ospt ALLIANCE

The OSPT Standard: CIPURSE™ Overview

5th June 2013
Bangkok

Jerome MONNOT

Table of Contents

Table of Contents

The OSPT Standard: CIPURSE™

- The OSPT Alliance is responsible for the Standards
  - The **CIPURSE™ Specifications**

- Principles throughout the CIPURSE specifications elaboration

1. Built on upon existing, proven and open standard
2. Reduced and fully defined feature set
3. Proven and State-Of-The-Art security

CIPURSE at a glance

- Command set and files system based on ISO/IEC 7816-4,-9
- Flexible file structure
  - Arbitrary number of files per applications
  - Arbitrary number of applications
- AES128 according to NIST Standard
- Flexible key assignment and security attributes
  - Security attributes individually per file and key
- Secure messaging with MAC'ing or Encryption
  - File/command individually secure messaging configuration
- Secured proven Protocol
  - Sequence integrity protection
  - inherently DPA/DFA-proof

CIPURSE Specifications

- The Core specification is defining
  - Mutual authentication scheme using AES128
  - Secure messaging (cryptography and APDU format)
  - Mandatory file types (binary, record, cyclic record, value)
  - Mandatory command set to operate these files
  - Keys and associated structure of file access conditions

- The Core specification is
  - RadioFrequency communication layer agnostic
    - Type A,B, C, …
  - Supported for optimized native chip as well as open JavaCard platform
  - Vendor & Provider independent

