sec-certs

Enhancing Transparency: Insights From the Common Criteria Certification Ecosystem

Vashek Matyas *matyas@fi.muni.cz*
Centre for Research on Cryptography and Security, Masaryk University, Czechia
Joint work with Petr Svenda, Jan Jancar, Adam Janovsky, Martin Ukrop, Stanislav Bobon, Martin Fryan, Milan Broz, Jaroslav Reznik, and many others (thank you all!)

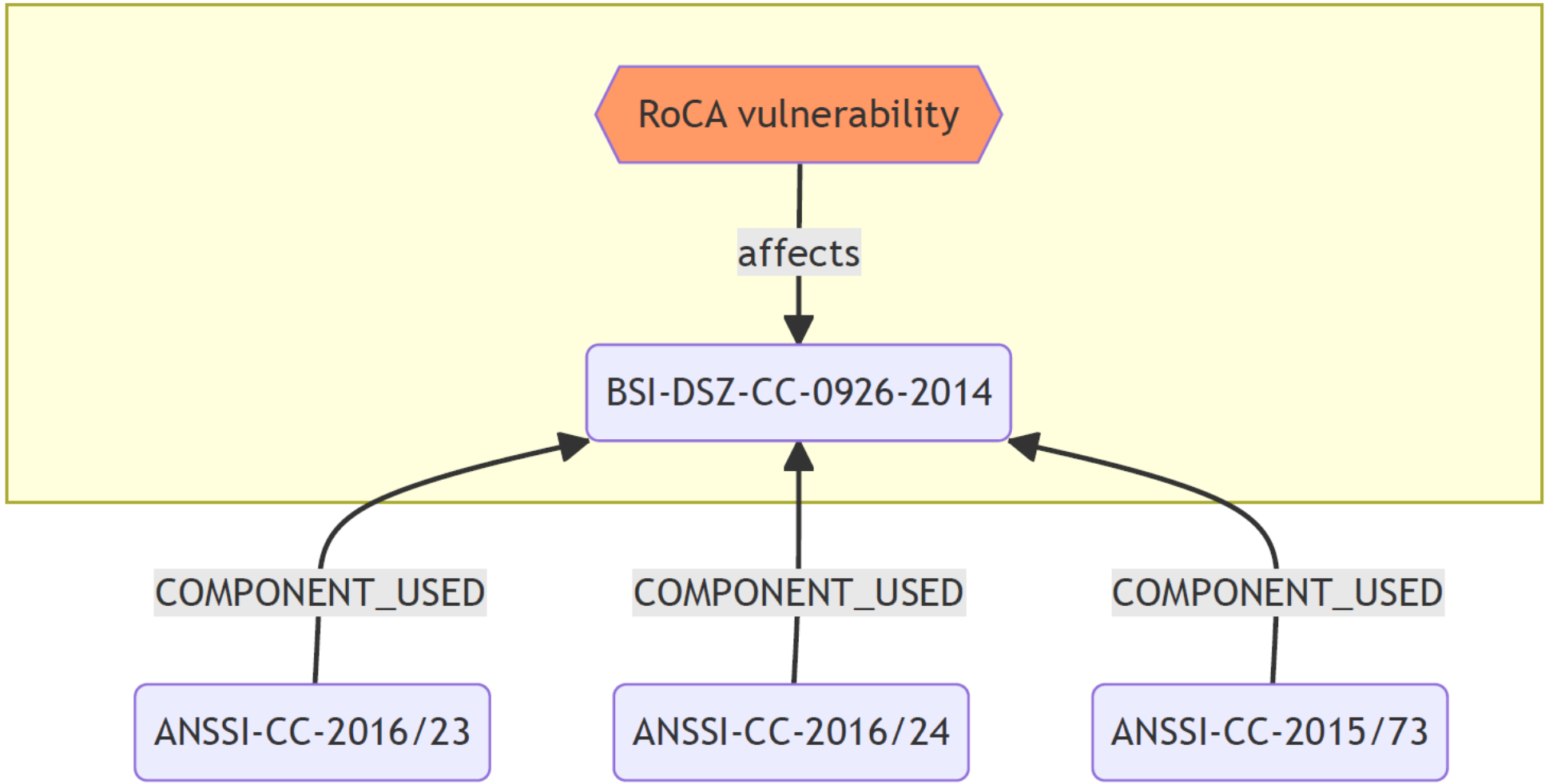
CROCS
Centre for Research on Cryptography and Security

