C-TAP Specifications
Introduction to C-TAP

Document C-TAP.000
Version 10.1 (1) Final
28 October 2016

CONFIDENTIALITY

COPYRIGHT

LEGAL DISCLAIMER

JURISDICTION AND APPLICABLE LAW

Table of Contents

Table of Figures

1. INTRODUCTION

1.1 C-TAP - A COMPREHENSIVE SET OF TERMINAL SPECIFICATIONS AND REQUIREMENTS

C-TAP is the abbreviation of Common Terminal Acquirer Protocol. The C-TAP specifications describe:

- The exchange of information with payment cards (EMV contact, contactless, mag-stripe) and alternate form factors of contactless cards and how these cards are recognised,
- The detailed flow for various types of transaction processing
- The association of a recognised card with an acquirer that will authorise and settle the transaction
- The data exchange with this processor
- The message and information processing requirement at the acquirers' host system

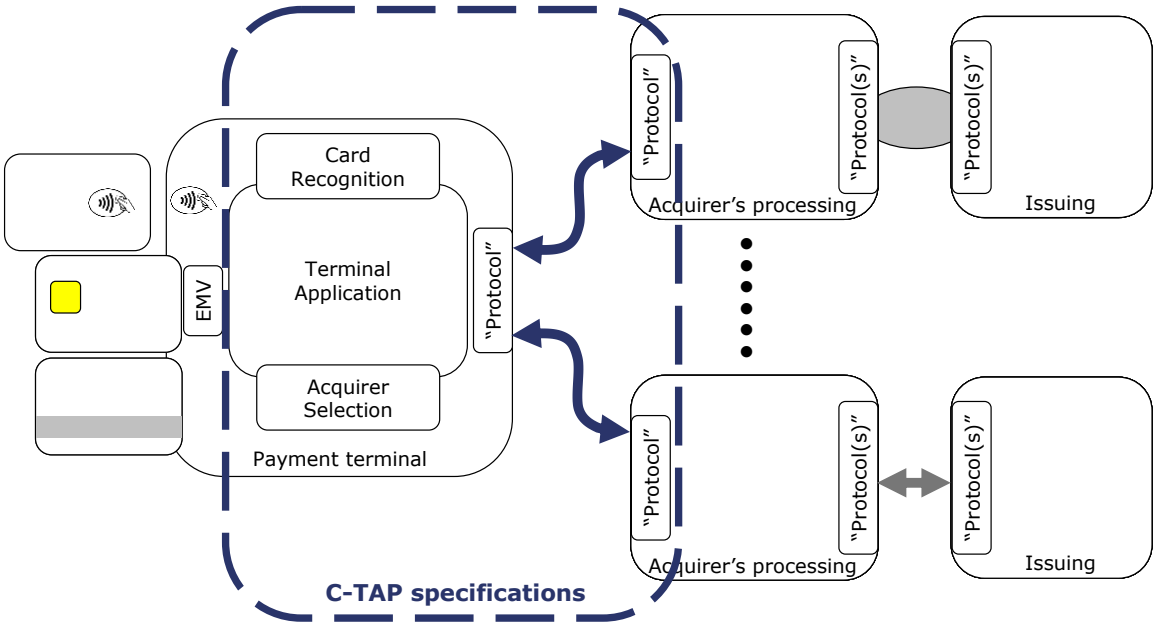

Figure 1 – Scope for the C-TAP specifications

In more detail, the C-TAP specifications indicate:

- Storage and management of card recognition criteria and multiple sets of instructions delivered by individual acquirers having a relationship with the merchant;
- The sequence of interactions with EMV smart cards on top of the EMV Level 1 and Level 2 specifications, as well as the reading of ISO tracks on magstripe cards;
- The support of the various CVM (Cardholder Verification Method) as personalised on the card by its issuer in combination with the directions delivered by the acquirer: clear text or encrypted PIN verified by the smart card, encryption and on-line verification of a PIN, signature or no CVM;
- The support of various modes of operation: on-line, semi-on-line and semi-off-line and off-line

- A range of solutions to guarantee message integrity and data protection
    - A specification called Terminal Secure Component (TSC) allowing for secure storage and management of multiple cryptographic keys and certificates for each of the acquirers that the terminal will access, both for cryptographic operations linked to the PIN control as well as to the secure data transport;
    - Mutual authentication between terminal and acquirer to provide secure transport over the Internet protected by TLS1.2;
- Interaction between the terminal supporting C-TAP and above mentioned acquirers having C-TAP acquirer host systems or arrangements with C-TAP acquiring processors;
- A comprehensive and multilingual cardholder and merchant guidance;
- Support for multiple standardised telecommunication technologies
- How acquirers or their processors communicate with their issuers is out of the C-TAP specification scope. However, as this communication is often regulated by card schemes, the C-TAP specifications will align with these requirements that call for data emanating from payment terminals or to be returned to payment terminals.

It is the objective of the C-TAP specifications to provide a solution to the processing of card transactions in SEPA. The principles contained in the present version of the standardisation work published as the "SEPA Cards Standardisation Volume - Book of Requirements" [ref: EPC020-08] by the European Payment Council (EPC) are followed. However, in some cases, the Acquiris stakeholders decide to slightly deviate from the standardisation volume. Where this "Book of requirements" is the result of a more theoretical discussion between multiple parties, the C-TAP specifications resulted from practical business requirements and C-TAP describes, in a very limited number of cases, alternatives that provide a more adequate response to Acquiris stakeholders' business requirements. These stakeholders of course remain open to a future alignment, if this would be beneficial to the C-TAP specifications users' community. A list of alternate implementations will be supplied once the "SEPA Cards Standardisation Volume - Book of Requirements" [ref: EPC020-08] is endorsed by the EPC.

1.2 ACQUIRIS AS A "SPECIFICATION PROVIDER"

The C-TAP specifications are licensed and managed by an independent organisation called Acquiris.

