Bundesamt
für Sicherheit in der
Informationstechnik

Fixed-Time Cybersecurity Evaluation Methodology for ICT Products and the European Cyber Security Act

Developments at CEN/CENELC JTC13 WG3

A few words about myself

1. I'm working at the German BSI ("Federal Office for Information Security") since 2005
2. My focus of work is certification (non-operational), recognition/accreditation
    1. for products
    2. for ISMS
3. I'm involved in several standardization bodies, e.g. DIN, CEN/CENELC, ISO/IEC
4. I participated in several pre-drafts of CSA schemes, also (auxiliary) involved in the EuCC scheme
5. I'm Editor (amongst others) of EN 17640

Bundesamt für Sicherheit in der Informationstechnik

Overview of the presentation

1. European landscape
2. Design principles of the standard
3. Development history and track of the standard
4. Structure and examples from the standard
5. Excursus: the Cyber Security Act (CSA)
6. How to use the standard in a CSA scheme (development)
7. Open topics / next steps
8. Summary

The fixed-time cybersecurity certification landscape in Europe

CSPN – Certification de Sécurité de Premier Niveau

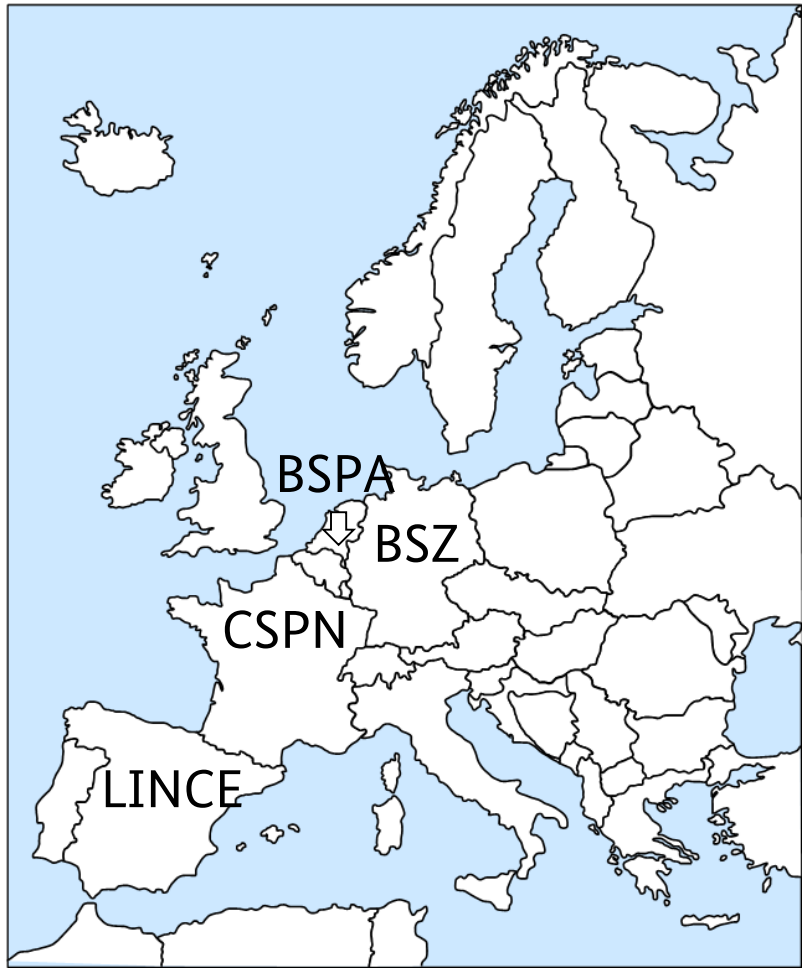
BSPA – Baseline Security Product Assessment

LINCE – National Essential Security Evaluation

BSZ – Beschleunigte Sicherheitszertifizierung

and possibly more ...

