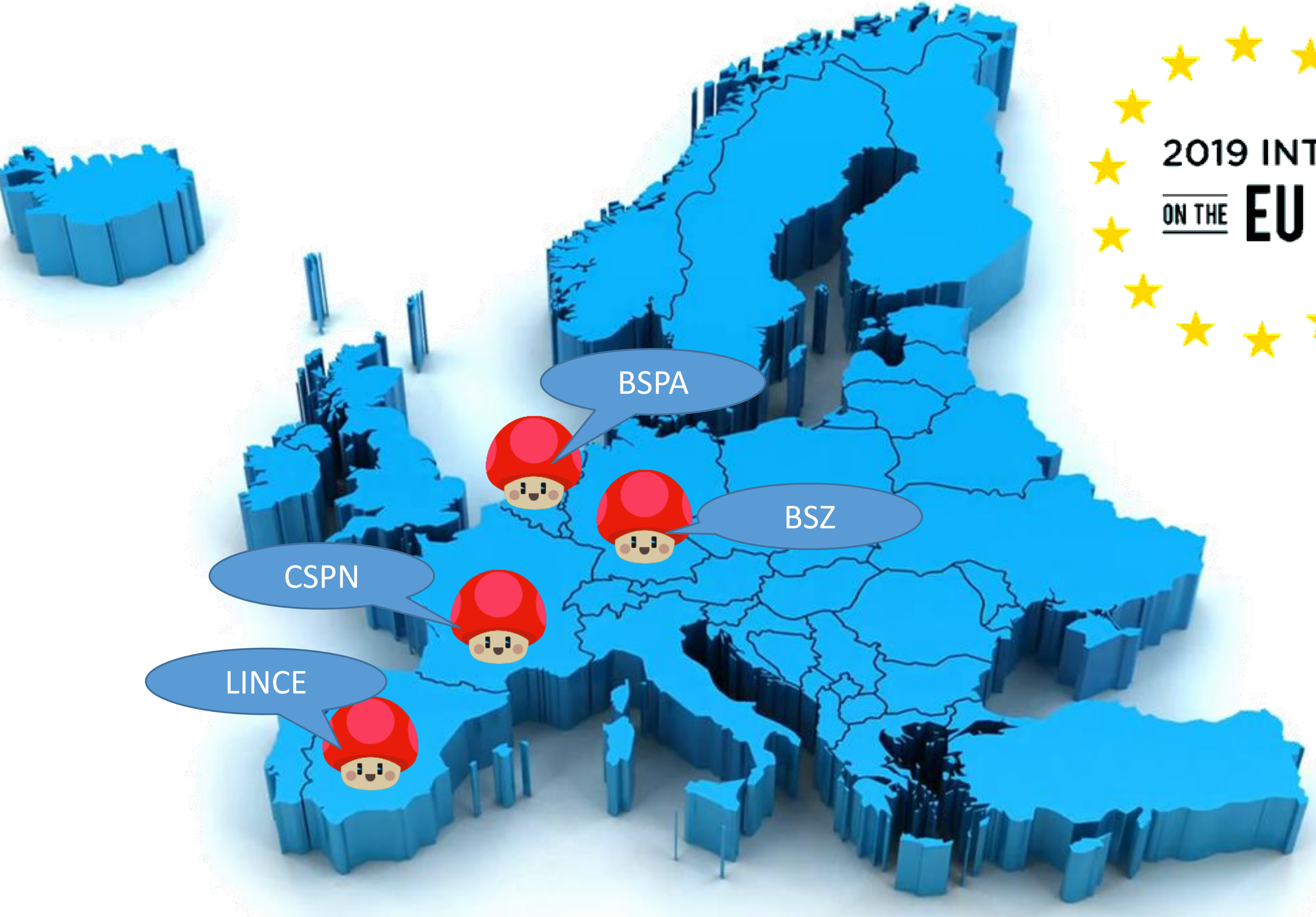
jtsec.

BEYOND IT SECURITY

2019 INTERNATIONAL CONFERENCE ON THE EU CYBERSECURITY ACT



Comparing National Lightweight Methodologies around Europe

About me

- **Javier Tallón - Technical Director**
- More than 12 years working in cybersecurity certification
- Full-stack ~~hacker~~ wannabe
- Common Criteria Expert
- Also PCI-PTS, FIPS 140-2, ISO 27K1, SOC2…
- Cyber Security Teacher at UGR (University of Granada)
- CISSP Certified
- Member of ENISA Ad-hoc Working Group on SOG-IS successor scheme.

- **jtsec Beyond IT Security**
- Services
  - Lightweight ITSEF (LINCE)
  - Certification Consultancy
  - Ethical hacking
- Created in July’17 ~ 12 Employees
- Based in Spain (Granada and Madrid)

Index

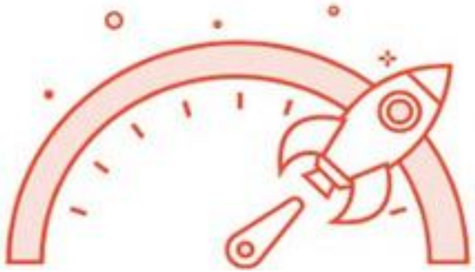
- Do we really need lightweight certifications?
- Different initiatives around Europe
  - CSPN
  - LINCE
  - BSPA
  - BSZ
- An aseptic comparison ☺
- Looking for a common methodology

Do we really need lightweight certifications?