CIPURSE is an interoperable & Open framework by design

CIPURSE Architecture

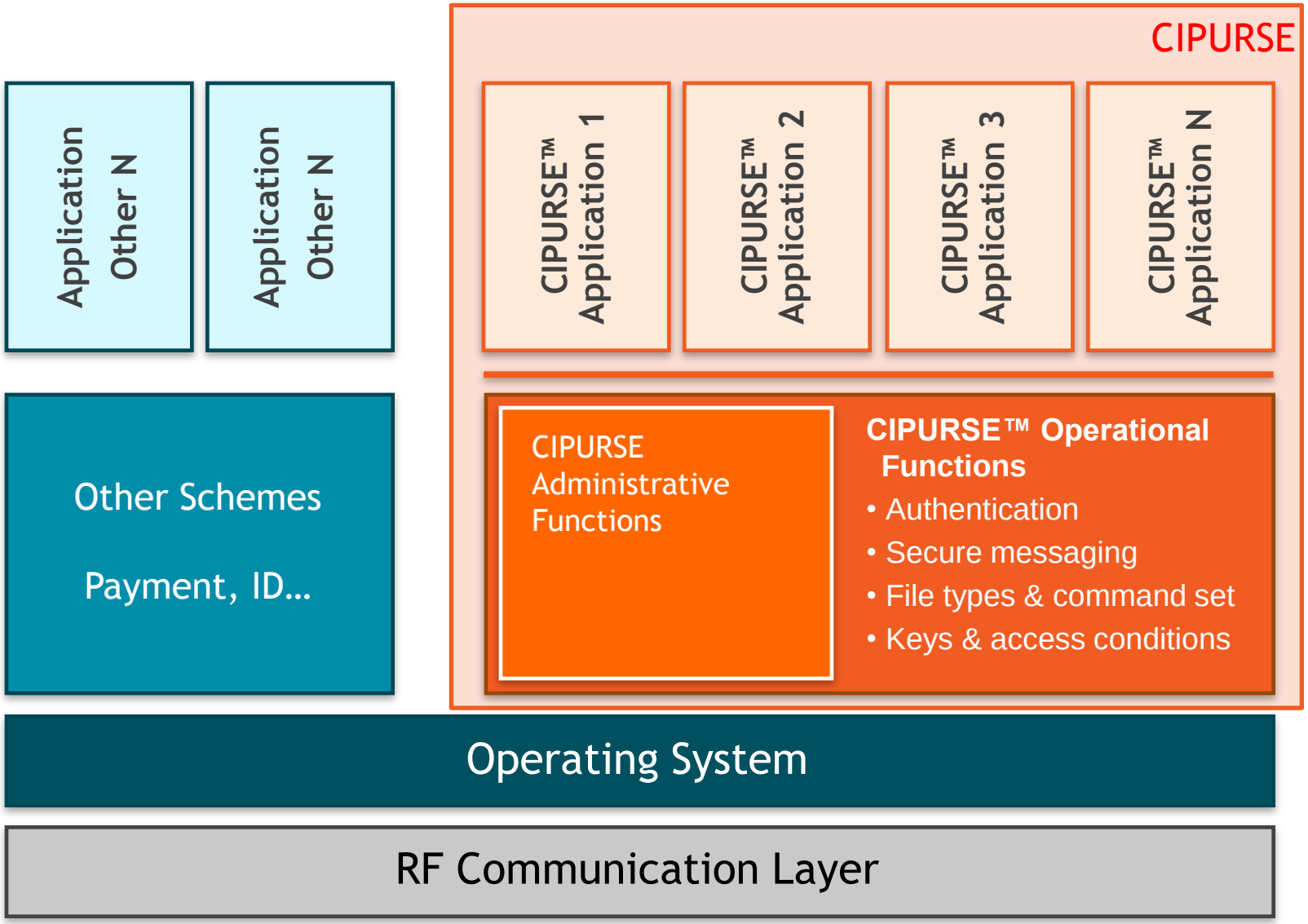


Table of Contents

CIPURSE™ V2 Family Concept

- Rationals
  - Diverse market requirements demand a broad variety of customer media
  - Avoid complexity of infrastructure to keep costs at affordable level
- Implementation
  - Core specification defining the technology
    - CIPURSE™ Operation and Interface Specification
    - CIPURSE™ Cryptographic Protocol
  - Several profiles defining media specific subsets
    - CIPURSE™ T, CIPURSE™ S
      - For rechargeable ticket applications supporting a specific number or time period of rides.

      or
      - For microprocessor-based transactions using smart cards, mobile phones and similar devices used in complex transit fare applications, such as monthly or annual tickets, multi-system tickets and loyalty programs
    - CIPURSE™ L
      - For inexpensive, disposable single-ride or daily ticket applications

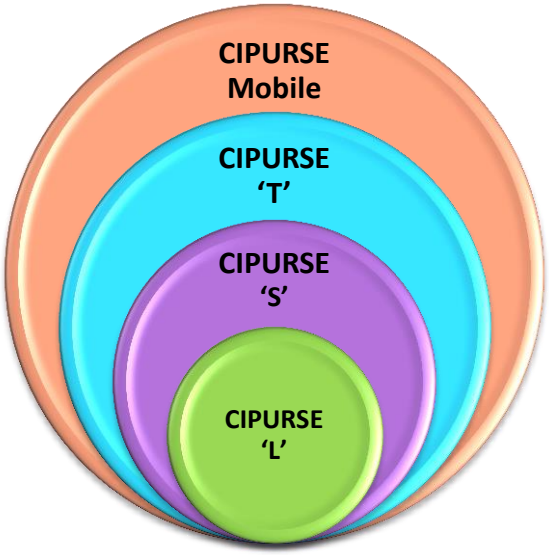
Scope of CIPURSE™ V2

CIPURSE™ V2 Specifications:

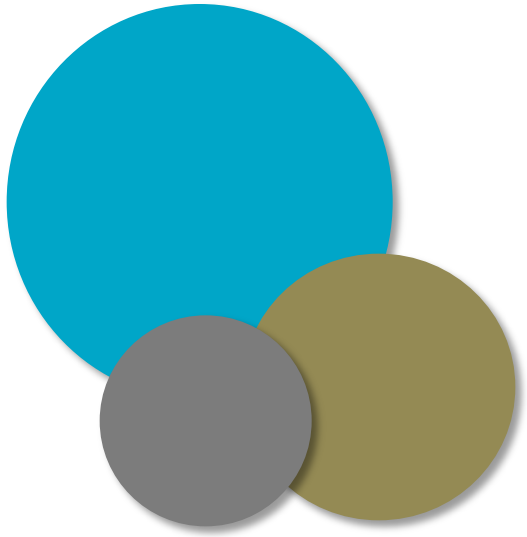
- Operation and Interface including
  - Personalization
  - Admin and Life-Cycle-Management
  - File structure
  - Command set
- Cryptographic Protocol
- Backward compatible with V1

