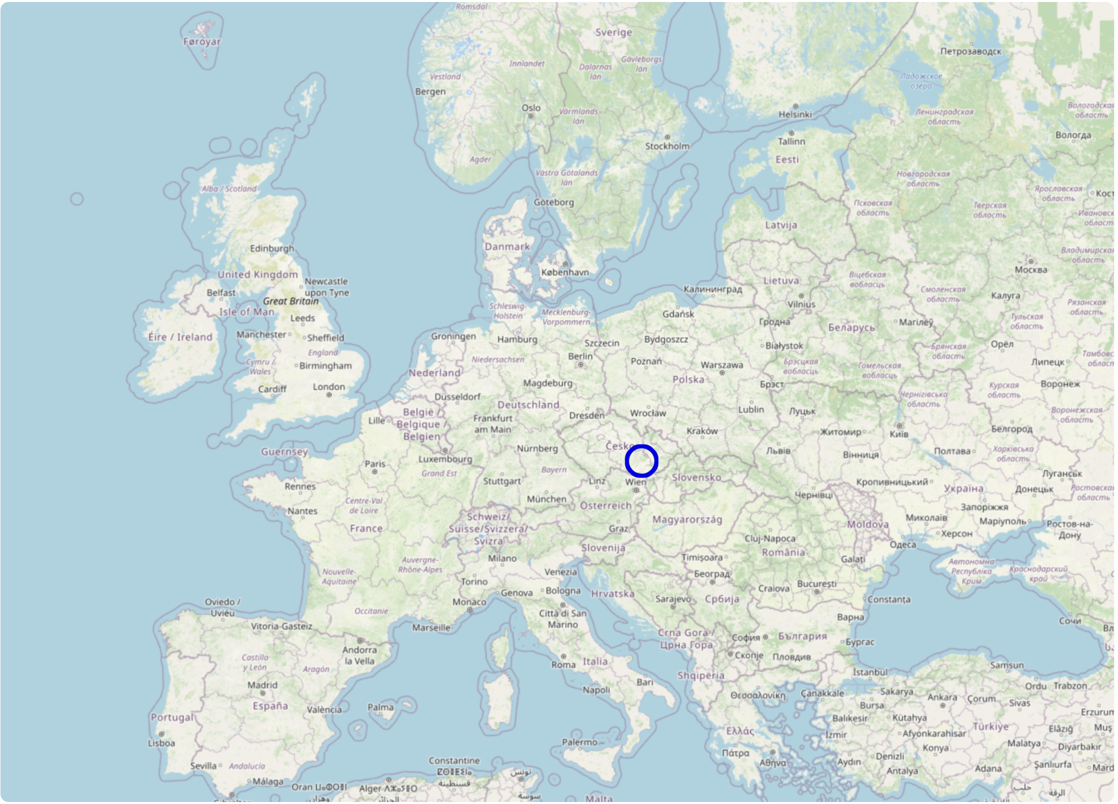
MUNI
FI

Insights from Automated Large-Scale Analysis of Common Criteria Certificates

EU CyberActs conference 2024

Adam Janovsky | adamjanovsky@mail.muni.cz


Føroyar
Sverige
Bergen
Oslo
Stockholm
Helsinki
Tallinn
Eesti
Петрозаводск
Вологда
Göteborg
Latvija
Danmark
København
Edinburgh
United Kingdom
Newcastle upon Tyne
Belfast
Great Britain
Isle of Man
Leeds
Éire / Ireland
Manchester
Sheffield
Birmingham
Cardiff
London
Lietuva
Vilnius
Москва
Калининград
Gdańsk
Hamburg
Groningen
Szczecin
Bydgoszcz
Berlin
Poznań
Warszawa
Polska
Nederland
Magdeburg
Deutschland
Dusseldorf
Dresden
Wrocław
Lublin
Беларусь
België / Belgique / Belgien
Frankfurt am Main
Kraków
Київ
Lille
Luxembourg
Nürnberg
Paris
Stuttgart
Linz
Wien
Slovensko
Україна
München
Österreich
Rennes
Nantes
France
Schweiz/ Suisse/Svizzera/ Svizra
Graz
Magyarország
Moldova
Slovenija
Milano
Venezia
Timişoara
România
Torino
Genova
Bologna
Hrvatska
Београд
București
Monaco
Sarajevo
Србија
Marseille
Oviedo / Uviéu
Vitoria-Gasteiz
Andorra la Vella
Roma
Italia
Црна Гора
София
България
Madrid
España
Portugal
Lisboa
València
Palma
Napoli
Bari
Shqipëria
İstanbul
Ankara
Türkiye
Ελλάς
Sevilla
Málaga
Palermo
Malta

MUNI

2017: Return of the coppersmith attack (RoCA)

2017: Return of the coppersmith attack (RoCA)

