



Everything about Cosy+ security

Deep dive in Security on Hardware





Jean-David Epailard

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

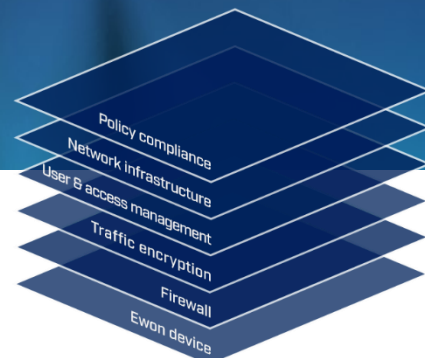


Certified Security



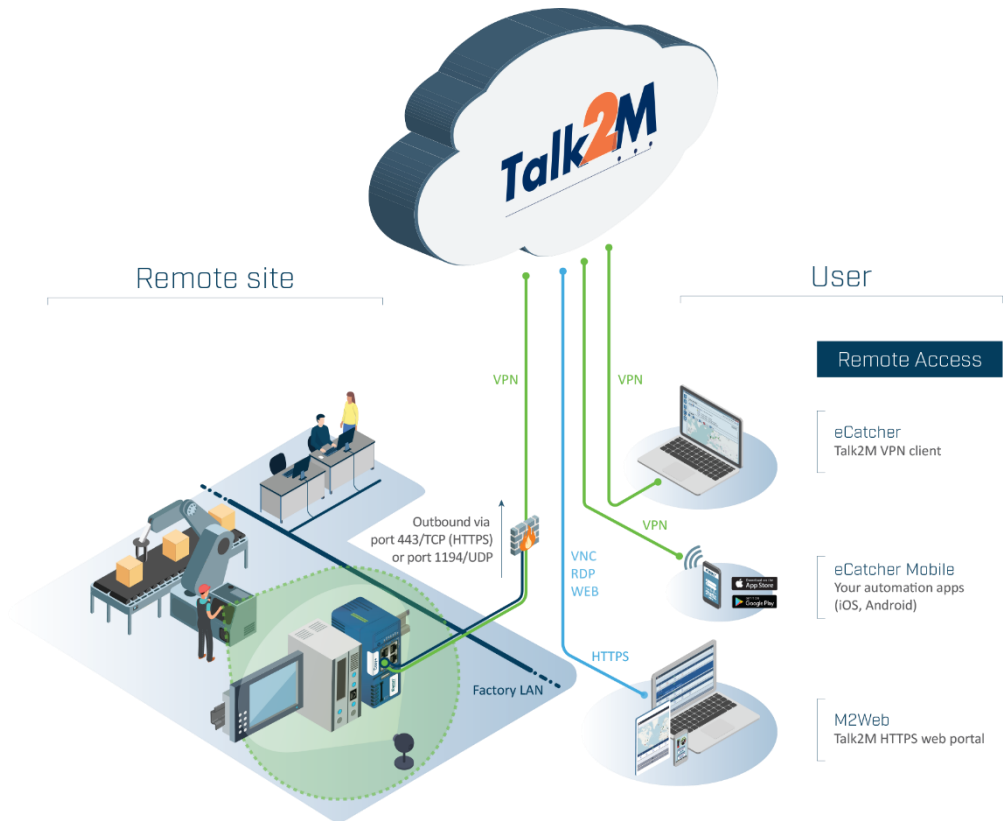
Testing Partner

Layered
security
approach

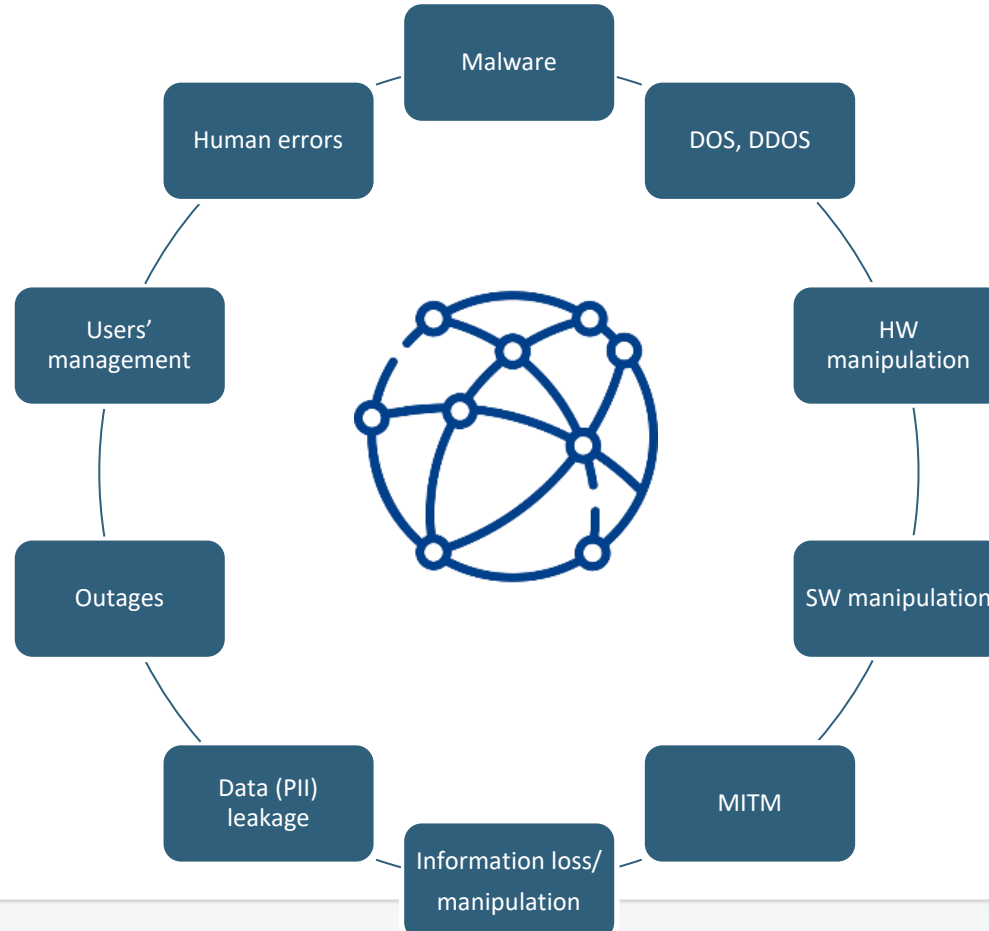




