

# / Cyber Resilience Act

A game changer for the IoT Market

AVNET<sup>®</sup> SILICA

Romain Tesnière – BDM EMEA Solution Sales



# / Some definitions

**Standard:** international consensus of experts about how to do something.

Standard are produced by public/non-profit organizations (ETSI, NIST, ANSI, IETF, OWASP, ...) or private (ISO).

Compliance to a standard is **voluntary**, unless mandated by market or contractual requirements.

**Regulation:** rules made by an authority in order to control the way something is done, or the way people behave.

In the context of EU,  
- a Regulation applies across EU states,  
- a Directive is declined by countries' laws.

Compliance to a regulation is **mandatory**

# Example of (European) regulations

## GDPR : General Data Protection Regulation

<https://eur-lex.europa.eu/eli/reg/2016/679/oj>

- Aims to protect EU citizen personal data. (in application since 2018)
- Not limited to cybersecurity, but obligation to protect the data that has been collected.

## RED : Radio Equipment Directive

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0053>

- Regulatory framework for placing radio equipment on the market (2014 -> 2022)
- High-level cybersecurity requirements added in 2019 in Article 3: 3.(d), 3.(e), 3.(f)

## NIS2 : Network Information and Systems Directive

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555>

- First EU-wide cybersecurity regulation
- Applies to Digital Service Providers and Operators of Essential Services.
- Imposes requirements to prevent security incidents, makes their reporting mandatory.

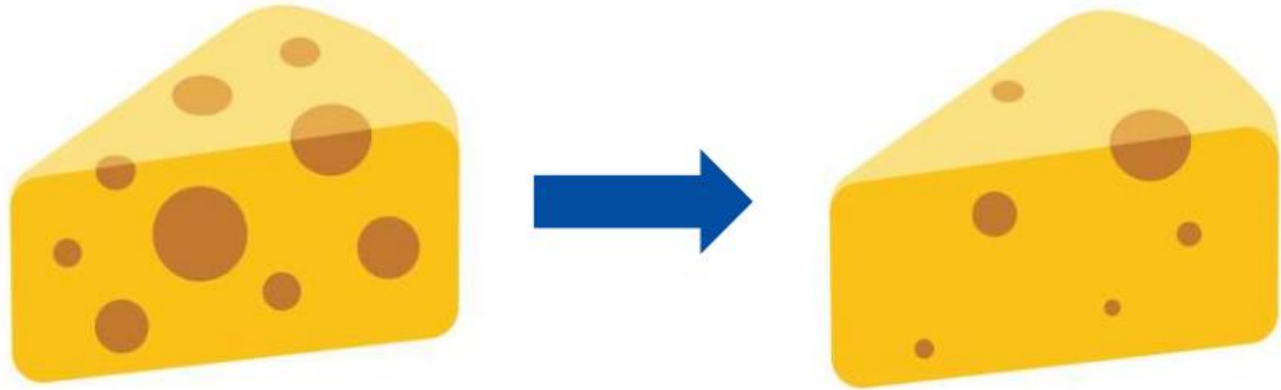
## CRA : Cyber Resilience Act

<https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

- Targets all products with a digital element
- Software AND hardware
- Broader scope than RED, stronger cybersecurity requirements.

# What is the CRA?

# CRA in a nutshell



**“Products with digital elements shall be delivered without any known exploitable vulnerabilities”**

# / What is the CRA?

- It's a legal framework
- It will
  - Ensure that products with digital elements placed on EU market have fewer vulnerabilities
  - Ensure that manufacturers remain responsible for cybersecurity
  - Improve transparency
  - Improve customer and business protection
- It defines
  - harmonized rules for **the placing on the market** of hardware and software product
  - essential cybersecurity requirements for the design and development (Annex I)
  - rules for the duty of care for the whole life cycle (Annex II)

<https://data.europa.eu/eli/reg/2024/2847/oj>

**Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)**

# Some definitions (as per the Blue Guide)

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC>

## 2.2. Making available on the market

- A product is made available on the market when supplied for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.
- The concept of making available refers to each individual product.

