Security Conference

How to reconciliate international standards and regional policy making on cybersecurity?

Presented by:

Eloïse RYON, Senior manager
Europe Digital Policy

Gabriel Faifman, Director Product
Security Standards & Governance

Monday 16th of October 2023

Internal

Agenda

1. Schneider Electric: who are we ?
2. Regionalization of cybersecurity policy trend
    - *Focus on cybersecurity policy in Europe, US & Asia.*
        - *Use case: Cyber resilience act (EU)*
    - *Role of international organization*
    - *US IOT labelling scheme: how to reconciliate regional policies and international standards.*
3. International standards
    - *How to optimize international standards in the regionalization of cybersecurity policies.*
        - *Composition/similarity and reusability of evidence and/or certification*
        - *Avoid multiple certification : bottlenecks in conformity assessment bodies, delays to entry to market & costs*
        - *Enables companies to be more competitive on the global market*
4. Key take aways

Internal


Schneider Electric
Who are we ?

Schneider Electric provides energy and automation digital solutions for efficiency and sustainability

Key figures for 2022

5% of revenues devoted to R&D

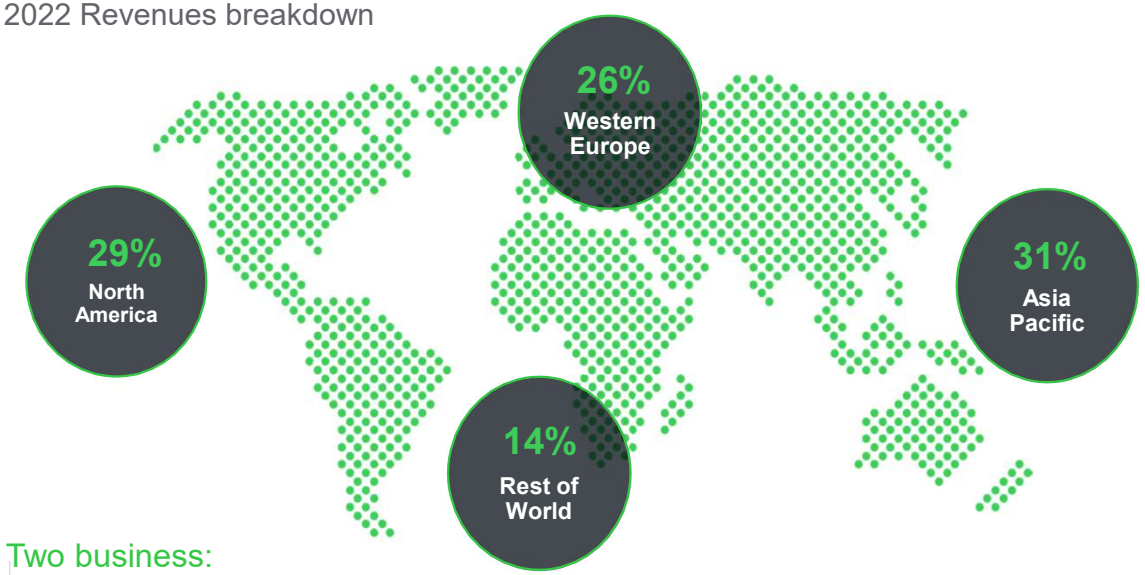
€34,1 billion
2022 revenues

43%
of revenues in new economies

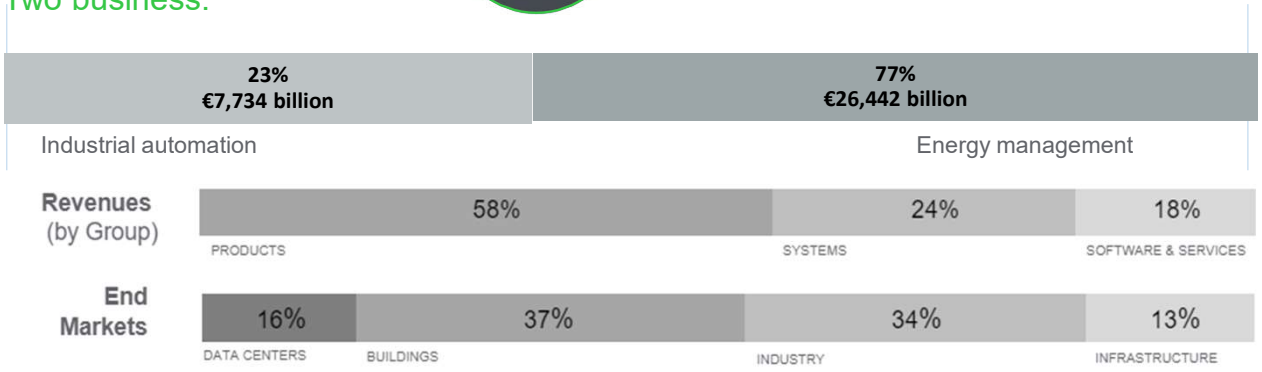
128,000+
Employees in over 100 countries

A well-balanced global presence

2022 Revenues breakdown



Two business:



How we scale cyber at the level of the company?