Securely connect machines to Talk2M cloud & users



Threats

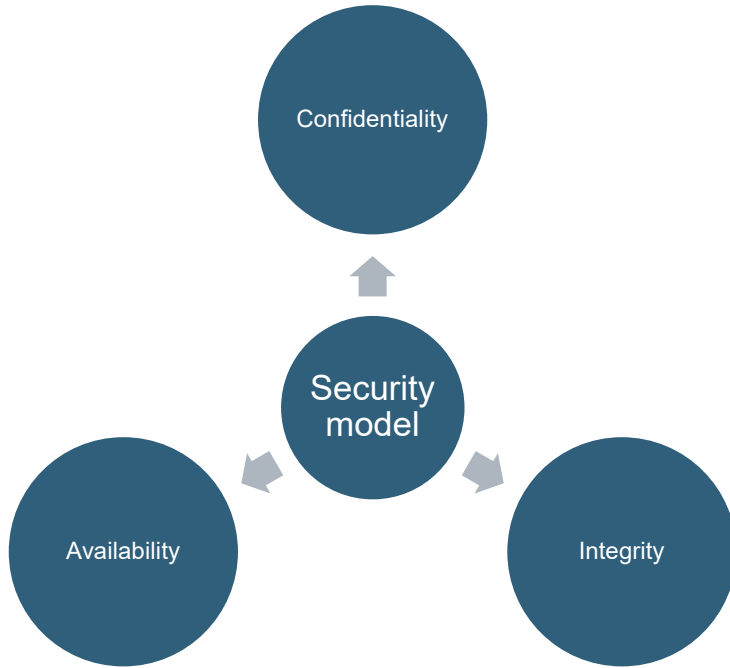


IIOT is a specific branch of IOT with different challenges

	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

HMS 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

HMS 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

