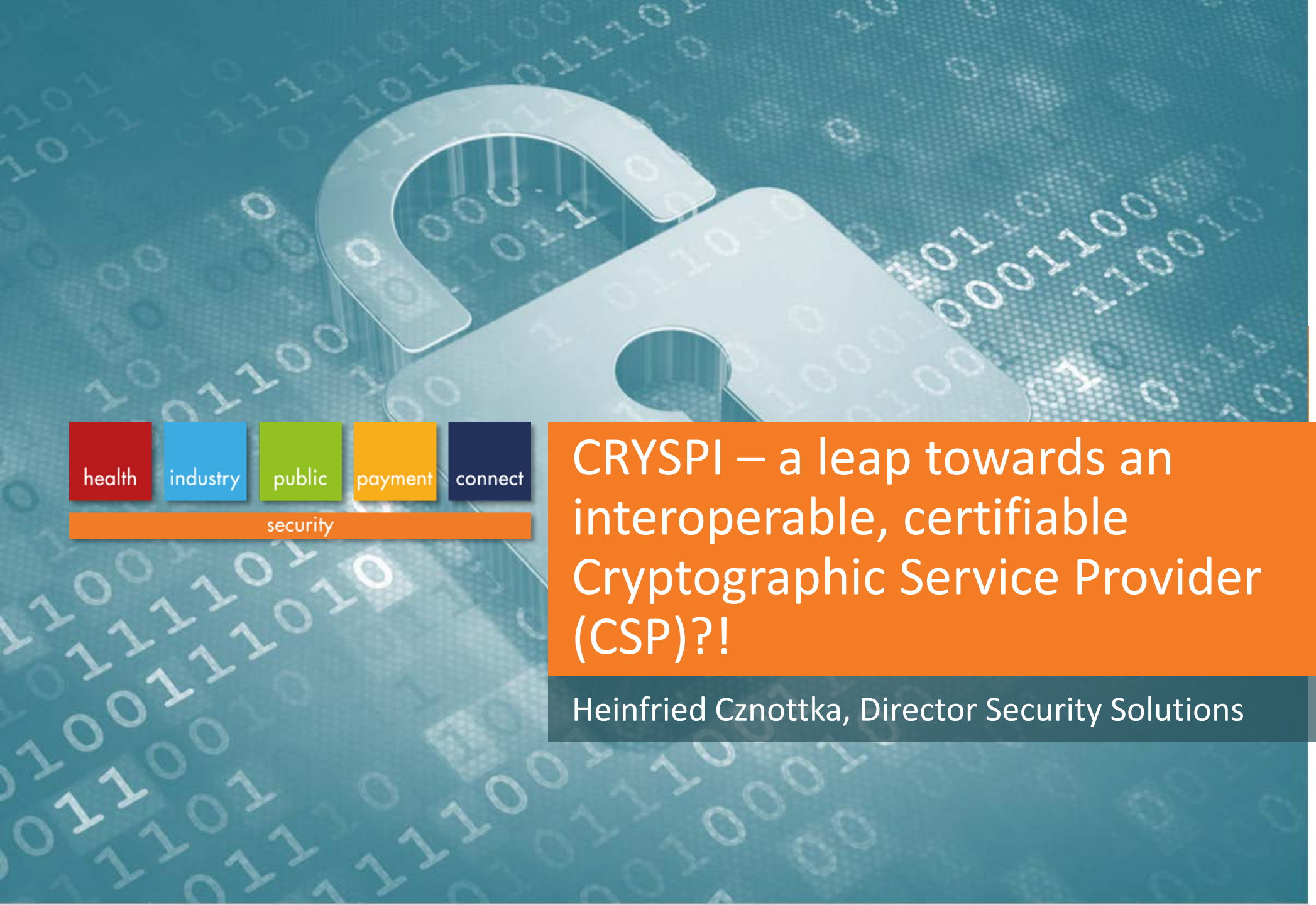


health industry public payment connect

security

CRYSPI – a leap towards an interoperable, certifiable Cryptographic Service Provider (CSP)?!