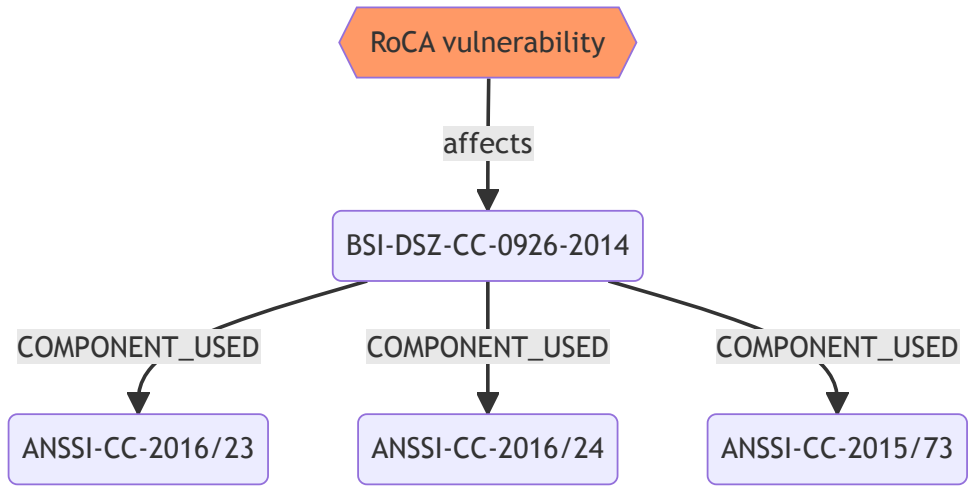
- CVE-2017-15361, practical factorization of widely used RSA moduli.

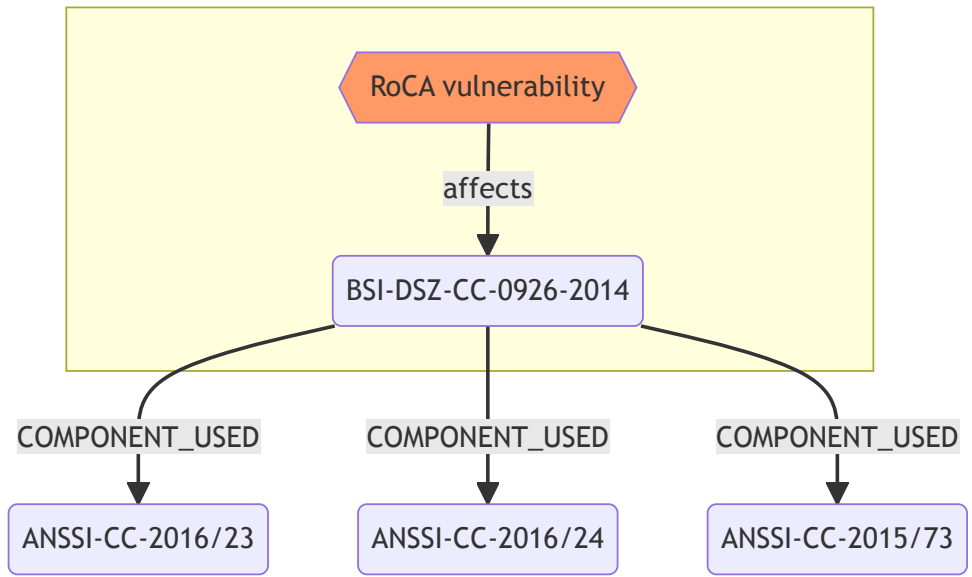
2017: Return of the coppersmith attack (RoCA)

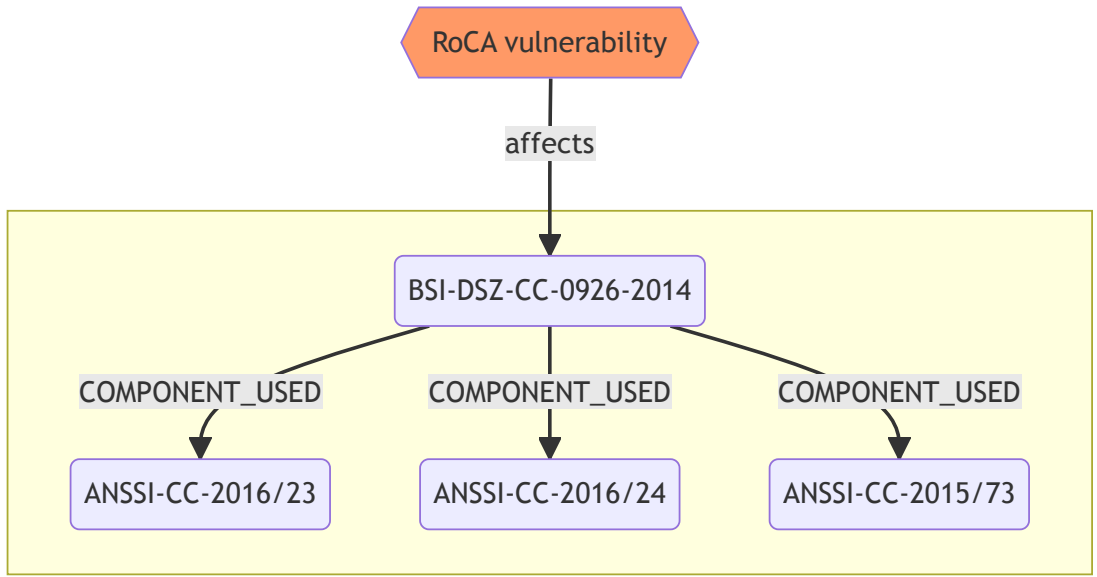
- CVE-2017-15361, practical factorization of widely used RSA moduli.
- Billion+ devices affected.

2017: Return of the coppersmith attack (RoCA)

- CVE-2017-15361, practical factorization of widely used RSA moduli.
- Billion+ devices affected.
- ⚠ *How many CC-certified products are impacted?*


RoCA vulnerability
affects
BSI-DSZ-CC-0926-2014
COMPONENT_USED
COMPONENT_USED
COMPONENT_USED
ANSSI-CC-2016/23
ANSSI-CC-2016/24
ANSSI-CC-2015/73


RoCA vulnerability
affects
BSI-DSZ-CC-0926-2014
COMPONENT_USED
COMPONENT_USED
COMPONENT_USED
ANSSI-CC-2016/23
ANSSI-CC-2016/24
ANSSI-CC-2015/73


RoCA vulnerability
affects
BSI-DSZ-CC-0926-2014
COMPONENT_USED
COMPONENT_USED
COMPONENT_USED
ANSSI-CC-2016/23
ANSSI-CC-2016/24
ANSSI-CC-2015/73

seccerts.org

Search

Search and browse through the certificates and our extracted metadata.

