ECBS

EUROPEAN COMMITTEE FOR BANKING STANDARDS

ECBS TERMINOLOGY

ORG9003 V4 — AUGUST 2003

Updates

Version 1   January 1996

Version 2   December 2000

Version 3   May 2002

Version 4   August 2003

TABLE OF CONTENTS

1   PURPOSE AND OBJECTIVES

1.1   Introduction

ECBS Standards are designed to be suitable for use in all ECBS member countries. These countries use many different languages, and have varying banking environments and payments systems infrastructures. Even when correctly translated, words may have different meanings in different countries. These different meanings can cause basic misunderstandings in the use of ECBS Standards.

The purpose of this document is to ensure a common understanding throughout ECBS member countries of terms used in ECBS standard specifications. It is not intended to impose new meanings of selected terms throughout Europe, and hence it must be recognised that the ECBS definition of a commonly used term may differ - and sometimes very substantially - from established local usage. The existence of the ECBS Terminology will go some way in ensuring unambiguous understanding of the intentions (and implications) of the term when it appears in an ECBS standard specification or other document.

ECBS Terminology also maximises consistency in the way terms are used in ECBS, CEN and ISO.

It is not the intention of the ECBS Terminology to describe the range of services (or other features) that different users may associate with a given term (e.g. a credit card service may, or may not, be associated with a revolving line of credit, however it may be defined in the ECBS Terminology).

1.2   Source

One of the main source documents is ISO 8908 Banking and Related Financial Services: Vocabulary and Data Elements. This very relevant standard was re-issued by TC68 in 1993, and lists every definition in every TC68 standard, as well as many from JTC1/SC17. However, there is some limitation to its value as an ECBS source document, for many terms in ISO 8908 have more than one definition, each derived from its own application specific standard. Beyond specifying the source standard, ISO 8908 gives no further guidance on which definition to choose.

Other source documents used have been the EMI Report on Pre-paid Instruments, issued in early 1994; the Report issued by Internal Market DG in early 1995 on its proposed Directive on Cross-Border Payments Systems, the Electronic Signature Directive issued in 1999, MeT[1] definitions, and ECBS publications. Where no suitable definition could be found for an essential ECBS term, an ECBS specific definition has been proposed. In some cases, a definition from an external source was found to be *almost* suitable, but some modification was needed. Modifications to existing published definitions from an external source have only been made when such changes were considered unavoidable. Modified definitions are described as *"Derived from"*.

The source and ECBS committee responsible for the term appear directly after the definition, e.g., *"EBS200 [TC2]"*.

1.3   Relationship with ISO and CEN definitions

It is important that every effort is made to keep ECBS definitions consistent with ISO and CEN definitions. However, *consistency* is not the same as *being identical to.* Objectives associated with the definitions in an ISO application specific standard, may not be the same as the objectives of the ECBS Terminology and therefore should not be blindly followed.

---

[1] MeT Limited is a company founded to establish a framework for secure mobile transactions, ensuring a consistent user experience independent of device, service and network.

Nor must it be assumed that ECBS definitions should always be identical to those in an ISO general purpose standard, such as ISO 8908. Divergence from ISO (and relevant CEN) definitions is bound to arise, but every effort must be made to minimise its occurrence, and where differences do occur, there must be a clear understanding of the reasons for such differences.

1.4 Maintenance of ECBS Terminology

Responsibility for maintaining a term lies with the Technical Committees or Technical Steering Committee, as appropriate. The committee responsible for maintaining that term follows the definition.

The ECBS Secretariat shall add new terms from published ECBS documents and responsibility for maintaining that term automatically lies with the Technical Committee responsible for the ECBS document from which it is taken. In addition, modifications to an existing term may come from any source but shall require the formal approval of the responsible committee. All proposals for modifications, before formal submission to the responsible committee, shall be sent to the ECBS Secretariat. The ECBS Secretariat has the responsibility for investigating where the terms are presently used, the implication of the change on any presently published ECBS documents using the term, and for confirming that the change has no adverse effect on any such published ECBS documents. The ECBS Secretariat shall submit those terms proposed for modification to the relevant committees once a year.

The Technical Steering Committee shall decide on the committee responsible for maintenance of a term in the event of a dispute.

1.5 Rules for using the ECBS Terminology

The Technical Steering Committee shall be responsible for ensuring that the following rules are conformed to in the preparation of all ECBS Standards, Technical Reports, and other published documents.

- All published ECBS standards documents (standard specifications, technical reports, regulations, recommendations, guidelines), shall conform to the ECBS Terminology.

- An ECBS standards document may need to define terms not yet included in the ECBS Terminology but which are necessary to define its own scope. Such terms shall be listed in the next published version of the ECBS Terminology.

- Where a standard uses an ECBS Terminology term, it shall only be used in the meaning assigned to it by the ECBS Terminology.

2 TERMINOLOGY

Accepting device
A device designed to:

- identify the relevant electronic purse;

- authenticate the electronic purse application;

- store securely the transaction or incrementation of its own balance by the transaction amount and, optionally, store the transaction information; and

- transfer securely the stored information to the acquiring technical operator.

TR103 [TC1]

Acceptor
A party accepting a financial transaction card for the provision of goods or services, or cash.
Modified ISO 8908 (10202 version) definition [TC1]

Account identification code
A code uniquely identifying an account held at a financial institution.
Derived from EBS200 & TR210 [TC2]

Account Number
Bank and account identifier(s) of the account to be credited or debited.
EBS206 [TC2]

ACH
See *Automated Clearing House*
TR210 [TC2]

Acquirer
A financial institution (or its agent, usually a card scheme), which acquires from the card acceptor the data relating to the transaction, and initiates that data into an interchange system.
(ISO 8583: 1993) [TC1]
Or
An entity providing transaction clearance services for the content provider. The entity and its supporting infrastructure are used synonymously.
(TR603) [TC6]

Acquiring
It is the process by which ordering customers make payments to beneficiaries using the IPI.
SIG208 [TC2]

Acquiring bank
See *Acquirer*
[TC1]

Acquiring technical operator
An organisation, which collects and possibly aggregates transactions from several Purchase Devices for delivery to one or more Purse Providers.
TR103 & TR104 (prEN 1546-1) [TC1]

Advance Notice
The notification provided by the creditor to the debtor of the amount, and in some National Direct Debit Schemes, of the date on which the debit is to be collected. The notice can be provided as a separate piece of information, or via inclusion in a regular statement of account, bill, or invoice.
TR201 & TR210 [TC1]

Advice
A message where the sender notifies the receiver of an activity that has been taken, requiring no approval but requiring a response.
ISO 8583: 1993 [TC1]

Aggregation
The process whereby the values of the individual transactions, in a given collection or group of collections, are accumulated and transmitted in a set of total amounts. No details of the individual transactions that make up the total are provided.
EBS111 [TC1]

Agent
A party performing specific functions on behalf of another party.
ORG9003 term [TC1]

Algorithm
A specified mathematical process for computation.
ISO 8908 [TSC]

Asymmetric algorithm
A cryptographic algorithm employing a public key and a private key. Together these form an asymmetric key set.
TR406 [TC4]

ATM (Automated Teller Machine)
An unattended mechanical device that permits authorised users, typically using financial transaction cards, to access financial services including cash withdrawal.
Derived from BIS [TSC]

Attended terminal
A card-accepting terminal requiring the involvement of a terminal operator / cashier.
ORG9003 term [TC1]

