Europäische KI-Normung – Endspurt zum AI Act

Webinar
17. Juli 2024
14:30-16:30 Uhr

Agenda

14:30 – 14:35	▪ Begrüßung
14:35 – 15:25	▪ Europäische KI-Normung: Weg zur Umsetzung des AI Act
15:25 - 15:45	▪ Erfahrungen und Herausforderungen als WG-Convenor im JTC 21
15:45 – 16:05	▪ Chancen und Herausforderungen aus Sicht der Prüfindustrie
16:05 – 16:25	▪ Normungsprozesse und Mitarbeit in Normungsgremien
16:25 – ca. 16:30	▪ Wrap-up

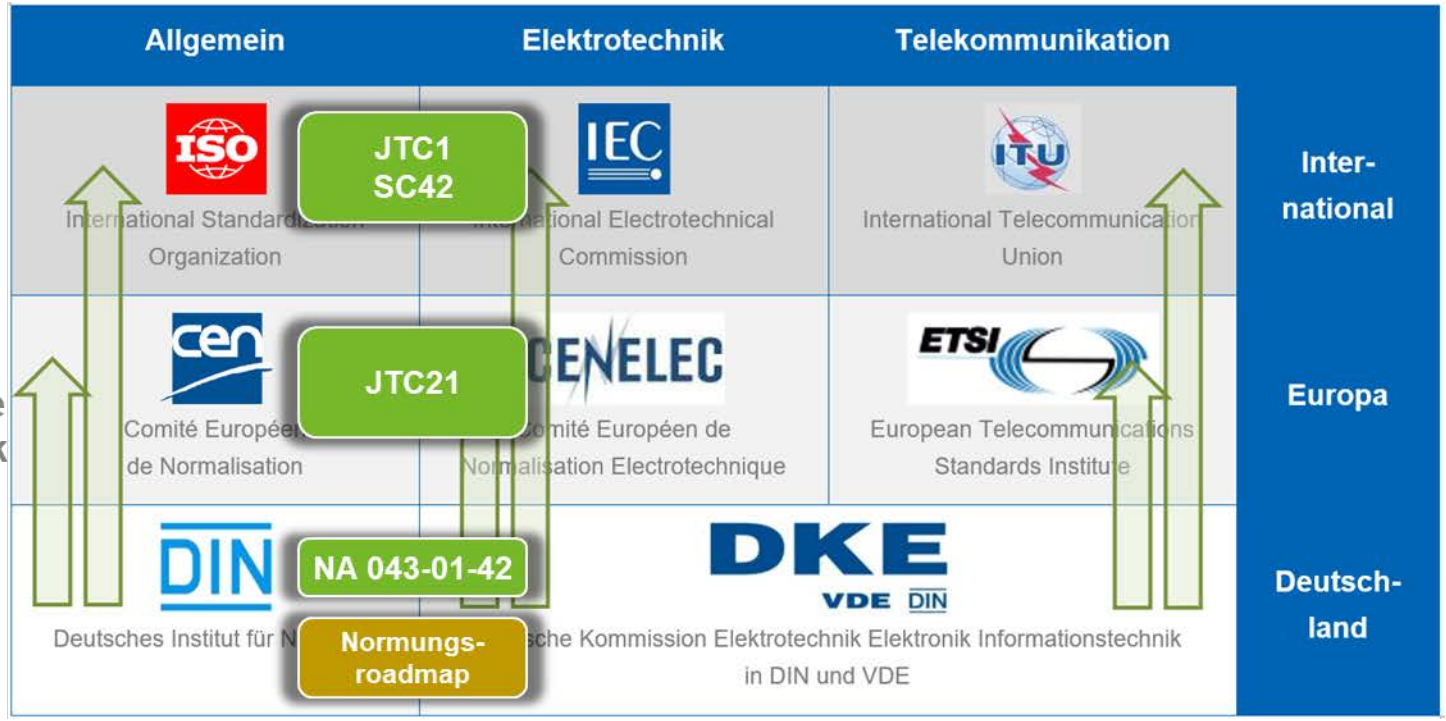
Europäische KI-Normung:
Der Weg zur Umsetzung des AI Act

Sebastian Hallensleben
Chair, CEN-CENELEC JTC21
17.07.2024

Wo findet europäische KI-Standardisierung statt?

