EU Cybersecurity Act

IT-Sicherheitszertifizierung in Europa

Jan-Peter Kleinhans
Projektleiter IT-Sicherheit im Internet der Dinge
jkleinhans@stiftung-nv.de

Stiftung
Neue
Verantwortung

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung

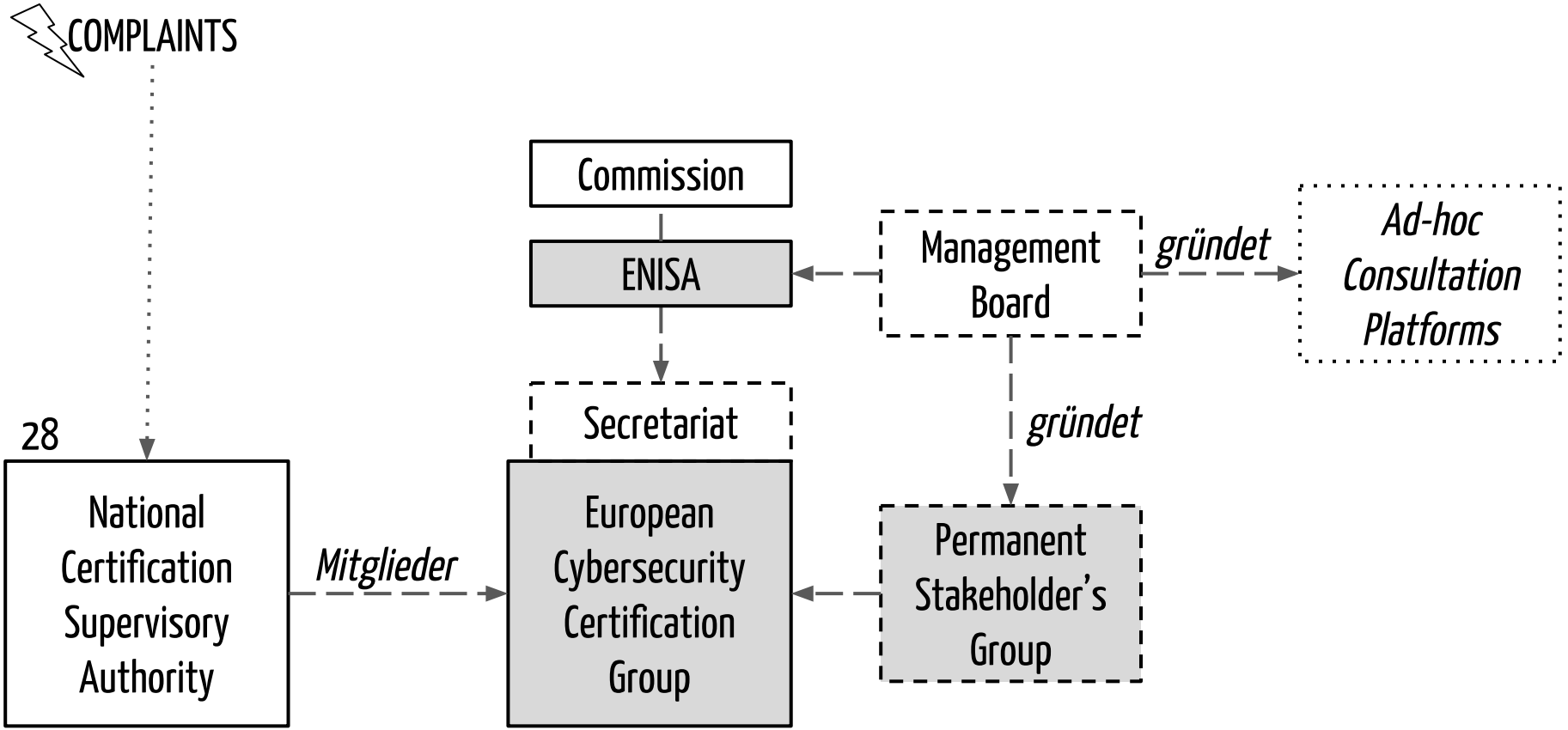
- Increasing the overall **transparency of cybersecurity assurance**[8] of ICT products and services to strengthen trust in the digital single market and in digital innovation; and
- Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across Member States and sectors.