Search

Search and browse through the certificates and our extracted metadata.

Vulnerabilities

Display existing vulnerabilities in the certified products.

Search

Search and browse through the certificates and our extracted metadata.

References

Explore an interactive graph of references in Common Criteria certificates.

Vulnerabilities

Display existing vulnerabilities in the certified products.

Search

Search and browse through the certificates and our extracted metadata.

References

Explore an interactive graph of references in Common Criteria certificates.

Vulnerabilities

Display existing vulnerabilities in the certified products.

Analysis

View a part of our results of our analysis of the Common Criteria certificate data.

Infineon Security Controller M7892 A21 with optional RSA 2048/4096 1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)

⚠ This certificate has known related **CVEs**, which means that the certified product might be vulnerable.

CSV information ?

Status	archived
Valid from	06.02.2012
Valid until	01.09.2019
Scheme	DE
Manufacturer	Infineon Technologies AG
Category	ICs, Smart Cards and Smart Card-Related Devices and Systems
Security level	AVA_VAN.5, EAL5+, ALC_DVS.2
Protection profiles	• PKISKPP, SECURITY_IC_V1.0

Heuristics summary ?

Certificate ID: **BSI-DSZ-CC-0758-2012**

Certification report

Certification report | PDF | TXT

Extracted keywords

- Cryptography
- Device
- Common Criteria
- Security
- Other

File metadata

Title:	Certification Report BSI-DSZ-CC-0758-2012
Subject:	Common Criteria Certification
Keywords:	"Common Criteria, Certification, Zertifizierung, Infineon Security Controller M7892 A21, Infineon Technologies AG"
Author:	Bundesamt für Sicherheit in der Informationstechnik
Creation date:	D:20120214152801+01'00'
Modification date:	D:20120214153307+01'00'
Pages:	44
Creator:	Writer
Producer:	OpenOffice.org 3.2

References

Incoming

- BSI-DSZ-CC-0833-2013 - CardOS V5.0 with Application for QES, V1.0
- BSI-DSZ-CC-0782-2012 - Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)

Heuristics ?

Certificate ID: **BSI-DSZ-CC-0758-2012**

Extracted SARs

ASE_TSS.1, ADV_TDS.4, AGD_PRE.1, APE_REQ.2, AVA_VAN.5, ALC_TAT.2, ADV_FSP.5, ALC_LCD.1, APE_INT.1, ASE_REQ.2, AGD_OPE.1, ASE_ECD.1, ADV_SPM.1, ADV_IMP.1, APE_ECD.1, ALC_DEL.1, ATE_FUN.1, ATE_DPT.3, APE_OBJ.2, ALC_FLR.3, ADV_INT.2, ATE_IND.2, ASE_SPD.1, ALC_CMS.5, ATE_COV.2, ASE_CCL.1, APE_SPD.1, APE_CCL.1, ALC_DVS.2, ALC_CMC.4, ASE_OBJ.2, ASE_INT.1, ADV_ARC.1

CPE matches

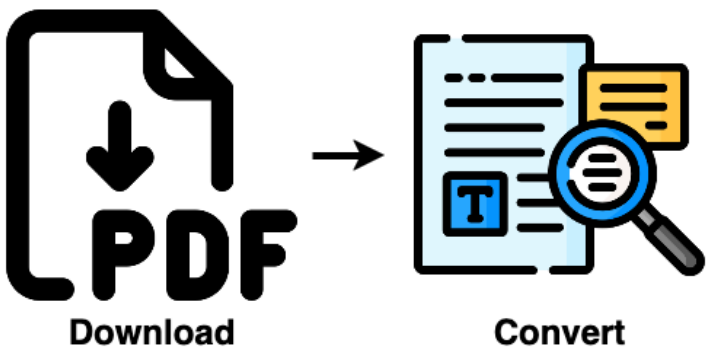
- cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*

Related CVEs

			CVSS Score			
ID	**Links**	**Severity**	**Base**	**Exploitability**	**Impact**	**Published on**
CVE-2017-15361	C M N	! MEDIUM	5.9		3.6	16.10.2017 17:29

