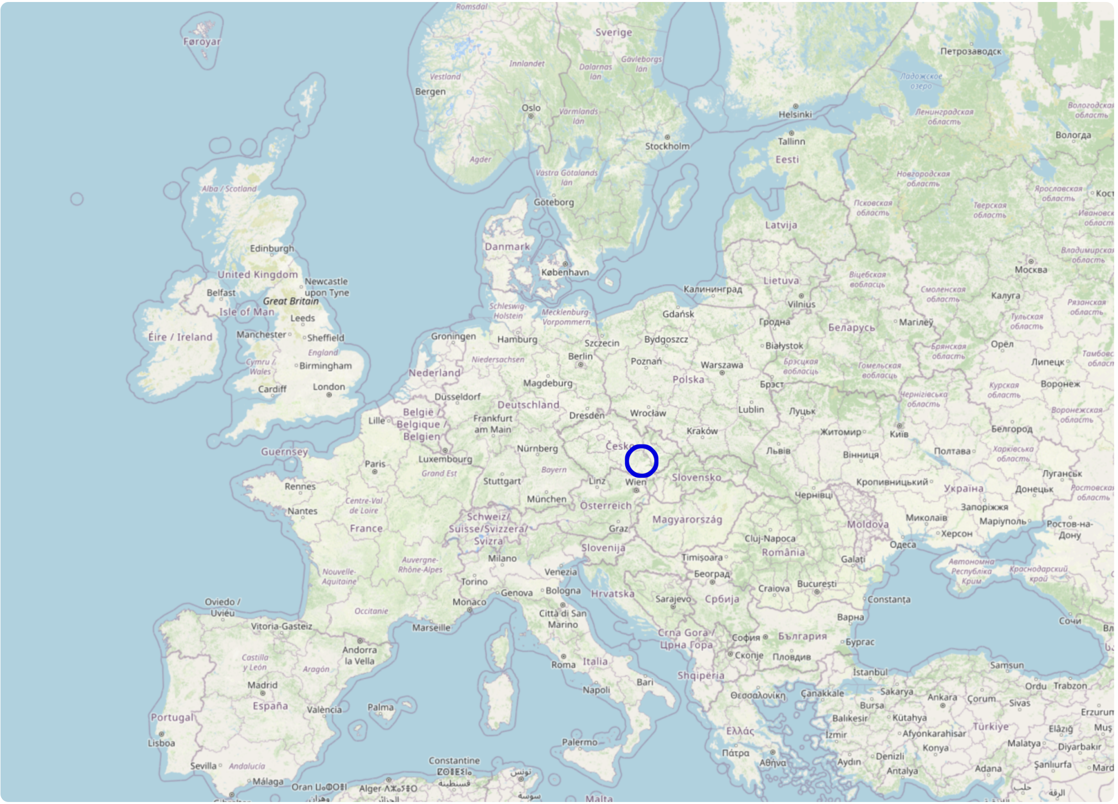
MUNI
FI

Chain of trust: Unravelling references among Common Criteria certified products

IFIP-SEC 2024

Adam Janovsky, Lukasz Chmielewski, Petr Svenda, Jan Jancar, Vashek Matyas

Adam Janovsky | adamjanovsky@mail.muni.cz


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

MUNI

Common Criteria 101

Common Criteria is a certification framework in which:

Common Criteria 101

Common Criteria is a certification framework in which:

1. Users specify their security requirements.

Common Criteria 101

Common Criteria is a certification framework in which:

1. Users specify their security requirements.
2. Vendors implement the security requirements in their products.

Common Criteria 101

Common Criteria is a certification framework in which:

1. Users specify their security requirements.
2. Vendors implement the security requirements in their products.
3. Evaluation laboratories evaluate the security of the products.

Common Criteria 101

Common Criteria is a certification framework in which:

1. Users specify their security requirements.
2. Vendors implement the security requirements in their products.
3. Evaluation laboratories evaluate the security of the products.
4. Certification bodies certify the products security by checking the correctness of all steps.

Common Criteria 101

Common Criteria is a certification framework in which:

1. Users specify their security requirements.
2. Vendors implement the security requirements in their products.
3. Evaluation laboratories evaluate the security of the products.
4. Certification bodies certify the products security by checking the correctness of all steps.

(This is a summary by Victor Lomne from ANSSI.)