Acquiris aims to be an appropriate answer to SEPA for cards by maintaining and promoting a terminal specification which:

- is adequate for usage throughout SEPA and beyond and compliant with the core requirements as drawn up by the EPC and laid down in the 'volume'. The EPC and Cards Stakeholders published the "SEPA Cards Standardisation Volume - Book of Requirements" [ref: EPC020-08]. Acquiris issues a voluntary conformance statement for the C-TAP specifications to clarify that implementations align with the SEPA Cards Standardisation. In addition, these specifications offer functionality that matches with market requirements that have not yet been formulated in the "Volume". A document illustrates the conformance of the C-TAP specifications for POI connecting to acquiring host systems and the Acquiris role as "Specification provider" and "Certification Provider" with this "Volume". Acquiris will act as "specification provider" and apply for a compliance label once the EPC or the regulators have agreed on a certification procedure for specifications;
- operates on the principles of an open market, ensuring a competitive market situation with a level-playing-field for all parties;

- is open in it's governance by allowing all current and future C-TAP stakeholders to directly or indirectly decide on relevant issues;
- is cost-effective as the supporting organisation works on a non-profit basis and all stakeholders will participate in a cost-sharing agreement;

1.3 ACQUIRIS AS A CERTIFICATION BODY

Acquiris is mandated by the member acquirers and acquiring processors to certify payment terminals and associated devices against the C-TAP specifications. Acquiris will manage and facilitate the central certification body, liaise with card scheme bodies and accredit functional testing laboratories. Acquiris is a single point-of-entry for the certification and approval.

Acquiris includes a 'Certification Procedure' in its contractual framework with acquirers, acquiring processors and terminal vendors.

1.4 ACQUIRIS AS A CENTRAL ADMINISTRATOR FOR COMMON DATA AND AS A PUBLIC KEY CERTIFICATION AUTHORITY

Acquiris collects technical information such as Application Identifiers, BINs, telecommunication parameters from acquirers and acquiring processors. This information is subsequently disseminated to terminal vendors that will load this information in the terminals for initial card recognition and association with the merchant's acquirers as specified by the merchant-acquirer relations.

In addition, Acquiris will also have operated a Public Key Certification Authority to support the range of solutions to guarantee message integrity and data protection.

Both the Public Key based TSC and TLS1.2 solutions are flexible:

- Terminals are personalised at production and initial installation in a secure environment and provided with the credentials that demonstrate that they can be accepted by Acquiris acquiring host systems
- Hosts are provided with these same credentials so that terminals can determine that they connect to genuine by Acquiris acquiring host systems
- Both systems are flexible and more vendors / more acquiring host systems can be added or credentials renewed without have to recall terminals for re-personalisation in a secure environment

1.5 AUDIENCE

The *C-TAP Terminal Specifications* are aimed at acquirers, acquiring processors and vendors that wish to support these specifications for transactional processing.

There are two target audiences:

- the technical information is aimed at analysts and programmers;
- the procedural information is aimed at the operational management department.

Readers should have a general knowledge of cards payment, the applicable industry standards for smart cards and related data security as well as a basic knowledge of communication protocols.

2. FUNCTIONAL DESCRIPTION

2.1 DIFFERENT ROLES FOR DIFFERENT PARTIES

The Acquiris organisation defines the different roles that stakeholders play as well as their relation to the C-TAP specifications:

- It is a core objective of Acquiris to prepare and manage technical specifications for acquirers that offer to support transactional card payment services to merchants.
- Acquirers participate to card schemes. Card schemes are organisations that group issuers and acquirers of cards and define a contractual and technical framework for the processing of payments initiated by cardholders.
- Card schemes issue common technical specifications such as EMV for smart cards. They also issue security requirements such as the PCI standards. The European Payment Council has issued a "SEPA Card framework" that regulates how financial institutions in the SEPA issue and acquirer cards. Next to this SCF, the EPC published a book of requirements – presently called the "Standardisation Volume" – that set principles and rules for interoperability for SCF complaint schemes, e.g. for the messaging between terminals and acquiring host systems. Acquiris will therefore also take scheme rules into account when elaborating technical specifications for these schemes that Acquiris members require. Target schemes are global schemes, SCF compliant schemes and proprietary schemes.
- Merchants decide to accept cards from one or more schemes and therefore seek support from one or more acquirers.
- In many cases a card transaction is initiated on a payment terminal that in turn requires a connection to an acquiring host system for authorisation (when operating in on-line mode) and for settlement. As often many schemes will be accepted, this same terminal will connect to multiple acquiring host systems. Acquiris therefore issues specifications that allow doing so. These Common Terminal Acquirer Protocol or **C-TAP specifications** describe how a terminal will operate. In many cases a terminal will control card readers, a secure keypad for PIN entry, the cardholder display, a merchant unit and a receipt printer.
- Acquirers operate or have operated acquiring host systems conforming to the C-TAP specifications to the dialogue with certified C-TAP payment terminals. The further acquirers' roles include e.g. the forwarding of authorisation requests to issuers and the translation of the issuers' responses in proper action requests to the terminal. These systems will also keep transaction log files.
- Vendors of payment terminals implement devices that match the Acquiris requirements, i.e. that meet preliminary requirements such as described and certified by EMVCo or PCI SSC and correctly operate according to the C-TAP specifications.
- Acquiris manages the functional certification of payment terminals.
- Once certified, these terminals can be proposed to merchants either by the vendors or their distributors.
- Acquiris collects and disseminates sets of data from acquirers to terminal vendors or their distributors. These are referred to as the **C-TAP Common Parameters**. Acquiris also provides additional services, such as Public Key Infrastructure support for some message integrity solutions.

- Vendors or their distributors operate or have operated terminal management systems to feed data from the C-TAP Common Parameters to these terminals. These systems also store configuration data, such as the decision of the merchant to accept a given brand with a given acquirer. These systems also allow secure software downloads to terminals.
- For one the message integrity solutions, a Security Provider is required that dispatches sufficient key material to the terminal and the acquiring host system to allow the acquirer to safely store symmetrical keys in terminals.

2.2 HEADLINES OF THE C-TAP SPECIFICATIONS

2.2.1 Overview

An overview is provided on the main functions defined by the C-TAP specifications

- The management by parameters
  - At initialisation, derived from the C-TAP Common Parameters
  - Customised by each acquirer
- The modes of operation
- Card entry modes
- Application and acquirer selection
- The transactional support
- Exchange of financial counters
- Transactional security
- Data communication

2.2.2 Management by parameters

2.2.2.1 Common parameters more in detail

To correctly operate card recognition and acquirer selection the terminal needs to be fed with systemic data (the C-Tap Common Parameters) on card identifiers, brands, acquirer information etc. Common parameters are bound to evolve in time and vendors and their distributors engage themselves to dispatch changes to all the terminals under their control.