Heinfried Cznottka, Director Security Solutions

achelos

Integriertes Managementsystem ISO 9001 ISO/IEC 27001

Allianz für Cyber-Sicherheit Partner

SecurITy made in Germany

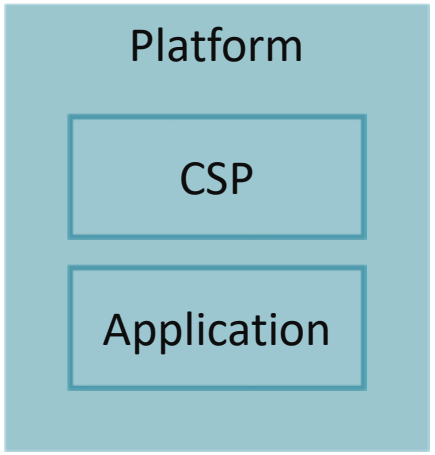
Trust Seal www.teletrust.de/itsmig

CRYSPI – What is CRYSPI?

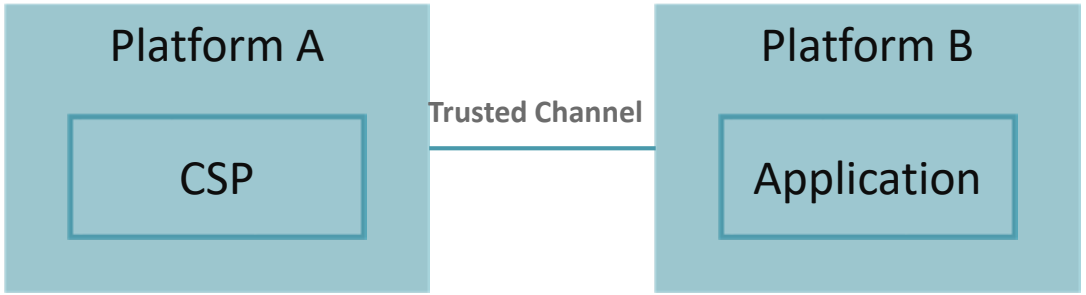
- BSI project
  - Prototypical implementation of a Cryptographic Service Provider (CSP)
  - CRYSPI is based on the draft of TR-CSP2 and
  - the existing security specifications (BSI-CC-PP-CSP)
- Main goal and motivation
  - Creation of a generic API interface description, test specification and executable tests on API level
  - Support implementation, certification and interoperability for secure applications

What has been achieved so far (1/3) ?

- CSP uses a generic approach, platform mode, client-server mode
- Focus on platform mode