New Legislative Framework

AI Act



Zusammenspiel von Regulierung und Standardisierung: Das New Legislative Framework

European Commission

- **Essential requirements** designed to ensure a high-level of protection of public interests. They define the results to be attained, or the hazards to be dealt with, but do not specify the technical solutions for doing so
- **Harmonized standards** detailing technical solutions to meet the essential requirements
  - Voluntary – manufacturers can use other methods
  - Presumption of conformity with the essential requirements they cover

- **Division of responsibilities** along the value & distribution chain of the product
  - Manufacturers, importers, distributors, authorized representatives
- **Conformity assessment procedures**
  - Internal checks
  - Third-party assessment

Standardisation request der EU

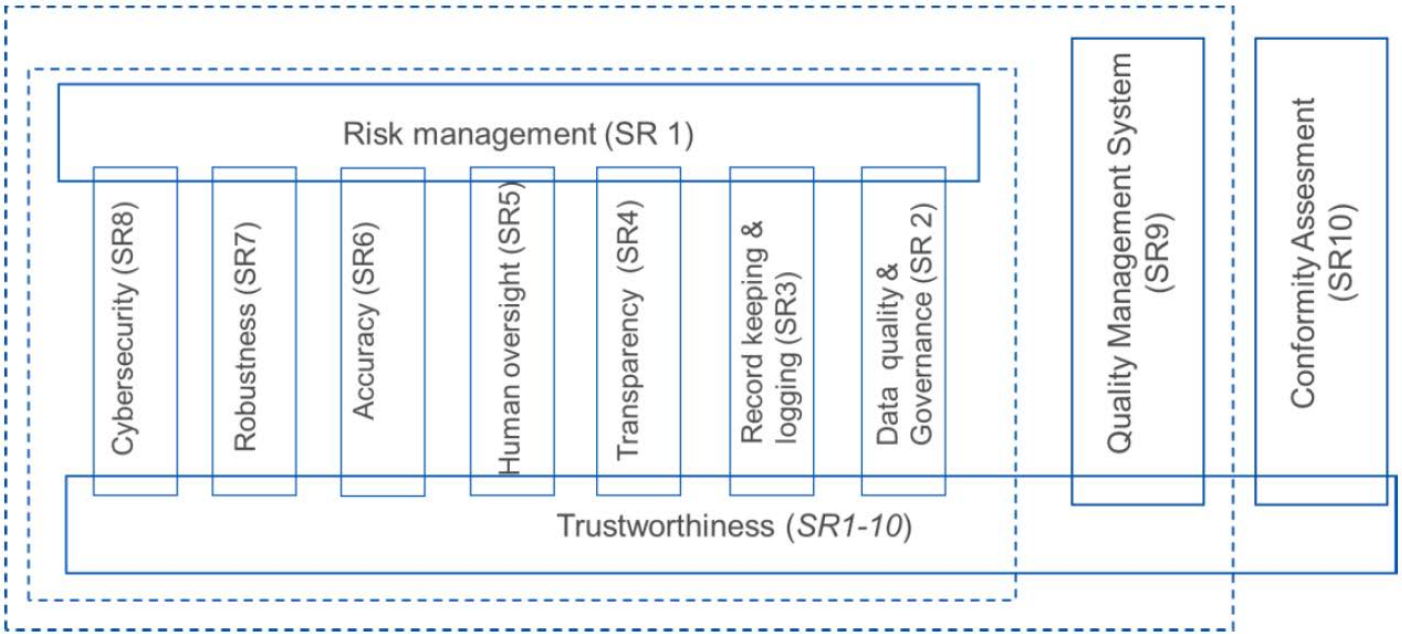
1.	European standard(s) and/or European standardisation deliverable(s) on risk management system for AI systems
2.	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems
3.	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems
4.	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions to the users of AI systems
5.	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems

Ergänzungen angekündigt:

11. ... ... nachhaltige KI ... ...
12. ... ... generative KI ... ...

6.	European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems
7.	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems
8.	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems
9.	European standard(s) and/or European standardisation deliverable(s) on quality management system for providers of AI systems, including post-market monitoring process
10.	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems

Architecture of standards zur Strukturierung



Working Groups

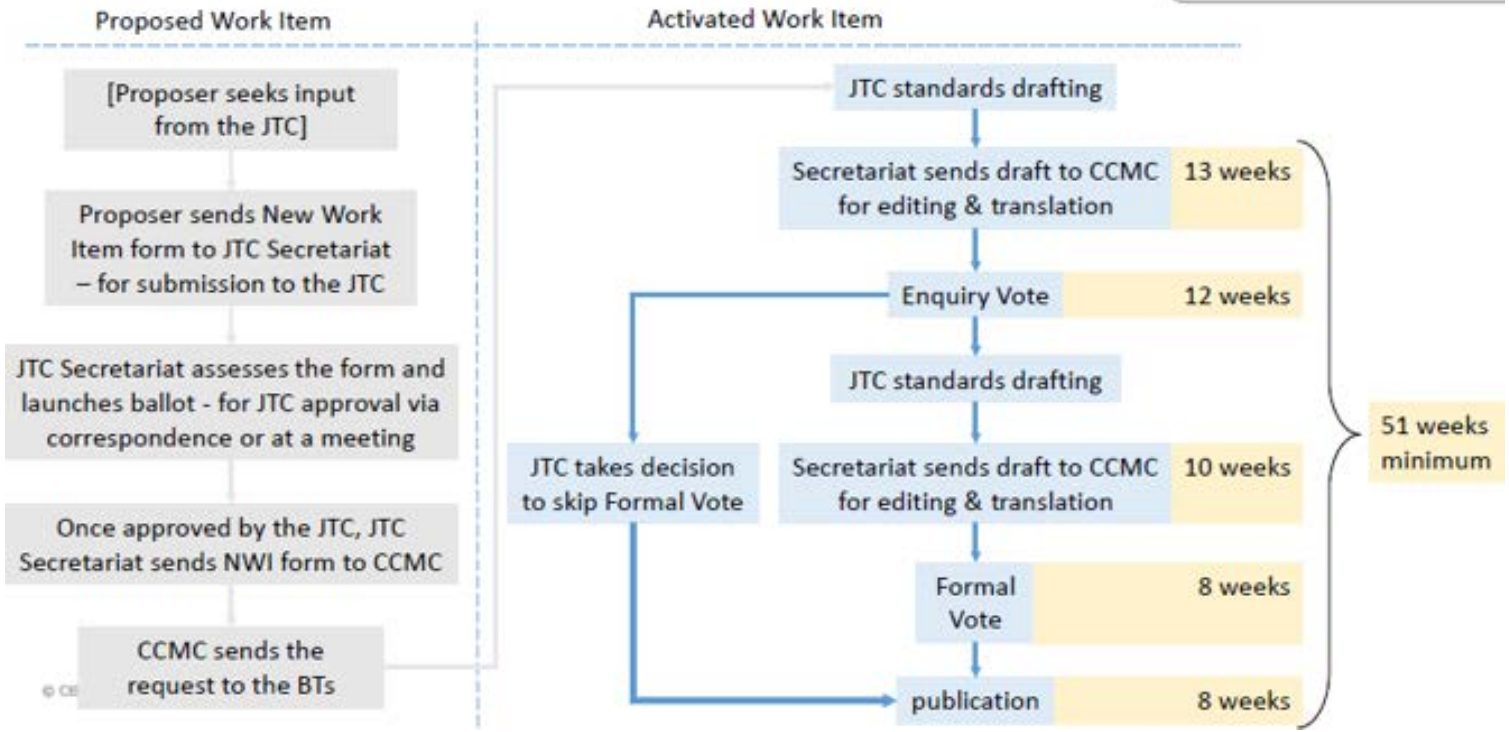
- WG1: Strategic Advisory Group
- WG2: Operational Aspects
- WG3: Engineering Aspects
- WG4: Foundational and Societal Aspects
- WG5: Cybersecurity

Zeitablauf

>1000 Experten
25 Länder
140 Experten direkt im JTC21

- Inhaltliche Arbeit für sämtliche erforderlichen Deliverables läuft,
  Strukturen stehen schon seit ca. Anfang 2023
- Fast die gesamte Aktivität des JTC21 zahlt auf den Standardisation Request / AI Act ein
  = **oberste Priorität**
- Entwürfe für die zu harmonisierenden Standards bis ca. **Ende 2024**
- Veröffentlichung spätestens ca. **Ende 2025**,
  ⇒ ca. **halbes Jahr Zeit zur Umsetzung** bis zum Wirksamwerden des AI Acts (**01.08.2026**)

"Homegrown" standards process



Zeitliche Risiken und deren Mitigierung

Risiken / Herausforderungen	Mitigierung
Endliche Bandbreite in der europäischen Normung	▪ Aufbau auf internationale Standards wo immer möglich ▪ **Direct adoption**, wo ausreichend ▪ **Modified adoption** als innovativer Prozess, von CEN-CENELEC bestätigt
Verzögerungen und inhaltliche Unwägbarkeiten in der internationalen Normung	▪ Sparsame Verwendung von „**parallel development**“ ▪ Adoption nur, wenn intl. Standard bereits (fast) fertiggestellt, d.h. inhaltlich und zeitlich stabil sind
Hoher Anspruch des AI Acts; Interpretationsspielräume; HAS Assessement	▪ Aktive Rolle der EU-Kommission (DG CNECT) in JTC21 bei Plenary Meetings sowie in den Arbeitsgruppen schon seit 2021 ⇒ frühzeitige Ausräumung von Unsicherheiten und Kontroversen ▪ Verzicht auf den HAS-Prozess, stattdessen direkte Beurteilung durch DG CNECT
z.T. schwierige Konsensbildung durch divergierende Interessen	▪ Regelmäßige Bereitstellung von Analysen durch den Joint Research Council ▪ Intensive politische Unterstützung und Flankierung durch die EU-Kommission ▪ Verdeutlichung der allseits unerfreulichen Auswirkungen von „common specifications“ ▪ Straffung von CEN-CENELEC-Prozessen ⇒ mehr Zeit für inhaltliches Alignment

Übernahme internationaler Standards ist der bevorzugte Weg, jedoch nicht immer gangbar: Beispiel ISO/IEC 42001 Management System for AI

- Veröffentlicht November 2023
- Integriert in die internationale Systematik von MS-Standards
- Bereits vielfältige Beratungs- und Prüfungsangeboten weltweit

Können wir die 42001 für Europa übernehmen?