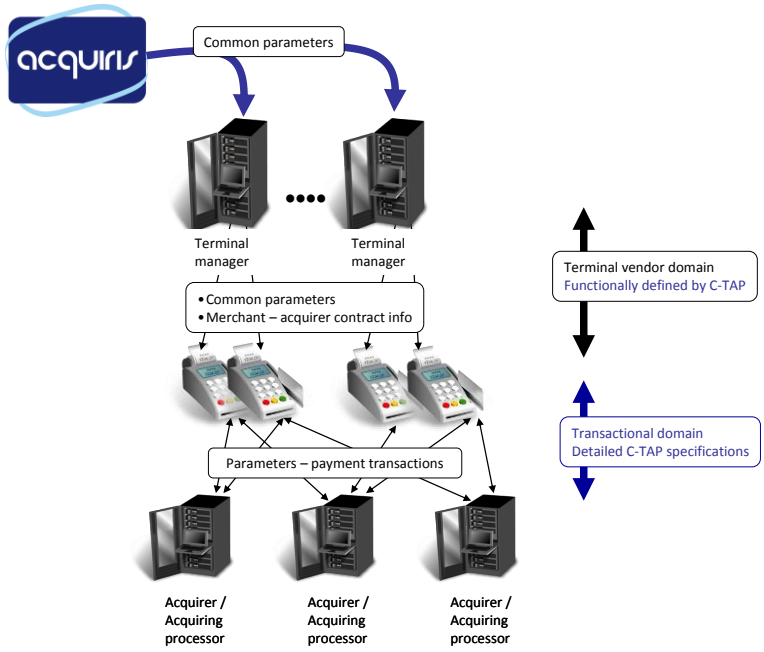

Figure 2 - Common parameters and their utilisation

Main data elements are:

- Card identifiers
  - Application IDs for smart cards
  - BINs and IINs for mag-stripe cards
- Brands
  - Scheme or commercial names for card brands
- Acquirers or their processors
  - Organisations that offer to process cards from schemes / brands to merchants
  - To each acquirer are associated a substantial number of technical parameters such as telephone numbers, urls and port numbers, technical data on modem standards, etc
- Security providers to which are associated a substantial number of technical parameters such as telephone numbers, urls and port numbers, etc
- A table of certified terminal vendors and their distributors, terminal types and terminal management systems identifiers
- Various other tables containing e.g. datacom supplier identifiers, scheme public keys, etc

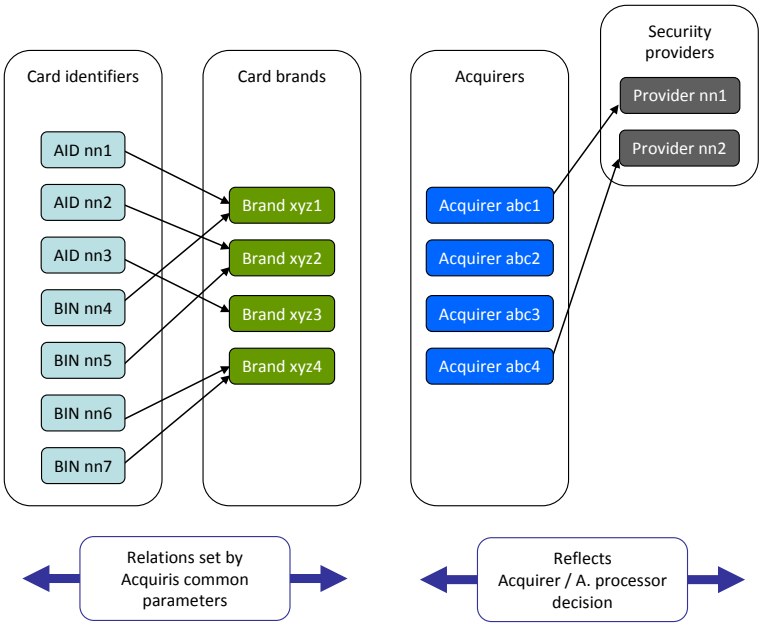

Figure 3 - Setting out the potentials for cards

2.2.2.2 Configuration of terminals

Once a terminal has been fed with the common parameters the actual configuration can be operated to reflect the merchant's decision to accept certain brands with certain acquirers.

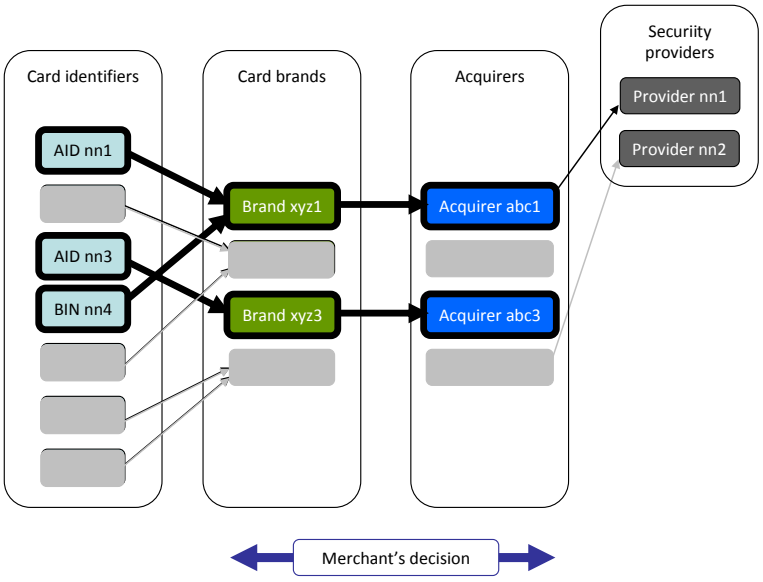

Figure 4 - Associating cards ID and brands to acquirers

The configuration can take place at the terminal or by remote configuration from the terminal management system.

2.2.2.3 Acquirers will further shape their individual transactional profiles

Once a relation has been made between brands and acquirers, the C-TAP specifications allow the terminal to collect additional parameters from each of the acquirers, to shape the individual transactional profiles, provide additional information and override setting by default.

To align with the merchants' contracts, each acquirer will define:

- which security mechanism will be used

- which services/functions are allowed for which card entry modes and by which CVMs
- sets of rules for transaction processing
- rules for output shaping (e.g. PAN truncation)
- rules by brand
- and many more …

As a result, the C-TAP terminal will have a specific behaviour for each acquirer as the C-TAP terminal connects to a specific acquirer in line with those acquirers' instructions.

2.2.2.4 Geared for change

Changes in merchants contracts can at any moment be reflected in the behaviour of the terminal by updating the links between card brands and acquirers

In addition, when systemic changes occur, these changes can be delivered to the terminals over their link with the terminal management systems. This allows the C-TAP terminal to accept new brands and to recognise cards on the basis of new identifiers.

2.2.3 Card entry modes

Different card entry modes are supported

- Magstripe support by reading the ISO-2 track
- EMV smartcards support, requiring the terminal to be certified by EMVCo
- Contactless chip for the EMVCo defined kernel services currently demanded by the market.
- Manual Entry of card number or, where relevant and as an optional function, by keying in a previously assigned token that the acquirer associated with a transaction

2.2.4 Cardholder verification methods

- No verification – the fact that the card data are supplied is sufficient to process a transaction
- Signature – the cardholder will be requested to sign a merchant ticket to confirm the transaction
- Off-line PIN - Local verification in the smartcard of PIN data entered by the cardholder on the terminal's PINPAD
    - In clear text – the PIN data are transmitted to the card without encryption
    - Encrypted – a session key is exchanged between card and PINPAD and the PIN is encrypted using this session key
- On-line PIN - the encrypted PIN data are transmitted to the acquirer for verification by the issuers or a stand-in
- On-Device Verification – the cardholder will be requested to provide identity verification using the mobile device that is used to perform the contactless transaction.

2.2.5 The modes of operation

The C-TAP specifications allow for different modes of operation

- On-line authorisation
    - Once the card is recognised the terminal will start transaction processing and during the course of transaction request the authorisation from the acquiring host.
    - Once the transaction is completed, the terminal will advise the acquiring host

- When the terminal cannot connect to the host, the processing of transactions will not be possible

- Off-line authorisation with the potential to authorise on-line (semi-on-line mode)
  - Once the card is recognised the terminal will start a local transaction processing based on the instructions received from the acquiring host at initialisation, information provided by the card, the transaction amount and a local black-list. The card transaction can either be processed, declined or the acquirer will be requested for an authorisation as for the on-line processing.
  - Once the transaction is completed, the terminal will advise the acquiring host.
- Off-line only authorisation (semi-off-line mode or off-line mode)
  - Once the card is recognised the terminal will start a local transaction processing based on the instructions received from the acquiring host at initialisation, information provided by the card, the transaction amount and a local black-list. The card transaction can either be processed or declined or the acquirer will be requested for an authorisation as for the on-line processing for the semi-off-line mode.
  - Once the transaction is completed, the terminal will advice the acquiring host either by a transaction-per-transaction dialogue or in batch mode

2.2.6 Terminal Types

- Attended terminals - the terminals are under direct merchant control (i.e. the transaction is initiated by the cashier; cardholder and cashier both provide input). For some transaction types manual entry can be allowed by the acquirer. In this case the merchant initiates the transaction on the basis of information supplied by cardholder, but neither the cardholder nor the card needs to be present.
- Unattended terminals or cardholder activated terminals - the cardholder performs the transaction without the Merchant being present (i.e. a self service environment);
- Mail Order / Telephone Order (MOTO) terminals - the merchant initiates the transaction on the basis of information supplied by cardholder, but neither the cardholder nor the card is present. Typical for mail-order/telephone order.

2.2.7 The types of transactions specified by C-TAP

The EPC “SEPA Cards Standardisation Volume - Book of Requirements” [ref: EPC020-08] specified the names for services. Although C-TAP was operational before the EPC document was released, the original C-TAP service names are replaced and the EPC service names are used in this overview, in the communication with the merchant / cardholder and even in the technical C-TAP specifications.

- Payment: purchase of goods, services, or both, generally at a merchant establishment
  - Optional function “cashback” – when the cardholder, next to the payment for goods or services, also requests some cash from the merchant, the transactional processing will indicate how much was due for services and what amount of cash was handed over to the cardholder
  - Optional function “extra amount” – when the cardholder, on top of the amount to be paid for goods or services, wants to add an extra amount to be paid to the merchant
  - Optional functions will allow
    - to partially approve a transaction , i.e approve a transaction for a maximum amount that is authorised by the issuer of the card, but which is below the amount requested by

the merchant. The remaining amount will have to be paid by other means.

  - to allow transaction only for certain product types
  - to operate Direct Currency Conversion that allows the cardholder to pay in the currency of his choice that is different from the merchant's currency

- Cash advance: similar to Payment transaction, only delivery of money instead of delivery of goods
- Cancellation: allows cancellation of a previously performed transaction (where a cancellation in turn cannot be cancelled)
- Refund: reimburse the cardholder (in case the goods are returned or the service is not consumed to the full extent)
- Card Validity Check: is an on-line service that allows the acquirer to verify the validity of the card. This gives no guarantee of funds (it is a transaction with a zero amount) but ensures that it is a valid card and that (at that moment) the card can be used normally.
- Pre-Authorisation and Payment Completion: a two step process where in the first step approval is given to allow the cardholder to use a service up to a specified amount, and afterwards the payment will be captured up to the reserved amount. A typical example of this transaction type is car rental.
- Update Pre-Authorisation: to modify an existing Pre-Authorisation.
- Deferred Payment: is similar to the Payment. For the Payment the transaction amount is known at authorization time, for the Deferred Payment an authorisation is required before the exact amount of the transaction is known. A typical example of this transaction service is the unattended self-service transaction at a petrol pump. As multiple cardholder can use a same terminal in this mode, multiple concurrent session will be supported.
- Voice Referral: A Function where the Payment is completed with a voice conversation to obtain an approval code. This Function does not necessarily involve the card or the Cardholder.
- Original Credit: A service which allows the card acceptor to effect a credit to a cardholder's account. An original credit is not preceded by another card payment.

2.2.8 Security Models

Within the C-TAP Terminal specification 3 security models are defined. These are:

- Message integrity: When sending and receiving a transaction message, a check is made that the message is transferred unmodified by use of a hash calculation [FIPS180-4];
- Mutual authentication and Secure Socket Layer: terminal and host mutually authenticate themselves and the data are encrypted before transmission (referred to as TLS1.2)
- "Transaction Security" based on TSC imposed: TSC: Terminal Security Component (TSC) is a specification that describes how terminals can safely store multiple keys for multiple acquirers and how these keys will be used to protect transaction data. The TSC has full control over the display, cardholder keyboard, magstripe - and smartcard readers. When the TSC Security Architecture is in place, a "Security Provider" role is introduced.

Acquirers will choose which model(s) they use. The C-TAP terminal should support all models to allow the acquirers to freely select amongst above-mentioned security models.