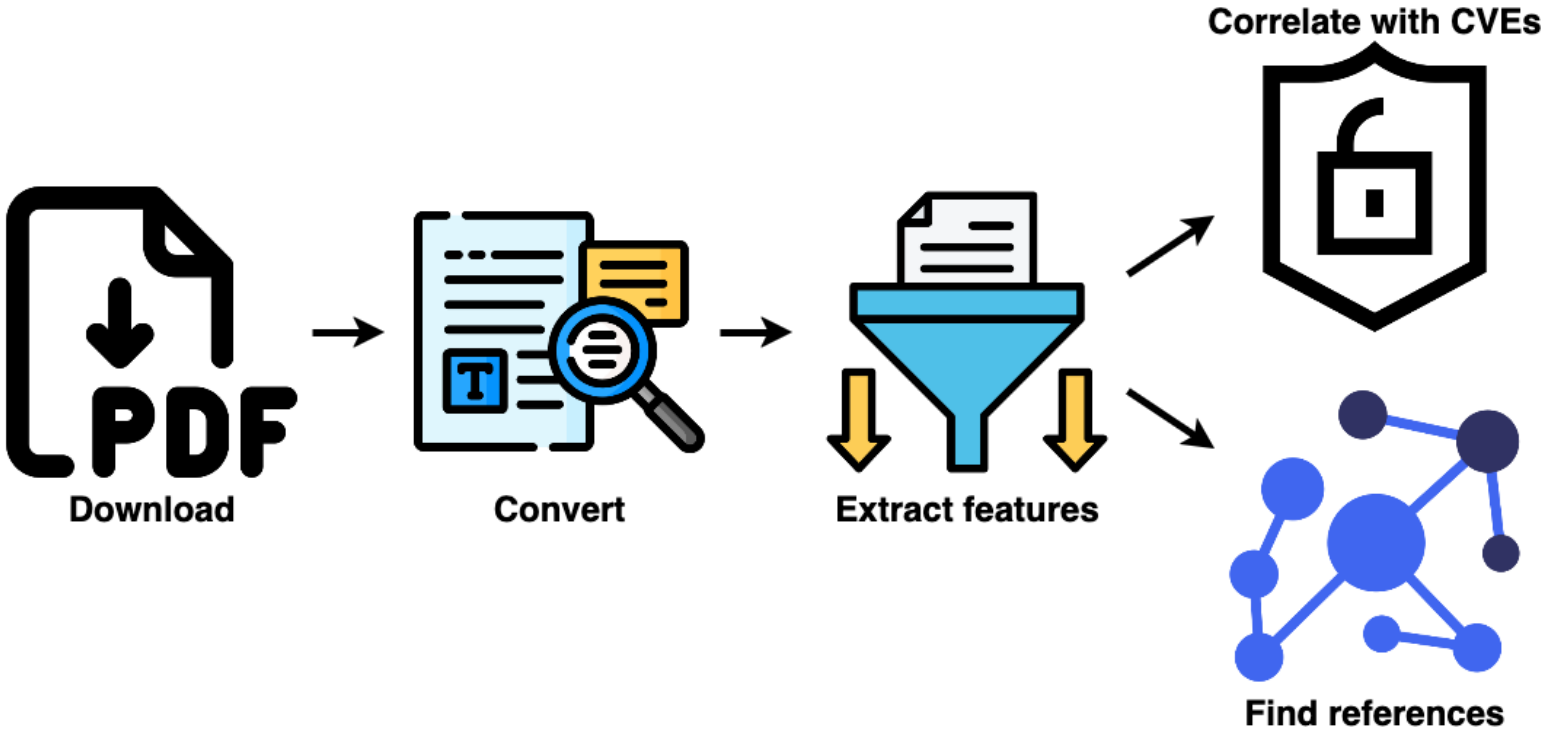
Processing CC artifacts

Processing CC artifacts



Processing CC artifacts

Processing CC artifacts



Correlating certified products with vulnerabilities

Correlating certified products with vulnerabilities

- Each vulnerability from NVD is assigned with Common Platform Enumerations (CPEs).
  - RoCA vulnerability lists `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`

Correlating certified products with vulnerabilities

- Each vulnerability from NVD is assigned with Common Platform Enumerations (CPEs).
  - RoCA vulnerability lists `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Each certified product has its unique title.

Correlating certified products with vulnerabilities

- Each vulnerability from NVD is assigned with Common Platform Enumerations (CPEs).
  - RoCA vulnerability lists `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Each certified product has its unique title.

> **Infineon** Security Controller M7892 A21 with optional **RSA** 2048/4096 **1.02.013**, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 **libraries** and with specific IC dedicated software (firmware)

Correlating certified products with vulnerabilities

- Each vulnerability from NVD is assigned with Common Platform Enumerations (CPEs).
  - RoCA vulnerability lists `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Each certified product has its unique title.

> **Infineon** Security Controller M7892 A21 with optional **RSA** 2048/4096 **1.02.013**, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 **libraries** and with specific IC dedicated software (firmware)

- Use machine learning to map the certified products to CPEs.

Correlating certified products with vulnerabilities

- Each vulnerability from NVD is assigned with Common Platform Enumerations (CPEs).
  - RoCA vulnerability lists `cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*`
- Each certified product has its unique title.

> **Infineon** Security Controller M7892 A21 with optional **RSA** 2048/4096 **1.02.013**, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 **libraries** and with specific IC dedicated software (firmware)

- Use machine learning to map the certified products to CPEs.
- Our model achieves 90% precision.

