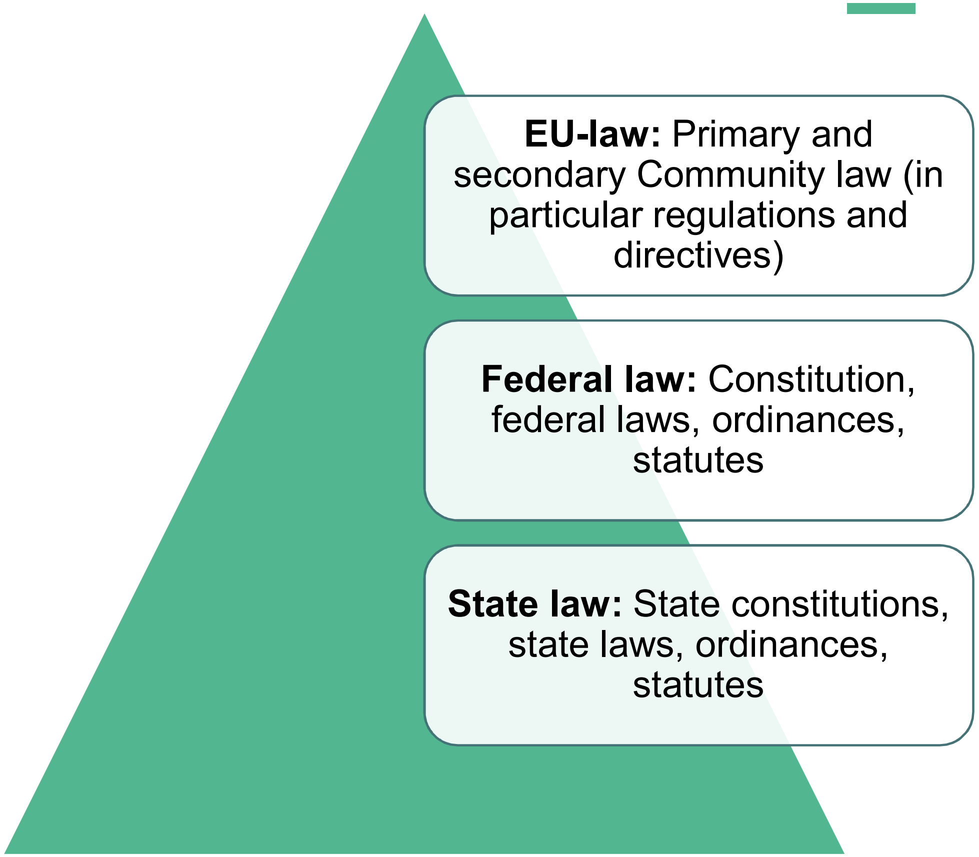
CERTAVO

Current EU and German legal framework on cybersecurity: Overall view



EU-law: Primary and secondary Community law (in particular regulations and directives)