3. SPECIFICATION MANAGEMENT

3.1 THE SPECIFICATION MANAGEMENT BOARD (SMB)

The C-TAP specifications are managed by the Specification management board:

- To properly manage the evolution of specifications, propose a lifecycle management model for these specifications, including:
  - Principles
    - Mandatory, scheme driven, optional and community specific amendments and extensions
    - Flexibility requirements for implementations, such as the possibility to add new fields in newer versions that will be ignored by existing implementations in line with the TLV (and XML) philosophy
    - Backward compatibility and limits for backward compatibility for specifications (sunset periods for obsolescent versions)
  - Rules & liabilities
- On the basis of requests coming from acquirers or acquirer processors seating in the Acquiris General Assembly, analyse requests to extend or amend C-TAP specifications, in following steps:
  - Translate business requirements in technical requirements
  - Draft new specifications for new functions or changes to the existing specifications for amendments
  - Assess the impact of these changes on the acquiring infrastructure and the terminal software
  - Draft a plan for the implementation of the modifications, in line with the lifecycle model
  - Package the draft of the specifications changes and the implementation plan for submission to the Acquiris General Assembly
- Upon request of the Acquiris Business Development department, perform a similar drafting of potential changes. In addition, the Business Development will indicate to the Acquiris General Assembly what would be the benefits for the implementation of such implementation.
- As changes might result from evolving scheme rules to which acquirers are committed, either acquirers or acquirer processors might submit direct change requests to the SMB. The SMB will prepare and package the draft of the specifications changes and the implementation plan for submission to the Acquiris General Assembly.
- At it is probable that multiple changes will intervene in parallel, the SMB will also keep a global calendar of planned or scheduled amendments or extension and group these in a release plan. Proposals to the Acquiris General Assembly will position the request in the ongoing release plan.

The SMB pays attention on backward compatibility when describing changes to the specifications, as they are likely to affect many live implementations, both at the level of the acquiring infrastructure and the payment terminals.

As with other global specifications such as EMVCo and PCI, when changes implicate that certain parts of the specifications should be discontinued and replaced by others, the Acquiris General Assembly will be aware that live specifications will remain active for a while (sunset period) and that parallel operation of 2 definition sets might be required during that period.

Upon proposal of the SMB, the Acquiris General Assembly also decides which changes will be considered as mandatory (the co-operative space) and for which specifications acquirers the support would be optional, i.e. that some acquirers would offer the extension as a service and that some vendors would implement it on their terminals to make it available for these acquirers' merchants.

The SMB is the guardian for the integrity and consistency of the evolving specifications in line with the C-TAP fundamental ideas and working principles.

3.2 ADDITIONAL OPTIONAL SPECIFICATIONS

While the main C-TAP specifications represent the interests of all parties involved, some extensions of the specifications might only be meaningful for more restricted groups of acquirers and issuers (or their representatives). These parties will be able to create membership subgroups that will enhance the specifications in line with the C-TAP methodology to avoid interoperability issues with the core C-TAP functions.

These sub-groups will be created *ad hoc* in agreement with the plenary and support all costs related to the enhancements on a separated cost-sharing basis and report the general principles of their achievements to the plenary. Would the interest for these enhancements broaden, the resulting specifications could be consolidated with the main C-TAP specifications and the members of the sub-group compensated for their anticipative investments.

To avoid unnecessary fragmentation of the C-TAP specifications, the creation of an AOS sub-group will be managed carefully by the members' assembly and be proven to represent interests which have a synergy with the overall specification but nevertheless require specific extensions of a more restricted interest.

4. CERTIFICATION MANAGEMENT

4.1 LAYERED APPROACH

Acquiris will functionally certify terminals against the C-TAP specifications. However, to satisfy scheme rules, preliminary certifications will be required

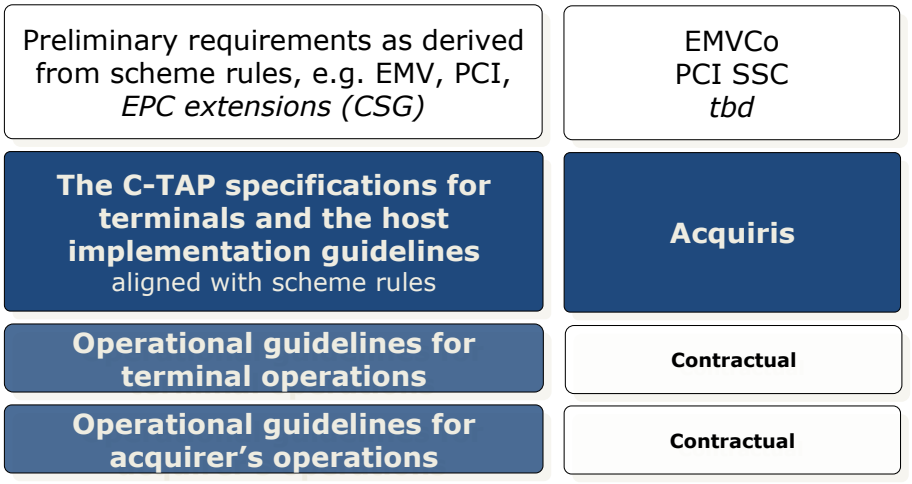

Figure 5 – Acquiris Certification stack

In addition terminal vendors or their distributors and acquirers or their processors will have to satisfy the operational guidelines that are part of their respective member contracts.

4.2 THE CERTIFICATION MODEL

4.2.1 Label Compliance

Consumer and office equipment needs to be compliant with CE regulations for electrical safety and communication equipment. The vendor will present the relevant certificates for the equipment that will be certified by Acquiris (See also [C-TAP.510])

4.2.2 The card interface device and kernels

The interface with the cards of different types is described by international organisations:

- ISO for the magnetic stripes (simple read-only interface)
- EMVCo for EMV smart cards
  - Describing the signalling and data communication between the card and the interface device integrated in the terminal (EMV L1)
  - Providing detailed functional and technical requirements for the cards
  - Describing "kernel" functions to be provided on the terminal to interact with the functions on the card (EMV L2)
- EMVCo and Card schemes for contactless cards

- Describing the wireless signalling and communication between the card and the interface device integrated in the terminal (EMV L1)
- Providing multiple detailed functional and technical requirements for the cards
- Describing multiple "kernel" functions to be provided on the terminal to interact with the functions on the card

The C-TAP specifications rely on these kernels to execute commands to interact with the smart / contactless cards.

Therefore, C-TAP terminals need to be certified by independent labs for these functions that support the cards that will be accepted on the terminal. The results of these independent EMVCo accredited labs will be controlled by EMVCo leading to an approval. See "Terminal type approval" on http://www.emvco.com/approvals.aspx?id=39. This website also allows consulting which terminals were approved.

The vendor will present the relevant certificates for the equipment that will be certified by Acquiris (See also [C-TAP.510])

4.2.3 PIN and Data Security

Terminals handle secure data and the Personal Identification Number of card holders.

