Republic of Estonia
Information System Authority

ROCA Vulnerability and eID: Lessons Learned

State-issued and backed electronic identity – the Estonian ID card, with its mobile ID and digital ID additional tokens – is among the pillars of Estonia's digital ecosystem. The functioning of Estonian digital way of life depends on the digital signature having equal status to a handwritten signature and the possibility of electronically authenticating oneself. In addition to citizens of Estonia, the card is also used by legal residents, e-residents and diplomats posted in Estonia.

On the evening of 30 August, 2017, a researcher with the Centre for Research on Cryptography and Security at Masaryk University[1] notified Estonia of a the security vulnerability on the chips used in the Estonian ID card. According to the analysis by the research group, the vulnerability, internationally known as ROCA (Return of the Coppersmith Attack), affects RSA cryptographic keypair generation in chips produced by one of the leading manufacturers, Infineon. Infineon, in turn, is a supplier for the Estonian ID card vendor Gemalto (operating as TRÜB Baltic). Over a billion chips were impacted globally, among them those used on Estonian ID cards issued since autumn 2014.

Theoretically, the security vulnerability could have allowed the private key (which is used for authentication and signing) to be calculated from the public key – in theory, making it possible to clone the victim's cryptographic keys and use them for authentication, sign or decrypt documents even without being in physical possession of the card.

Exploiting the vulnerability would not have been easy or inexpensive, and there were no known cases of successful exploitation of the ID card or similar chips. In fact, no such cases were known by the time Estonia revoked the affected certificates.

Besides a person's public key, an exploit would also have required significant expertise in cryptography, custom-made software and remarkable computing power, estimated to cost up to USD 80,000.

WHAT ELSE DOES THE ROCA SECURITY FLAW AFFECT?

Estonia's 800,000 ID cards with the security vulnerability in question make up a negligible share of ROCA's global impact. An estimated minimum of 1 billion affected chips are used around the world in a variety of computing devices and on plastic cards. The Infineon chips that led to the vulnerability in the Estonian ID cards are used in driving licences, passports, access cards and elsewhere.[2]

The identity documents of at least 10 countries were affected. Chips with the same flaw are known to have been used in identity documents in Slovakia, Austria, Poland, Bulgaria, Kosovo, Italy, Taiwan, Spain, Brazil and Malaysia. In Spain alone, the vulnerability affected 17 million cards. However, the other countries depend less than Estonia as the ecosystem of e-services is far less lively.

Trusted platform modules. TPMs are the basis for modern computers' security architecture. The vulnerability is known to affect at least Lenovo, HP, Toshiba and Fujitsu computers. TPMs are primarily used in enterprise client computers, so home users are generally not impacted. For example, in Microsoft Windows, a TPM protects BitLocker disk encryption and other security mechanisms in the operating system. Microsoft issued a temporary patch through Windows Update that essentially replaces the TPM with a software solution and other manufacturers have released similar patches.

Security tokens or authentication devices used for virtual private network (VPN) access, email security and other critical security operations. Of these, at least Gemalto and Yubico products were affected, with Yubico replacing the defective products at its own expense.

It is possible that some **payment cards** with chips are also vulnerable.

1 https://crocs.fi.muni.cz/
2 https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf

At the same time, it was evident that, if the certificates remained valid, the risk of exploitation would increase significantly as soon as the methodology used by the research group became public.

Due to the large number of the digital certificates affected and their broad use in both state and private sector services, revoking the cards would have meant extensive impact to the availability of or access to digital services – such step would have disrupted the use of e-health systems, the digital services of Tax and Customs Board and government document exchange platform as well as financial transactions. Work at and between government agencies would also have been disrupted. The security flaw did not affect mobile ID, but that alternative token was used by only slightly more than 100,000 people at that time, and a number of digital services did not support it.

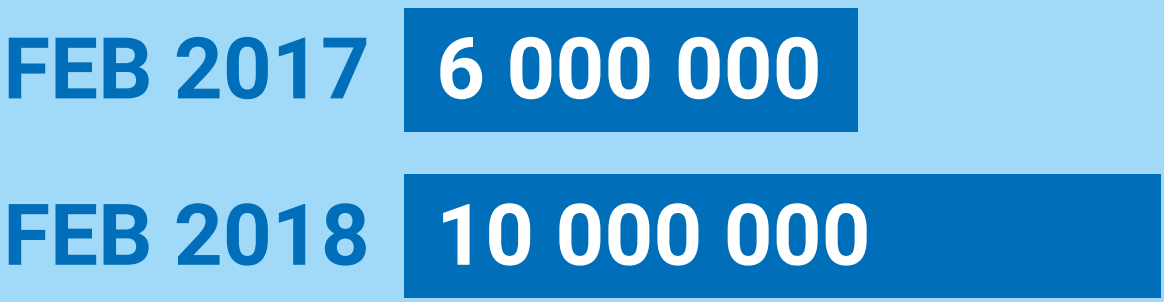
The solution to the situation had to restore the security of the ID card without affecting the availability of services. In essence, the Estonian Information System Aythority found themselves in a race against time in early September, looking for a new secure solution with the Police and Border Guard Board and other partners, and preparing to implement it while knowing full well that sooner or later, the affected certificates would have to be suspended.