2017: Return of the coppersmith attack (RoCA)

2017: Return of the coppersmith attack (RoCA)

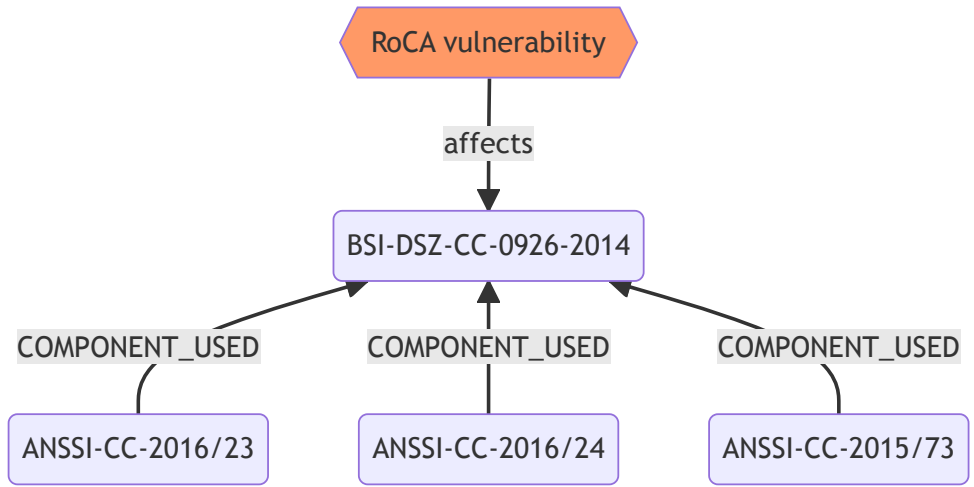
- CVE-2017-15361, practical factorization of widely used RSA moduli.

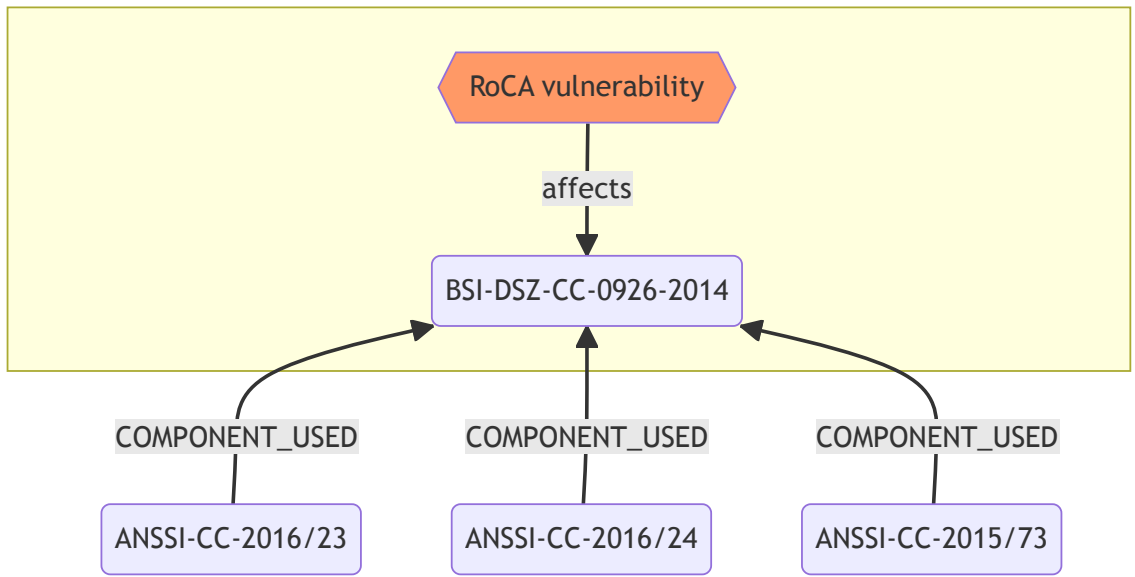
2017: Return of the coppersmith attack (RoCA)

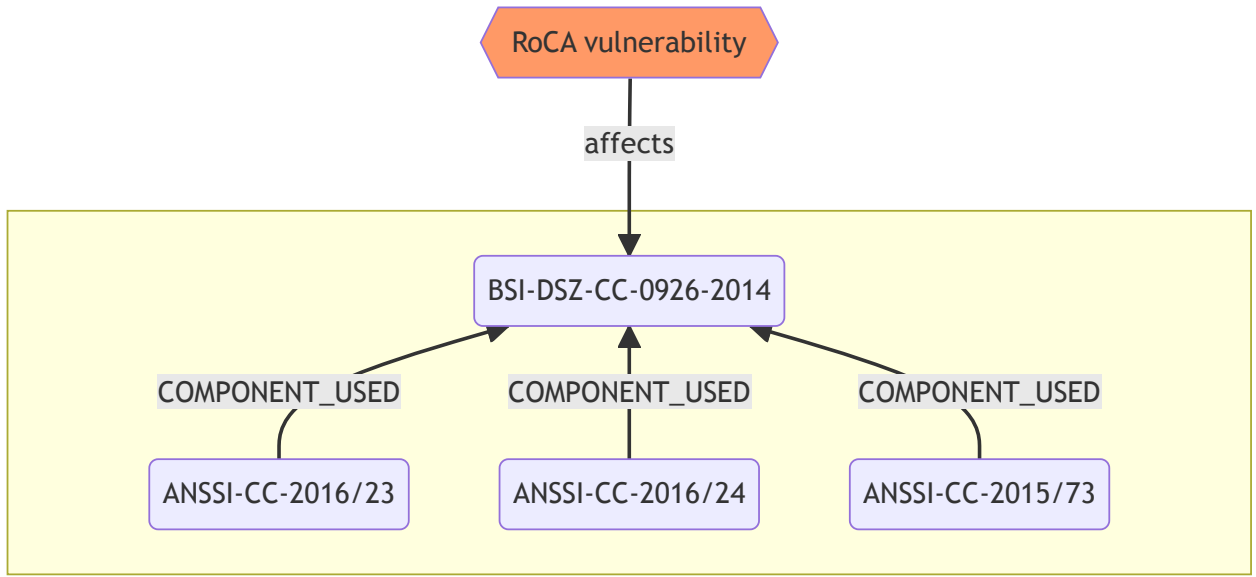
- CVE-2017-15361, practical factorization of widely used RSA moduli.
- Billion+ devices affected.