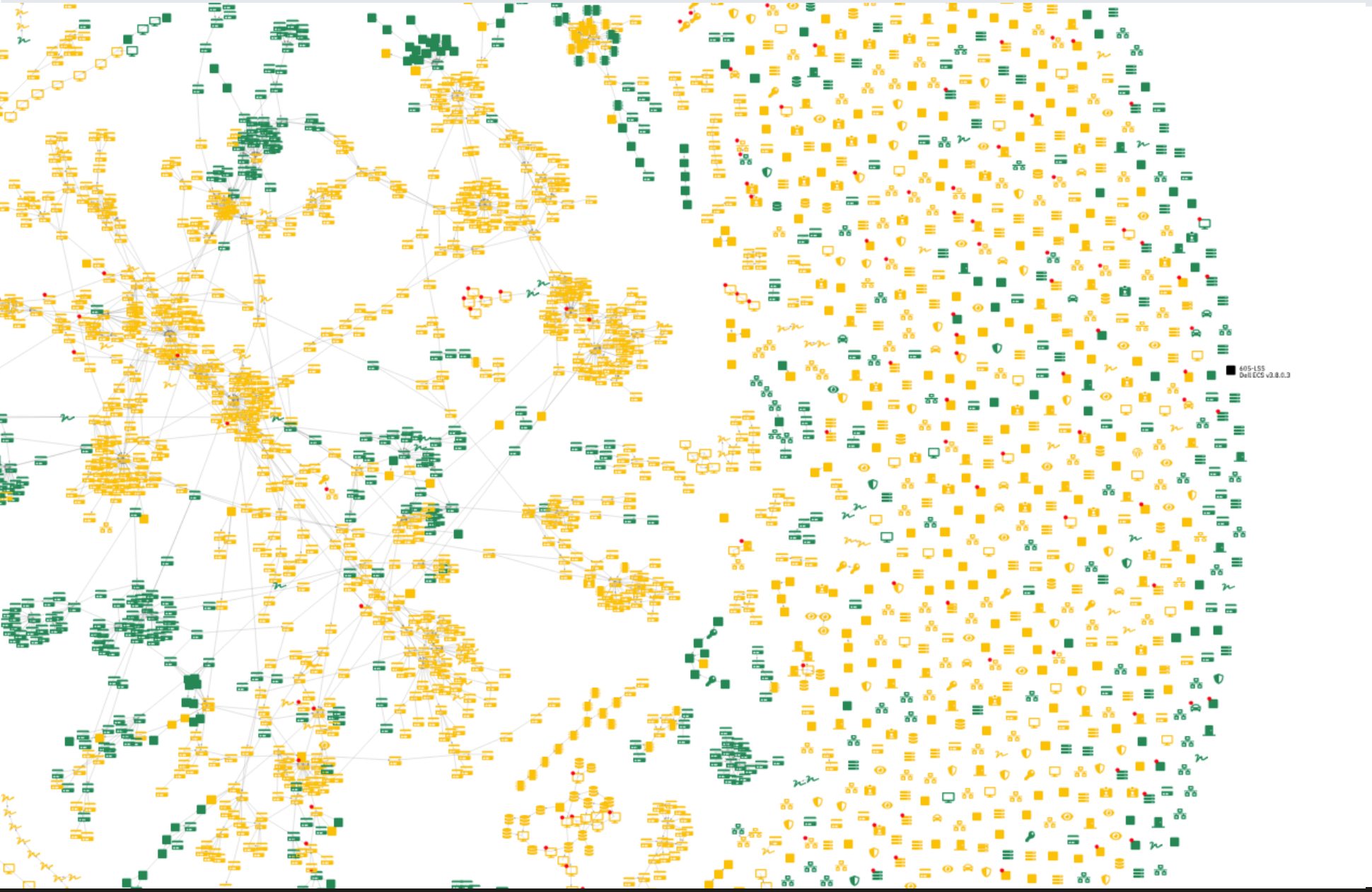
CVE-2017-15361 (RoCA)

