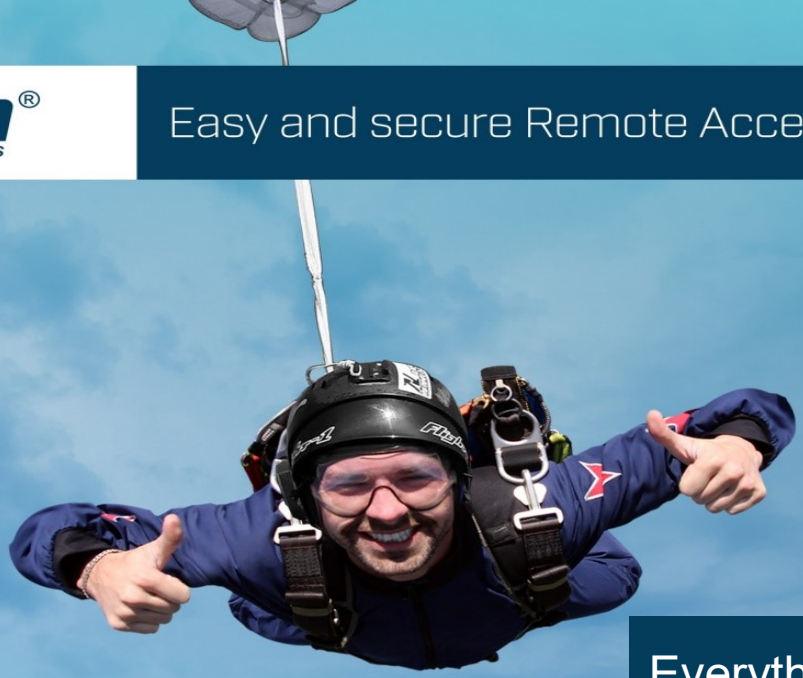
Ewon® BY HMS NETWORKS

Easy and secure Remote Access to your machines

Ewon 20 years Connected!



