



SmartCards as electronic signature devices

Progress of standardization

Helmut Scherzer, CEN TC224/WG16 (Editor)
IBM Germany
scherzer@de.ibm.com

Active CEN working groups(today)

- ❑ TC224 : "Machine readable cards, related device interfaces and operations"

Chair: René Beltrando (FRANCE)

Secretary: Catherine Protic (AFNOR)

Active CEN working groups(today)

- WG6 : "Man Machine Interface"

Chair: René Beltrando (FRANCE)

Secretary: Catherine Protic (AFNOR)

- WG 11: "Surface transport applications"

Chair: Jürgen Wehnert (Germany)

Active CEN working groups(today)

- ❑ **WG15 : "European Citizen Card"**

Chair: Lorenzo Gaston (France)

- ❑ **WG 16: "Application Interface for SmartCards used as Secure Signature Creation Devices"**

Chair: Gisela Meister (Germany)

- ❑ **WG 17: "Protection Profiles in the context of electronic signature"**

Chair: Massimo Actis Dato (Italy)

ISO related standardization groups

- SC17/WG4 : "Organization, security and commands for interchange"

Chair: René Beltrando (France)

... responsible for the creation of the 7816-x smart card standards

History of prEN 14890

- ❑ **Initial documents**
 - EU directive for electronic signatures
 - ESIGN Workshop G1 “Security requirements for signature creation applications”
 - ESIGN G2 Procedures for Electronic Signature Verification
 - ESIGN Workshop F “Secure Signature creation devices” (Protection Profile)

- ❑ **Foundation of ESIGN-K group (12.7.2001)**
 - **Chair:** Gisela Meister (G&D), **Editor:** Helmut Scherzer (IBM)
 - Technical specification ESIGN-K (CWA 14890, Part 1 and 2) approx. 250 pages
 - **final delivery: March 2004**

- ❑ **CEN BT159 to decide future development**

- ❑ **CEN TC224 WG16 established** in response to the resolution number 693 approved by the 41th CEN TC224 Plenary meeting (**18.4.2005**)

Mission of TC224/WG16

□ The task ...

- Development & maintenance of CWA 14890
- Smart Card shall be able to produce a '**qualified electronic signature**'.
- Additional services to be supported (covered in Part 2)
- responsible for technical compatibility of standards developed under its authority. (Example ECC-2)

- Physical, electrical and transport protocol characteristics are out of the scope of this standard

Road Map of TC224/WG16

- ❑ As the first objective the CEN TC224 WG16 shall prepare a working draft for the new European Standard EN Application Interface for smart card used as Secure Signature Creation Device based on the CWA 14890 parts 1 and 2.
- ❑ This new standard is intended to support the concrete implementation of the European legal framework for electronic signatures
- ❑ This standard is specially expected to be the base standard by card personalized with Identification, Authentication and Digital Signature (IAS) services.
- ❑ The standard will enable the development of interoperable cards issued by any card industry sector.
- ❑ The standard will describe an application interface and behavior of the SSCD i.e. it should be possible to implement on e.g. native and interpreter based cards.
- ❑ The standard shall be compliant with other European standards developed in the framework of the European Directive 1999/93.

Road Map of TC224/WG16

- ❑ According to the previous division of the CWA 14890-1 and 2 the WG16 will produce **two separate working drafts**.

- ❑ Both working drafts shall be sent to the CEN TC224 Secretariat for circulation and ballot **not later than June 2006**.

Documents referring CWA 14890

- ❑ ICAO : Advanced Security Mechanisms for Machine Readable Travel Documents
- ❑ Identification card systems — European Citizen Card — Part 2: Logical data structures and card services
- ❑ Electronic Health Card Specification (Germany) - Part 2: Basic Applications and Functions
- ❑ Global Platform
- ❑ Internet search engine: "CWA 14890" ⇒ approx. 160 hits

Additions and modifications

- ❑ Chapter 3: Normative references
 - Update all documents to last available versions
 - Removed some references (e.g. DIN 66291)

- ❑ Chapter 4: Terms and abbreviations
 - minimum changes required (e.g. AES added)