Audit journal
A chronological record of system activities which is sufficient to enable the reconstruction, review and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results.
TR402 (ISO 15782) [TC4]

Authentication
Process used between a sender and a receiver to provide data origin verification.
> Derived from ISO 8908 [TC2]

Or

Verification of identity.
> TR603 (MeT definition) [TC6]

Authorisation
The approval or guarantee of funds given by the card issuer or, on behalf of the card issuer by the acquirer (or his agent).
> Derived from ISO 8583 [TC1]

Automated Clearing House (ACH)
An organisation for the automated processing of payments, which may be a part of the domestic clearing system and/or act as an entry point for cross border payments.
> EBS200 & TR210 [TC2]

Automated Teller Machine
See *ATM*
> [TSC]

Availability
The property of no hindrance to the supply of data and processing to any party authorised to receive it.
> ORG9003 term [TC4]

Bank
A financial institution authorised or chartered by its national regulatory authority to be designated as a bank.
> EBS206 (ISO 8908) [TSC]

Bank identifier
A code that uniquely identifies a bank, and possibly a branch as part of a financial institution.
> Derived from EBS 200 & EBS206 [TC2]

Bank Identifier Code (BIC)
An 8 or 11 character ISO code assigned by SWIFT and used to identify a financial institution in financial transactions.
> EBS 206 (ISO 9362) [TSC]

Bank operation code
A code, which indicates the type of operation (e.g., credit transfer, reject, enquiry or the response to an enquiry).

The bank operation code is part of the non-ambiguous identification of the national direct debit scheme. For some direct debit schemes this code must be used in conjunction with a transaction code. In those cases:
- the bank operation code identifies the national direct debit scheme and the accounting mechanism; and
- the transaction code contains other relevant information: type of underlying agreement between creditor and debtor, rejection/revocation conditions, etc.
> EBS 200 & TR210 [TC2]

Banking business day
A day when financial institutions are open for conducting funds transfers activities. Banking business days can differ from country to country and within a country.
> EBS200 [TC2]

Basic Bank Account Number (BBAN)
The identifier used by financial institutions in individual countries as part of a National Account Numbering Scheme(s), which uniquely identifies an account of a customer at a financial institution. (ISO 13616). The BBAN includes an explicit bank identifier.
> EBS200 & SIG203 [TC2]

Batch
A collection of data sharing the same characteristics, which is gathered for processing as a single group.
> Derived from EBS200 & TR210 [TC2]

Batching criteria
The condition under which transactions are collected to form a batch.
> Derived from EBS200 & TR210 [TC2]

Batch Reference
Sender's unique reference for a batch.
> TR210 [TC2]

BBAN
See *Basic Bank Account Number*
> SIG203 [TC2]

Beneficiary
The ultimate party to be credited or paid as a result of a transfer.
> EBS206, EBS602 (ISO 8908) [TSC]

Beneficiary's Financial Institution (BFI)
The BFI holds the account of the beneficiary.
> EBS602 [TC6]

BFI
See *Beneficiary's Financial Institution.*
> EBS602 [TC6]

BIC
See *Bank Identifier Code*

EBS206 & TR210 [TSC]

Block cipher
A cryptographic algorithm which maps n-bit plaintext blocks to n-bit ciphertext blocks. n is called the blocklength.

TR406 [TC4]

Bluetooth
A short-range radio technology designed to eliminate the need for cables between devices (for example, computer to printer connections achieved without wire and within a local area).

TR603 [TC6]

CA
See *Certification Authority*

[TC4]

CAD
See *Card Accepting Device*

[TC1]

CAH
See *Card Accepting Host*

[TC1]

NEW Cancellation
A request by the sender of the original message to cancel the original transaction (see also reversal).

TR210 [TC2]

Capture of IBAN
The process of converting an IBAN from paper to electronic format.

SIG203 [TC2]

Card Accepting Device (CAD)
The device used in conjunction with the card and the point of sale to perform a financial transaction.

EBS105 Part 1 [TC1]

Card-Accepting Host (CAH)
Host processing system that forms the interface between the CAS and the CIS and to which the CADs are connected. The CAH collects from the CADs the data relating to the card transaction and initiates that data to the CIS. For the processing of security related data an SCD is part of the CAH processing system.

EBS105 Part 1 [TC1]

Card-Accepting Scheme (CAS)
A set of technical concepts, rules, protocols, algorithms, functions, commercial agreements and administrative procedures which form the basis for a card payment system. The CAS is controlled by its responsible Administrator (CAS Administrator).

EBS105 Part 1 [TC1]

Card-Issuing Scheme (CIS)
A set of technical concepts, rules, protocols, algorithms, functions, commercial agreements and administrative procedures which form the basis for the issuance of a payment card. The CIS is controlled by its respective administrator (CIS Administrator).

EBS105 Part 1 [TC1]

Card issuer
An institution, which issues the financial transaction card to the cardholder, and which bears ultimate financial responsibility for a card originated transaction.

A substantially modified version of the ISO 8583 definition
[TC1]

Card scheme
A body representing a group of card issuers, one purpose of which is to facilitate the issuance and acceptance of the cards of that group. Interchange among the card scheme members must be covered by a set of operating procedures.

The definition used in ISO 7812-2 [TC1]

Card Session
A link between the card and the terminal starting with the Answer to Reset and ending with a subsequent reset or a deactivation of the contacts.

EBS111 [TC1]

Cardholder
A customer associated with the account identification on the card or customer owning the card in the case of anonymous card products not related to any account.

Derived from ISO 8583 (ORG9003 term) [TC1]

CAS
See *Card Accepting Scheme*

[TC1]

Certificate
The public key and identity of a user, together with some other information, rendered authentic by signing the certificate with the private key of the certifying authority, which issued that public key certificate.

Derived from TR402 (Derived from ISO 9594-8 & almost
TR408 Part 2 (ISO 15782). [TC4]

Certificate database
Storage area in the PTD (personal trusted device) for service certificates and root certificates.

TR603 [TC6]

Certificate policy
A named set of rules indicating the applicability of a certificate to a particular community and/or class of application with common security requirements.

TR402 [TC4]

Certificate Revocation List (CRL)
A signed list of invalidated certificates.
Derived from TR402 (Derived from ISO 15782) [TC4]

Certification Authority (CA)
An entity entrusted by one or more entities to create and assign certificates, and to manage the revocation of public key certificates.
EBS111 & TR402 Part 2 (Almost ISO 15782) [TC4]

Certification path
An ordered sequence of certificates of entities, which, together with the public key of the initial entity in the path, can be processed to obtain the public key of the final entity in the path.
TR402 (ISO 15782) [TC4]

Certification Practice Statement (CPS)
A statement of the practices, which a Certification Authority employs in issuing certificates.
TR402 (ISO 15782) [TC4]

Charge card
A card issued by non-banks indicating that the cardholder has been granted a line of credit.
The definition used by BIS to define a Travel and Entertainment card [TC1]

Chargeback
A transaction from the card issuer to the acquirer and/or acceptor used to partially or completely reverse a previously completed financial transaction.
The 8583 definition (with the addition of "and/or acceptor") [TC1]

Charging option
Stipulation of how charges for a direct debit are split between the creditor and the debtor.
TR210 [TC2]

Check digit
A digit or digits (character(s)) which may be used to verify the accuracy of the string through a mathematical relationship to the string.
Derived from ISO 7064 definition [TSC]

Cheque guarantee card
A card issued as part of a cheque guarantee system.
BIS definition [TC1]

CIS
See *Card-issuing scheme*
[TC1]