Frühzeitiges „Nein“ der EU wegen mehrfachem Mismatch:

42001	Bedarf für AI Act
Risikoverständnis nach ISO 31000 / Guide 73: Risiko = Unsicherheit	Risikoverständnis nach IEC Guide 51: Risiko = Schaden x Eintrittswahrscheinlichkeit
Bezieht sich auf eine Organisation	Bezieht sich auf ein Produkt
Fokus auf Good Practice	Focus auf messbaren, durchsetzbaren Anforderungen

Vorgehen im JTC21:

Europaspezifische Standards für Qualitäts- und Risikomanagement, aber mit starker Referenzierung von 42001, 14791 etc.

Was können Unternehmen tun?

	Ab sofort	Ab Frühjahr 2025	Ab Anfang 2026
Zu Normen beitragen, mitgestalten	• **Aktive Mitgliedschaft** im GA 043-01-42 und im JTC21 • Einbringung von **technischer Expertise** und **Konsensbildungstalent** • **Pragmatismus**: „Perfekt“ wird es in endlicher Zeit nicht geben.	• Fokussierte und konstruktive **Kommentierung im Enquiry Vote** • ggf. Ausloten von Konsensräumen auch mit Kollegen in den National Committees anderer Länder	• Unterstützung von **Lieferanten und Kunden** bei Interpretation und Umsetzung der Normen
Das eigene Unternehmen vorbereiten	• **Analyse AI Act:** Was ist *außerhalb* des Standardisation Request für mein Unternehmen relevant? z.B. Einstufung von Anwendungen / Systemen nach Risikoklassen • **Analyse Geschäftspotenzial**: Wo bringt eine (Über)Erfüllung des AI Act auch einen Wettbewerbsvorteil? ggf. Mitgliedschaft in AI Trust Alliance	• Mitwirkung im GA 043-01-42 und **Auseinandersetzung mit** den stabiler werdenden **Normenentwürfen** • Definition der **Umsetzungsprojekte** • Reservierung von **Ressourcen**	• **Umsetzung der endgültigen Normen** als rechtssicherer Weg zur Compliance im Juli 2026

Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner:

Dr. Sebastian Hallensleben

VDE e.V., Leiter AI & Digital Trust

Tel.: +49 69 6308 305
E-Mail: sebastian.hallensleben@vde.com

Erfahrung aus der Arbeit als WG-Convenor im JTC 21 und Herausforderungen

CEN CENELEC JTC 21 WG 5 Cybersecurity

CEN CENELEC JTC 21 WG 5 Cybersecurity

Erwartungen der EC an die Normung → Cybersecurity Standardisation Request

SR8: **European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems**

- [**AIM**] This (these) European standard(s) or European standardisation deliverable(s) **shall provide** suitable organisational and technical solutions, to ensure that AI systems are resilient against attempts to alter their use, behaviour, or performance or to compromise their security properties by malicious third parties exploiting the AI systems' vulnerabilities.
- [**COVERAGE**] Organisational and technical solutions shall therefore include, where appropriate, **measures to prevent and control cyberattacks trying to manipulate AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial examples), or trying to exploit vulnerabilities in an AI system's digital assets or the underlying ICT infrastructure. These technical solutions shall be appropriate to the relevant circumstances and risks.**
- [**CRA**] This (these) European standard(s) or European standardisation deliverable(s) shall take due account of the essential requirements for products with digital elements as listed in Sections 1 and 2 of Annex I to the proposal for a Regulation of the European Parliament and the Council on horizontal cybersecurity requirements for products with digital elements.

The AI Act and the SR – 4 main elements:

- High-risk AI systems should be ensured and designed to be resilient against attempts to alter their use, behavior, and performance and to compromise their security properties by malicious third parties exploiting the AI systems' vulnerabilities.
- Organizational and technical solutions shall be implemented to address these goals.
- A cybersecurity risk assessment shall be done for high-risk AI systems.
- Technical solutions shall be appropriate to the relevant circumstances and risks.

Berücksichtigung bestehender internationaler Standards

Berücksichtigung bestehender internationaler Standards

- ISO/IEC 27 Reihe insb. 27001/27002 ff. 27090 (WD) AI treats and mitigations
- Ggfs. relevante Standards aus SC 42
- Ggfs. relevante Standards der Sektoren wie Functional Safety and AI, Autonom Driving and AI……..
- Ggfs. relevante Standards von ETSI o.a.
- Gaps in Bezug auf Produkt-Security ?

neue Standards auf EU Ebene (JTC 13 zu CRA; AI spezifische aus JTC 21)

- hEN Cybersecurity for AI Systems (product)
- AI Cybersecurity Risk Assessment
- Cybersecurity AI Conformity Assessment ?
- Einbindung JTC 13
  CRA Standards, zu spät für den AI Act;
  RED Standards
- Verbindungen zu den anderen AIA SR ´s ?
- ETSI Einbindung

Herausforderungen als Convenor

- Heterogener Expertenkreis und unterschiedliche Expertise für Cybersecurity oder AI.
- Missverständliche Position von Cybersecurity im AI-A in Verbindung mit anderen SR´s und zum holistischen Ansatz (all Hazard) aus bestehenden Regulierungen und Standards.