The crisis management team made the decision early on to be transparent in its public communication. This step cut potential speculations and allowed to focus on finding a fix to the problem itself. Ultimately, it meant that the new solution – based on elliptic curve cryptography (ECC) instead of an RSA library – was available before Estonia needed to suspend the affected certificates. Moreover, user confidence was maintained and electronic services remained available. For example, a record number of Estonian people (31.7% of all voters) i-Voted in the October 2017 local elections. The number of transactions performed using ID cards remained at a normal level in the days and weeks that followed and the trust in eID was not corroded through the process. To compare: 6 million digital signatures were given in February 2017 and 10 million were given in the same month in 2018.

Estonia is unique in that it offered the possibility of updating certificates remotely – people were able to update their ID card software from any computer connected to the internet and equipped with an ID card reader – as well as the possibility of suspending the affected certificates.

Estonia is unique in that it offered the possibility of updating certificates remotely – people were able to update their ID card software from any computer connected to the internet and equipped with an ID card reader – as well as the possibility of suspending the affected certificates. Other national authorities in a similar situation did not have these two possibilities and had to find a way to issue new ID cards or update the existing ones at government service offices.

DIGITAL SIGNATURES USING ESTONIAN ID CARD



THE ESTONIAN ID CARD: A UNIQUE PLATFORM

- **1,295,844** valid ID cards, of which 26,199 e-residency cards in a total 142 countries (2018)
- First document signed with ID card on **7 October 2002**
- Almost 500 million digital signatures and over 670 million authentications as of May 2018
- **747,580** ID cards are used electronically at least once a year; about 42,000 people use their ID card digitally at least one hundred times in a three-month period
- The Estonian Information System Authority (RIA) is responsible for the digital elements on the ID card since 2016. As an identity document, the card remains in the jurisdiction of the Police and Border Guard Board. The certificates for the ID card are issued by SK ID Solutions AS
- The 2017 Emergency Act specifies authentication by ID card and digital signature as a **vital services**
- Estonia was notified of a cryptographic weakness in late summer 2017; it made the ID card theoretically vulnerable and affected approximately **800,000 cards** issued since October 2014
- The (remote) **updating** of the ID card – the replacement of the certificates with new ones – became possible on 25 October 2017
- The faulty certificates were **suspended** on 3 November 2017
- The faulty certificates were **revoked** on 1 April 2018 and could no longer be updated. **94%** of ID-cards that had been electronically used were updated; of the 494,000 ID cards that were renewed, 354,000 were updated remotely
- As of the end of 2017, 160,000 people were using mobile ID and 140,000 were using Smart-ID

How to Be Better Prepared for the Next Vulnerability

The ID card security vulnerability illustrates how much societies depend on fundamental digital infrastructure. In Estonia, the crisis management efforts underscored the need to review specific processes – among them administration of the ID card, risk assessment and mitigation as well as inter-agency cooperation. Given the global nature of the vulnerability, conclusions need to be drawn internationally across the public and private sector.

Information sharing and vulnerability disclosure. The anticipated sources of information – international notification mechanisms and notification from vendors – failed Estonia this time while information provided by an international group of researchers allowed to address the issue. It was felt that the notification mechanisms are designed for incidents with demonstrated impact and thus not well-suited to address vulnerabilities in earlier stages of crises. The case allows to revisit both supply chain management and notification mechanisms. In particular, EU Member states might want to compare interpretation and the emerging practice of Article 19 of the eIDAS regulation. Overall, the possible gaps in notification mechanisms have to be assessed and national practice of international risk and vulnerability sharing addressed in a joint manner.

