OSeC Open Standards for Security and Certification
A EUROPEAN INITIATIVE
FOR CARD PAYMENTS IN EUROPE

Evaluation and Certification Framework

Implementation Document

Draft Version 0.6

30 August, 2010

Notice

This Document has been prepared by the Participants of the OSeC Steering Committee. Permission is hereby granted to use the document solely for the purpose of implementing the Contents of the Document subject to the following conditions: (i) that none of the participants of the OSeC Steering Committee nor any contributor to the contents of the Document shall have any responsibility or liability whatsoever to any other party from the use or publication of the Document, (ii) that one cannot rely on the accuracy or finality of the Document; and (iii) that the willingness of the participants of the OSeC Steering Committee to provide the Document does not in any way convey or imply any responsibility for any product or service developed in accordance with the Document and the participants of the OSeC Steering Committee as well as the contributors to the Document specifically disclaim any such responsibility to any party.

Implementation of certain elements of this Document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of the OSeC Steering Committee and any other contributors to the Document are not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. **This Document is provided "AS IS", "WHERE IS" and "WITH ALL FAULTS", and no participant in the OSeC Steering Committee makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights (whether or not the Participants of the OSeC Steering Committee have been advised, have reason to know, or are otherwise in fact aware of any information), and fitness for a particular purpose (including any errors and omissions in the Document).**

To the extent permitted by applicable law, neither the Participants of the OSeC Steering Committee nor any contributor to the Document shall be liable to any user of the Document for any damages (other than direct actual out-of-pocket damages) under any theory of law, including, without limitation, any special, consequential, incidental, or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, nor any damages arising out of third party claims (including claims of intellectual property infringement) arising out of the use of or inability to use the Document, even if advised of the possibility of such damages.

The Document, including technical data, may be subject to export or import regulations in different countries. Any user of the Document agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import the Document.

Table of Contents

1 Introduction

1.1 Definitions

Certification / Certification Body / Certificate

Certification means a process that aims at ascertaining that a payment scheme component complies with the set of functional or security requirements mandated by the payment scheme. A certificate, which is the written result of the certification in form of a document, is issued by a Certification Body. Certificates can be granted for security and/or functional compliance.

Approval / Approval Body / Approval Letter

Approval means that a payment scheme is prepared to accept operation of a payment scheme component, which itself has achieved certification issued by a eligible certification body, within its scheme. The approval letter is issued by the responsible body of that payment scheme, the Approval Body. For approval payment schemes may also take other considerations beyond security and interoperability compliance into account, e.g. for own risk management policies, own regional requirements or configurations.

JTEMS

„JTEMS“ stands for „JIL Terminal Evaluation Methodology Subgroup. The Subgroup was initiated by the CAS Initiative. It is comprised of Approval Bodies coming from CAS, CC Certification Bodies, CC Laboratories and vendors. The main task of JTEMS is to transform the high level security requirements defined by CAS and published in version 4.5 of the EPC Volume/Book of Requirements [BoR] into a CC Protection Profile. As a CC expert group JTEMS thus defines the implementation specification of the CAS/EPC security requirements and will support the CC related technical issues of the pilot.

CAS

“CAS” stands for “Common Approval Scheme”. This Working Group is comprised of Approval Bodies of the European and Global Card Schemes and acts since 2004 as an industry initiative to harmonize security requirements of smartcards and POI. The security requirements of smartcards were finalized in October, 2008, in a document called “Guidance how to write a Security Target for a smartcard embedded payment application”; the security requirements for POI were finalized in January, 2010, and are published in the EPC Volume/Book of Requirements version 4.5. CAS established JTEMS in order to provide for an CC ISO 15 408 implementation specification of the POI security requirements and established the OSeC Steering Committee in order to provide for an adequate and efficient implementation of the JTEMS implementation specification.

The ECB and representatives of the Eurosystems participate in CAS as observers.

1.2 Target

This document designs an implementation of the overall business and security requirements described in the master documentation of the Eurosystem and EPC listed in chapter 1.2 initially for POS terminals. The certification of cards is currently out of scope of this concept as well as the functional evaluation aspects.
In order to coordinate the implementation the "Open Security and Certification Standards Steering Committee OSeC" was established. The OSeC Steering Committee is comprised of representatives of Approval Bodies, which is a known and accepted function within a SEPA compliant card scheme, or within a recognised card payment market within SEPA, that grants approval for the deployments of products and/or services within its scheme or market.

The OSeC Steering Committee members signed the Memorandum of Understanding (see annex 1).