Unravelling the relations between certified products

Unravelling the relations between certified products

1. Collect certificate identifiers and references to other identifiers from the artifacts.
   - `BSI-DSZ-CC-0926-2014`

Unravelling the relations between certified products

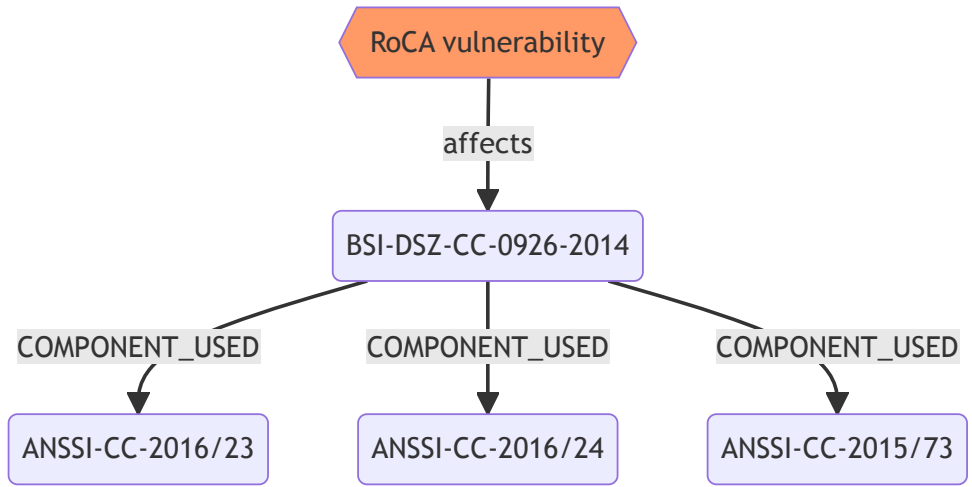
1. Collect certificate identifiers and references to other identifiers from the artifacts.
   - `BSI-DSZ-CC-0926-2014`
2. Build a directed graph out of the identifiers.

Unravelling the relations between certified products

1. Collect certificate identifiers and references to other identifiers from the artifacts.
   - `BSI-DSZ-CC-0926-2014`
2. Build a directed graph out of the identifiers.
3. Understand the different meanings behind the references.

Unravelling the relations between certified products

1. Collect certificate identifiers and references to other identifiers from the artifacts.
   - `BSI-DSZ-CC-0926-2014`
2. Build a directed graph out of the identifiers.
3. Understand the different meanings behind the references.
4. Use natural language processing to label the edges with context.


RoCA vulnerability
affects
BSI-DSZ-CC-0926-2014
COMPONENT_USED
COMPONENT_USED
COMPONENT_USED
ANSSI-CC-2016/23
ANSSI-CC-2016/24
ANSSI-CC-2015/73

Ecosystem insights: general trends

Ecosystem insights: general trends

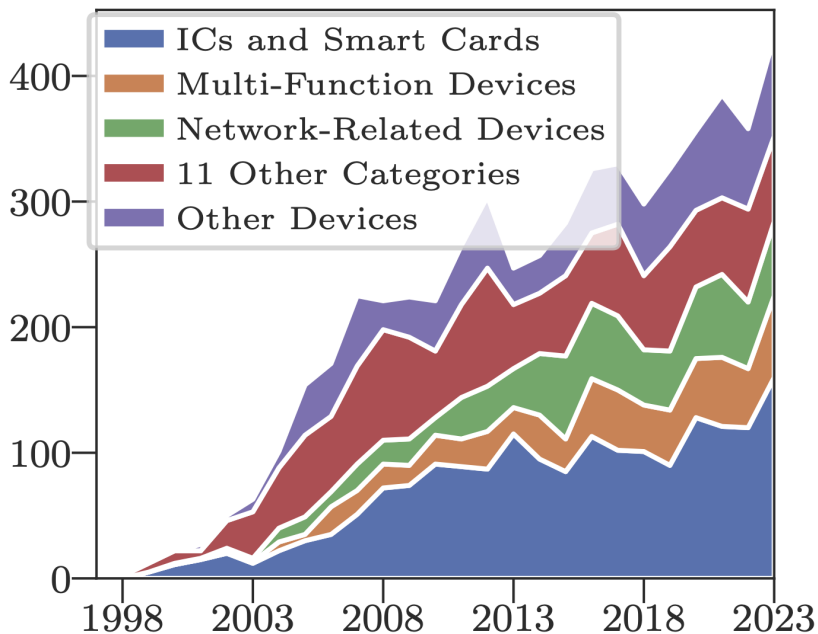


Figure: number of issued certificates.

Ecosystem insights: general trends

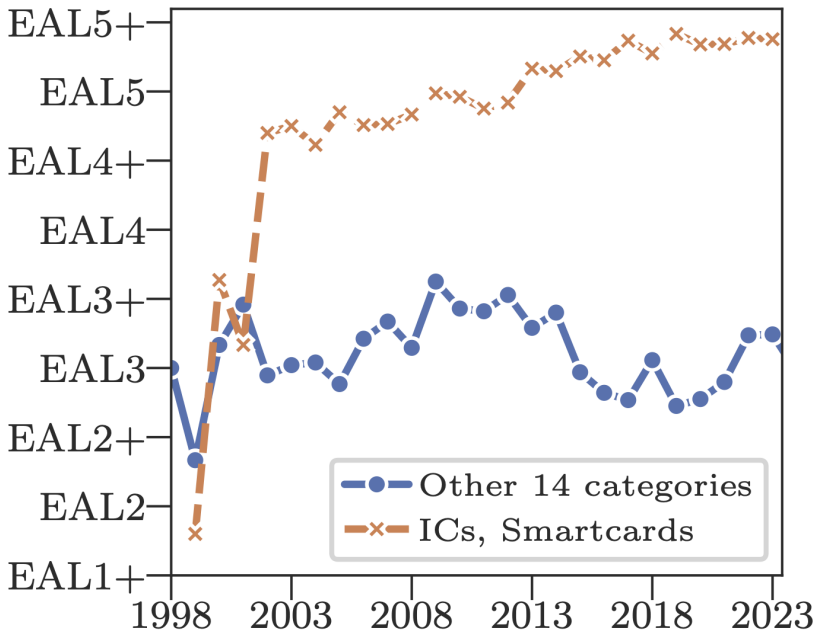


Figure: average EAL in time.