Everything about Cosy+ security

Deep dive in Security on Hardware

April 2021
TLP:
Classification: Internal

HMS

Jean-David Epaillard

Information Security & Technology Manager
jdep@hms-networks.com

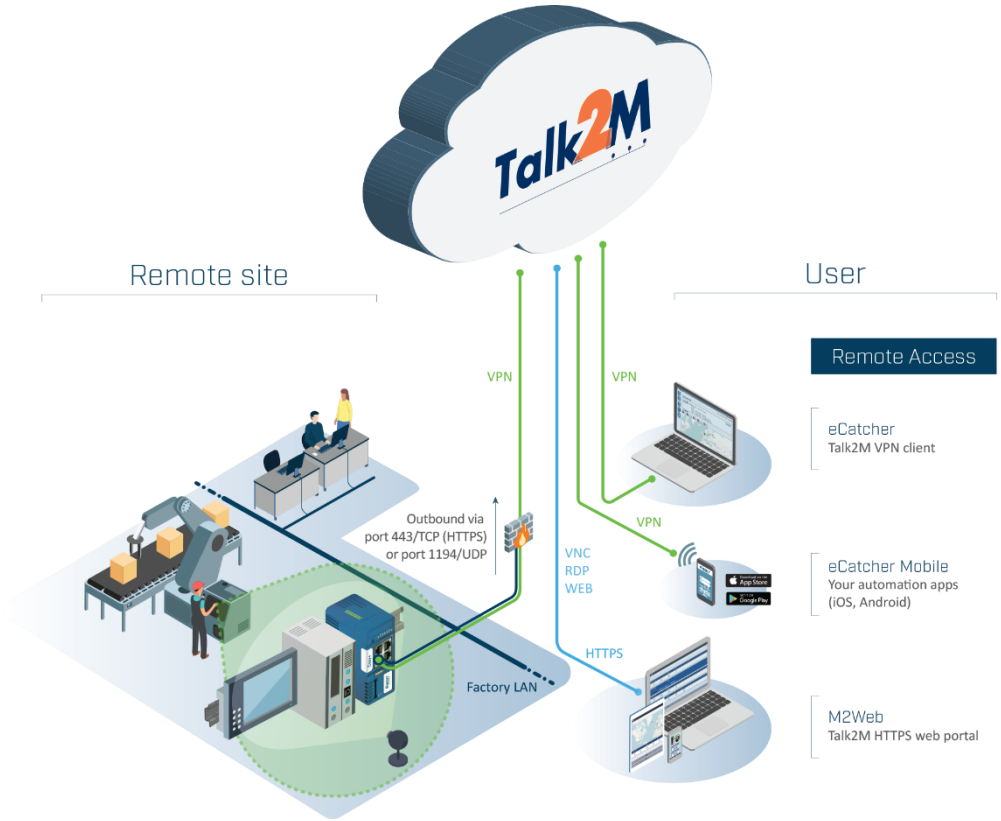
ISO 27001 INFORMATION SECURITY MANAGEMENT
CERTIFIED BY VINÇOTTE

Certified Security

nviso
Testing Partner

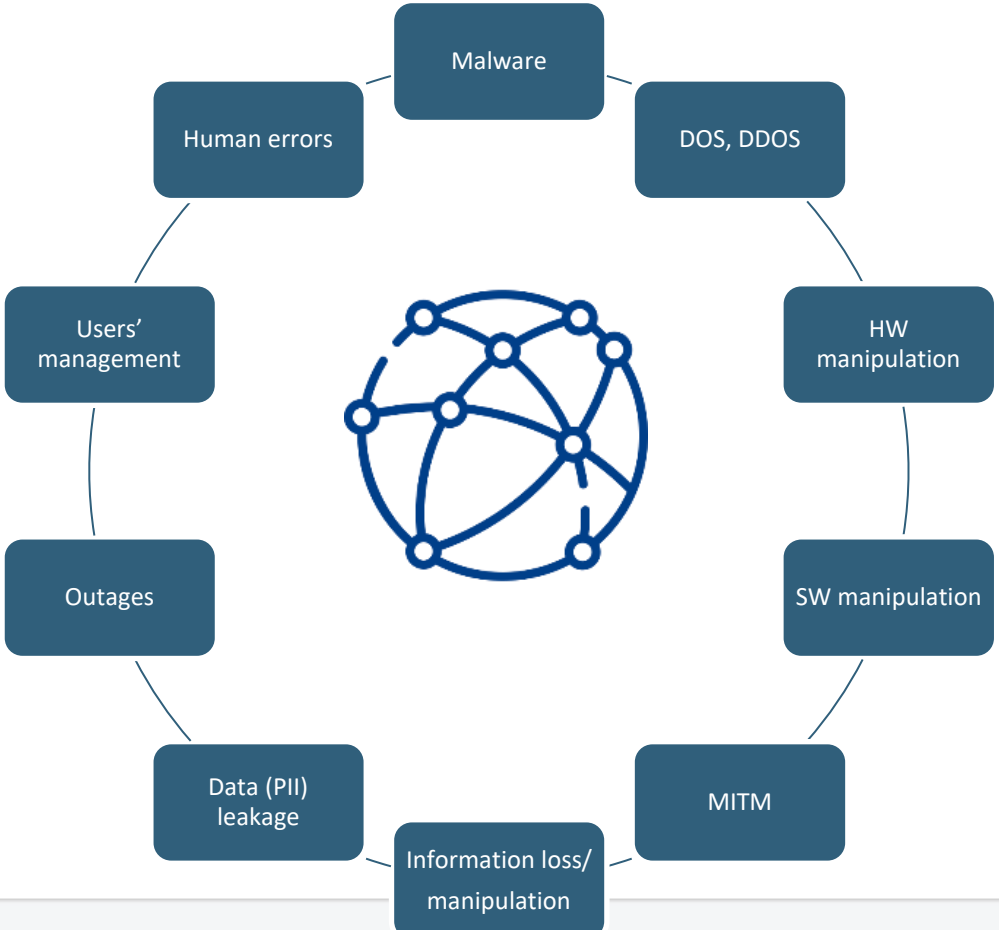
Layered security approach

Securely connect machines to Talk2M cloud & users



Security aspects in developing a connected product

Threats

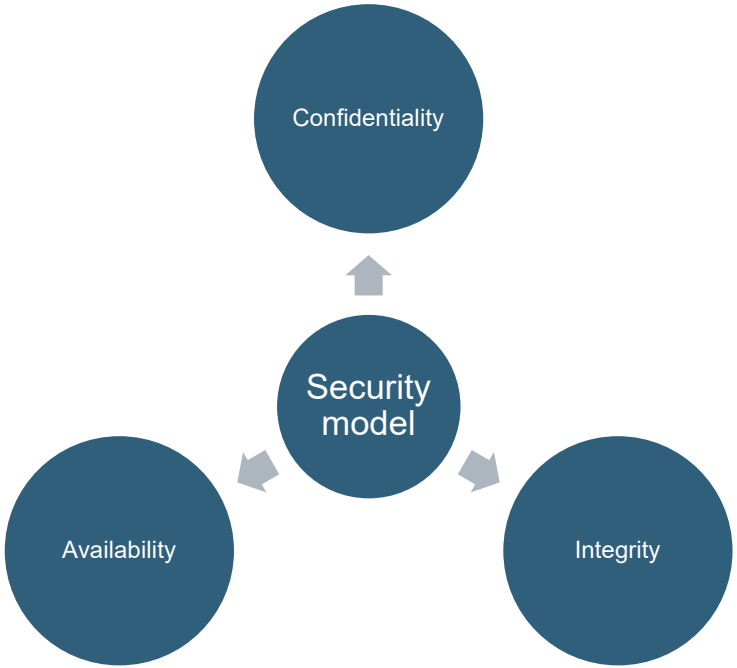


IIOT is a specific branch of IOT with different challenges

	IOT	Industrial IOT
Focus	Easyness	Prevention of process interruption
Failure implication	No critical	Impact on production, physical threats
Patch management	Possible during operation	Need to be scheduled, may be postponed for considerable time
Lifecycle	Frequent changes	Lifespan of 10 years
Reachability	At home, wearable	Not always close to humans, might be physically exposed to hacker

What do we want from an IIOT device connected to a machine?