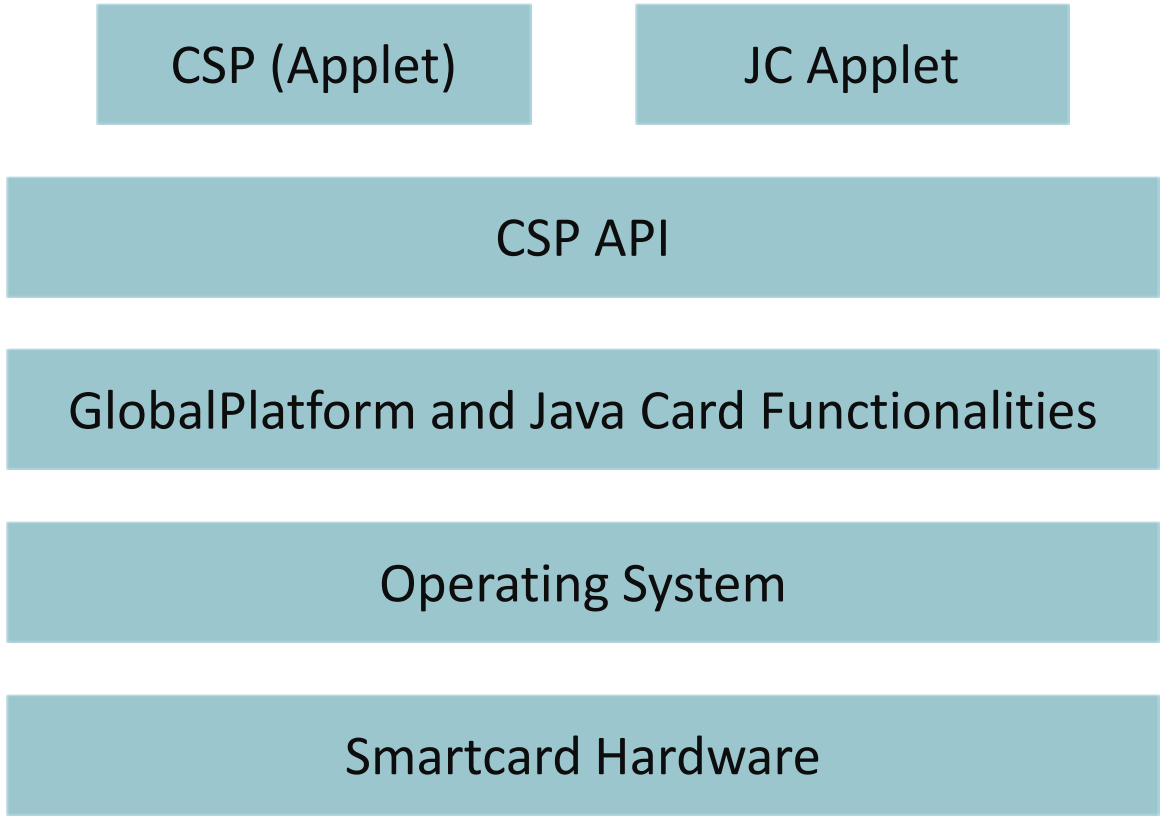
Platform mode



Client-Server mode

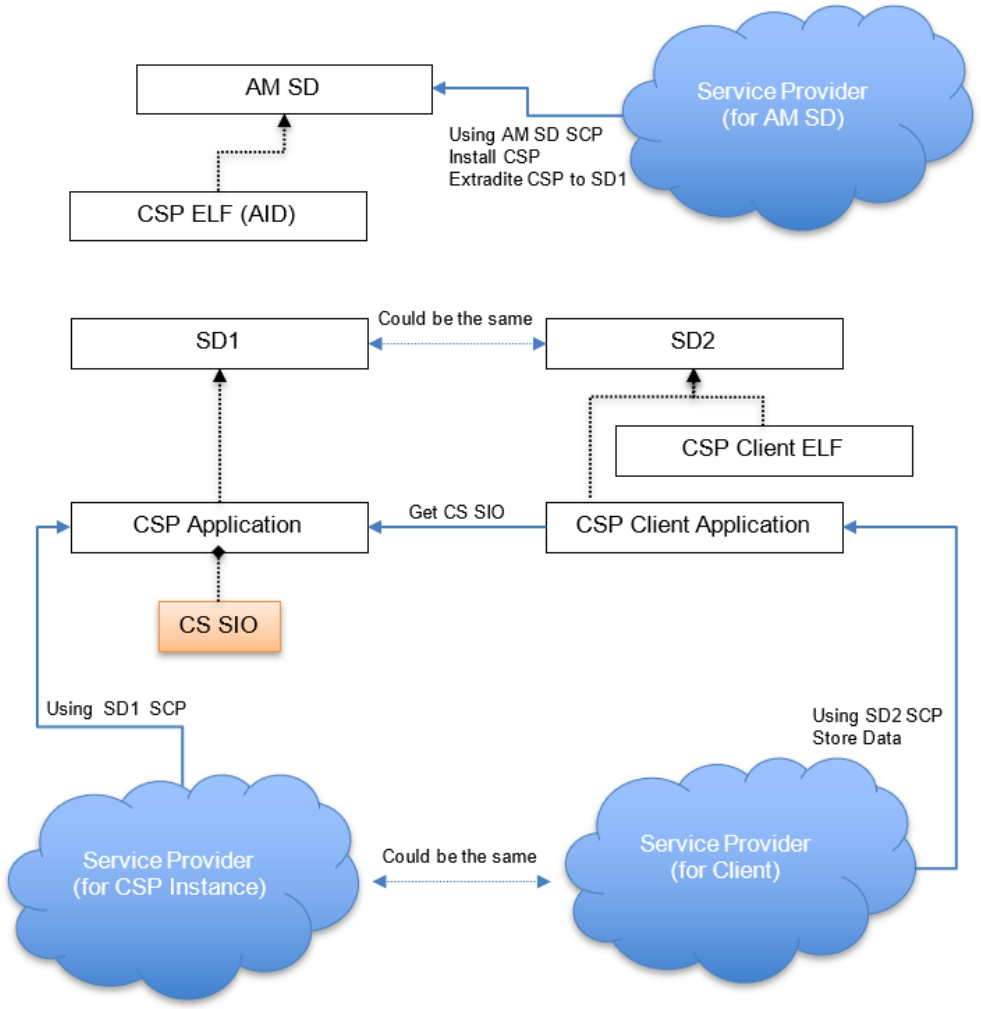
What has been achieved so far (2/3) ?