- Konsensfindung basiert auf den unterschiedlichen Ansichten.
- Ein JTC 21 Konsens könnte deshalb zu Schwierigkeiten mit bestehenden Standards führen bzw. den Interessen der europäischen Industrie wiedersprechen.

- Zu wenig (deutsche) Experten, die schreiben – wer schreibt der bleibt !!!
- Verbleibendes Zeitfenster

Motivation zur Mitarbeit

- **gewünschte Expertise im JTC 21**
  - Cybersecurity Experten mit Motivation für AI
  - AI Experten mit Motivation für Cybersecurity
  - insbesondere zu Themen wie Testen, Robustness, Accuracy, Explainabiltiy, Logging, Data, Conformity Assessment und Produktüberwachung postmarket
- **denkbare Möglichkeiten um sich geeignet in den Sektoren bei JTC 21 einzubringen**
  - Es gibt aktuell keine relevanten sectorspezifischen Vertretungen/Gruppen mit Experten zu AI und Cybersecurity bei CEN CENELEC, **das wäre sehr wünschenswert.**
  - Zusammenarbeit mit JTC 21 AI Act Themen/WGs, um die sektorspezifischen Anforderungen geeignet zu positionieren/berücksichtigen und/oder in die eigenen Standards zu integrieren.

Kontakt

Annegrit Seyerlein-Klug

Dipl. Ing. TU Berlin, Medizintechnik
M Sc. Security Management
M Sc. Technologie und Innovationsmanagement

- Nixdorf/ Siemens Nixdorf/ Siemens Business Services
- Siemens/Siemens Enterprise/Unify
- Secunet
- Neurocat (AI security and robustness)
- Zertifizierung in ISO 27001 und ITIL
- Dozentin Technische Hochschule Brandenburg
- European Academy for Freedom of Information and Data Protection (EAID)
- Kompetenzzentrum Kritische Infrastruktur BB (KKI)
- **DIN Security/KI, CEN CENELEC JTC 21 WG5 Convenor**

annegrit.seyerleinklug@th-brandenburg.de

Chancen und Herausforderungen aus Sicht der Prüfindustrie

Standardization Request No. 10 und der NLF

Susanne Kuch

Agenda

1)	▪ Braucht es eine Prüfindustrie für den EU AI Act?
2)	▪ Aktuelle Pain Points und Herausforderungen für die Prüfindustrie
3)	▪ Notwendige Expertise / Notwendige Aktivitäten für Prüfindustrie im JTC 21

Braucht es eine Prüfindustrie für den EU AI Act?

- **EU AI Act** ist in den **New Legislative Framework eingebettet**
- Eine **Prüfung durch unabhängige Dritte ist für Hochrisiko KI-Systeme notwendig**.
  - Notifizierte Stellen bewerten **Qualitätsmanagementsystem** sowie **technische Dokumentation** auf Konformität (AI Act Anhang VII)
- Antwort ist also: **Ja, wir brauchen eine Prüfindustrie**

- Wir brauchen für **Hochrisikosystemen** vor allem **Zertifizierungsstellen für Produkte, Prozesse und Dienstleistungen (gemäß DIN EN ISO/IEC 17065) und für Managementsysteme (DIN EN ISO/IEC 17021-1)**
  - Weitere mögliche Stellen: Prüflabore (DIN EN ISO/IEC 17025); Inspektionsstellen (DIN EN ISO/IEC 17020) sowie Validierungs- und Verifizierungsstellen (DIN EN ISO/IEC 17029)

Aktuelle Pain Points und Herausforderungen für die Prüfindustrie

Fehlende Grundlagen(forschung)

- Aktuell erst **in Entwicklung befindliche Anforderungen an KI-Systeme** in Standardisierung entwickelt (Parallelisierung)
- **Kaum wissenschaftlich fundierte, vertrauenswürdige Testverfahren** für KI-Modelle
  - **Fehlende Metriken** für Prüfverfahren (gemäß DIN EN ISO/IEC 17025)
  - **Fehlende** qualitativ hochwertige **Referenzdaten** für Anwendungen

Internationales System ist einzuhalten

- Standardization Request: Entwicklung von Konformitätsbewertungsstandards, die
  - **Verfahren & Prozesse** für **Konformitätsbewertungstätigkeiten** im Zusammenhang **mit KI-Systemen** (17065) **& QMS** (17021-1) **von Anbietern**
  - **Kriterien** für die **Bewertung der Kompetenz** der mit der Konformitätsbewertung beauftragten Personen beauftragt sind (17024).