Basic Model



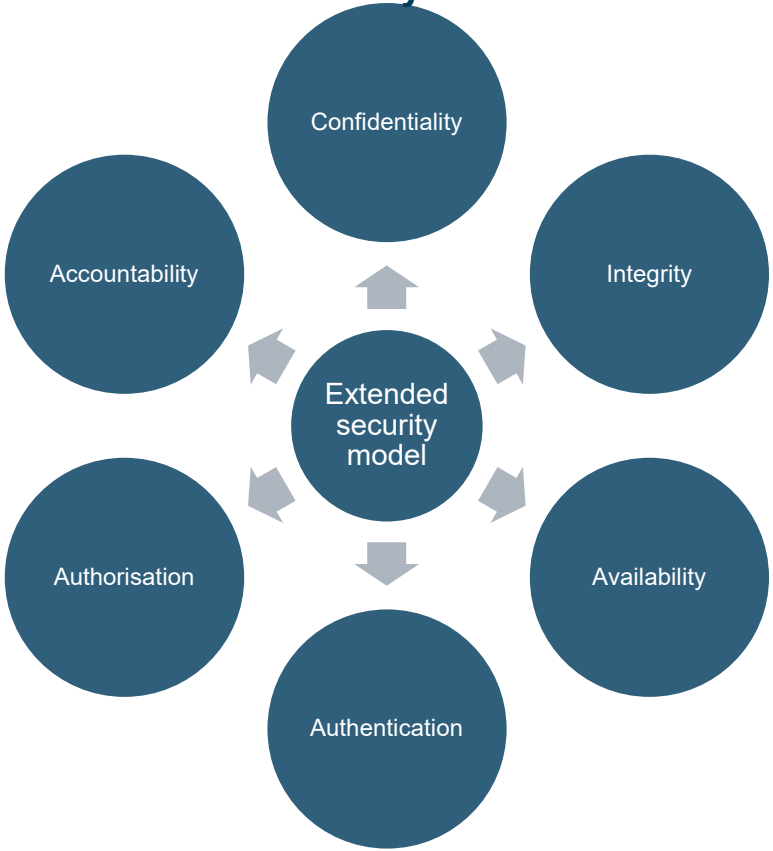
C Confidentiality:
No-one can intercept information

I Integrity:
Information & code are not modified or destroyed

A Availability:
Information (device) is available when needed

What do we want from an IIOT device connected to a machine?

The extended security model



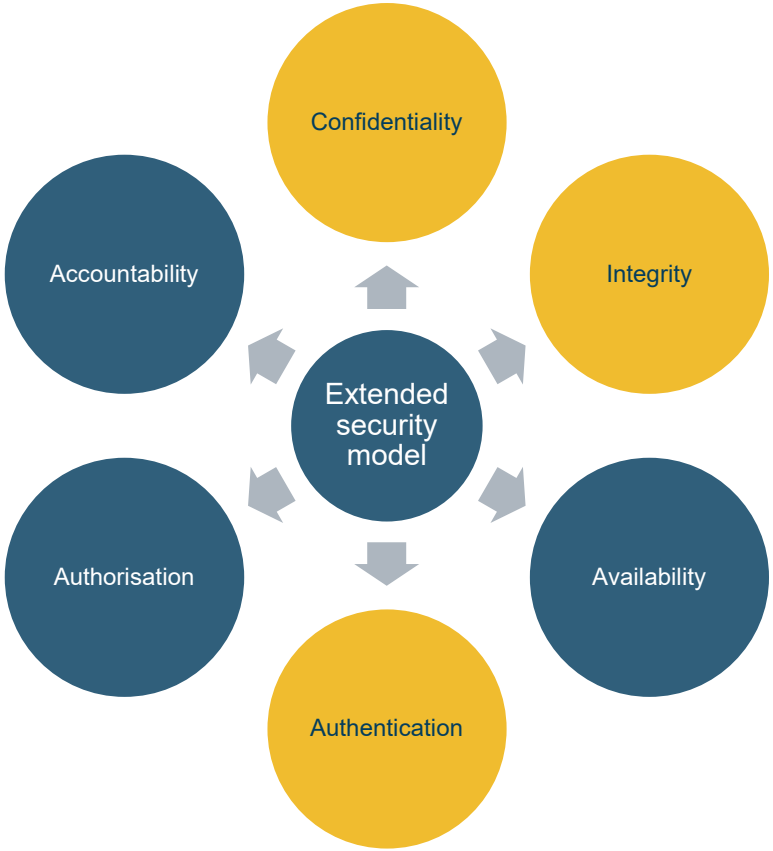
Au **Authentication**:
Agents involved in the communication are identified

Ar **Authorization**:
What can/can't be done (by user, or system)

Ac **Accountability**:
What has been done, when, by who, for how long

What do we want from an IIOT device connected to a machine?