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

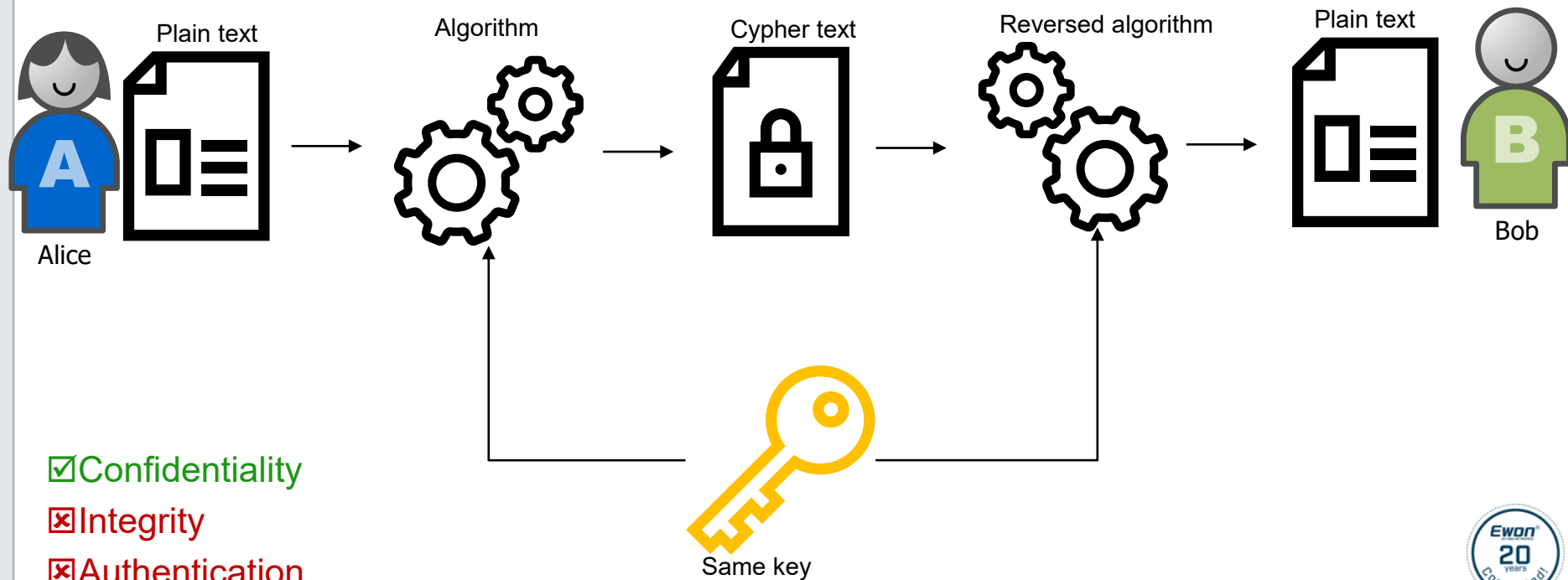
The extended security model



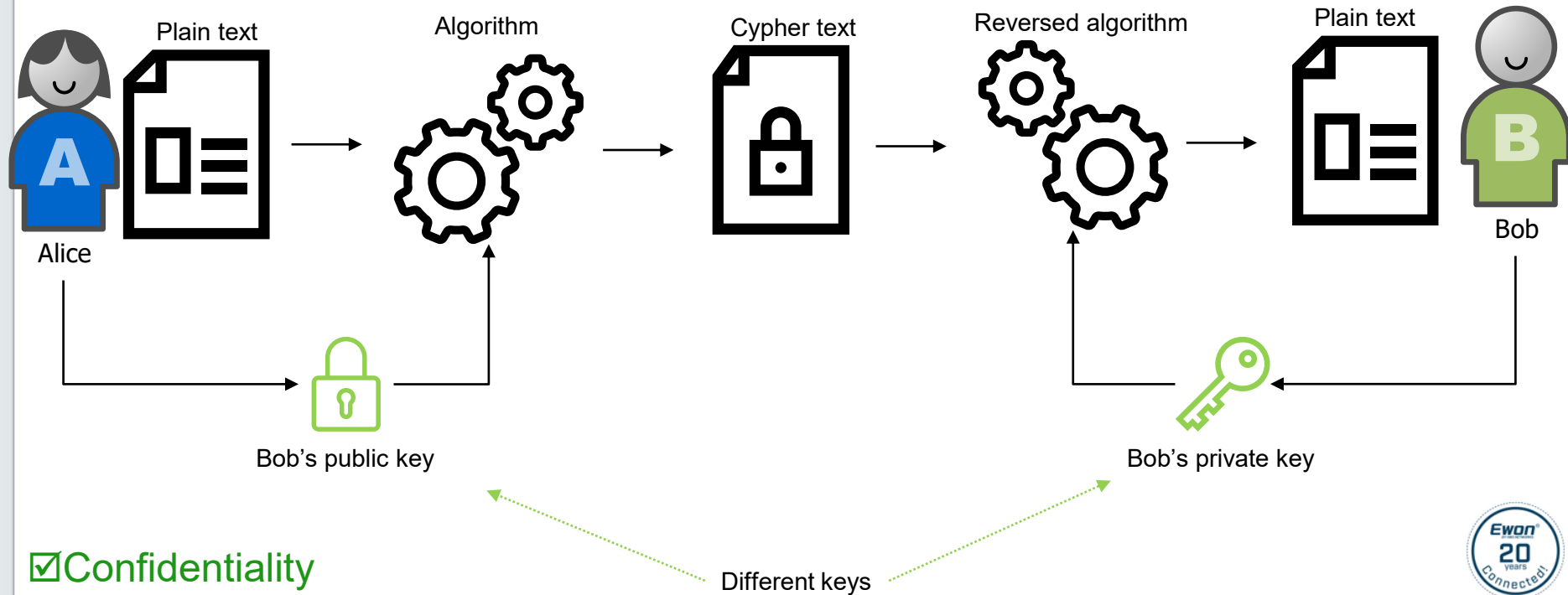
- Asymmetric cryptography
 - Confidentiality = Encryption
 - Integrity = Code signing
 - Authentication = Identity

But what is cryptography?