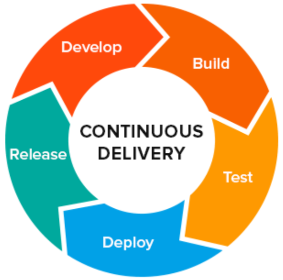
- **Benefits**
  - Powerful! – Testing, Life Cycle, Product documentation, etc…
  - Versatile - Applicable to all types of products
  - Flexible - Different assurance levels (EALs)
  - Internationally recognized certificates
- **Drawbacks**
  - Lengthy duration in time.
  - High cost of the certification process.
  - Technical difficulty in complying with/understanding the standard.
  - Excessive strictness.
  - A lot of paperwork, not everything clearly improves security.
  - Created by large companies, less accessible to SMEs.

Do we really need lightweight certifications?

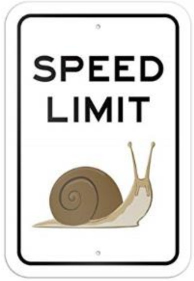
- **PRODUCT TIME TO MARKET!**



- Continuous delivery is a reality
  - Product changes almost everyday



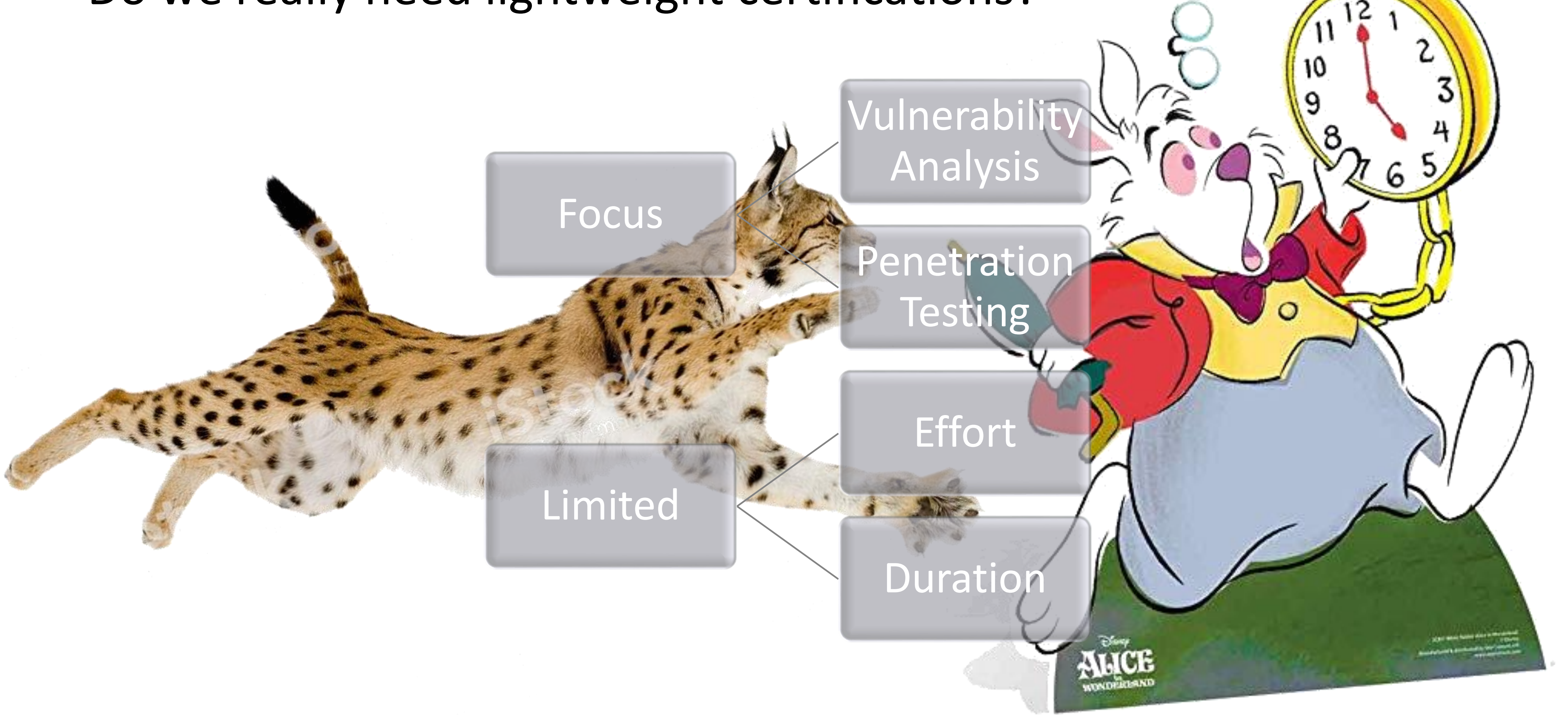
- But certification is painfully slow



- We need to **adapt**!

Do we really need lightweight certifications?

Do we really need lightweight certifications?



