EUROPEAN FORUM
ON THE SECURITY OF RETAIL PAYMENTS

ECB-PUBLIC

29 January 2014

COMMENTS ON THE DRAFT "RECOMMENDATIONS FOR THE SECURITY OF MOBILE PAYMENTS"

Contact details: **Mobey Forum**		**Sirpa Nordlund, Executive Director, Mobey Forum**
	Address **Aleksis Kiven Katu 3-5, VC210** **FIN-00020 NORDEA, FINLAND**	
	E-Mail:, Tel.; Sirpa.nordlund@mobeyforum.org, +358405683436	
☐	The comments provided should NOT be published	

The table below shall serve as a template collecting comments received in a standardised way.

- Please **add** to the table **only issues where you consider that a follow-up is necessary**, i.e. no general statements like "We welcome the recommendations."
- All comments should be **separated per issue** concerned so that a thematic sorting can be easily applied later on. (i.e. one row for each issue).
- If needed, replicate page 2 for the provision of further comments.

Originator:

Name of the originator (e.g. name of the company or association)	Mobey Forum (its European members)	ISO code of the country of the originator	FI

N°	Issue	Comment	Reasoning
1	General	The regulation of mobile payments is considered premature.	• Reliable experience in Mobile Payments is in practice not yet available to a sufficient extent. Thus, a basis for proportionality of regulatory measures does not yet exist. Maybe there is a need for regulation in the future. • This results in constraints long before the market can evolve, therefore, innovation is hindered. This is in contrary to the principle of the self-regulation of markets in a healthy environment. • As there are no mature solutions/products on the pan-European market today it is too early for a regulation of mobile payments.
2	General	Clarification , Bring the recommendations for mobile payments in line with the recommendations for the security of internet payments where applicable.	• The document reflects the increasing maturity of the forum's security recommendations. The wording and underlying aims have been developed further. • In this sense some phrases which should be identical with the recommendations for the security of internet payments differ. • This has immediate impact on established security processes. It could lead to unnecessary differences in the security processes for mobile payment and internet payments, as in general, the differentiation of internet payments and mobile payments is undesirable since there is a smooth transition between both. • To avoid misinterpretations a sufficient explanation is necessary.
3	General Comment Page 4.	Clarification.	• The document states that transactions that do not exceed EUR 50 and the cumulative value of payment transactions do not exceed EUR 200 in any billing month should be excluded.
4	General Comment Page 5; requirement for MSPS's to ensure, that	Clarification	• A two-factor solution comprises strong authentication, because while it may be easy to steal one factor, it is difficult to steal two matching factors. • It is not possible to prevent PIN compromise, if entered on a e.g. SmartPhone, which is what everyone wants. It is only possible on

	entry of PIN is not compromised, is too harsh		dedicated hardware (like a SSCD), which no one wants especially in connection with Smartphone usage – it is way too inconvenient. • Also it is not necessary – e.g. a key logger can be allowed to read the PIN, if the other factor is not easily obtainable through that channel. Protection is obviously preferable, but not necessary, and it is possible to make secure solutions without protecting against e.g. key loggers. • Later there's talk of "risk appetite" and "proportionate security measures", which are angles not seemingly reflected within the recommendations – that is stated to be implemented by 2017!?
5	General Comment Page 5: Requirement that software should be installed via a secure channel (and regularly checked against tampering) is too harsh	Clarification	• This statement seems aimed at locking distribution to AppStore or Google Play or similar. These channels are not given to be secure, nor is any other channel really. • It should be sufficient to state, that the customer should be able to assure herself within reason, that the correct software is running, and that communication between the client and the server should contain measures to ensure, that the correct software is running. It should not be stated how – there are many good and creative solutions and options out there, some probably not seen yet.
6	General Comment Page 5: Requirement of de-activation is too specific	Clarification	• Deactivation is a different thing than "uninstall" or "delete profile", etc. But these are equally effective against this goal, it seems, and it should be up to each party to decide which level of user handling and convenience is necessary and wanted.
7	General Comment Page 5: Clarify "secure processes for	Clarification	• Only 2½ line here for this area, which is really the hardest one... obtaining a valid signature on a transaction and deploy fraud detection on it. • There could be mentioning of "What you see is what you sign" interface requirements here – especially considering the depth gone to in the other areas. Perhaps this is due to an assumption that a SSCD is