The **final objective** of the implementation concept described in this document is to provide an evaluation and certification framework that will ensure that the security features of a POI needs be evaluated and certified only once in order to secure approval from any Approval Body that agrees to operate within the framework. This concept therefore aims at multiple acceptance of terminal security certifications performed by the Approval Bodies of the participating card schemes or banking organisations.

No further centralized functionality is foreseen. This implementation framework leverages the existing certification infrastructure of the current Approval Bodies and enhances it by implementing innovative evaluation and certification processes of ISO 15 408 Common Criteria CC.

The final objective described above will be accomplished by a convergence approach: To gain trust in the new methodology the participating Approval Bodies will start the process by gaining all possible insights of the evaluations itself. This can be achieved by producing two separate evaluation reports, one CC report, and one proprietary report out of one evaluation. In a second phase insights of the evaluation report, which offers a structured and risk oriented summary of the evaluation results, will be sufficient until in the final phase the pure certificate issued by the Certification Body will be the only source for approval. The certificate must provide assurance and information to the Approval Body for purpose of Risk Management.

The final objective includes, that the CC evaluation results are utilized by PCI SSC and are not in conflict with PCI SSC.

The target situation is described as follows:

From a vendor's point of view:

A vendor gets all the relevant information from the OSeC web site. This information consists of all technical and procedural documents and details regarding the specification to be implemented; plus the process of how to achieve a certificate including the list of all accredited certification bodies/test labs.

The vendor selects a Certification Body and a test lab and gets into contact with both instances. The resulting certificates can be used to get an approval of all participating Approval Bodies.

From a banks and or payment schemes point of view:

The banks define the generic principles for security and certification at the EPC level (see [SCF] and [BoR] described in chapter 1.2). Due to the Eurosystem's Oversight Framework (see [OF] described in chapter 1.2) the Card Payment Schemes are responsible for providing an adequate certification infrastructure, through establishing and running the OSeC Steering Committee. Here Approval Bodies define and implement the operational rules and detailed requirements for certification bodies and test laboratories, named Evaluation and Certification Framework in this document.

The EPC is invited to monitor the progress; the Eurosystem is invited to observe the process.

The organizational rules for the certification infrastructure are maintained by the OSeC. These rules and requirements are reviewed and updated periodically in a structured and transparent process, which is achieved by multiple consultancy processes with all involved stakeholders.

From a retailers point of view

The retailer decides – according to his business needs – which payment cards he wishes to accept. This business decision defines the approved POS terminal he is able to use. The vendor sells the terminal supporting the business need of the retailer.

1.3 Relationship to the EPC/Eurosystem Documentation

This Evaluation and Certification Implementation Framework is based on the

- SEPA Cards Framework, version 2.1 [SCF],
- the current version of the EPC Volume / Book of Requirements [BoR] and
- Oversight Framework For Card Payment Schemes – Standards, January, 2008 [OF].

[SCF] defines as a banking resolution the high level principles and rules for SEPA card payments, which are to be achieved in a self regulation process. This process must be

market driven and eligible for a strong competition between payment schemes. One of the commitments describing the "Principles for Interoperability" relates to "Standardisation Activities", where "Certification Principles" [SCF, chapter 3.6.3.2], "Terminal certification" [SCF chapter 3.6.3.3] and "Scheme Rules" [SCF chapter 3.6.3.4] are defined as follows:

"A common process for certification of terminals, cards, and network interfaces will be defined …. Card schemes commit to support and implement the resulting process. Under this process, any card, terminal, and/or network interface, certified by an accredited body can be deployed and used anywhere throughout SEPA…..Card schemes commit to make available to SEPA banks, payment institutions and card schemes, upon request, their terminal security requirements. Card Schemes will engage in mutual recognition for type approval. Any terminal certified for SEPA transactions by a Certification Body in one SEPA country can be deployed in any SEPA country for acceptance of SEPA cards across all SCF compliant schemes. …Card schemes commit to investigate, and whenever possible deliver, areas of convergence as regards their respective rules – where there are non-competitive elements. …"

[BoR] specifies this vision, by

- outlining a harmonized list of generic security requirements for cards and POS terminals [chapter 5], which can be used by the card schemes depending on their business options and risk strategies [see BoR chapter 2.2.3.1] and
- defining generic business and functional requirements including a role model for the SEPA certification framework [chapter 6].