Clearing
The process of exchanging payment orders or security transfer instructions prior to settlement, including netting of instructions and the establishment of final positions for settlement.
Derived from BIS [TC2]

Clearing cycle
The length of time in banking business days or hours between the input of payments to the clearing system and the availability of funds to the beneficiary's financial institution. There may be different cycles for different types of transactions.
TR210 [TC2]

Clearing system
The banking systems and procedures for the clearing of payments between banks.
TR210 [TC2]

Completion code
A part of the response from any component on a given command. It indicates whether the command was successful or not. In the latter case the completion code indicates the reason why it was not successful.
EBS111 (prEN 1546-2) [TC1]

Confidentiality
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
TR406 (ISO7498-2) [TC4]

Consistent User Experience (CUE)
A similar user experience among phones of different make and type. For example, the user experience of Web shopping shall be largely similar among MeT compliant phones. CUE also includes consistency of user experience when using the same core function in different usage scenarios (user authorisation, for example, shall generate the same user experience in the usage scenarios Web shopping and retail shopping).
TR603 (MeT definition) [TC6]

Content provider
The content provider provides goods and services to the user by hosting a content server.
TR603 (MeT definition) [TC6]

Counter-value payment
A transaction denominated in one currency and the instruction that the equivalent amount in another currency is to be paid to the beneficiary.
ORG9003 term [TC2]

CPS
See *Certification Practice Statement*
[TC4]

Credit card
A card indicating that the holder has been granted a line of credit.
The first sentence of the BIS definition [TC1]

Credit transfer
A direct payment from one bank account to another initiated by the payer.

ORG9003 term [TC2]

Creditor
The party, which is owed funds by the debtor.

TR205 & TR210 [TC2]

Creditor's financial institution
The financial institution with whom the creditor maintains holds an account on which he receives the funds are credited. It may also be the financial institution, which is responsible for supporting the creditor's application to join a direct debiting scheme (sponsoring financial institution).

TR210 [TC2]

Creditor's identification number
A number identifying the creditor within a National Direct Debit Scheme. It may be:
- The bank account number,
- A unique number for each creditor given by a national organisation,
- Any other type of identifier.

TR210 [TC2]

Creditor's transaction reference
Transaction identification initiated by creditor, and can be part of creditor's own accounting/invoicing system.

TR210 [TC2]

CRL
See *Certificate Revocation List*

[TC4]

Cross-border payment
A payment by an originator whose account from which payment is to be made, is held by an institution or its branch in one country, to be made available to a beneficiary at an institution or its branch in another country.

Derived from Internal Market DG [TSC]

Cross-certification
A process by which two Certification Authorities mutually certify each other's public keys.

TR402 (ISO 15782) [TC4]

Cryptographic module
A set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, and is contained within the cryptographic boundary of the module. (FIPS PUB 140-1).

TR402 (Almost ISO 15782) [TC4]

Cryptography
The discipline, which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.

TR406 (ISO 7498-2) [TC4]

Cryptoperiod
See key cryptoperiod.

TR406 & TR408 [TC4]

Currency
The medium of exchange of value defined by reference to the geographical location of the authorities responsible for it.

ISO 8908 (also ISO 4217: Currency codes) [TSC]

Customer
Person having subscribed to a domestic or international payment scheme of an issuing bank or institution.

TR603 [TC6]

Cut-off time
A time of day specified by the receiver before which a batch must be received for processing to commence on that day.

EBS200 & TR210 [TC2]

Data elements
The items of variable information printed by the beneficiary or supplied by the ordering customer.

EBS206 [TC2]

Data element descriptions
The text that describes each data element on the IPI form.

EBS206 [TC2]

Data Encryption Algorithm (DEA)
See *DES*

[TC4]

Data Encryption Standard (DES)
See *DES*

[TC4]

Data integrity
The property that data has not been altered or destroyed in an unauthorised manner.

TR406 (7498-2) [TC4]

Data key
A cryptographic key used for the encipherment, decipherment, verification or authentication of data.

TR101 [TC4]

Data origin authentication
The corroboration that the source of data received is as claimed.

EBS111, TR402 & TR406 (ISO 7498-2) [TC4]

DEA
See DES *(Data Encryption Standard)*
[TC4]

Debit advance advice
Advice sent by or on behalf of the debtor's financial institution to the debtor to inform him that a debit is to be made.
Derived from TR205 & TR210 [TC2]

Debit advice
Advice sent by the debtor's financial institution to the debtor to inform him that a direct debit is to be or has been made.
Derived from TR205 & TR210 [TC2]

Debit card
A card enabling the cardholder to have his purchases directly charged to funds on his account at a financial institution.
Modified BIS definition [TC1]

Debit transfer
See *Direct debit*
[TC2]

Debtor
The party, which owes funds to the creditor.
TR210 (ORG9003 term) [TC2]

Debtor's financial institution
The financial institution with whom the debtor holds an account on which the funds are debited.
TR210 [TC2]

Decipherment
The reversal of a corresponding reversible encipherment.
TR406 (ISO 7498-2 [19]) [TC4]

Decryption
See *Decipherment*.
TR406 [TC4]

DES (Data Encryption Standard)
Data Encryption Standard (also known as DEA, Data Encryption Algorithm): symmetric block cipher encryption algorithm defined in the American standard FIPS 46-2 (1977). DES is used either as "single DES" with a 56 bit key, or as "triple DES" with 112 bits or 168 bits keys.
(ORG9003 term) [TC4]

Digital signature
Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient.
(ISO 7498-2) [TC4]

Direct debit
The automated transfer of funds from a debtor's account to a creditor's account at the initiative of the creditor and based on the debtor's authorisation.
Derived from TR205 & TR210 [TC2]

Direct debit contract
An agreement between the creditor and the creditor's financial institution and possibly a third party, which allows the creditor to originate direct debits.
Derived from TR205 & TR210 [TC2]

Direct debit mandate
An agreement authorised by the debtor allowing the creditor to originate direct debits for debiting the debtor's account.
Derived from TR205 & TR210 [TC2]

Dual chip
A payment solution in which the banking data (especially authentication credentials) and sometimes also the payment application is located on a bank-issued second chip, independent of the SIM. The second chip is semi-permanently installed in the mobile device by the end-user or a service provider.
TR603 [TC6]

Dual slot payment solution
A payment solution in which the device is equipped with a card reader in which the customer inserts his/her payment card when paying. In this model, part of the banking application resides in the SIM. In the future, the second reader may sometimes be dissociated from the mobile device, and dialogue with it using a wireless protocol (e.g. Bluetooth).
TR603 [TC6]

Due date/maturity date
The date - agreed date between creditor and debtor - on which the beneficiary is credited (credit transfers) or when the debtor is debited (direct debits). An agreed payment date between creditor and debtor. It is also known as date of maturity. Some domestic banking payment standards support due date.
TR205 & TR210 [TC2]

EEBSF
See *European Electronic Banking Standards Framework*
[TC6]

EEP
See *European Electronic Purse*
EBS111 [TC1]

EF
See *Elementary File*
EBS111 [TC1]

Electronic banking
Provision of banking services from a bank to a customer using a customer-supplied device (e.g. personal computers, small and medium-sized enterprise, or corporate customer) using a customer device connected to a network.

TR600 & TR601 [TC6]

Electronic banking standard
Specification covering formats, protocols, and interfaces to meet a particular set of business requirements.