Card schemes have set up an organisation called "The PCI Security Standards Council" or PCI SSC. This organisation offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step.

Terminal vendors will submit their equipment for approval after an audit by PCI SSC accredited labs. A list of Approved PIN Transaction Security Devices can be consulted on

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

The vendor will present the relevant certificates for the equipment that will be certified by Acquiris (See also C-TAP.510 § 3.1)

4.2.4 Additional requirements

The C-TAP.510 contains a number of additional requirements that are of a more practical nature:

- Recapitulating card scheme requirements
- Setting standards in areas where card schemes have not yet issued an opinion, but which ensure that terminals have a minimum level of quality
- To enforce common parameter loading that is essential in a multi-acquirer environment

Acquiris or the Acquiris certified labs will verify if these requirements are met.

4.2.5 Functional certification

The C-TAP specifications mainly focus on functional requirements that support and provide card payments. Acquiris' accredited labs will certify that terminals operate according to the C-TAP specifications at different levels:

- Interface with the relevant card kernels
- Interfacing with the users (cardholders, merchants)
- Linking up to acquiring host systems over multiple types of communication networks
- Controlling the correct operation of security mechanisms (SHA, TLS1.2, TSC)

In a last phase of the functional certification, acquirers will be invited to test functionally tested terminals in their own environment (the non-disturbance tests or NDT).

4.2.6 Acquiris approval

Acquiris will approve a terminal if all of above conditions are met:

- Covered by external certificates: label compliance, EMVCo, PCI SSC
- Based on Acquiris accredited labs investigations: additional requirements, functional certification
- Based on the results if the acquirers' NDT

4.2.7 Post-approval

Acquiris will monitor the market situation based on problem reports of acquirers and further investigate with terminal vendors to enforce corrections when required.

4.2.8 Certification framework

When vendors apply for certifications, the rules and liabilities for vendors are described in a "Certification Framework" and its appendices. As a first step in the process the vendor will agree with the terms and conditions of this document.

5. DOCUMENTS STRUCTURE

5.1 OVERALL DOCUMENTS STRUCTURE

The C-TAP Terminal Specifications consist of a set of documents, each addressing a specific area of the terminal specification. A number of the documents are common for all implementations. Other documents describe additional functionality that can be used optionally on top of common implementations.

The Acquiris documents related to C-TAP did start with a version number 10.0, to mark the difference in regard of previous C-TAP versions that were operated at national level. The latest version number is 10.1.

Document identifier	Purpose: Common Terminal Acquirer Protocol, Terminal Specification –	Version[1]	Date of edition
C-TAP.000	Introduction to C-TAP	10.1(1)	October 2016
C-TAP.200	Online Terminal Functionality	10.1(1)	October 2016
C-TAP.220	Data Dictionary	10.1(1)	October 2016
C-TAP.202	Process using the TSC	10.1(1)	October 2016
C-TAP.203	Dynamic Currency Conversion	10.1(1)	October 2016
C-TAP.204	Partial Approval	10.1(-)	April 2016
~~C-TAP.205~~	~~Product Selection~~	~~10.1( )~~	~~April 2016~~
C-TAP.206	Backup Mode	10.1(-)	
C-TAP.230	Semi-Online Terminal Mode	10.1(-)	April 2016
C-TAP.240	Offline Terminal Functionality	10.1(1)	October 2016
C-TAP.212	TSC Operations	10.1(-)	April 2016
C-TAP.401	Responsibilities Personalization Provider	10.1(-)	April 2016
C-TAP.402	Responsibilities Security Provider	10.1(-)	April 2016
C-TAP.410	Public Key and Certificate Exchange	10.1(-)	April 2016
C-TAP.260	Communication Protocols & Strategies	10.1(-)	April 2016
C-TAP.500	Requirements for Host Operations	10.1(-)	April 2016
C-TAP.510	Requirements for Terminal Operations	10.1(2)	October 2016
C-TAP.520	Requirements for Gateway Operations	10.1(2)	October 2016

[1] (-) indicates this is a final approved release and no edition number applies

5.2 THE MAIN COMMON FUNCTIONAL SPECIFICATIONS

The following documents are common for all parties involved:

- The Online Terminal Functionality document describes the functional behaviour of the terminal, including the interface with card readers and card associated kernels, card recognition, transaction processing, the cardholder interface, the merchant interface, acquirer selection and the message protocol with the acquiring host systems.
- The Data Dictionary document contains details on the messages, the message layout and the fields exchanged between terminals and acquiring host systems.

5.3 THE SPECIFICATIONS RELATED TO MESSAGE AND DATA SECURITY

The C-TAP terminal specification supports three Security Architectures:

- Data integrity based on SHA. International standards apply. [FIPS180-4]
- Mutual authentication and data confidentiality based on TLS1.2. Information on the TLS1.2 usage is provided in:

C-TAP.260	Communication Protocols & Strategies

- Data encryption / Message authentication based on bilateral keys shared between terminal and acquirer with key management provided by TSC. Following documents apply:

C-TAP.202	Process using the TSC
C-TAP.212	TSC Operations
C-TAP.401	Responsibilities Personalization Provider
C-TAP.402	Responsibilities Security Provider
C-TAP.410	Public Key and Certificate Exchange

5.4 DATA COMMUNICATION

Terminals connect to acquiring hosts in multiple ways and rely on the services of telecommunication providers. For each of the supported technologies, guidelines and requirements are detailed in:

C-TAP.260	Communication Protocols & Strategies

5.5 COMMON PARAMETERS

As the behaviour of C-TAP terminals is driven by parameters that are collected from acquirers / acquiring processors and disseminated to terminal vendors, the Common Parameters document is a key information repository for the Acquiris community. Vendors of C-TAP terminals will integrate the relevant data in their terminal management systems and download this information to the payment terminals that are installed with merchants.

- Book 1 contains information that is driving card recognition and acquirer selection. This document will be updated each time acquirers or acquiring processors require it and vendors will relay these changes to the payment terminals.

- Book 2 contains more general technical and public key infrastructure information that is equally important for terminal operation, but will be less subject to regular updates.
- Book 3 contains the IP addresses and, where applicable, domain names required for configuration when using firewalls. The terminal will request to access these IP addresses to the firewall and these specific IP addresses should therefore be accessible for outgoing and incoming traffic. These IP addresses cannot be published on the website as this would facilitate the attacks from parties launching Denial-of-Service attacks.
- Book 4 contains the tables with the translations in the 4 mandatory languages (and possibly other supported languages) of the different message screens that are used for the cardholder interface; the Service Label Names; the Standard Receipt Text; the standard used Cardholder & Merchant Texts.

Common parameters will not follow the release cycles and will be updated independently from specifications changes to reflect changes in brand parameters, acquirer or acquiring processor data or other definitions. For that reason, C-TAP.CP1; C-TAP.CP2 and C-TAP.CP4 will have version numbers that are not directly linked to the C-TAP specifications version numbers. As indicated in the terminal vendor's "Certification Framework" (under Modifications by Acquiris) a vendor is imposed strict guidelines to implement changes in the common parameters on the installed terminal configurations he manages.

5.6 ADDITIONAL OPERATIONAL REQUIREMENTS AND GUIDELINES

The C-TAP interoperability requires that acquirers / acquiring processors and terminal vendors comply to a series of operational requirements and guidelines. These are detailed in:

C-TAP.500	Requirements for Host Operations
C-TAP.510	Requirements for Terminal Operations
C-TAP.520	Requirements for Gateway Operations

5.7 ADDITIONAL OPTIONAL SPECIFICATIONS

The support of following specifications can be added to either terminal or acquiring host functionality. These functions will of course only be supported if both terminal and acquiring host offer this functionality.

C-TAP.230	Semi-Online Terminal Mode
C-TAP.240	Offline Terminal Functionality
C-TAP.203	Dynamic Currency Conversion
C-TAP.204	Partial Approval
C-TAP.205	Product Selection
C-TAP.206	Backup Mode

6. CONVENTIONS - GLOSSARY – REFERENCES – DOCUMENT HISTORY

6.1 REQUIREMENT CLASSIFICATION LEVELS

The C-TAP specifications will use the following words, with their usual meaning:

- "shall": this word, or the adjective "required" or "mandatory", means that the definition is an absolute requirement of the specification;
- "shall not": this phrase, or the adjective "forbidden", means that the definition is an absolute prohibition of the specification;
- "should": this word, or the adjective "recommended", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. Such a decision shall be documented for later review.
- "may": this word, or the adjective "optional", means that this item is one of an allowed set of alternatives; an implementation that does not include this option shall be prepared to inter-operate with another implementation that does include the option.

6.2 DATA ELEMENT CONDITION CODES

This specification describes both the presence and the support of the data elements, i.e. the fields in the messages between the Terminal and the Acquirer, messages that the Terminal generates or receives and processes or relays; cf. the message layout in ref. [C-TAP.220]. Whenever this specification describes a class of data structure (e.g. a message, a group or a table) having components (e.g. fields, members or records), each component is assigned one of the following grades (levels) on its demanded presence. The presence of each data element (field, sub-field) is qualified as follows (for information, it is based on the ITU-T Rec. X.402):

M **Mandatory**
A mandatory component shall be present in every instance of the class.

O **Optional**
An optional component may be present in an instance of the class at the discretion of the entity (e.g. Terminal or Acquirer) supplying that instance; in its absence, a default value can apply, which shall be used as specified by this specification.

C **Conditional**
A conditional component shall be present in an instance of the class as dictated by this specification; where it shall be present, this is explicitly defined, and when the condition is encountered the component is mandatory; the presence of conditional elements can be dependent on the presence or the value of other elements.

E **Echoed**
An echoed component shall be present in an instance of the class and its value shall be equal to the corresponding instance of a previous related message. The echoed component shall be present only if the corresponding instance was present.

The presence of a data element also implies the corresponding support and the requirements for the implementations to be able to generate, to receive and to process that argument, as appropriate (the 'receiving' role includes relaying where appropriate).

On the origination, implementations conforming to this specification shall generate the mandatory elements in all information objects in which, according to the specification, they shall occur; for the optional elements, implementations conforming to this specification may optionally be capable of generating these elements but are not required to do so.

On the reception, implementations conforming to this specification shall process the elements appropriately according to their semantics.

6.3 REFERENCED DOCUMENTS

[C-TAP.xxx] For C-TAP references, please refer to 5.1

[EPC020-08] European Payments Council
SEPA Cards Standardisation (SCS) "Volume"
Payments and Cash Withdrawals with Cards in SEPA
Applicable Standards and Conformance Processes
EPC020-08, v7.R2.V1 December 2015.

[EMV Book 1] EMVCo,LLC, EMV – Integrated Circuit Card – Specifications for Payment Systems
Book 1 – Application Independent ICC to Terminal Interface Requirements
Version 4.3 – November 2011.

[EMV Book 2] EMVCo,LLC, EMV – Integrated Circuit Card – Specifications for Payment Systems
Book 2 – Security and Key Management – Version 4.3 – November 2011.

[EMV Book 3] EMVCo,LLC, EMV – Integrated Circuit Card – Specifications for Payment Systems
Book 3 – Application Specification – Version 4.3 – November 2011.

[EMV Book 4] EMVCo, LLC, EMV – Integrated Circuit Card – Specifications for Payment Systems
Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements
Version 4.3 – November 2011.

[EMV Book A] EMV – Contactless Specifications for Payment Systems
Book A – Architecture and General Requirements – Version 2.5 – March 2015.

[EMV Book B] EMV – Contactless Specifications for Payment Systems
Book B – Entry Point Specification – Version 2.5 – March 2015.

[EMV Book C-1] EMV – Contactless Specifications for Payment Systems
Book C-1 – Kernel 1 Specification – Version 2.5 – March 2015.

[EMV Book C-2] EMV – Contactless Specifications for Payment Systems
Book C-2 – Kernel 2 Specification – Version 2.5 – March 2015.

[EMV Book C-3] EMV – Contactless Specifications for Payment Systems
Book C-3 – Kernel 3 Specification – Version 2.5 – February 2015.

[EMV Book C-4] EMV – Contactless Specifications for Payment Systems
Book C-4 – Kernel 4 Specification – Version 2.5 – March 2015.

[EMV Book C-5] EMV – Contactless Specifications for Payment Systems
Book C-5 – Kernel 5 Specification – Version 2.5 – March 2015.

[EMV Book C-6] EMV – Contactless Specifications for Payment Systems
Book C-6 – Kernel 6 Specification – Version 2.5 – February 2015.

[EMV Book C-7] EMV – Contactless Specifications for Payment Systems
Book C-7 – Kernel 7 Specification – Version 2.5 – March 2015.

[PCI DSS] PCI Security Standards Council LLC, Payment Card Industry (PCI), Data Security Standard, Requirements and Security Assessment Procedures, Version 3.1, April 2015

[PCI PA-DSS] PCI Security Standards Council LLC, Payment Card Industry (PCI), Payment Application Data Security Standard, Requirements and Security Assessment Procedures, Version 3.1, May 2015.