## 2.3. Placing on the market

- A product is placed on the market when it is **made available** for the first time on the Union market. According to Union harmonisation legislation, each individual product can only be placed once on the Union market.
- Products made available on the market must comply with the applicable Union harmonisation legislation at the moment of placing on the market.

# / Products classification

- **Critical Products** **Very High Risk & Very High Impact products**
- **Important Products**
  - Class II **High Risk & High Impact products**
  - Class I **Medium Risk & Medium Impact products**
- **Not listed (default)** **Products that do not have a core security function**

**It's NOT about the components your products is made of, it's about what are the use cases of your product: a TPM is critical, still a product containing a TPM might be of a lower class, even default**

# Categories Technical Description as per EU/2025/2392

[https://eur-lex.europa.eu/eli/reg\\_impl/2025/2392/oj/eng](https://eur-lex.europa.eu/eli/reg_impl/2025/2392/oj/eng)

## Critical Products

- Hardware Devices with Security Boxes
- Smart meter gateways and other devices for advanced security purposes
- Smartcards or similar devices, including secure elements

## Important Products of class II

- Hypervisors and container runtime systems
- Firewalls, intrusion detection and prevention systems
- Tamper-resistant MCUs and MPUs

## Important Products of class I

- Identity and privileged access management systems
- Standalone and embedded browsers
- Password managers
- Software that searches/removes/quarantines malicious software
- VPN
- Network management systems
- Security information and event management (SIEM) systems
- Boot managers
- Public key infrastructure and digital certificate issuance software
- Physical and virtual network interfaces
- Operating systems
- Routers, modems intended and switches
- MCUs, MPUs, ASICs, FPGAs with security-related functionalities
- Smart home general purpose virtual assistants
- Smart home products with security (locks, cameras, baby monitors, alarms)
- Internet connected toys with social features or location tracking
- Personal wearable products for health tracking or for children

# Conformity Assessment Procedures (as per 768/2008/EC)

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008D0768>

## Module A: Internal production control

- No notified body required
- Manufacturer makes self assessment based on technical documentation & tests reports

## Module B: EC-type examination

- Notified body is required
- Manufacturer provides technical documentation and test specimens
- Notified body checks the technical documentation and performs tests

## Module C: Conformity to type based on internal production control

- Based on Module B and individual product
- No notified body required
- Manufacturer makes self assessment based on technical documentation & tests reports

## Module H: Conformity based on full quality assurance

- Notified body required
- Manufacturer provides process documentation about the whole product life cycle (design, prod, VM, maintenance)
- Notified body checks the process and performs audits

# / Different assessments for each category

- **Whatever the class, requirements are the same, the conformity assessment procedure differs**
- **Default** → Self assessment is enough (use module A)
- **Class I** → Compliance to a harmonised standard (module A) or Third-party assessment (module B+C or module H)
- **Class II** → Third-Party assessment (module B+C or module H)
- **Critical** → European CC-based cybersecurity certification scheme (EUCC) or Third-Party assessment of level Substantial or Higher if no EUCC
- **FOSS** → If free, not covered otherwise Self assessment is enough (Module A)  
(Free & Open Source Software)

***Check recital (91)***

# / Regulations & Harmonised standards

Harmonised standard: defined in 1025/2012 Article 2, point (1)(c)

<https://eur-lex.europa.eu/eli/reg/2012/1025/oj>

As per [https://europa.eu/youreurope/business/product-requirements/compliance/conformity-assessment/index\\_en.htm](https://europa.eu/youreurope/business/product-requirements/compliance/conformity-assessment/index_en.htm) :

Harmonised standards, where they exist, can help you demonstrate compliance with EU rules.

## What are harmonised standards?

**Harmonised standards** are developed by recognised European Standards Organisations: [CEN](#), [CENELEC](#), or [ETSI](#). Following harmonised standards in the design and manufacture of your products will ensure your products are in line with corresponding EU rules; this is known as 'presumption of conformity'.

