTUS
REPUBLIC OF ESTONIA DIPLOMATIC IDENTITY CARD
DIPLOMAADIKAART
A / 0000006
Digimaa Vabariigi
Suursaatkond
THOMPSON
STEVEN PAUL
SPECIMEN
11.08.1975
37508110387
Suursaadik
02.03.2017
01.03.2021
A1
Kaardi kasutaja kasutab Eestis välisriigi diplomaadile ette nähtud puutumatust ja eesõigusi.
Kaardi kasutajal on õigus Eestis elada kuni kaardi kehtivusaja lõpuni ning koos kehtiva reisidokumendiga siseneda Schengeni riikidesse.
This identity card entitles the bearer to reside in Estonia until the date of expiry of the card and together with a valid travel document, to enter the territory of the Schengen States.
Välisministeerium / Ministry of Foreign Affairs

Figure 6: jTOP SLE78-powered *diplomatic identity card* issued from 2017 [15]

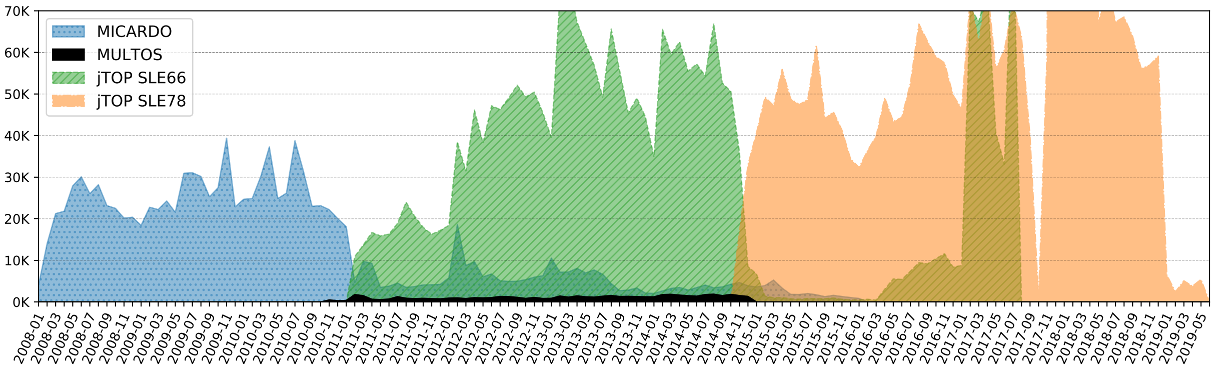

Figure 7: ID card certificates analyzed in this work (by issuance month)

2.4 Certificate repository

All valid ID card certificates issued by SK are available in the public LDAP directory `ldap://ldap.sk.ee` [16]. The publication of certificates is motivated by the document encryption use case, providing convenient means for senders to obtain public keys of recipients.

ID card certificates contain the cardholder's full name and personal identification code (personal ID code). The personal ID code is a unique 11-digit number that generally remains fixed for the lifetime of the person and therefore is widely used in public and private databases to identify persons. The validity period of the certificate usually corresponds to the validity period of the identity document in which the corresponding private key resides.

2.5 Certificates analyzed in this work

Over the years, we have collected more than 7 million ID card certificates published in LDAP certificate repository. The certificate search in the repository is restricted to the personal ID code. However, since the search space for all possible personal ID codes is relatively small, over time certificates of all possible personal ID code holders could be crawled. Our certificate dataset is not complete, but we believe that it contains a representative sample of ID card certificates issued throughout the years. Figure 7 shows the distribution of ID card certificates in our dataset by issuance month (based on the certificate's `notBefore` field[1]) for different ID card platforms. The corresponding platforms have been determined by the certificate fields and properties of the public keys. Due to the crawling process, the dataset lacks certificates issued from 2002 to 2007 and certificates which have been valid for a short period of time. Therefore, in general, our findings provide only a lower bound for the number of affected certificates.

We also collected certificate revocation information accumulated in publicly available CRLs [17]. The information in CRLs can be used to deduce the time when the cardholder visited the document issuer to receive their new ID card and the old one was revoked. This information and also some other peculiarities of the ecosystem allowed us to deduce many important insights for this study.

3 Related work

Over the 17 years of the Estonian ID card history, several ID card-related security flaws have been publicly disclosed.

More than 700 000 ID cards powered by the jTOP SLE78 platform were affected by Infineon's RSA key generation flaw (the ROCA flaw) [18]. The vulnerability in Infineon's proprietary RSA key generation algorithm allowed the factoring of 2048-bit RSA key in only 140.8 CPU-years. The discovery of this flaw in 2017 started the so-called Estonian ID card crisis, which was mitigated by switching to the ECC algorithm implemented by the platform and revoking vulnerable RSA certificates [19].

Publicly less noticed was a flaw in the jTOP SLE66 ID cards issued in 2011. Due to a publicly undisclosed flaw in EstEID JavaCard applet developed by the ID card manufacturer, 120 000 ID cards issued in 2011 were recalled [20]. While the authorities claimed that the card is secure and all transactions made with the card are fully reliable [20], later after the ROCA flaw broke out, it was disclosed in the media that the flaw in the 2011 ID cards was exploitable by having access to the card [21]. The context indicates that this may have been a type of PIN bypass flaw.

In 2002, it was discovered that PIN codes were printed in too dark, allowing for them to be seen through the PIN envelope [22]. Ironically, the same flaw in PIN envelopes was reintroduced by IDEMIA in 2018 after taking over the manufacturing of ID cards [23].

There have been incidents of including duplicate email addresses in certificates [24], issuing certificates with incorrectly encoded public keys [25], failing to revoke certificates of deceased persons [26] and others. Detailed analysis of these and other flaws related to the Estonian ID card are covered in [19].

[1] The `notBefore` field represents the time at which the certificate starts to be valid and usually corresponds to the time when the certificate was issued.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**