[OF] finally establishes a minimum set of oversight standards for card schemes, where standard 3 covers the adequate degree of security, operational reliability and business continuity regarding e.g. card based transactions. Standard 3 requires a design and manufacture of card payment components, which rely on uniformly adequate, up-to-date security standards and are regulated by an approval procedure, based on rules defined by the card scheme's governance authority.

The Evaluation and Certification Framework described in this document presents a solution to implement these visions and generic requirements because:

- The coordination of the implementation is given to the Approval Bodies, the dedicated part of the card schemes' governance authority, which is responsible for certification and approval.
- The process leverages on the existing certification infrastructures.
- The open and transparent requirements of [BoR] are – as a starting point - transformed into three different set-ups enabling competitive risk management strategies of the card schemes.

- The selected CC methodology promises the best achievable results for the level of security, transparency, comparability and tracebility.
- The common selection of a methodology and of certification procedures pave the way to multiple acceptance of certifications and of approvals in the end.
- The commitment of Approval Bodies fixed in a Memorandum of Understanding on
    - a willingness to recognise and support a single evaluation and/or certification process in order to obtain multiple approvals from Members based upon evidence provided by the JTEMS Common Criteria approach
    - a willingness to bring to and share with other members and to use the evidence that was used in granting approval in order to facilitate multiple approvals by all members of the Steering Committee.
    - a willingness to work with vendors, evaluation labs, and certification bodies to allow information generated in single approvals to be used by the Steering Committee to facilitate multiple approvals. Information about evaluations discussed during the Steering Committee sessions shall be considered confidential

  creates a reliable environment for all stakeholders.
- The OSeC Steering Committee acts as a Level Playing Field and addresses the International Card Schemes as well as the European Card Schemes being represented by their Approval Bodies. Approval Bodies may delegate the participation in the Steering Committee to their Certification Bodies, if they cannot provide for the relevant expertise by themselves due to internal procedures.

1.4 Approach Taken

In order to fully implement an effective Evaluation and Certification Framework it is necessary to undertake a two phase approach to the project.

Phase 1 conducts a pilot to prove that the objectives can be achieved.

Phase 2 reviews and implements the lessons learnt during phase 1. It refines the overall certification framework process and its governance, and rolls out the process.

Both phases will be used to identify the key actors within the framework and to define the relationships between them.

1.5 Organisation and Management Structure

Participation in the **OSeC Steering Committee** is open only to representatives of **Approval Bodies**, which have signed the OSeC Memorandum of Understanding (see annex 1). Up to now the MoU is signed by Cartes Bancaires, Consorzio Bancomat, Currence, MasterCard International, The UK Card Association, Visa Europe and ZKA.

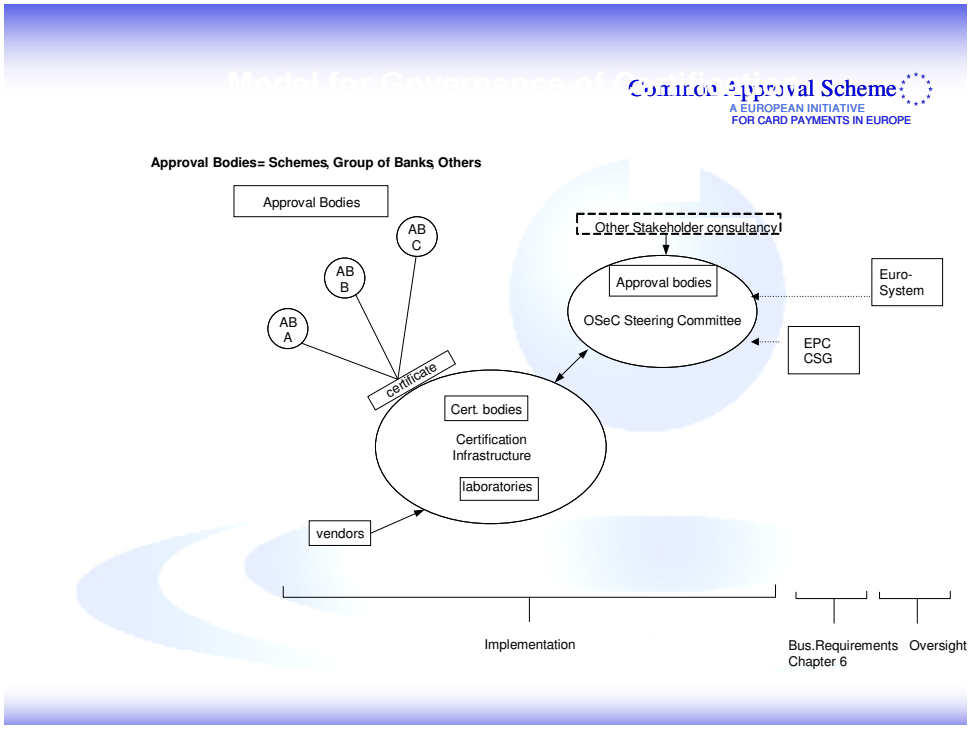
An Approval Body is a function within a SEPA compliant card scheme, or within a recognised card payment market within SEPA, that grants approval for the deployments of products and/or services within its scheme or market. These partners will be in charge of carrying out the pilot related to the definition of the Evaluation and Certification Framework. According to [OF], where Approval Bodies are called Approval Authorities, Approval Bodies have the responsibility to provide for adequate assurance measures to achieve the necessary high quality of security in a payment scheme.
The work of the OSeC Steering Committee is coordinated by the Steering Committee Co-ordinator, which is elected by the Steering Committee. The Co-ordinator is responsible for the overall management of the Pilot, chairing the Steering Committee, preparation of the meetings and decisions of the Steering Committee.

