

Breaking the Estonian ID card revisited: tools and methods for security assessment



Are we better off now than in 2017?

Petr Švenda  svenda@fi.muni.cz  [@rngsec](https://twitter.com/rngsec)

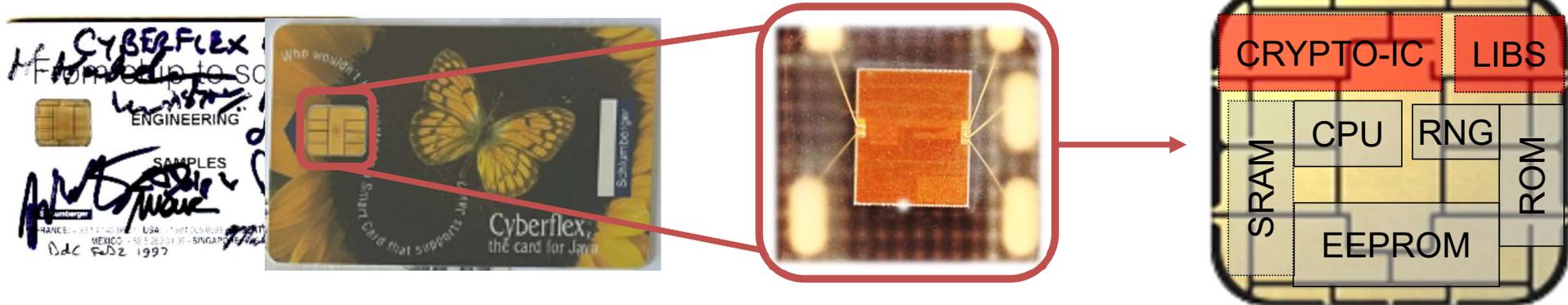
Centre for Research on Cryptography and Security, Masaryk University
Joint work with many amazing people from CRoCS - thank you all!

- As much as possible is kept proprietary (IP, JIL rating, certification req.)
 - Design details, hardware layout, firmware code, JCRE, packages, vendor's API...

Open JavaCard API ✓

```
KeyPair.genKeyPair()
```

```
Signature.sign()
```



Vendor



- Great understanding of target implementation (whitebox)
- Limited knowledge in security testing, advanced attacks, equipment
- Conflict between time-for-testing and time-to-market

Eval lab



- Great knowledge in security testing, specialized equip., process knowledge
- Moderate understanding of target implementation (whitebox, but !enough time)
- Conflict between tough analysis and keeping vendor as a customer

Scheme (BSI, ANSSI, NIAP...)



- Some experts, no direct testing (“impartial”)
- Aim to keep security bar reasonably high
- Stronger ties to bigger players

User



- Lack of knowledge, test outsourcing (certification)
- Do not know what was tested!

Ideal setup for finding bugs

1. Complete knowledge of design and implementation (whitebox)
2. Great experience in security testing, specialized equipment, automated testing, advanced attacks, vulns in related devices
3. A lot of time for testing

Academia, security researchers

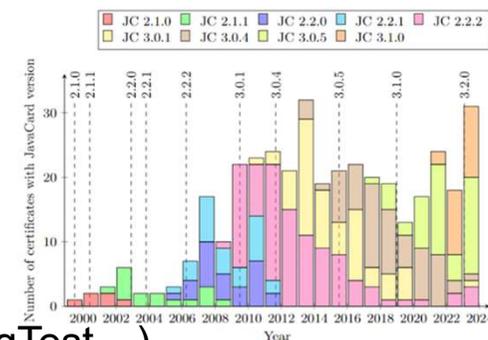
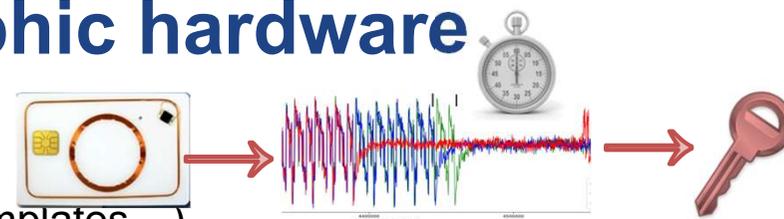