... and then came the “Cybersecurity Act” with 3 assurance levels.
... and possible verticals using them (e.g. IACS)



Design principles of EN 17640 (extract)

- Flexible application:
  - All CSA evaluation assurance levels, including self-assessment
  - Horizontals and verticals
  - Adaptable by parameters where possible

- Bare minimum required by CSA shall be possible
- Existing methodologies (LINCE, CSPN, ...) should be reproducible

- The work load on the developer shall be reduced where possible
  - This might imply higher work load for evaluators

- Evaluator competence is important

- This is not a “lightweight” CEM (ISO/IEC 18045)

Development of the standard

- Preparatory (**experts**)
  - 2018/12 (Delft) – First ideas, call for contributions
  - 2019/07 (Paris) – New Work Item Proposal (NWIP)
  - 2019/11 (Bucharest) – Review of NWIP-Feedback, Selection of Editors
- Formal vote/decision in **Technical Board** of CEN/CENELC
- Development on **expert** level
  - 2020/01 – Development of first draft
  - 2020/03 (virtual) – First meeting to discuss technical contents
  - … several virtual meetings, both general and topic related
  - 2020/11 (virtual) – Finalizing the technical content (what‘s in/what‘s out)
  - 2021/01 – JTC13 chair recommends EN 17640 for voting
- Q3/2021 – Translation into French/German and formal **national body** vote (Enquiry Draft)
- Beginning of 2022: Expected publication

The structure of EN 17640

1 Scope
2 Conformance
3 Normative references
4 Terms and definitions
5 General concepts
6 Evaluation tasks
Annex A - Example for a structure of a Security Target
Annex B - Example for a structure of a Protection Profile
Annex C - Acceptance Criteria
Annex D - Guidance for integrating the methodology into a scheme
Annex E - Parameters of the methodology and the evaluation tasks
Annex F - Calculating the Attack Potential
Annex G - Reporting the results of an evaluation

Example Evaluation Task / Work unit(s)

6.x **Title of the Evaluation Task**
6.x.1 **Aim**
The aim of this evaluation task is ...

6.x.2 **Evaluation method**
This evaluation task is ...

6.x.3 **Evaluator qualification**
The evaluators need to have knowledge of ... need to be able to ....

6.x.4 **Evaluator work units**
6.x.4.1 **Work unit 1**
....

Evaluation tasks

- Completeness check
- Protection Profile / Security Target evaluation / Review of security functionalities
- Development documentation

- Evaluation of the TOE installation

- Conformance testing
- Vulnerability review
- Vulnerability testing
- Penetration testing

- (Basic) crypto analysis
- Extended crypto analysis

Bundesamt für Sicherheit in der Informationstechnik

Acceptance criteria

The objective of Acceptance Criteria is to help evaluators or testers to specify test cases. Acceptance criteria are an implementation-independent definition of test case "expected results" criteria.

Security Requirement Attributes	Evaluation Acceptance Criteria
...	
General Authentication	
login feedback	– sensitive data concerning the authentication process – no different feedback for wrong password or username – no timing differences for error and correct login

For I&A, Secure Boot, Cryptography, Secure State after Failure, Least Functionality, Update mechanism, ...