- CSP uses a secure element as basis
- Use/Reuse of technological standards from Java Card and GlobalPlatform
- CSP client applet as Java Card applet



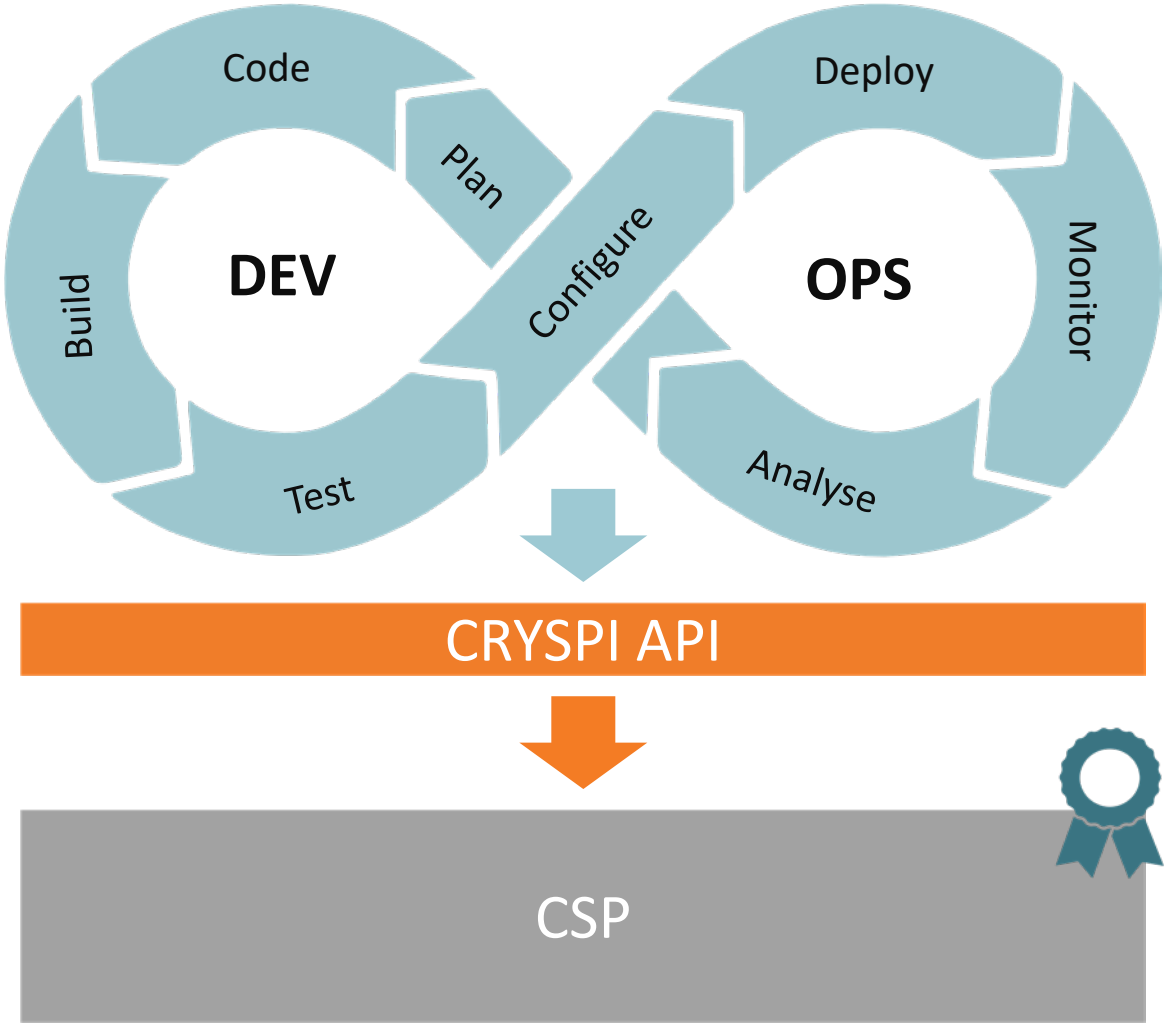
What has been achieved so far (3/3) ?