- Small understanding of implementation (frequently blackbox)
- Great knowledge of *some* advanced attacks, *some* equipment
- A lot of time, focus on publishable, more complex results
- Not focused on specific device, wide-scale testing suitable

DIFFICULTY OF ANALYSIS CRYPTOGRAPHIC DEVICES IN TIME

Independent analysis of cryptographic hardware

- ~2000
 - Fresh powerful side-channel attack ideas (SPA/DPA/CPA/Templates...)
 - No card samples for testing (minus points in JIL rating), heavy reliance on black-box as protection
 - CC/FIPS reports very different variable (no template), little to no public info about testing performed
 - No mature open-source testing tools, scattered knowledge
- ~2010-2017
 - Advanced testing setups available at vendor and evaluation labs
 - Availability of (some) smartcards in small quantities for independent testing
 - Practical application of more attacks (lattice attacks on ECC nonce leaks...)
 - Growing open-source community (Chipwhisperer, Sakura, ASCAD dataset, JCAIlgTest...)
- ~2018-now
 - Deep learning SCA attacks (boom from 2016/17), improved lattice-based attacks...
 - Academic researchers typically focus on white-box targets (FPGA...), not smartcards!
 - Still only somewhat older cards available for testing (1-2 generations back, unofficial samples...)



CRoCS 's way

- Focusing on new attacks on **blackbox** targets
 1. Design **technique to probe** cryptographic target
 2. Implement **open-source tool** for testing it
 3. Perform the test on **wide range of targets** (cards, cryptolibs...)
 4. Spot biases and develop **academically publishable** exploitation method
 - Ideal outcome: method can be published, real-world impact can be demonstrated, open analysis tool available for others and future (CI)
- ➔ Reverse engineering (steps 1.-3.) typically revealed some weakness (step 4.)
- Wide-range testing is amplifying (otherwise low) changes to find something!



RSA pubkey origin attribution (no CVE)

[Svenda et.al., The Million-Key Question – Investigating the Origins of RSA Public Keys, USENIX'16]

[Janovsky et.al., Biased RSA private keys: Origin attribution of GCD-factorable keys, ESORICS'20]

ROCA (CVE-2017-15361)

[Nemec et.al., The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli, ACM CCS'17]

Minerva (CVE-2019-15809)

[J.Jancar, V.Sedlacek, P.Svenda, M.Sys. Minerva: The curse of ECDSA nonces, CHES'20]

[J.Jancar, V.Suchanek, P.Svenda, V. Sedlacek, L. Chmielewski. pyecsca: Reverse engineering black-box elliptic curve cryptography via side-channel analysis, CHES'24]

TPMScan (CVE-2020-25082, “NineSig” - no CVE)

[Svenda et.al., TPMScan: A wide-scale study of security-relevant properties of TPM 2.0 chips, CHES'24]

(stay tuned)

[anonymized for review]