Federal law: Constitution, federal laws, ordinances, statutes

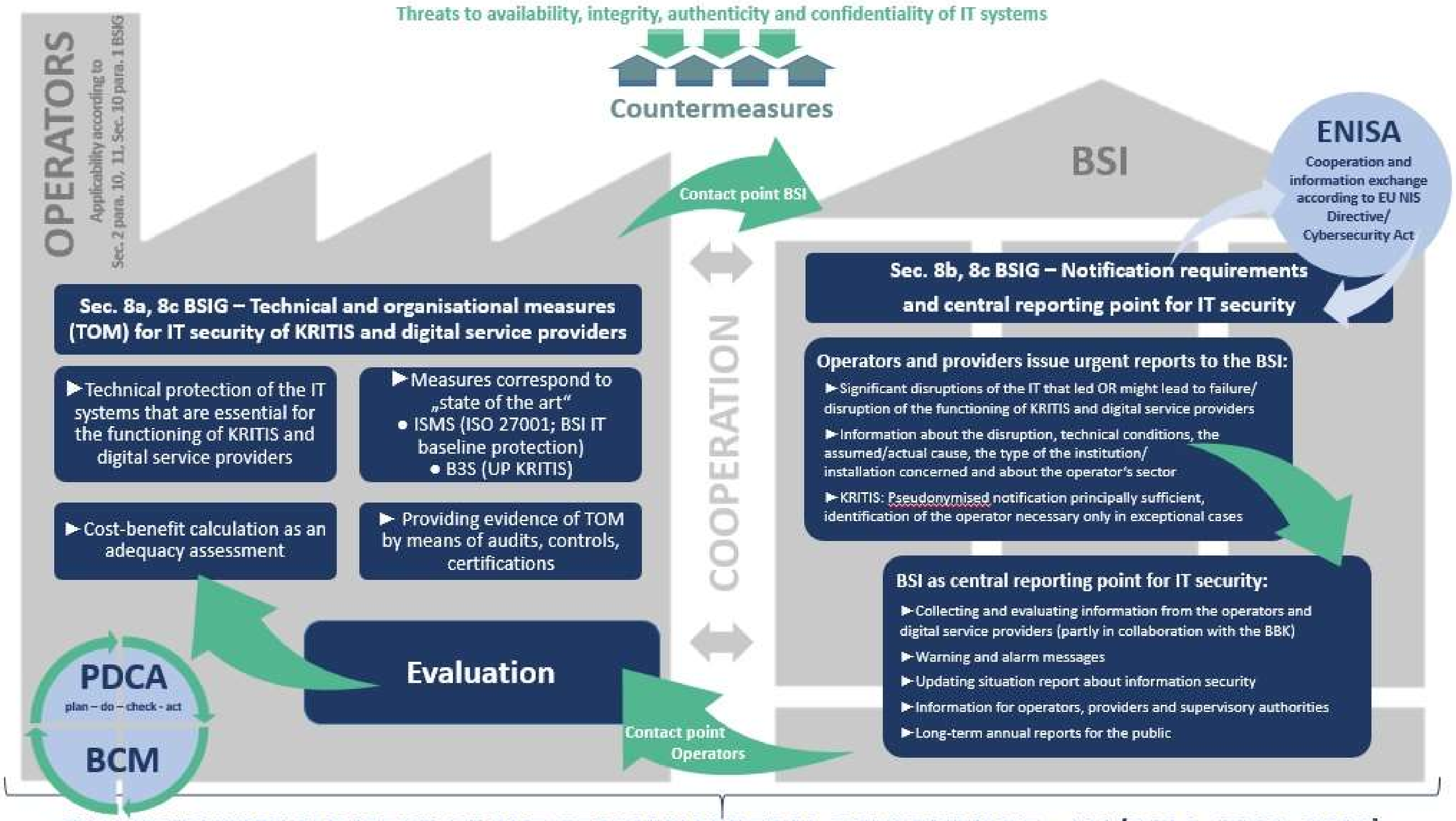
State law: State constitutions, state laws, ordinances, statutes

- **EU Network and Information Security Directive** (NIS, 2016)
- **EU General Data Protection Regulation** (GDPR, 2016, 2018, also requirements for data security inter alia according to Art. 32, as far as personal data is concerned)
- **EU CybersecurityRegulation** (Cybersecurity Act, CSA, 2019)
- **EU Regulation for a Centre of Excellence on Cybersecurity** (2018, draft)

- **IT-Security Law** (IT-SiG, 2015)
  - BSI-Kritisverordnung (BSI-KritisV, 2016, 2017)
- **IT-Security Law 2.0** (IT-SiG 2.0, 2019, draft)
- **2. Data Protection Adaptation and Implementation Act EU** (2. DSAnpUG-EU, 2019, Adaptation of the sector-specific German data protection law also with regard to IT security)

IT-Security Law (IT-SiG) and EU Network and Information Security Directive (NIS)

INFORMATION FLOWS AND PROTECTION PROCESSES IN THE IT SECURITY OF CRITICAL INFRASTRUCTURES AND DIGITAL SERVICE PROVIDERS



Threats to availability, integrity, authenticity and confidentiality of IT systems

Countermeasures

OPERATORS

Applicability according to Sec. 2 para. 10, 11, Sec. 10 para. 1 BSIG

Sec. 8a, 8c BSIG – Technical and organisational measures (TOM) for IT security of KRITIS and digital service providers

- ►Technical protection of the IT systems that are essential for the functioning of KRITIS and digital service providers
- ►Measures correspond to „state of the art"
  - ISMS (ISO 27001; BSI IT baseline protection)
  - B3S (UP KRITIS)
- ►Cost-benefit calculation as an adequacy assessment
- ► Providing evidence of TOM by means of audits, controls, certifications

Evaluation

PDCA

plan – do – check - act

BCM

Contact point BSI

COOPERATION

Contact point Operators

BSI

ENISA

Cooperation and information exchange according to EU NIS Directive/ Cybersecurity Act

Sec. 8b, 8c BSIG – Notification requirements and central reporting point for IT security

Operators and providers issue urgent reports to the BSI:

- ►Significant disruptions of the IT that led OR might lead to failure/ disruption of the functioning of KRITIS and digital service providers
- ►Information about the disruption, technical conditions, the assumed/actual cause, the type of the institution/ installation concerned and about the operator's sector
- ►KRITIS: Pseudonymised notification principally sufficient, identification of the operator necessary only in exceptional cases

BSI as central reporting point for IT security:

- ►Collecting and evaluating information from the operators and digital service providers (partly in collaboration with the BBK)
- ►Warning and alarm messages
- ►Updating situation report about information security
- ►Information for operators, providers and supervisory authorities
- ►Long-term annual reports for the public

CYBERSECURITY STRATEGY OF THE GERMAN FEDERAL GOVERNMENT + EU (2011, 2013, 2016)

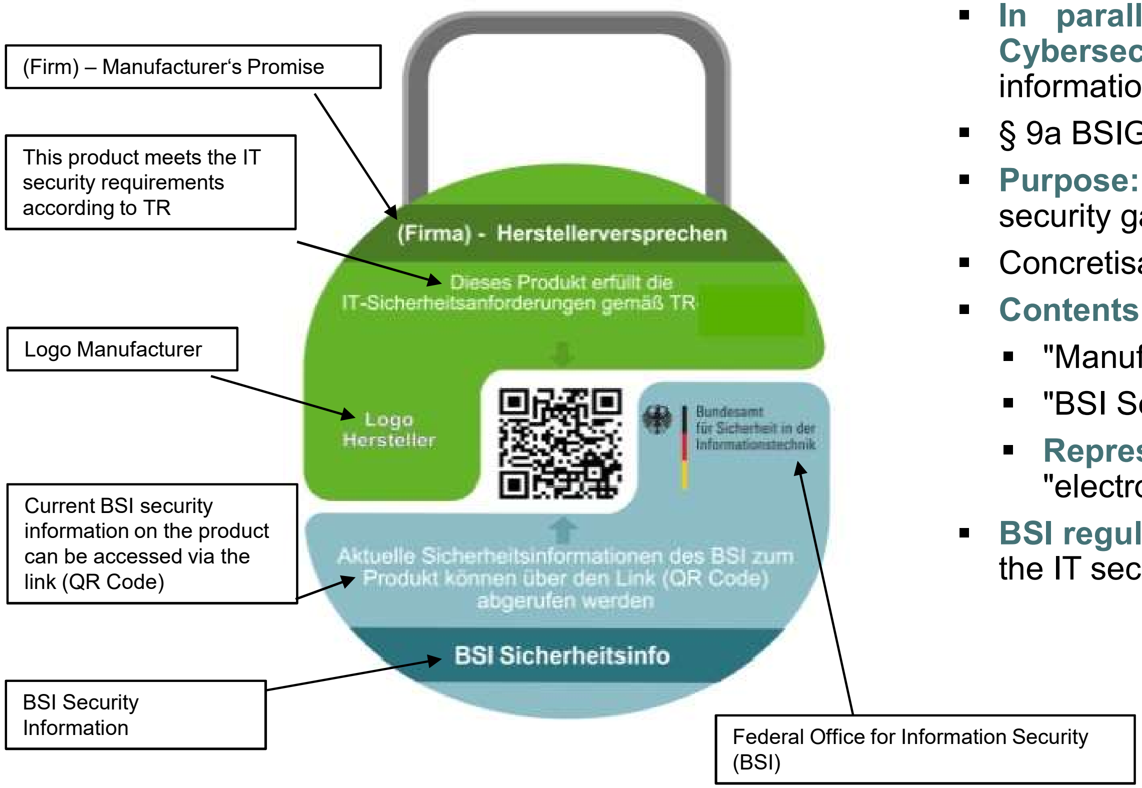
Dr. Dennis-Kenji Kipker, Bremen

IT-Security Law 2.0 (IT-SiG 2.0)

Background and changes

- **Long-awaited, much speculated:** Publication of the draft bill at the beginning of April 2019
- Lead management by **Federal Ministry of the Interior (BMI)**
- Actually: "Second law to increase the security of information technology systems"
- Content adapted to the “new” **Cyber-Security Strategy** of the Federal Government from 2016
- This means not only economic protection, but also in particular protection of citizens + public authorities
- **Key points of content:**
- More tasks and competences for the Federal Office for Information Security (BSI)
- Extended obligations for operators of critical infrastructures (KRITIS), e.g. for the detection of supply chains in KRITIS core components, extension of the circle of addressees of the regulations in the BSI Act (inter alia “cyber-criticality” and infrastructures in the “special public interest”), extension of product-related reporting obligations
  - Establishment of an "IT security mark", more in the following section...

