EU CSA
Aktueller Stand der Umsetzung

Dr. Dennis-Kenji Kipker
Legal Advisor
CERT@VDE

DKE
VDE DIN

I. Einstieg und Rahmenbedingungen

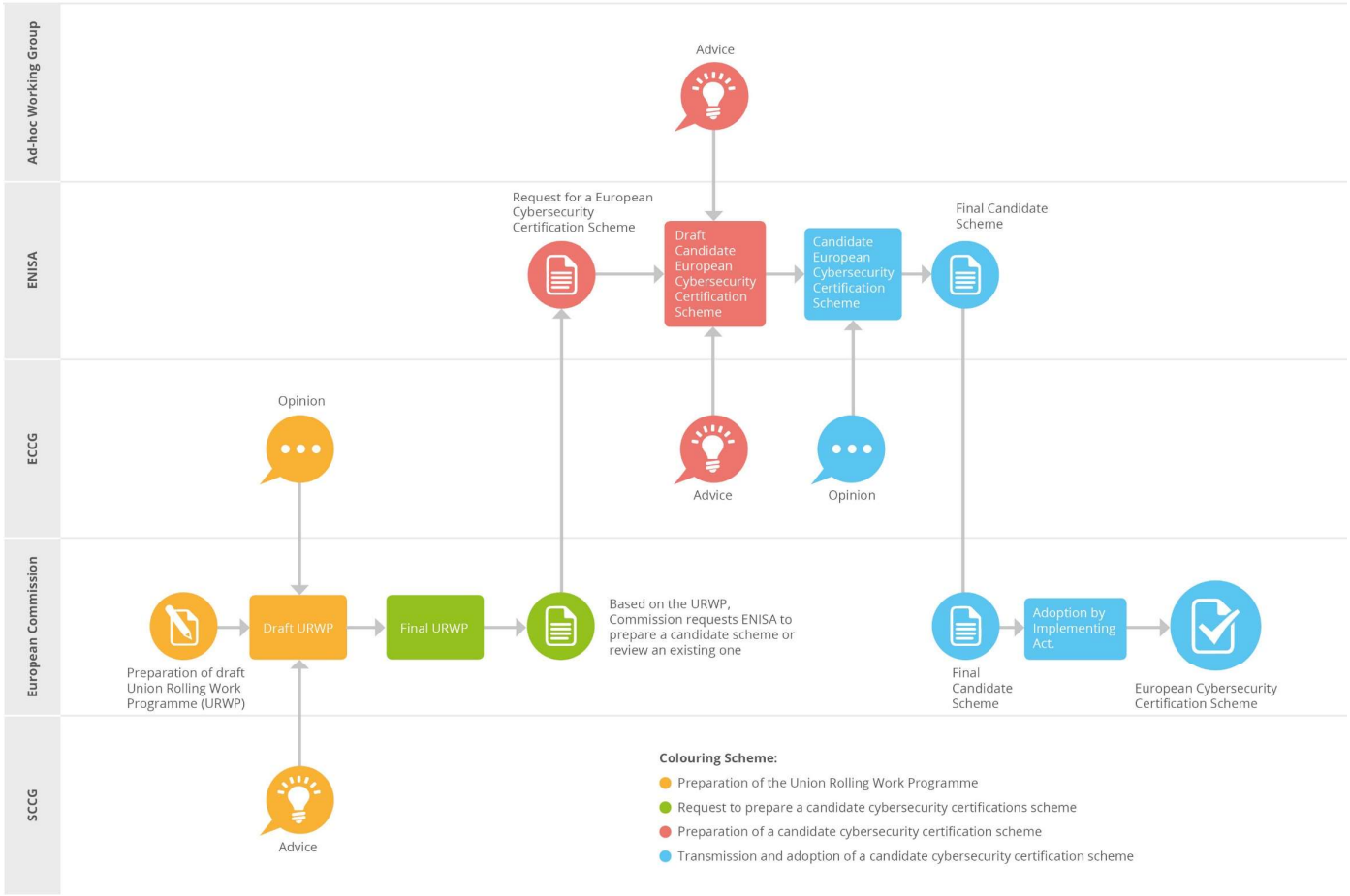
- **27.06.2019:** Inkrafttreten des CSA
- Bis 28.06.2019: Definition der für die Implementierung des EU Cybersecurity Act relevanten IKT-Produkte und Dienste in einer Liste im Rahmen des laufenden Arbeitsprogramms (**Union Rolling Work Programme, URWP**) der EU-Kommission (CSA, Verordnung EU 2019/881)
- → Stand der öffentlichen Diskussion zum Thema?!