Year	Vulnerability / nickname	Hardware target	Attack class	Public ID	Discoverer
1996	RSA timing attack	Smart-card	Side-channel – timing	—	Academic (Kocher)
1997	Boneh–DeMillo–Lipton RSA-CRT fault	Smart-card	Physical – fault	—	Academic (Stanford)
1999	Differential Power Analysis (DPA)	Smart-card	Side-channel – power	—	Academic (Kocher et al.)
2004	“Sorcerer’s Apprentice” voltage/laser survey	Smart-card	Physical – fault	—	Evaluation-lab + academic
2008	MIFARE Classic / CRYPTO-1 break	Contactless card	Logic + side-channel	—	Academic (Radboud U.)
2011	Java Card operand-stack laser fault	Java Card	Physical – laser	—	Academic (Télécom ParisTech)
2011	Mifare DESFire MF3ICD40	Smart-card	Side-channel – power	—	Academic (Oswald&Paar)
2013	Weak RSA key generation (factorable)	Taiwanese Citizen-ID	Logic – keygen, TRNG	—	Academic (Bernstein et al.)
2013	Yubikey 2 OTP key extraction	Smart-card	Side-channel – power	—	Academic (Oswald et al.)
2014	EMV foreign-currency limit bypass	EMV chip card	Logic – protocol	—	Academic (Newcastle U.)
2015	HMAC_SHA1 key extraction	DS28E01/DS2432 IC	Side-channel – power	—	Academic (Oswald)
2017	ROCA weak RSA keygen	Infineon cards & TPMs	Logic – math	CVE-2017-15361	Academic (Masaryk U.)
2019	Java Card RI multiple bugs	Java Card	Logic – code	Oracle CPU (no CVE)	Commercial (Security Explorations)
2019	Yubikey reduced initial randomness on FIPS	Yubikey FIPS token	Logic –randomness	YSA-2019-02	Vendor (Yubico)
2019	Deep learning on RSA implementations	ARM Core SC 100 EAL4+ IC	Side-channel – EM	—	Evaluation-lab + vendor
2019	TPM-Fail ECDSA timing leaks	Intel fTPM & ST dTPM	Side-channel – timing	CVE-2019-11090, -16863	Academic
2020	Estonian ID-card duplicate keys	National ID smart-card	Logic – key mgmt	—	Academic (Paršovs)
2021	NXP SmartMX EM leak (Titan/SJTT)	SmartMX & A7x secure MCUs	Side-channel – EM	CVE-2021-3011	Commercial (NinjaLab)
2021	STSAFE-J / J-SAFE3 ECDSA leak	Java Card SE	Side-channel – timing	CVE-2021-43392/43393	Vendor (ST)
2023	TPM 2.0 ref-lib OOB R/W	Discrete & firmware TPM	Logic – mem-corr	CVE-2023-1017/1018	Commercial (Quarkslab)
2023	faultPM full-state extraction	AMD fTPM	Physical – fault	—	Academic (TU Berlin)
2023	STSAFE-A1 middleware overflow	Secure element	Logic – buffer-overflow	CVE-2023-50096	Commercial (Elttam)
2024	TPMScan nonce-bias & timing	Multi-vendor TPM 2.0	Side-channel	—	Academic (Masaryk U.)
2024	NineSig: Intel fixed nonce bits	Intel fTPM	Logic – randomness	—	Academic (Masaryk U.)
2024	EUCLeak EM leak in Infineon lib	Infineon SE (YubiKey 5/HSM 2)	Side-channel – EM	CVE-2024-45678	Commercial (NinjaLab)
2025	YubiKey CTAP v2 partial-sig check	YubiKey 5/Bio/HSM 2	Logic – protocol	CVE-2025-29991	Vendor (Yubico)

Bias in past publicly reported vulnerabilities

- Based on public reports, vulnerabilities seems to be primarily found by academic researchers and freelancers/independent labs
 - People operating in black-box attacker model => harder to spot problems (than white-box)



Public disclosure might be a side-effect of academics desire to publish and independent commercial labs to advertise themselves

- Rarely vendor itself (Yubico seems to be exception)



How likely is that blackbox analysis spotted all the vulnerabilities?

- Likely many problems completely missed (blackbox) or neglected (second defensive layer)
- Likely many problems undisclosed (vendor/eval.labs: before/after deployment/certification)
- Reported vulnerabilities with low visibility (no CVE, no public security bulletin...)
 - E.g. Intel fTPM “NineSig” vulnerability (TPMScan), no CVE because product is “outdated”