## Do you have to follow harmonised standards?

No, the use of harmonised standards remains **voluntary**. You are free to choose another technical solution to demonstrate compliance with the mandatory legal requirements.

# Are there Harmonised Standards for CRA ?

Harmonised standard: defined in 1025/2012 Article 2, point (1)(c)

<https://eur-lex.europa.eu/eli/req/2012/1025/oj>

EN18031 has been accepted (with restrictions) for the cybersecurity requirements of the RED directive (2014/53/EU)

[https://eur-lex.europa.eu/eli/dec\\_impl/2025/138/oj](https://eur-lex.europa.eu/eli/dec_impl/2025/138/oj)

Harmonised standards are work in progress:

1. On February 3<sup>rd</sup> the EU issued Mandate M/606 for CRA Harmonised Standards
2. On April 3<sup>rd</sup> “the Standardization Request for the Cyber Resilience Act (CRA) was officially accepted by CEN, CENELEC, and ETSI. In response to [Mandate M/606](#) from the European Commission, the three European Standardization Organizations have committed to delivering harmonized standards well in advance – at least one year before the CRA enters into application.”
3. Progress is publicly visible:

ETSI : <https://docbox.etsi.org/CYBER/EUSR/Open>

CEN/CENELEC : <https://www.stan4cra.eu/>



↓	sort by name/desc	sort by date/desc	sort by size/desc
<input type="checkbox"/>	EN-304-617_V0.0.6_2025-11-03_Browsers-2.pdf	2025-11-07 14:57	3438,3 KB
<input type="checkbox"/>	EN-304-618_v0.0.3_2025-09-29_Password_Managers.pdf	2025-10-01 12:46	1579,4 KB
<input type="checkbox"/>	EN-304-619_V0.0.12_2025-12_Antivirus-Antimalware_Mature-draft.pdf	2025-12-11 7:17	1626,3 KB
<input type="checkbox"/>	en-304-620-1_v0.0.13_2025-10-20.pdf	2025-10-22 13:24	810,4 KB
<input type="checkbox"/>	en-304-620-2_v0.0.9_2025-10-20.pdf	2025-10-22 13:24	803,4 KB
<input type="checkbox"/>	EN-304-621_v0.0.7_2025-10-22_Network_Management_Systems.pdf	2025-11-21 18:45	678,7 KB
<input type="checkbox"/>	EN-304-622_V0.0.4-2025-11-03_SIEM.pdf	2025-11-06 11:09	1082,7 KB
<input type="checkbox"/>	EN-304-623_V0.0.9_2025-11-20_Boot_Managers.pdf	2025-11-21 17:47	1119,7 KB
<input type="checkbox"/>	EN-304-624_v0.0.6-2025-12-02_PKI.pdf	2025-12-04 7:54	1649,3 KB
<input type="checkbox"/>	EN-304-625_V0.0.5-2025-09-22_Network_Interfaces.pdf	2025-10-01 10:49	1231,4 KB
<input type="checkbox"/>	EN-304-626_V0.0.6-2025-09-22_Operating_Systems.pdf	2025-10-01 10:52	1099,5 KB
<input type="checkbox"/>	EN-304-627_V0.0.11_2025-11-24_Routers-modems-switches_Mature-draft.pdf	2025-12-02 14:52	1197,9 KB
<input type="checkbox"/>	EN-304-635_V0.0.10_2025-12-09_Virtualisation-Container_Mature-draft.pdf	2025-12-09 17:17	2584,7 KB
<input type="checkbox"/>	EN-304-636_V0.0.6_2025-11-10_Firewalls.pdf	2025-11-10 12:54	1782,4 KB

# / What's in?



## Documentation

- Open VS closed source
- Risk assessments
- List of harmonized EU cybersecurity standards the product meets
- A SW and HW BoM
- Security breach awareness



## Device authentication

- One or two authentication
- TLS
- Certificates based
- Pre-shared keys (PSK)
- Token based