IT-Security Mark:
More consumer protection and transparency


(Firma) - Herstellerversprechen
Dieses Produkt erfüllt die IT-Sicherheitsanforderungen gemäß TR
Logo Hersteller
Bundesamt für Sicherheit in der Informationstechnik
Aktuelle Sicherheitsinformationen des BSI zum Produkt können über den Link (QR Code) abgerufen werden
BSI Sicherheitsinfo

(Firm) – Manufacturer‘s Promise

This product meets the IT security requirements according to TR

Logo Manufacturer

Current BSI security information on the product can be accessed via the link (QR Code)

BSI Security Information

Federal Office for Information Security (BSI)

- **In parallel with the legal developments of the EU Cybersecurity Act, see Art 55 CSA:** Supplementary information on the cybersecurity of certified ICT products
- § 9a BSIG-E: Establishment of a **voluntary IT security label**
- **Purpose:** Implementation of the official mandate to warn of IT security gaps, consultation of various bodies
- Concretisation through a formed legal ordinance of the BMI
- **Contents:**
  - "Manufacturer’s declaration" contains IT security features
  - "BSI Security Information" informs about security gaps
  - **Representation**: Physically on product/repackaging, "electronic reference", probably **QR code**
- **BSI regularly checks** for compliance with the requirements of the IT security mark

Expected impact on businesses and consumers

- Trend towards **comprehensive IT security regulation** clearly visible, notably IoT
- **Further legislative changes** on IT security expected
- **Regulations of the BMI** probably bring more clarity about addressees, scope, etc.
- Not only data protection, but also consumer-related IT security becomes more and more of a **sales argument**
- **Substantial amount of sanctions** adapts IT security law to data protection law: max. €20,000,000 or 4% of global annual turnover
- In particular, also **foreign companies** will pay more attention to IT security regulation in the EU and Germany in the future

EU Cybersecurity Act (CSA)

General information

- **27.06.2019:** The CSA comes into force
- **Core content:** Introduction of a dual European system for (basically voluntary) certification of cybersecurity (in addition to restructuring ENISA)
- **Determination of aims:** Protecting the digital EU Single Market, facilitating foreign market access through recognition in all member states
- **Key statements:**
  - *"European cybersecurity certification scheme means a comprehensive set of rules, technical requirements, standards and procedures established at Union level for the certification or conformity assessment of certain ICT products, services and processes."*
  - *"European Cybersecurity Certificate means a document certifying that a specific ICT process, ICT product or ICT service has been assessed for compliance with fulfilling specific safety requirements, which are defined in a European system for cybersecurity certification.“*
- Until 28.06.2020: Definition of ICT products and services relevant for the implementation of the EU Cybersecurity Act in a list within the frame of the current work programme (Union Rolling Work Programme, URWP) of the EU Commission