II. Was wird gemacht, und wer wird tätig?

- **Zwei zentrale Fragestellungen:**
  - Wie arbeiten die neuen Zertifizierungsschemata mit bestehenden Regelungen, insbesondere solchen des New Legislative Framework (NLF), zusammen?
  - Wie funktionieren und kooperieren die (zahlreichen) verschiedenen Gruppen und Einrichtungen miteinander, die im CSA genannt werden?
- „Bestehende Vorgaben aus NLF und neue Zertifizierungsschemata aus dem CSA können und sollen zueinander nicht in einem Widerspruch stehen“ → **NLF soll als „Baukasten“ oder „Toolbox“** verwendet werden, um die inhaltliche Grundlage für die neuen Zertifizierungsschemata gemäß CSA zu bilden
- **Schemata gem. CSA = Verfeinerung des NLF**
- Überdies: zurzeit generell noch freiwillige Zertifizierungen gem. CSA zumindest für bestimmte Stufen **auf Dauer nicht freiwillig**, insb. KRITIS-Sektor

III. Unterschiedliche Akteure, unterschiedliche Aufgaben

- **Komplexes Netzwerk** verschiedener Akteure zur Erarbeitung der Schemata gem. EU CSA:
  - ENISA (European Union Agency for Cybersecurity)
  - Europäische Kommission
  - SCCG (Stakeholder Cybersecurity Certification Group)
  - ECCG (European Cybersecurity Certification Group)
  - Sog. Ad-hoc Working Groups (Ad-hoc WG)
- → **Zum Zusammenspiel im Folgenden…**


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

IV. Die Ad-hoc Working Groups als Bestandteil eines komplexen Netzwerks

- Für die Ausgestaltung der Zertifizierungsschemata und die praktische Mitarbeit an den konkreten Anforderungen sind vor allem für Unternehmen die **Ad-hoc WG von Interesse**
- Jedoch: in den Ad-hoc WG werden keine „finalen“ Entscheidungen getroffen → fachliche Beteiligung von **„subject matter experts“**, unterstützen bei Entwurfserstellung und Beratung von ENISA
- **„Herrin des Verfahrens“:** EU-Kommission trifft finale Entscheidung über die Annahme des Entwurfs für ein Zertifizierungsschema

DKE
VDE DIN

V. Teilnahme an und Aufbau der Ad-hoc Working Groups

- **Teilnahme an Ad-hoc WG:** Potenziell für jeden interessierten Experten möglich, bestehende und neu hinzutretende Ad-hoc WG sind auf ENISA-Website ausgeschrieben
- „Terms of Reference“ (online) von ENISA legen Auswahl der Bewerber fest:
  - 20 Teilnehmer insgesamt
  - Gleichmäßige Beteiligung relevanter Interessenkreise
  - **Non-disclosure (NDL) Policy**
  - Unterscheidung zwischen gewählten Vertretern und „Observers“ als beigeordnete Fachexperten ohne eigene direkte Mitwirkungsmöglichkeit/Stimmberechtigung (z.B. nationale Behördenvertreter)

V. Teilnahme an und Aufbau der Ad-hoc Working Groups

- Zurzeit existieren diese Ad-hoc WG bzw. sind in Planung:
  - **Ad-hoc WG 01** – Transposition of the SOGIS-MRA certification framework (Call 01/19)
  - **Ad-hoc WG 02** – Cloud Services (in Planung, Call for Participation 02/19 ist am 20.01.2020 abgelaufen)
  - **Ad-hoc WG 03** – 5G (in Planung, bisher noch kein offizieller Call von der ENISA kommuniziert)
- Bleibt wahrscheinlich zunächst bei diesen drei Gruppen
- Zahl der Ad-hoc WG bemisst sich an der Anzahl der zu erstellenden Zertifizierungsschemata
- Voraussichtlich im **unteren zweistelligen Bereich**
- Aussicht, dass zukünftig auch eine Ad-hoc WG mit Schwerpunkt auf **Industrial Security** angelegt wird