- ❑ Chapter 5: Application selection
 - AID.ESIGN = `A0 00 00 01 67 || "ESIGN"`
 - Note: SELECT needs to be in clear when in JAVA cards

- ❑ Chapter 6: User verification
 - added the notion of sensor-on/off card

Additions and modifications

□ Chapter 7: Signature creation

- Refined the description of hashing
- Added functionality to modify hash template of current SE

□ Chapter 8: Device authentication

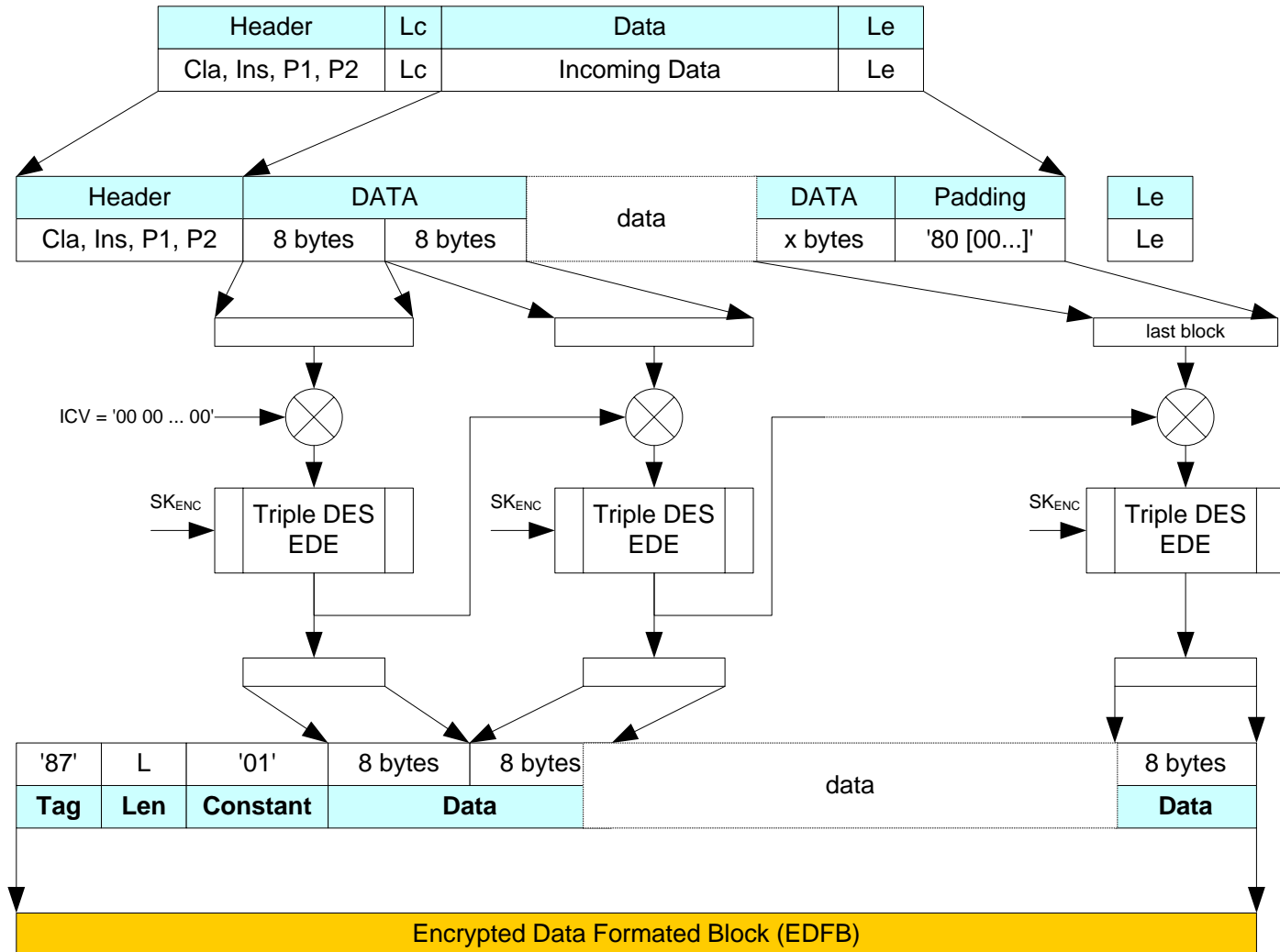
- Off-card sensor mandates device authentication
- Added privacy-constrained protocol
- Corrected 7F21 retrieval problem (according to ISO7816-4)
- Session key computation available with AES
- Post authentication chapter describes conditions that end the secure session.