- [CVE-2017-15361]: practical factorization of certain RSA keys.
- Billion+ devices affected.

- ⚠ How many products certified under Common Criteria are impacted?

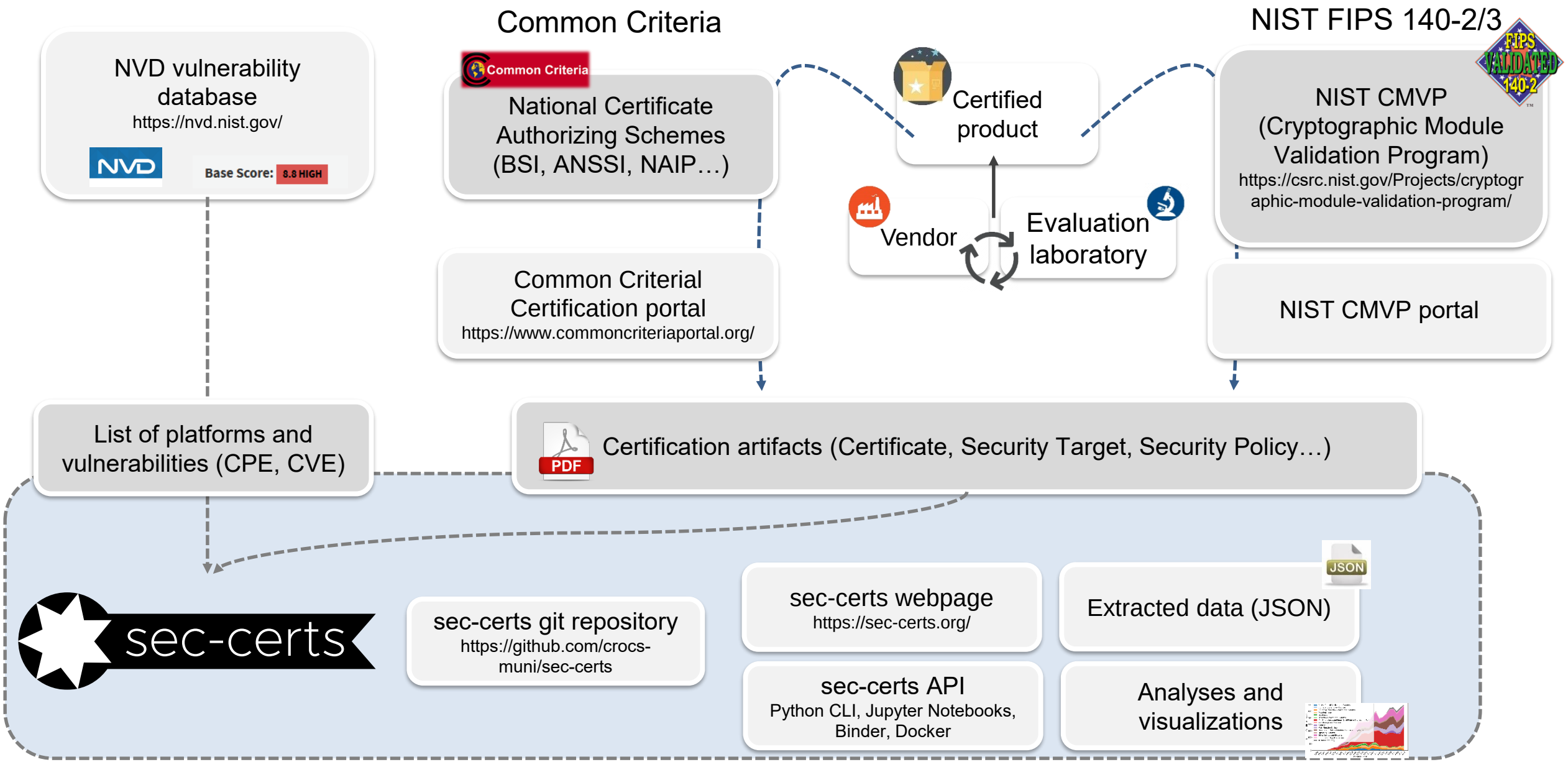
CVE-2017-15361




605-LSS
Dell ECS v3.8.0.3

What if you need help answering questions like

- What processor architectures are commonly used in certifications/products of interest?
- How do we compare with our competitors (their certified products)?
- Check how long evaluations take for certain labs, types of products, etc.


Common Criteria
NIST FIPS 140-2/3
NVD vulnerability database
https://nvd.nist.gov/
NVD
Base Score: 8.8 HIGH
Common Criteria
National Certificate Authorizing Schemes (BSI, ANSSI, NAIP…)
Certified product
Vendor
Evaluation laboratory
FIPS VALIDATED 140-2
NIST CMVP (Cryptographic Module Validation Program)
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/
Common Criterial Certification portal
https://www.commoncriteriaportal.org/
NIST CMVP portal
List of platforms and vulnerabilities (CPE, CVE)
PDF
Certification artifacts (Certificate, Security Target, Security Policy…)
sec-certs
sec-certs git repository
https://github.com/crocs-muni/sec-certs
sec-certs webpage
https://sec-certs.org/
JSON
Extracted data (JSON)
sec-certs API
Python CLI, Jupyter Notebooks, Binder, Docker
Analyses and visualizations

Main functionality of *sec-certs.org* project

- Fulltext search over all CC and FIPS 140 certificates
- Continuous insight into certification ecosystem
- Extracted graph of references between certificates
- Mapping to NIST National Vulnerability Database (CVEs)