- System management architecture
  - Hardware and vendor neutral approach
  - Security domains act as the on-card representatives of off-card authorities
  - Security domains ensure separation between card issuer and service providers



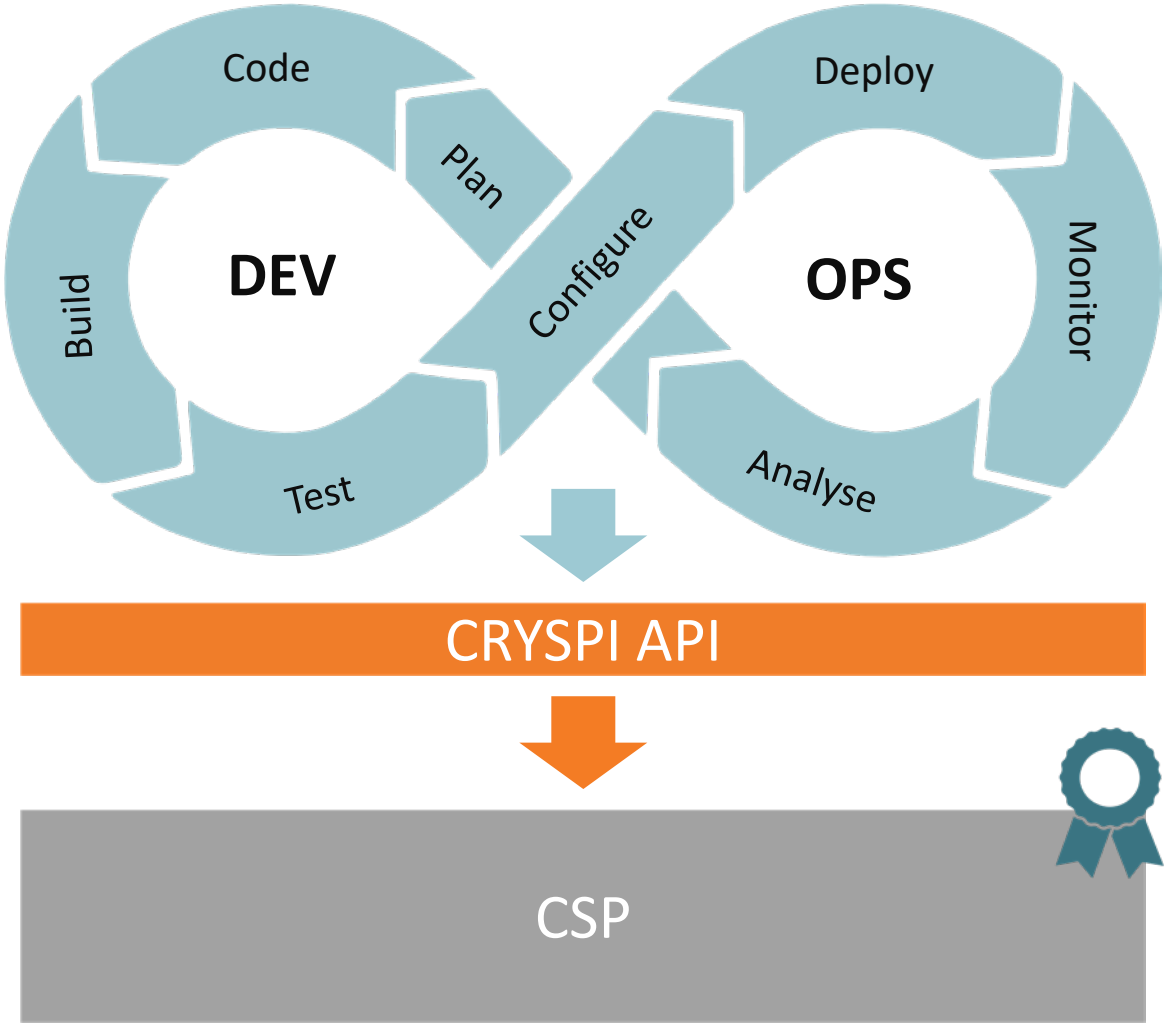
Requirements for developing secure applications