Additions and modifications

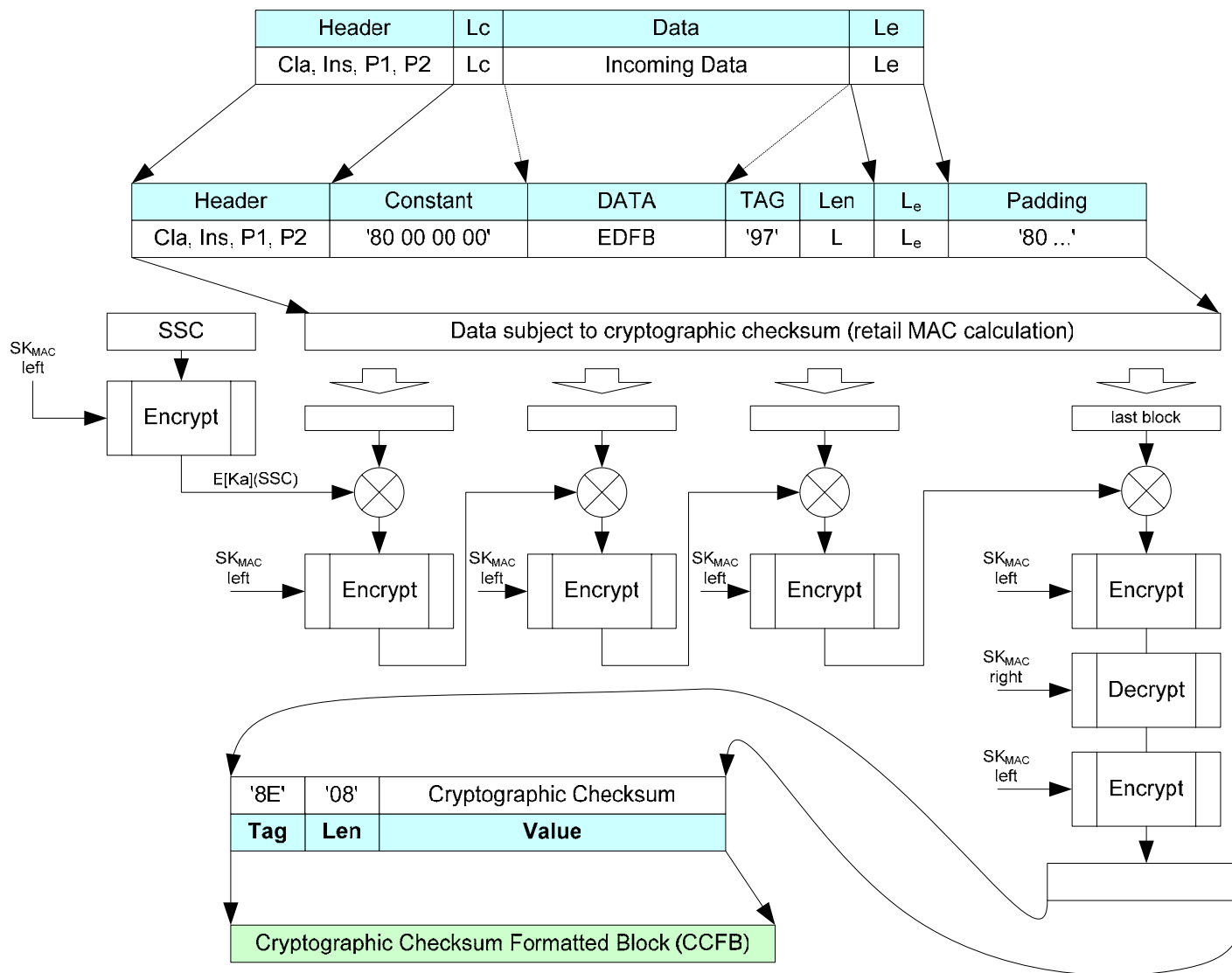
❑ Chapter 9: Secure messaging

- Odd/Even instruction codes are supported now
- Improved figures, taken from TC224/WG15 documents