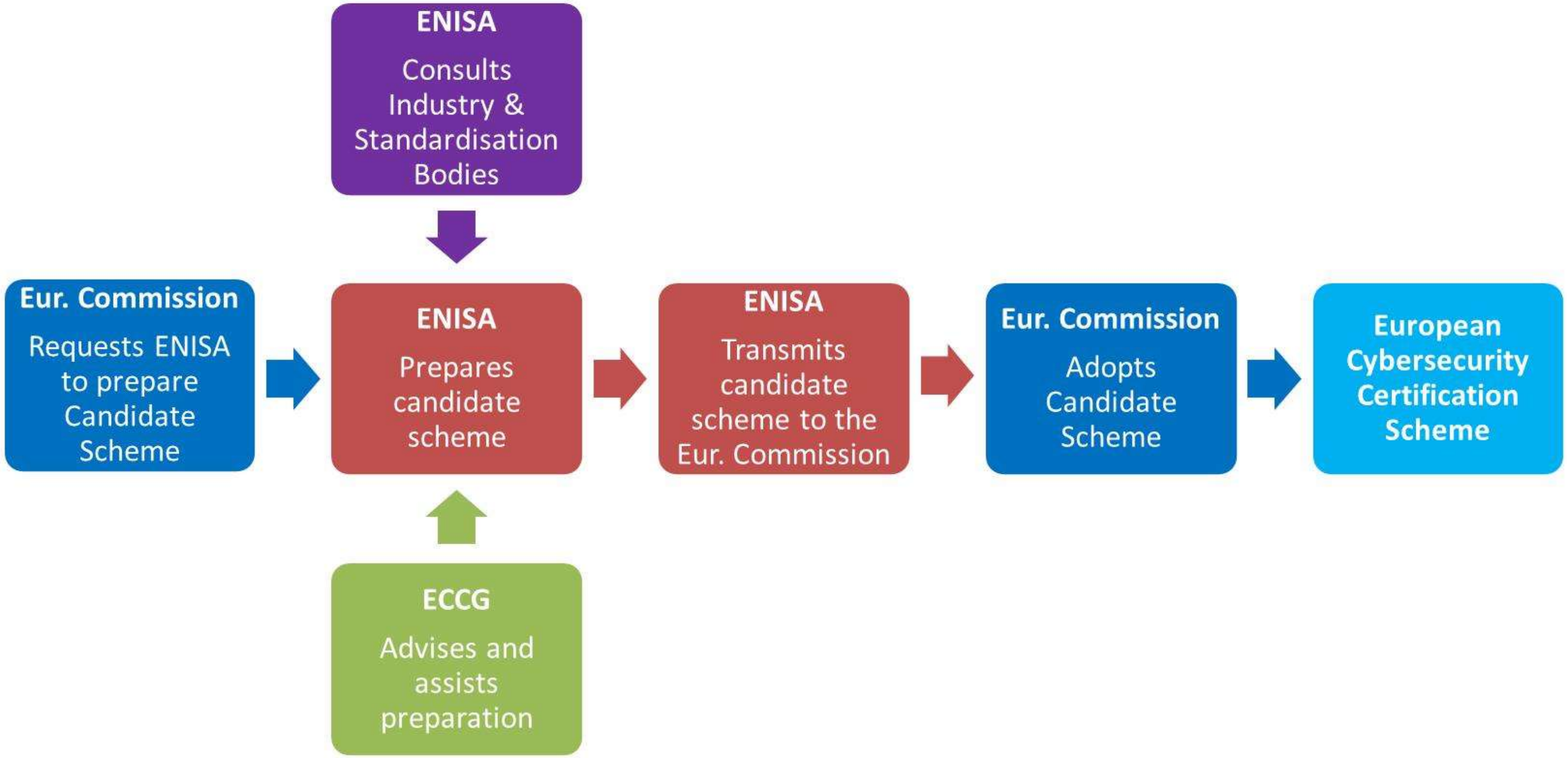
Key questions and requirements

- **Two key questions:**
  - How do the new certification schemes work together with existing regulations, especially those of the **New Legislative Framework (NLF)**?
  - How do the (numerous) different groups and institutions mentioned in the CSA function and cooperate with each other?
- "Existing requirements from NLF and new certification schemes from the CSA cannot and should not contradict each other" → **NLF is to be used as a "building block" or "toolbox"** to form the content basis for the new certification schemes in accordance with the CSA.
- **Schemes according to CSA = Refinement of the NLF**
- Moreover: generally at present, still voluntary certifications according to the CSA, at least for certain levels, are **not voluntary in the long term**, especially in the KRITIS sector

