

Digital certificates in an air-gapped high-security environment

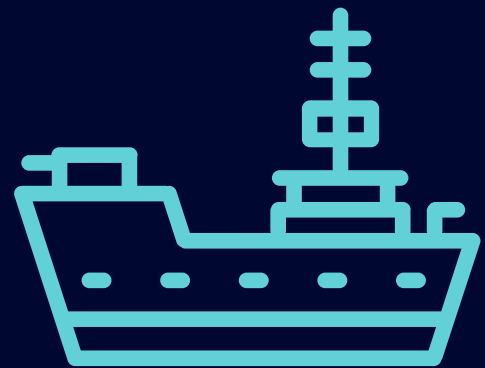
Kerstin Honskamp, Eviden Digital Identity

AGENDA

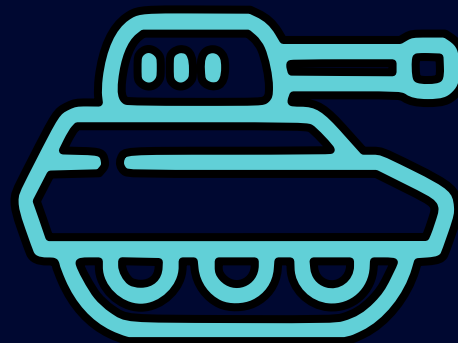
1. **The challenge**
2. The solution
3. Customer benefits
4. A look at our products
5. Conclusion

A company in the defense industry ...

... provides IT-solutions for defense platforms



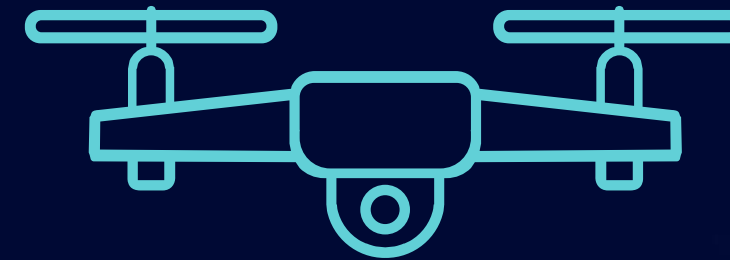
Ship



Tank



Missile base



Drone platform

...

Other

Self-contained, air-gapped systems

General security requirements



- Authentication of persons and components
- Confidentiality
- Authorization (need-to-know principle, dual-control principle)
- Tamper-proof logging

**Secure identities
necessary**

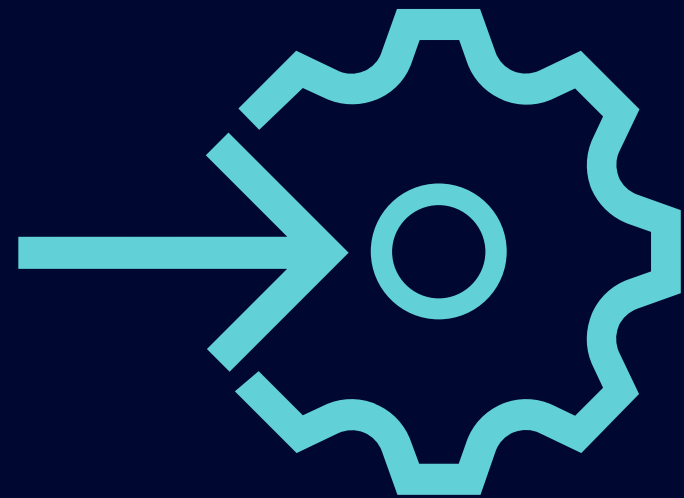
More security requirements



- No online updates
- Long-term protection

**Secure identities
necessary**

Special requirement: supply-chain security



Authorized code ...

- enables traceable code versioning
- avoids malware

**Secure identities
necessary**

Cryptographically secured identities needed

Every person is
assigned an
identity



Every major
component is
assigned an identity



Every identity gets a
digital certificate

**PKI is
necessary**

AGENDA

1. The challenge
- 2. The solution**
3. Customer benefits
4. A look at our products
5. Conclusion

Two PKI segments required



**Separation for
security reasons**

Multi-application PKI applications



*No permanent external
connection (air-gapped)*

- TLS connections
- Secure data exchange
- Certificate-based login
- Signed log-data
- ...