2017: Return of the coppersmith attack (RoCA)

- CVE-2017-15361, practical factorization of widely used RSA moduli.
- Billion+ devices affected.
- ⚠ *How many devices certified under Common Criteria 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

sec-certs.org

sec-certs: Examining the security certification practice for better vulnerability mitigation

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

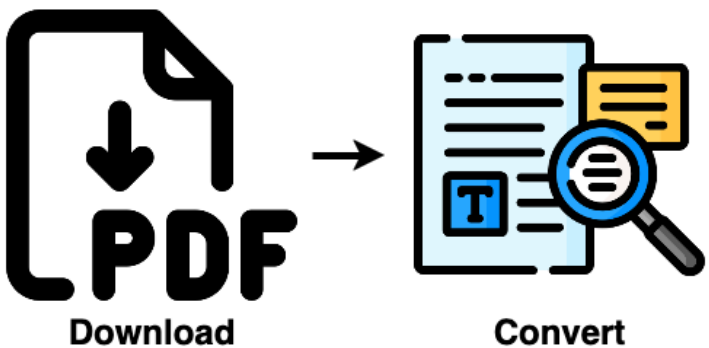
- cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*:*

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

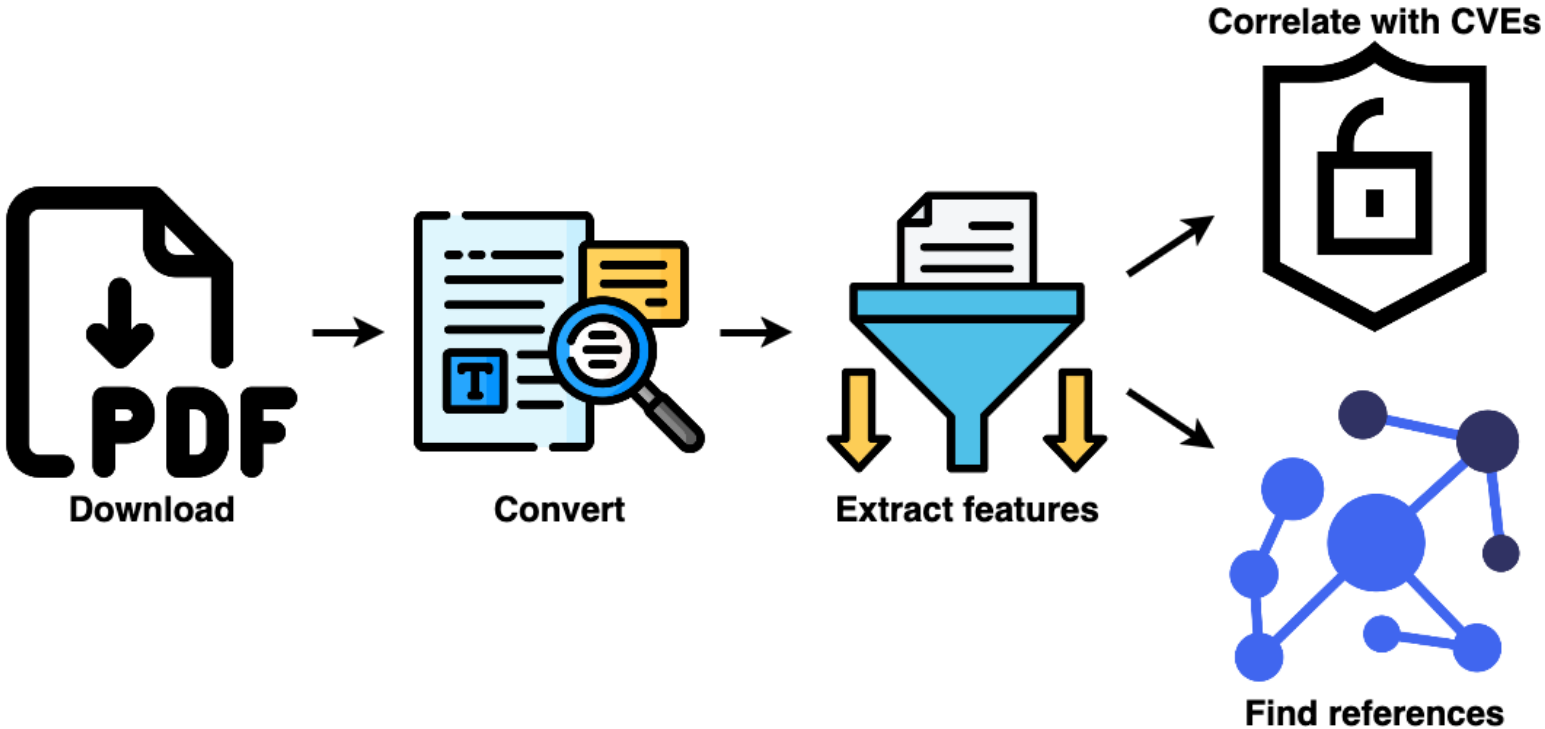
Processing CC artifacts

Processing CC artifacts



Processing CC artifacts

Processing CC artifacts



Building the reference graph

Building the reference graph

- Each device is a **vertex**.

Building the reference graph

- Each device is a **vertex**.
- A reference from device A to device B is a **directed edge**.
  - The reference is indicated by the presence of a foreign certificate ID within the artifacts.

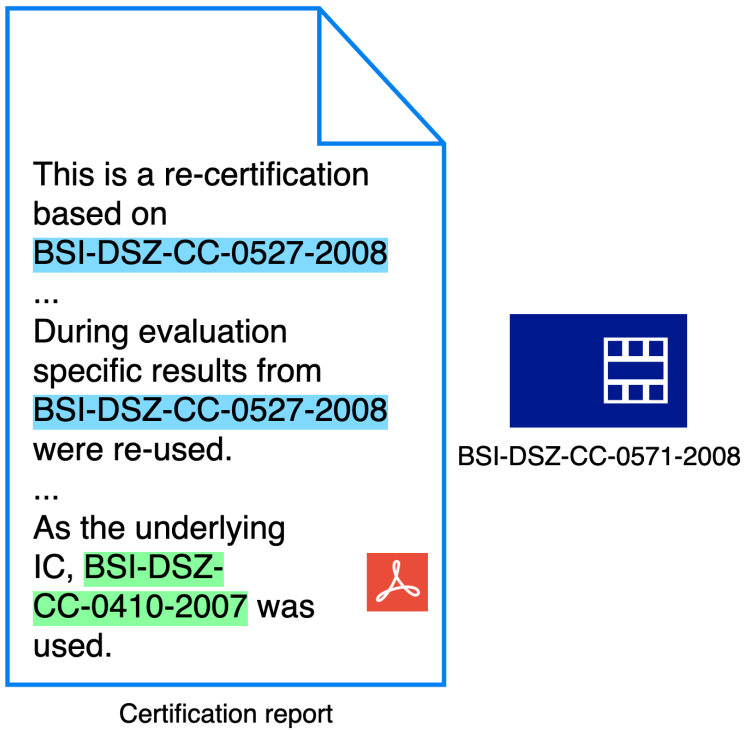
Building the reference graph

- Each device is a **vertex**.
- A reference from device A to device B is a **directed edge**.
  - The reference is indicated by the presence of a foreign certificate ID within the artifacts.
- The categorical context of the reference, e.g. `` `COMPONENT_USED` ``, is an **edge label**.