- Profiles (Family concept)
  - CIPURSE™ L, S, T
  - User Memory minimal size requirement
- Java Card API specs
- SAM Specifications
- Key Management specs

CIPURSE V2 vs. Other Solutions



- CIPURSE products are **unified**, by design
- CIPURSE products are **scalable**
- All specification levels use same memory structure, command set, crypto algorithm and protocol
- Only CIPURSE guarantees coexistence of different specification levels (ticket types) running in one transportation ecosystem without changes
- CIPURSE allows switching between specification levels (ticket types) and form factors in the transportation ecosystem

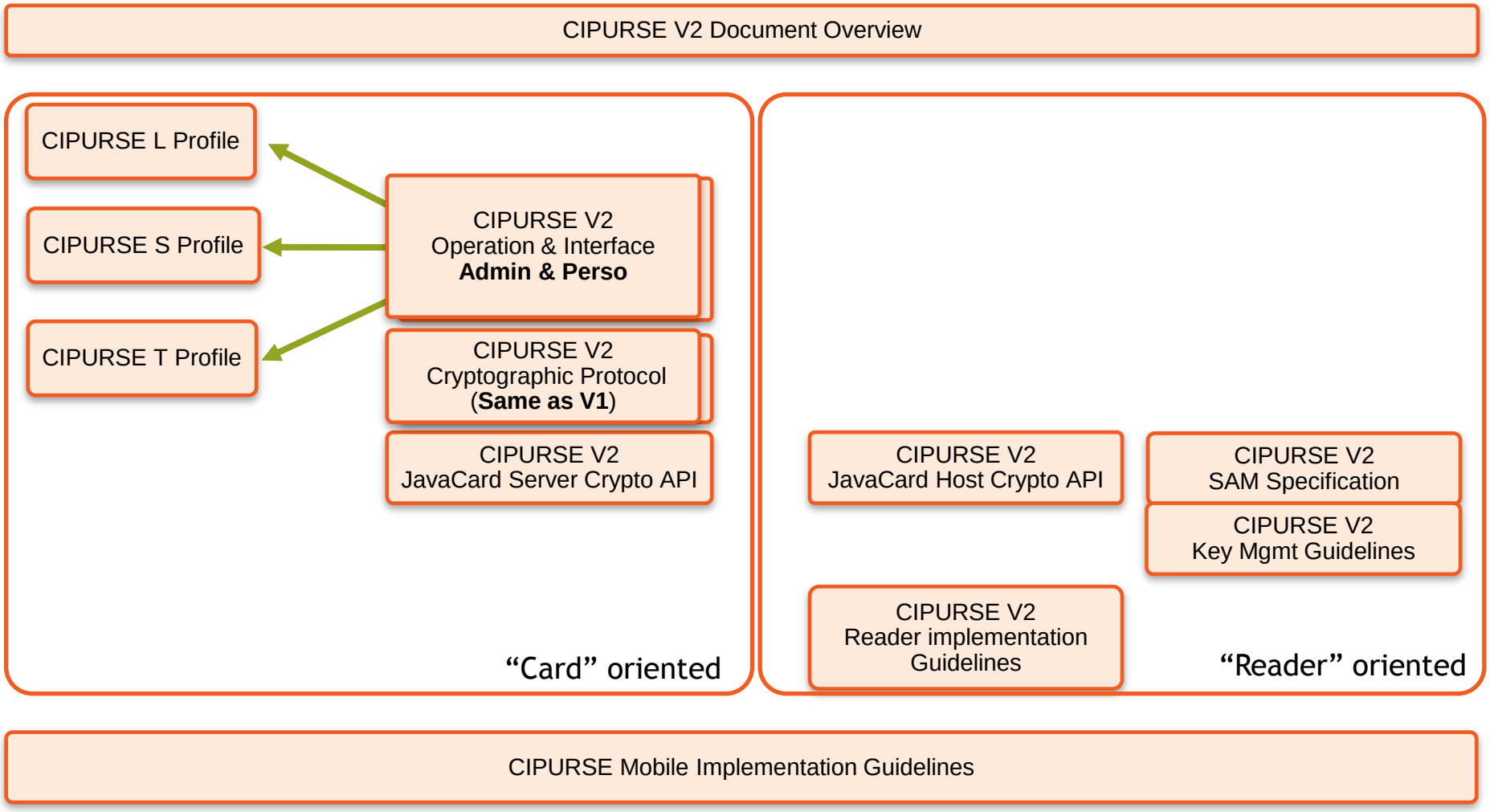


- Solutions are NOT scalable
- Product levels have different memory structures
- Different communication standards are used (e.g ISO 14443-3 and ISO 14443-4)
- Security algorithms and command sets are different in throughout the product levels
- It is not possible to use different product levels in the same transportation ecosystem without Software and/or Hardware changes. Expensive system changes are needed