Notwendige Expertise / Notwendige Aktivitäten für Prüfindustrie im JTC 21

Expertise

- Welche Prüfmethoden sind robust genug, um sie für Konformitätsbewertung zu nutzen und zu standardisieren?
- Für welche Konformitätsbewertungsstandards braucht es KI-spezifische Spezifikationen?
- Wie stelle ich fest, ob sich KI-System um ein Sicherheitsmodul handelt?

→Für diese Fragen braucht es **Expertise von Konformitätsbewertungsstellen,**

Aktivitäten

- Aktive Teilnahme auf CEN/CENELEC Ebene an Standardisierung
- Aufklärungsarbeit mit leisten, wie NLF funktioniert

→ Austausch auf internationaler Ebene ist auch wichtig (in IAF, ILAC sowie ISO/IEC)

Kontakt

Susanne Kuch

Referentin für Digitalisierungspolitik der Qualitätsinfrastruktur

Deutsche Akkreditierungsstelle (DAkkS)

Project Editor ISO/IEC 42006

susanne.kuch@dakks.de

Webinar: Europäische KI-Normung – Endspurt zum AI Act

Normungsprozesse

17. Juli 2024

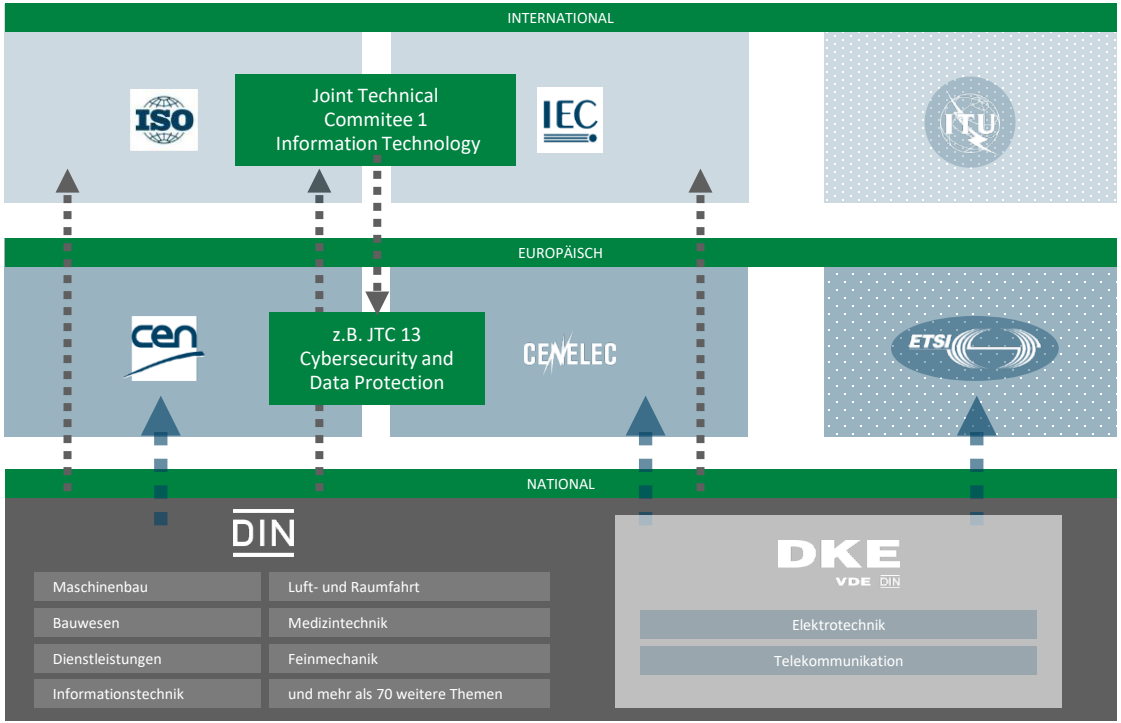
Peter Deussen