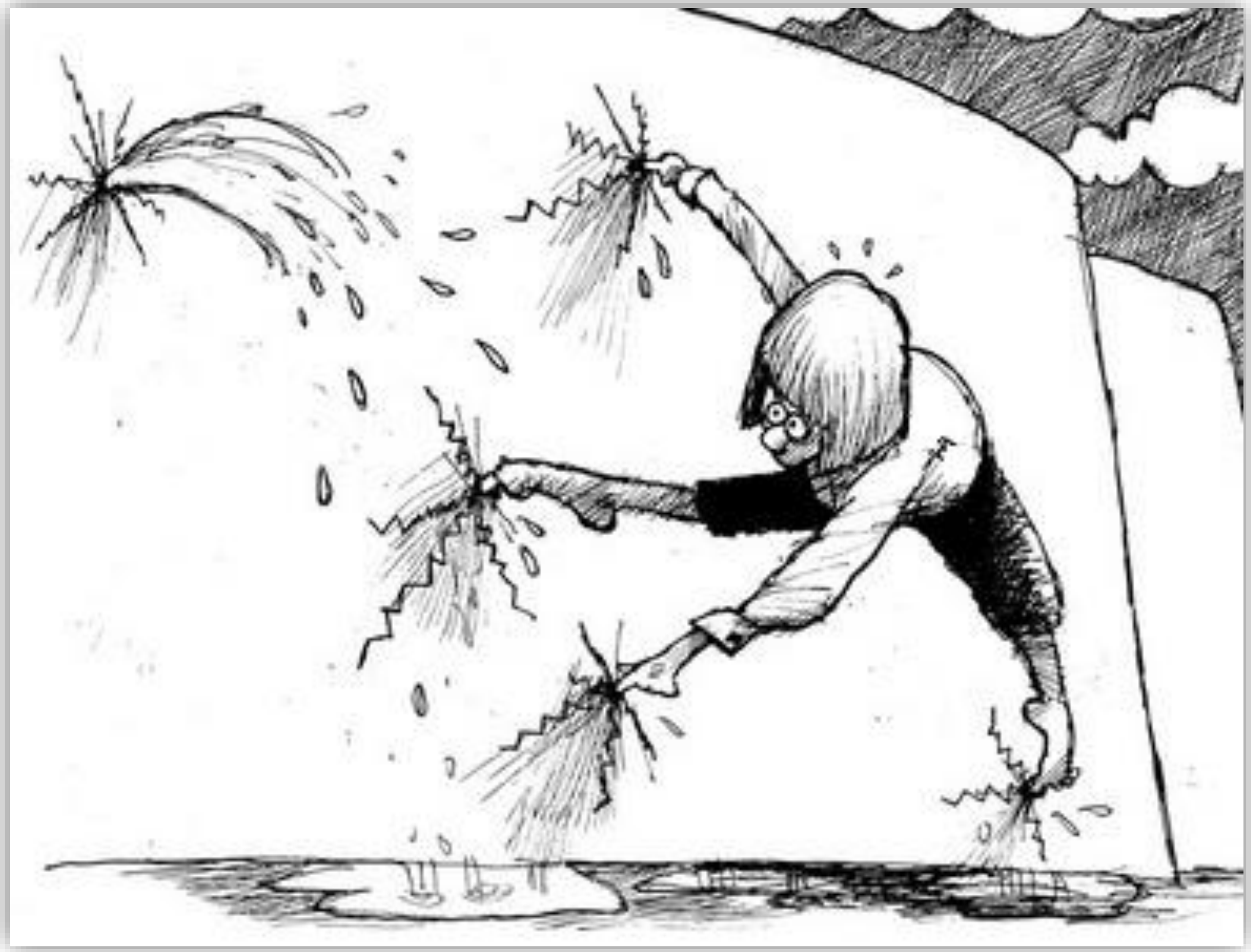
Focus

- Vulnerability Analysis
- Penetration Testing

Limited

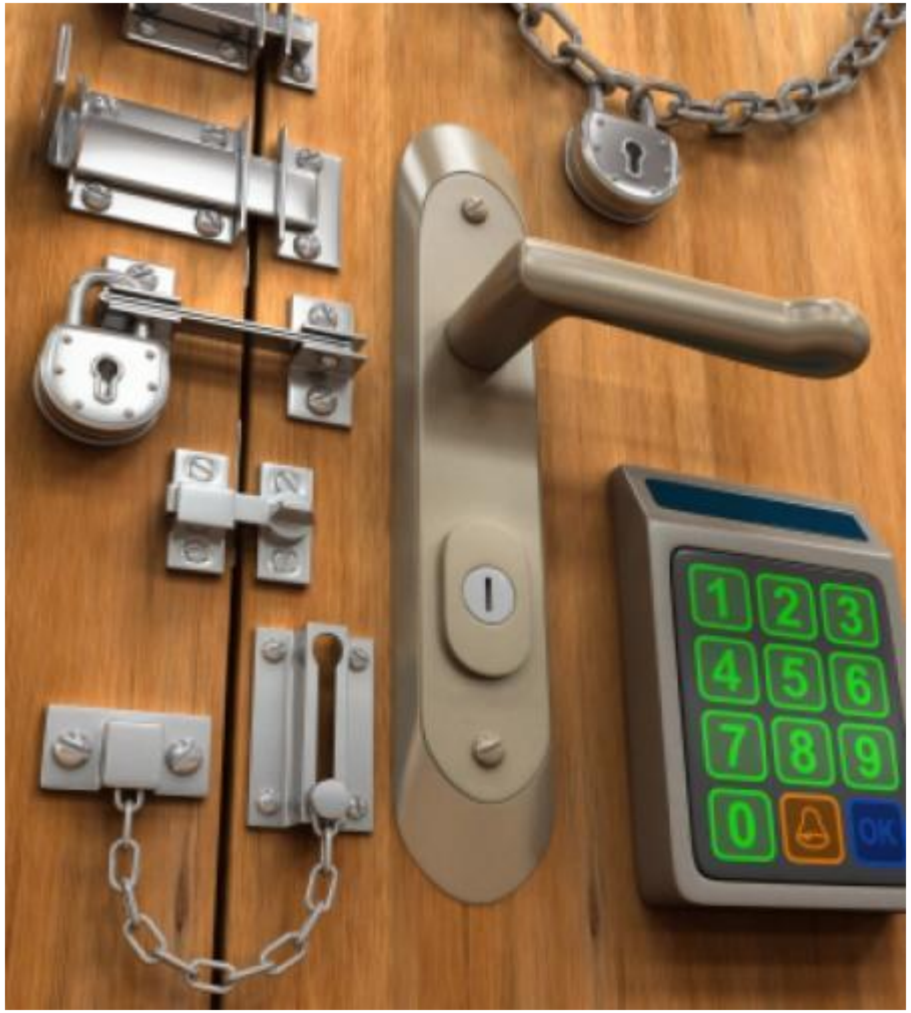
- Effort
- Duration

Do we really need lightweight certifications?



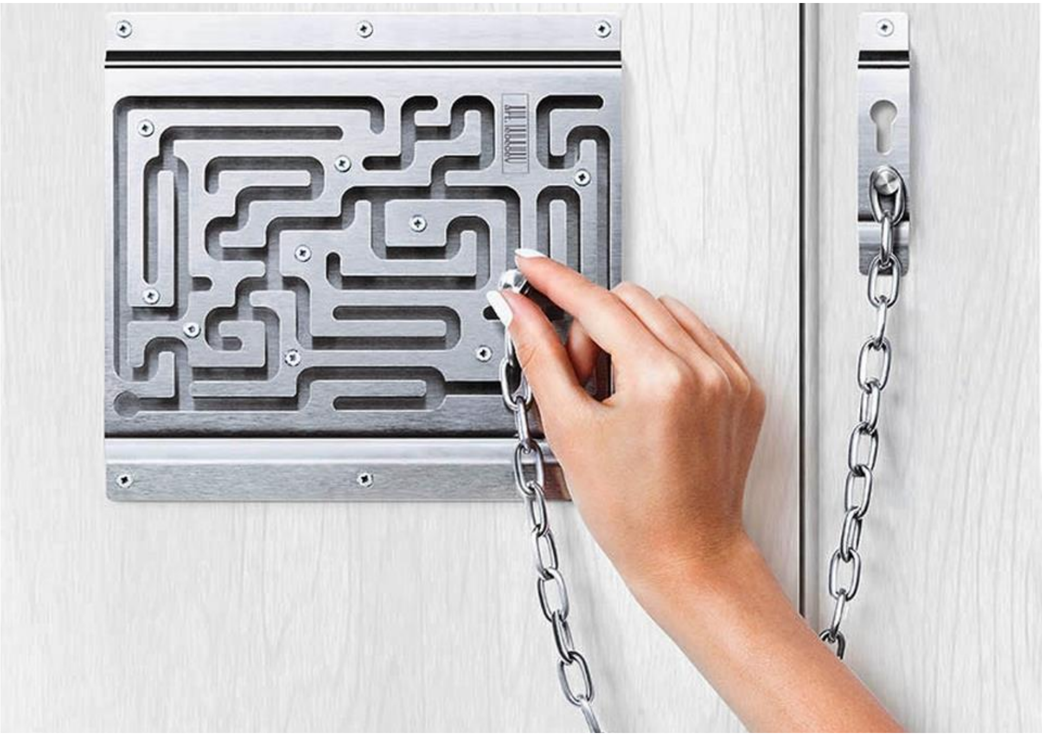
- **Not the panacea**
- Limited assurance
- Need experienced evaluators
- Need technical knowledge

Do we really need lightweight certifications?



Do we really need lightweight certifications?

Lightweight Cybersecurity Evaluation



Low Assurance Common Criteria

Do we really need lightweight certifications?

- ❑ Two trends to solve the problem
  - ❑ **North American view**:

    "Let's create cPPs providing methodology to use CC as a compliance tool and try to be as repeatable and automatic as posible".

- ❑ This will however low the assurance because there is no penetration testing and no vulnerability análisis.
  - ❑ But may be aplicable for big vendors with no evident vulnerabilities

Do we really need lightweight certifications?