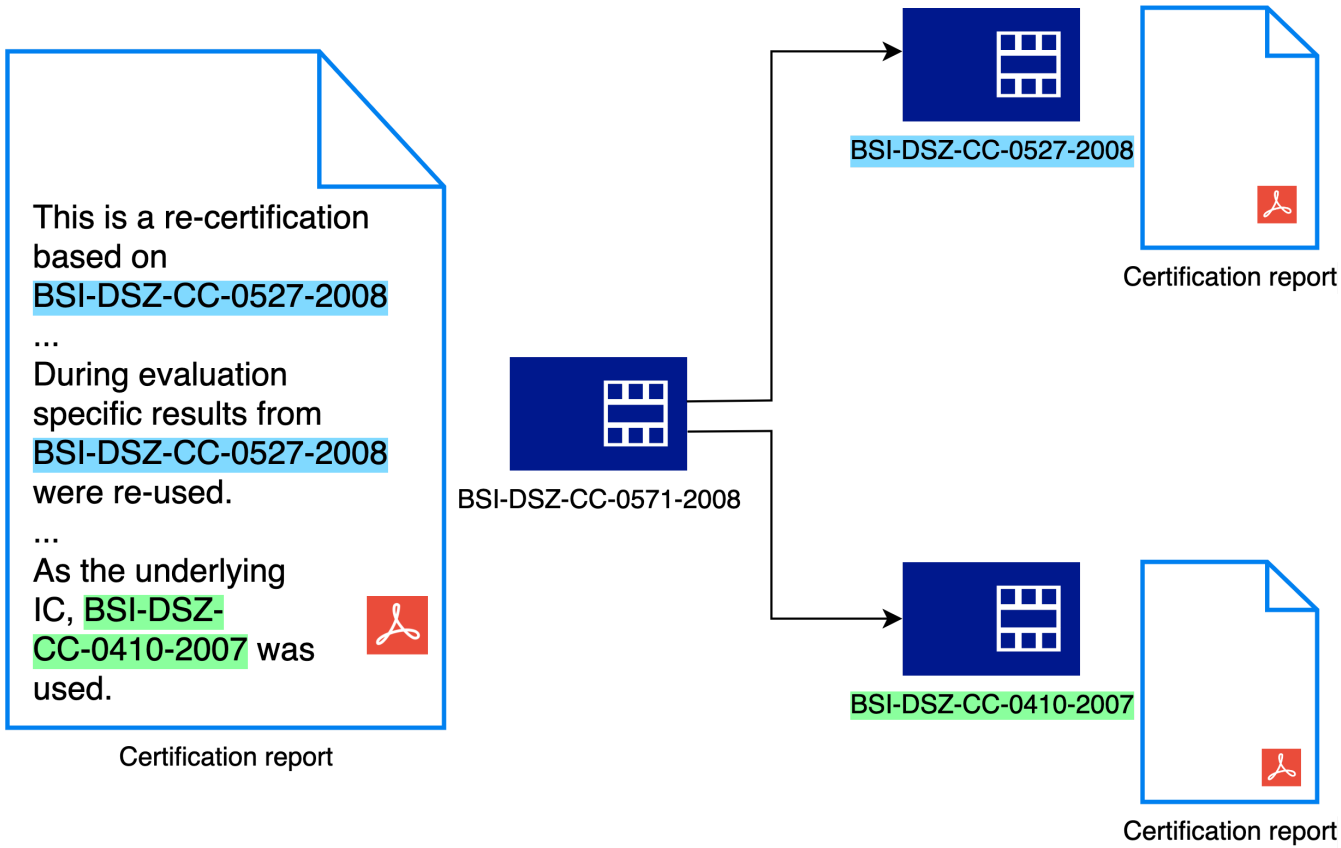
Building the reference graph

- Each device is a **vertex**.
- A reference from device A to device B is a **directed edge**.
  - The reference is indicated by the presence of a foreign certificate ID within the artifacts.
- The categorical context of the reference, e.g. `` `COMPONENT_USED` ``, is an **edge label**.
- We work with **5394** vertices and **2712** edges.