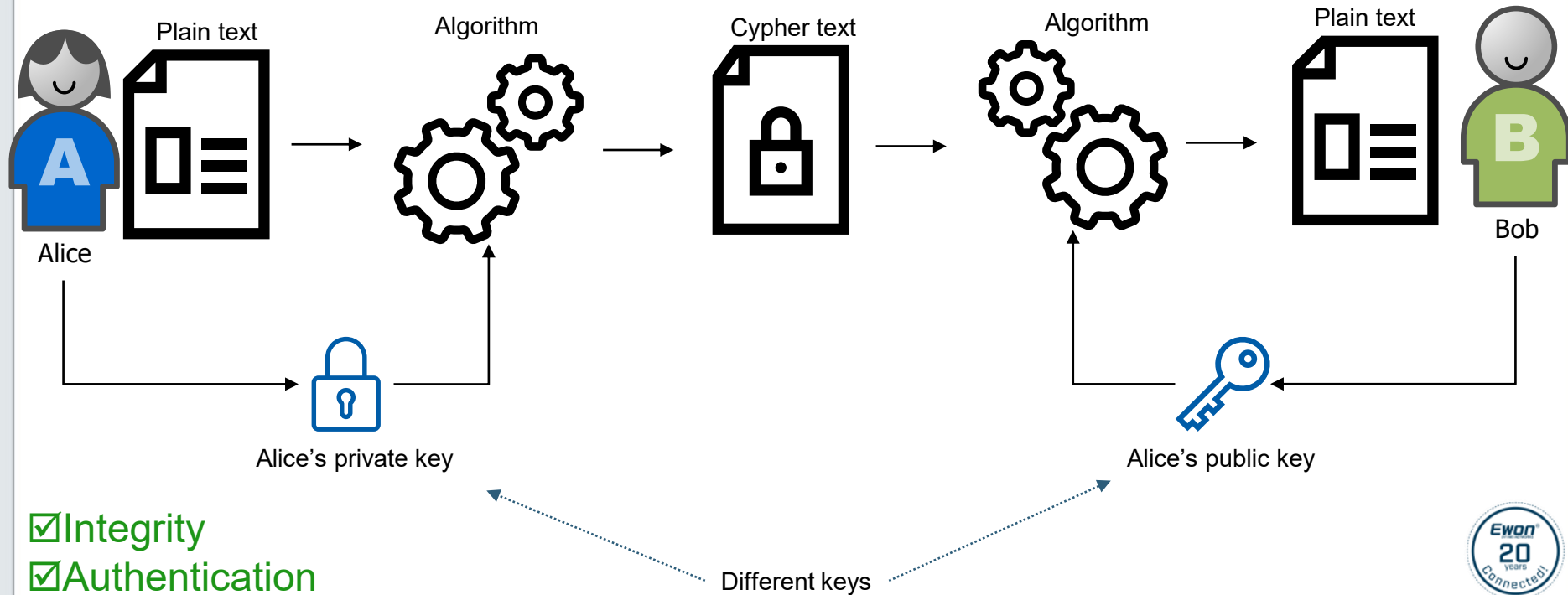
Encryption



Encryption



Signature





Focus on: HMS public key

https://www.hms-networks.com/cybersecurity/hms-disclosure-program



ABOUT HMS ▾ PRODUCTS ▾ SOLUTIONS ▾

HMS Responsible Disclosure Program Introduction

HMS place the utmost importance on the security of our products and services.

We recognize the valuable role of the digital community in identifying vulnerabilities.

We prefer to be informed as soon as possible of any vulnerabilities discovered.

If you have identified a vulnerability, we encourage you to report it to us.

For this operation to take place in an organized and secure manner, we have established a Responsible Disclosure Program.

Contact

If you believe that you have discovered a security vulnerability in any of our products or services, please contact us at security@hms-networks.com.

The following public PGP key is available for our communications:



Key ID: 029CE763

Key fingerprint: D2E9 27A8 4F09 B1E5 022A 7B13 1A04 4C2K 0HC5 4X0K

Please provide the following information:

- The nature of the error or discovery identified.
- The steps necessary to replicate it.