The extended security model

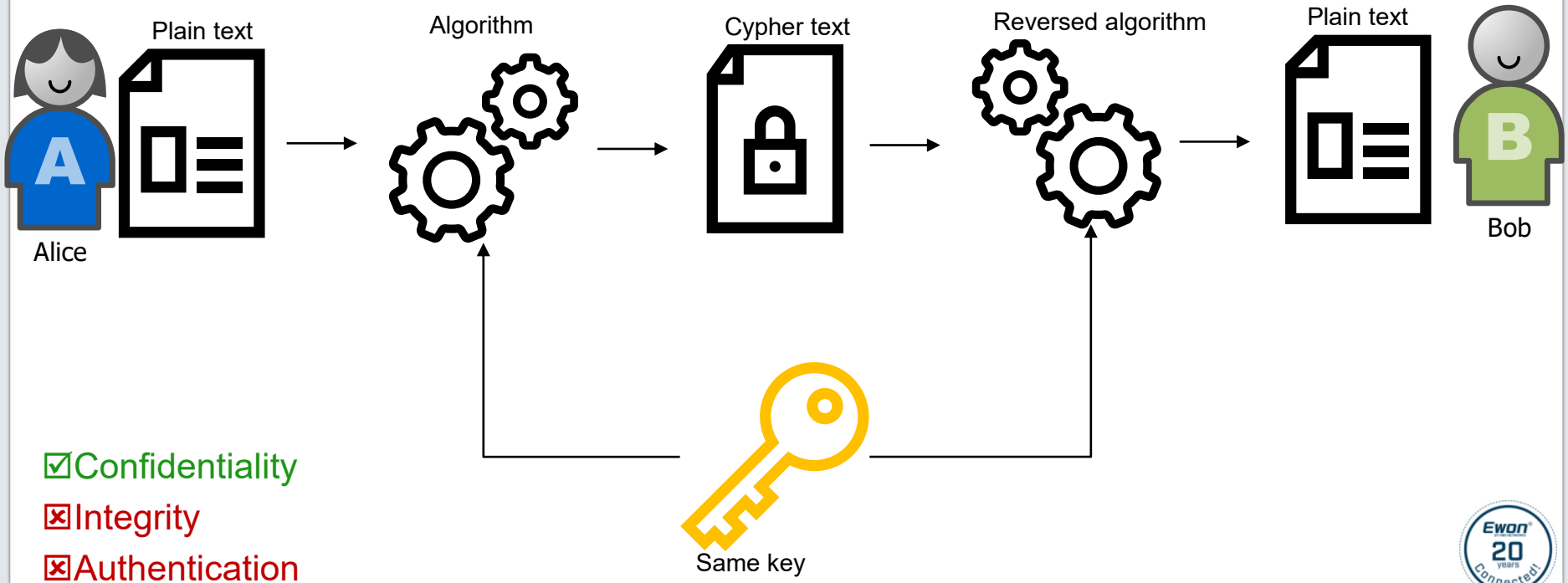


- Asymmetric cryptography
  - Confidentiality = Encryption
  - Integrity = Code signing
  - Authentication = Identity

But what is cryptography?