Questionnaire for requirements for a common EEBSF
TR601 [TC6]

Electronic commerce
Transactions relating to commercial activities that are based upon the processing and transmission of digitised data.

OECD [TC6]

Electronic purse
An application able to store and process electronic value.

TR103 [TC1]

Electronic services
Services offered by banks to their customers via electronic means.

TC6's Terms of Reference [TC6]

Electronic signature
Data in electronic form which are attached to or logically associated with other data and which serve as a method of authentication.
[TC4 Note: An electronic signature concept makes use of a "digital signature" mechanism but may involve additional data or procedural requirements.]

Electronic Signature Directive [TC4]

Electronic value (EV)
The counterpart of a bank deposit. It is value stored and exchanged in an electronic purse scheme and has no legal tender status.

Derived from EBS111 & TR103 [TC1]

Elementary File (EF)
A set of data records which share the same file identifier. It cannot be the parent of another file.

EBS111 [TC1]

Encipherment
The cryptographic transformation of data (see cryptography) to produce ciphertext.

TR406 (ISO 7498-2) [TC4]

Encryption
See *Encipherment*

TR406 [TC4]

Entity authentication
The corroboration that an entity is who it claims to be.

EBS111 [TC1]

Entry Point Financial Institution (EPFI)
The first financial institution or ACH that receives a cross-border transaction in the receiving country.

TR210 [TC2]

EPFI
See *Entry Point Financial Institution*

[TC2]

European Electronic Banking Standards Framework (EEBSF)
Compilation of mandatory and optional European electronic banking business requirements. The standards framework applies to all electronic distribution channels and covers the requirements of personal, SME and corporate markets.

Questionnaire for requirements for a common EEBSF
TR601 [TC6]

European Electronic Purse (EEP)
European Electronic Purse. An ICC application as described in this Standard.

EBS111 [TC1]

European Electronic Purse (EEP) Message
A string of bytes transmitted by the terminal to the card or vice-versa, excluding transmission control characters.

EBS111 [TC1]

European Electronic Purse (EEP) ID
The unique identification of an EEP. It consists of the Purse Provider ID and the Purse ID.

EBS111 [TC1]

European Electronic Purse (EEP) Scheme
A Purse Scheme that conforms to this Standard. (See Purse Scheme).

EBS111 [TC1]

Exchange rate
Rate used to convert an amount from one currency into another.

EBS200 [TC2]

Financial institution
An institution authorised to accept deposits (licensed deposit taker), and to provide financial services directly to a customer.

ORG9003 term [TSC]

Financial Institution Entry Point (EPFI)
The first Financial Institution that receives a transaction in the receiving country.

TR210 (ORG9003 term) [TC2]

Float

A float is collected as payment for the loading operation. It is used to pay liability due to acquiring banks and purse holders and allows a guarantee to be given to acceptors. A float is never considered as the purse holder's deposit. There is no net creation of money.

TR103 [TC1]

Four-box model

The "four-box model" could be described as the banking version of open standards where the payer and the payee can interact although they have agreements with two different (and competing) banks. The reason for this is that the banks themselves have an agreement to participate in an enabling network (such as Visa, MasterCard, SWIFT, giro systems).

TR603 [TC6]

Generation of ePI

The process of creating an ePI. An ePI is created by, or on behalf of, the beneficiary.

EBS602 [TC6]

Generation of IBAN

The one time process of creating an IBAN for an account. This process is under the sole responsibility of the bank servicing the customer's account.

SIG203 [TC2]

Hash function

A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A 'good' hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range.

TR406 (ISO 9594-8) [TC4]

IBAN

See *International Bank Account Number*

SIG203 [TC2]

ICC

See *Integrated Circuit Card*

[TC1]

IC

See *Integrated Circuit*

[TC1]

Initialisation

Provisioning the PTD (Personal Trusted Device) with one or more public-private key pairs and root certificates.

TR603 (MeT definition) [TC6]

Initiation of Funds Transfer Instruction

The creation of a funds transfer instruction by the ordering customer based on the ePI data e.g. importation of ePI data elements at the ordering customer's site into an electronic payment order, such as a cross-border payment template in an electronic banking application.

EBS602 [TC6]

Integrated Circuit (IC)

An electronic component designed to perform processing and/or memory functions.

ISO 8908 [TC1]

Integrated Circuit Card (ICC)

An ID-1 card type (as specified in ISO 7810, ISO 7811 parts 1-5, ISO 7812 & ISO 7813) into which has been inserted one or more integrated circuits.

ISO 8908 [TC1]

Integrity

The property of ensuring that information is not altered in any way, either by accident or with fraudulent intent.

Derived from EBS 200 [TC4]

Interbank settlement amount

Amount paid by the receiving bank to the sending bank.

TR 210 [TC2]

Interbank settlement date

The date on which reimbursement funds are available to the sender (direct debits).

TR210 (ORG9003 term) [TC2]

Interbank settlement value date

The date on which reimbursement funds are available to the receiver.

EBS200 [TC2]

International Bank Account Number (IBAN)

An expanded version of the Basic Bank Account Number (BBAN) used internationally to uniquely identify the account of a customer at a financial institution.

SIG203 (ISO 13616) [TC2]

International Payment Instruction (IPI)

A paper form for credit transfer instructions to be combined with [cross-border] invoices in order to facilitate automated [cross-border] credit transfers.

EBS206 [TC2]

IPI

See *International Payment Instruction*

[TC2]

Issuer

The financial institution which issues payment cards.

EBS105 Part 1 [TC1]

Or

An entity which has issued a service certificate for a key pair in the PTD. Typically this might be a bank or a credit card company. The entity and its supporting infrastructure are used synonymously.

TR603 (MeT definition) [TC6]

Issuing
It is the process by which beneficiaries prepare and send out IPIs to ordering customers for payment.

SIG208 [TC2]

Issuing bank
A financial institution that issues a means of payment to its customers. A means of payment could be a real card, a virtual card, cash, virtual cash, etc.

TR603 [TC6]

Key
A sequence of symbols that controls the operations of encipherment and decipherment.

TR406 (ISO 7498-2) [TC4]

Key cryptoperiod
The time period over which a key is valid for use by legitimate parties.

TR406 [TC4]

Key establishment
A process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use.

TR406 [TC4]

Linked load
A load against the EEP's associated account.

EBS111 [TC1]

Linked purse
An EEP application with a reference to a funding account. This reference shall reside either in the EEP application or on the Purse Provider host.

EBS111 [TC1]

Load device
A physical device operated by a load agent and used jointly by a purse holder and the load agent to transfer value to the purse holder's electronic purse.

EBS111 [TC1]

Load Secure Application Module (LSAM = Load SAM)
A SAM installed at the Loading Operator's Side, providing the necessary security for the communication between the Loading Operator and the Purse Provider.

EBS111 [TC1]

Load transaction
The transaction performed using a load device whereby electronic value is transferred to an electronic purse.

EBS111 [TC1]

Loading operator (or agent)
An organisation, which operates load devices. It collects, processes and forwards all applicable transaction details to the purse provider.

EBS111 [TC1]

Local environment
An MeT-defined environment in which the PTD accesses content via local or personal area network.

TR603 (MeT definition) [TC6]

LSAM
See *Load Secure Application Module*

[TC1]

MAC
See *Message Authentication Code*

TR406 [TC4]

Macro payment
Typically those payments above €25.

TR603 [TC6]

MD
See *Mobile device*

TR603 [TC6]

MDC
See *Modification Detection Code*

[TC4]

Medium payment
Typically those payments between €2 and €25.