Family Concept introduced in CIPURSE™ V2

- Subsets of CIPURSE™ V2 support application-specific profiles
  - **CIPURSE™ L**
    - Single-application profile with reduced file system
    - 2 AES Key set
    - AES Authentication + MAC'ed
    - User Memory: 256 Bytes minimum
  - **CIPURSE™ S**
    - Multi-application profile supporting several pre-defined applications
    - 8 AES Key set
    - AES Authentication + MAC'ed + ENC'ed
    - User Memory: 1024 Bytes minimum
  - **CIPURSE™ T**
    - Multi-application profile supporting consistent transaction mechanism
    - Same as CIPURSE™ S with On-Card Transaction Mechanism (i.e. Session atomicity)
    - 8 AES Key set
    - AES Authentication + MAC'ed + ENC'ed
    - User Memory: 4096 Bytes minimum

CIPURSE™ V1 and V2 Specifications



CIPURSE™ enables NFC-device/application acceptance

- Establishes standards for security and data structure for NFC-based applications and mobile devices – minimizing adverse impacts of proprietary and evolving NFC technologies
- Ensures seamless interoperability between NFC-based devices and contactless cards and readers
- Eliminates the requirement for back-end enhancements to accommodate NFC-based fare payments
- Creates foundation for self-service mobile sales and downloads of agency fare products

CIPURSE Benefits

- Especially designed for contactless card and NFC-based fare collection systems
- Vendor-independent (all card suppliers can support CIPURSE)
- Technology providers free to add functionality outside the common core (multi-application support)
- Incorporates advanced security based on AES standard
- Reader independent: Any compliant ISO14443 reader can be used
- All CIPURSE products undergo rigorous certification testing by third-party organization (Keolabs)

Table of Contents

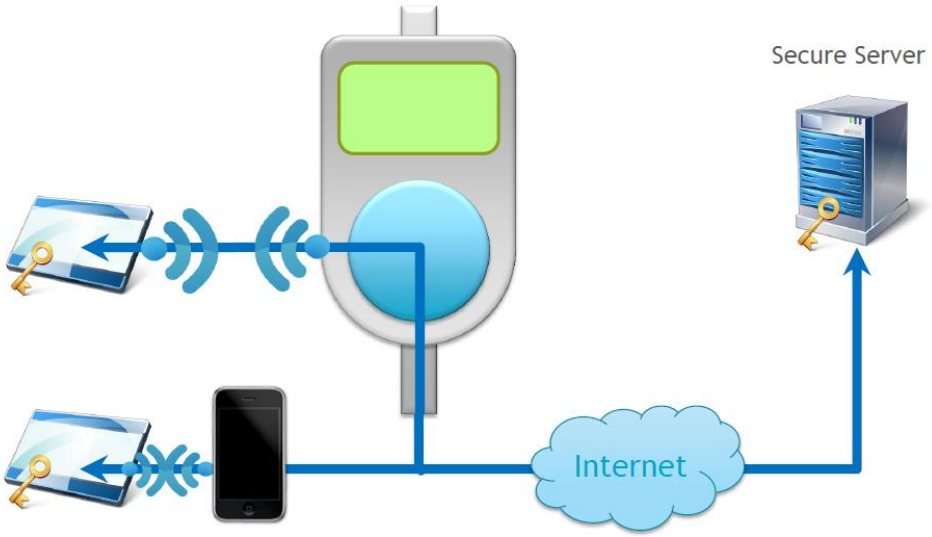
Cryptographic overview

- CIPURSE: The chosen security standard
- Based on AES-128 (NIST)
- State-of-the-art Security. Resistant to multiple attacks:
  - Brute Force
  - DPA (Differential Power Analysis)
  - DFA (Differential Fault Analysis)
  - Man in the Middle