The **EPC** will be invited to be involved to monitor and observe in order to ensure that the requirements defined in [BoR] are met. The EPC will particularly be asked for the frequency of reporting.

The **Eurosystem** will be invited to be involved to monitor and observe in order to ensure the delivery of the objective.

The organisation of the OSeC Steering Committee and its relationship to the respective stakeholders can be described detailed below, all members of the OSeC shall have equal standing within the committee and all decisions will be made by consensus

The organisation of the OSeC Steering Committee and its relationship to the respective stakeholders can be described as follows:



2 First Phase: The Pilot

The pilot's objective as outlined in chapter 1.1 will be achieved, if a vendor obtains approvals based on the evaluation and certification achieved within the pilot process by several Approval Bodies, which participate in this framework.

Key aspects which need to be addressed by the pilot include:

- organisation and management structure,
- scope,
- duration,
- publication and stakeholder involvement,
- costs,
- ownership of the results and intellectual property rights,

definition of success criteria to initiate phase 2.

2.1 Scope

The scope of the pilot covers the following packages:

2.1.1 Coordinate the activities needed to deliver a successful Pilot

Monitor the JTEMS PP Evaluation and Certification

The JTEMS document ”POI Protection Profile” will be used as the implementation specification [see JTEMS PP]. The specification contains three CC Protection Profiles PP, which were identified according to specific market needs:

- The PED-Only Configuration, covering the PCI POS PED v2
- The POI-Comprehensive Configuration, covering the whole set of requirements and
- The POI-Option Configuration covering the whole set of requirements without the protection of offline plaintext PIN and the magnetic stripe reader.

All three PPs base on the set of generic POI security requirements of [BoR, chapter 5]. [JTEMS PP] were given to ANSSI, the French CC Certification Body, which volunteered to coordinate the certification of the three JTEMS PPs. According to the CC standard process, this certification is a prerequisite for the pilot and it is envisaged, that the certification process will be finalized in 3rd quarter of 2010. The certification is being done by Thales CNES.

The preferred configuration of the JTEMS PP used for the pilot should be the “Comprehensive” configuration as this includes all security requirements and therefore provides full coverage of all work undertaken. Using either of the other two configurations would result in some requirements not being assessed, and would therefore lead to certain parts of the process not being evaluated as part of the pilot. This could lead to problems when the process is rolled out in Phase 2.

The technical aspects of the certification process is supported by PP Certification Task Force comprised of Trusted Labs, SRC and SIVenture, who are the authors of [JTEMS PP] in coordination with JTEMS. Issues coming out of this work regarding the security requirements are reported by the Task Force to the OSeC Steering Committee for decision. In order not to delay the PP certification process, a Subgroup comprised of Cartes Bancaires, ZKA, Currence and Visa Europe will deal with the questions and agree on solutions via conference calls.

Coordinate the additional documentation for the pilot evaluation

JTEMS is working on the following supporting documents, which are – due to the CC standard processes – necessary for a transparent and confident CC evaluation:

- Attack Method Document
- Guidance for the application of the PP for vendors and laboratories, which enforces the properties of the methodology in the guideline document (transparency, independency, repeatability, etc.)
- Common Criteria Evaluation Methodology CEM Refinement.