- Issues
  - Fast development cycles vs. need for certification
  - Lacking know how about crypto functionality and usage
  - High efforts for implementation of crypto functionality
  - Need to follow protection profiles (PP) and technical guidelines (e.g. TRs)
  - Time consuming certification process
- Solution
  - Secure foundation for Crypto functionality



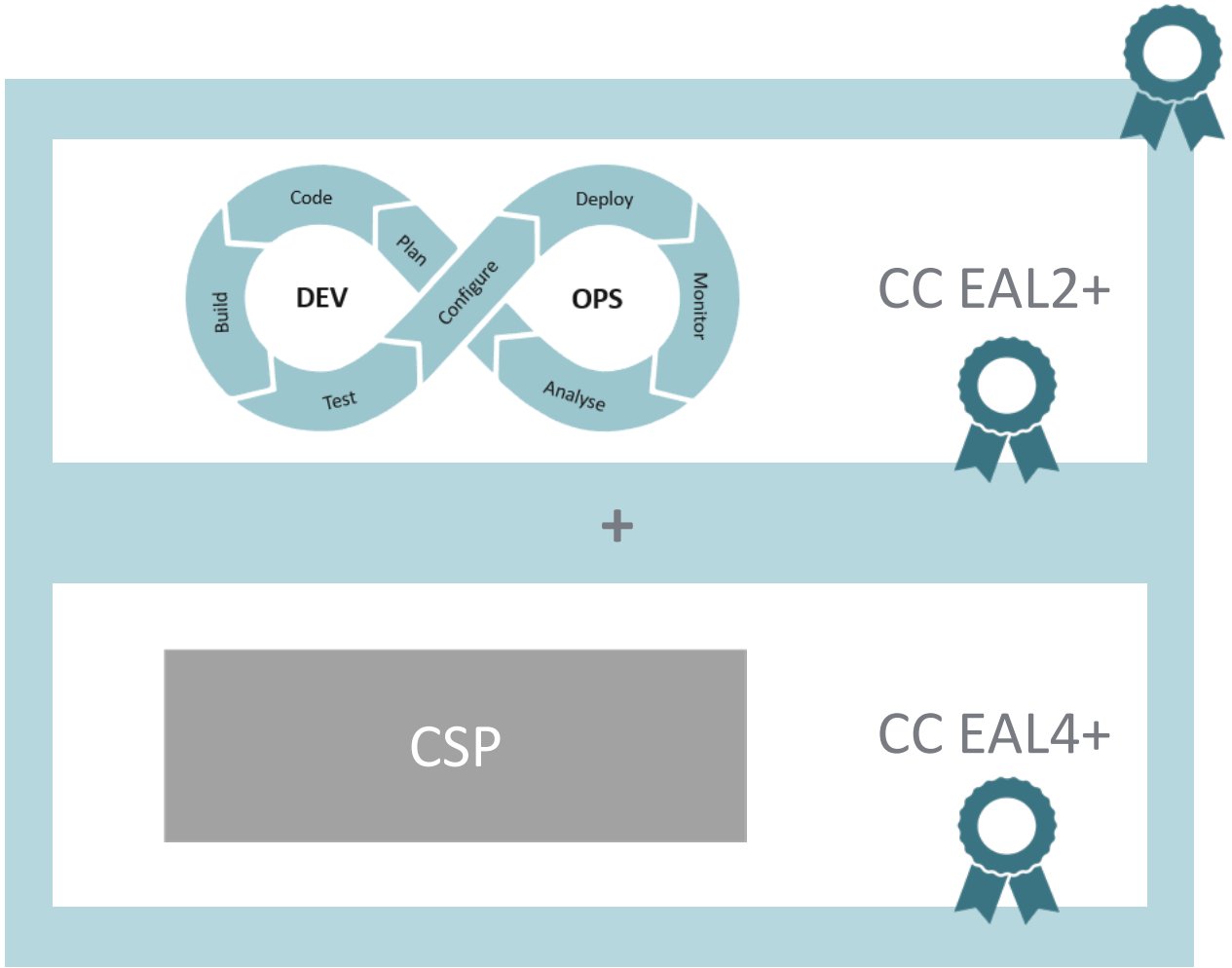
How does CRYSPI help with implementation?