Obmann DIN/DKE Gemeinschaftsausschuss KI

Microsoft Deutschlang GmbH

peter.deussen@microsoft.com

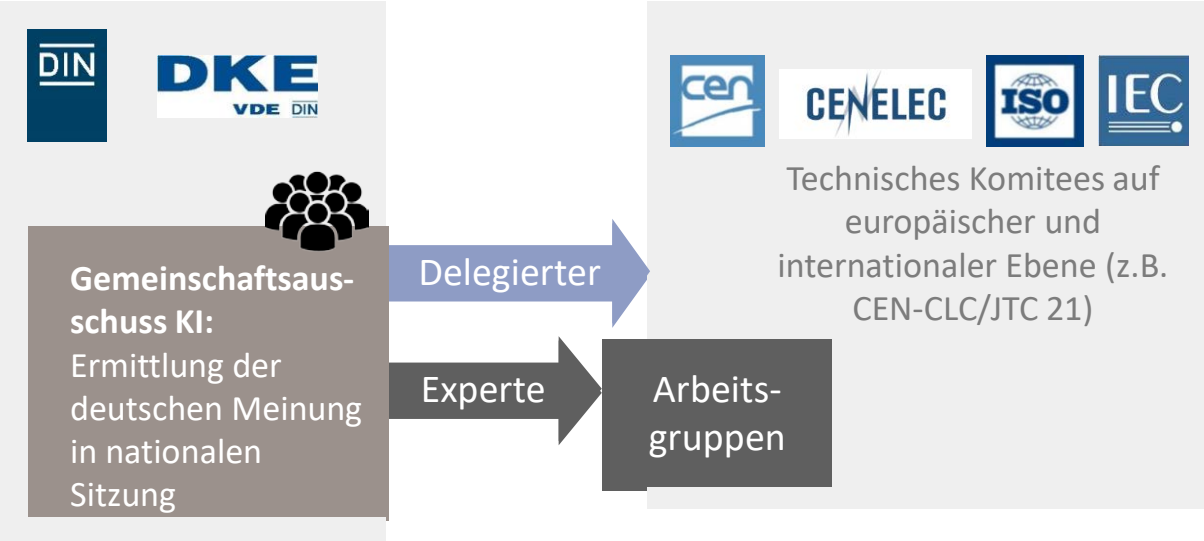
Übersicht Normungsumfeld



ISO:	Internationale Organisation für Normung
IEC:	Internationale Elektrotechnische Kommission
ITU:	Internationale Fernmeldeunion
CEN:	Europäisches Komitee für Normung
CENELEC:	Europäisches Komitee für Elektrotechnische Normung
ETSI:	Europäisches Institut für Telekommunikationsnormen
DIN:	Deutsches Institut für Normung e.V.
DKE:	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

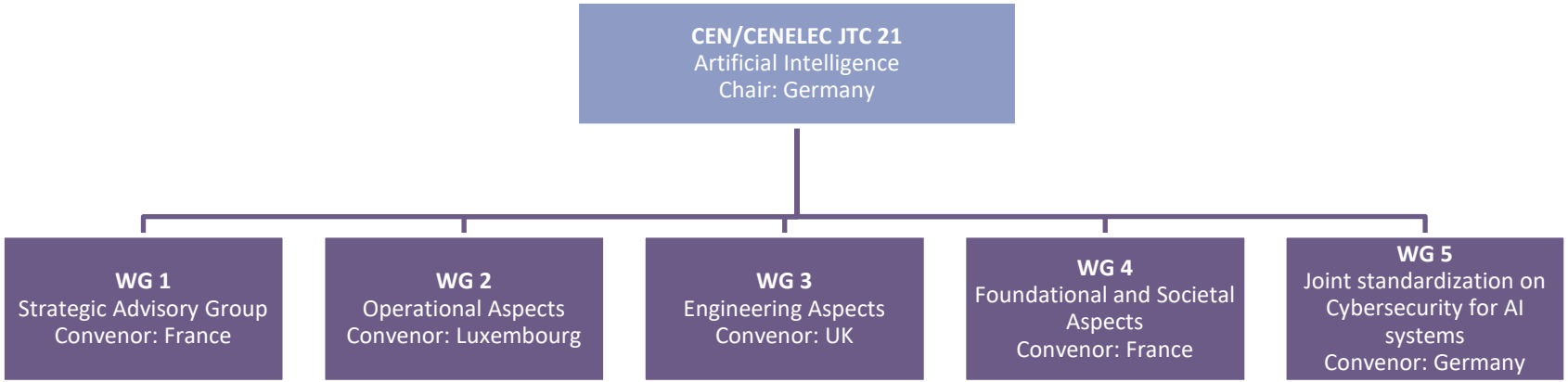
DIN und DKE vertreten die nationalen Interessen in der europäischen und internationalen Normung.

Mitarbeit in europäischen und internationalen Normungsgremien



- *Beitragen der deutschen Meinung in europäischen/internationalen Sitzungen (Plenary, 2-3 pro Jahr)*
- *Beitragen der Expertenmeinungen (meist national erarbeitet) in Arbeitsgruppen (mehrmals jährlich bis zu monatlich)*