**Many different
applications
possible**

Multi-application PKI requirements



*No permanent external
connection (air-gapped)*

- Environments may vary
- No external PKI components
- Limited resources
- High availability and robustness
- Easy administration

Key protection in the Multi-application PKI

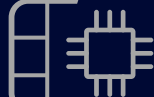


*No permanent external
connection (air-gapped)*

Certification Authority:

 HSM

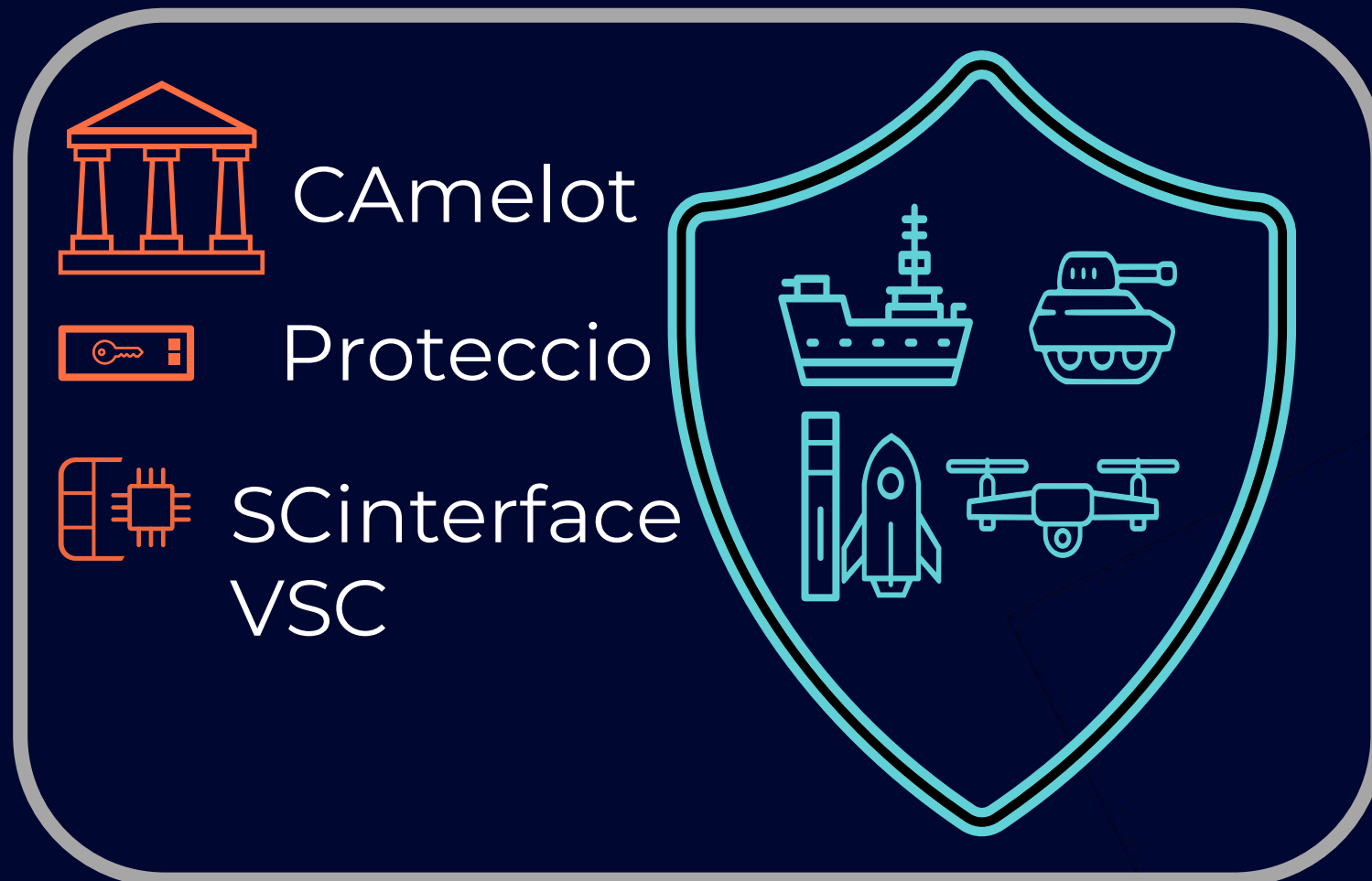
Users/components:

 Middleware VSC

 HSM

 Software keys

Eviden products in the Multi-application PKI



No permanent external connection (air-gapped)

CAmelot: Eviden's modular CA solution

Proteccio: Eviden's Hardware Security Module (HSM)

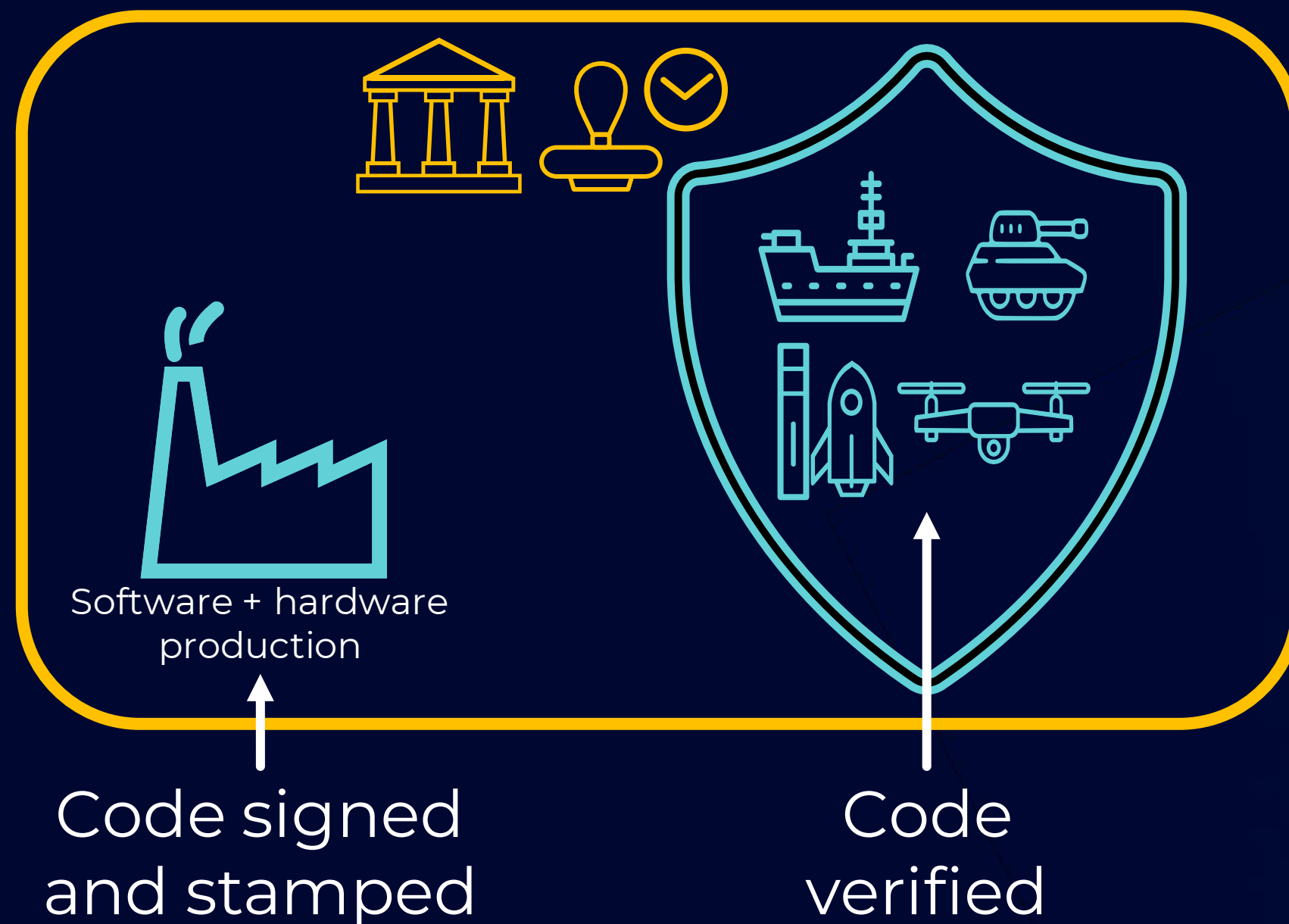
SCinterface VSC: Eviden's Middleware Solution