Cybersecurity & Product Security,
reporting to Governance

Thought Leadership & Trust

Governance & Technology

- Strategy & Governance
- Technology & Innovation
- Training & Awareness
- Digital Policy & Standards

Strategic initiatives

- Installed Base Security
- Supply Chain Security

Defense & Exposure Management

- Cyber Defense
- Vulnerability Management

Regional CISOs

- Europe, Middle-East & Africa
- Asia & Pacific
- Americas
- China

Product, Service, Software and Digital security

- Product Security EM
- Product Security IA
- EcoStruxure Platform Security
- Digital Offers Security
- Customer Experience
- Front Offices Security
- Industrial Security
- Projects, Services Operations
- Finance Operations Risk
- HR Operations Risk
- Engineering Security
- Source Code Security
- Data Security
- Artificial Intelligence Risk
- IT Security
- Digital Certification
- Prosumers

Indirect reports

Direct reports

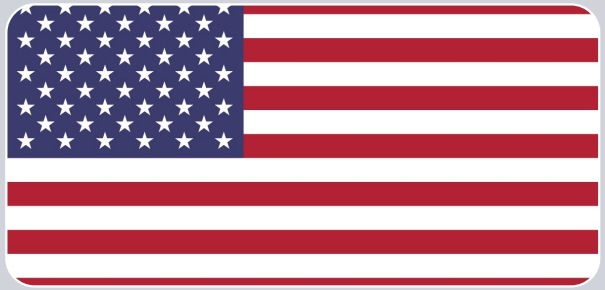
Regionalization of cybersecurity policy

A key trend for global companies

“**Fragmentation** is a natural **inhibitor** for **adoption**”

Regionalization of cybersecurity policies: a key trend.

As cybersecurity threats hightens, more and more nations are providing for their own security



US

- US California Connected Device Law
- IOT Cybersecurity Improvement Act
  - NIST Mandate
- Executive Order 14028 Improving the Nation's Cybersecurity
- US Cyber Trust Mark voluntary consumer IoT label

Europe

- NIS 2 directive
- Cyber Resilience Act
- Cybersecurity Certification Schemes
  - Cloud providers (EUCS)