## Device Identity management

- Public Key Infrastructure
- Certificate revocation



## Device Access management

- Roles Based Access Control (RBAC)
- Azure Services
- AWS Services



## Data integrity

- Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification



## Data confidentiality

- Protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms;



## Upgrade mechanism

- Is a MUST to ensure security over product Lifecycle
- Protect the integrity (signature) and optionally the confidentiality (encryption) of the code being sent during firmware update

# 13 cybersecurity requirements (Annex I.1)

1. Be made available on the market without known exploitable vulnerabilities;
2. Be made available on the market with a secure by default configuration,
3. Ensure that vulnerabilities can be addressed through security updates,
4. Ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, as well as report on possible unauthorized access;
5. Protect the confidentiality of stored, transmitted or otherwise processed data
6. Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration
7. Process only data, personal or other, that are adequate, relevant and limited to what is necessary ('minimisation of data');
8. Protect the availability of essential and basic functions,
9. Minimize the negative impact by themselves or connected devices on the availability of services provided by other devices or networks;
10. Be designed, developed and produced to limit attack surfaces
11. Be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;
12. Provide security related information by recording and/or monitoring relevant internal activity
13. Provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure this is done in a secure manner.

# 8 vulnerability mngt requirements (Annex I.2) AVNET SILICA

1. Identify and document vulnerabilities and components contained in the product,
2. Address and remediate vulnerabilities without delay, including by providing security updates. Where technically feasible, new security updates shall be provided separately from functionality updates;
3. Apply effective and regular tests and reviews of the security of the product with digital elements;
4. Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities,
5. Put in place and enforce a policy on coordinated vulnerability disclosure (CVD);
6. Take measures to facilitate the sharing of information about potential vulnerabilities in their product;
7. Provide for mechanisms to securely distribute updates for products to ensure that vulnerabilities are fixed or mitigated in a timely manner, and, where applicable for security updates, in an automatic manner;
8. Ensure that available security updates are disseminated without delay and, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product, free of charge.

# / Covered or not by the CRA ?

- **Not covered**

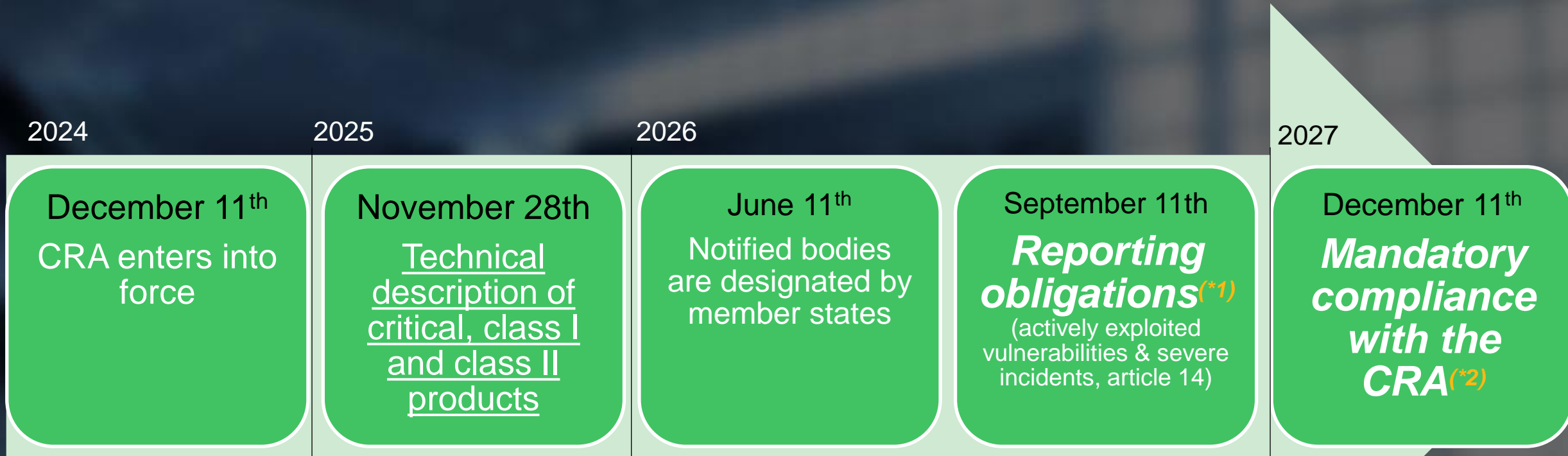
- Medical Devices (2017/746, 2017/745)
- National Security & Defense
- Automotive (2019/2144)
- Aviation (2018/1139)
- Marine (2014/90)
- Anything covered by the NIS2 Directive (2022/2555)
- Machinery-carrying vehicles