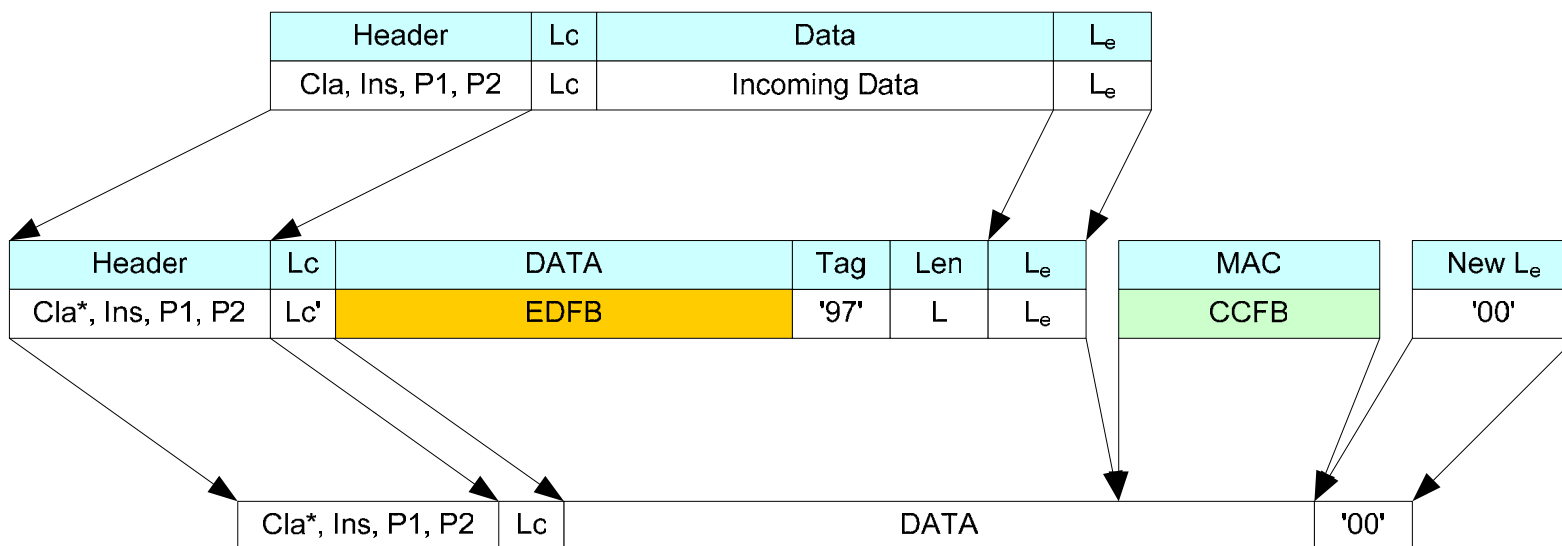
Command APDU creation (CG)