	authorising transactions"		in place already, but it has to be assumed, that it is not and won't be ever in general.
8	General Comment Page 7	Clarification	• The mobile payment ecosystem can involve several stakeholders who plays a crucial role for enabling mobile payments but they are not under the same supervisory competence as PSPs, and may meet different requirement if any at all. It may lead to an "un-levelled playing field"
9	General Comment	Clarification	• It is very important to point that: "This document does not attempt to set specific security or technical solutions. Nor does it redefine, or suggest amendments to, existing industry technical standards. In this respect, the Forum welcomes the development by the market of technical and security standards for mobile payment services which include objectively necessary non-discriminatory measures to reduce the potential risk associated with these services. Neither does the report redefine, or suggest amendments to, the authorities' expectations in the areas of data protection, anti-money laundering and business continuity. When assessing compliance with the security recommendations, the authorities may take into account conformity with the relevant international standards." • According to this statement I suggest to make separately from this document a selection of technical recommendations and standards of standardization institutes for Security requirements and Security means for m-commerce and m-banking systems., There are standards and recommendations of ISO and NIST exist. As an example of such recommendation I want to introduce ITU-T recommendation Y.2740 "Security requirements for mobile remote financial transactions in next generation networks" http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11013 This recommendation describes security requirements for the mobile financial transactions, based on four specified security levels. It outlines probable risks in mobile commerce and mobile banking systems, and specifies means for risk reduction. Despite the fact that this recommendation is done for NGN it can be successfully used for any mobile network. • Definition of levels of security will allow rating of security of different mobile payment systems, what, from the point of view of ECB

			Recommendations for the security of mobile payments is very important, because according to it "MPSP's should engage in enhancing understanding and provide information on security issues related to the use of mobile payment services with a view to enabling customers to use such services in a safe and secure manner".
10	Scope and addressees	Clarification , Define clearly the methods or payment instruments in scope.	• It is difficult to decide which payment method is in scope and which is not. • e. g.: an authentication app used for payments seems not to be in scope. But how about a banking app with separated (sw/hw) authentication app/module?
11	Scope and addressees	Clarification , Define clear use cases	• It would be more helpful to distinguish between: - Who makes the payment to whom? - amounts of payment (low- vs. high-value) - Forms of payment (refundable, non-refundable, legal constraints, etc.) - What is being paid (physical good, digital good/service, pure money transfer)? - Where is the payment happening (on POS, internet, intra-country)? ⇨ These aspects are the drivers for appropriate security decisions and use cases, not for example how a payment was initiated (e. g. via NFC or QR Code)
12	Scope and addressees	Amendment, The recommendations should consider various security architectures (e.g. cloud services), and should not focus solely on architectures using secure elements and trusted service managers.	• The recommendations assume an underlying infrastructure very close to the concept of trusted service manager and hardware based (secure element) security architecture. This is not necessarily the underlying infrastructure for mobile payment apps and restricts the solution space.

13	Scope and addressees	Clarification	• It is not clear which specific payment methods are to be included within the scope of the Recommendations - for example when reviewing the document we have made the assumption that Contactless Cards are out of scope, however this is not expressly stated and may significantly alter our view on a number of the KCs if it were to be included.
14	General Part	Amendment/Deletion, The solely comparison of mobile payments and card payments is one possible form for a risk structure and therefore should be deleted or highlighted as an example.	• The forum compares mobile payments with card payments. This approach should be reconsidered, as the different possibilities of risk structuring depending on the underlying payment instrument. A direct adoption of chip card security measures for mobile payments is does not appear proportionate. • The recommendations imply that a MPSP can administer a (customer owned) mobile device in the same way a PSP can administer a payment card. The mobile device is owned and administered by the customer, whereas a chip card is owned by the PSP and the usage is restricted for specific/closed environments.
15	R1: Governance	Amendment, The recommendations should support an integrated and holistic security management approach and avoid specific small scale security policies for different products.	• MPSPs providing both an internet payment and a mobile payment solution have to support two different security policies. One for each payment method. Although, several security standard for different products are common, it is not common to manage specific security policies for different products. A policy is defined as a high level statement of the organization's believes, goals, and objectives and the general means for their attainment for specified subject area. A policy is brief and set at a high level.

