LESSONS LEARNED:

Estonian ID-card

The electronic identity (eID) is a crucial cornerstone of the Estonian digital ecosystem. The ID-card, as its physical manifestation, is a means of authentication and electronic signing for about 5,000 public and private sector services. Over 99% of Estonians have an ID-card and 70% of the population use it on a regular basis. In 2017, a significant security vulnerability was discovered on the chips used on a large part of Estonian ID-cards. While exploitation would not have been easy nor inexpensive, the weakness was significant enough to trigger an immediate response from state authorities and mitigate the risk as fast as possible. This case has now become a significant learning experience for effective risk management, information sharing, the importance of openness as well as strengthening our digital infrastructure.

Chronology

→ Late at night on **30 August 2017,** Czech researchers informed the Estonian Information System Authority (RIA) of a security weakness detected in the course of their research. The security weakness would have theoretically allowed anyone who knows the public key of an ID card to compute the private key and use it to take control of a person's identity in an e-environment without being in possession of the physical ID card.

→ On **31 August 2017,** the RIA informed the Police and Border Guard Board (PPA) of the vulnerability, which concerns all documents in the ID-1 format: ID card, residence permit card, digital ID card, e-Residency digital ID card, and diplomatic ID card. The affected cards were issued after 16 October 2014. Documents issued earlier are unaffected by the risk.

→ In **September and October,** RIA held meetings with various agencies to identify the details of the security weakness and offer solutions to the situation.

→ On **5 September 2017,** at the request of the PPA, SK ID Solutions AS closed the LDAP directory service (public directory service for identity document certificates) to block access to public keys.

→ On **5 September 2017,** a special press conference was held where Prime Minister Jüri Ratas, Minister of Entrepreneurship and Information Technology Urve Palo, PPA Director General Elmar Vaher and RIA Director General Taimar Peterkop informed the public of the security risk that concerned about 750,000 documents at the time.

→ At the same time, work began on a technical alternative solution to bypass the security weakness. As the weakness was in the chip, Estonian state authorities were not able to remove it.

→ On **21 September 2017,** PPA filed a claim to Gemalto AG concerning breach of contract.

→ On **25 October 2017,** the first cards free of the security weakness were line-produced and **the test period for remote updates began.** From 25 to 31 October a total of 24,336 updates were performed (4,750 at PPA service points and 19,586 through remote channels). By the beginning of the test period and the moment of updating the production line, the **security risk concerned about 800,000 cards in total.**

→ On **30 October 2017,** the paper by the Czech researchers was published in full, which considerably enhanced the likelihood that the security risk would be acted upon and realised.

→ **From 31 October 2017** remote updating was available to everyone whose card was affected by the security risk. The remote update solution failed due to overload and only a few thousand users were able to access the update on 31 October and 1 November. As of 31 October, 24,000 cards had been updated, including 19,500 through remote channels and 4,700 at service points.

→ On **2 November 2017,** the Government's cabinet meeting discussed the ID card security risk and the suspension of certificates. On the evening of 2 November Prime Minister Jüri Ratas with PPA Director General Elmar Vaher and RIA Director General Taimar Peterkop gave a press conference at Stenbock House on the suspension of the affected cards to take effect in the late evening of 3 November.

→ The Government agreed on the **vital and strategic areas, the employees of which could update their ID cards between 3 and 5 November as a matter of priority** both at PPA service points and in major hospitals and through remote channels. This priority list of ID card holders included about 35,000 document numbers.

→ **At midnight on 3 November 2017,** the certificates of all affected cards were suspended, totalling about 750,000 card certificates; about 40,000 cards had been updated by the moment of the suspension. The suspended cards include< about 120,000 documents issued to children.

→ In total, of the 494,000 ID cards that were renewed, 354,000 were updated remotely.

→ By now, all ID cards issued **since 26 October 2017** contain the latest softwared

→ On the **9th of May 2018,** RIA hosted an international conference on the lessons learned from this technological vulnerability, which has since then become a valuable experience to strengthen the eID system and Estonia's digital infrastructure as a whole.

Messages and narrative

→ The security risk was caused by a chip produced by Infineon, one of the world's leading chip producers, which is used by a large number of card and electronics manufacturers globally.

→ **RIA , PPA and other partners came together to find a solution to mitigate the risk and extract vital lessons to be better prepared for upcoming vulnerabilities.** This case is a good example of how the Estonian state can improve its digital infrastructure through the cooperation between researchers, experts and different government agencies.

→ We are the pathfinders of e-Governance. We are the first to do things, the first to get hit and the first to solve the issue. We learn from our mistakes and then teach others. This is our success story.

→ It is not technology but the way we use technology that makes Estonia an e-state. A number of European countries have by now closed down hundreds of thousands and even millions of ID cards without much news coverage. If 90% of our daily affairs are still conducted using pen and paper, it hardly matters that some certificates have been blocked — most people won't even notice. Estonia's 5,000 public and private sector e-services are an integral part of people's daily lives.

→ If, as the outcome of the situation, many people have also obtained Mobile ID in addition to an ID card, we have definitely come out as winners. This would once again be a unique situation: a country actively using two parallel means of access to e-services and giving digital signatures, and if a problem or security weakness should be identified in either of these means in the future, the other one can be used.

→ The current security risk will not be the last one. The risk was discovered in a chip made by one of the world's largest manufacturers, which had all the required certificates. A product meeting all the requirements and used by Microsoft, Google, Lenovo and many other large businesses, proved to be breakable.

→ Estonia's e-Governance is based on trust. E-services would be useless if people didn't have trust in using them. To build and keep trust, people have to be communicated with openly, including about threats.