- Scalable for products used in any application from limited used tickets to multi-application cards / Mobile

Cryptographic strength

- Robust Secure Channel
  - A Secure Channel provides a secure communication between 2 parts.
  - All communications may be Encrypted or Signed
  - A sequence number is used and incremented in each frame in order to avoid Man in the Middle attach
- 100% Secure Channel
  - None Command Vulnerability
  - Including KeyLoading phase



Authentication & Key Scheduling Principle

- Authentication
  - Three-pass challenge-response protocol (as per ISO9798-2)
  - Based on AES128 (NIST), including a pre-function invoked once
- Data exchange protocol inherently DPA and DFA resistant
  - During authentication, both parties agree on the “very first” session key k(i=0)
  - Key scheduling: With each data block transferred in secure messaging, a “new” session key k(i+1) is generated
  - The key scheduling “links” all transferred commands/responses together → sequence integrity protection
- No DPA-resistant AES implementation needed
  - Neither during authentication nor during data exchange the original key is vulnerable to DPA (given by principle)

Secure Messaging Principle

- Communication security levels
  - Confidential (“ENC’ed”): AES128 encryption + CRC32 integrity
  - Integrity protected (“MAC’ed”): AES128 MAC (8 byte)
  - “Virtually” integrity protected (“SM_PLAIN”): No MAC in message, but each endpoint pursues the key scheduling
    - SM_PLAIN messages are verified later on by MAC’ed/ENC’ed messages
    - Interleaving of “plain” messages in integrity protected sequence
- Configurability
  - For each data exchange, the PCD may configure the communication security level for the command and response separately
  - The PICC checks the applied communication security level based on “secure messaging rules” assigned to file objects, and responds accordingly
  - This enables adjustment of communication security levels to the security level of the environment (e.g. for privacy protection)

CIPURSE Crypto Protocol Awards

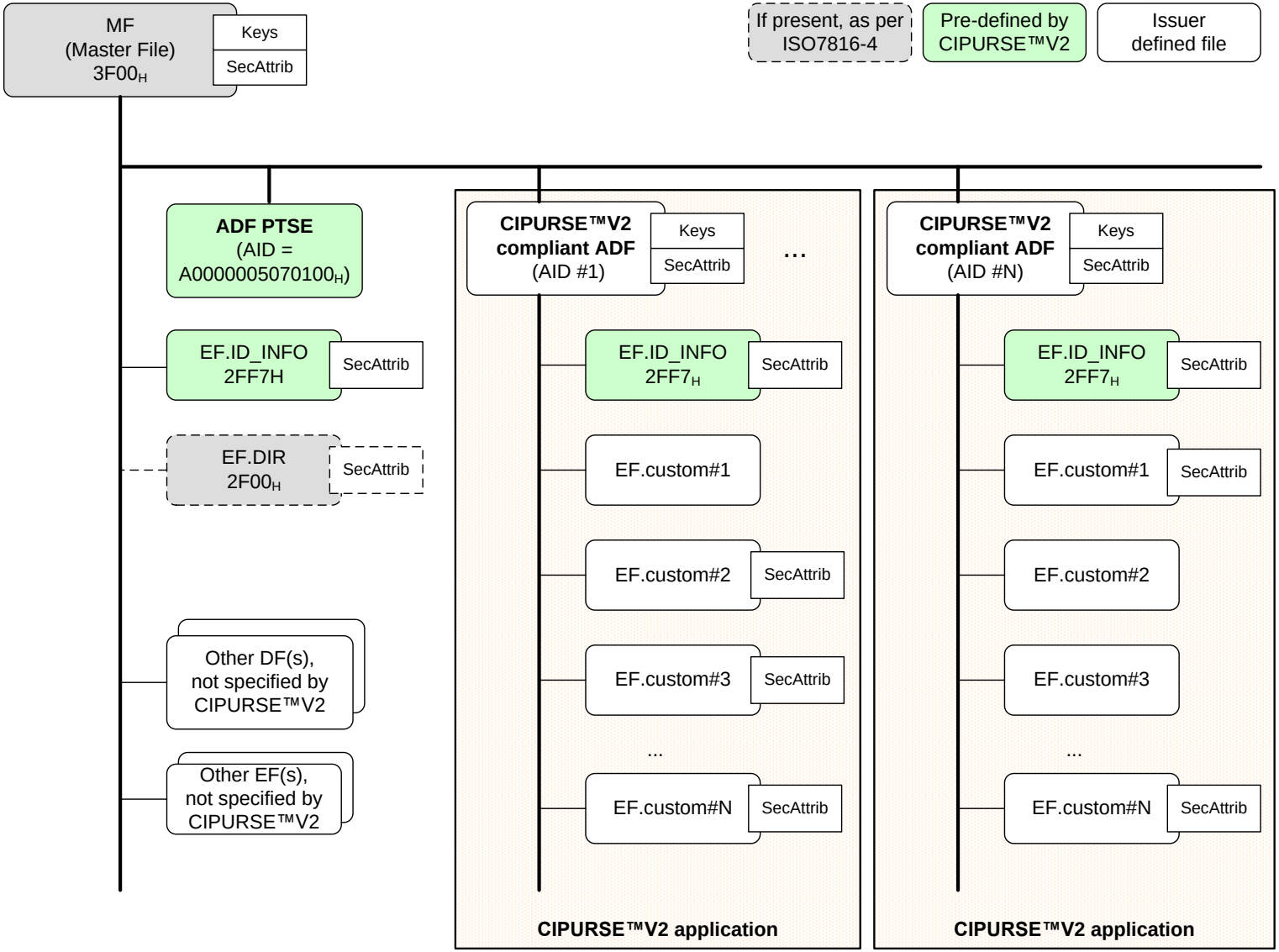
- 1st prize of the **German IT-Security Prize 2012** for the research project
  - *Cryptographic Protocol with Inherent Side-Channel Resistance, 29.11.2012*
    for B.Gammel, W.Fischer & S.Mangard