Limited reference to international standards

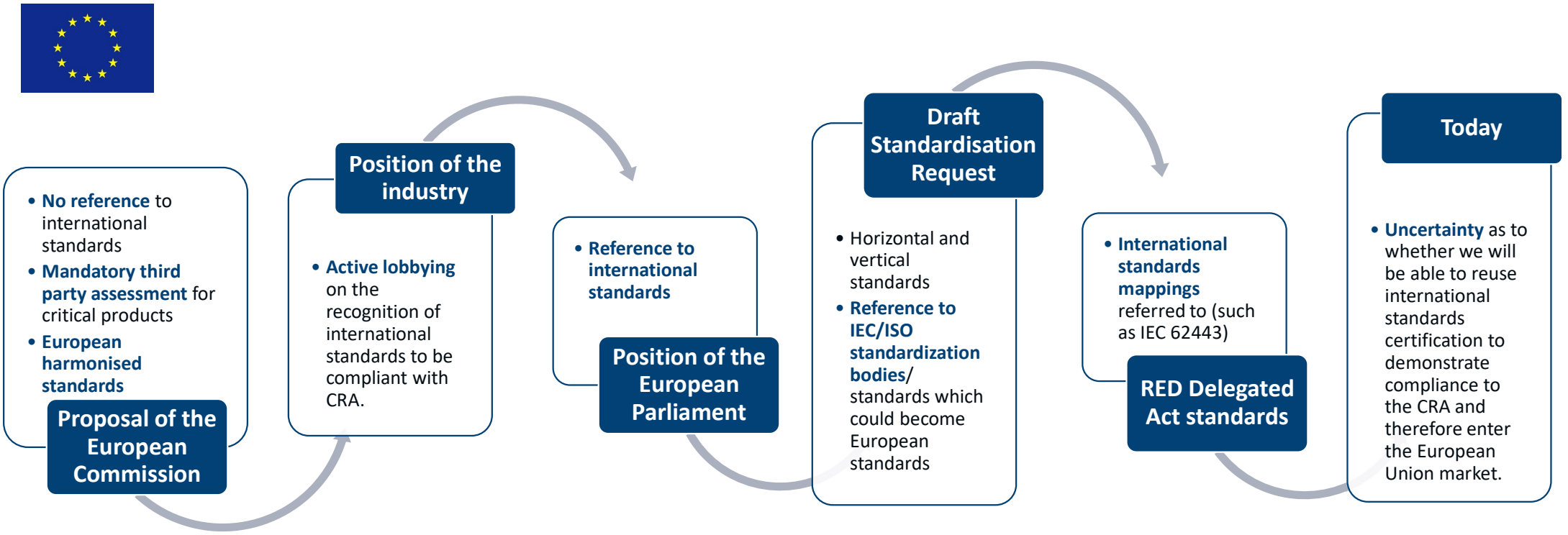
Asia

- Singapore
  - Cybersecurity Code of Practice (current version is CCoP 2.0), issued pursuant to the Cybersecurity Act 2018
- Australia
  - Critical Infrastructure Risk Management Program Rules (CIRMP Rules)
    - in line with international standards like the various ISO/IEC standards

Internal

Focus on the Cyber Resilience Act.

A regional cybersecurity policy dismissing international standards



Internal

Bringing back the cybersecurity discussion in the global arena.

Putting cybersecurity back on top of the agenda of international organizations.

G7 2023 HIROSHIMA SUMMIT

WORLD ECONOMIC FORUM

OECD

International standards on cybersecurity

How can they support regional regulations ?

International standards in regional cybersecurity policy: key for efficient implementation.

1. Crucial to ensure **global competitiveness and innovation** of industries.
2. To **avoid Notified Bodies bottlenecks and delays** to enter the regional market.
3. To **harmonize requirements** and **enable mutual recognition agreements** for cybersecurity.
4. To **avoid leaving small and medium entreprises behind** (and therefore sever innovation).
5. To **mitigate the costs of compliance** and therefore the costs of products.

Internal

Focus on the role of international standards in the CRA (EU)