Code Signing PKI applications



- Code signing
- Time stamping

Code Signing PKI requirements



- Developers sign code used in the system
- Developers don't have access after delivery

Key protection in the Code Signing PKI



Certification Authority:

 HSM

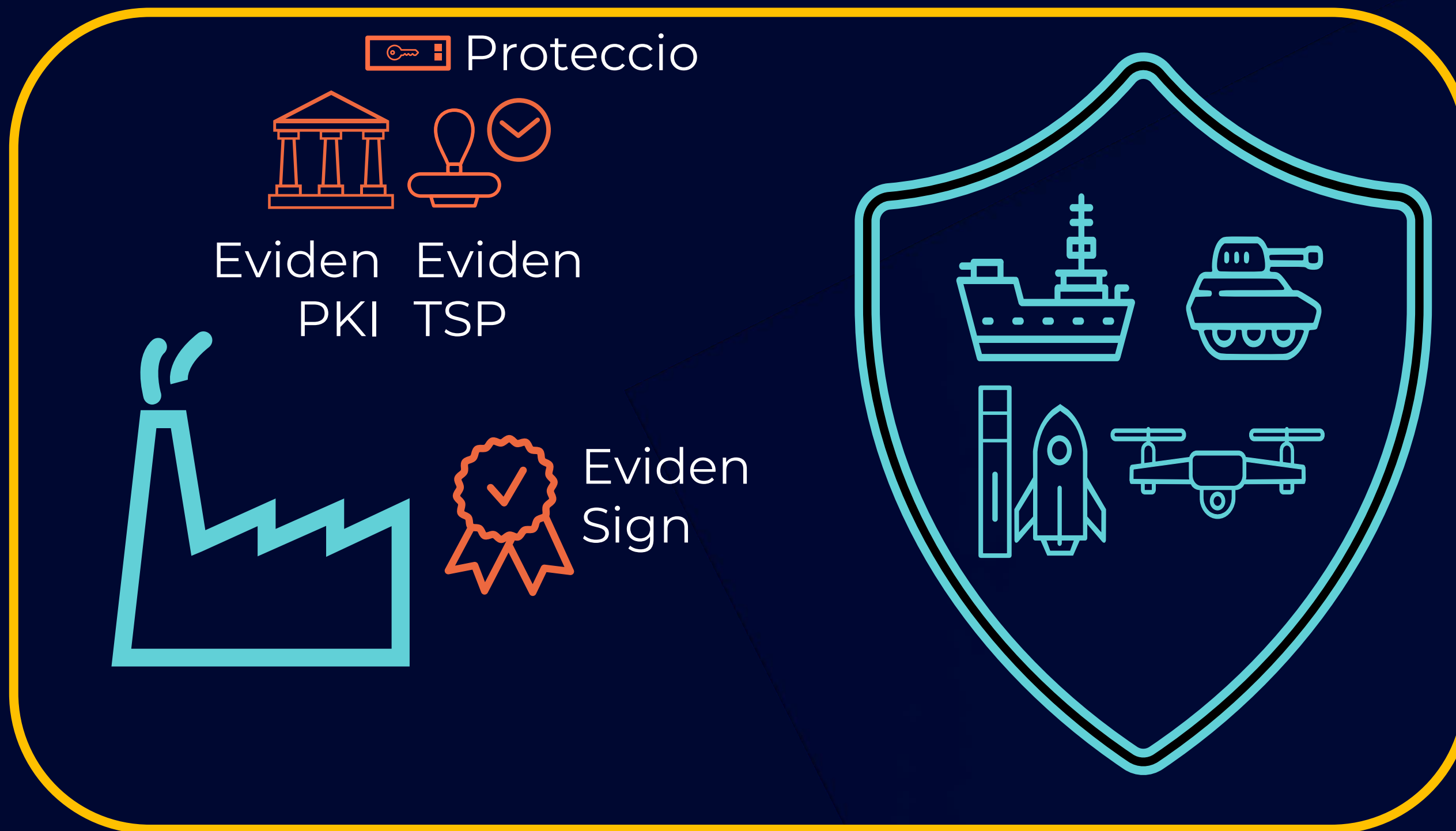
Time Stamping Service:

 HSM

Codesigners:

 HSM

Eviden products in the Code Signing PKI



Eviden PKI: Modular CA solution

Eviden TSP: Time Stamping Service

Eviden Sign: Code-signing solution

Proteccio: Hardware Security Module (HSM)

AGENDA

1. The challenge
2. The solution
- 3. Customer benefits**
4. A look at our products
5. Conclusion

Customer benefits



- Reduced project and liability risks
- Secure operation in air-gapped scenarios
- Long-term operation
- Modular and scalable
- Enhanced auditability
- “Made in Europe” ensures sovereignty

AGENDA

1. The challenge
2. The solution
3. Customer benefits
- 4. A look at our products**
5. Conclusion

Eviden products & services used in this project



Eviden
PKI



CAmelot



Eviden
Sign



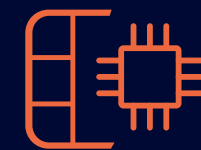
Consulting



Eviden
TSP



Proteccio

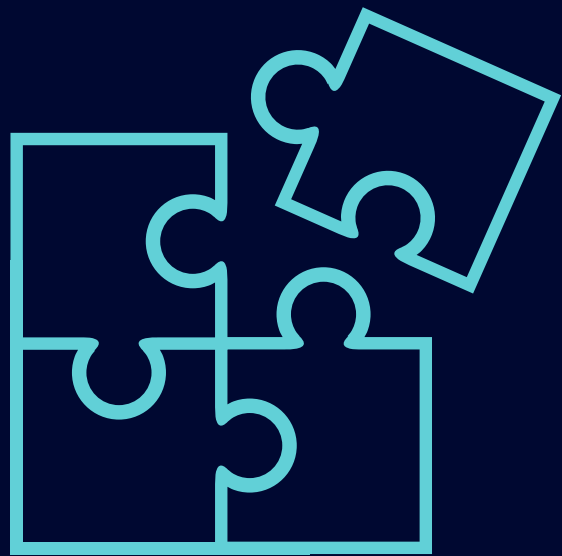


SCinterface
VSC

**All digital-certificate
solutions from one
hand**

Our products

... are modular and scalable



They are ...

- suitable for many different environments
- scalable to different sizes

Our products

... are developed and manufactured in Europe

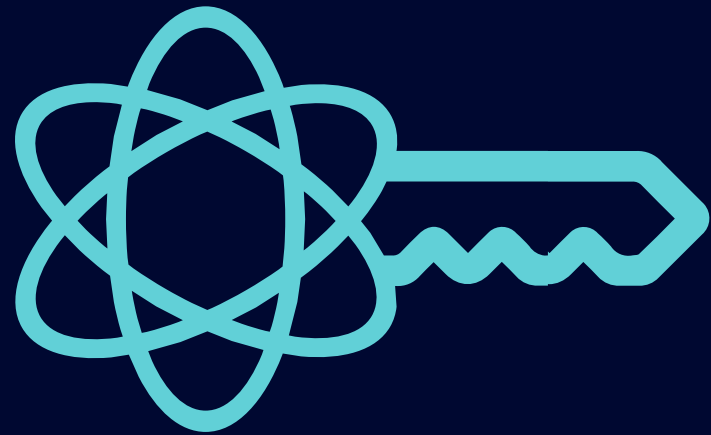


They align with ...

- European standards
- European data protection principles
- European digital sovereignty requirements

Our products

... are crypto-agile and PQC-ready



They allow for ...

- easy change of crypto algorithms
- migration to PQC

AGENDA

1. The challenge
2. The solution
3. Customer benefits
4. A look at our products
- 5. Conclusion**

Conclusion



- Eviden created a tailor-made security backbone for defense platforms
- Code-signing ensures supply-chain security
- Many other security applications are supported

**A success of Eviden's
products and
expertise**

Thank you

Kerstin Honskamp, Eviden Digital Identity