The Attack Method Document must be available for the pilot evaluation. JTEMS will deliver it before the pilot evaluation starts.
The appropriate time to specify and develop the Guidance document and the CEM Refinements for JTEMS is during the pilot phase. The participants and especially the laboratories, which are responsible for the CEM Refinements, need the experiences made during the pilot to specify these documents. Thus both documents will be results of the pilot and will therefore be delivered when the pilot ends.

Inform and guide the criteria by which Laboratories can be accredited by JIL to do POI evaluations

The accreditation criteria for CC accredited laboratories are defined by the CC Certification Bodies. Experience in the evaluation of smartcards has shown, however, that there is the need to define additional stringent criteria for those laboratories evaluating hardware platforms. In the case of POI evaluations this same process will be followed with the Certification Bodies of JIL and the OSeC Steering Committee. They will work together to enhance the existing accreditation criteria for CC laboratories to cover the new CC technical evaluation and certification area “POS terminals”.

Promulgate information on candidate laboratories and participating CBs

The European usage of the CC for POS terminal evaluation and certification is new for all participants including the laboratories and certification bodies. To enter into the pilot process they need all the necessary information and motivation coming from the standardization processes of CAS, JIL, JTEMS or other initiatives, the payment schemes and the regulators.

The pilot is open for all laboratories, which obtain the new CC accreditation for POI, and for all volunteering CC Certification Bodies.

The information platform will be the OSeC web site, which will be posted by the OSeC Steering Committee.

If a vendor wishes to secure PCI approval for global card scheme requirements then it will be necessary to select a lab that is a PCI recognised laboratory.

Raise familiarity of the type of evaluation reports with the participant Approval Bodies they will be approving

Approval Bodies have little or no contact with CC Certification Bodies and currently rely upon their proprietary evaluation and certification infrastructure. In future, the CC evaluation reports will be the main dependency between the Approval Bodies and the CC Scheme and will present the main source of information, and of trust, upon which the approval is based upon. There is therefore a need to define additional measures in order to build this trust in the pilot and to provide the foundation for the future.

ETR for Risk Management

The current CC evaluation reports must be analysed and depending on the outcome of the analysis they may need to be enhanced or optimized in order to facilitate approval. An objective of the pilot is, therefore, to define the contents of a standardized Evaluation Technical Report ETR for risk management that will benefit all approval bodies. A first draft has been prepared by CAS, which will be updated in August/September, 2010. The main contents will be based on the CC concept of identifying "residual vulnerabilities", these are the key issues that must be assessed by the Approval Bodies. Further information given covers a description of the TOE related to POI

- high level description of internal workings TOE,
- overview of hardware and logical countermeasures,
- vulnerabilities related to different kind of attacks (penetration, manipulation, substitution etc),
- strengths,
- need to know items (new features, new attack potentials, attack potentials with relative less points for exploitation, etc).

Confidence Building Measures

One of the main targets of the pilot is to build trust in the CC approach and methodology with the participating Approval Bodies. The Approval Bodies of the OSeC Steering Committee will decide, along with vendors , laboratories, JIL and CBs, how to facilitate this trust building process. The candidate options to support this are:

1. to be provided with insight to all CC evaluation results,
2. to perform comprehensive and open inquiries with the laboratories over the pilot's time and especially regarding the whole contents of the full CC evaluation technical report.
3. to map the results of the CC evaluation with the current scheme specific evaluation report,

The CC ETR for risk management will be the basis for approval bodies to make their approval decisions during the pilot. Wherever possible they will use option 2 to build understanding and facilitate approval. It is not possible to discount that in rare cases it may be necessary to adopt option 3.

If vendors wish to secure PCI approval there is need for the vendors to submit a PCI report to PCI SSC.

The OSeC Steering Committee will coordinate and support these processes.

Coordinate the milestone phases of the deliverables of the evaluation of any product with Approval Bodies

The pilot will cover the usage of a new PP and the establishment of this new PP at vendors, laboratories, Certification and Approval Bodies. Therefore the evaluation needs to be structured in different milestone phases in order to oversee the whole evaluation process and optimize and steer the process. As a result a work plan with defined work packages is expected form the vendors and their pilot teams.

The OSeC Steering Committee members are obliged to respect the 1 January, 2011, as the SEPA target date defined in the SCF. Due to this date the following milestones are defined as a guidance for the vendor's project plan.