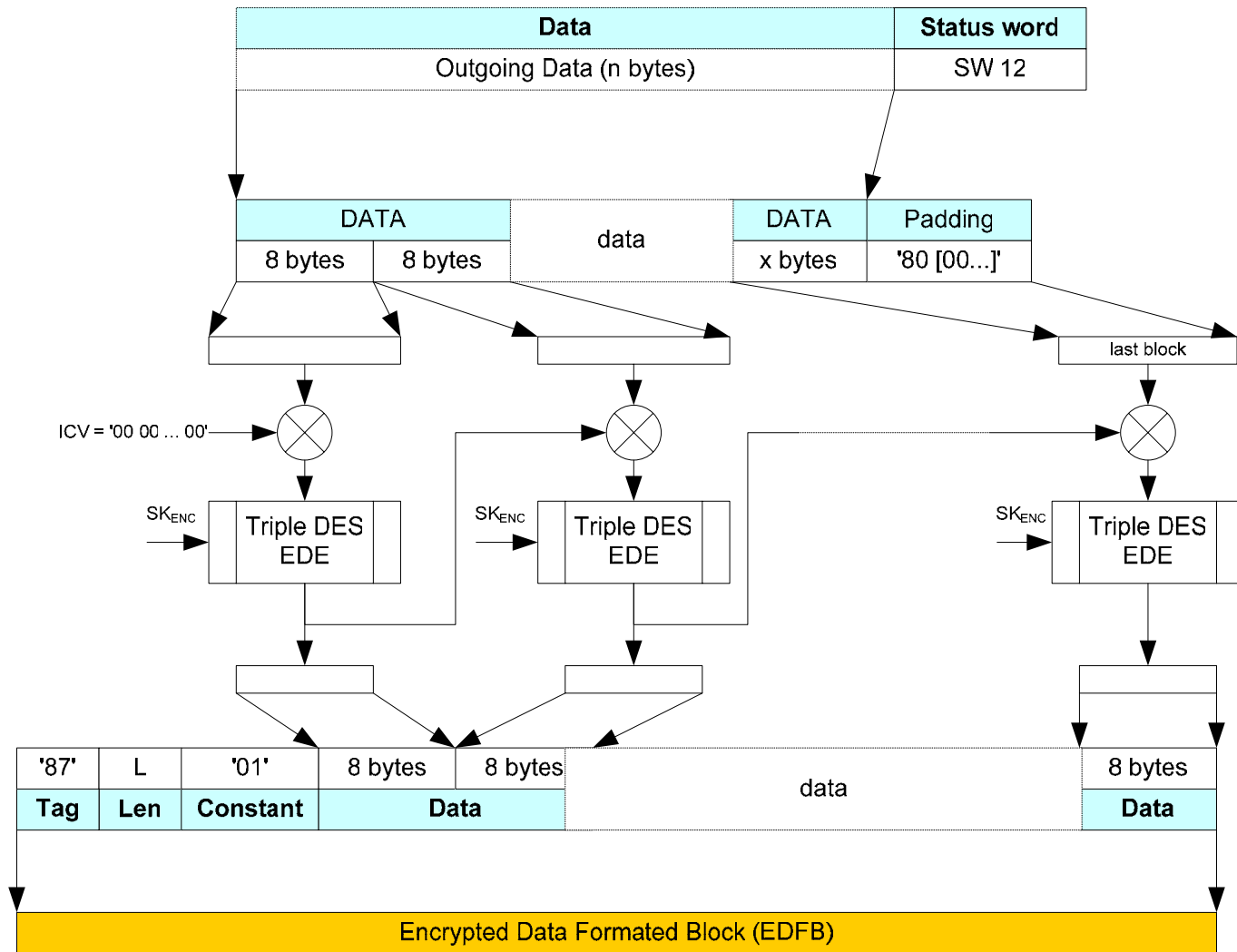
Command APDU creation (CC)