- Automatic notification of events for observed certificates (RSS feed)
- Correlation of certification requirements and vulnerability occurrence
- Python API for custom queries, preprocessed datasets for downloads
- Connecting additional metadata about certified items (tests, information)
- Local processing with inclusion of non-public documents

Users of the sec-certs.org tool

- Owners/users of certified devices / security researchers
  - What security claims are made?
  - What certificates to additionally monitor?
  - Notification after new (possibly relevant) vulnerability is found
  - Analyze impact of vulnerability (e.g., ROCA case)
- Vendors of certified products
  - Are we under/over certifying with respect to competition?
  - Who is certifying products of our type and what were requirements in past?
- Certification bodies
  - Performance of labs, suspiciously short validity, non-standard cert. claims…
  - Impact of certification requirements (SARs) on the actual security

Users of the sec-certs.org tool

- Certification laboratories
  - Are we comparable with other laboratories? What are the trends?
- Government agencies & corporations
  - Processing additional non-public documents
  - Attaching additional metadata (test results, powertrace…) and its governance
    - Generate sec-certs “web” locally with additional information
- General public
  - Easy access to information (interactive webpage, info from multiple sources…)
  - Ecosystem insights: What is standardized? Change in time?

sec-certs.org as other metadata aggregator

… any future metadata overlay

RSA/ECC keys analysis

ECTester ecc analysis

Power traces (SCRUTINY)