Milestone	**Date**
Vendor's written statement of interest. This statement is necessary to attend the Pilot Kick Off meeting, 14 October, 2010.	Until 15/09/2010
Kick Off Meeting; start of the pilot Vendors attending this meeting because of their statement of interest must announce officially, that they will participate in the pilot	14/10/2010, Madrid
Vendors to send in the filled in application form (see annex 2 of this document)	Until 1 January, 2011 at the latest..
End of the pilot; including certifications. Within the 2 year's pilot period, the pilot evaluations are expected to take no longer than 8 months. [1)] The precise schedule is decided by the vendor and his pilot team.	14/10/2012

(1) It is expected, that vendors, which are experienced in CC evaluations can pass the evaluation in a shorter timeframe, e.g. within three months.

This activity shall not include the security evaluation as such, which must be left to the expertise of the laboratories and certification bodies. It is not in scope of the pilot to investigate the comparability of evaluation results by e.g. a parallel evaluation of the same product by two different laboratories.

2.1.2 Establish and Coordinate the Pilot

Promote the pilot through the identification of candidate vendors

A successful pilot can only be achieved by the support and participation of a terminal vendor. Participation in the pilot is open for all POS terminal vendors willing to be actively engaged in the necessary activities.

Vendors wishing to participate in the pilot must fill in the OSeC application form (see annex 2 of this document). The application form describes the vendor's project and collects information, which may impact the pilot's performance or indicate to OSeC, which support will be necessary to achieve the pilot's success criteria. The vendor is responsible for its content and quality.

The contents of the Application Form will be reviewed by the OSeC Steering Committee and feedback will be given to the vendor before the vendor team starts its activities. The contents of the application form must be presented by the vendor to the OSeC Steering Committee until 1 January, 2011 at the latest.

Support Pilot Evaluations and Certifications

JTEMS will assist the laboratories and vendors in providing appropriate clarifications and support during evaluations. JTEMS will assist the Certification Bodies and will give the clarifications needed.

Appropriate feedback must be provided about the evaluation to the OSeC.

Particular attention will be given to agreement with the Certification Bodies on their approach and responsiveness to deliver certification reports covering both the high quality of the proved security requirements and a performance covering the market needs.

2.2 Publication and Stakeholder Involvement

The results of the OSeC's work and the progress of the certification process will be published regularly on the OSeC web site.

The pilot shall involve all interested stakeholders and shall be conducted in a multi-scheme context. This demands a close cooperation of all parties involved. It is proposed to achieve this cooperation by the following process:

- The vendor stakeholders will be encouraged to support the pilot through engagement within JTEMS as the primary stakeholder group for the pilot.
- A special Pilot Task Force PTF or PTFs of actively engaged vendors and their selected laboratories and Certification Bodies will be established to coordinate the pilot activities in an efficient way and in order to drive the evaluation process. A representative of the OSeC Steering Committee will coordinate the PTF's work in order to make it a success. The coordinator informs the OSeC

Steering Committee about the progress made and escalates open issues to JTEMS.

- The OSeC Steering Committee has the right to establish other Task Forces to advise and support the Steering Committee in the proper management and co-ordination of the pilot.
- The OSeC Steering Committee will report to all stakeholders as required. The reporting includes the CSG, the retailers, the vendors, JIL, CAS and others. It is proposed to get into contact with these stakeholder groups in order to agree on the desired reporting type and cycle, e.g. a quarterly report. The same procedure is proposed to keep the European Commission informed. All stakeholders are encouraged to use the report sessions for input and feedback.

2.3 OSeC Memorandum of Understanding

The pilot shall come into force as of the date of the signatories of the MoU attached to this document and shall continue in full force and effect until terminated in accordance with Section 2.5 hereunder or until complete discharge of all obligations for carrying out of the pilot undertaken by the Parties participating in this framework.

The MoU is fixed to 24 months (see annex), which can be expanded.

2.4 Define Success Criteria for the Pilot

The success criteria for the pilot are defined in order to achieve a clear entrance into phase 2.

- Successful completion of the evaluation resulting in the certification and approval of the terminal.
- Recognition of the evaluation results by the OSeC membership, including PCI SSC, taking into consideration the approval strategies of the applying vendors.
- Availability of a well defined and well understood concept to implement a standard certification process. This concept includes:
    - A concept how transparent processes and repeatable evaluation results are achieved
    - A concept how overall cost efficiency is achieved, e.g.
        - The achievement, that the costs of an evaluation are not prohibitive and do not outweigh the alternative of multiple evaluations for the various schemes,

- The achievement, that the costs of an evaluation borne by the vendor must be commensurate with giving the necessary assurance that the security requirements have been met.

- The claimed JTEMS PPs can be released for further usage..
- Participating of at least one pilot project team.
- Availability of an ETR for Risk Management, that can be used in phase 2.