pgp-encryption-key.asc - Notepad

File Edit Format View Help

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFW3ugBCACVEFM2SJMPL37AjkJGCMxP4PM4iIdymUffVDKHafSrAgEjgqj;
 KiIxb91t4FoDPvyKGwKbcTkQXGQ/4M6J1IdNfNnIiukPBvY5GtHgeW6LU8bv1SzI
 wEa0JMJKHfP61rVNIq/2A7YMDMzF4kpG3xLP78kMEJQ01f017K/06gKDYqWYMM+I
 M75bj3kTVb+RuKKV2t9Q64zbr1br1weA0UFI4KHoS0wuglx9p4KsuAIU2w4ueIKj
 OzXe4GdWTUa/WFnNhqcHoD1c713UmpYpLhZ/HEX9UhlNIGNfE5kmx08DQqCq06d.
 LdAtu6Hn2KR03SKDQ7oT4JP30g50mVtpuc3ABEBAAG0PEhNlUyBDeWJ1c1BTZWln
 cm10eSB5S2XNwb25zZSBUZWFtIDxobXMtY3NldEBoBXMtbnV0d29ya3MuY29tPoki
 VAQTAQgAphYhBNlPj6hPCbH1Ai1GbNi6e10CnOdjBQjcBN7oAhsDBQkFygPIBQs:
 CACBhUKQgLAQQAQwMBAh4BAheAAAoJENi6e10CnOdjFPAH/08XnXhwDTvrG4b:
 mt2MsKLvBP4nXeCKjAZQrQWmz6nAntJ4xG9BwXhr/+0j8vX81XSQu9Q6a/P6k13I
 p/BCZx8bKayL22NjX1Q+0ar1ESiSuf1QU7ErmyIo9Zk+ylNsZx1uzCyQtX51jPi
 G7yTr6671KIqMYN7mGRhTrnNniN6ZcYvHxiMk4kMjgJgpMGPE5giIXSCLGmZ:
 Paycu/1f1PVqvnaXjwDLUPfDKwQ/7P8Z8326sLzU9bdsxK7MrnNK/xuRe/dRRIVj
 7rp1fR+uLMguQMKUCy8k7wRbetEZw4LOPT+09V3ITcJWlWGa9v9qqCFHC67xp
 VRzAeq5AQ0EXATE6AEIAPoES437GaR3CtR2eMPD6PDC6rZp/r0rHu02bw19Q+m
 LYsevp91Kz9wWnI+Iq6TFwXc9sS/1NiwD3AqJz0KKK8J0W0vX8ZAtTDx9vCrDOXI
 zTuF4WJLnIXEUM0k0wFpFjFwNlxavEB2PM4bH6nxcctK3ET1T+qZDR/XUjY0Ipgl
 vv6q1WfhsDThwTInZqQ0eDdpEK5B4z1hC9C6QmsH2RkeAYNz+Kz51VRr4dmbK1:
 Nr54VQjH9ZhP8H8F13jSwddq5kea6tr1+mm1W/eSx0QRtI2tXRdRF7TfCYq6q
 jJY2zybPnIPNF17tFkJBL31XAum4pwPw0bHqE18K/iUAEQEAAYk80vQAQgAjhYI
 BNlPj6hPCbH1Ai1GbNi6e10CnOdjBQjcBN7oAhsMBQkFygPIAAoJENi6e10CnOd:
 SKQH+JpGfjJLAWPHDhQDbwHNLop0Hqao73Db6b7P/U9NqUuIoU4YC2k0HC54X0Kl
 Eay9Mr0LR67YpABm1Znj0H13mtj78TIjW50gGusxPurZi3UvnuIAI+84nU3aXNIE
 OULqHSZ9+o+LKVxI6jhZ0w/1jknW7iWY0cZf28oE2D08RYuzSTZPrHasAQF03:
 SybAYqRxxQoqEBEDTiw/6g6ITJmEkTwbFz2Zyb1prMFt1D3vxEWpGwdolwYLIL:
 Bw3ARQd5akG3qCcTkR1Lqn1P3f9IjvCUH9xex8iaIDTJ0WRpSKxT1xLBgkFDC5I
 ANfs+VEGdQoZk/88o28wHxMpg==
 =xnbn



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 <small>(hash verification concept non explained here)</small>	✗	✓