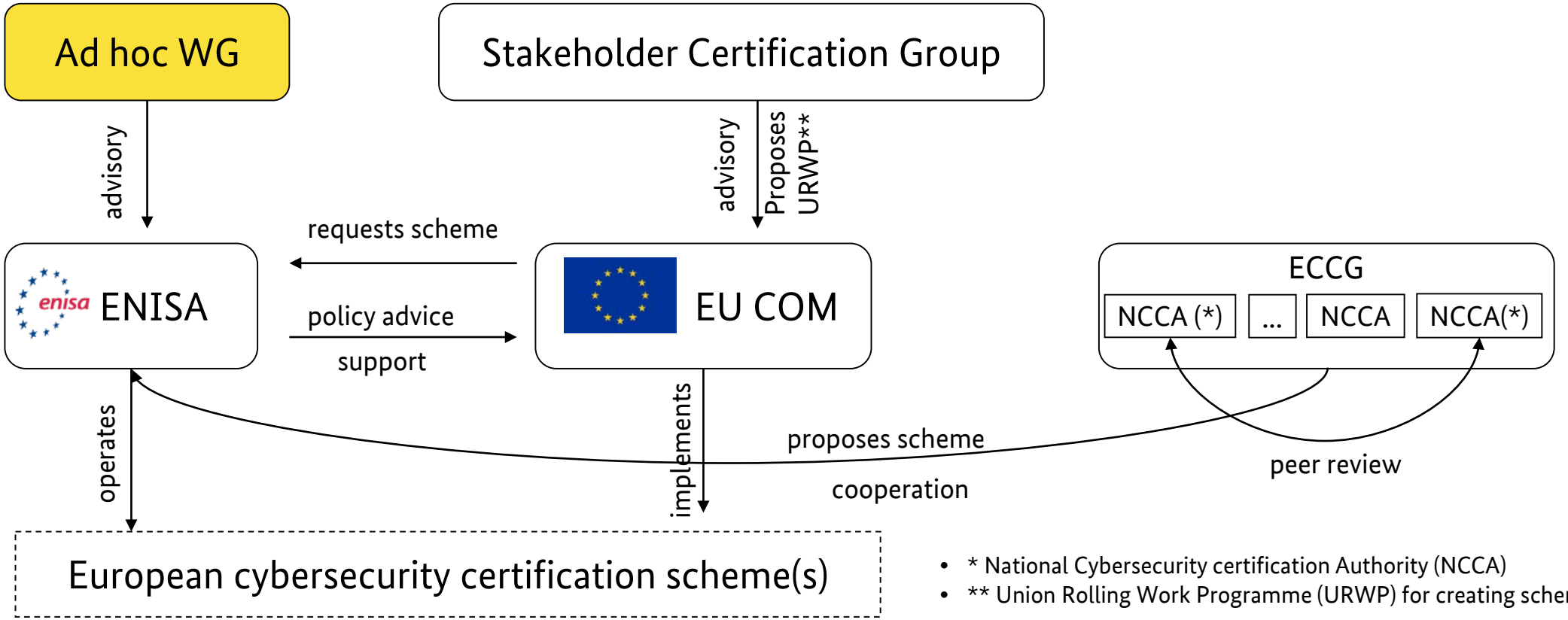
Excursus: The Cyber Security Act (2019)

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 17 April 2019
on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

- Part on ENISA establishment (not relevant in this context)
- Part on the
  - development of and
  - requirements for
- European cybersecurity certification schemes

- 3 assurance levels: basic (including statement of conformity), substantial and high

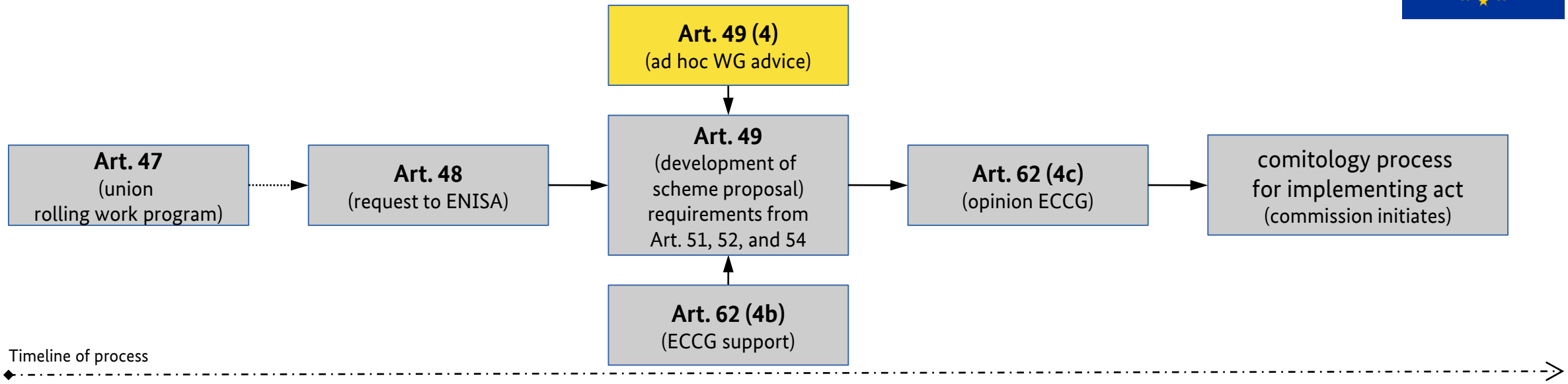
Stakeholder relations according to the CSA



- * National Cybersecurity certification Authority (NCCA)
- ** Union Rolling Work Programme (URWP) for creating schemes

Bundesamt für Sicherheit in der Informationstechnik

How is a scheme prepared?



Steps in the process “Scheme Development” according to CSA:

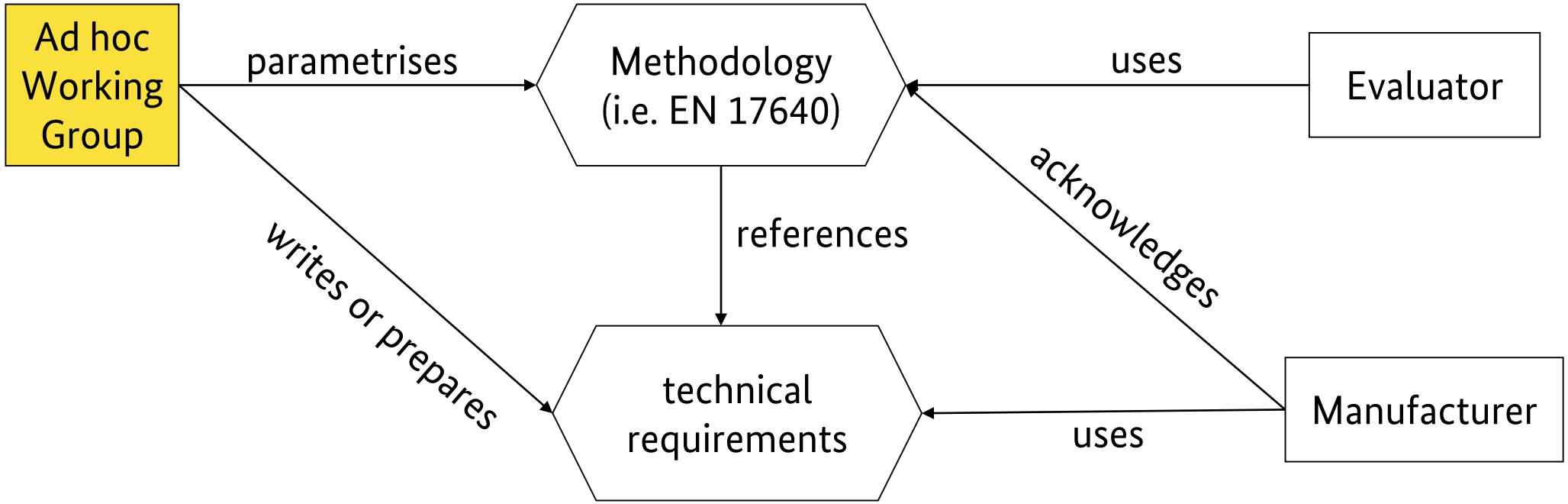
1. Art. 47: ENISA prepares and updates the rolling work program
2. Art. 48: EU COM or ECCG request ENISA to draft scheme
3. Art. 49: ENISA develops scheme proposal under advice of Ad hoc WG and with support of ECCG
4. Art. 62: ECCG gives opinion to scheme proposal, ENISA takes utmost account to ECCG opinion
5. Scheme proposal passed to EU COM for adoption by implementing act

Current scheme proposals

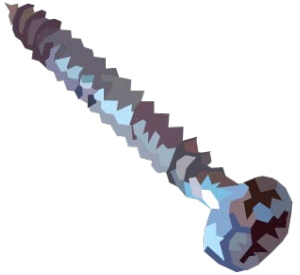
- Common Criteria – Implementing act under discussion in ECCG
  - Still work in ad hoc WG on details
  - For substantial and high
- Cloud – Ad hoc WG work
  - First draft available
  - Standardization request in progress
- 5G – Ad hoc WG call for experts issued
  - “Focus” on basic (and substantial)

- Status of URWP unclear
- Possible future candidates
  - Internet of Things (IoT)
  - Industrial Automation and Control Systems (IACS - including FIT CEM?)
  - FIT CEM?