[PCI PTS] PCI Security Standards Council LLC, Payment Card Industry (PCI), PIN Transaction

Security (PTS), PIN Security Requirements v2.0, December 2014

[PCI PTS POI] PCI Security Standards Council LLC, Payment Card Industry (PCI), PIN Transaction Security (PTS), Point of Interaction (POI) Modular Security Requirements, Version 4.1c, October 2015.

[EN 726-4] EN 726-4: 1994.
Identification card systems – Telecommunications integrated circuit(s) cards and terminals – Part 4: Application independent card related terminal requirements.

[ENV 1375-1] ENV1375-1:1994.
Identification card systems – Intersector integrated circuit(s) card additional formats – Part 1: ID-000 card size and physical characteristics.

[FIPS140-2] Federal Information Processing Standards Publication – Security requirements for cryptographic modules, Issued May 25, 2001.

[FIPS180-4] Federal Information Processing Standard Publication – Secure Hash Standard
FIBS PUB 18-4 August 2015.

[IEEE 802.3] IEEE Std 802.3 : Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3:
Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

[ISO 639-1] ISO 639-1:2002 Codes for the representation of names of languages.

[ISO 10116] ISO/IEC 10116:2006, Information technology - Security techniques - Modes of operation of an n-bit block cipher

[ISO 15668] ISO 15668:1999, Banking – Secure file transfer (retail)

[ISO 18033-3] ISO/IEC 18033-3:2010 Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers

[ISO 3166-1] ISO 3166:2013, Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes

[ISO 4217] ISO 4217:2015, Codes for the representation of currencies and funds

[ISO 4909] ISO 4909:2006, Bank cards – Magnetic stripe data content for track 3

[ISO 7810] ISO/IEC 7810: 2003 Identification cards - Physical characteristics.

[ISO 7811] ISO/IEC 7811: 2014 Identification cards - Recording technique.

[ISO 7812] ISO/IEC 7812: 2015 Identification Cards- Identification of Issuers.

[ISO 7813] ISO/IEC 7813: 2006 Identification cards - Financial transaction cards.

[ISO 7816] ISO/IEC 7816-1: 2011. Identification cards – Integrated circuit cards
Part 1: Cards with contacts – Physical Characteristics.
ISO/IEC 7816-2: 2007. Identification cards – Integrated circuit cards
Part 2: Cards with contacts – Dimensions and location of the contacts.
ISO/IEC 7816-3: 2006. Identification cards – Integrated circuit cards
Part 3: Cards with contacts – Electronic signal and transmission protocols.
ISO/IEC 7816-4: 2013. Identification cards – Integrated circuit cards
Part 4: Organization, security and commands for interchange.

[ISO 8583] 8583-1:2003 Bank card originated messages – Interchange message specifications – Content for financial transactions.

[ISO 8859] ISO/IEC 8859:2003 Information processing – 8 bit single-byte coded graphic character sets.

[ISO 9564] ISO 9564-1: 2011. Financial services -- Personal Identification Number (PIN) management and security -- Part 1: Basic principles and requirements for PINs in card-based systems.
ISO 9564-2: 2014. Financial services -- Personal Identification Number (PIN) management and security -- Part 2: Approved algorithms for PIN encipherment.

[ISO 9797-1] ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher

[RFC 1042] Standard for the transmission of IP datagrams over IEEE 802 networks.
[RFC 1332] PPP Internet Protocol Control Protocol (IPCP).
[RFC 1542] Clarifications and Extensions for the Bootstrap Protocol.
[RFC 1618] PPP over ISDN.
[RFC 1661] The Point-To-Point Protocol (PPP).
[RFC 2131] Dynamic Host Configuration Protocol.
[RFC 2132] DHCP Options and BootP Vendor Extensions.
[RFC 5246] The Transport Layer Security (TLS) Protocol
[RFC 6101] The Secure Sockets Layer (SSL) Protocol Version 3.0
[RFC 768] User Datagram Protocol.
[RFC 791] Internet Protocol.
[RFC 793] Transmission Control Protocol.
[RFC 951] Bootstrap Protocol (BootP).
[SP 800-22] NIST Special Publication 800-22 R1a, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April, 2010
[X9.24] ANS X9.24 Part 1-2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

6.4 ABBREVIATIONS

a.k.a.	also known as
ANS	American National Standard
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
ATM	Automated Teller Machine
BIN	Bank Identification Number
BKS	Banksys (now Atos Worldline)
BC/MC	Bancontact / MisterCash
CAD	Card Acceptance Device
CAM	Card Authentication Methode
CAT	Cardholder-Activated Terminal
CBC	Cipher Block Chaining
CDA	Combined dynamic Data Authentication
Cert	Certificate
CRC	Cyclic Redundancy Check
CSM	Chip Security Module
C-TAP	Common Terminal Acquirer Protocol
DDA	Dynamic Data Authentication
EFT	Electronic Funds Transfer
e.g.	exempli gratia - for example
EMV	Europay MasterCard Visa
FC	Format Code
FS	Field Separator
hex.	hexadecimal
HSM	Host Security Module
i.e.	id est
I/O	Input / Output
ICC	Integrated Circuit Card
IEC	International Engineering Consortium
IFD	Interface Device
IPN	Interpay Nederland (now Equens)

ISO	International Organisation for Standardisation
MAC	Message Authentication Code
max.	maximal
MGF	Mask Generation Function
MPT	Magstripe Protection Table
MSR	Magnetic Stripe Reader
N.a.	Not applicable
NL	Nederland
PAN	Primary Account Number
PCI	Payment Card Industry
PED	PIN Entry Device
PIN	Personal Identification Number
POS	Point Of Sale
RSA	Rivest Shamir Adleman
SAM	Secure Application Module
SDA	Static Data Authentication
SecScheme	Security Scheme (provider)
SHA	Secure Hash Algorithm
Sign	Signature (provider)
t.b.d.	to be defined / to be done
TC	Terminal Component
TC-n	Terminal Component - non sensitive
TC-s	Terminal Component - sensitive
TE	Tamper Evident
TLV	Tag Length Value
TR	Tamper Responsive
TRi	Tamper Resistant
TSC	Terminal Security Component
UKPT	Unique Key Per Transaction
XOR	eXclusive OR

6.5 DOCUMENT HISTORY

Date	Note	Version
April 2011	First draft based on Dutch version	10.0 (2)
February 2012	Final version	10.0 (4)
January 2016	Adjusted to Updates for 10.1	10.1.0