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



Communications
between
components
are secured



Software is
genuine



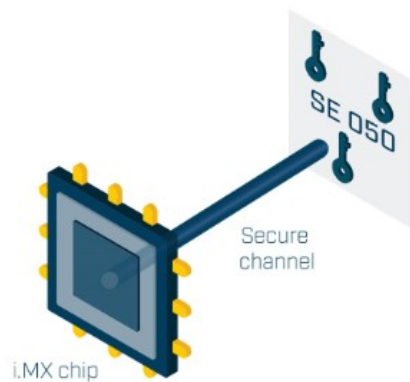
Updates are
legitimate

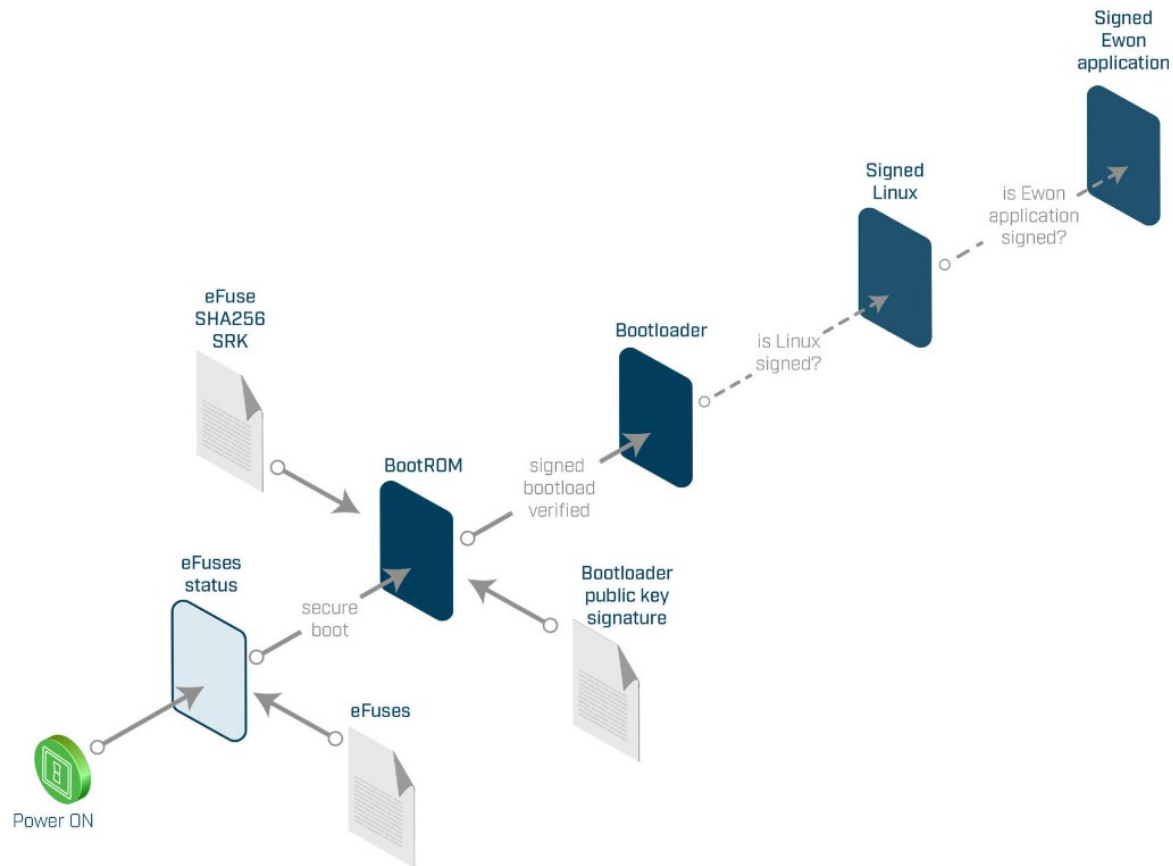




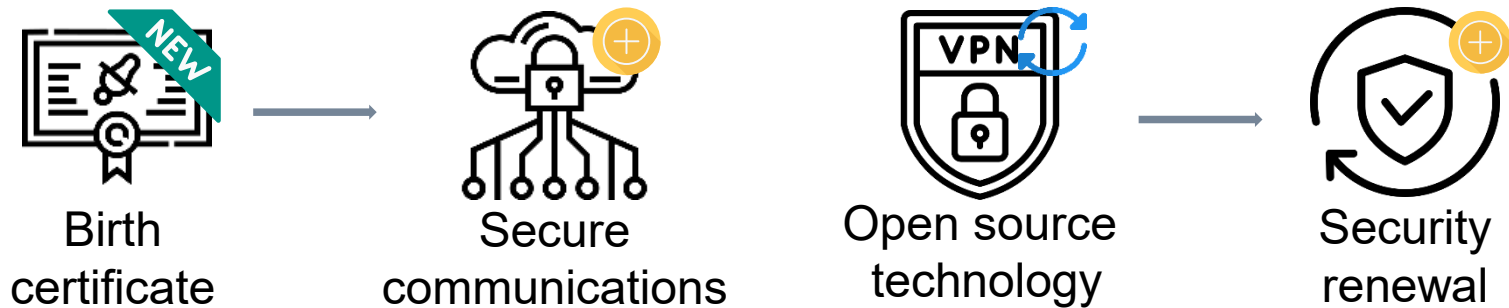
Secure element /
Security on Hardware

CPU





Security from machine to user, wherever in the world



Insurance that...