How to use the standard



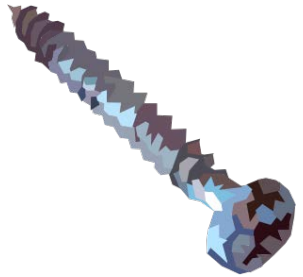
Fictitious example: Smart Screw CSA Scheme (full example in the actual standard)



List of documents and other decisions (e.g. on attack potential, evaluator competence)

CSA level	Chosen evaluation task	Parameters and notes
Basic	Completeness check	
	Review of security functionality	
	Development documentation	The checklist contains only the technical data sheet
	Evaluation of the TOE installation	

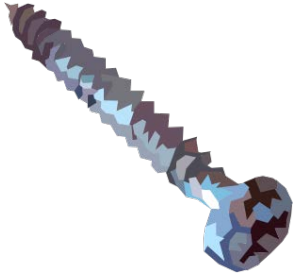
Fictitious example: Smart Screw CSA Scheme (full example in the actual standard)



List of documents and other decisions (e.g. on attack potential, evaluator competence)

CSA level	Chosen evaluation task	Parameters and notes
Substantial	Completeness check	
	Security Target Evaluation	
	Development documentation	The checklist contains only the technical data sheet
	Evaluation of the TOE installation	
	Conformance testing	The evaluators shall use sampling of *n* days per smart functionality (and additional *m* days if chirality support is included).
	Vulnerability testing	The evaluators shall use the STOP list as pre-defined source and use sampling of *x* days per smart functionality (and additional *y* days if chirality support is included).
	Basic crypto analysis	The SOG-IS crypto catalogue is mandated.

Fictitious example: Smart Screw CSA Scheme (full example in the actual standard)



List of documents and other decisions (e.g. on attack potential, evaluator competence)

CSA level	Chosen evaluation task	Parameters and notes
High	Completeness check	
	Security Target Evaluation	
	Development documentation	The checklist contains … and the architectural overview
	Evaluation of the TOE installation	
	Conformance testing	The evaluators shall completely test the conformance (full coverage) using the scheme defined Acceptance Criteria.
	Penetration testing	The evaluators shall use sampling of u days per smart functionality (and additional v days if chirality support is included). Vulnerability research beyond STOP is required.
	Extended crypto analysis	The SOG-IS crypto catalogue is mandated. The vulnerability analysis shall be performed within *z* days.

(Major) open topics

- Development process
  - Secure development as basis for secure products
  - Several approaches: „CC like“ or „62443 like“
  - How to design an effective audit process
  - What kind of evidences are sensible in product evaluations

- Composition
  - Using certified products (e.g. trust anchors) *properly*
  - How to compose assurance statements
  - Actual evaluation steps necessary to evaluate compositions
  - To compose and to be composed (“be part”)

Current and next steps

- **Enquiry vote in progress, document update and publication**
  - Visit your national standardization body for details

- Review and work on the open issues
- Consider novel issues (like patch management)
  - both possible for next revision, pending progress

- Possible usage of EN 17640 in
  - emerging schemes like “Industrial Automation and Control Systems” (IACS)
  - dedicated „fixed-time“ schemes (aka „lightweight“)