Risk management and continuity planning. In Estonia, ID card is means of authentication and electronic signing for close to 5,000 public and private sector services. In most of these cases, the option of face-to-face authentication and handwritten signatures is no longer an acceptable alternative. Therefore, electronic alternatives to the ID card are being developed and integrated into services. For other governments and private companies, this serves as a useful case of risk management and continuity planning. Even with remote updating and certificate suspension being available, Estonia would have been much more severely impacted if there were not several crypto libraries embedded in the firmware of the ID card.

Role of governments in introducing innovation. Government agencies constantly face the dilemma of developing technology in-house versus procuring innovation from the market. Few governments possess the entire necessary skill sets; most of the competence lies in the private sector. With globally used technologies, governments cannot fully solve problems inherent in technologies they are merely a customer of. In addition to supply chain management and business continuity planning, governments can also pool their influence in developing, procuring and certifying technology.

Openness. Risks arising from vulnerabilities in fundamental digital infrastructure cannot be managed without the involvement of the stakeholders, including the public and the media. Broad-based cooperation between national, international and corporate stakeholders with different expectations, roles and levels of readiness is a sine qua non. Furthermore, only such cooperation can lay basis for long-term solutions that allow to overcome problems not yet seen beyond the horizon.

TIMELINE: ROCA VULNERABILITY AND ESTONIAN ID CARD

30 August 19:35	A member of an international cryptography research group sends CERT-EE an official notification regarding a security vulnerability associated with Infineon chips that affects Estonian ID cards. The risk lies in a vulnerability of a cryptographic library used in RSA keypair generation.
31 August	Estonian Information System Authority (RIA) confirms the possibility of the vulnerability in preliminary assessment. The Police and Border Guard Board (PPA) and the Ministry of Economic Affairs and Communications are informed.
1 September	The Minister of Economic Affairs and Communications is briefed on the matter. RIA involves external technical experts as well as partners from the government and private sector (Cybernetica, Nortal). The heads of institutions convene, a strategic crisis management team starts to form.
3 September	The Prime Minister and other ministers involved meet. RIA and PPA working groups assess scenarios and impacts to make recommendations.
4 September	The Government of the Republic holds an extraordinary meeting. PPA with RIA and other agencies form a media and strategic communication staff. Private and public sector stakeholders like banks and telecoms are notified. Public access to the certificate database (LDAP) is closed.
5 September	The international partners are notified of the vulnerability. The Prime Minister, Minister of Entrepreneurship and Information Technology, and the directors general of RIA and PPA hold a joint press conference to inform the public. An information gateway is opened at www.id.ee and kept updated, in cooperation between RIA, PPA and SK ID Solutions.
September	Working groups focusing on technical solutions, crisis management, legal aspects and communications meet regularly. Other institutions and other external experts are called on as needed.
5-11 October	Municipal elections are held. The elections see a record participation among internet voters. Those voting over the internet make up 31.7 per cent of all participants – slightly higher than in past elections.
16 October	The global impact of the vulnerability becomes apparent: Microsoft, Google (Chrome OS), Yubico, Gemalto and a number of larger computer manufacturers (Lenovo, Fujitsu) release security reports.
25 October	The issuing of new ID cards that rely on ECC encryption algorithm begins. The testing period for the online updating of Estonian ID cards begins. Over six days of testing, close to 20,000 ID cards affected by the vulnerability are updated.
30 October	The research paper[3] by the international group of cryptographers on the vulnerability in the RSA encryption library is published.
31 October	Card holders are called on to update their cards. Demand for the service is high, resulting in downtime of the remote updating solution. Systems stabilise by 2 November. Slovakia revokes 60,000 certificates with the ROCA vulnerability, and the card holders have to apply for new cards.
1 November	Spain revokes a total of 17 million affected cards.
2 November	The research is presented in full at an academic conference in the US.
3 November	Certificates on a total of 740,000 affected Estonian ID cards are blocked, but the cards can be updated online to make them electronically usable again. In addition, PPA opens additional service offices to update certificates.
5 November	Service usage statistics show that the suspension of the affected certificates did not result in a drop in the digital use of ID cards. Digital transactions by e-residents have increased.
End of 2017	A total of 400,000 ID cards updated. The number of mobile ID and Smart ID users and their level of activity have increased.
February	RIA commissions a Tallinn University of Technology research group for a neutral synthesis of the lessons learned.
5 February	RIA's eID domain manager Margus Arm and PPA's Kaja Kirch, head of identity management at PPA, receive state decorations.
1 April	Certificates that have not been updated are revoked and can no longer be used electronically. 94% of ID-cards that had been electronically used have been updated.
9 May	RIA hosts an international conference on lessons learned from the ROCA vulnerability.

2017

2018

[3] https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf