Use Case Related to the evaluation of SimplySign Signature Activation Module with the Highest Attack Potential

Elżbieta Andrukiewicz
Piotr Krawiec
National Institute of Telecommunications
– State Research Institute

Ałła Stoliarowa-Myć
Asseco Data Systems Inc.

20b

Agenda

- Brief presentation of the Developer and ITSEF
- High attack potential required by Common Criteria- how to assess the atack potential in absence of reference documents?
- Description of methods of attack potential calculation
- Presentation of the use case
- Results related to the TOE and other components that protect the TOE
- Actual calculations of attack potential for the use case
- Benefits for the Developer
- Conclusions

Asseco Group – a global software producer

over 30 years of experience

Presence in 60 countries

Listed on stock exchanges
in Warsaw, New York and Tel Aviv

6th largest software house
in Europe

EUR 3.2 bn revenues in 2021

30.4 thous. employees

EUR 318 m operating profit in 2021

EUR 640 m dividends
paid

Certum - Trust Service Provider is a global supplier of Security and Trust Services

Experience. Safety. Trust.

6 continents
where Certum services operate

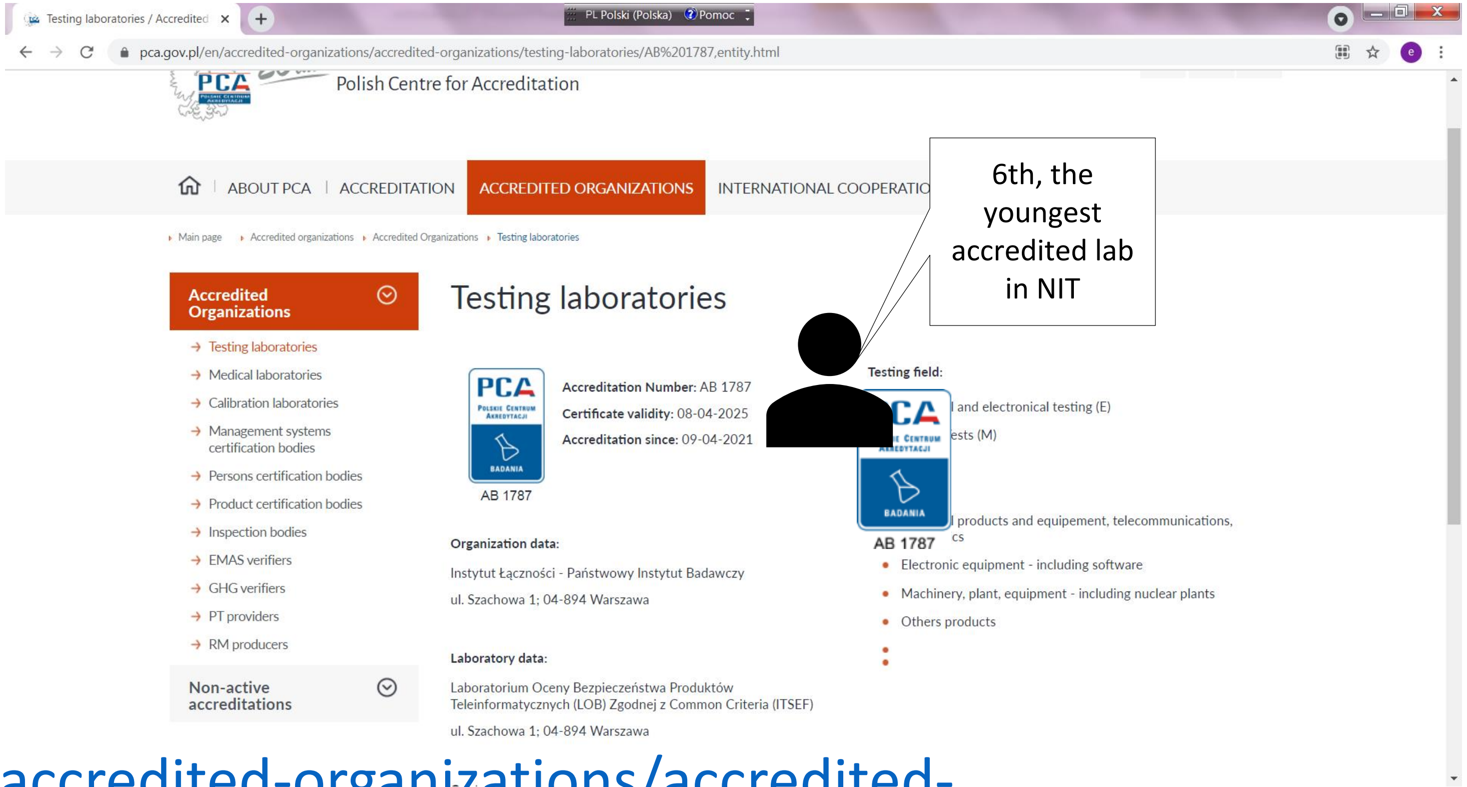
+10 million
certificates issued

+1.1 thousand
outlets

380 thousand
clients from all around the world

+400
business partners around the world

Accredited ITSEF in the National Institute of Telecommunications



Testing laboratories

Accreditation Number: AB 1787

Certificate validity: 08-04-2025

Accreditation since: 09-04-2021

Organization data:

Instytut Łączności - Państwowy Instytut Badawczy

ul. Szachowa 1; 04-894 Warszawa

Laboratory data:

Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych (LOB) Zgodnej z Common Criteria (ITSEF)

ul. Szachowa 1; 04-894 Warszawa

Testing field:

l and electronical testing (E)

ests (M)

l products and equipement, telecommunications, cs

- Electronic equipment - including software
- Machinery, plant, equipment - including nuclear plants
- Others products
-
-

6th, the youngest accredited lab in NIT

https://www.pca.gov.pl/en/accredited-organizations/accredited-organizations/testing-laboratories/AB%201787,entity.html

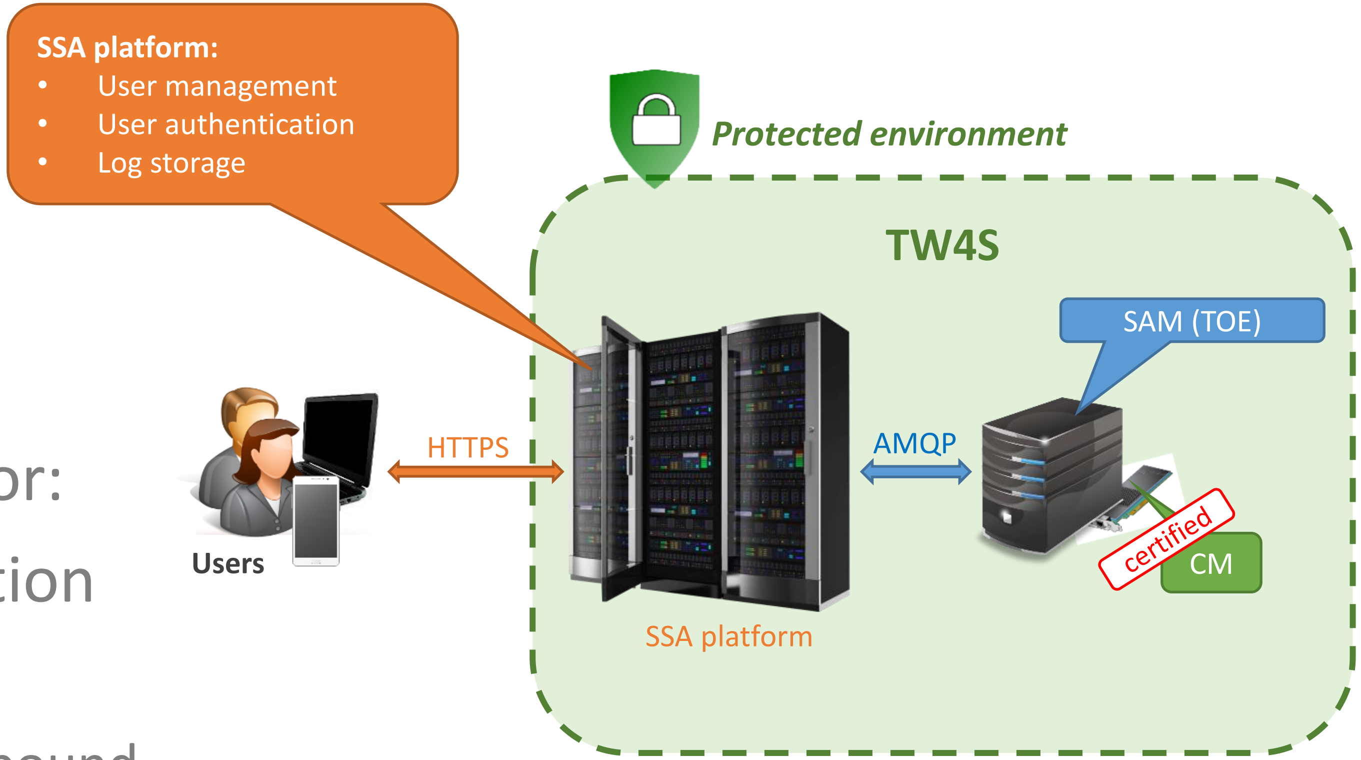
Proven capabilities to perform attacks on software with the attack potential ‚high’

TOE - Signature Activation Module (SAM)

SimplySign is a TW4S (Trustworthy System Supporting Server Signing) system that offers a remote qualified electronic signature as a service.

TOE (**SimplySign SAM**) is responsible for:

- authorization of the signature operation
- checking:
  - If the signer authentication is properly bound with the signing key and data to be signed
  - if the signer is authenticated



SSA platform:

- User management
- User authentication
- Log storage

Conformance Claims driven by Protection Profile

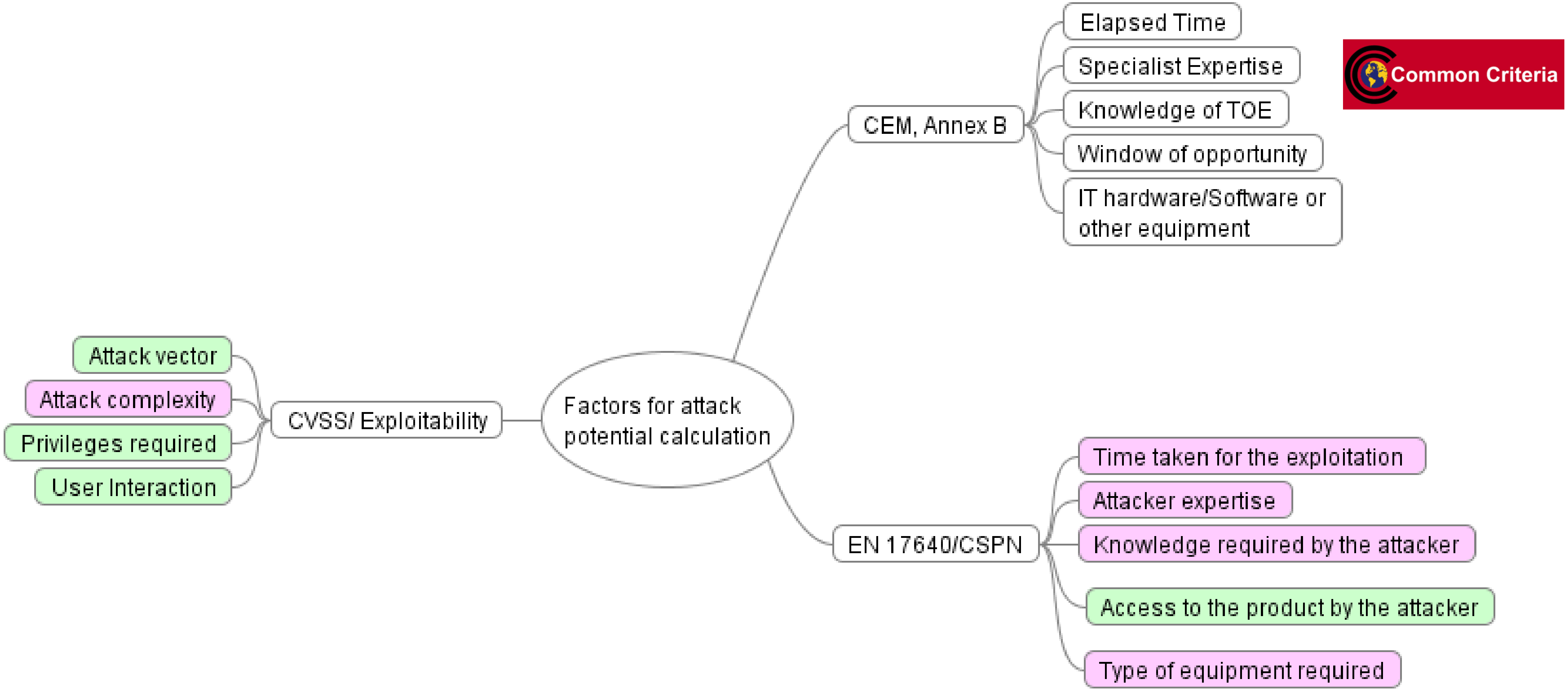
- The Security Target claims strict conformance with the Protection Profile contained in EN 419 241-2 *Trustworthy Systems Supporting Server Signing Part 2: Protection Profile (PP) for QSCD for Server Signing*.
- The assurance requirement of this security target is EAL4 augmented. Augmentation results from the selection of: AVA_VAN.5 Advanced methodical vulnerability analysis
- Attacks with the potential level „high" to be demonstrated in absence of any direct references to documents containing description of attacks with calculated potential on that level

Common Criteria

Referencing sources in support of the attack potential calculation for software

- CEM presents generic approach to the attack potential calculation
- Consider the following:
  - ISO/IEC TR 20004:2015 *Refining Software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045* followed by:
  - https://www.first.org/cvss/ Common Vulverability Scoring System (CVSS)
  - EN 17640:2022 *Fixed-time cybersecurity evaluation methodology (Annex F)*
- CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity
  - Part of these characteristics (Base measure) is „Exploitability” which relates to the attack potential

Useful mapping between scoring systems



Factors for attack potential calculation

CVSS/ Exploitability
- Attack vector
- Attack complexity
- Privileges required
- User Interaction

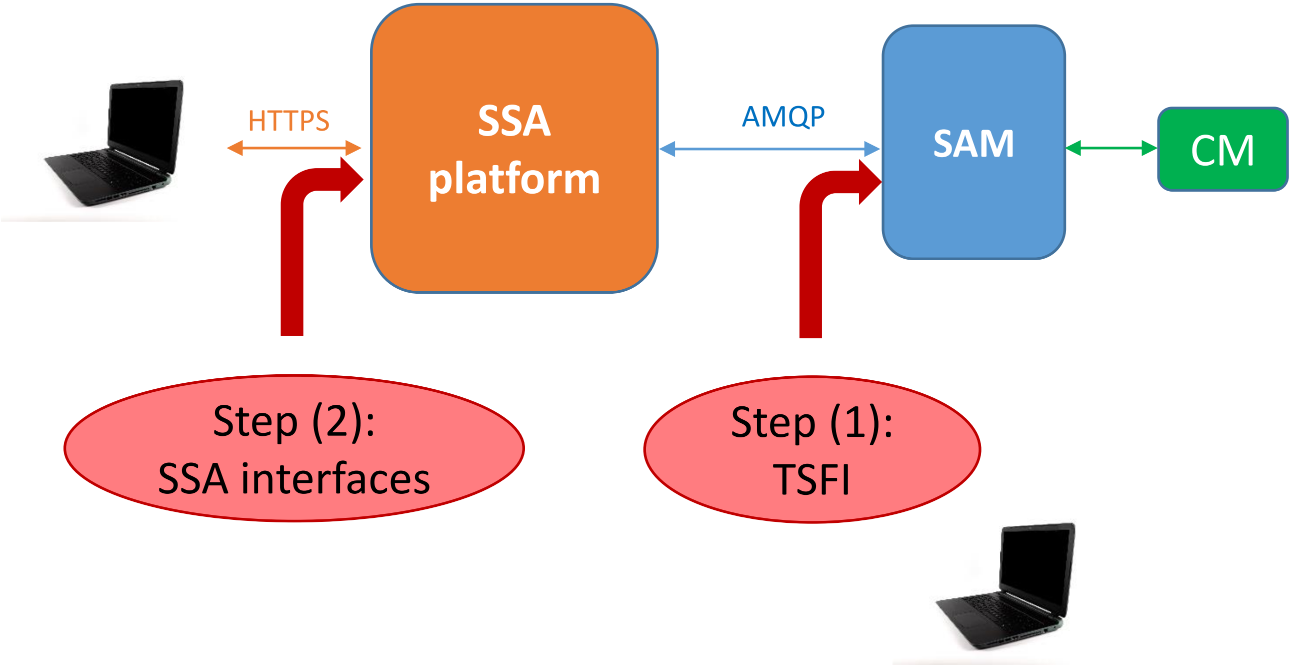
CEM, Annex B
- Elapsed Time
- Specialist Expertise
- Knowledge of TOE
- Window of opportunity
- IT hardware/Software or other equipment

Common Criteria

EN 17640/CSPN
- Time taken for the exploitation
- Attacker expertise
- Knowledge required by the attacker
- Access to the product by the attacker
- Type of equipment required

Vulnerability Analysis and pentesting – ITSEF approach

- Step (1) – vulnerability analysis and demonstration of its exploitability through the available TSFI
- Step (2) – verification of applicability of potential vulnerabilities in the TOE operational environment



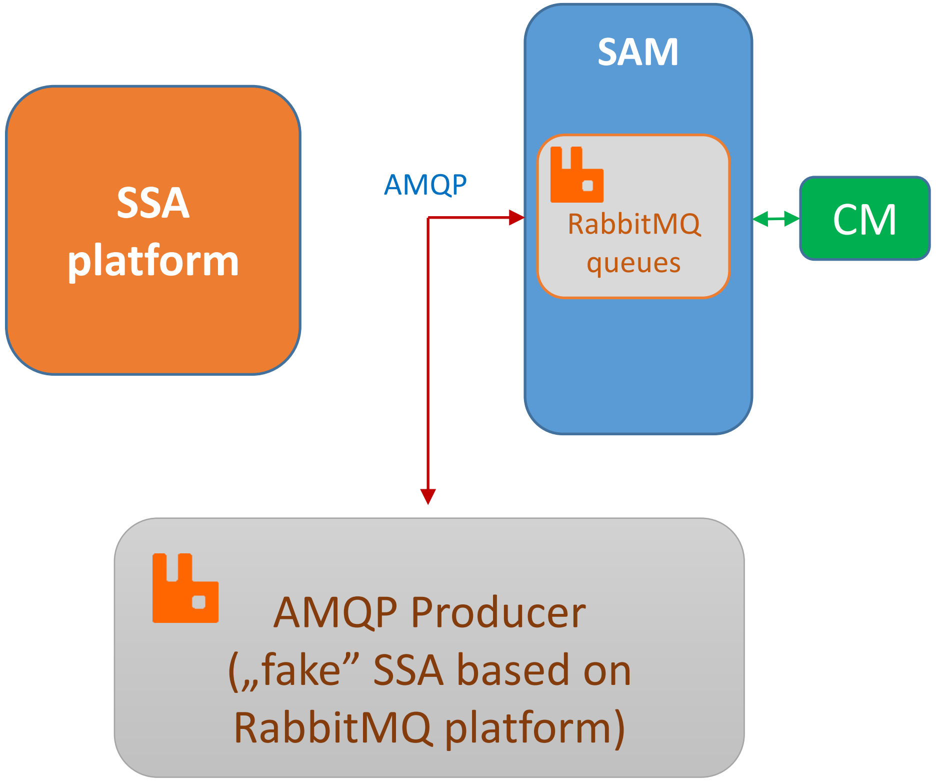
Step (1): TSFI vulnerability analysis and pentests

a) Analysis of the functionality, used protocols, source code

b) Identification of the entry points (RabbitMQ queues)

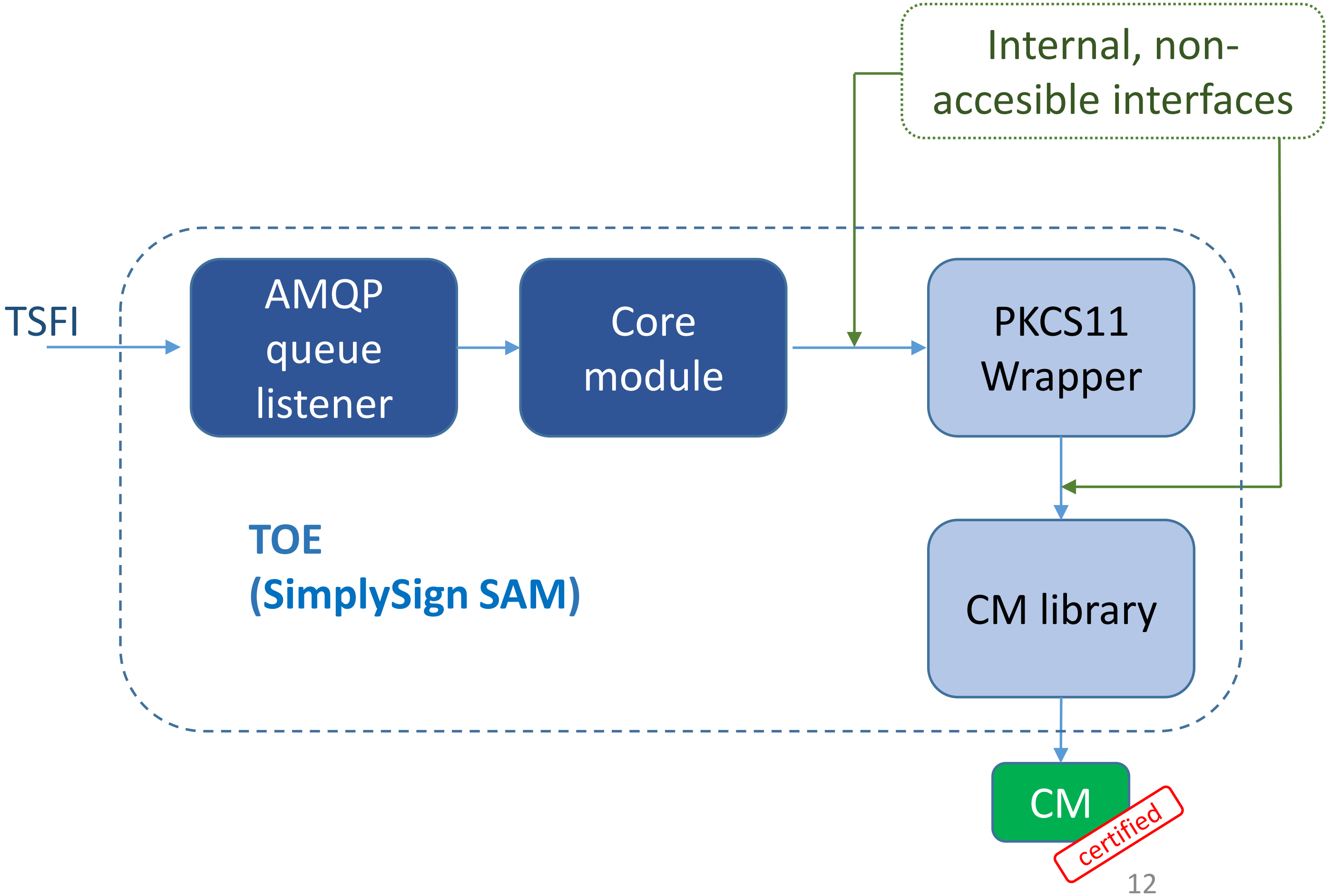
c) Preparation of „fake” SSA – cooking the RabbitMQ Producer