TPMAlgTest

JCAlgTest performance results

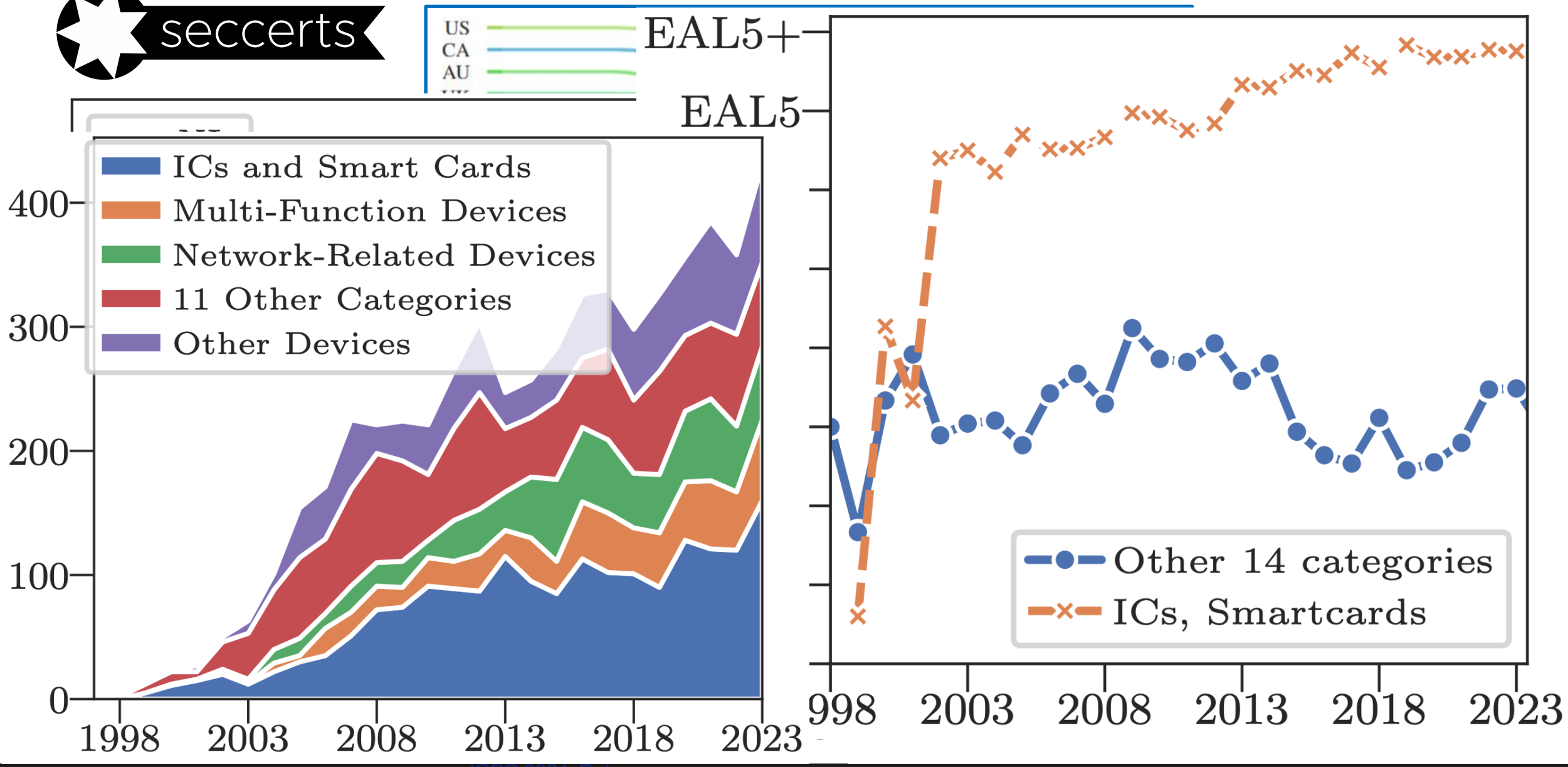
TRNG randomness assessment

CVE database

Certified items from Common Criteria, FIPS 140, EUCC, EMVCo…

VARIOUS ECOSYSTEM INSIGHTS

seccerts

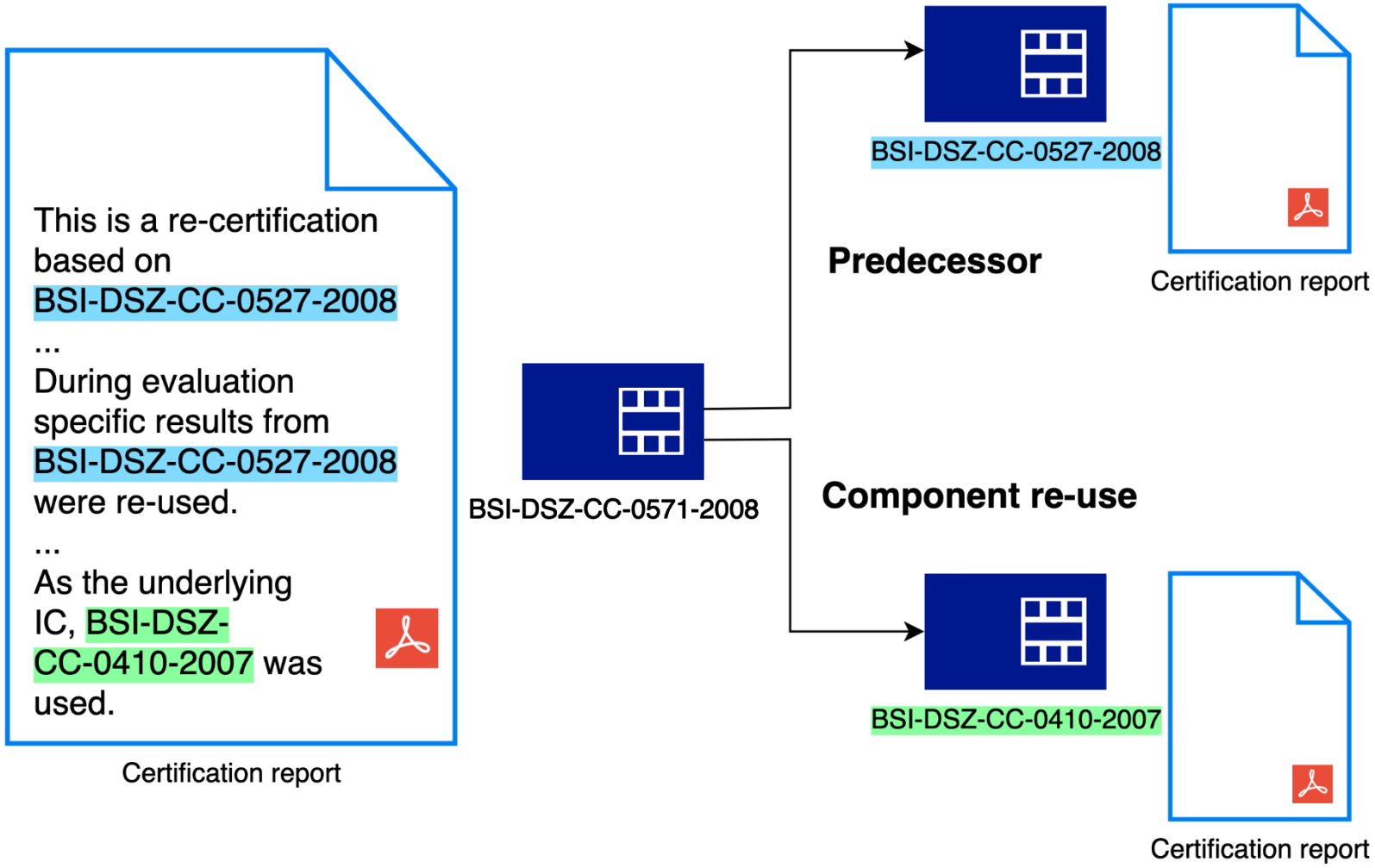

US
CA
AU
EAL5+
EAL5
ICs and Smart Cards
Multi-Function Devices
Network-Related Devices
11 Other Categories
Other Devices
400
300
200
100
0
1998
2003
2008
2013
2018
2023
Other 14 categories
ICs, Smartcards

REFERENCES, REFERENCES, REFER…

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 worked with 5780 vertices and 3007 edges.