16	R1: Governance	Amendment	• It is our belief that the Security Policies referenced in the KCs should be discussed / considered at Industry level also to gain a more collaborative approach.
17	KC 1.3	Clarification / Deletion	• It is a well meant suggestion but in reality it is not possible to enforce.
18	KC 1.3	Clarification	• Can ECB enforce MNOs and TSMs providers to fulfill a requirement?
19	KC 2.1	Amendment	• The control only mentions inherent factors of risk and not external factors such as publicly available attack vectors, attacker groups, skills, etc. • I would suggest to modify the last sentence in the following way: "The assessments should incorporate the results of the security incident monitoring process and vice versa (see Recommendation 3)." Because the results of the risk assessment are particularly relevant to focus incident monitoring efforts.
20	KC2.2	Clarification / Amendment	• What requirements will be placed upon 3rd Party Suppliers in terms of identifying and assessing their security measures? This Recommendation should relate to all parties and not just MPSPs.
21	KC 2.4, KC 3.3, KC 3.5	Amendment	• The relationship between a MPSP and 'his' merchants is a commercial issue
22	KC2.3	Amendment	• The concept of risk owner as introduced by the recent ISO27001:2013 could be reflected in the control.
23	BP3.1	Clarification	• In my opinion this best practice is very difficult to implement in practice.

24	KC 3.1	Clarification	• This implies dome form of SIEM. This process itself will require to be secured, by definition the only way this can work is through a software reporting mechanism which is vulnerable. • None of this will work if the device can be removed from connection to the host. Airplane Mode does this.
25	KC 3.2	Clarification	• This relates to previous point. This cannot be run from within a secure element (no space or processing capability) nor can it easily relay on an OS.
26	KC 3.5	Clarification	• The relationship between a MPSP and 'his' merchants is a commercial issue
27	KC 3.5	Clarification / Amendment	• We require clarity on the ECB's definition of 'Mobile Acquirer', in order to ensure that we achieve full compliance with this point. • We would encourage an industry-wide standard / guidance to encourage merchant participation in the reporting process and would not envisage the key responsibility for driving such activity to sit with the MPSP.
28	KC 4.3	Clarification	• List misses out the most important component: the app running on a mobile device. This too needs to be protected at s fundamental level. It also need to be able to react to attack attempts, report and be replaceable with a new, "good" version.
29	KC 4.5	Delete last sentence.	• The MPSP has no control over the functionality and access control mechanism of the mobile operating system.
30	KC 4.5	Clarification	• This can ONLY work when an OS or underlying system is itself protected. Such OS protection generally relies on trust in the platforms,

			something that simple jail-breaking will overcome. Applications themselves should protect themselves and data managed by them from "side-loading" and other similar attacks. Sand-boxing isn't enough.
31	KC 4.6	Clarification , Define more precisely payment-related software and limit recommended security measures to those that can be implemented by a MPSP.	• Next to the payment application, payment related software could be any piece of software on the mobile device (address book app, camera app, keyboard app, tcp/ip stack). The MPSP is not in a position to control/manage the software environment on the user's device. • The MPSP has no direct access to the hardware and operating system of the user's mobile devices. A verification of the payment-related software is so far limited to the internal control processes of the application of the MPSP.
32	KC 4.6	Clarification	• Further clarification from the ECB is sought regarding the term 'each access to the service' to ensure that our understanding aligns and we are able to achieve full compliance.
33	KC 4.7	Amendment, The recommended security measures should be limited to those that can be implemented by a MPSPs.	• In analogy to KC 4.6, the MPSP is limited to its own payment-related software, which he releases and develops. • The MPSP can control his own payment related software. The administration and validation of third party software is not possible and should be excluded from his responsibilities.
34	KC 4.7	Clarification	• We do not believe that it should be the MPSP's responsibility to ensure a customer's security patches etc. are up to date. As the owner of the mobile device, the customer should be held more accountable.
35	KC 4.8	Clarification	• This is obvious and necessary; however it relies on an old and weak model of "knowing what the attack threat is". Such active detection methods have significant faults in practice, as is demonstrated daily but traditional IT anti-virus and firewalls.

			• Mobile devices too have processing, storage and power restrictions that obviate against techniques developed for desk-top or network systems
36	KC 4.8 and KC 4.9	Amendment	• In my opinion this control shall be divided in three different control. The first one can be mixed with KC 4.9.: • 1. Security measures for mobile payment services should be periodically assessed, for instance using the firm's 3LoD model, to ensure their robustness and effectiveness. • 2. All changes should be subject to a formal change management process ensuring that changes are properly planned, tested, document and authorized. • 3. Ob the basis of the changes made and the security threats observed. Regression testing should be performed to incorporate scenarios of relevant and known potential attacks.
37	KC 4.9	Clarification	• Clarification of responsibility for the undertaking of audits, between MPSPs and external parties, such as Industry Schemes is sought. How will this requirement be fulfilled in practice?
38	KC 5.1	Clarification	• Again without the ability to be sure that the App generating this information has not been compromised this cannot be trusted. Spoofing will override, alter and fool monitoring systems without a significantly hardened and randomized challenge response system,
39	KC 5.2	Clarification	• We require clarification from the ECB as to whether the requirement for the retrieval of historical data is just for mobile payments, or for all financial transactions.