VI. Aufgaben der Ad-hoc Working Groups

Bemessen sich an den inhaltlichen Anforderungen, die an ein EU-Zertifizierungsschema zur Cybersicherheit gem. **Art. 54 CSA** anzulegen sind, z.B.:

- Festlegung von Gegenstand und Anwendungsbereich des Schemas
- Ermittlung und Evaluierung anwendbarer Standards
- Einordnung des Zusicherungsniveaus des Schemas
- Bestimmung von Anforderungen an Konformitätsbewertungsstellen
- Entwicklung der Evaluationskriterien und Methoden
- Bestimmung von Mitwirkungsanforderungen des Antragstellers
- Festlegung des Rahmens für die gegenseitige Anerkennung mit Drittstaaten

VII. European Cybersecurity Certification Group (ECCG)

- Setzt sich aus Vertretern der **nationalen Cybersicherheitszertifizierungsbehörden** zusammen
- **Aufgaben:** Unterstützung von ENISA bei Erarbeitung der Zertifizierungsschemata; Ratschläge und Stellungnahmen zu fertig gestellten Entwürfen
- **Erste informelle Sitzung:** Herbst 2019, nahezu sämtliche mitgliedstaatlichen Vertreter anwesend → wirtschaftlicher Stellenwert/EU-Binnenmarkt
- Bildung von Unterarbeitsgruppen (**Subgroups**) innerhalb der ECCG:
  - Vorbereitung inhaltlicher Diskussionen, administrative Aufgaben
  - Bemessen sich inhaltlich an den Themen der Ad-hoc WG

VIII. Stakeholder Cybersecurity Certification Group (SCCG)

- Verglichen mit ECCG und Ad-hoc WG **strategische Beratungsaufgaben** gegenüber EU-Kommission und ENISA; Erarbeitung des laufenden Arbeitsprogramms URWP → **„politisches Gremium“**
- **Insgesamt 50 Mitglieder**, breit gefächert: wissenschaftliche Einrichtungen, Verbraucherorganisationen, Konformitätsbewertungsstellen, Standardisierer und entsprechende Organisationen, Einzelunternehmen, European co-operation for Accreditation (EA), European Data Protection Board (EDPB)
- **Ausschreibungsfrist abgelaufen am 17.09.2019**, Ziel: paritätische Besetzung zur Abdeckung der Bandbreite verschiedener Interessen
- Überzeichnung (mehr als doppelte Bewerberzahl), bisher noch nicht gebildet
- Ebenfalls wie in ECCG Bildung von **Subgroups** möglich

IX. Horizontaler oder vertikaler Ansatz für Zertifizierungsschemata?

- Im Wesentlichen bisher wohl Verfolgung von **horizontalem Ansatz** zur Festlegung der Zertifizierungsschemata
- Verarbeitung bestehender normativer Anforderungen, z.B. aus Common Criteria (CC) und/oder ISO/IEC 27001 zu neuen Schemata z.B. für **Cloud Services, IoT, 5G und ISMS**
- **Problem:** Unzureichende Abbildung vertikaler Anforderungen, wie sie teils durch gesetzliche Vorgaben wie EU DS-GVO oder EU eIDAS-Verordnung geschaffen werden