Table of Contents

Structure of a CIPURSE™ Application

- An application DF (ADF) hosts:
  - An arbitrary number of elementary files (EFs)
  - ADF security attributes: Access Rights and Secure Messaging Rules
  - Keys, key security attributes enable hierarchical structure
  - Selection of ADF by AID (as per ISO7816-4) supported, optionally by FID
- Supported file types
  - Binary, record, cyclic record (as per ISO7816-4); value record
  - Typical for transport and e-Purse applications
  - EF security attributes (Access Rights, Secure Messaging Rules) may be assigned to each file individually
  - Assignment of short EF identifiers (as per ISO7816-4) supported
- Pre-defined file EF.ID_INFO holds unique manufacturer data
  - Security attributes may be assigned for privacy protection
- Coexistence of “secure” and “non-secure” objects in one ADF

CIPURSE™ Application File Structure



CIPURSE™V2 Profiles

	CIPURSE™T	CIPURSE™S	CIPURSE™L
ADF PTSE	✓	✓	✓
Transparent File	✓	✓	
Linear Record File	✓	✓	✓[1])
Cyclic Record File	✓	✓	
Value Record File	✓	✓	✓
Transaction Mechanism	✓		
Authentication	✓	✓	✓
SM-MAC	✓	✓	✓
SM-ENC	✓	✓	
# of ADFs	8	4	1
# of keys in ADF	8	8	2
# of EFs in ADF	32	8	2
User data/bytes	4096	1024	256

[1]) Record size: 4, 8, or 16 bytes

Conclusion

A foundation for multiple services — Security scheme can be the basis for a variety of products and components across the entire fare collection system

Secure — Utilizes the 128-bit key length Advanced Encryption Standard (AES), complemented by superior secure messaging

Compatible with legacy systems — Based on the ISO 7816 smart card standard and the ISO/IEC 14443-4 protocol

Flexible — Common command set and architecture supports new schemes for transit fare collection, as well as common legacy applications

Form-factor independent — Works with variety of smart cards, as well as NFC-enabled phones secure NFC microSD cards, e-SecuredElement, SIM card.

Scalable — From transit-only to multi-application smart cards and NFC devices

Interoperable — Vendor neutral. Certified by independent third-party

ospt ALLIANCE

Thank you

For more information about CIPURSE™, please visit:
www.osptalliance.org