- **Covered**

- Machinery (as per 2023/1230)
- Anything explicitly excluded by the regulations in the « not covered » list

***Check Article 2 and Recital (53)***

# CRA timeline – It's now!



**(\*1) Reporting obligations are mandatory for ALL products**

**(\*2) Products placed on the market MUST comply with the CRA if substantially updated after December 11<sup>th</sup> 2027 (article 69 & paragraphs 38 to 42)**

# Questions?

- Is my product concerned ?  
(*trying to escape*)
  - YES, if that individual product was placed on the market after Dec 11<sup>th</sup> 2027
  - YES, if that individual product was placed on the market before Dec 11<sup>th</sup> 2027  
AND it has received a SUBSTANTIAL update after Dec 11<sup>th</sup> 2027  
(article 69)
- Are products built outside of EU concerned ?  
(*complaining about unfair competition*)
  - YES, any product has to comply when placed on the EU market
- Are non-connected products concerned ?
  - YES, any product with digital element placed on the EU market has to comply  
AND connected doesn't mean what you think (means connected to a system)
- How long is the reporting & monitoring & fixing obligation for CVE ?
  - The lifetime of the product, or at least five years  
(but **SHOULD** support more than five years is intended to be used for longer)  
(recital 60)

# Other regulations

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0053>

- Regulatory framework for placing radio equipment on the market (2014 -> 2022)
- High-level cybersecurity requirements added in 2019 in Article 3:
  - (d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
  - (e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
  - (f) radio equipment supports certain features ensuring protection from fraud;
- Delegated Act regarding application of these essential requirements  
[https://eur-lex.europa.eu/eli/reg\\_del/2022/30/oj](https://eur-lex.europa.eu/eli/reg_del/2022/30/oj)
- EN18031:2024 has been accepted as a harmonised standard for the RED directive  
[https://eur-lex.europa.eu/eli/dec\\_impl/2025/138/oj](https://eur-lex.europa.eu/eli/dec_impl/2025/138/oj)  
With restrictions:
  - Passwords are mandatory
  - Parental control is mandatory for toys
  - Security updates mechanisms in EN18031-3(financial):2024 are not sufficient

# CRA & RED: a common Security approach

## Radio Equipment Directive (RED)

Objective: Essential requirement for radio equipment

- EMC, Safety/health, privacy & fraud protection
- Update mechanism for patching
- Conformity assessment with risk-based approach according to the usage and environment of the device.
  - HW Component : N/A
  - IoT Consumer & Industrial Device : Self-Declaration
  - Medical & Auto devices excluded

## Cyber Resilience Act (CRA)

Objective: Ensure Security over HW & SW products

- Monitor vulnerabilities
- Update mechanism for patching
- Documentation (HW & SW, assessments)



# / US Cyber Trust Mark

<https://www.fcc.gov/CyberTrustMark>

- **This is a voluntary program (not a regulation)**
- Scope:
  - The program applies to consumer wireless IoT products
  - Excluded from the program:
    - Medical devices regulated by the Food and Drug Administration
    - Motor vehicles and equipment regulated by the National Highway Traffic Safety Administration
    - Wired devices
    - Products primarily used for manufacturing, industrial control or enterprise applications
    - Equipment on the FCC's Covered List and equipment produced by an entity on the covered list
    - IoT products from a company on other lists addressing national security
    - IoT products produced by entities banned from Federal procurement

What are the next steps ?