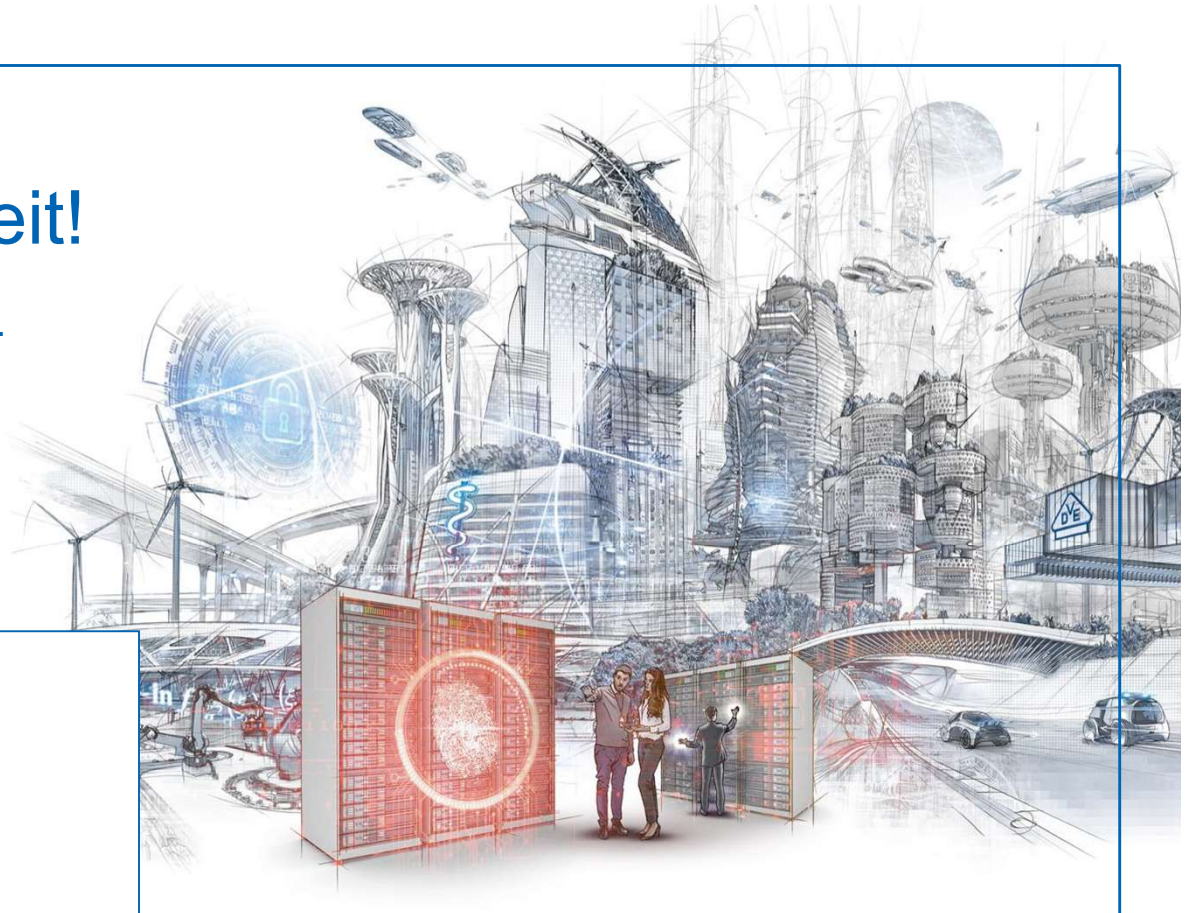
  → Konformität mit diesen Rechtsvorschriften setzt im Regelfall mehr als die Erfüllung nur eines horizontalen Schemas voraus
- Zertifizierungen aber **regelmäßig nicht einziger Weg** zur Abbildung eines angemessenen IT-Sicherheitsniveaus gemäß „Stand der Technik“

X. Fazit und Ausblick

- Operationelles Netzwerk des CSA setzt sich aus **komplexem Verbund verschiedener Einrichtungen und Gruppen** zusammen, die teils noch nicht vollständig gebildet sind
- Insbesondere **SCCG** besitzt erheblichen strategischen Stellenwert und sollte deshalb schnellstmöglich gebildet werden
- Erfolg des CSA in entscheidender Weise davon abhängig, dass relevante Stakeholder in einem **engen Austausch und in intensiver Abstimmung** zueinander stehen
- EU-Netzwerk grds. geeigneter Handlungsrahmen, aber zurzeit (noch) zu **wenig Transparenz** und hinreichende Öffentlichkeit
- Fraglich, ob erstes **URWP** tatsächlich bis **Ende Juni 2020** publiziert wird

Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.



Ihr Ansprechpartner:

Dr. Dennis-Kenji Kipker

Legal Advisor, CERT@VDE

Tel. +49 151 40223163

dennis-kenji.kipker@vde.com