Device is
legitimate

Au Ar

UpToDate
encryptions protocols

C I

No security by
obfuscation

A

Security remain
UpToDate during
lifetime

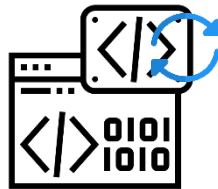
A



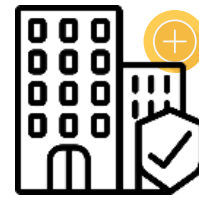
Vaults



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

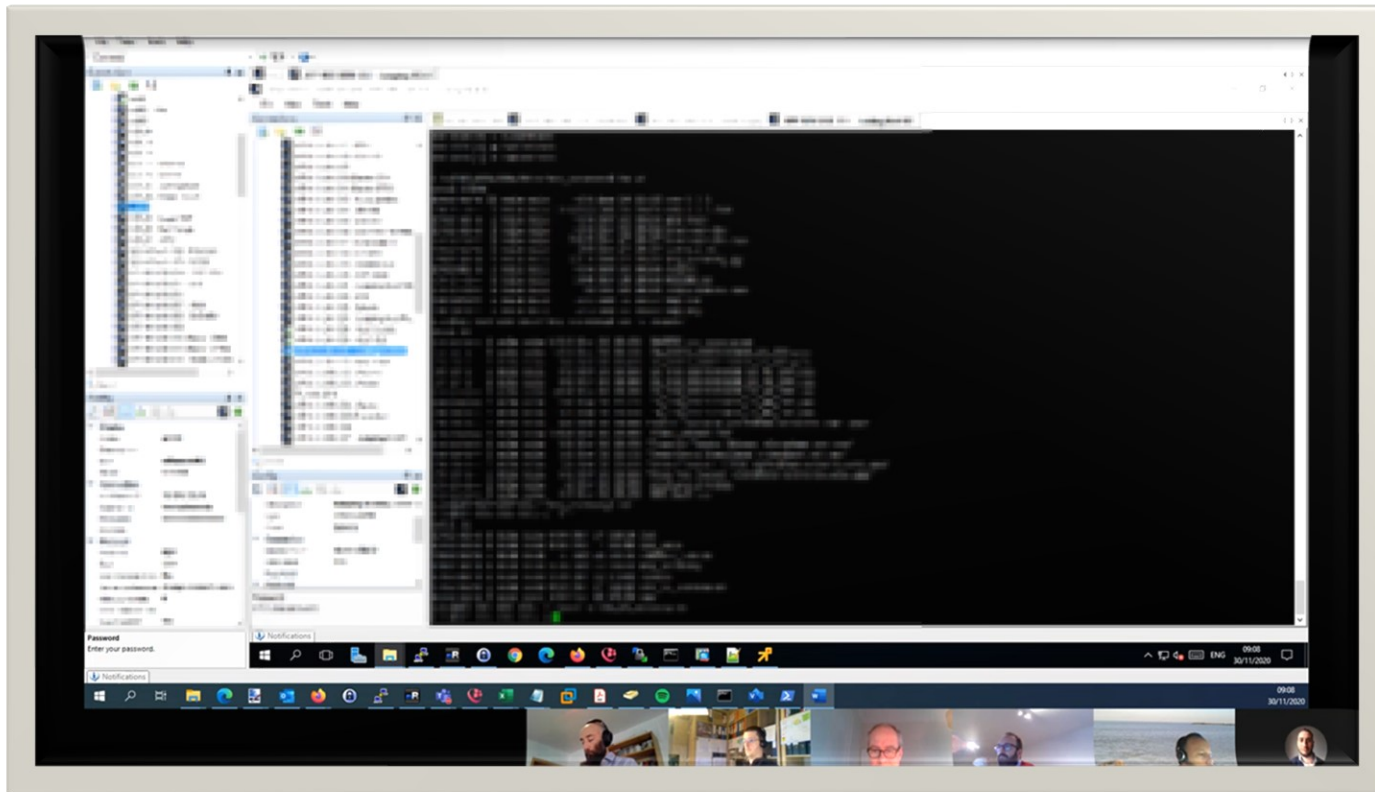
I

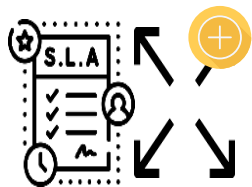
Code is
protected

C I A Au Ar Ac

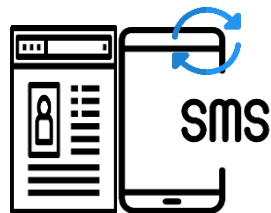


The 2 hours that produced all secrets for Cosy+





Availability
Scalability



Users'
management



Logs



Users'
awareness

Insurance of...

Resilience

A

Need to know
need to do
principle

C I Au

Controls and
accountability

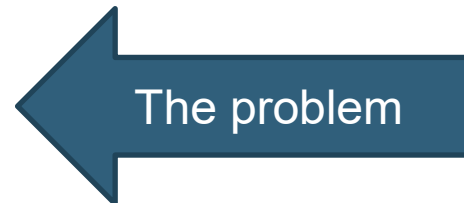
I Ac

Right
implementation

C I A



Focus on availability

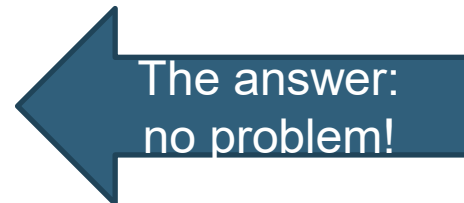


2021/03/10

[update]

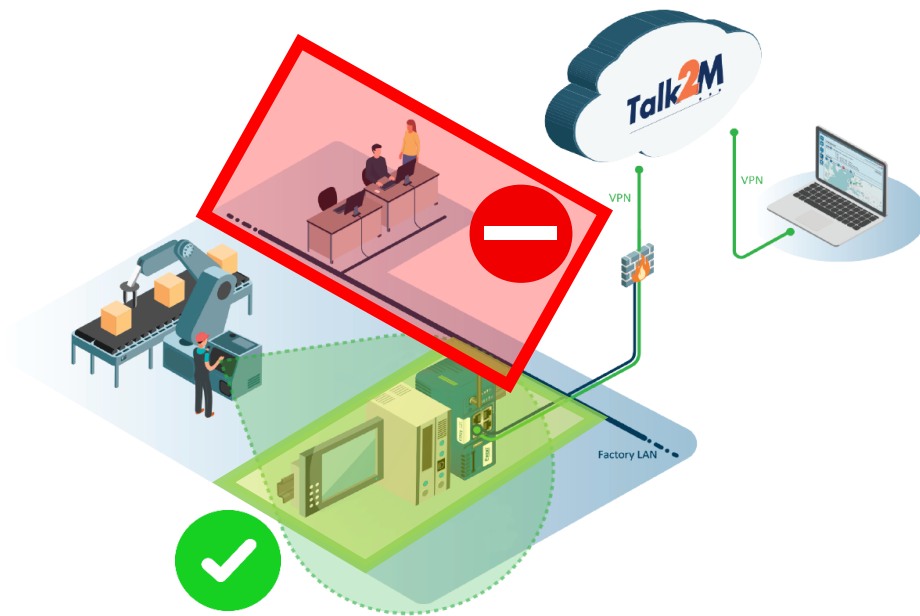
Issue on some of our European Free+ VPN server ^

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.



