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.