- ❑ Two trends to solve the problem

  - ❑ **European view**:

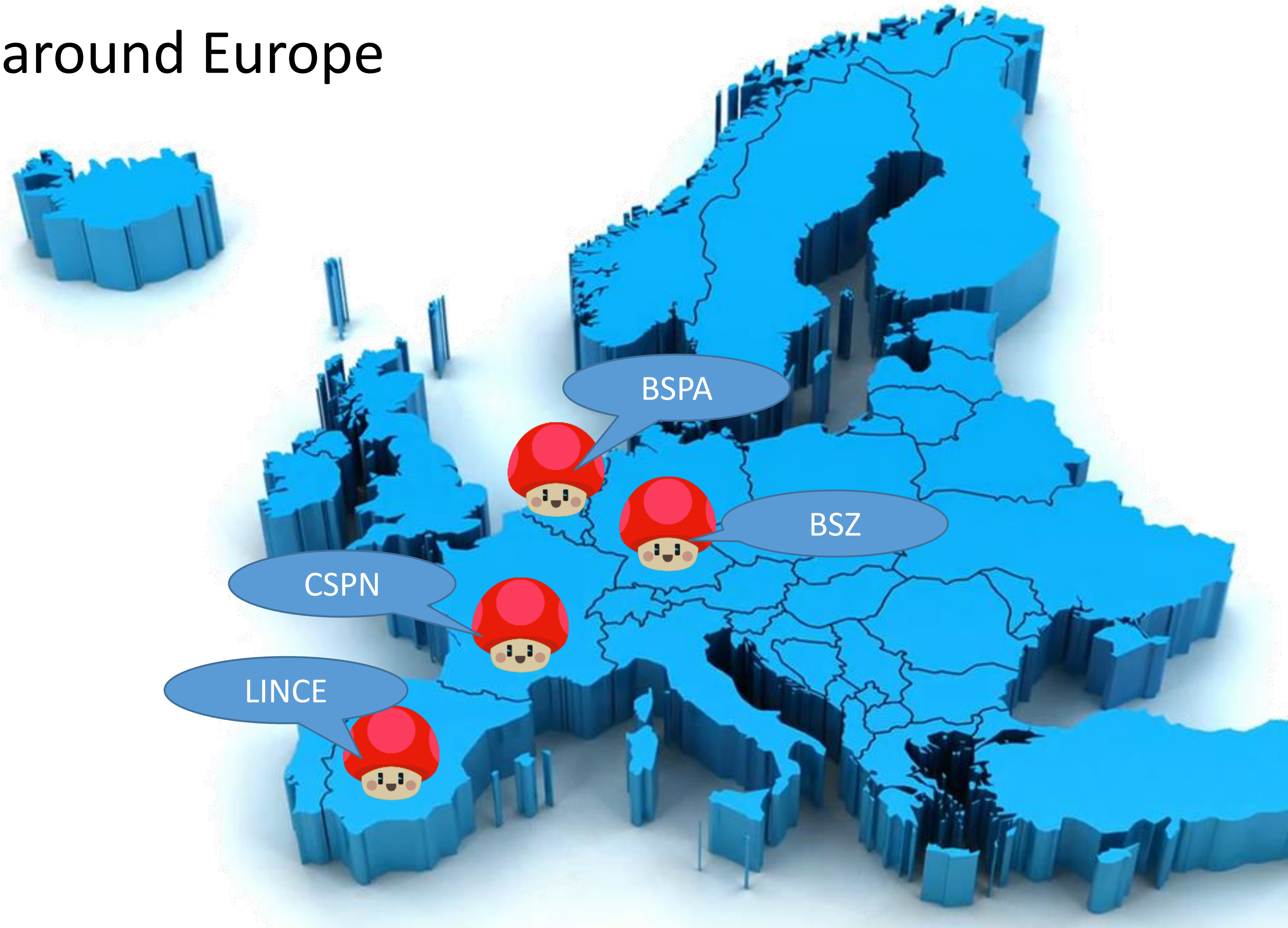
  “Let’s differentiate High and Low assurance scenarios!”.

- ❑ **‘High’ Assurance:** Let’s keep traditional use of CC while developing the standard to be able to reuse as much work as possible and maintain the warranty despite software changes.

- ❑ **‘Low’ Assurance:** Let’s create agile product evaluation and certification standards **focused on vulnerability analysis and penetration tests** and with limited effort and duration.

Different initiatives around Europe

- **Started with CSPN (2008)**
- Clear trend during last years
- Also
  - CPA (UK)
  - TSA (Malaysia)
  - AISEP (Australia)

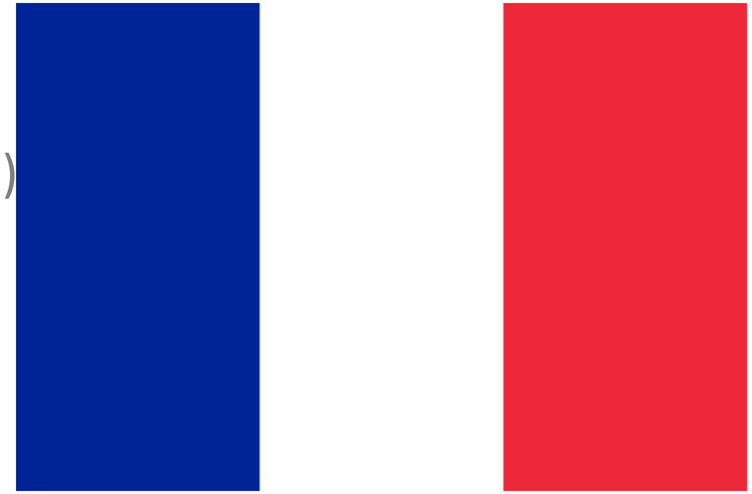


Different initiatives around Europe - Disclaimer

- The information contained in this presentation has used public sources.
- There could be some errors.
- Do not hesitate to comment it in order to solve them.