Ecosystem insights: general trends

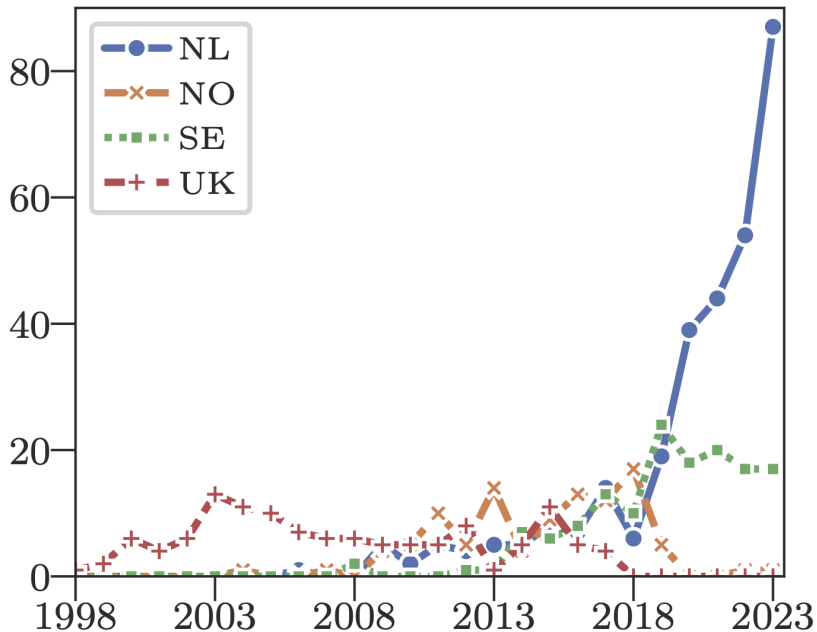


Figure: emerging national schemes.

Ecosystem insights: weaknesses, the usual suspects

CWE-ID	CWE name	# CVEs
CWE-119	Buffer overflow	892
CWE-20	Improper Input Validation	487
CWE-200	Sensitive information exposure	349
CWE-264	Access control error	316
CWE-787	Out-of-bounds Write	297
CWE-125	Out-of-bounds Read	208
CWE-399	Resource Management Errors	180
CWE-79	Cross-site Scripting	148
CWE-416	Use After Free	122
CWE-362	Race Condition	115

Figure: Weaknesses in certified products.

Ecosystem insights: weaknesses, the usual suspects

CWE-ID	CWE name	# CVEs
CWE-119	Buffer overflow	892
CWE-20	Improper Input Validation	487
CWE-200	Sensitive information exposure	349
CWE-264	Access control error	316
CWE-787	Out-of-bounds Write	297
CWE-125	Out-of-bounds Read	208
CWE-399	Resource Management Errors	180
CWE-79	Cross-site Scripting	148
CWE-416	Use After Free	122
CWE-362	Race Condition	115

Figure: Weaknesses in certified products.

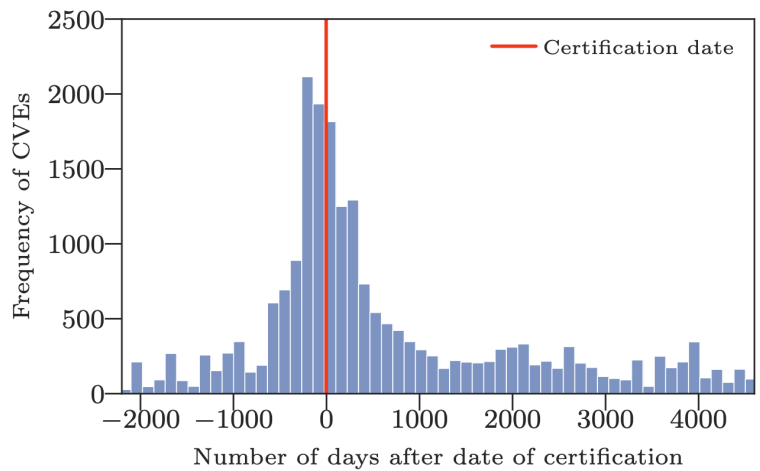


Figure: Product lifecycle.

Ecosystem insights: inter-certificate relations

Ecosystem insights: inter-certificate relations

- As of early 2024, the graph has 5601 vertices (products) and 2966 edges (connections).

Ecosystem insights: inter-certificate relations

- As of early 2024, the graph has 5601 vertices (products) and 2966 edges (connections).
- Two fundamental reasons to reference another product:
  - **Component reuse**
  - **Predecessor**

Ecosystem insights: inter-certificate relations

- As of early 2024, the graph has 5601 vertices (products) and 2966 edges (connections).
- Two fundamental reasons to reference another product:
  - **Component reuse**
  - **Predecessor**
- Smartcards massively using certified dependencies (61.78%).