TR603 [TC6]

Merchant
A professional (or body) that is authorised to receive funds in exchange for the delivery of goods or services and that has established an agreement with a bank for accepting the said funds (means of payment). A merchant may operate a server (merchant's server), which may enable a customer to choose a means of payment and which stores the transaction for eventual compensation.

TR603 [TC6]

Message Authentication Code (MAC)
This is a code contained in a message between a sender and receiver used to validate the source and part or all of the text of the message. The code is the result of an agreed calculation.

TR406 [TC4]

MeT

Mobile electronic transactions. Technical framework and application guidelines for secure transactions with mobile trusted devices.

TR603 (MeT definition) [TC6]

Micro payment

Encompasses the lowest payment values, typically under €2.

TR603 [TC6]

Mobey Forum

Financial industry-driven forum, whose mission is to encourage the use of mobile technology in financial services.

TR603 [TC6]

Mobile banking

A range of traditional banking services, including push payments, where a customer gives the order to the bank to execute a transfer of funds, conducted via a mobile trusted device.

TR603 [TC6]

Mobile commerce

Electronic commerce using mobile devices as the customer device, e.g., mobile phones.

ORG9003 term [TC6]

Mobile device (MD)

A set of seamlessly compatible hardware and software used interactively by a customer for making transactions wirelessly to other receiving parties which can be remote (e.g., server located on some communication network including the Internet) or face-to-face (e.g., electronic terminals like POS, vending machines, parking meters). Examples of mobile devices are mobile phones, PDAs and interactive laptops [See also *mobile trusted device* and *personalised mobile trusted device*].

TR603 [TC6]

Mobile payment (m-Payment)

A mobile payment is not by itself a new payment instrument but an access method to activate an existing means of payment for financial transactions processed by banks between bank customers. An m-payment involves a wireless device that is used and trusted by the customer. M-payments may be card based or non-card based, in both the real and virtual world.

TR603 [TC6]

Mobile Payment Forum (MPF)

Established by American Express, JCB, MasterCard and Visa end 2001, MPF is the successor to CMCIG.

TR603 [TC6]

Mobile Trusted Device (MTD)

A mobile device used by the customer to perform a transaction, which meets the standards for the schemes in which it will be used. This system may be owned by the customer or by a service provider or bank, e.g. PC, mobile phone, card reader provided by one's bank, etc. [see also *mobile device* and *personalised mobile trusted device*].

TR603 [TC6]

Modification Detection Code (MDC)

An unkeyed hash function whose specific purpose is message integrity.

TR406 [TC4]

Money laundering regulations

Regulations that describe the way that financial institutions should act to prevent money laundering.

TR210 [TC2]

Mutual authentication

The process, whereby, during a transaction (and for every step in an incremental Purchase Transaction) the EEP is authenticated by the terminal and the terminal is authenticated by the EEP.

EBS111 [TC1]

National direct debit scheme

A set of rules and operational procedures built by a national banking community in order to operate efficient and secure direct debiting in an individual country. According to local domestic needs there may exist one or more National Direct Debit Schemes in a country.

TR205 & TR210 [TC2]

Network service provider

An institution responsible for routing, and/or providing other value added network services, on information passing between acceptor and card issuer.

ORG9003 term [TC1]

Non-pre-authorised direct debits

Direct debits based on rules that require a specific agreement from the debtor for each individual transaction to be effected.

TR210 [TC2]

Non-repudiation

A process that involves delivering data in such a way that the receiver cannot deny receipt, and the sender cannot deny sending it.

EBS200 [TC4]

Nostro account

A record kept by an account-owner bank of an account serviced on its behalf by an account-servicing bank.

ISO 8908 [TSC]

Notification of credit
Reporting to the beneficiary of incoming funds by the BFI with or without additional remittance information.
EBS602 [TC6]

Notification of IBAN
The one time operation of informing the account owning customer of the IBAN generated for the account.
SIG203 [TC2]

Off-line
Deferred processing without direct communication.
ORG9003 term [TC2]

Off-line PIN verification
The process whereby the integrated circuit card checks the transaction PIN.
EBS111 [TC1]

Off-line transaction
A transaction that does not require a real-time connection to a secure application module.
EBS111 [TC1]

On-line
Direct communication between devices with electronic capability (terminals, networks, hosts, etc.).
ORG9003 term [TC2]

On-line PIN Verification
The process whereby the PIN is sent to the issuer for checking.
Derived from EBS111 [TC1]

On-line transaction
A transaction that requires a real-time connection to a secure application module.
EBS111 [TC1]

Ordering customer
The initiator of a funds transfer instruction. The term Ordering Customer is used as a synonym for the ECBS term Originator.
EBS206 [TC2]

Ordering customer's financial institution (OFI)
The OFI holds the account of the ordering customer and executes an initiated payment on behalf of the ordering customer.
EBS602 [TC6]

Original ordered amount
The transaction amount instructed by the debtor.
TR210 [TC2]

Originator
The initiator of a funds transfer instruction.
EBS200 [TC2]

PAN
See *Primary Account Number*
[TC1]

Payment order
An instruction in any form, given to a financial institution, to place at the disposal of a beneficiary an amount of money.
Derived from Internal Market DG [TC2]

PDA
See *Personal Digital Assistant*
TR603 [TC6]

PDF417
Two-dimensional bar code: Portable Data File 417.
TR210 [TC2]

PED
See *PIN Entry Device*
[TC1]

Personal Digital Assistant (PDA)
Any small mobile handheld device that provides computing and information storage and retrieval capabilities for personal or business use.
TR603 [TC6]

Personal Identification Number (PIN)
Code or password the customer possesses for verification of identity.
ISO 9564-1 [TSC]

Personal Mobile Trusted Device (PMTD)
A mobile trusted device where personal customer information can be stored (through registration, e.g. of service certificates) that is used for his/her authentication [See also *mobile device* and *mobile trusted device*].
TR603 [TC6]

PIN
See *Personal Identification Number*
[TSC]

PIN Entry Device (PED)
Device into which the cardholder inputs the PIN. A PED may also be called a PIN pad.
EBS100 (ISO 9564-1) [TC1]

PIN entry keyboard
A keyboard with the digits assigned in three columns, digits 1, 2 and 3 appearing in the top row, and digit 0 being located in the central column in the bottom (fourth) row of the keyboard.
EBS100 [TC1]

PKI
See *Public Key Infrastructure*
[TC4]

PMTD
See *Personal Mobile Trusted Device*
TR603 [TC6]

Point of Sale (POS)
The provision of goods and services at attended and unattended terminals.
Derived from EBS105 Part 1 [TC1]

POS
See *Point of Sale*
EBS105 Part 2 [TC1]

PPSAM
See *Purse Provider SAM*
[TC1]

Pre-authorised direct debit
Direct debit based on an initial general mandate given by the debtor.
TR210 [TC2]

Primary Account Number (PAN)
A number used to identify a customer account or relationship. The PAN identifies the card issuer and the cardholder. This number is composed of a card issuer identification number, an individual account identification number and an accompanying check digit.
(Derived from ISO 8908) [TC1]

Private key
In a public key cryptosystem that key of a user's key pair which is known only by that user.
EBS111 & TR406 (ISO 9594-8) [TC4]

PSAM
See *Purchase SAM*
[TC1]

Public key
In a public key cryptosystem that key of a user's key pair which is publicly known.
EBS111 & TR406 (ISO 9594-8) [TC4]