40	KC 6.1	Deletion	• In many use cases the mobile handset can be seen as a new way of using existing payment instruments, where the due diligence has already been made upon the time of issuing. This should be sufficient.
41	KC 6.1, 6.2, 7.1	Clarification	• Are all actors required to do this? I mean, other MSP providers than Banks should also establish the required authentication mechanisms.
42	KC 7.1	Clarification, The requirement for a strong customer authentication infrastructure should depend on the design of mobile payment product.	• If the mobile payment method does not involve any process where strong customer authentication is required (e. g solely low-value payments, customer registration via face-to-face-context) the implementation of an infrastructure for strong costumer authentication should be optional.
43	KC 7.1	Clarification, The requirement for a strong customer authentication infrastructure should depend on the design of mobile payment product.	• It is not clear if the possession of the mobile device itself could count as a first factor of authentication. If that is not the case, in my opinion, the addition of two additional authentication factors on top of it can jeopardize the usability and widespread deployment of mobile payments.
44	KC 7.2	Amendment, The requirement of strong customer authentication as default is not appropriate. It should only be applied when the risk analysis of the payment transaction requires it. Alternative authentication methods should in particular be allowed for transactions within associated MPSPs, in addition to the already considered transactions within one MPSP.	• The technological development of mobile devices and of mobile applications, suggests that in the near future manifold solutions for innovative authentication methods and also new risk mitigation tools will come onto the market. Therefore, the here mentioned specific requirements for strong costumer authentication hinder innovation and could obstruct the development of the digital market. • The choice of a method for user authentication should be based on the technical capabilities of current and future mobile end devices and enable innovative safety systems of the MPSPs when implemented.

45	KC 7.3	Glossary	• What are these? How/who manage these? What is the legal status of white lists?
46	KC 7.4	Deletion	• The recommendation ignores the limits of MPSPs regarding their capabilities to control the customer's device. The MPSP cannot manage the costumer's device. MPSPs have to rely on the correct implementation of security standards by mobile device manufacturers.
47	KC 7.4	Clarification / Amendment	• We would suggest that word 'passcode' is preferable to 'PIN', as this would help to sway customers away from the practice of using their Debit Card PIN number as another means of authentication. • We believe that it would be useful to specify the type of measures that would be expected here, for example PIN checking locally (i.e. in the App itself) or centrally by the MPSP.
48	KC 7.5	Clarification	• Usually, the merchant's acceptance device is not under direct control of the MPSP. Generally there is no direct (bilateral) communication between MPSP and acceptance device / payment terminal.
49	R8: Enrolment for and provision of authentication tools and/or software	Amendment, Remove direct dependencies of MPSPs from the processes of the telecommunication sector and their product life cycles, e.g. of application stores.	• The requirements were derived from the processes and procedures of telecommunication providers and their product life cycle process of the software distribution (application stores). It is difficult for MPSPs to comply with the requirements, without direct involvement of the MPSPs into the procedures of the telecommunication providers.
50	KC 8.1	Deletion/Amendment	• The current common „distribution channels"(App store, over-the-air deployment) for mobile device software are not under control of a MPSP. The MPSP can take third parties distribution channels into account for its risk analysis.

51	KC 8.2	Clarification / Amendment	• We require clarity as to whether this point relates specifically to NFC transactions.
52	KC 8.3	Amendment, The formulation should be changed. "The MPSP should be able to deactivate the payment function by appropriate adjustment of its systems."	• The MPSP has no access to the devices of the customer. However, he may disable the payment function of a specific client by configuring his **own** systems in such a way so that they no longer accept a transaction request of the customer.
53	KC 8.3	Deletion	• *"be in a position to deactivate the payment functionality of mobile devices remotely."*
54	KC 8.4	Clarification / Amendment	• It is our view that the responsibility for the cancellation of a device and subsequent reenrolment, does not sit with the MPSP. We do however accept that that the MSPS would have a role to play in educating the customer of the correct procedures to follow in the event of cancellation etc.
55	KC 8.3, KC 11.6, BP 11.2	Clarification	• This recommendation requires the handset to be 'online' which they not always are.
56	KC 9.1	Clarification	• It would be useful to be provided with some guidance on the one-time password timeframes that the ECB would consider as the 'strict minimum necessary'.
57	KC 10	Clarification	• As we already undertake transaction monitoring across our various payment channels, further clarity is sought from the ECB as to what is different for Mobile compared to other channels?
58	KC 10.2	Clarification	• Clarity is sought regarding the monitoring of payment activity and whether this relates to the sending of payments, the receiving of payments, or both.