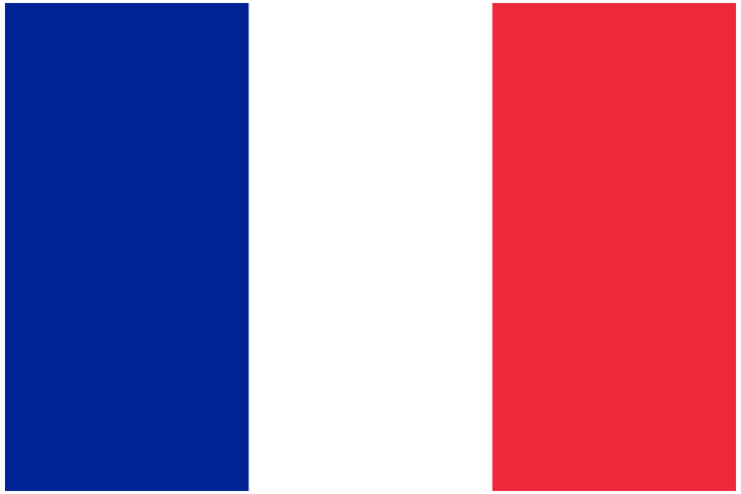
Different initiatives around Europe - CSPN

- Certification de Sécurité de Premier Niveau (First Level Security Certification)
- Launched **eleven** years ago
- Used to guide **acquisitions** by the public administration
- ANSSI issues around 100 certificates a year: 90% CC and 10% CSPN.
- As of 2019/11/14, 345 products had been evaluated. 149 certified. (43%)
- 10 licensed labs (50% only for CSPN)
  - Pilot evaluation required (CC labs dispensed)
  - 17025 not required
  - 12 technical domains for labs/products



Different initiatives around Europe - CSPN

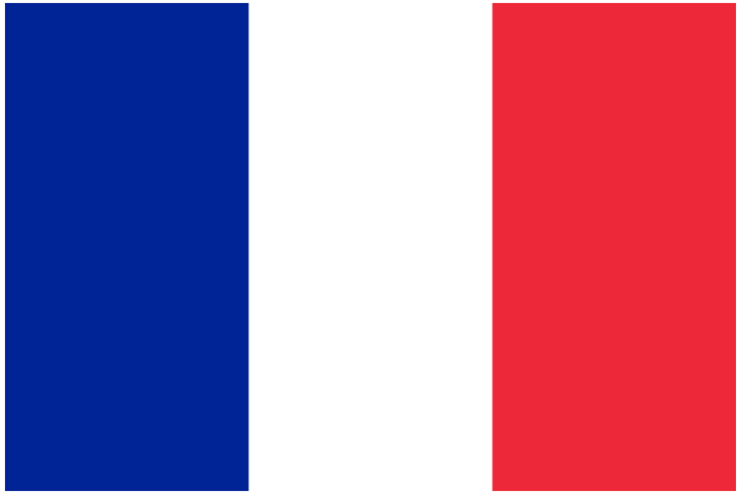
- 11 Phases
  - 1 Security Target Analysis
  - 2 Product Installation
  - 3 Conformity Analysis – Documentation Analysis
  - 4 Conformity Analysis – Source Code Review (If Available)
  - 5 Conformity Analysis – Product Testing
  - 6 Resistance Of The Mechanisms/Functions
  - 7 Vulnerability Analysis (Intrinsic, Construction, Exploitation, Etc.)
  - 7A Host System Vulnerability Analysis
  - ! 8 Ease Of Use Analysis
  - 9 Meetings With The Developers (Optional)
  - 10 Cryptography Evaluation (If the product implements cryptographic mechanisms)



Different initiatives around Europe - CSPN

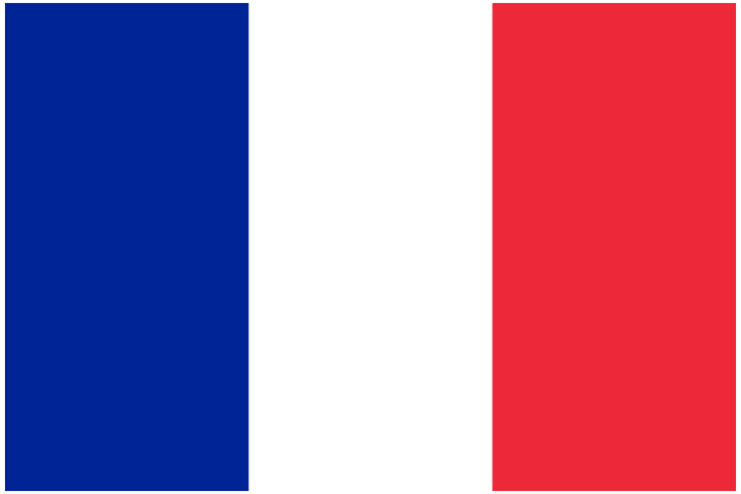
- Evaluation inputs
  - Security Target
  - TOE
  - Test equipment if it is specific or dedicated
  - Secure user guidance
  - Source code (if available?)
  - If crypto
    - Mechanisms description
    - Crypto output || (crypto source)

