Note

P10726 FEB166736
Patrick Wynant
Final

ECB draft recommendations for the security of internet payments

Febelfin comments

Febelfin is the Belgian Financial Sector Federation representing 238 members. It tries to reconcile their interests with those of the policy makers, supervisors, trade associations and pressure groups at the national and European level.

Febelfin is grateful to the European Central Bank for the opportunity to comment on the draft "recommendations for the security of internet payments" in the framework of the consultation process. It sincerely hopes that the comments which Febelfin has the honour to provide will contribute to the European Central Bank's analysis and help it to identify the right way to improve the security of internet payments.

We support the comments from the European Payments Council (EPC). In a few cases, we wish to make the case stronger (particularly about prescribed technological solutions that may become obsolete, eg. 3-D Secure) and we provide additional or complimentary support to their comments.

General part comments

Retail (Consumer to Business e-commerce) internet payments predominantly involve card based payments (illustrated by the documents own focus on 3-D Secure). One of the largest international card payments security efforts underway in the industry (and directly applicable to many PSP's within Europe) are the **PCI Council's Payment Card Industry Data Security Standards**. As this document does not address "PCI like" directly, while apparently borrowing many specific terms from the PCI security documents, it appears an overview.

We suggest an explicit explanation and reference (in the Annex) or an effort to align or differentiate this document from the PCI requirements. Without alignment and clear delineation, a risk of duplication and/or conflicting security standards may occur which could lead to degraded security and compliance. PCI DSS is aligned with the ISO 27000 series and following such a framework is generic and provides a security baseline in a recognisable manner, unlike this recommendation.

The objective "*The ultimate aim is to foster the establishment of a harmonised EU/EEA-wide minimum level of security, as well as to facilitate a common understanding between the relevant authorities*." could be improved with a reference as to why this is important. Additional text such as: "***Enhancing***

***and increasing consumer use and trust in e-commerce transactions is identified as an economic priority for EU Member States and this document aims to address the core issues of consumer and brand protection while reducing fraud and the overall effectiveness of the criminal internet payments fraud underground*"** would improve the contextual understanding and intent of the document.

paragraph 5: suggestion to add : Rules on security measures just like PCI DSS :
Rules on security measures just like" PCI DSS" should be consistent with other regulated domains such as cybercrime, data protection, anti-money laundering, etc.

Comments on recommendations

Recommendation comments 4.2 KC : Please correct "PSPs should use firewalls, proxy servers or other similar security solutions that protect networks, websites, servers and communication links against attackers or abuses such as "man in the middle" and "man in the browser" attacks." Man-in-the-browser attacks cannot be prevented by the methods requested. Mobile banking via phones is on the rise but man-in-the-mobile attacks is not mentionned. This point is very prescriptive and precise in parts, yet misses other equally important points. Hardening doesn't only occur on servers for instance.

Recommendation 5 comments :

We suggest to ensure that requirements are in-line with the risk assessment conducted. The specific requirement to log all read actions to transaction data may be very impactful, particular on customer self-check, but return very little risk reduction benefits.
Does this only relate to customer access on the front end or also back end access by PSP staff?
We would expect to see non-repudiation under this recommendation.

Recommendation 6 comments If we agree with those recommendations, warnings on social engineering attacks should be included in 6.2. KC:

6.2 KC - For a customer who has multiple banks in a country (or different countries) this may result in different requirements by each bank to have different end-user controls on a customer's home PC. It may not be possible or reasonable for customers to align all potentially conflicting requirements from different PSP's active in markets in the EU. How the 'requirements' term would be monitored and enforced by a PSP would need clarification.

Recommendation 7 comments:
Proposal to drop the first sentence because it is too card specific:
Customers should only be allowed to enter their credentials and authentication codes by themselves in a secure environment as indicated and approved by the issuing PSP.
Proposal to replace issuing PSP by customer PSP : here it is impossible for the customer PSP to distinguish between the actual fraudulent and/or in the secure banking environment.

7.3 KC "All cards issued must be technically ready (registered) to be used with strong authentication

(e.g. for 3-D Secure, registered in the 3-D Secure Directory) and the customer must have given prior consent to participating in such services." implies many issues:

The "e.g. for 3-D Secure" reference is virtually requiring that all card transactions in all Member states of the EU must be incorporated into the 3D-Secure systems developed by Visa and adopted by other Card Schemes. This could imply a technology 'lock-in'. Are all competing Card Schemes allowed to use 3-D Secure?

- The 3-D Secure technology Security Controls "3-D Secure™ Security Requirements Enrolment and Access Control Servers Version 1.1 January 1, 2004" are not consistent with current industry trends or best practices and were last updated, effectively, in 2003. No updates to this standard are planned or communicated. The underlying assumptions and approaches predate many of the secure technologies and methods of operation expected today (security controls assumes/requires stand-alone dedicated servers with internal hard drives, no capability to handle virtualisation, SAN, etc.). Basing internet payment security on a 10 year old security framework is not appropriate. The control set is not aligned with the support of the PCI programs and this disconnection can only harm the further integration of card security in card-presence as well as card-not-present transactions.

Recommendation 11 comments:

11.3 KC Card schemes should (also) encourage e-merchants.

Recommendation 13 comments:

13.1 KC and 13.1 BP: Due to the existing legal framework, the consumer is already informed about the way of using the payment services offered by his PSP, including their spending limits. Furthermore, payment on internet is one of the channels to order a payment and not a payment instrument as such. In some situations, it even might be a multi-channel. Therefore, we recommend that these KC/BP are not necessary.

Recommendation 14 comments:

14.1 KC – Clarification as to intent of "*at any time*" is needed. Does this force no downtime requirements on PC Banking solutions? Or down-time windows only when branches are open? Is "*check transactions and account balances*" intended to be real-time, near real-time, daily? Additional clarification on this section is needed. Some issues are already covered by SEPA and so alignment is suggested.

14.2 KC - Apparently are using specific terms that are by implication related to PCI "*sensitive payment data should not be included in such statements or, if included, they should be masked.*" Specific 'masking' criteria (leading 6 and last four numbers) are called out in PCI. We suggest to include a direct reference and acknowledgement and use of PCI or re-create the full lists of definitions and applicability here. Cases have occurred where one system uses the central data elements and the other uses the end data elements and the conjunction of two sources leads to a data compromise.

Comments on annexes

- The glossary should be improved for many explicit terms that are undefined. Some definitions

can be found in other sources (e.g. PCI). However specific references and precise definitions are needed.

- As discussed above, explicit and detailed inclusion, explanation and promotion of 3-D Secure commercial and proprietary technology (in the special Annex section) is not appropriate in this ECB Recommendations documents.
- As with defining PSP by referring to PSD, we suggest to mention other and all official external sources used in this document.
- Annex 2 includes important references to the existing international compliance ecosystem (particularly built around cards). Including explicit references to international and industry evolving standards (e.g. PCI etc.) and driving towards adoption of commercial and proprietary un-evolving system (e.g. 3-D Secure) is not consistent with the direction of the industry and European Commission policies (e.g. increased competitiveness in the internet commerce and card markets).