Building on the above developments, the proposed Regulation establishes a European Cybersecurity Certification Framework (the "**Framework**") for ICT products and services and specifies the essential functions and tasks of ENISA in the field of cybersecurity certification. The present proposal lays down an overall framework of rules governing European cybersecurity certification schemes. The proposal does not introduce directly operational certification schemes, but rather create a system (framework) for the establishment of specific certification schemes for specific ICT products/services (the "European cybersecurity certification schemes"). The creation of European cybersecurity certification schemes in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.

Vorgeschlagene **Governance-Struktur** des European Cybersecurity Certification Frameworks

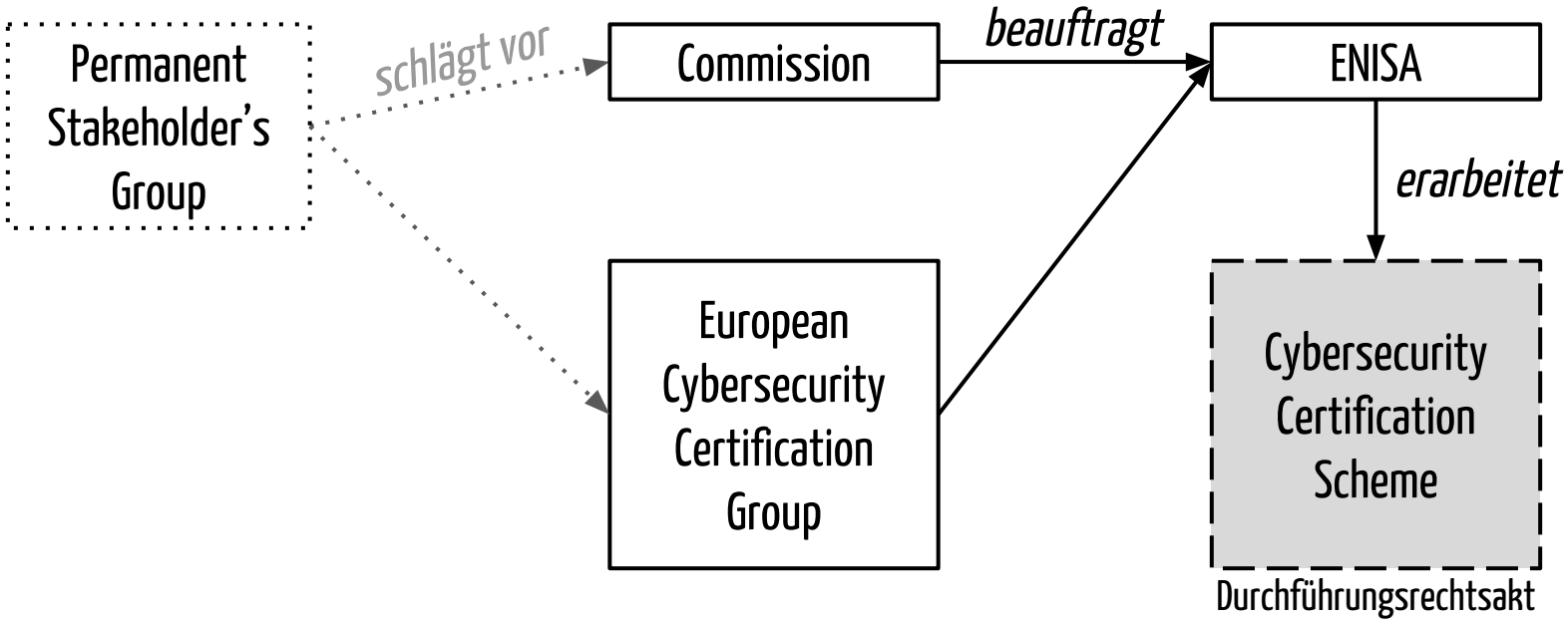
Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung

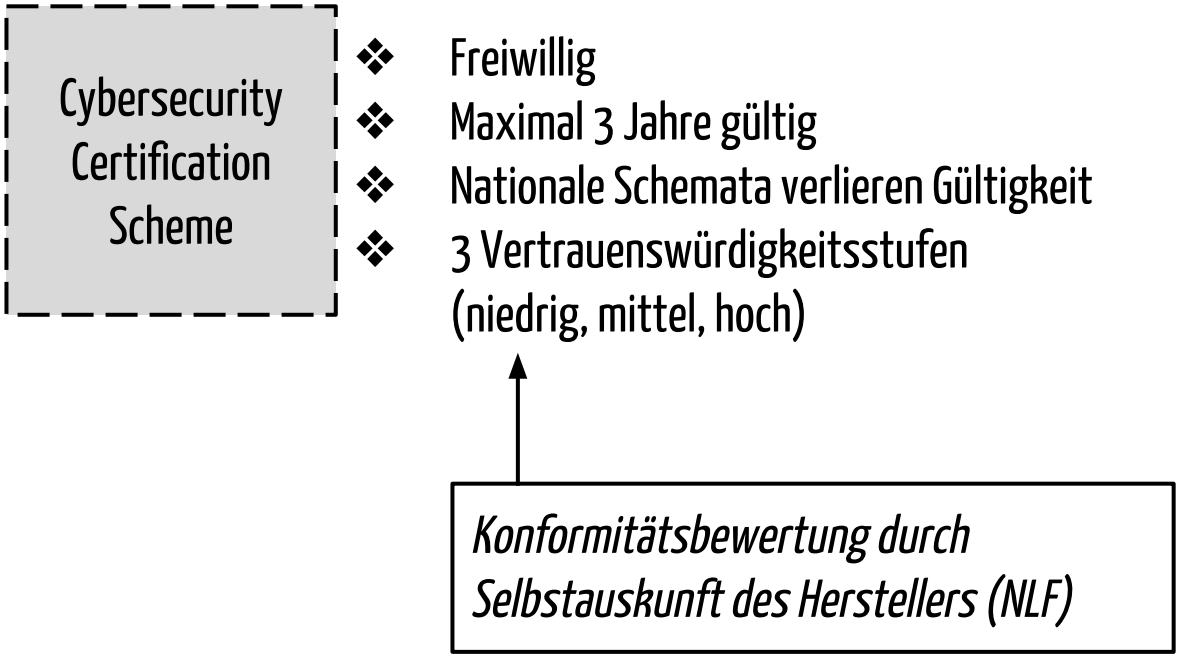


Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung



Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans



Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Alles super?

Natürlich nicht.

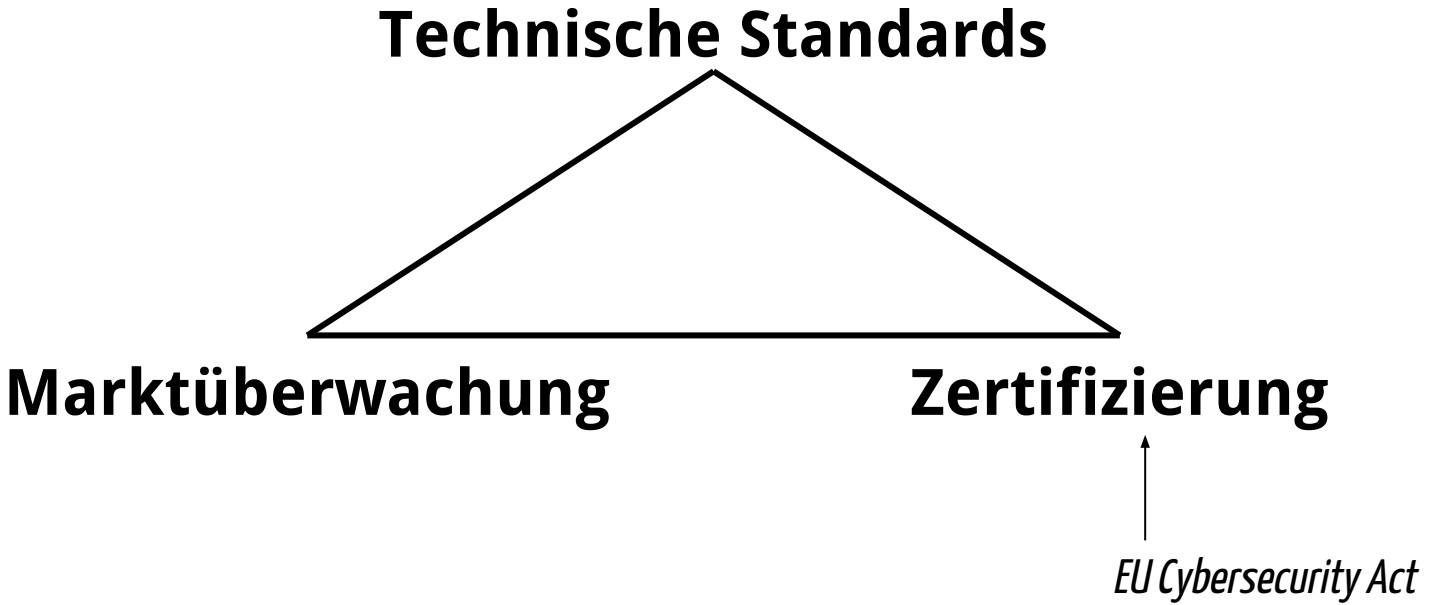
Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung

IT-Sicherheit ist Fleißarbeit.

Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung
Neue
Verantwortung



Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung

Marktüberwachung ist besonders wichtig bei IT-Sicherheit, da Zertifizierung immer nur eine Momentaufnahme sein kann.

Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung

Marktüberwachung ist Informationsproblem.

Marktüberwachung muss daher stärker in Informationsflüssen gedacht werden!

Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung

Unabhängige Dritte (Sicherheitsforscher:innen, Hacker:innen, etc.)

Verbraucher:innen

Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung

Idee einer **Produktdatenbank** in EU 2017/1369 (Energieverbrauchskennzeichnung)

(29) Um ein nützliches Instrument für die Verbraucher einzurichten, Händlern die Möglichkeit zu geben, Produktdatenblätter auf alternativen Wegen zu erhalten, und die Einhaltung der Vorschriften leichter überwachen und aktuelle Marktdaten für den Rechtsetzungsprozess zur Überarbeitung produktspezifischer Etiketten und Datenblätter bereitstellen zu können, sollte die Kommission eine über ein Online-Portal zugängliche Produktdatenbank einrichten und pflegen, die aus einem öffentlich zugänglichen Teil und einem Konformitätsteil besteht.

(30) Unbeschadet der Marktüberwachungspflichten der Mitgliedstaaten und der Pflicht der Lieferanten zur Überprüfung der Produktkonformität sollten die Lieferanten die erforderlichen Informationen über die Konformität ihrer Produkte elektronisch in der Produktdatenbank zur Verfügung stellen. Die für Verbraucher und Händler relevanten Informationen sollten im öffentlichen Teil der Produktdatenbank öffentlich zugänglich gemacht werden. Diese Informationen sollten als offene Daten zur Verfügung gestellt werden, damit die Entwickler von mobilen Anwendungen und anderen Vergleichsinstrumenten sie nutzen können. Durch nutzerorientierte Instrumente, etwa einen dynamischen Quick-Response-Code (QR-Code) auf dem gedruckten Etikett, sollte ein einfacher Direktzugang zum öffentlichen Teil der Produktdatenbank ermöglicht werden.

Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung

Alle suchen nach Strukturen, um Marktüberwachung an unsere digitale Realität anzupassen. *(siehe zB DSGVO Art 43)*

c) Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzzertifizierung sowie der Datenschutzsiegel und -prüfzeichen festgelegt haben;

d) Verfahren und Strukturen festgelegt haben, mit denen sie Beschwerden über Verletzungen der Zertifizierung oder die Art und Weise, in der die Zertifizierung von dem Verantwortlichen oder dem Auftragsverarbeiter umgesetzt wird oder wurde, nachgehen und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent machen, und

Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Marktüberwachung ist Fleißarbeit und daher die **Achillessehne** vieler Regulierungsinitiativen. Wenn Datenschutz und Datensicherheit **im EU Binnenmarkt substantiell gestärkt** werden sollen, müssen wir **skalierbare Prozesse und Strukturen** der Marktüberwachung entwerfen!

Jan-Peter Kleinhans | jkleinhans@stiftung-nv.de | Twitter: @JPKleinhans

Stiftung Neue Verantwortung