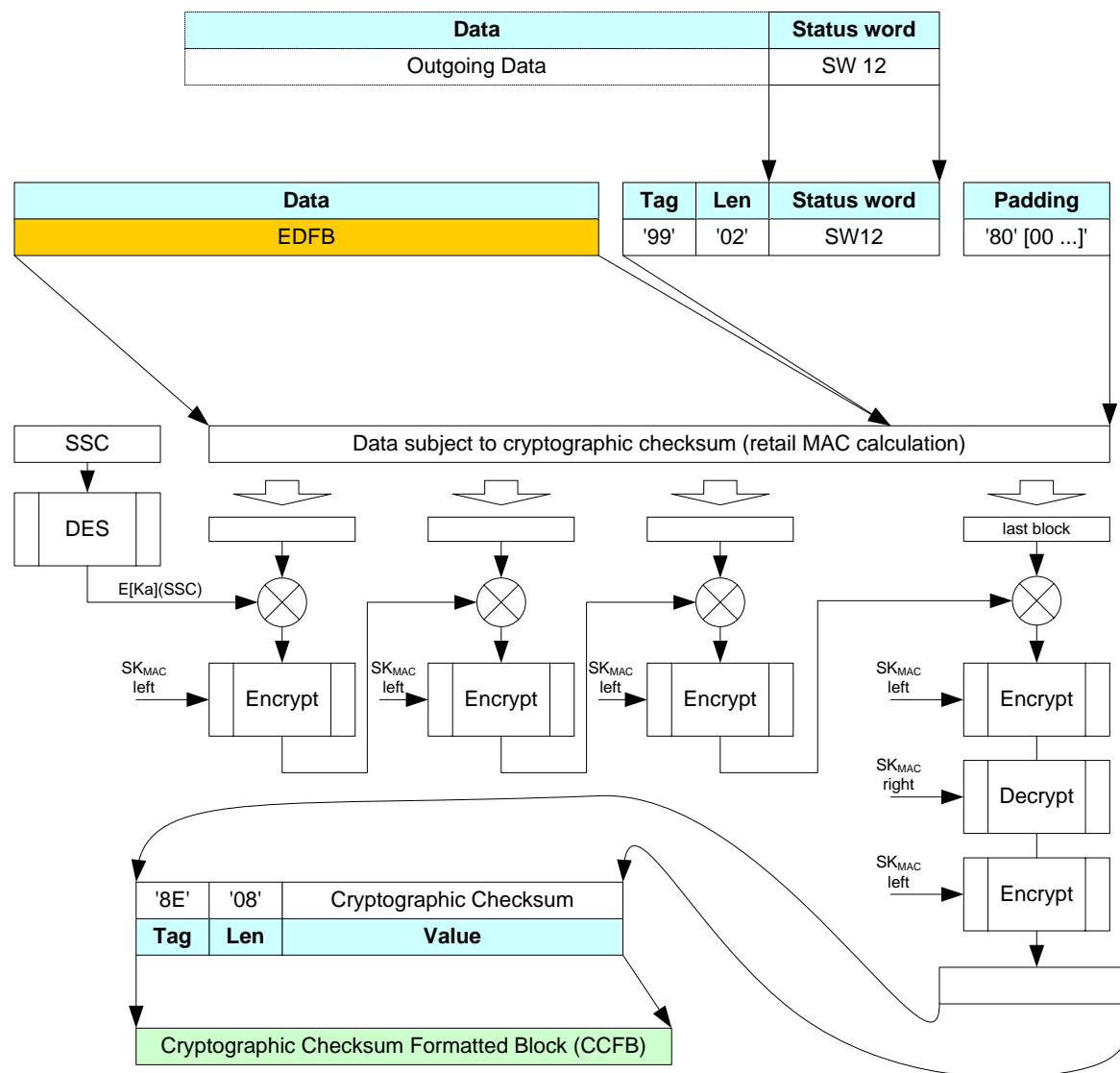
Command APDU creation



Response APDU creation (ENC)



Final response APDU creation



Additions and modifications

- ❑ **Chapter 10: Key generation**
 - Created an overview on the relevant chapters, related to alternative key generation schemes

- ❑ **Chapter 11: Key identifiers and parameters**
 - minor changes

- ❑ **Chapter 12: APDU data structures**
 - Added CRTs for key selection during device authentication

- ❑ **Chapter 13: AlgIDs, Hash- and DSI Formats**
 - SHA-224/256/384/512 and the appropriate object identifier

Additions and modifications

- ❑ **Chapter 14: Certificate Formats**
 - Card verifiable certificates chapters added
 - Improved description of certificate fields
 - New tables for role ID
 - New Certificate fields **CED** (Certificate Effective Date) and **CXD** (Certificate expiration date)
 - Certificate signature described according to WG15

- ❑ **Chapter 15: Files**
 - **EF.ELC** added for the privacy constrained device authentication

- ❑ **Chapter 16: Cryptographic Information Application**
 - To be replaced or removed - under discussion.

- ❑ **Annex 1:**
 - Added the cryptographic description of the privacy constrained device authentication protocol.

Some extra features

- ❑ PDF is cross referenceable throughout Part1 / Part 2
- ❑ Separation of execution flow and data content

prEN 14890 - Part 2

- Under construction
- First round, February 9th, 2006.