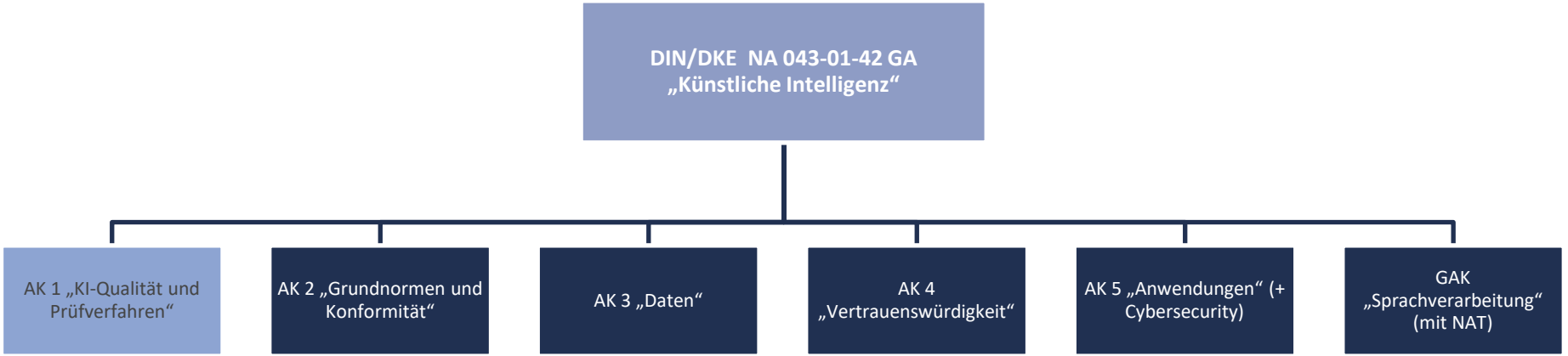
Struktur CEN/CENELEC JTC 21



Anmerkungen

- Working Groups im JTC 21 bilden i.d.R. “Task Groups” zur Bearbeitung einzelner Projekte
- WG 1 leistet selbst keine Standardisierungsarbeit

Struktur DIN/DKE Gemeinschaftsausschuss KI



Anmerkungen

- AK 1 ist nicht aktiv, Themen werden primär in den AKs 2 und 4 behandelt
- Struktur des GA folgt der Struktur des ISO/IEC Gremiums für KI, nicht der des JTC 21

→ Zuordnung von JTC 21 Projekten an die AKs wird von Fall zu Fall entschieden

JTC 21 Standardisierung aus deutscher Perspektive*

JTC 21 Projekt	JTC 21 WG	Spiegel-AK	Anmerkungen
Quality management system	WG 2	AK 2	Projekt unter initialer Abstimmung [Anleihen an ISO/IEC 42001 (AI MS) und ISO 13485 (Med. Devices QMS)]
Risk management	WG 2	AK 2	Erste Version erwartet für Ende des Jahres [Wird voraussichtlich in weiten teilen der ISO 14971 (RM für Med. Devices) folgen]
Conformity assessment	WG 2	AK 2	Projekt unter initialer Abstimmung [Inhalte zur Zeit noch unklar]
Trustworthiness framework	WG 4	AK 4	Übergreifendes Dokument zu allen Anforderungen des AI Acts [Sehr umfangreiches Dokument mit einer Vielzahl von Anforderungen]
Data quality Bias	WG 3	AK 3	Projekte unter initialer Abstimmung
Accuracy for NLP Accuracy für Computer Vision	WG 3	GAK NAT AK 5	Projekt in Zusammenarbeit mit ISO/IEC Gremium für KI Projekt unter initialer Abstimmung
Cybersecurity	WG 5	AK 5	Projekt unter initialer Abstimmung [Inhalte zur Zeit noch unklar, vermutlich starke Anleihen an ISO/IEC 27090]

*Liste der Projekte ist unvollständig und spiegelt im wesentlichen die augenblickliche Interessen deutsche Experten

Aufruf zur Mitarbeit

- Sparten-Diversität ist notwendig zur Erstellung von Europäischen Normen für den AI Act, die für alle akzeptierbar und mit vertretbaren Aufwand und Kosten implementierbar sind!
- Diskussion wir zur Zeit dominiert von:
  - Zivilgesellschaftlichen Organisationen
  - Universitäten/Forschungseinrichtungen
  - IT-Branche
  - Beraterfirmen
  - Medizingerätebranche
- Zeitrahmen für die Erstellung der Normen ist sehr eng gefasst!

- Wir benötigen die aktive Mitarbeit von Firmen aus anderen Branchen!
- Der DIN/DKA GA KI kann helfen, entsprechend eigener Interessen einen Einstieg in die europäische Standardisierung zu finden

Vielen Dank für Ihre Aufmerksamkeit!

Ihre Ansprechpartnerin:

Katharina Sehnert
Projektkoordinatorin

Katharina.Sehnert@din.de
+49 (0) 30 2601-2507

Ihr Ansprechpartner:

Peter Deussen
Obmann DIN/DKE NA 043-01-42 GA

Peter.Deussen@microsoft.com
+49 (0) 151 4406 3650

Ihre Mitarbeit zählt !

Ihre Ansprechpartnerin:

Dr. Claudia Reinel
Projektmanagerin Strategische Entwicklung Künstliche Intelligenz

Kuenstliche.Intelligenz@din.de
+49 (0) 30 2601-2115

Ihre Ansprechpartnerin:

Katharina Sehnert
Projektkoordinatorin

Katharina.Sehnert@din.de
+49 (0) 30 2601-2507