Dr. Jochen Friedrich – Technical Relations Executive
jochen@de.ibm.com

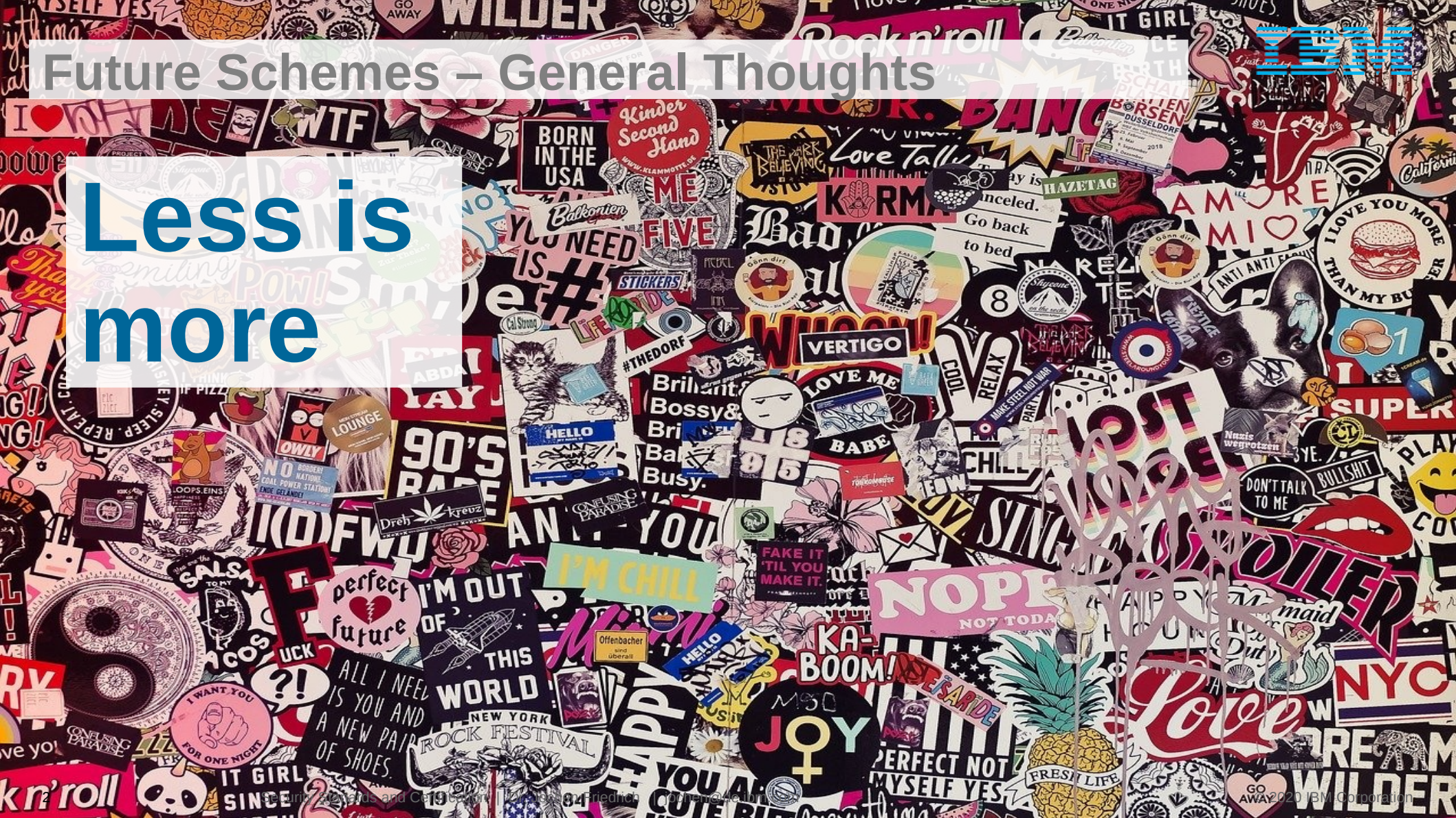
# Security Standards and Certification

#trust
#state-of-the-art
#serving_the_market

**Standardisation and the Cybersecurity Act – what's up?**
**3 February 2020**



# Future Schemes – General Thoughts



# Future Schemes – General Thoughts

**Less is more**

**Key objective as given in the EUCA (Recital 65):**
**”Increasing trust and security in ICT products, services and processes”**

**Focussed activity in certification will help to meet the objective.**

**Balanced approach.**


Security Stanards and Certification | Dr. Jochen Friedrich | jochen@de.ibm.com

# Why to focus on standards

| | |
|---|---|
| **Quality** | Standards reflect the state of the art of technology<br>Key global experts from academia and industry contribute |
| **Innovation** | Standards are maintained and regularly updated<br>Ongoing responsibility of experts and new experts joining |
| **Global relevance** | Standards include requirements from stakeholders – including governments – from all over the world |
| **Trans-parency** | Standards are available for everyone<br>Industry can plan their work according to standards<br>Processes for regularly adding functionality<br>In Europe: Annex III organisations involved throughout process |

# Early planning for standards


# EU Rolling Plan for ICT Standardisation

Requirements for standardisation and proposals for new standards developments

Updated on annual level

Global attention and impact

Chapter 3.1.5: Cybersecurity

! Find ways how to link EU Multi-Stakeholder Platform on ICT Standardisation and Rolling Plan closely with EUCA activities

**ACTION 2** SDOs to assess existing standards required to support the European Cybersecurity Certification Framework to ensure that standards are available for providing the core of any certification activity. In particular, SDOs are encouraged to work on standards related to the specification and assessment of security properties in ICT products and services as well as those related to security in processes related to the design, development, delivery and maintenance of an ICT product or service.

# Charter of Trust

Security by Default

Risk-based approach

Covering full supply chain

17 Baseline Requirements

Mapping to International Standards

| Category | Baseline Cybersecurity Supply Chain Requirements |
|---|---|
| Data Protection | Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data |
| | Data shall be protected from unauthorized access throughout the data lifecycle |
| | The design of products and services shall incorporate security as well as privacy where applicable |
| Security Policies | Security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443 shall be in effect |
| | Guidelines on secure configuration, operation and usage of products or services shall be available to customers |
| | Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services. |
| Incident Response | For confirmed incidents, timely security incident response for products and services shall be provided to customers |
| Site Security | Measures to prevent unauthorized physical access throughout sites shall be in place |
| Access, Intervention, Transfer & Separation | Encryption and key management mechanisms shall be available, when appropriate, to protect data |
| | Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced |
| Integrity and Availability | Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed |
| | Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments |
| | Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicable |
| | A process shall be in place to ensure that products and services are authentic and identifiable |
| Support | The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available |
| | Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support |
| Training | A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness) |



Security Stanards and Certification | Dr. Jochen Friedrich | jochen@de.ibm.com