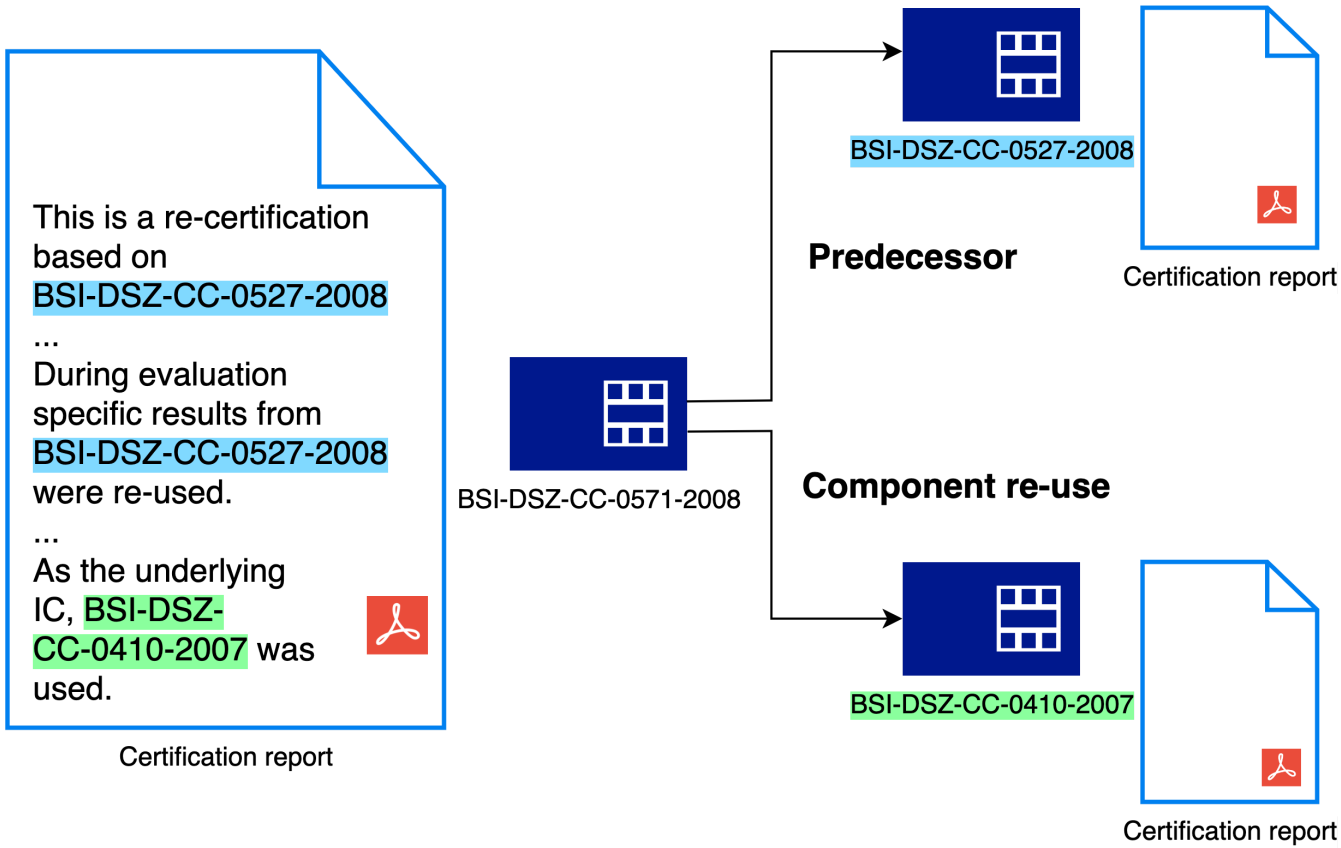
Building the reference graph



Building the reference graph



Building the reference graph



Inferring reference contexts

Manual annotations

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.
- Two co-authors annotated 400 references (**15%**), agreement **0.94**.

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.
- Two co-authors annotated 400 references (**15%**), agreement **0.94**.
- *75% of references constitute real dependencies, 25% are predecessor references.*

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.
- Two co-authors annotated 400 references (**15%**), agreement **0.94**.
- *75% of references constitute real dependencies, 25% are predecessor references.*

Training a model

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.
- Two co-authors annotated 400 references (**15%**), agreement **0.94**.
- *75% of references constitute real dependencies, 25% are predecessor references.*

Training a model

1. Isolate segments around certificate identifiers in pdfs.

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.
- Two co-authors annotated 400 references (**15%**), agreement **0.94**.
- *75% of references constitute real dependencies, 25% are predecessor references.*

Training a model

1. Isolate segments around certificate identifiers in pdfs.
2. Use sentence transformers to encode the segments.

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.
- Two co-authors annotated 400 references (**15%**), agreement **0.94**.
