# PCI SSC:
# PCI Data Security Standard (DSS), Version 1.2

## EPSM Feedback:
Date: 30th October 2009

We appreciate the opportunity for an open feedback want in addition to our comments at the meeting with European associations last Wednesday in Prague to comment as follows:

### 1. *General Comments*

Achieving maximised data security for card payments is important and the work of the PCI SSC is very valuable to achieve this goal.

For service providers and card-not-present merchants (e-commerce, Moto) the requirements are generally appropriate, but for most POS merchants the PCI DSS requirements are too burdensome and too costly.

Therefore the stated goal of PCI SSC should be to minimize the impact of the security requirements to POS merchants, e.g. by strong emphasise on end-to-end encryption, tokenization and/ or "capsuled POS terminals".

**Its should become possible, that by using a PCI DSS compliant service provider using these technologies, a merchant becomes practically "out of scope" for PCI DSS, that means, a POS merchant will have no access to card data.**

### *2.* ***Specific Comments***

For detailed technical comments and unclarities, we want mainly to refer to the inputs of other participating organizations and QSAs.

- In general:
  It would be good to have to each requirement further descriptions and notes in an easily readable form.

  This "PCI DSS explanatory notes" can be a separate document, which can include recent Q&As to specific requirements. This document should be updated monthly or quarterly according to recent market information.

- Page 5:
  It should be clearly stated that truncated PANs are no cardholder data according to the table on page 5.

- Page 9:
  As much confidential information is e.g. in a network diagram, it should be clearly and transparently stated who will have access to the report content. Also strict and transparent NDA rules should apply for entities that have access to any confidential information.

- Page 18
  In order to avoid "social engineering" a new requirement should be implemented, that passwords for access in PCI DSS secured environments should be used only in these environments, and must especially not taken for private use. (e.g. do not use your Facebook-password for access to a PCI DSS secured environment).

- Page 19:
  The work of the virtualization SIG should be considered in a new version or in some explanatory notes.

- The requirements 12.1.1 and 12.2. are very generic. They could be cancelled (or specified more).

- Are the payment schemes Service Providers? Does 12.8.2 include the payment scheme networks?
  (This becomes important, if under the SEPA project, payment networks can process also transactions from other schemes, e.g. a Visa transaction routed or cleared by the MasterCard network).

- It should be clarified that e.g. tax authorities and legal enforcement authorities do not have to comply with PCI DSS requirements when they perform their legal duties.

- The public information, if an entity is PCI DSS compliant should be on the PCI DSS website (like with PCI PED) and not on the website of a payment scheme.

- For a better promotion of PCI standards, it should become possible to set direct links from a participating organization's webpage to all PCI DSS documents. The lawyers should find ways to avoid the "licence agreement" which currently inhibits this practice.

3. **Approach to get merchants "out of scope"**

**As described before, it should become possible for POS merchants, to outsource all management of card holder data to PCI DSS compliant providers. This can be achieved by a combination of minimized "end-to-end encryption" (at least encryption from terminal to PCI DSS compliant terminals", tokenization (for print-outs) and tamper resistant, capsuled terminals.**

**It is clear that in this case the key management and other access to the terminals may only performed by the PCI DSS compliant service provider.**

**In such a case, the merchant SAQ should be strongly simplified.**

**As a conclusion, it should be possible that the brief SAQ 1 should be available also to POS merchants.**

4. **Further issues**

We want to highlight, that especially in clearing, settlement and fraud communication to the payment schemes, the payment scheme networks frequently require non encrypted cardholder data, especially PANs. PCI DSS should clarify indicate that these scheme requirements do not violate the PCI DSS compliance.

= =