Symmetric cryptography

Encryption



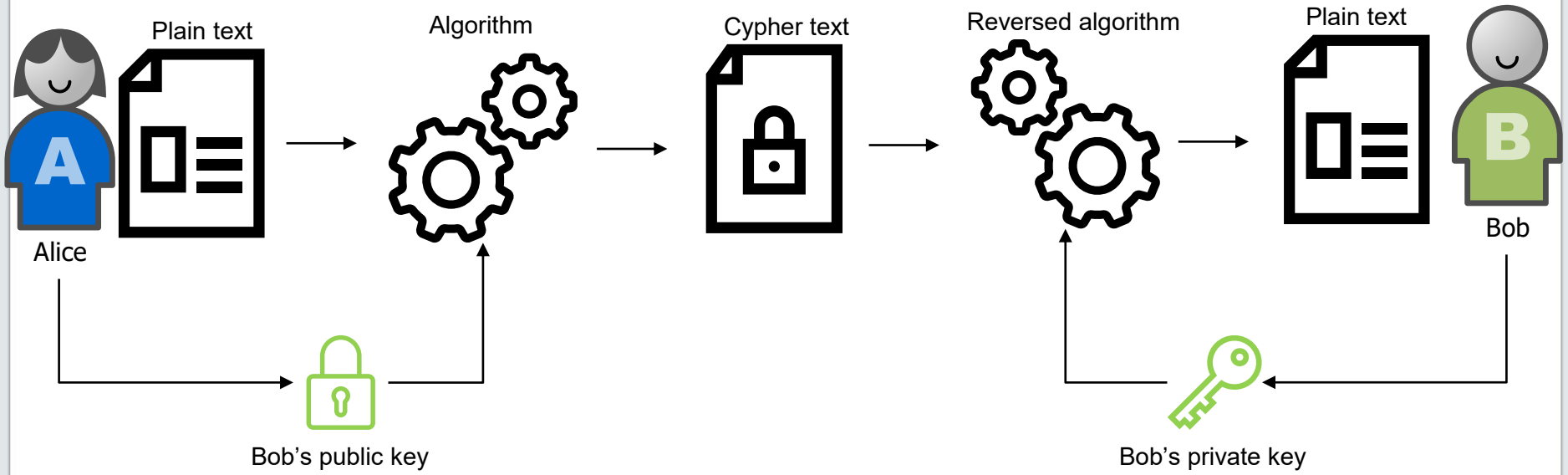
☑Confidentiality

☒Integrity

☒Authentication

Asymmetric cryptography

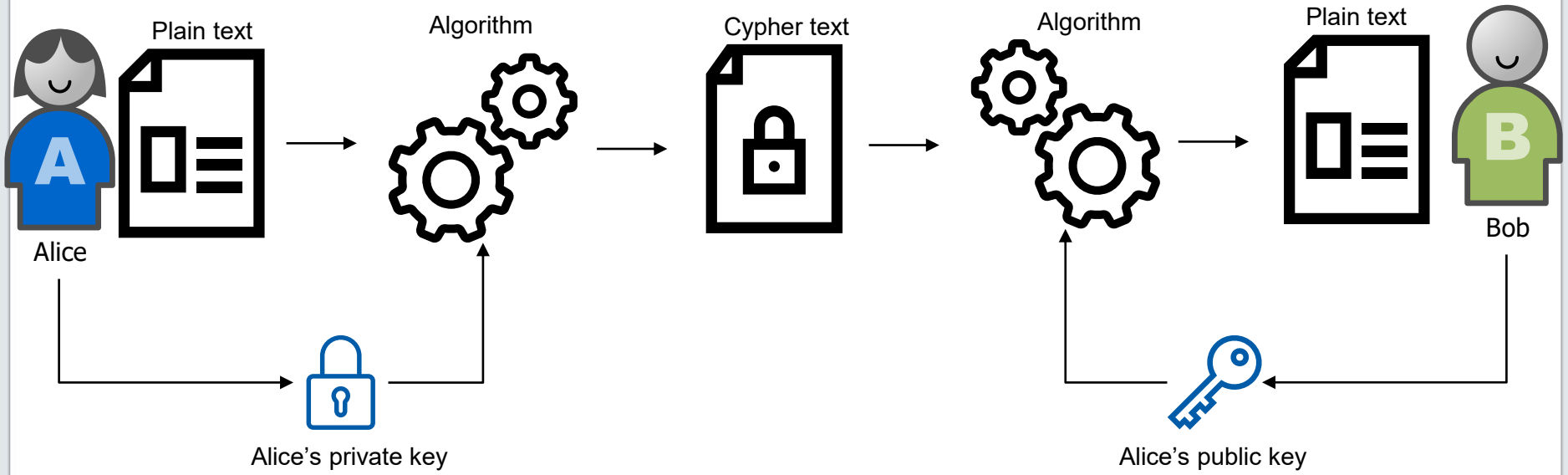
Encryption



☑Confidentiality

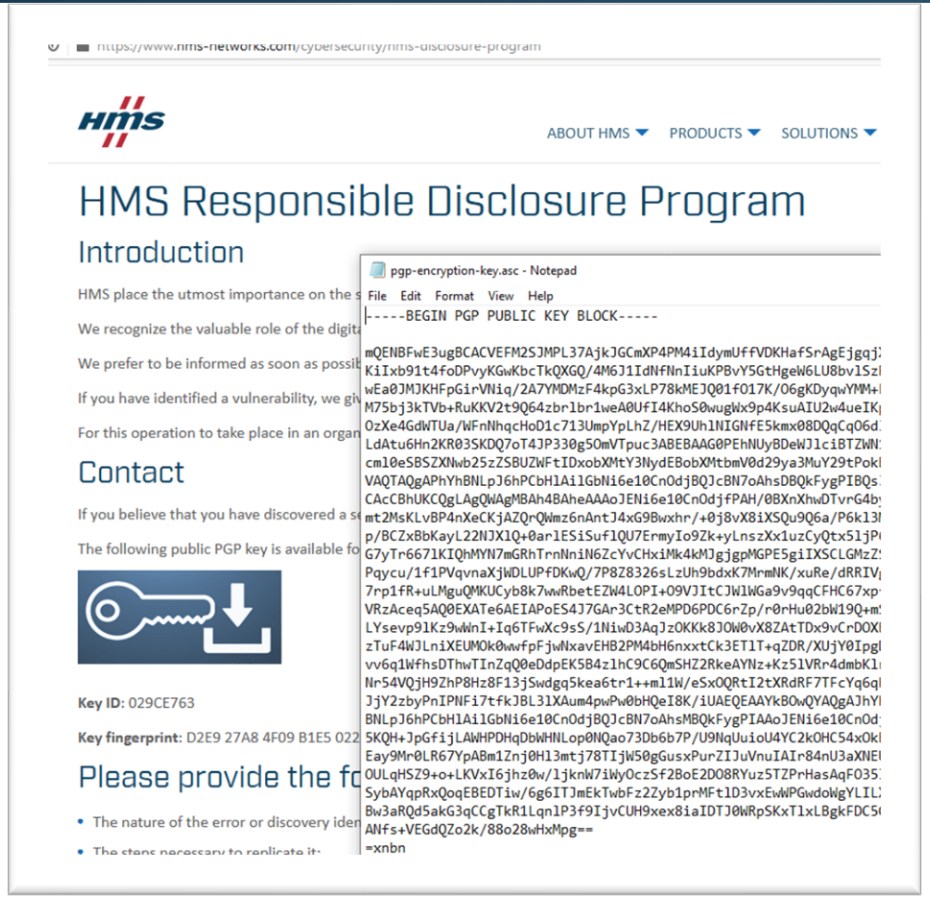
Asymmetric cryptography

Signature



☑Integrity
☑Authentication

Focus on: HMS public key



The key to keep a secret is to keep the key secret !

	SYMMETRIC	ASYMMETRIC
Strength	Strong	Strong
Speed	Faster	Slower
Keys	Must be shared (danger !)	Private key remains private
Easiness	High volume of keys (1 per actor)	Improved scalability (management of own private key)
Confidentiality	✓	✓
Authentication	✗	✓
Integrity (hash verification concept non explained here)	✗	✓

Preliminary conclusion

Given, that:

- We identified threats.
- To mitigate threats & get proper security, we need:
  - C Confidentiality,
  - I Integrity,
  - A Availability,
  - Au Authentication,
  - Ar Authorization,
  - Ac Accountability.
- C I Au are ensured by cryptography.
- In cryptography, keys must remain secret and untampered at all costs.

Only one way: Security on Hardware

Security on Hardware

HW Root of Trust

Security at component level

Secure boot

Digitally signed code

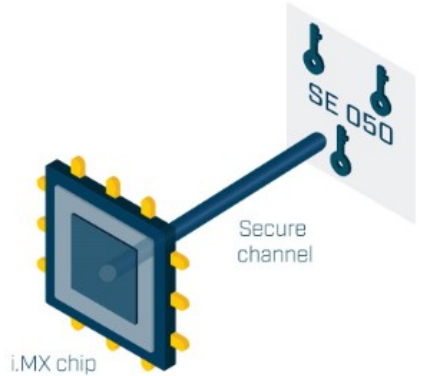
Insurance that…

- Secrets remain secret and unchanged — C, I
- Communications between components are secured — C, I, Au
- Software is genuine — I
- Updates are legitimate — I