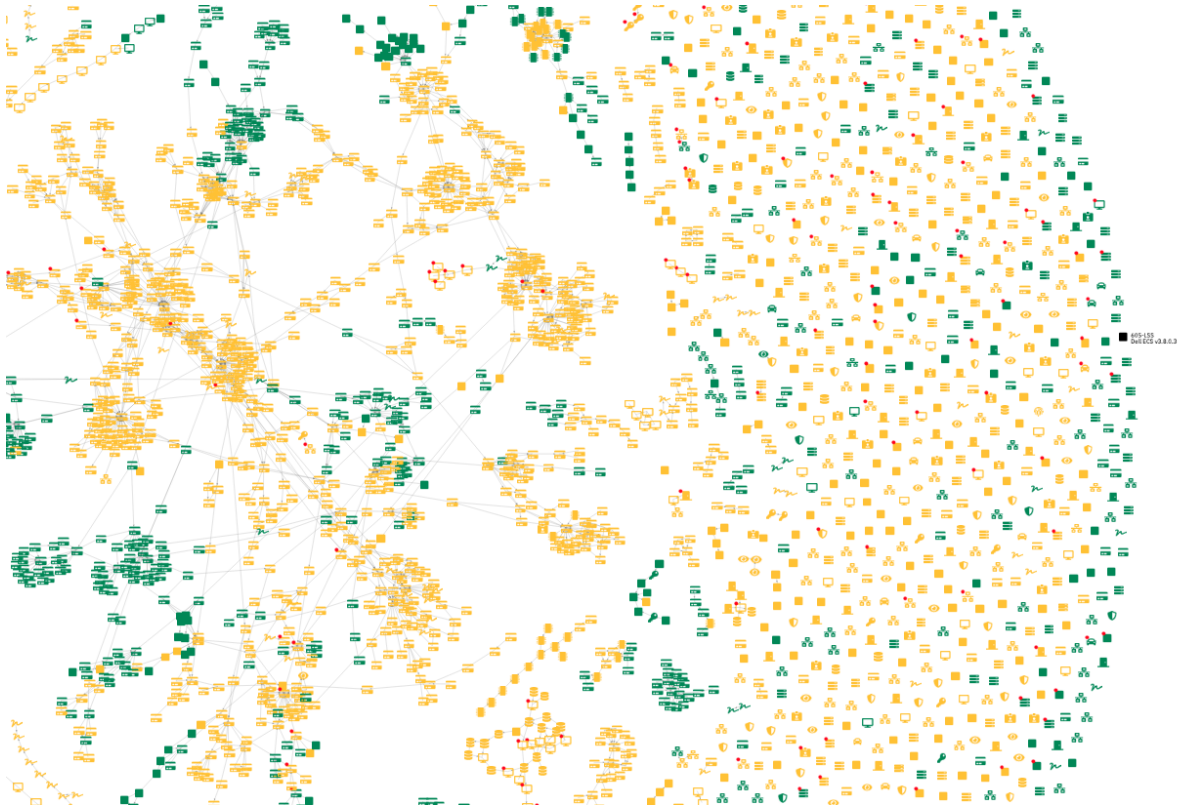
Ecosystem insights: inter-certificate relations

- As of early 2024, the graph has 5601 vertices (products) and 2966 edges (connections).
- Two fundamental reasons to reference another product:
  - **Component reuse**
  - **Predecessor**
- Smartcards massively using certified dependencies (61.78%).
- Smartcard-unrelated products rarely have certified dependencies (2.77%).

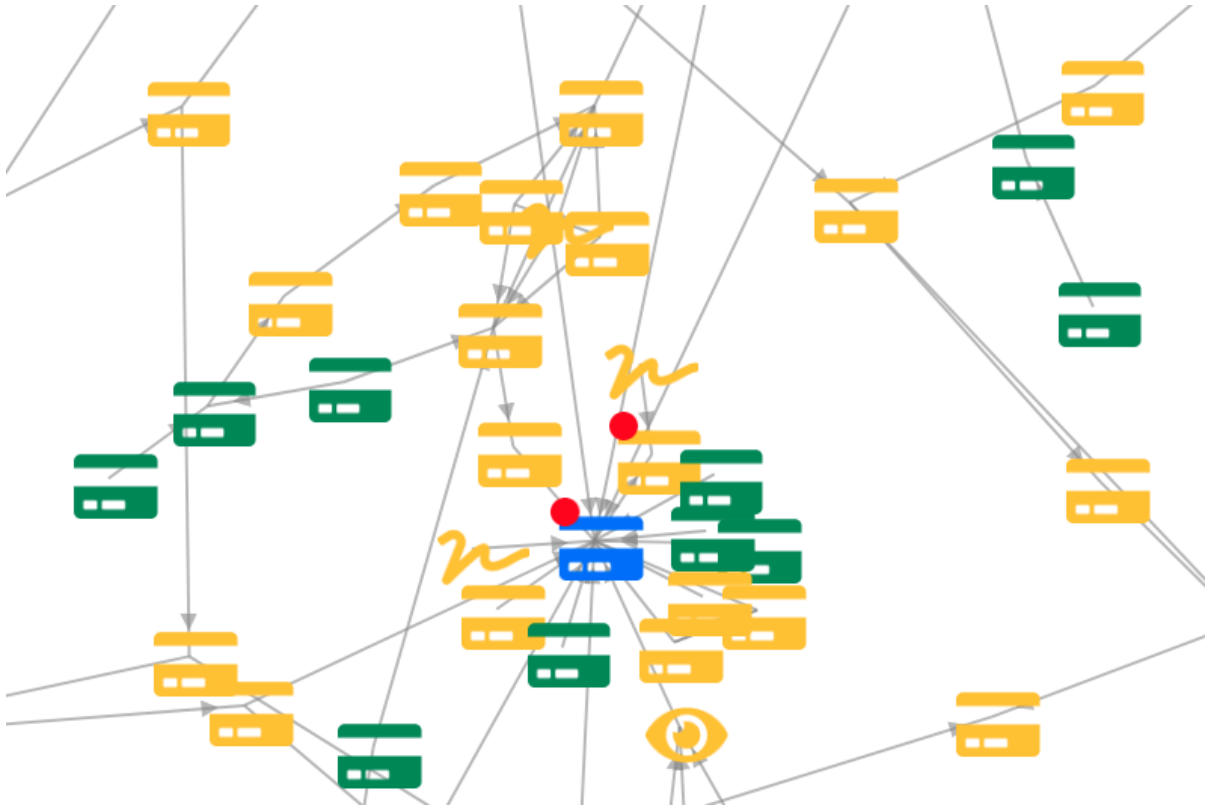
Ecosystem insights: inter-certificate relations

- As of early 2024, the graph has 5601 vertices (products) and 2966 edges (connections).
- Two fundamental reasons to reference another product:
  - **Component reuse**
  - **Predecessor**
- Smartcards massively using certified dependencies (61.78%).
- Smartcard-unrelated products rarely have certified dependencies (2.77%).
- Average smartcard reaches 2 other certified products.