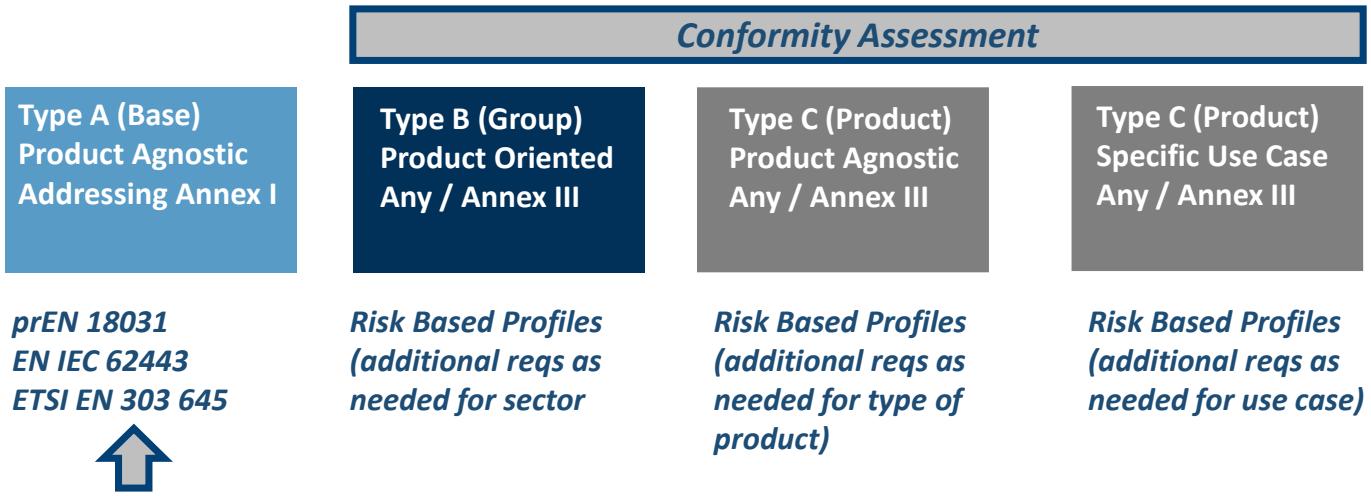
International Standards as a solution to match the ambitious timeline and the scope of the CRA.

→ **Reuse existing** mature international **standards**.

→ **Reuse confomity assessments**, **certifications** and **evidences**.

→ **Role of CEN-CENELEC** to base harmonized standards on international standards.

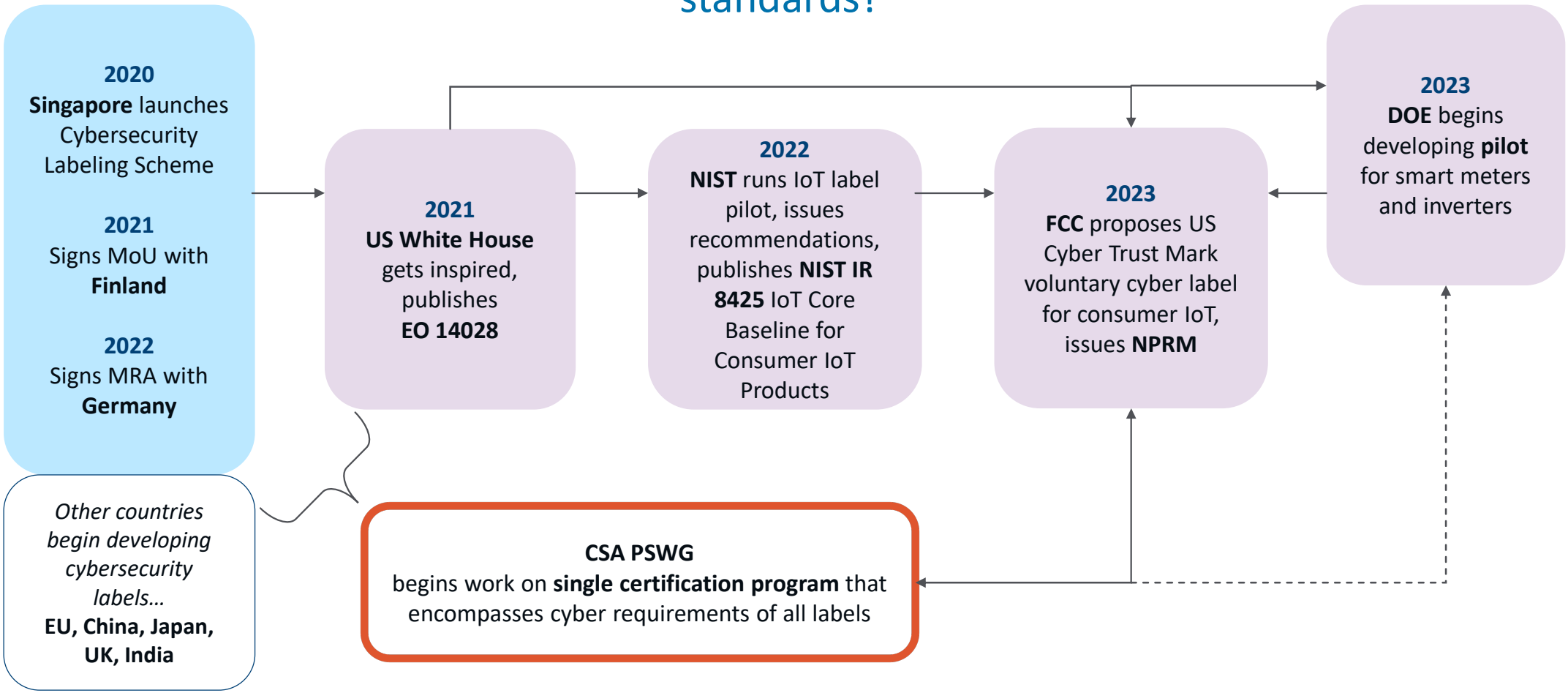
→ Have a mapping referred to directly in the harmonized standard.