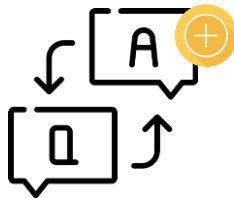
The LAN is safe!

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





Due diligence



NVISO.eu



ISO 27001

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 builder



End user



Production Manager



IT Manager



OT minded

Focus on reliability



IT minded

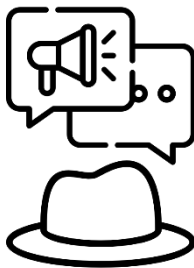
Focus on Security

Overall equipment efficiency

Response to vulnerabilities and incidents



Adversaries



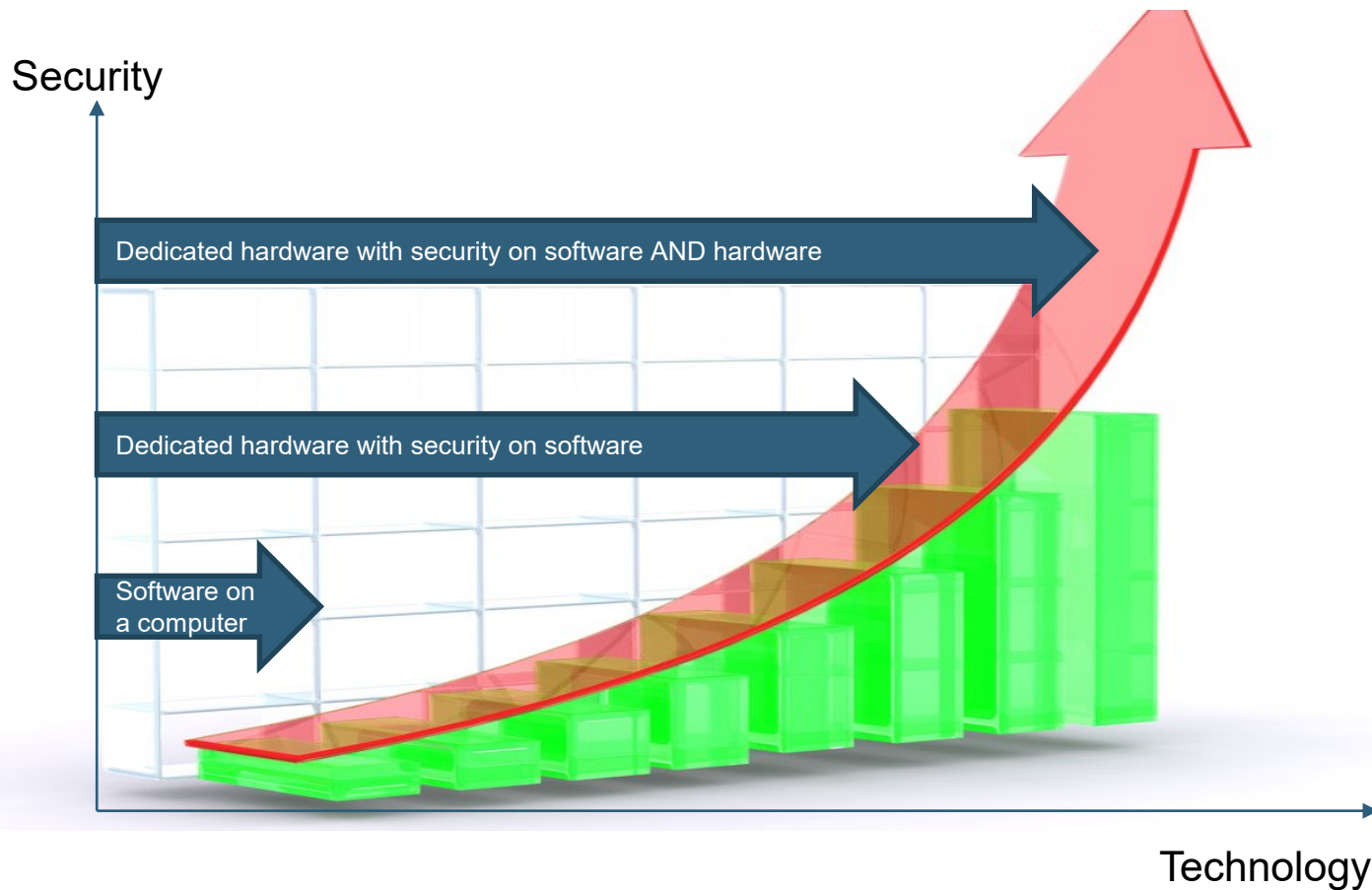
Responsible
disclosure
program



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'



A solid security chain without weak link!



35+ Servers

Redundant infrastructure

99,6%

Total Service Availability + SLA





Trusted: Secure & future proof

Ewon[®]
BY HMS NETWORKS

EASY

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

FUTURE PROOF

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

SECURE

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

TALK2M INFRA.

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



- 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?

A dark blue background featuring a world map with glowing nodes and connecting lines, overlaid with binary code (0s and 1s).

STAY CONNECTED!

www.hms-networks.com