d) Fuzzing of TSFI parameters



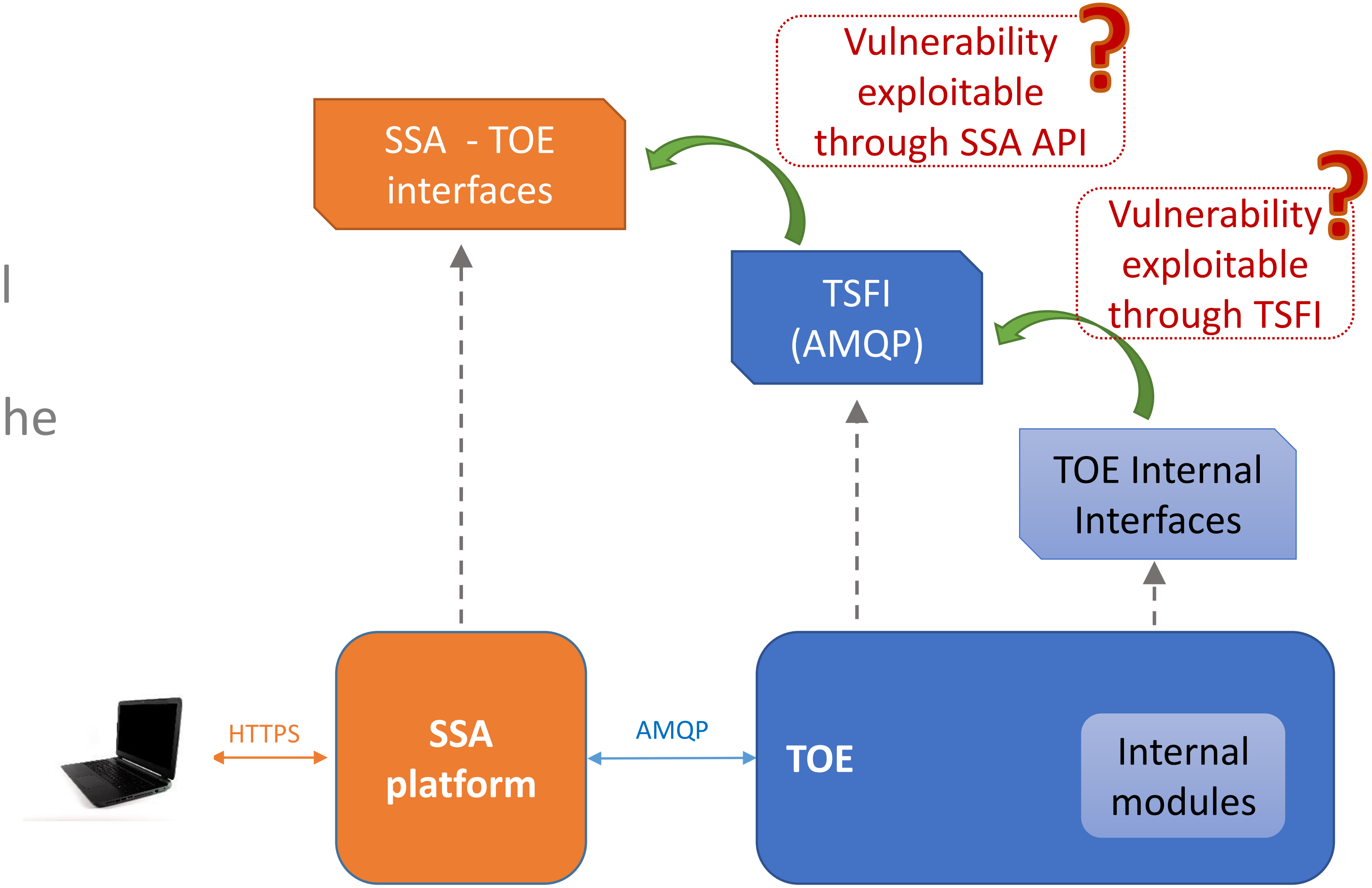
Step (1a): Internal modules analysis

- Vulnerability analysis of internal modules (*PKCS11 Wrapper* and *CM library*)
  - Dynamic analysis (fuzzing)
  - Static analysis
  - Manual analysis



Step (2): pentests in TOE operational environment

- Cascade attack vector
  a) Internal TOE interface
  b) TSFI (AMQP) – external TOE interface
  c) External interfaces of the SSA platform



Actual calculation of attack potential

Common Criteria

Attack potential factor (based on the CSPN Table*)	Value	Score	Remarks
Time taken for the (identification and) exploitation	>1 month	7	Two different types of software to be investigated and in-depth fuzzing required
Attacker expertise	Multiple experts	8	Complex software to be developed
Knowledge required by the attacker	Critical	11	Source code reviewed
Access to the product by the attacker	Easy	1	Access to the SSA as the user
Type of equipment required	Specialized software	2	See the category 'Attacker Expertise'
TOTAL		**29**	**>25 i.e. Very High**

** CRITERIA FOR EVALUATION IN VIEW OF A FIRST LEVEL SECURITY CERTIFICATION, section 5.6, ANSSI-CSPN-CER-P-02_v4.0*

Examplary reference to CVSS/Exploitability

CWE-787 Out-of-bounds Write
CVSS:3.1/AV:N/AC:H/PR:L/UI:N - > Attacker capabilities: high

Benefits for the Developer

- 3rd party independant comprehensive review of the TOE code
- Golden rule: „Do not trust anybody – even yourself”
    - It was demonstrated that there are no vulnerabilities that could be exploitable
    - In fact, the SSA platform appeared to be efficient in blocking any attack performed via https platform
    - However, the developer has decided to fix identified „internal” vulnerabilities so the TOE security is less dependant on the operating environment

Conclusions

- Absence of CC-related reference documents supporting the calculations of attack potential (similar to JIL documents for technical domains) does not make the evaluators’ life easier
  - Other scoring systems, like CVSS, cannot be directly adopted although thay can be used to support basic calculations
- It was unique opportunity for the ITSEF to demonstrate its capabilities in performing attacks with potential level even beyond high
- The evaluation activity resulted in verdict PASS (i.e., the product is resistant to attacks with the attack potential ‚high’)

Thanks for your attention
Dziękujemy za uwagę

Elżbieta Andrukiewicz
Piotr Krawiec
Ałła Stoliarowa-Myć