Next meetings CEN TC224/WG16

- 9th February 2005 in Madrid
- 21 – 22th March in France (Gemplus)
- 26th – 27th April in Berlin
- 7th – 8th June in Munich (G&D)

European Citizen Card (ECC) (WG15)

Information provided by Gisela Meister (G&D)

- **The European Citizen Card (ECC) provides**
 - **An MRTD (Machine Readable Travel Document) functionality according to the ICAO specifications and/or**
 - **IAS (Identification, Authentication and electronic signature) services based on CWA 14890 (E-Sign K specification)**

- **The ECC standard**
 - **is prepared by the technical committee CEN/TC224 'Machine readable cards, related device interfaces and operations' (WG15)**
 - **consists of the following parts:**
 - **Part1: ECC Physical, Electrical and Transport Protocol Characteristics (CD)**
 - **Part2: Logical data structures and security services (CD)**
 - **Part 3: NWI (Personalisation) & Part 4:Planned (Middleware)**
 - **is a technical standard, i.e. not mandated for national ID cards**
 - **is compliant with ISO/IEC 7816 and suitable for native & Global Platform (Java) cards**

ECC Part 2: Scope

□ Scope

➤ Interoperability for the citizen in the usage phase

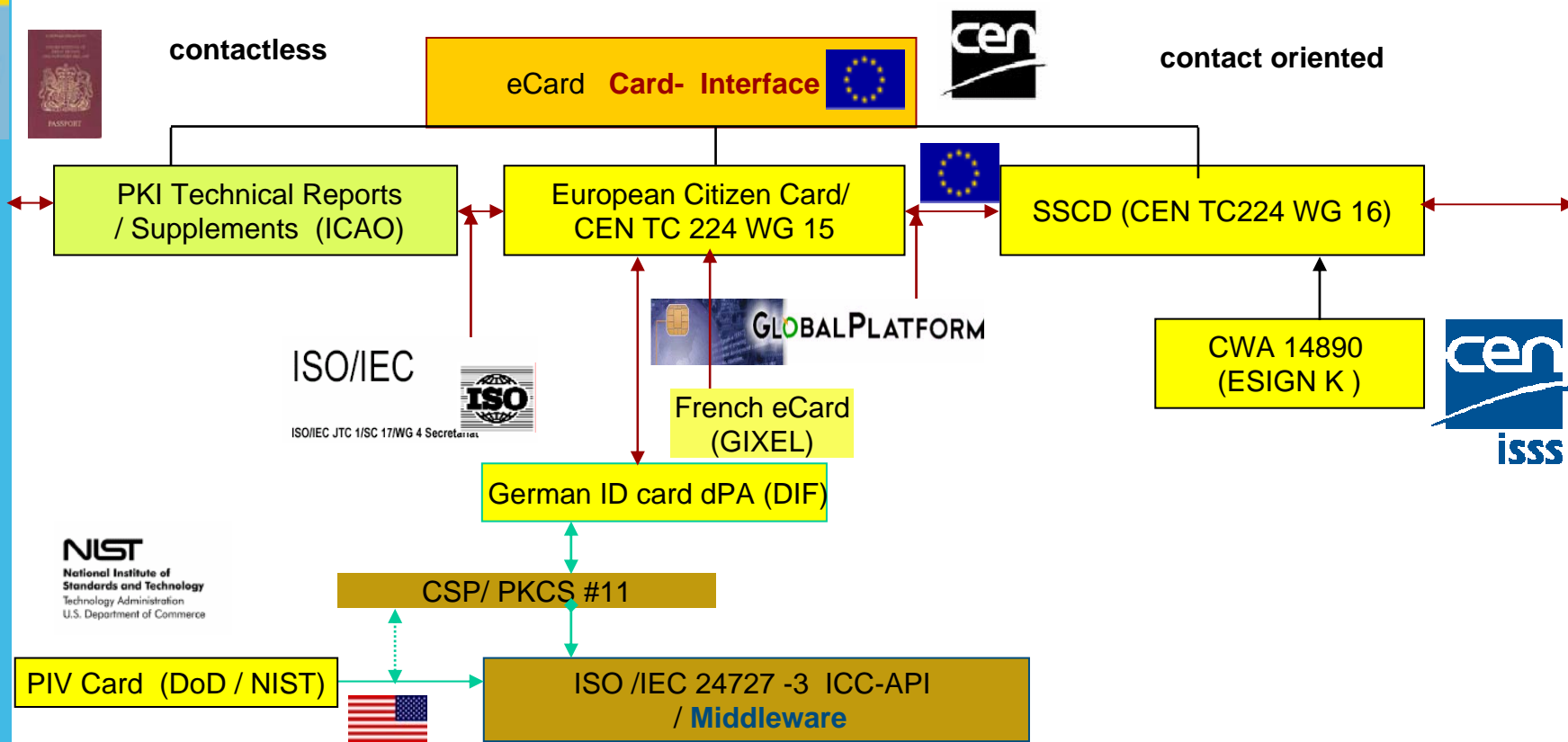
- Specification of security services for the MRTD application based on requirements/definitions of national authorities
- Specification of the IAS Services (not applications!)
- Specification of the card edge interface
- Definitions for extended length fields, logical channels
- Specification of the card capability description