- *75% of references constitute real dependencies, 25% are predecessor references.*

Training a model

1. Isolate segments around certificate identifiers in pdfs.
2. Use sentence transformers to encode the segments.
3. Aggregate multiple embeddings related to single reference.

Inferring reference contexts

Manual annotations

- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.
- Two co-authors annotated 400 references (**15%**), agreement **0.94**.
- *75% of references constitute real dependencies, 25% are predecessor references.*

Training a model

1. Isolate segments around certificate identifiers in pdfs.
2. Use sentence transformers to encode the segments.
3. Aggregate multiple embeddings related to single reference.
4. Train a boosted tree classifier.

Inferring reference contexts

Manual annotations

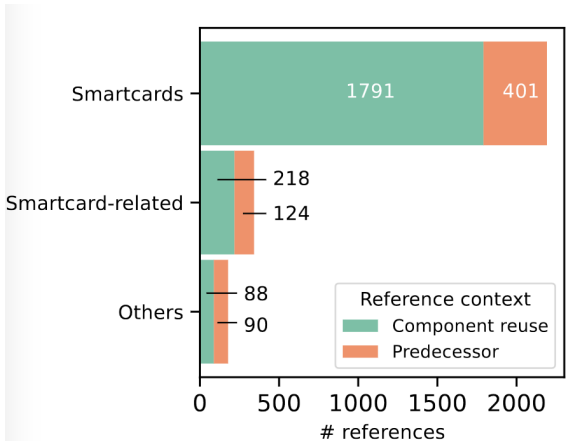
- Initial exploratory study of different contexts in 100 pdf documents to set up a codebook.
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`.
- Two co-authors annotated 400 references (**15%**), agreement **0.94**.
- *75% of references constitute real dependencies, 25% are predecessor references.*

Training a model

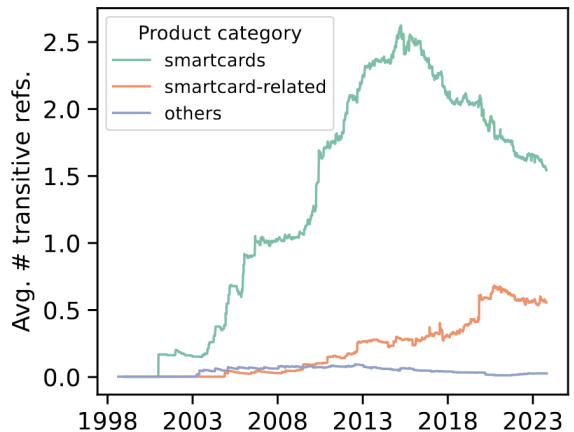
1. Isolate segments around certificate identifiers in pdfs.
2. Use sentence transformers to encode the segments.
3. Aggregate multiple embeddings related to single reference.
4. Train a boosted tree classifier.

Weighted F1 score: **0.89**, combine with 15% of manually annotated dataset.