Public Key Infrastructure (PKI)
A combination of hardware and software products, policies and procedures that provide the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed can communicate securely through a chain of trust. A Public Key Infrastructure is based on digital certificates that act like "electronic passports". It should consist of a security policy, a certification authority, a registration authority, a certificate distribution system and PKI-enabled applications.
TR408 Part 2 [TC4]

Or

A collection of hardware, software, policy and human roles that successfully bind a subscriber's identity to a key pair (public and private) through the issuance and administration of digital certificates throughout their "life-cycle" (creation, maintenance, archival records and destruction).
TR603 [TC6]

Purchase cancellation trace
A set of data elements specifying all relevant details of a Purchase Cancellation Transaction kept in the Purchase Device.
EBS111 [TC1]

Purchase cancellation transaction
A transaction performed at a Purchase Device in order to cancel the last Purchase Transaction in the EEP.
EBS111 (prEN 1546-1) [TC1]

Purchase device
A physical device, operated by the Acceptor, used to accept payment from an EEP in a Purchase Transaction.
EBS111 [TC1]

Purchase reversal
A part of a Purchase Transaction that recovers the previous status of the EEP if a problem prevented the Purchase Transaction from being finished successfully.
EBS111 [TC1]

Purchase SAM (PSAM)
A SAM (Secure Application Module) installed in connection with a Purchase Device providing the necessary security for purchase-related transactions and the collection process.
EBS111 (prEN 1546) [TC1]

Purchase SAM ID (PSAM ID)
The unique identification of a PSAM (Purchase Secure Application Module). It consists of the Acquiring Technical Operator ID and the PSAM number.
EBS111 [TC1]

Purchase trace
A set of data elements specifying all relevant details of a Purchase Transaction kept in the Purchase Device.
EBS111 [TC1]

Purchase transaction
The transaction performed using a Purchase Device whereby value is transferred from an EEP to the Purchase Device in exchange for goods or services.
EBS111 (prEN 1546-1) [TC1]

Purse holder
Any person in possession of an electronic purse.
EBS111 & TR103 [TC1]

Purse provider

The organisation that is responsible for installing the electronic purse application in the integrated circuit card and guaranteeing the electronic value in the electronic purse.

Derived from EBS111 [TC1]

Purse Provider SAM (PPSAM)

The SAM of the Purse Provider providing the necessary functionality for the secure transactions of the EEP Scheme as seen from the Purse Provider's viewpoint (e.g. secure activation, load and auditing functions).

EBS111 (prEN 1546) [TC1]

Purse scheme

A set of rules and regulations for issuance, acceptance and use of electronic purse cards established and enforced by an organisation(s).

EBS111 [TC1]

Purse scheme administrator

The entity responsible for the purse scheme rules, security and overall scheme management.

EBS111 [TC1]

Qualified certificate

A certificate that meets specific requirements laid down by Annex I of the EU directive on electronic signatures and is provided by a certification-service-provider who fulfils requirements laid down by Annex II of the same directive.

TR408 Part 2 (EU directive) [TC4]

RA

See *Registration Authority*

[TC4]

Real time

The transmission, processing or settlement of a funds or security transfer instruction on an individual basis at the time it is initiated.

BIS [TSC]

Reading device

A physical device allowing at least the balance of an EEP to be read and displayed. May be owned and operated by the card holder personally. May also be integrated into Purchase and Load Devices.

EBS111 [TC1]

Reason code for batch rejection

Coded information describing the reason why a receiver has rejected a batch.

TR210 [TC2]

Reason code for ejection

Coded information describing the reason why a receiver has rejected a transaction.

TR210 [TC2]

Reason code for return

Coded information describing the reason why a receiver has returned a transaction.

TR210 [TC2]

Receiver

The Receiver of the message currently being referred to.

TR210 (ORG9003 term) [TSC]

Receiver's correspondent

Financial institution which holds the receiver's settlement/ reimbursement account.

TR210 (ISO 8908) [TSC]

Receiver's correspondent account

The receiver's settlement/reimbursement account at the receiver's correspondent.

TR210 [TC2]

Receiver's transaction charge

Charge levied on the receiver's side in respect of a specific transaction.

TR210 [TC2]

Record

A string of bytes which is retrieved as a whole from the card and referenced by a record number.

EBS111 [TC1]

Record number

A sequential number assigned to each record, which uniquely identifies the record within its EF.

EBS111 [TC1]

Reference for return

Unique reference generated by the sender of a returned transaction.

TR210 [TC2]

Registration

Provisioning the PTD with a service certificate that is related to a public-private key pair residing on the PTD.

TR603 (MeT definition) [TC6]

Registration Authority (RA)

An entity responsible for the identification and authentication of subjects of certificates, but which does not sign or issue certificates.

TR402 & TR408 Part 2 (Derived from ISO 15782) [TC4]

Regulatory authorities

National bodies, which require the collection of information on cross-border payments.

TR205 & TR210 [TC2]

Regulatory reporting information

Information on cross-border payments, which has to be reported to relevant bodies.

EBS200 & TR210 [TC2]

Rejection
A rejection is a refusal to execute a direct debit instruction. Rejection is initiated by the debtor's bank or by an ACH.

TR210 [TC2]

Reimbursement
An arrangement by which a party is repaid for payments made according to the instructions of another party.

ISO 8908 [TSC]

Relying party
Recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

TR408 Part 2 (ETSI) [TC4]

Remittance information
Information supplied by the creditor to be passed to the debtor.

TR210 [TC2]

Remote environment
An MeT-defined environment in which the PTD accesses content via a public mobile network.

TR603 (MeT definition) [TC6]

Repudiation
Denial by one of the entities involved in a communication of having participated in all or part of the communication.

TR406 (ISO 7498-2) [TC4]

Requested execution/processing date
Date provided by the sender on which the Entry Point Financial Institution (or an ACH acting on behalf of the Entry Point Financial Institution) should initiate the transaction. If no date is specified or the date is not a banking business day, the transaction will be executed at first opportunity.

TR210 [TC2]

Return
In case of a single direct debit included in a batch can not be processed by the debtor's bank for technical reasons, e.g. account blocked or frozen, this direct debit is returned to the creditor's bank without debiting the debtor's account.

TR210 [TC2]

Reversal
A transaction from the acquirer, and/or acceptor, to the card issuer informing the card issuer that the previously initiated transaction cannot be processed as instructed, i.e., is undeliverable, unprocessed, or cancelled by the receiver.

The 8583 definition (with "and/or acceptor" added)

[TC1]

Or:
A recall of funds from the creditor to the debtor relating to a previous settlement. A reversal instruction is initiated by the creditor.

TR210 [TC2]

Revocation
Revocation is a process to claim for reimbursement of direct debit after settlement.
A revocation instruction is initiated by the debtor or his the debtor's bank.

TR210 [TC2]

Rivest Shamir Adleman (RSA)
See *RSA*

[TC4]

RSA (Rivest Shamir Adleman)
Rivest Shamir Adleman (names of the inventors: public key cryptosystem that may be used either to produce and verify digital signature or for confidentiality. RSA was published initially in "Communications of the ACM, 21 (1978)."

(ORG9003 term) [TC4]

SATK
See *SIM toolkit*

TR603 [TC6]

SCD
See *Secure Cryptographic Device*

EBS105 Part 1 [TC1]

Secret key
A key used with symmetric cryptographic techniques and usable only by a set of specified entities.