Trying to...
“BREAKING” THE ESTONIA ID TODAY

<https://www.id.ee/wp-content/uploads/2021/08/td-id1-chip-app-4.pdf>

TD-ID1-Chip-App



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

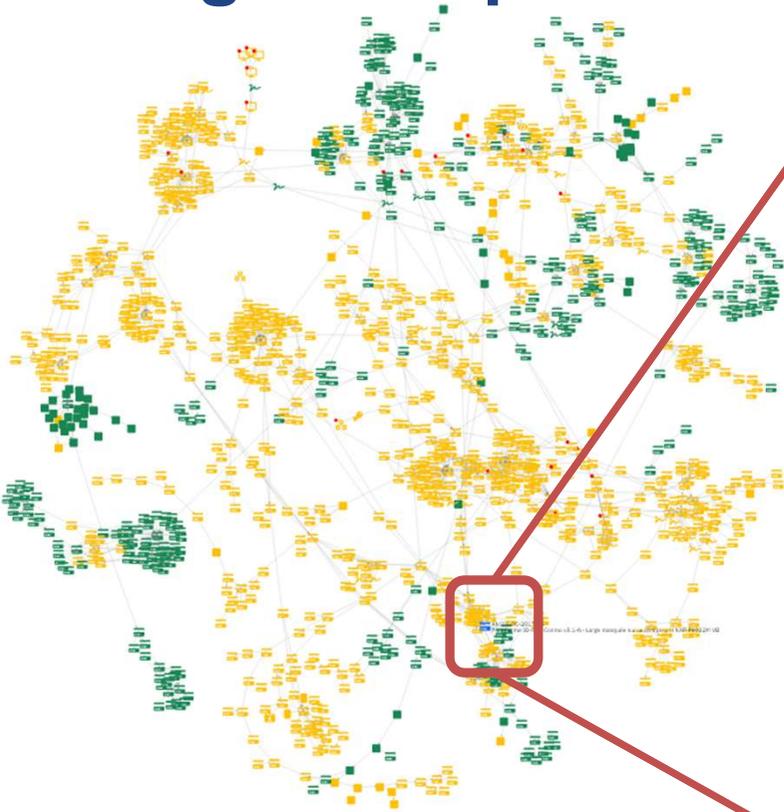
1 JAVA GLOBAL PLATFORM

ID-One™ Cosmo v8.1 and v8.2 are certified as an open platform CC EAL5+ As a result, even if a non-evaluated applet is loaded the security is not compromised. The certification of an external application is also strongly simplified on the platform. The Cosmo is compliant with the latest inter-

- JavaCard™ 3.0.4 Classic Edition
- Global Platform v2.2.1 (ID Configuration v1.0)
- ISO/IEC 7816 parts 1, 2, 3, 4, 5, 6, 8 and 9
- ISO/IEC 14443 Type A

Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145		Rapport de certification ANSSI-CC-2019/28
Référence du rapport de certification		
ANSSI-CC-2019/28		
Nom du produit		
Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145		
Référence/version du produit		
Identification du matériel : 091121		
Conformité à un profil de protection		
[PP JCS-O] Java Card Protection Profile Open Configuration, version 3.0		
Critères d'évaluation et version		
Critères Communs version 3.1 révision 5		
Niveau d'évaluation		
EAL 5 augmenté ALC_DVS.2, AVA_VAN.5		
Développeurs		
Idemia 2 place Samuel de Champlain 92400 Courbevoie, France	NXP Semiconductors GmbH Troplowitzstasse 20 22529 Hamburg, Allemagne	
Commanditaire		
Idemia 2 place Samuel de Champlain 92400 Courbevoie, France		
Centre d'évaluation		
CEA - LETI 17 avenue des martyrs, 38054 Grenoble Cedex 9, France		

Regular expression to search for certificate IDs



Frontpage

Certificate ID ANSSI-CC-2019/28

Certified item Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145

Certification lab CEA - LETI 17 avenue des martyrs, 38054 Grenoble Cedex 9, France

Developer Idemia 2 place Samuel de Champlain 92400 Courbevoie, France NXP Semiconductors GmbH Troplowitzstasse 20 22529 Hamburg, Allemagne Commanditaire Idemia 2 place Samuel de Champlain 92400 Courbevoie, France