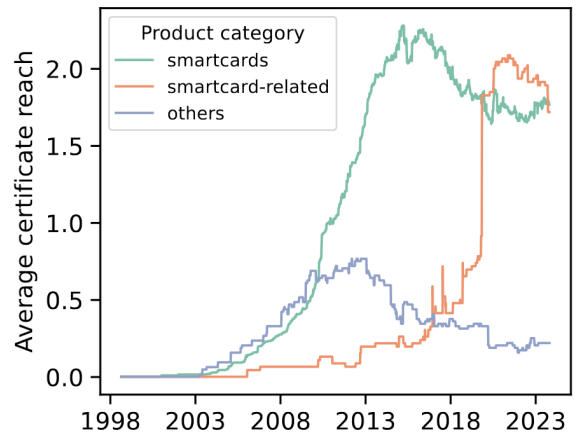
Ecosystem trends



(a) Reference context freq.



(b) Avg. # trans. refs



(c) Average product reach

High-reach components

High-reach components

- Top-10 smartcards are used as (transitive) dependencies in 16% of all active smartcards.

High-reach components

- Top-10 smartcards are used as (transitive) dependencies in 16% of all active smartcards.
- These are microcontrollers, typically with cryptographic functionality.

High-reach components

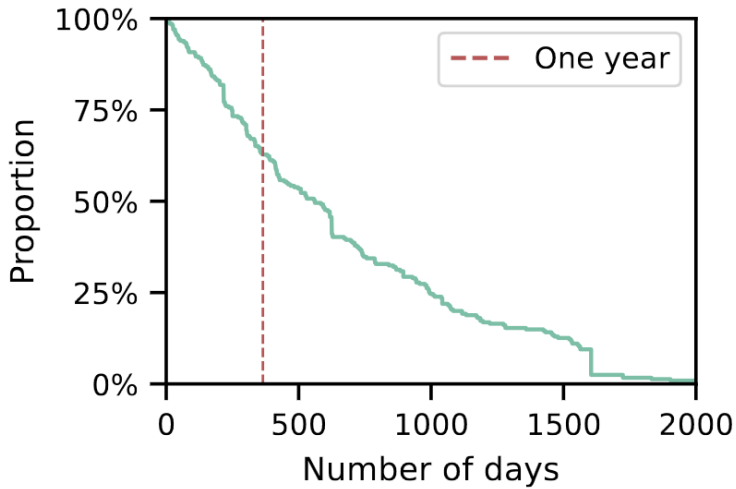
- Top-10 smartcards are used as (transitive) dependencies in 16% of all active smartcards.
- These are microcontrollers, typically with cryptographic functionality.
- Higher reach is positively associated with higher evaluation assurance level (Spearman's rank 0.23, $2.73\mathrm{e}^{-23}$ p-value).

High-reach components

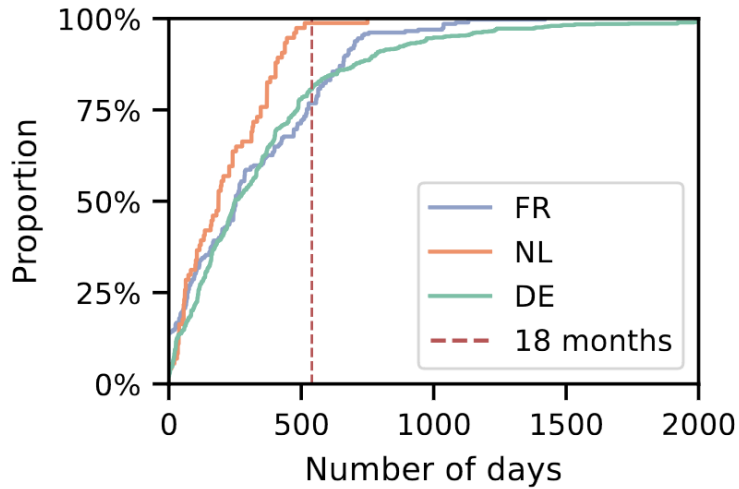
- Top-10 smartcards are used as (transitive) dependencies in 16% of all active smartcards.
- These are microcontrollers, typically with cryptographic functionality.
- Higher reach is positively associated with higher evaluation assurance level (Spearman's rank 0.23, $2.73\mathrm{e}^{-23}$ p-value).
- We also measured that a vulnerability in cryptographic functionality would spread from high-reach devices to approx. 70% of their dependants.

Ageing references

Each product is valid for 5 years, some schemes require re-evaluation after 18 months in composite chains.



(a) Ratio of component-reuse referenced certificates with > 0 reach at n days post-archival (only includes products with positive reach on the date of their archival).



(b) CDF: the age of the referenced certificate on the issuance date of the referencing certificate.

Summary

Summary

- We have developed a pipeline for automated processing of Common Criteria artifacts.

Summary

- We have developed a pipeline for automated processing of Common Criteria artifacts.
- The analysis is tedious due to artefacts produced by humans and meant to be consummed by humans.