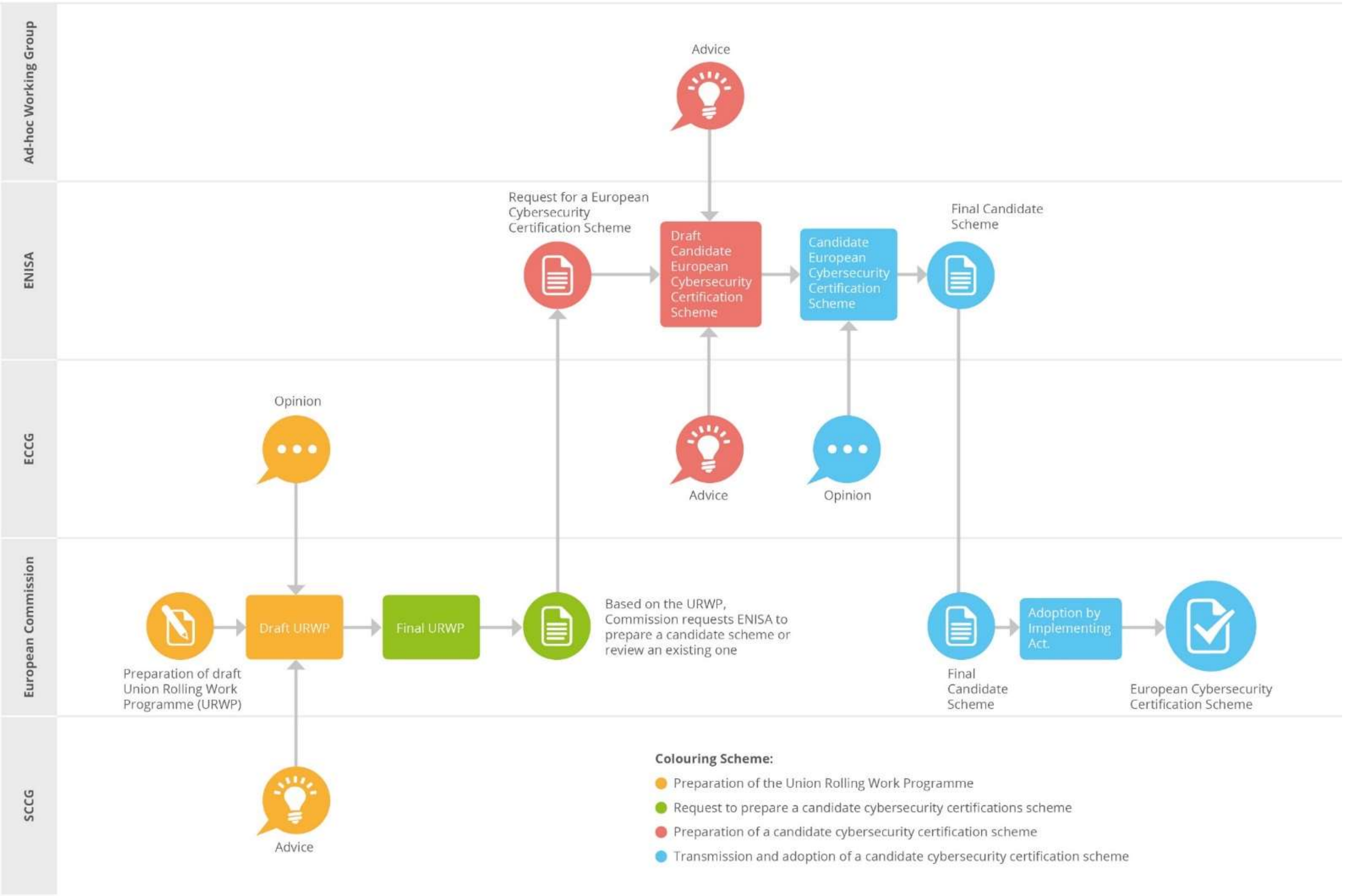
Key actors and groups in the CSA

- **Complex network** of different actors for the development of certification schemes according to EU CSA:
- ENISA (European Union Agency for Cybersecurity)
  - European Commission
  - SCCG (Stakeholder Cybersecurity Certification Group)
  - ECCG (European Cybersecurity Certification Group)
  - So-called Ad-hoc Working Groups (Ad-hoc WG)
- **→ More on the interaction in the following...**

Development of the certification schemes



ENISA
Consults Industry & Standardisation Bodies
Eur. Commission
Requests ENISA to prepare Candidate Scheme
ENISA
Prepares candidate scheme
ENISA
Transmits candidate scheme to the Eur. Commission
Eur. Commission
Adopts Candidate Scheme
European Cybersecurity Certification Scheme
ECCG
Advises and assists preparation