References

Outgoing

- [ANSSI-CC-2017/49](#) - archived - Plateforme ID-One Cosmo v8.1-N- Large masquée sur le composant NXP P6022M VB
- [BSI-DSZ-CC-1059-2018](#) - archived - NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software

Incoming

- [ANSSI-CC-2019/47](#) - archived - LDS Applet BAC with CA and AA on ID-One V8.2 Platform on NXP P60D145 (Version 03 00 00 00)
- [ANSSI-CC-2019/43-R01](#) - active - Application CPS2ter, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2 Code SAAAAR Applet : 0708312 ; Code SAAAAR Patch : 093072
- [ANSSI-CC-2019/36](#) - archived - IAS ECC V2, Version 1.3 en configuration #4 sur la plateforme ID-One Cosmo v8.2
- [ANSSI-CC-2019/35](#) - archived - IAS ECC V2, Version 1.3 en configuration #3 sur la plateforme ID-One Cosmo v8.2
- [ANSSI-CC-2019/43](#) - archived - Application CPS2ter v1.12, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2 (Identification 01 12)
- [ANSSI-CC-2019/50](#) - archived - LDS Applet PACE with CAM, CA and AA on ID-One V8.2 Platform on NXP P60D145 (version 03 00 00 00)
- [ANSSI-CC-2019/41](#) - archived - ID-One Cosmo v8.2 embedding VITALE application (Version 2.0.83)
- [ANSSI-CC-2020/26](#) - active - Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145
- [ANSSI-CC-2019/33](#) - archived - IAS ECC V2, version 1.3 en configuration #1 sur la plateforme ID-One Cosmo v8.2
- [ANSSI-CC-2019/48](#) - archived - LDS Applet EAC with AA on ID-One V8.2 Platform on o NXP P60D145 (versi on 03 00 00 00)
- [ANSSI-CC-2019/34](#) - archived - IAS ECC V2, version 1.3 en configuration #2 sur la plateforme ID-One Cosmo v8.2
- [ANSSI-CC-2019/49](#) - archived - LDS Applet EAC with PACE on ID-One V8.2 Platform on NXP P60D145 (version 03 00 00 00)



what smartcard chip is used in electronic identity documents of estonia

Thought for 1m 28s >

The Estonian Police and Border Guard Board's current ID-card, e-resident digi-ID, residence-permit card and other electronic identity documents are built on IDEMIA's "ID-One Cosmo v8.x" Java-Card platform, running on an NXP SmartMX2 P60 secure micro-controller (P60D081 / P60D1... was introduced in December 2018 (Cosmo v8.1) and upgraded to Cosmo v8.2 – capability – on 1 August 2021.

Period of issuance	Hardware platform (chip)	Notes
2021 → present	ID-One Cosmo v8.2 on NXP P60 SmartMX2	Adds ICAO-c dual contact
Dec 2018 – Jul 2021	ID-One Cosmo v8.1 on NXP P60 SmartMX2	First batch m contract end
Jan 2015 – Nov 2018	jTOP SLE78 (Infineon SLE78 secure controller)	Affe pha
2011 – 2014	jTOP SLE66 (Infineon SLE66 series)	Still
2002 – 2006	Micardo Public 2.1 (Siemens/Infineon 8-bit)	Firs

Affected by the 2017 ROCA vulnerability; phased out by 2019. Useenix Hacker News

Still in use until cards Useenix

First-generation Esto

[PDF] Estonian Electronic Identity Card: Security Flaws in Key Management

August 12, 2020 — The jTOP SLE78-powered ID cards were issued until the end of 2018. ID cards manufacture...