- Evaluation outputs
  - ETR
  - Secure use recommendations (if needed)



Different initiatives around Europe - CSPN

- Specific **methodology** for some kinds of products
  - Set Top Boxes
  - Industrial PLCs
  - Others (not public)
- **How do they speed up?**
  - ETR & ST templates
  - Limited workload (25 man/days + 10 if crypto)
    - Customizable when another specific workload is recommended or agreed between the parties
  - Limited duration (8 weeks normally)
  - If product only partially meets its security target but realistic environmental counter-measures can be identified, the product will be considered as meeting its security target



Different initiatives around Europe - BSPA

- Baseline Security Product Assessment
- Still in **pilot** stage
  - No public numbers available
- Managed by the Netherlands National Communications Security Agency (NLNCSA), a cyber defense unit of the Dutch Intelligence and Security Service (AIVD).
- 3 Licensed labs (33% only BSPA)
  - Pilot evaluation required
  - 17025 not required
  - 8 technical domains for labs/products

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Different initiatives around Europe - BSPA

- Steps
  - Conformance analysis
  - Strength analysis
  - Impact assessment on the security of the host system
  - Evaluation Technical Report (ETR)
  - Deployment Advisory (DA) that advises users on how to configure and use the product in order to meet the requirements of the Dutch Government Security Baseline (BIR) using do’s and don’ts
    - The DA includes also, the scope and limits of evaluation, residual risks and a statement of conformity of the product to the security target.

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Different initiatives around Europe - BSPA

- Evaluation inputs
  - Security Target
  - TOE
  - Secure user guidance
  - Public information (e.g. source code if opensource)
  - Test equipment if it is specific or dedicated
  - Vulnerabilities known by the Sponsor
- Evaluation outputs
  - ETR
  - Deployment Advisory (DA)

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Different initiatives around Europe - BSPA

- **How do they speed up?**
  - Limited workload (25 man/days)
    - Customizable under “special circumstances”
  - Limited duration (8 weeks normally)
  - ST & ETR templates
  - Statement of conformity & DA templates

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Different initiatives around Europe - BSZ

- Beschleunigte Sicherheitszertifizierung (BSZ, Accelerated Security Certification)
- Still in **pilot** stage
  - No public numbers available
- Managed by the BSI
  - Actively seeking **mutual recognition** with ANSSI CSPN
- Unknown number of licensed labs
  - Pilot evaluation required
  - 17025 required
  - No technical domains for labs/products (under preparation)
    - **List of requirements** to be fulfilled by every TOE

Federal Office
for Information Security

Different initiatives around Europe - BSZ

Federal Office
for Information Security

- 4 Phases
  - Phase 1 – Preparation for a BSZ (CB not involved)
    - Step 1 – Review the TOE, the cryptography and the ST
    - Step 2 – Estimate the evaluation
  - Phase 2 – The Kick-Off
    - Step 1 Preparation
  - Phase 3 – The Evaluation
    - Step 1 – Evaluate the Secure User Guide
    - Step 2 – Evaluate the Conformity
    - Step 3 – Evaluate the Resistance (VA / Pentesting)
    - Step 4 – Cryptographic Evaluation
    - Step 5 – Prepare ETR
  - Phase 4 – Final Interview

Different initiatives around Europe - BSZ

- Evaluation inputs
  - Security Target + overview of the principle design + list of libraries used
  - TOE (3 samples) + unencrypted firmware (if applicable)
  - Secure User Guide
  - Technical description of the update mechanism
  - If crypto
    - Cryptographic specification
      - Random source description
      - Key management description
    - Crypto implementation representation

- Evaluation outputs
  - ETR
  - If needed, additional steps to reach a secure configuration.

Federal Office
for Information Security

Different initiatives around Europe - BSZ

Federal Office
for Information Security

- **How do they speed up?**
  - Limited workload (15-50 man/days without ST preparation)
    - Customizable using specific methodology
      - +10 md if crypto
    - Recertification from 10 man/days
  - Fixed schedule (instead of limited duration)
  - No intermediate results (only one version of the TOE)
  - No *formal* vulnerability analysis, just penetration testing (usually you are not required to calculate attack potential). If something found vulnerable DO NOT attempt to exploit.
  - Risk based sampling
  - Specifically required competencies for evaluators

- No templates, but outlined in the methodology

Different initiatives around Europe - LINCE

- National Essential Security Evaluation
- Managed by the CCN
- Version 0.1 published and **officially launched** (Feb’19)
- Used to guide **acquisitions** by the public administration
- 17 files open / 1 product certified (2019/11/14)
- 3 licensed labs (4 more in process) (12,5% only LINCE)
  - Pilot evaluation required
  - 17025 required
  - No technical domains for labs but 36 **product families** with list of requirements for each one**. ST must be approved by a procurement department**