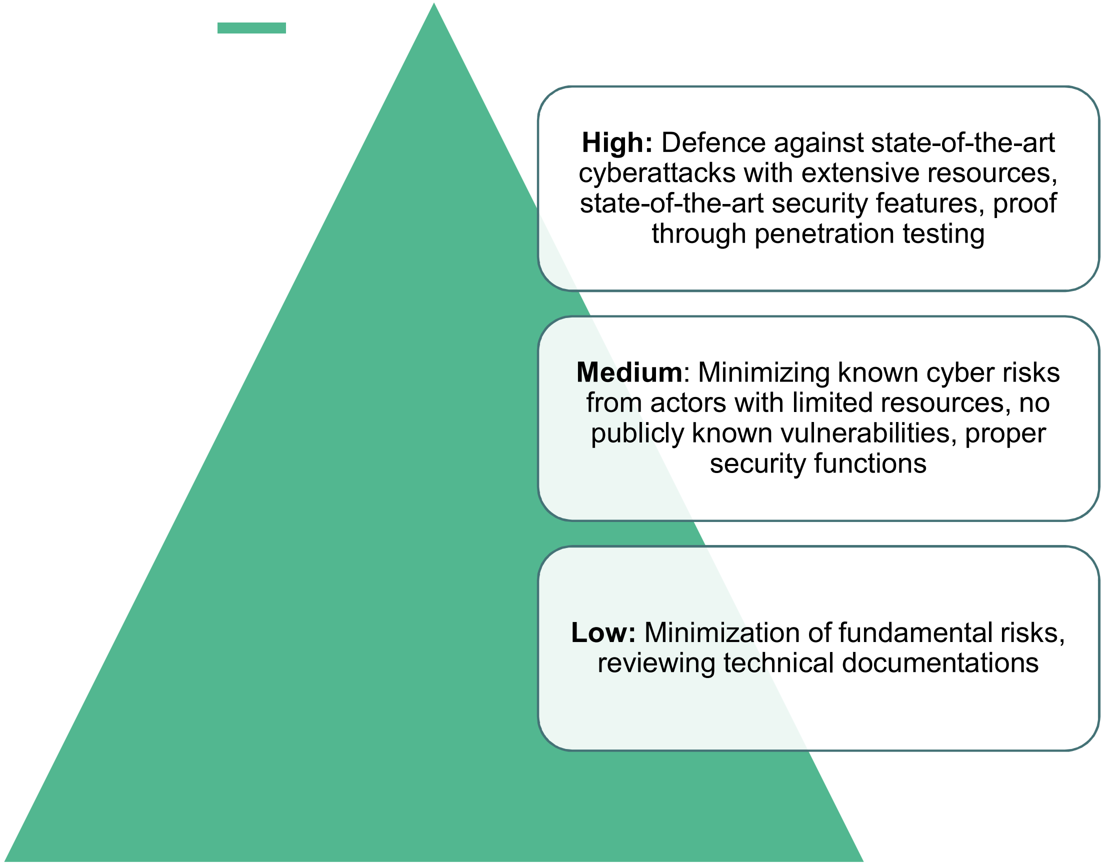

Ad-hoc Working Group
ENISA
ECCG
European Commission
SCCG
Advice
Request for a European Cybersecurity Certification Scheme
Draft Candidate European Cybersecurity Certification Scheme
Candidate European Cybersecurity Certification Scheme
Final Candidate Scheme
Opinion
Advice
Opinion
Preparation of draft Union Rolling Work Programme (URWP)
Draft URWP
Final URWP
Based on the URWP, Commission requests ENISA to prepare a candidate scheme or review an existing one
Final Candidate Scheme
Adoption by Implementing Act.
European Cybersecurity Certification Scheme
Advice
Colouring Scheme:
● Preparation of the Union Rolling Work Programme
● Request to prepare a candidate cybersecurity certifications scheme
● Preparation of a candidate cybersecurity certification scheme
● Transmission and adoption of a candidate cybersecurity certification scheme

Definition of the requirement levels of the schemes

Level of requirements depending on the respective risk of use

Rolling EU-COM work programme defines list of relevant ICT products/services until 1 year after entry into force of the Regulation (28.06.2020)

Product or service-related information obligations of the manufacturer/supplier



High: Defence against state-of-the-art cyberattacks with extensive resources, state-of-the-art security features, proof through penetration testing

Medium: Minimizing known cyber risks from actors with limited resources, no publicly known vulnerabilities, proper security functions

Low: Minimization of fundamental risks, reviewing technical documentations

The ad-hoc working groups as part of a complex network

- The **ad-hoc WGs are of particular interest** for companies for the design of the certification schemes and the practical participation on the specific requirements
- However: no "final" decisions are taken in the ad-hoc WGs → technical participation of "subject matter experts", support in drafting and consulting of ENISA
- **"Mistress of the procedure":** The EU-Commission makes the final decision on the adoption of the draft certification scheme

Participation in and structure of the ad-hoc working groups

- **Participation in ad-hoc WGs:** Potentially possible for any interested expert, existing and new ad-hoc WGs are advertised on the ENISA website
- ENISA's "Terms of Reference" (online) define the selection of candidates:
- 20 participants in total
  - Equal participation of relevant stakeholders
  - **Non-disclosure (NDL) Policy**
  - Distinction between elected representatives and "observers" as associated experts without their own direct participation/voting rights (e.g. national representatives of public authorities)

Participation in and structure of the ad-hoc working groups

- Currently, these ad-hoc WGs exist or are in the planning stages:
  - **Ad-hoc WG 01** – Transposition of the SOGIS-MRA certification framework (Call 01/19)
  - **Ad-hoc WG 02** – Cloud Services (Call for Participation 02/19 expired on 20.01.2020, start of work on 06.03.2020)
  - **Ad-hoc WG 03** – 5G (in planning, no official call has yet been communicated from ENISA)
- Probably remains for the time being with these three groups
- Number of ad-hoc WGs is based on the number of certification schemes to be created
- Expected to be in **the lower two-digit range**
- Prospect that in the future an ad hoc WG with a focus on **Industrial Security** will also be created