Estonian Electronic Identity Card: Security Flaws in Key Management

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

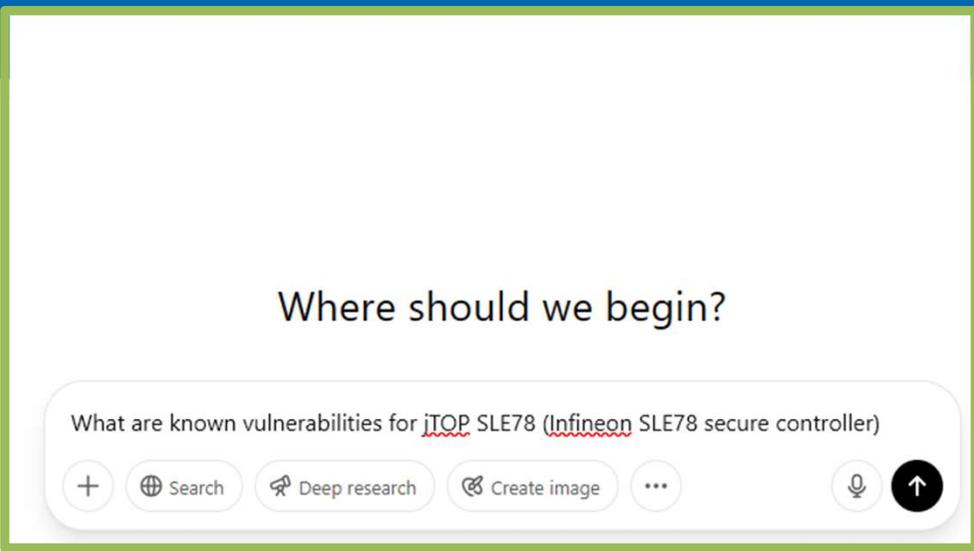


what are known vulnerabilities for jTOP SLE78 (Infineon SLE78 secure controller)

Thought for 2m 6s

Bottom-line first (no fluff)

Only two public, technically solid breaks exist for the jTOP SLE78 platform—and they’re both Infineon-library screw-ups, not spectacular “chip hacks”:



Vuln / CVE	How you exploit it	Practical risk today
ROCA – CVE-2017-15361 <small>NVD crocs.fi.muni.cz</small>	Zero physical access; you just grab the public key, run the ROCA test, and factor a 2048-bit modulus in a few CPU-weeks/cloud dollars.	Dead serious if the card still uses a ROCA-bred RSA key. Estonia revoked 750 000 certs and forced an on-card key-gen update in 2018; everyone else either patched or abandoned RSA.
EUCLEAK – CVE-2024-45678 (Infineon ECDSA side-channel) <small>Cryptology ePrint Archive</small> <small>BleepingComputer NVD</small>	You need the token in hand, an oscilloscope, and a €1-2 k EM probe; collect ~1 000 signatures → lattice attack → full key.	Lab-grade, high-value-target scenario only. Firmware 5.7.0 (YubiKey) and the patched Infineon crypto-lib eliminate the leak.



Straight-talk details

- ROCA in SLE78



- Root cause: Infineon's RSALib built primes with a fixed low-entropy template. Researchers reversed the pattern and published a public-key fingerprint test and factorisation method. cros.fi.muni.cz

FAIL

- Affects *only* keys generated by the chip **before November 2017**. If you imported an externally generated RSA key, you're safe. 



- Mitigation is binary: replace the key or stop using RSA on these cards. Firmware patches disabled the bad algorithm, but the rotten keys stay rotten.

If you're still running SLE78 cards



1. **Audit every on-card RSA key** with the publicly available ROCA test. Nuke and re-issue any hit.
2. **Kill RSA key-gen on the card**—force 3072-bit+ ECC or import keys from a sane HSM.
3. **Check your firmware / crypto-lib version**. If it predates Infineon's July 2024 patch, you're vulnerable to EUCLEAK on ECC. Update or block ECDSA.
4. **Limit signature sessions** (PIN entry per sign) and keep the PIN retry counter low; it neuters casual side-channel harvesting.
5. **Have an emergency revocation plan**. Hardware lasts a decade, crypto screw-ups happen every few years—be ready.

Problem with LLMs: Fact checking and nuances

- Users will use LLM chatbots to get information they are missing
- False positives and false negatives, nuances!
- Problem for vendors / gov. agencies
 - LLM summary is out of their control, wording, interpretation...
- Initial information needs to be public at the first place!
 - Possibly even higher motivation for vendor to hide info behind walls from LLMs?