2.5 Costs

Each party shall bear its own costs incurred in connection with the performance of the Pilot. This includes the laboratories, the certification bodies and the vendors.

2.6 Ownership of the results and intellectual property rights

The IPR of all documentation, which is produced within the OSeC pilot process relies to the Members of the OSeC Steering Committee. The vendor owns all results of the evaluation. In order to support the trust building process of the OSeC membership and to achieve the acceptance of the evaluation results, the vendors assure full access to the OSeC membership.

2.7 Preparation of Phase 2

Throughout the pilot phase the whole process will be documented and stored in order to collect the experiences made for further assessment. Important information to be documented are e.g.

- Problems, which occur,
- Solutions, which were found.

This pilot documentation will be used as input for the most valid model for the second phase.

The documentation will be maintained by the PTF and the OSeC Chairperson.

3 Second Phase: Establish the Enduring Framework

3.1 Target

The second phase is designed to optimize all lessons on governance and operation generated during the pilot in order to transition to an enduring but responsive framework with a formalised governance and organisational structure. The second

phase will probably commence during the pilot phase in order to contribute to transitioning to then arrangements as soon after the end of the Pilot as possible.

It is understood that a new MoU will be required for the second phase, and the work on the MoU will also begin during the pilot.

3.2 A Preview: Optimized Lessons

As seen today lessons to be learnt must influence and solve the following issues, in no particular order, plus any others that emerge during the pilot phase:

- Governance issues, stakeholder consultation modalities.
- Relationships needed to sustain the framework and the processes and frequency of meetings to do so: JIL, EPC, Eurosystem, CAS, vendor bodies etc
- Organization: budget, secretariat, meetings.
- Coordination with the body maintaining the Security Requirements:
  - Bilateral dialogue on current and future requirements
  - Processes to share information on new threats vulnerabilities, and identifying with whom.
- Endorsement of new security requirements and the commissioning the development of additional PPs
- Maintenance of the list of participating Certification Bodies and approved technically capable laboratories for POI evaluations
- Facilitate resolution of any conflicts arising between vendors/labs/certification bodies
- Repository of information about SEPA security certification (documents, certified products...)
- Work with the global schemes for use of evaluations results
- Future maintenance of the framework and maintaining alignment between CAS and PCI requirements and the EPC [BoR]
- Future application of the framework and approach beyond POI issues to embrace cards and functional issues
- Production of a document, which describes the high level mechanisms for evaluation and certification for the enduring framework.

Annex 1 of the OSeC Evaluation and Certification Framework – Implementation Document, Draft Version 0.6, 30 August, 2010.

Open Security Standards for Evaluation and Certification (OSeC)

Steering Committee

Memorandum of Understanding (MoU)

The signatories to this MoU agree to set up the OSeC Steering Committee ("the Steering Committee"), whose members ("the Members") will be representatives of Approval Bodies ("Approval Body"). An Approval Body is a function within a SEPA compliant card scheme, or within a recognised card payment market within SEPA, that grants approval for the deployments of products and/or services within its scheme or market. A Member will be both deeply involved at a technical level in SEPA standardisation initiatives and committed to the technical implementation of the objectives of the Steering Committee.

The first objective of the Steering Committee is to coordinate and monitor a field pilot and any subsequent pilot which will achieve multiple approvals from a single evaluation and/or certification.

The second objective is to guide the establishment and implementation of a permanent structure to steer a certification framework infrastructure incorporating the lessons learnt from the first objective.

The Steering Committee is open to any Approval Body based on their readiness to contribute and to commit resources, in terms of time and effort, from their organisation to the objectives of the Steering Committee.

The commitment of a member of the Steering Committee is threefold:

1. A willingness to recognise and support a single evaluation and/or certification process in order to obtain multiple approvals from Members based upon evidence provided by the JTEMS Common Criteria approach

2. A willingness to bring to and share with other members and to use the evidence that was used in granting approval in order to facilitate multiple approvals by all members of the Steering Committee.

3. A willingness to work with vendors, evaluation labs, and certification bodies to allow information generated in single approvals to be used by the Steering Committee to facilitate multiple approvals. Information about evaluations discussed during the Steering Committee sessions shall be considered confidential.

The duration of this understanding shall be 24 months from the date that the first two or more members become signatories to this MoU.

The Steering Committee recognises that transparency, good governance arrangements and stakeholder involvement are crucial elements in establishing acceptance, trust and legitimacy of the common evaluation and certification process. Throughout this period the Steering Committee will therefore consult with both Regulators and other interested parties, including the wider stakeholder community, in a timely fashion in order to achieve the objectives set out in this MoU.