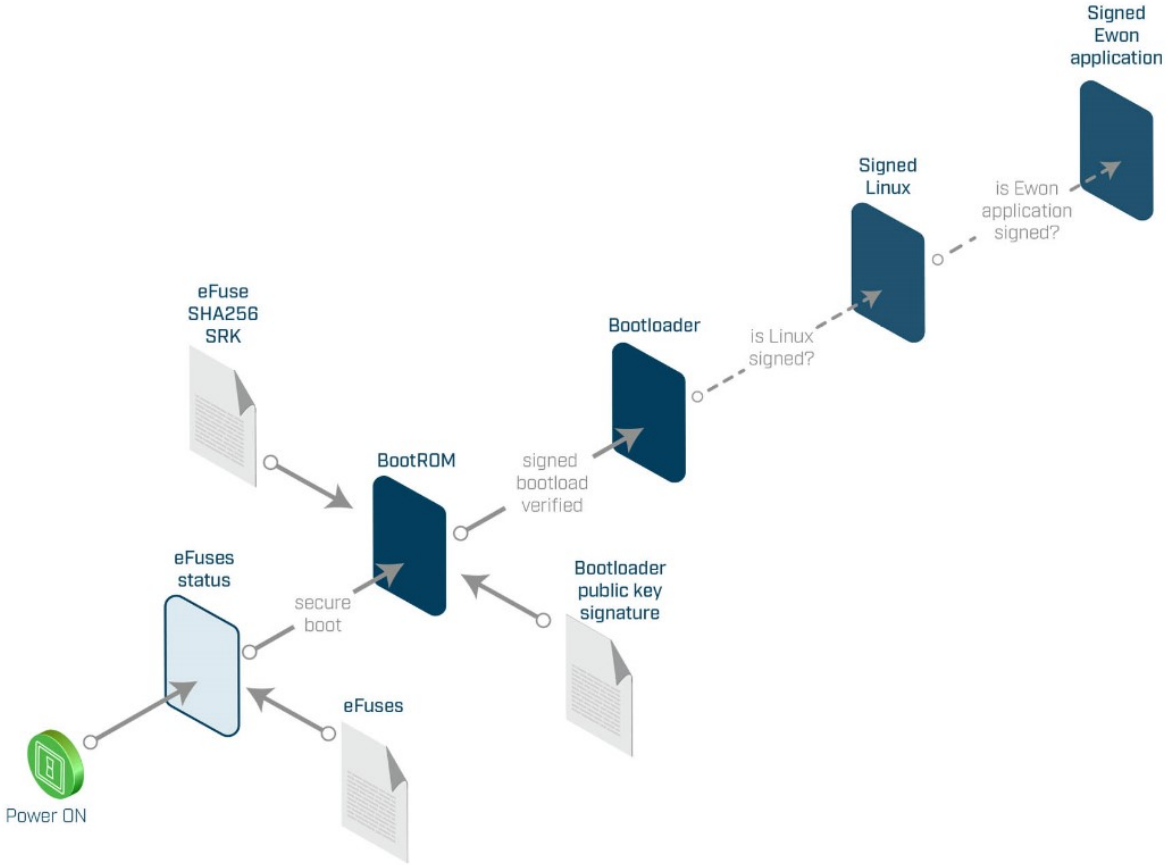
What's new?

Secure element / Security on Hardware

CPU



Chain of trust in secure boot



Security from machine to user, wherever in the world

Birth certificate

Secure communications

Open source technology

Security renewal

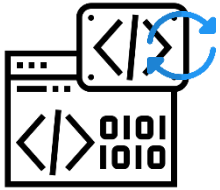
Insurance that…

- Device is legitimate — Au Ar
- UpToDate encryptions protocols — C I
- No security by obfuscation — A
- Security remain UpToDate during lifetime — A