EBS111 & TR406 (ISO11770-1) [TC4]

Secure Cryptographic Device (SCD)
A secure cryptographic device (SCD) is a physically and logically protected hardware device that provides a secure set of cryptographic services. In assessing the physical security of any device, the operational environment is an important consideration.

EBS105 Part 1 [TC1]

Sender
Originator of the message currently being referred to.

TR210 (ORG9003 term) [TSC]

Sender's correspondent
Financial institution, which holds the sender's account.

TR210 [TC2]

Sender's correspondent account
The sender's account at sender's correspondent.

TR210 [TC2]

Sender's reference
Sender's unique reference for a batch.

TR210 [TC2]

Sender's transaction charge
Charge levied on the sender side in respect of a specific payment transfer transaction.

TR210 [TC2]

Sender to receiver information
Additional information for the receiver.

TR210 [TC2]

Server
A computer program that provides services to other computer programs in the same or other computers.

TR603 [TC6]

Service certificate
Certifies that a public-private key pair is valid for a specific service.

TR603 (MeT definition) [TC6]

Settlement
An act that discharges obligations in respect of funds or securities transfers between two or more parties.

EBS111 (BIS) [TSC]

Settlement institution
A financial institution through which reimbursement is (to be) effected.

ORG9003 term [TSC]

Short Message Peer to Peer (SMPP)
This is an open, industry standard messaging protocol designed to simplify integration of data applications with wireless mobile networks.

TR603 [TC6]

Short Message Service (SMS)
The exchange of short messages between mobile trusted devices and possibly even computers in "store and forward" mode.

TR603 [TC6]

Signatory
A person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.

Electronic Signature Directive [TC4]

Signature-creation data
Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Electronic Signature Directive [TC4]

Signature-creation device
Configured software or hardware used to implement the signature-creation data.

Electronic Signature Directive [TC4]

Single SIM payment solution
A payment solution in which part or all of the banking data and sometimes of the banking application necessary to perform a payment resides on the SIM.

TR603 [TC6]

SIM
See *Subscriber Identification Module*

TR603 [TC6]

SIM toolkit (SATK)
The SIM Application Toolkit allows to develop applications on the SIM card (ETSI: GSM 11.14).

(MasterCard Europe definition) TR603 [TC6]

Single authentication
The process, whereby, during a transaction (and for every step in an incremental Purchase Transaction), the EEP is authenticated by the terminal but the terminal is not authenticated by the EEP.

EBS111 [TC1]

SMPP
See *Short Message Peer to Peer*

TR603 [TC6]

SMS
See *Short Message Service*

TR603 [TC6]

Sponsoring bank
The sponsoring bank is the creditor's bank that initially sponsors the creditor into a National Direct Debit Scheme. The sponsoring bank acts as guarantor of the creditor's direct debiting procedures.

TR210 [TC2]

Stream cipher
A cryptographic algorithm which encrypts individual character (usually binary digits) of a plaintext message one at a time. A stream cipher may be defined as a block ciper where blocklength is equal to one.

TR406 [TC4]

Subscriber Identification Module (SIM)
A mobile operator's smart card that contains its subscriber's relevant data and applications (e.g. telephone application, message service, e-mail service, etc).

TR603 [TC6]

Symmetric algorithm
A cryptographic algorithm employing the same value of key for both enciphering and deciphering or for both authentication and validation.

TR406 [TC4]

Test key
A code used to validate the source, and part or all of the text of a message, and which is capable of manual calculation.

ORG9003 term [TC4]

Ticket
A downloaded object that shows that a fare or admission has been paid.

TR603 (MeT definition) [TC6]

Transaction amount
The amount of a transaction as it crosses the border.

TR210 [TC2]

Transaction code
In addition to the bank operation code, the transaction code contains other relevant information: type of underlying agreement between creditor and debtor, rejection/revocation conditions, etc.

TR210 [TC2]

Transaction details
A set of data elements specifying all relevant details of an EEP transaction.

EBS111 [TC1]

Transaction reference
Sender's unique reference for a transaction.

TR210 [TC2]

Transaction reference by creditor
Transaction identification initiated by creditor, and can be part of creditor's own ac-counting/ invoicing system.

TR210 [TC2]

Transaction type code
A code that identifies the nature, purpose and/or reason of an individual transaction, primarily used for regulatory reporting requirements.

TR210 [TC2]

Transfer of ePI
Transport of the ePI via electronic means from or on behalf of the beneficiary to the ordering customer.

EBS602 [TC6]

Transfer of funds
Processing and payment execution.

EBS602 [TC6]

Transfer of IBAN
Transport of the IBAN in an operational message.

SIG203 [TC2]

Transfer of Payment Order
Sending the completed payment order from the ordering customer to the OFI.

EBS602 [TC6]

Truncation
A procedure in which the physical movement of paper payment instruments (e.g. paid cheques or credit transfers) within a bank, between banks, or between a bank and its customer is curtailed or eliminated, being replaced, in whole or in part, by electronic records of their content for further processing and transmission.

EBS111 (BIS) [TSC]

Trusted Third Party (TTP)
An organisation, which delivers services to increase the reliability of electronic exchange of information. Such services may include archiving of certificates, time stamping, attribute certification. A CA must have the status, credentials and qualifications of a TTP.

TR402 [TC4]

TTP
See *Trusted Third Party*

[TC4]

Unattended terminal
A terminal designed to be used by the cardholder in self-service mode.

ORG9003 term [TC1]

Unlinked Purse
An EEP application without a reference to a funding account.

EBS111 [TC1]

Unstructured Supplementary Service Data (USSD)
The exchange of short messages between mobile trusted devices and possibly even computers in "dialogue" mode.

TR603 [TC6]

Usage Scenarios
Examples of how MeT can be applied when providing services such as retail or web shopping, web banking, ticketing, etc. to end users.

TR603 (MeT definition) [TC6]

User
The person in possession of a PTD and able to verify him/herself to the PTD.

TR603 (MeT definition) [TC6]

User interface
The man-machine interface between the user and the PTD.

TR603 (MeT definition) [TC6]

USSD
See *Unstructured Supplementary Service Data*

TR603 [TC6]

Value
Currency code and amount.

ORG9003 term [TSC]

Value date
The date on which interest is earned.
ORG9003 term [TSC]

Vostro account
Account serviced by a bank on behalf of an account owner bank.
ISO 8908 (deprecated term) [TSC]

Wallet
Something that contains a means of payment, e-commerce wallets are PC software, which contain the necessary sensitive information to handle payment transactions over the Internet.
TR603 (MasterCard Europe Definition) [TC6]

WAP
See *Wireless Application Protocol*
TR603 [TC6]

WIM
See *WAP Identity Module*
TR603 [TC6]

WIM card
WIM implemented on a smart card.
TR603 (MeT definition) [TC6]

Wireless Application Protocol (WAP)
A specification for a set of communication protocols to standardise the way that wireless devices (e.g. mobile phones) can be used to access information on the Internet.
TR603 [TC6]

WAP Identity Module (WIM)
A tamper-resistant device which is used in performing WTLS (Wireless Transport Layer Security) and application level security functions, and especially, to store and process information needed for user identification and authentication.
TR603 (WAP Forum Definition) [TC6]

3 COMMON ORGANISATION ABBREVIATIONS

ANSI
American National Standards Institute

APACS
Association of Payment Standards Institute

BITS
Banking Industry Technology Secretariat

CCIMB
Common Criteria Interpretation Management Board

CCMB
Common Criteria Management Board

CEN
European Committee for Standardisation (Comité Européen de Normalisation)