Summary

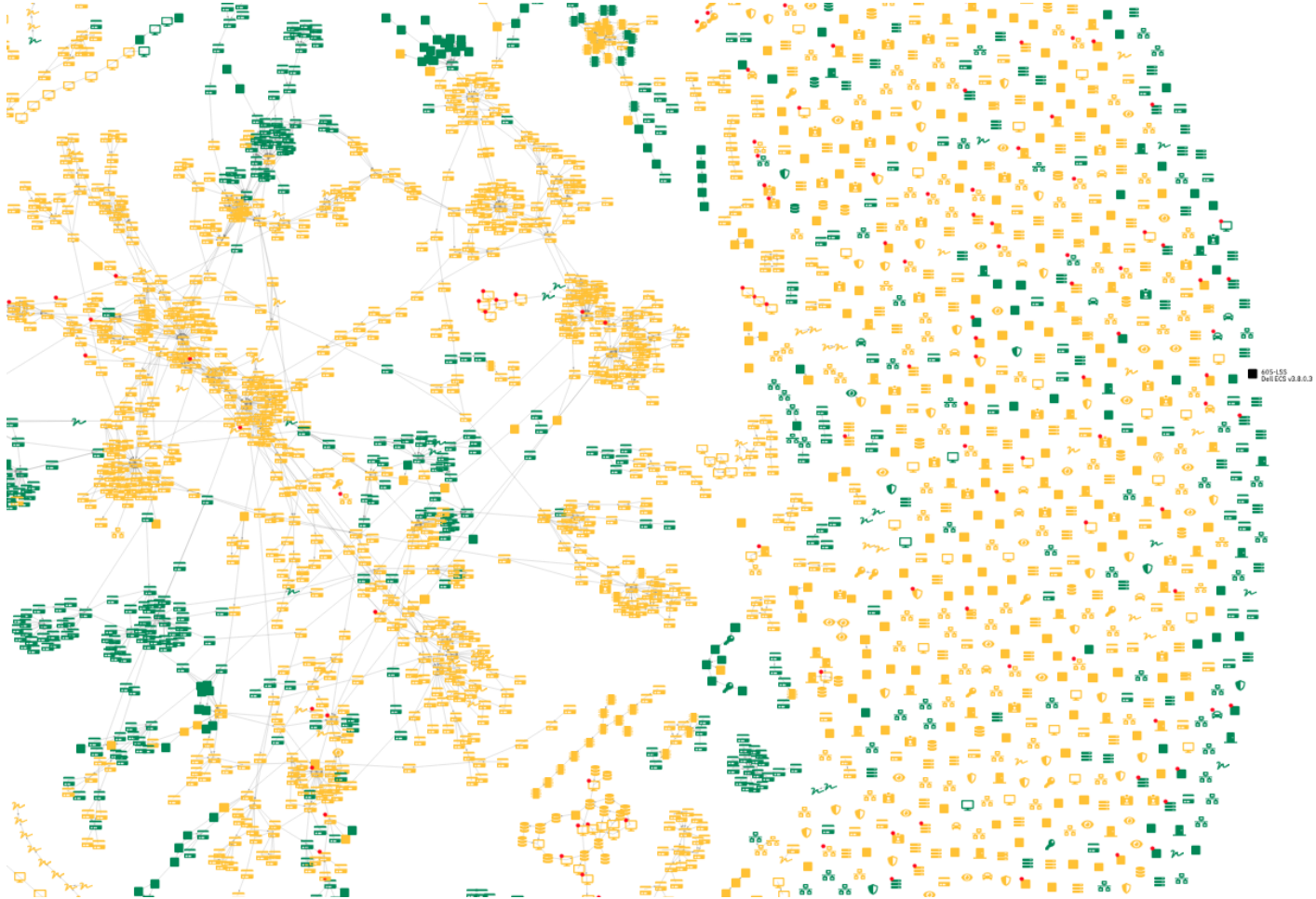
- We have developed a pipeline for automated processing of Common Criteria artifacts.
- The analysis is tedious due to artefacts produced by humans and meant to be consummed by humans.
- Actual dependencies can be inferred from inter-certificate references.

Summary

- We have developed a pipeline for automated processing of Common Criteria artifacts.
- The analysis is tedious due to artefacts produced by humans and meant to be consummed by humans.
- Actual dependencies can be inferred from inter-certificate references.
- Certified dependencies popular among smartcards, more than 10% of all smartcards depend on top-10 smartcards.

Summary

- We have developed a pipeline for automated processing of Common Criteria artifacts.
- The analysis is tedious due to artefacts produced by humans and meant to be consummed by humans.
- Actual dependencies can be inferred from inter-certificate references.
- Certified dependencies popular among smartcards, more than 10% of all smartcards depend on top-10 smartcards.
- Affecting 50+ certified products, RoCA was not an outlier.


605-LSS
Dell ECS v3.8.0.3

Learn more at sec-certs.org

Slides at ajanovsky.cz/ifip-sec.pdf