Ecosystem insights: excerpt of the reference graph



Ecosystem insights: excerpt of the reference graph



Ecosystem insights: core of the graph

Ecosystem insights: core of the graph

- Just a dozen of products impact more than 10%

  active products at any given time.

Ecosystem insights: core of the graph

- Just a dozen of products impact more than 10% active products at any given time.
- In 2023, just 10 ICs are used in **23%** of active certified products.

Ecosystem insights: core of the graph

- Just a dozen of products impact more than 10% active products at any given time.
- In 2023, just 10 ICs are used in **23%** of active certified products.

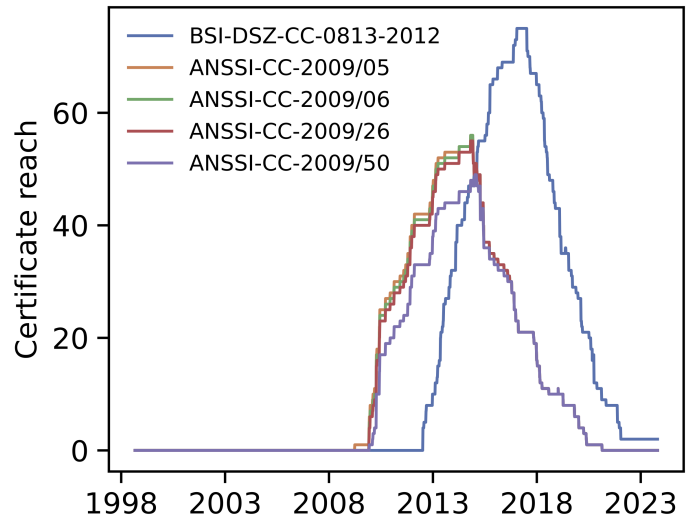


Figure: Top-5 popular ICs.

Ecosystem insights: impact of RoCA

Ecosystem insights: impact of RoCA

- In the end, RoCA likely impacted 50+ certified products.

Ecosystem insights: impact of RoCA

- In the end, RoCA likely impacted 50+ certified products.
- We modelled a vulnerability propagation from the high-reach ICs.

Ecosystem insights: impact of RoCA

- In the end, RoCA likely impacted 50+ certified products.
- We modelled a vulnerability propagation from the high-reach ICs.
- The vulnerability propagates to (up to) 70% of the products that reference the IC.

Ecosystem insights: impact of RoCA

- In the end, RoCA likely impacted 50+ certified products.
- We modelled a vulnerability propagation from the high-reach ICs.
- The vulnerability propagates to (up to) 70% of the products that reference the IC.
- RoCA is no outlier, it is an expected value!

Lessons learnt

Lessons learnt

- Data analysis of human-centric documents is hard.

Lessons learnt

- Data analysis of human-centric documents is hard.
- Smartcards are prominent in the ecosystem.

Lessons learnt

- Data analysis of human-centric documents is hard.
- Smartcards are prominent in the ecosystem.
- Certified products suffer from weaknesses similar to open-source software.

Lessons learnt

- Data analysis of human-centric documents is hard.
- Smartcards are prominent in the ecosystem.
- Certified products suffer from weaknesses similar to open-source software.
- Certified products are not isolated, they have complex relations.

Lessons learnt

- Data analysis of human-centric documents is hard.
- Smartcards are prominent in the ecosystem.
- Certified products suffer from weaknesses similar to open-source software.
- Certified products are not isolated, they have complex relations.
- Our results (updated weekly) are available from seccerts.org.

Lessons learnt

- Data analysis of human-centric documents is hard.
- Smartcards are prominent in the ecosystem.
- Certified products suffer from weaknesses similar to open-source software.
- Certified products are not isolated, they have complex relations.
- Our results (updated weekly) are available from seccerts.org.

Follow-up

Lessons learnt

- Data analysis of human-centric documents is hard.
- Smartcards are prominent in the ecosystem.
- Certified products suffer from weaknesses similar to open-source software.
- Certified products are not isolated, they have complex relations.
- Our results (updated weekly) are available from seccerts.org.

Follow-up

- Talk to us at the conference.

Lessons learnt

- Data analysis of human-centric documents is hard.
- Smartcards are prominent in the ecosystem.
- Certified products suffer from weaknesses similar to open-source software.
- Certified products are not isolated, they have complex relations.
- Our results (updated weekly) are available from seccerts.org.

Follow-up

- Talk to us at the conference.
- Visit seccerts.org.

Lessons learnt

- Data analysis of human-centric documents is hard.
- Smartcards are prominent in the ecosystem.
- Certified products suffer from weaknesses similar to open-source software.
- Certified products are not isolated, they have complex relations.
- Our results (updated weekly) are available from seccerts.org.

Follow-up

- Talk to us at the conference.
- Visit seccerts.org.
- Mail us your feature requests.

Learn more at seccerts.org

Slides at ajanovsky.cz/euca.pdf