- Faster implementation
- “Easier” usage of an API rather than developing crypto functionality
- No detailed crypto know how necessary
- Domain knowledge powers the application logic



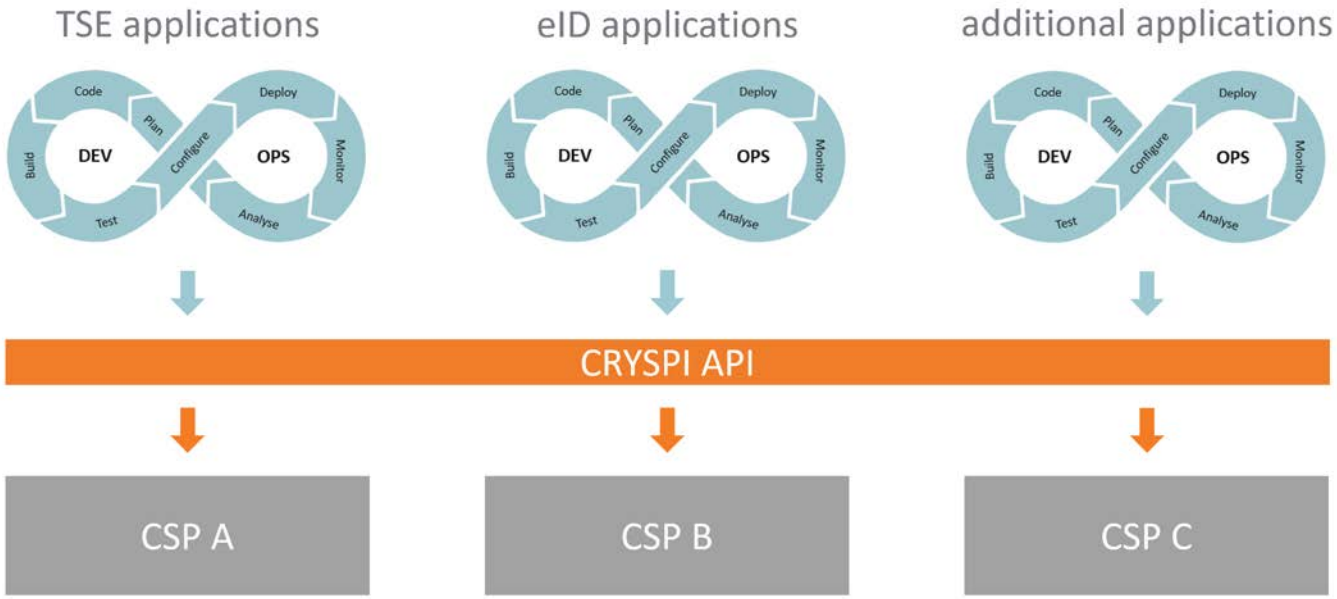
How does CRYSPI help with certification?

- Coordinated certification
- Application logic can be certified (e.g. EAL 2) independently from the CSP (EAL 4+)
- Time and money for the certification can be reduced significantly



How does CRYSPI help with interoperability?

- The application logic can be based on different implementations of the CSP
- Implementation can support different platforms and architectures



Conclusion

- CRYSPI helps to simplify and accelerate the implementation and independent security certification of applications based on a CSP while ensuring interoperability of applets for different CSPs!

- The API is published as open source
- The project can only succeed if the API is used!

Head office	achelos GmbH | Vattmannstraße 1 | 33100 Paderborn | Germany
Management board	Kathrin Asmuth, Thomas Freitag
Company	Manufacturer-independent system house for cyber security and digital identity management in Paderborn, founded in May 2008
Competences	Comprehensive IT security expertise with a specialist knowledge in cryptography, embedded development, PKI, telematics infrastructure (TI), eSIM management
Target markets	Security, health, industry, public, payment, connect
Offer	System integration, consulting, development, testing, security engineering, certification support, managed services, test suites & simulations, e-SIM management
Focus	Comprehensive IT security topics and industrial solutions for the national and international market
Customers | Partner	Private companies, government institutions and organizations with a need for cyber security solutions in security critical application fields

achelos

Vielen Dank! | Thank you!

Heinfried Cznottka – heinfried.cznottka@achelos.de
achelos GmbH
Vattmannstraße 1 | 33100 Paderborn | GERMANY
T +49 5251 14212-0 | info@achelos.de