CEN/ISSS
European Committee for Standardisation (Comité Européen de Normalisation) Information Society Standardisation System

CENB
Comité Européen de Normalisation Bancaire (European Committee for Banking Standards)

CENELEC
Comité Européen de Normalisation Electrotechnique

CMFB
Committee for Monetary Financial Balance of Payment Systems

COCOM
Co-ordinating Committee on Multilateral Export Controls

COGEPS
Contact Group on Euro Payments Strategy

EACB
European Association of Co-operative Banks

EBA
European Banking Association

ECB
European Central Bank

ECBS
European Committee for Banking Standards

ECITC
European Commission for IT Testing and Certification

ECSA
European Credit Sector Association

EDIFACT
Electronic Data Interchange for Administration Commerce and Transport

eESC
eEurope Smart Card

EESSI
European Electronic Signature Standardisation Initiative

EMV
Europay-MasterCard-Visa

EPC
European Payments Council

EPS
European Payment System

ePSO
Electronic Payment Systems Observatory

ESBG
European Savings Bank Group

ESCB
European System of Central Banks

ESI
Electronic Signature Infrastructure working group

ETSI
European Telecommunication Standards Institute

FBE/EBF
Banking Federation of the European Union

FIPS
Federal Information Processing Standards

GMCIG
Global Mobile Commerce Interoperability Group (superseded by the Mobile Payment Forum)

GSEC
Group for Standardisation of Electronic Commerce

ICT
Information & Communications Technologies

ICTSB
Information & Communications Technologies Standards Board

IEC
International Electrotechnical Commission

IETF
Internet Engineering Task Force

IPRA
Internet Policy Registration Authority

IPTS
Institute for Prospective Technological Studies

ISIS
Information Society Initiative for Standardisation

ISO
International Organization for Standardization

ISSS
Information Society Standardisation System

IST
Information Society Technologies

ITU
International Telecommunication Union

JRC
Joint Research Centre (of the EU)

JTC
Joint Technical Committee

MeT
Mobile electronic Transactions

MPF
Mobile Payment Forum

NESSIE
New European Schemes for Signatures, Integrity and Encryption

NIST
National Institute of Standards and Technology

OASIS
Organisation for the Advancement of Structured Information Standards

PASG
Payment Advisory and Steering Group

PSG
Payment Systems Group

PSSG
Payment System Steering Group

PSTDG/PSULG
Payment Systems Technical Development Group/Payment Systems Users and Liaison Group

PSWG
Payment System Working Group

SCSUG
Smart Card Security Users Group

SWIFT
Society for Worldwide Interbank Financial Telecommunication

TeleTrusT
Non-profit organisation to promote the security of information and communication technology in an open systems environment.

UN
United Nations

4 OTHER COMMON ABBREVIATIONS

3GPP
3rd Generation Partnership Project

AAV
Accountholder Authentication Value

ACS
Access Control Server

AES
Advanced Encryption Standard

AID
Application identifier

ARPU
Average Revenue per User

B2B
Business to Business

B2C
Business to Client

BIN
Bank Identification Number

CA
Certification Authority

CAD
Card Accepting Devise

CAS
Card-Accepting Scheme

CAVV
Cardholder Authentication Verification Value

C2B
Customer-to-business

C2C
Customer-to-customer

CBC
Cipher Block Chaining

CC
Common Criteria

CCRA
Common Criteria Recognition Arrangement

CEPS
Common Electronic Purse Specification

CFB
Cipher Feedback

CIS
Card-Issuing Scheme

CRM
Customer Relationship Management

CRT
Chinese Remainder Theorem

CV
Control Vector

DDE
Dynamic Data Exchange

DIS
Draft International Standard (ISO)

DPI
Dots per inch

DSA
Digital Signature Algorithm

DSS
Digital Signature Standard

DUKPT
Derived Unique Key Per Transaction

ECDSA
Elliptic Curves Digital Signature Algorithm

EEP
European Electronic Purse

EEPROM
Electrically Erasable Programmable Read-Only Memory

ERP
Enterprise Resource Planning

EMV
(Eurocard-MasterCard-Visa) Integrated Circuit Card (ICC) Specification for Payment Services

FINREAD
Financial Transaction IC Card Reader

FTP
File Transfer Protocol

GSM
Global System of Mobile Communications (2nd generation mobile network standard)

GPRS
General Packet Radio Service

HSM
Host Security Module

HTML
HyperText Markup Language

HTTP
HyperText Transfer Protocol

IAS
Identification, Authorisation and Electronic Signatures

ICC
Integrated Circuit Card (chip card)

IDEA
International Data Encryption Algorithm

IDTV
Interactive Digital Television

IFES
Integer Factorization Encryption Scheme

IMSI
International Mobile System Identifier

IP
Internet Protocol

ISDN
Integrated Services Digital Network

ISIN
International Securities Identification Number

ISP
Internet Service Provider

ITSEC
Information Technology Security Evaluation Criteria

IV
Initialisation Vector

J2ME
Java 2 Platform, Micro Edition

KEK
Key Encrypting Key

MD
Message Digest

MIF
Multilateral Interchange Fee

MOSS
MIME Object Security Services

MPI
Merchant Server Plug-In

MSISDN
Mobile Subscriber Identification Service Digital Number

MT
Message Type

NFC
Near Field Communication

OAEP
Optimal Asymmetric Encryption Padding

OFB
Output Feedback

OLE
Object Link Embedding

OTA
Over The Air

P2P
Person to Person

PAYMENT GATEWAYSSL
Secure Socket Layer

PC
Personal Computer

PDA
Personal Digital Assistant

PGP
Pretty Good Privacy

PIN
Personal Identification Number

PKCS
Public Key Cryptographic Standard

PKI
Public Key Infrastructure

PKIX
Public Key Infrastructure X509

POS
Point of Sale

PP
Protection Profile

PTD
Personal Trusted Device

RF
Radio Frequency

RFC
Request For Comments

RIPEMD
RACE Integrity Primitives Evaluation Message Digest

RTD
Research and Technological Development

S/MIME
Secure MIME

SCD
Secure Cryptographic Device

SEPA
Single Euro Payment Area

SET
Secure Electronic Transaction

SGML
Standardised Generalised Markup Language

SHA
Secure Hashing Algorithm

S-HTTP
Secure HyperText Transfer Protocol

SIM
Subscriber Identification Module

SIT
Système Interbancaire Télécompensation

SME
Small and Medium Enterprises

SMTP
Simple Mail Transfer Protocol

SSL
Secure Socket Layer

STLP
Secure Transport Layer Protocol

SWIM
A SIM card with WIM application

TC
Technical Committee

TCP
Transport Control Protocol

TELNET
Terminal Access over Network

TLS
Transport Layer Security

TPDU
Transmission Protocol Data Unit

TR
Technical Report

TRSM
Tamper-Resistant Security Module

TSC
Technical Steering Committee

UCAF/SPA
Universal Cardholder Authentication Field/ Secure Payment Application

UCP
Universal Communication Platform

UMTS
Universal Mobile Telecommunications System

URL
Uniform Resource Locator

UUID
Universally Unique Identifier

VRU
Voice Recognition Unit

VNO
Virtual Network Owner

WPKI
Wireless PKI, PKI optimised for WAP

WTLS
Wireless Transport Layer Security, the WAP equivalent of TLS

XML
Extensible Mark-up Language

5 INDEX

--3--

--A--

--B--

--C--

--J--

--K--

--L--

--M--

--N--

--O--

--P--