The initial activities that the Steering Committee will undertake are set out in Annex A; these will be subject to change through the life of the understanding in order to meet the overall objectives.

SIGNATURES

Approval Body A

_____

Name

Title

_____

Date

_____

Approval Body B

_____

Name

Title

_____

Date

_____

Approval Body Z

_____

Name

Title

_____

Date

_____

Annex A to the MoU

INITIAL ACTIVITIES OF THE STEERING COMMITTEE

Define the Principles and Success Criteria of a Pilot

The overall target of a field pilot coordinated and monitored by the Steering Committee is to prove that multiple approvals from a single evaluation and/or certification procedure can be achieved. Although this could be deemed to have been achieved if two schemes approve a product from one evaluation and/or certification procedure, it will be important to broaden the success criteria in order to capture the lessons learnt in order to develop the case for the establishing the long-term future of the certification framework beyond the life of the MoU.

The Technical Evaluation against the JTEMS Protection Profile

The Common Criteria methodology is well established in the field of smartcards. In the field of POI first experiences have been made in the United Kingdom, where The UK Cards Association has for several years required CC evaluations for its PEDs for its own PP. The JTEMS PP (containing three set-ups) represents an innovation regarding the target of evaluation, which is the whole POI, and includes some new PP concepts developed by JTEMS, e.g. the EAL POI. These innovations must be proven, in the sense that they technically work in practice, and can be evaluated against.

Cost Efficiency of the Evaluation against the JTEMS Protection Profile

Security evaluation and certification is a requirement for vendors to have access to a scheme or market. It is, however, vital from the vendors perspective that the cost of an evaluation [and its subsequent certification], which will provide the evidence to secure multiple approval, is not prohibitive and does not outweigh the alternatives of multiple evaluations for the various schemes or markets they would have chosen to target. Moreover from the Approval Bodies perspective the costs of any evaluation borne by the vendor must be commensurate with giving the necessary assurance that security requirements have been met. Therefore the overall cost efficiency of the evaluations conducted during the pilot will be closely monitored during the pilot in order to adjust the guidance to evaluators as necessary.

Engagement with the CC Certification Bodies

This approach requires the full support and participation from Certification Bodies, as they will be required to certify the results of any evaluation conducted by any laboratory that they supervise. The new CC POI approach must be acceptable by the Certification Bodies. Due to this the Steering Committee will maintain a close liaison with the Certification Bodies in order to handle the new concepts found by JTEMS to assure the necessary high level of security and to establish an optimized performance. The Steering Committee will in addition establish the

necessary communication channels between the Certification Bodies and the Approval Bodies.

Approval by Approval Bodies

Evaluation and certification are conditions in order to request an approval for a product for market deployment. Therefore the activities are focussed on the coordination of CC Approvals for certified POI by the Approval Bodies. This coordination of Approvals will take into consideration the re-use of current types of certificates in order to leverage as much as possible on these evaluations and/or certifications and to pave the way for proper migration. I.e. Approval Bodies will consider composite evaluation/certification in their approval process for POI. The Steering Committee will facilitate the approval process working with Members to achieve their own approvals and the work needed to secure multiple approvals across several approval bodies.

Ensuring and promoting Vendor Engagement in a Pilot

For the objectives to be achieved it is essential that vendors come forward with products that they wish to be evaluated and for which they wish to secure multiple approvals. The Steering Committee will develop, through Member engagement with vendors, the overall market landscape of potential products and vendors. The Steering Committee and Members individually will lobby vendors and promote the value and importance of participation within a pilot.

Governance arrangements

Whereas the Steering Committee's Members are Approval Bodies, work will start to guide the establishment and implementation of a permanent structure to steer a certification framework infrastructure in which more stakeholders could be represented. From the outset, the meetings of the Steering Committee will be open for an observer from the EUROSYSTEM/Eurosystem, as well as from the European Payments Council as decision-making body of the European payments industry.

Stakeholder involvement

The Steering Committee will consult with both regulators and other interested parties, including the wider stakeholder community. For this purpose, it foresees firstly to open a dialogue with the EPC and its Cards Stakeholders Group. Secondly, the possibility will be assessed to a) establish a Steering Committee website, b) establish 'Stakeholder Councils' for other stakeholders and c) organise public consultations on prospective Steering Committee implementation standards and/or rules. The Steering Committee will share on a quarterly basis technical results with the stakeholders.