□ Out of scope

➤ Card and application management

- Loading of applications (ISO/IEC 7816-13 not yet finalized)
- Administrative tasks in the usage phase
- Initialization / Personalization

Relation to other Standards and national eCard Projects



ICAO Security Mechanisms for MRTD Applications

❑ **Passive Authentication (mandatory)**

- Data of MRTD application are signed
- proves data authenticity

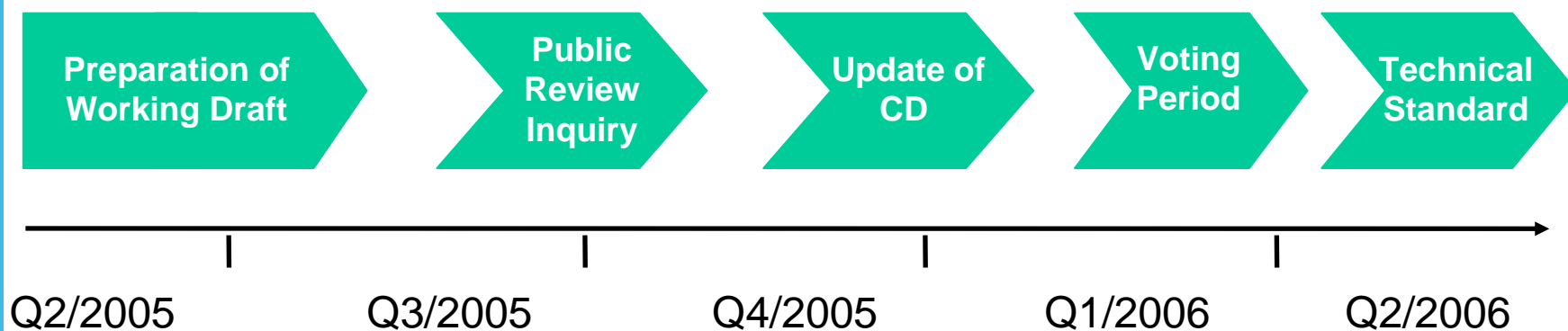
❑ **Basic Access Control (optional)**

- Retrieve key from MRZ (Machine readable zone) for symmetric device authentication with session key establishment
- prevents skimming and eavesdropping

❑ **Active Authentication (optional)**

- proves authenticity of ICC
- ICC signs IFD's random number with ICC specific private key
 - Problem: Tracing of citizen possible if random number has a semantic (e.g. contains information about place and time)

ECC Part 2: Roadmap



Summary ECC-2

- ❑ ECC-2 is a technical standard, compatible to
 - ICAO Technical report in case of use as MRTD
 - CEN CWA 14890 (CEN TC 224 WG 16), in case of use for IAS Services

- ❑ building the base for national ID card specifications as e.g.
 - the German ID card (dPA), its specification to be provided by the German Industry Association DIF
 - French Government Cards, their specification to be provided by the French Industry Association GIXEL

- ❑ ECC-2 is planned to be used together with Part 3 (Middleware API) of the International Standard Draft series ISO/IEC 24727
 - to provide interoperable Card Services for eGovernment applications