Different initiatives around Europe - LINCE

- 6 Stages
    - 1 Security Target Assessment
    - 2 TOE Preparation And Configuration
    - 3 Conformity Assessment – Documentation Analysis
    - 4 Conformity Assessment – Functional Tests
    - 5 Vulnerability Analysis
        - 5.1 Security Mechanisms/Functions Resistance Assessment
        - 5.2 Source Code Revision (Optional Module)
    - 5.3 Cryptographic Evaluation (Optional Module)
        - 5.3.1 Cryptographic Verification Using Functional Tests
    - 6 TOE Penetration Testing

Different initiatives around Europe - LINCE

- Evaluation inputs
  - Security Target
  - TOE
  - Secure User Guidance
  - Test environment
  - If source code module
    - Implementation representation under scope
  - If crypto module
    - Cryptographic specification
    - Open sample to test the algorithms
- Evaluation outputs
  - ETR & ORs

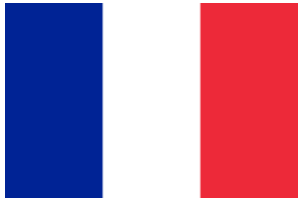
Certificación Nacional Esencial de Seguridad
CCN

Different initiatives around Europe - LINCE

- **How do they speed up?**
  - ST & ETR templates
  - Limited workload (25 man/days + 5 man/days per module)
  - Limited duration (fixed to 8 weeks + 2 weeks per module)
  - Only one ETR (changes to the evidence allowed if it does not affect the workload)

An aseptic comparison – Security Target

LINCE ST	**CSPN ST**	**BSPA ST**	**BSZ ST**
TOE Identification	TOE Identification	TOE Identification	TOE Identification
TOE Usage	TOE Usage	TOE Usage	TOE Usage
TOE Description	TOE Description	TOE Description	TOE Description
Operational Environment	Operational Environment	Operational Environment	Operational Environment
Assumptions	Assumptions		Assumptions
Assets	Assets	Assets	Assets
			Attackers
Threats	Threats	Threats	Threats
Security Functions	Security Functions	Security Functions	Security Functions
	Limits of evaluation (CR)	Limits of evaluation (DA)	Limits of evaluation (ST)



	LINCE	CSPN	BSPA	BSZ
ST Review	Yes	Yes	Yes	Yes
Guidance Review	Yes	Yes	Yes (implicitly)	Yes
Product Installation	Yes	Yes	Yes	Yes
Time / Duration	25d/8w + modules	25d/8w +10d if crypto.	25d/8w	15d-50d/agreed schedule
Customizable time/duration	With modules	If agreed	Special circumstances	Always. Rules provided
Source Code review	Optional Module ❗	For quality & crypto	No	For crypto
Security Functionality testing	Yes	Yes	Yes	Yes
Analysis of the resistance of the mechanisms/functions	No	Yes	Yes	Implicitly done
Vulnerability Analysis	Yes	Yes	Yes	As part of Resistance Phase but without formalism ❗
Penetration Testing	Yes	As part of VA	As part of Strength Analysis	As part of Resistance Phase but explicitly without exploiting
Ease of use Analysis	No	Yes ❗	No	No
Impact assessment on the security of the host	No	Yes	Yes	No
Crypto Evaluation	Optional Module (Conformance testing)	Mandatory if implemented (Conformance and VA, PT only if needed)	???	Mandatory if implemented (VA & PT) (Under discussion)
Interview Phase with CB	On CB demand	Yes	???	Yes
Intermediate Results	Yes (time constrains) ❗	No	???	No, only one TOE

Looking for a common methodology

- Lightweight certification are already working in practice!
  - Countries are gaining **experience**
  - Mainly used by national **administration**, but applicable to consumer market.
  - Mutual **recognition** shall be possible!

- Manufacturers are being forced to certify their products under the schemes of each country
  - Increase in cost
  - Inconvenience to competitiveness
  - Betrayal of the principles of the European Union

Looking for a common methodology

- Evaluation methodologies **are very similar** with slight differences
  - Thanks to CSPN being the first and an inspiration for the others
    - It should be affordable to create a common methodology!!!
  - Mutual recognition of already certified products shall be considered

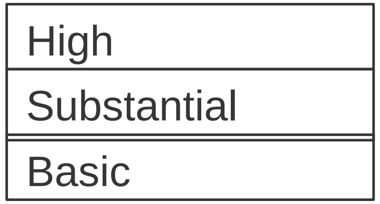
- Evaluation procedures are a bit more different and more difficult to harmonize between the different schemes

- **JTC13 WG3** is already working towards this direction
  - European Project under CEN-CENELEC to create a common methodology: *Cybersecurity Evaluation Methodology for ICT Products*
  - **No direct match** between lightweights and EUCA assurance levels

Looking for a common methodology

- EUCA mentions specifically the following **evaluation activities** for each assurance level:
  - Basic:
    - Technical documentation review
  - Substantial:
    - Security Functional Testing
    - Check against known vulnerabilities
  - High:
    - Pentesting

European Commission



EU Cybersecurity Act Assurance Levels

- Current **goals**
  - Re-use as much as possible the current content of these methodologies and make sure that the different options are taken into account.
  - Create a methodology that is straight forward for new schemes under CSA
  - Harmonize existent national methodologies from the technical point of view

Contact Data

jtsec BEYOND IT SECURITY

jtsec: Beyond IT Security

Granada & Madrid – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es