Tasks of the ad-hoc working groups

Measured by the content requirements to be applied to an EU certification scheme for cybersecurity according to **Art. 54 CSA**, e.g.:

- Definition of the subject matter and application field of the scheme
- Identification and evaluation of applicable standards
- Classification of the assurance level of the scheme
- Determination of requirements for conformity assessment bodies
- Development of evaluation criteria and methods
- Determination of participation requirements of the applicant
- Establishing the framework for mutual recognition with third countries

European Cybersecurity Certification Group (ECCG)

- Consists of representatives of the **national cybersecurity certification authorities**
- **Tasks:** Assisting ENISA in the development of certification schemes; advice and opinions on finalised drafts
- **First informal meeting:** autumn 2019, almost all member state representatives present → economic importance/EU internal market
- Creation of **subgroups** within the ECCG:
  - Preparation of content discussions, administrative tasks
  - Content is based on the topics of the ad-hoc WGs

Stakeholder Cybersecurity Certification Group (SCCG)

- Compared to ECCG and Ad-hoc WG **strategic advisory tasks** towards EU Commission and ENISA; preparation of the current URWP work programme → **"political body"**
- **50 members in total**, broadly diversified: scientific institutions, consumer organisations, conformity assessment bodies, standards bodies and related organisations, individual companies, European co-operation for Accreditation (EA), European Data Protection Board (EDPB)
- **Tender deadline expired on 17.09.2019**, objective: equal representation to cover the range of different interests
- Oversubscription (more than double the number of applicants), not formed yet
- Formation of **subgroups** also possible as in ECCG

Horizontal or vertical approach to certification schemes?

- Essentially, the **horizontal approach** to defining certification schemes has probably been followed so far
- Processing of existing normative requirements, e.g. from Common Criteria (CC) and/or ISO/IEC 27001 to new schemes e.g. for **Cloud Services, IoT, 5G and ISMS**
- **Problem:** insufficient mapping of vertical requirements, as partly created by legal requirements such as the EU GDPR or EU eIDAS Regulation

  → Conformity with this legislation normally requires more than compliance with just one horizontal scheme
- However, certifications are **regularly not the only way** to map an appropriate IT-security level according to the "state of the art"

Implementation of a certification

- **Dual testing system:** distinction between self-assessment of conformity by the manufacturer or supplier and the third-party certification
- **Content of the self-assessment:** Issuance of an EU Declaration of Conformity confirming that compliance with the requirements set out in the relevant system has been demonstrated → Manufacturer assumes personal responsibility in this respect
  - Only possible for the **"low" trust level**
  - Issuance of the EU Declaration of Conformity is **basically voluntary**
- **Content of the cybersecurity certification ("third party assessment"):**
  - Issuance of an **EU cybersecurity certificate** by a conformity assessment body or by an accredited public body/national cybersecurity certification authority
  - **Includes all levels of trust:**
    - "Low" and "medium": responsibility mainly rests with the (private) conformity assessment bodies
    - "High": responsibility basically rests with the national cyber security certification authority
  - An issued certificate is valid for the duration **specified in the respective certification system** and can be **renewed** if the requirements are met

Conformity assessment bodies and accreditation

- **Accreditation** of conformity assessment bodies by national accreditation bodies according to Regulation (EG) 765/2008 (**DAkkS**) is necessary
- **Annex to the regulation:** Comprehensive requirements for (private) conformity assessment bodies, in particular with regard to independence, competence and transparency
- Accreditation is granted for a maximum period of **five years**

  → An **extension is possible** if the requirements are still fulfilled
- For each adopted EU cybersecurity certification scheme, the national cybersecurity certification authority **notify** the corresponding conformity assessment bodies to the EU Commission
- The EU Commission publishes the **list of notified conformity assessment bodies** in the EU Official Journal

Conclusion and outlook

- The operational network of the CSA consists of a **complex network of various institutions and groups**, some of which are not yet fully formed
- The **SCCG** in particular is of considerable strategic importance and should therefore be formed as soon as possible
- The success of the CSA is crucially dependent on **close communication and coordination** between relevant stakeholders
- EU network basically suitable framework for action, but currently (still) too **little transparency and sufficient publicity**
- Highly questionable whether the first **URWP** will actually be published by the **end of June 2020**

Many thanks for your attention!

Dr. Dennis-Kenji Kipker

Executive Director

Certavo GmbH – international compliance management

dennis.kipker@certavo.de

+49 421 218 66049