Security, surrounding the IIOT solution

Vaults

Key ceremony



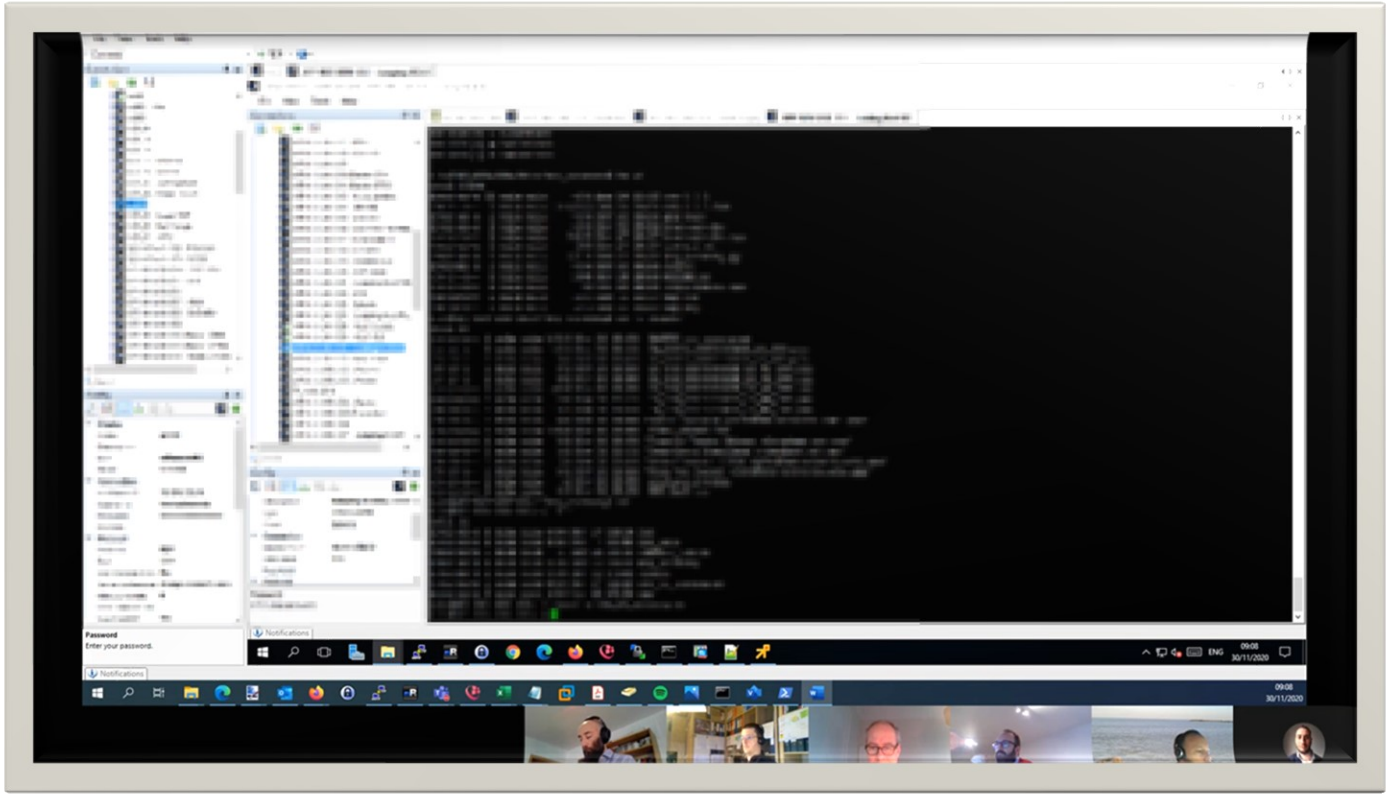
Secure coding

Internal security and processes

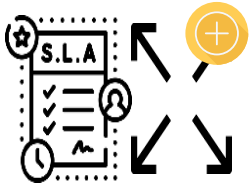
Insurance that…

- Secrets… remain secrets — C I A
- Secrets are not seen, not tampered — C I
- Security is well implemented — I
- Code is protected — C I A Au Ar Ac

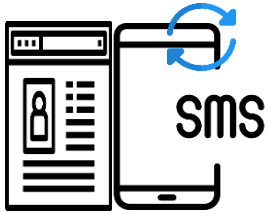
The 2 hours that produced all secrets for Cosy+



Security is also…

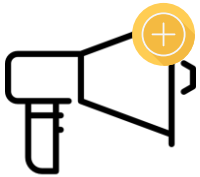


Availability
Scalability



Users'
management

Logs



Users'
awareness

Insurance of…

Resilience

A

Need to know
need to do
principle

C I Au

Controls and
accountability

I Ac

Right
implementation

C I A

Focus on availability

The problem

2021/03/10 [update]

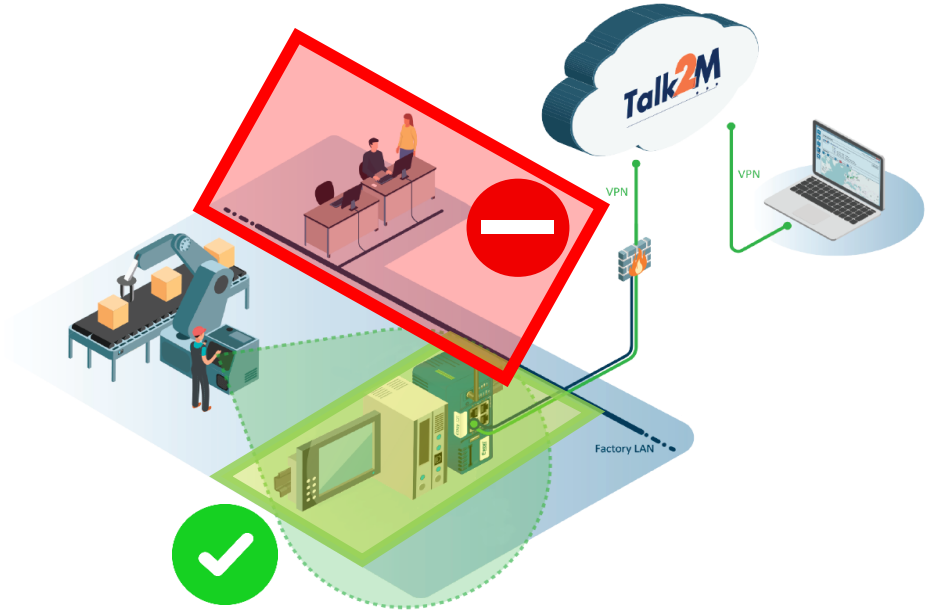
Issue on some of our European Free+ VPN server

A fire partially destroyed a datacenter of one of our hosting providers. The datacenter site is entirely down. Two of our European Free+ VPN servers hosted there are offline since 2021-03-10 01:27 UTC. In order to ensure service continuity, impacted Ewon devices have been temporarily rerouted to different VPN servers. If your Ewon device is not online on Talk2M, it might be due to local firewall policies preventing it from communicating with the substitute servers. The device will be back online when the infrastructure is completely recovered. To take full advantage of the global Talk2M infrastructure, please review the best practices related to ports and addresses used by Talk2M (as explained here below on this webpage). --- Devices have been moved back to previous servers endpoints/IPs since 20210316 19:30 UTC.

The answer: no problem!

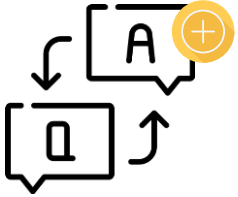
The LAN is safe!

LAN segregation (reach only the target devices → no access to the factory network !)



Challenge & be challenged!