Building the reference graph

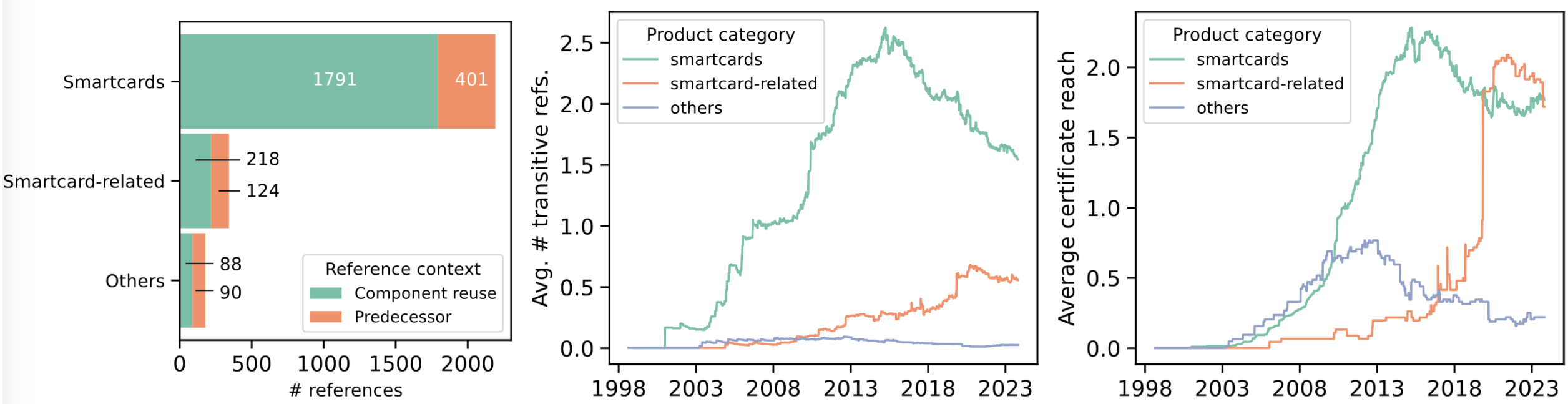


Inferring reference contexts

- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`
  - Component used (C)
  - Component shared (C)
  - Evaluation reused (C)
  - Re-evaluation (P)
  - Previous version (P)

- *75% of references constitute real dependencies, 25% are predecessor references.*

Ecosystem trends



(a) Reference context freq. (b) Avg. # trans. refs (c) Average product reach

Few major observations from reference analyses

- Top-10 products are used in 16% of all active smartcards.
  - These are microcontrollers, typically with cryptographic functionality.
- Higher reach is positively associated with higher evaluation assurance level.
- A vulnerability in cryptographic functionality would spread from high-reach devices to approx. 70% of their dependents.
  - Affecting 50+ certified products, RoCA was not an outlier.

In a nutshell

- We have developed a pipeline for automated processing of Common Criteria artifacts.
  - We also cover FIPS 140 and NVD vulnerability DB.
  - Mapping of dependencies among certificates
  - Continuous insights into certification ecosystem
  - Support for more transparency in security certifications

- The analysis is tedious due to artefacts *produced by humans and meant to be consumed by humans*.

Come and play – with sec-certs!

https://sec-certs.org/

Thank you for your attention!

sec-certs

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Cyber Security for Europe

Red Hat