# / How to prepare and comply

- Read the CRA <https://data.europa.eu/eli/reg/2024/2847/oj>
- Identify your products classes & your compliance strategy
- Assess your security documentation level
- Perform a risk assessment & threat analysis
- Identify the proper security measures
- Define & setup your vulnerability posture (disclosure, resolution, ...)
- Pick the appropriate software bill of material
- Pick the appropriate hardware bill of material
- Define your production strategy (including the provisioning aspects)

# / AVNET Silica Value Proposition

- Read the CRA <https://data.europa.eu/eli/reg/2024/2847/oj>
- Identify your products classes & your compliance strategy
- Assess your security documentation level
- Perform a risk assessment & threat analysis
- Identify the proper security measures
- Define & setup your vulnerability posture (disclosure, resolution, ...)
- Pick the appropriate software bill of material
- Pick the appropriate hardware bill of material
- Define your production strategy (including the provisioning aspects)



# Why **SECURE** **PROVISIONING** **SERVICES?**

# Secure Provisioning is required for many use cases

Every application that wants to comply with one or several of these use cases will require specific customisation (certificates & keys)



**AWS Connection**

**Azure Connection**

**IoTConnect**



**IP Protection**

**Secure boot**

**Secure Firmware upgrade  
over the air**



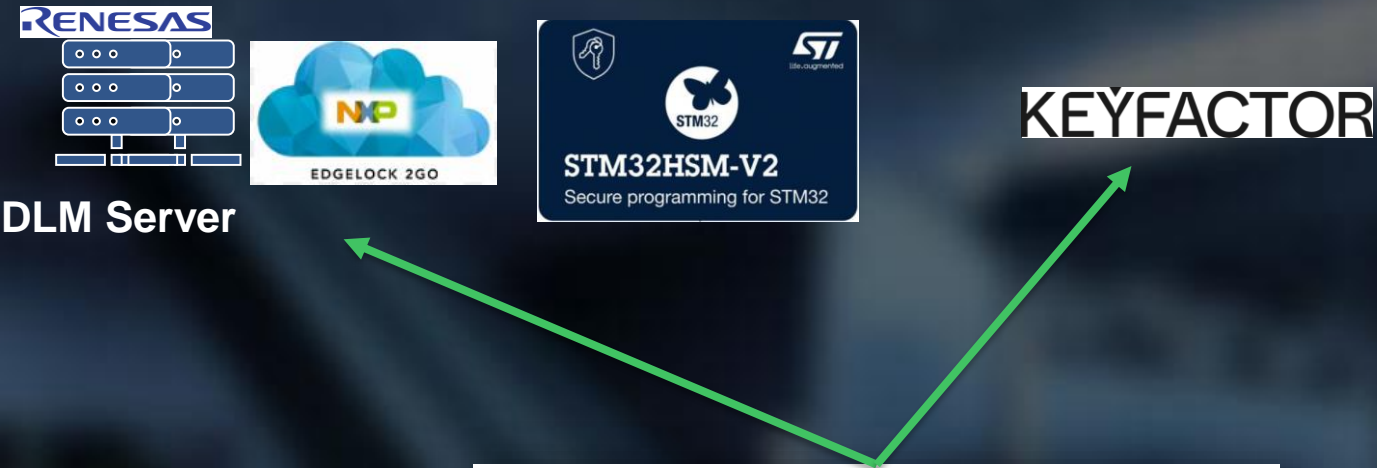
**EV Charging**

**Wireless Charging (Qi)**

**Matter**

Secure provisioning is a big part of a proper Security architecture, and it should be taken into consideration as well as security countermeasure

# Avnet Silica Warehouse



## • Pros

- Full control on what and how the provisioning is done
- Locks the device during transportation
- Locks the device, then EMS just need to load FW
- One-Stop-Shop (components + Services)