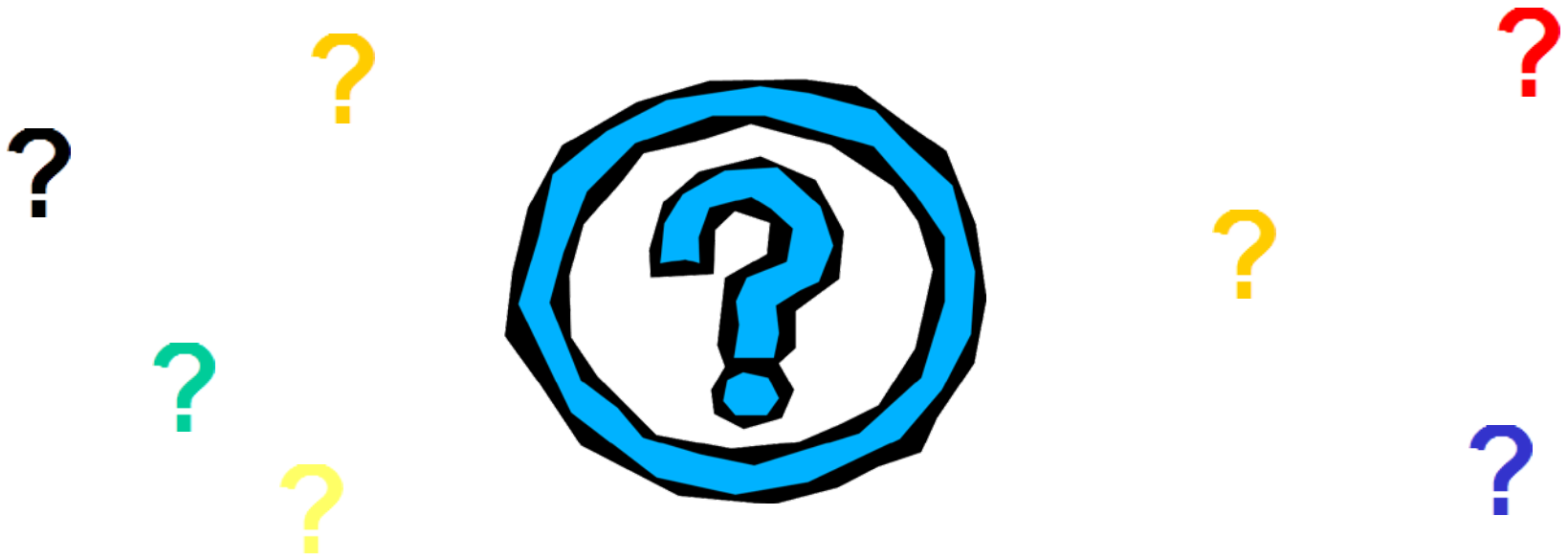
Summary

EN 17640 is

- an evaluation methodology for products
- novel, but with proven background
- highly flexible
- designed for „fixed time“ evaluations

Ideally suited for usage in future CSA schemes and similar approaches

Questions



About the speaker

Contact

Bundesamt für Sicherheit in der Informationstechnik
Referat SZ 12
Godesberger Allee 185-189
53175 Bonn

Hr. Dr. Helge Kreutzmann
helge.kreutzmann@bsi.bund.de
www.bsi.bund.de
Tel. +49 (0)228 99 9582-5244
Fax +49 (0)228 99 10 9582-5244

Bundesamt
für Sicherheit in der
Informationstechnik

	LINCE	CSPN	BSPA	BSZ
ST Review	Yes	Yes	Yes	Yes
Guidance Review	Yes	Yes	Yes (implicitly)	Yes
Product Installation	Yes	Yes	Yes	Yes
Other documentation analysis	No	Yes	No	Yes
Source Code review	Optional Module	If available	No	For crypto
Security Functionality testing	Yes	Yes	Yes	Yes
Analysis of the resistance of the mechanisms/functions	No	Yes	Yes	No
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 but no PT)	???	Mandatory if implemented (VA & PT) (Under discussion)
Interview Phase with CB	No	No	No	Yes
Intermediate Results	Yes (time constrains)	Not specified	Not specified	No, only one TOE

Source: Javier Tellon (Jtsec / Spain)