Steps to get from a threat modelling and context (e.g.: considering the sectorial risk assessment and security environment) towards the selection of the security measures (type A):
" In particular, wherever relevant, the standards developed under this section should include specifications on secure software development".

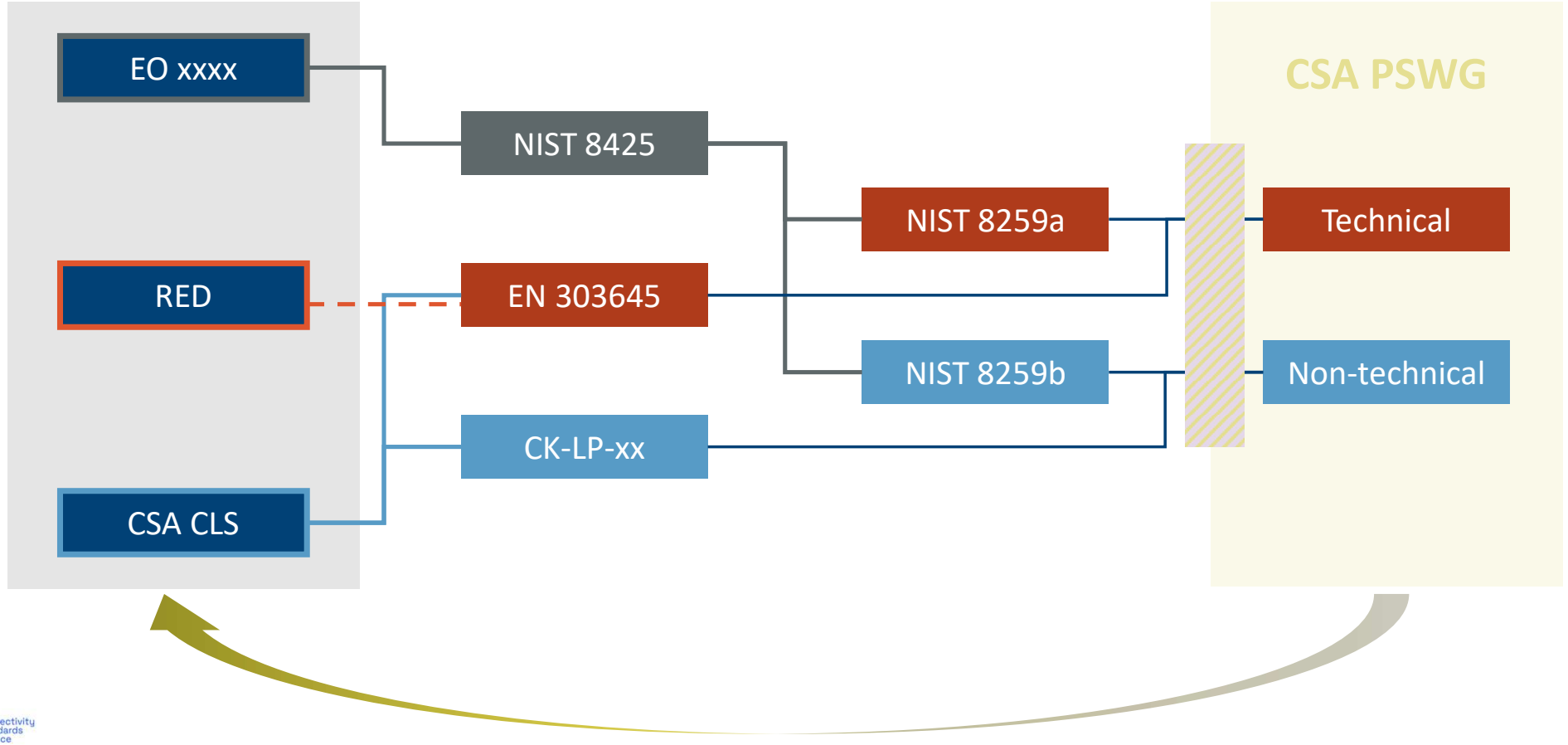
Internal

Focus on US IoT Label: how to reconciliate regional policy and international standards?



Internal

Baseline

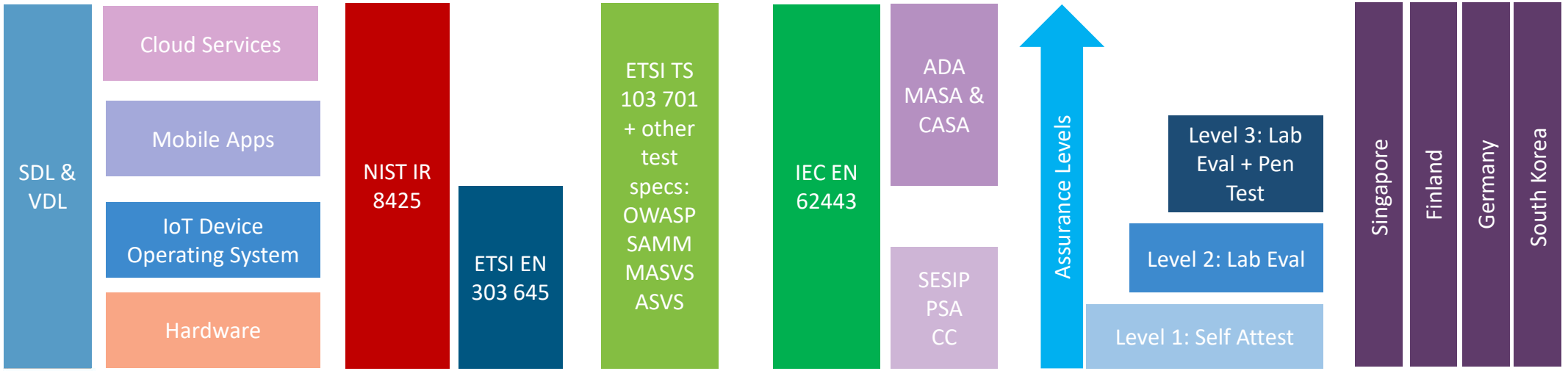


Connectivity Standards Alliance © 2023

CSA – PSWG Scheme Composition & Inheritance

Optimizing the use of existing international standards and certification programs

PSWG Target of Evaluation ⇨ **Baseline Standards** ⇨ **PSWG Test Specs** ⇨ **Conformance & Composition Recognition** ⇨ **Assurance Levels** ⇨ **Mutual Recognition**



Internal

Conclusion

Regionalization of cybersecurity policy should go hand in hand with international standards.

The recognition of international standards by regional cybersecurity policy will strengthen cybersecurity overall.