## • Cons

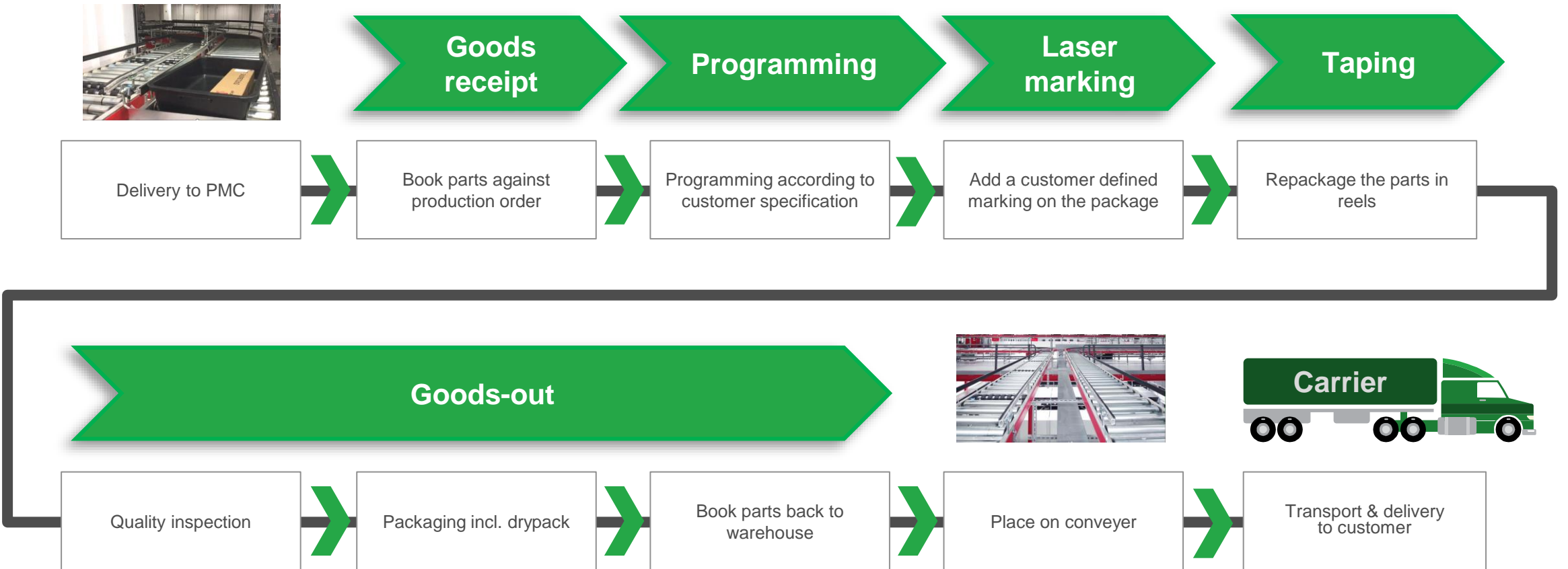
- Requires customization content to be ready when shipping components

# Product Modification Center

AVNET SILICA



# / PMC process flow



# / Programming

Program parts according to customer specification with customer software.



# SECURITY OFFER

From product to services



## 1. Secure Elements

Full range of companion chips for authentication, cryptographic tasks, keys/certificates storage coming from STMicro, Microchip and NXP.



## 2. Secure MCUs & MPUs

Processing units embedding security features from STMicro, NXP, Renesas, Nordic, Ublox, Tria...



## 3. Secure Provisioning services

Keys, certificates, bootloader, FW injection into MCU, SoM, modules in a secure manner

PKI  
Managed  
Services

## 4. Public Key Infrastructure (PKI)

Keys, certificates management over product lifecycle. FW signing, FW updates

An aerial photograph of a mountain range. The foreground and middle ground are dominated by a thick, white sea of clouds that fills the valleys and lower slopes of the mountains. The mountain peaks and ridges are visible above the clouds, appearing in shades of blue and grey. The sky is a pale, clear blue, suggesting a bright, sunny day. The overall scene is serene and majestic.

/ Q&A

**AVNET<sup>®</sup> SILICA**