Back to Cosmo 8.2 (estID)

Straight-up reality check

- No CVE or remotely exploitable bug has ever been published for Cosmo v8.x itself. Public CVE feeds, vulnerability trackers and stack.watch all show *zero* entries for SmartMX2 P60 since its 2016 release.

Stack Watch Stack Watch

- The only concrete attack with a working PoC against P60 silicon is the PIN-length timing leak – and it's a nuisance, not a break.
- Every other threat you'll hear ("ROCA", "Titan leak", "MIFARE Classic crack") hits *older* or *different* chips.

- Independent analysis

- Can we get design files and firmware source code? (no)
- Can we security test ourselves? (you are on your own)
- Can we get some Cosmo 8.2 samples (no... or only if you would sign NDA... and then you can't publish results)

How to improve trustworthiness

- By authority?
 - Vendors + evaluation labs + govts. bodies did a lot of work to increase security baseline
 - Still quite closed system, no public detailed eval. reports, EUCC changed little
- By end-user verifiability?
 - Tools for self-verification, find relevant info and security events notification
 - LLMs to search (less need to build dedicated search tool like <https://sec-certs.org>), but problem with verifiability of claims (false positives, negatives, nuances)
- By wisdom of crowd?
 - Might be messy as is permissionless, reputation of submitter



Idea: Let's do security testing, metadata collection and facts checking collaboratively, sign results, and cryptographically tie to the product



PRODUCTS

(ProductEvent)

BINDINGS

(BindingEvent)

METADATA

(MetadataEvent)

Infineon M7794A12
 BSI-DSZ-CC-0814-2012
 CC EAL4+




CSV information

Status ● archived

Valid from 26.07.2012

Valid until 01.09.2019

Scheme ● DE

Manufacturer [Infineon Technologies AG](#)

Category ■ ICs, Smart Cards and Smart Card-Related Devices and Systems

Security level ■ [Security level](#)

Protection profiles ● [SECURITY_IC_V1.0_PKISKPP](#)

● Binding ● 

● Binding ● 

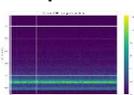
● Binding ● 

● Binding ● 

RSA keypairs
 Distribution of primes P and Q




ECDSA signature
 Dependency of sig time on private key




CVE-2017-15361
 Vulnerability in keygen (ROCA)




ChatGPT summary
 Prompt: Vulnerabilities in jTOP SLE78




JSON blobs for products/metadata/bindings

Filtering based on trust to signer

NOSTR for format and propagation network



PRODUCTS (ProductEvent)

BINDINGS (BindingEvent)

METADATA (MetadataEvent)

Infineon M7794A12
BSI-DSZ-CC-0814-2012
CC EAL4+




CSV information

Status: archived
Valid from: 26.07.2012
Valid until: 01.09.2019
Scheme: DE
Manufacturer: Infineon Technologies AG
Category: ICs, Smart Cards and Smart Card-Related Devices and Systems
Security level:
Protection profiles: SECURITY_IC_V1.0_PKISKPP

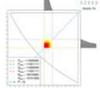
● Binding ● 

● Binding ● 

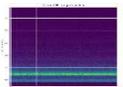
● Binding ● 

● Binding ● 

RSA keypairs
Distribution of primes
P and Q 



ECDSA signature
Dependency of sig time on
private key 



CVE-2017-15361
Vulnerability in keygen
(ROCA) 



ChatGPT summary
Prompt: Vulnerabilities in
jTOP SLE78 



JSON blobs for products/metadata/bindings
Filtering based on trust to signer
NOSTR for format and propagation network



Summary – from the perspective of external researcher

- Better availability of open tools for end-user (but more needed)
- Not much changed in certification ecosystem
 - System still not accommodating academic/independent researchers
 - More openness and availability of information needed
- LLMs is/will be used by end-users (and attackers as well)
- Advent of open cryptographic hardware?