Due diligence



NVISO.eu

ISO 27001

Challenges brought by our customers

Maturity arising…

- MB vs IT manager, IT/OT convergence
- More informed, aware of risks
- Monitor vulnerabilities
- Certification scheme
- Device/solution vouching and Fleet standardization

Machine builer

End user

Production Manager

IT Manager

OT minded
Focus on reliability

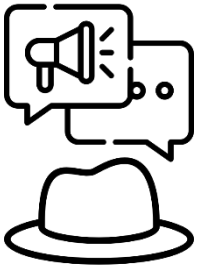
IT minded
Focus on Security

Overall equipment efficiency

External challenges

Response to vulnerabilities and incidents

Adversaries

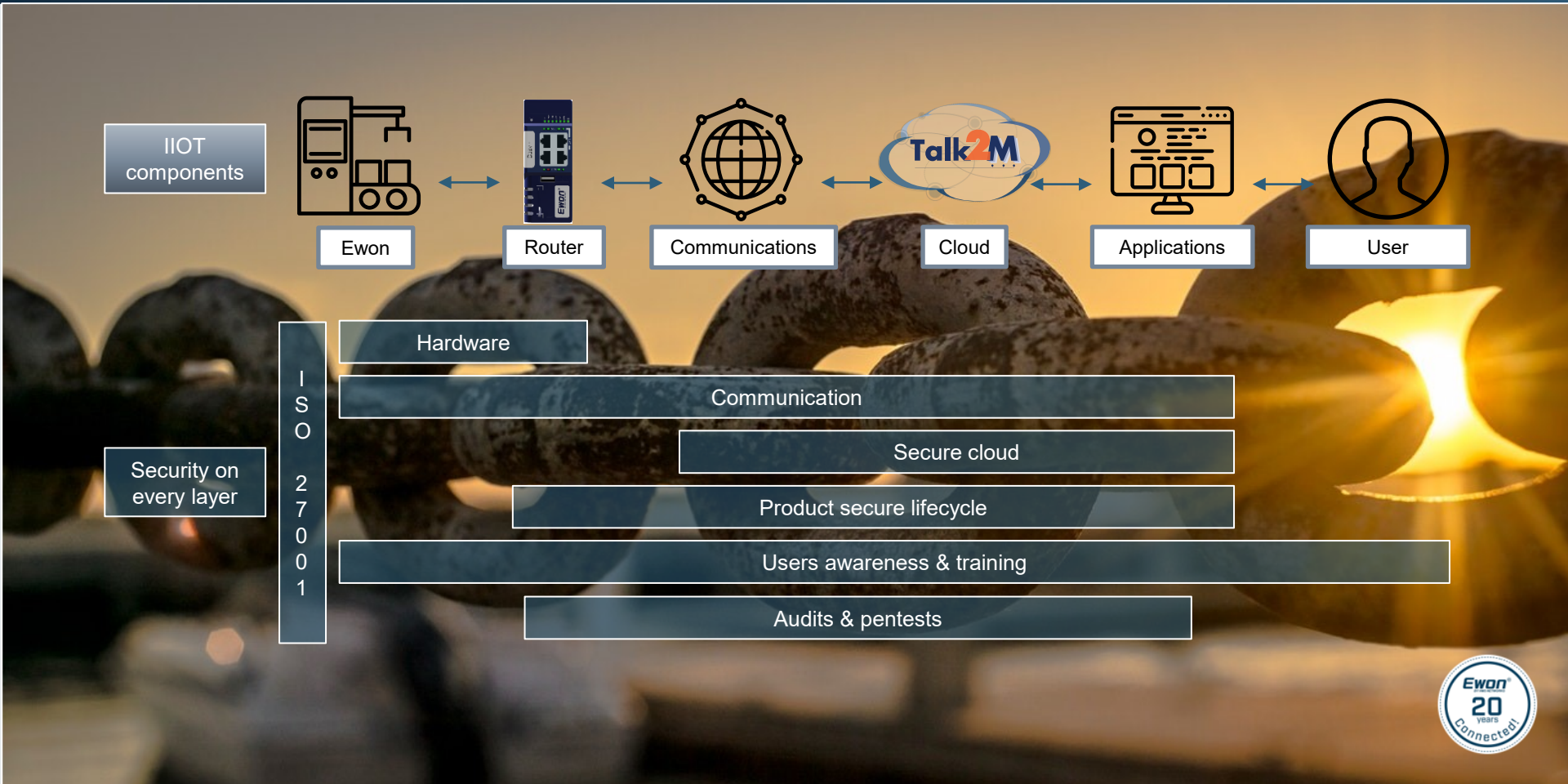


Responsible disclosure program

BCP/DRP
Crisis management

RA solutions currently on the market

A solid security chain without weak link!



Cosy+ performs at its best with Talk2M ‘enriched’

ISO 27001 INFORMATION SECURITY MANAGEMENT VINÇOTTE

nviso

35+ Servers

Redundant infrastructure

99,6%

Total Service Availability + SLA

Ewon 20 years Connected!

Trusted: Secure & future proof

EASY

- ✓ Straightforward setup
- ✓ Freemium model
- ✓ Simple pricing

SECURE

- ✓ ISO 27001 certification
- ✓ Access control & visibility
- ✓ LAN segregation

FUTURE PROOF

- ✓ Leadership
- ✓ Standard technologies
- ✓ Quality local support

TALK2M INFRA.

- ✓ Global
- ✓ Reliable (SLA)
- ✓ Scalable

Wrap up

- Security by design,
- Risk assessment,
- Security on hardware,
- Secure Element to protect secrets on device & allow secure communication,
- Whole structure to manage secrets at Ewon level and push them on devices,
- Secrets protected all along the chain: bullet proof solution,
- Cosy+ must not be seen alone, but as part of an **integrated secure solution** including Talk2m & the applications.

QUESTIONS?


STAY CONNECTED!
www.hms-networks.com