59	BP 11.1	Deletion	• There is no need for issuing dedicated cards to mobile transactions. That is a commercial decision.
60	KC 11.2	Clarification	• Who should approve the hardware/software and to what standards?
61	KC 11.2	Delete "approved" or urge approval process.	• The client's hardware is not within the control of the MPSP. Although, there is a comprehensive risk analysis, there is no certification process that verifies the safety of the customers' mobile devices in the context of mobile payments. Also, this would not be feasible for a MPSPs at a reasonable cost seen the variety of hardware vendors, and the potential hardware-software combinations. A MPSP can test and further develop the software released and managed by him. For the software quality of third-party manufacturers he cannot make any statement.
62	KC 11.2	Amendment	• Also not every platform supports SEs, (iOS devices for example) and with he launch of Android 4.4 transactions from an NFC payment need not be routed through an SE.
63	KC 11.3	Clarification, This KC is ambiguous and should be adjusted.	• The requirement of end-to-end encryption in the context of mobile payments hinders competition and innovative activities of the market. A MPSP must have the opportunity to achieve maximum security through choosing the most suitable method available. This not necessarily achieved by end-to-end encryption. It must be guided by the specific system architecture of the mobile payment method. • In addition, it is unclear which data is to be transported by an end-to-end encryption. KC 11.3 is understood in such a way that the joint transport of sensitive payment data and personal data is considered as a special scenario where the data requires a special treatment.

			• The definition of end-to-end encryption should be specified in such a way that an end-to-end encryption can take place between trustfully network segments/nodes within an IT-system, respectively. A combination of several such sections must be possible.
64	KC 11.4	Deletion	• The implementation of contactless technology in the customer's mobile device is not under control of the MPSP.
65	KC 11.5	Amendment, This KC should be modified.	• A MPSP may take measures for the components that are directly and immediately under his control. For all other components that are beyond his control, the requirement cannot apply.
66	KC 11.6	This KC should be modified.	• A MPSP can only control parts of the transactions within his **own** system (e.g. not accepting transaction requests of a customer). The MPSP cannot control transactions which run solely on the mobile device (offline transactions). Deactivation of system components in the client's device cannot be part of KC 11.6., as the hardware is under the control of the customer and that external intervention is technically impossible for the MPSP and legally questionable.
67	KC 11.7	This requirement should be deleted.	• The requirement of special access data for mobile payment is regarded as disproportionate. • The design of payment systems and the security level must be assessed in the overall context. The use of uniform access data to different application scenarios is not considered as being critical. At the same time, the management and the user experience is improved and the tendency to wrongdoing is reduced. (For example, many customers write their data down when they need to remember too many data of the MPSP. This is not wanted from the perspective of a MPSP.)11.7 KC is absolutely impossible for MPSP regarding payment methods this

			MPSP does not offer or doesn't even know about. A MPSP cannot be made responsible for the solutions of other payment providers. • Regarding 11.7 KC a MPSP has no capability to avoid the re-usage of credentials in payment methods not under the control of this MPSP. He even doesn't know the (plaintext) credentials his customers use in his own solution.
68	KC 11.7	Clarification	• In order to aid understanding of what the ECB are looking achieve through this point, we would ask that they provide some narrative on the scenarios they consider could lead to cross-contamination risks.
69	BP 11.2	Clarification	• All of these rely on remote access to the device, something that is impossible to guarantee.
70	KC 12.1	Clarification	• Clarity is sought from the ECB on what they would deem a "secure channel" for customer education.
71	R12: Customer education and communication	Replace phrases regarding virus scanners, firewall and security patches in 12.4 KC by more feasible ones.	• Given the current mobile environments it is not feasible to require the installation of a firewall on a mobile. A common use case on the mobile is multimedia functionality offering several network services from the mobile to the local network (UPnP, Bluetooth, WLAN-File-Services, etc.). It is practically not viable to require or deny such services on mobiles. • And finally the customer and the MPSP both have nearly no influence on security patches. Most smartphone vendors, operating system providers, and app store providers usually do not support long term usage of their products and rarely offer security patches at all.

72	KC 13.2	Amendment	• These methods should be multiple and include out-of-band avenues in order to minimize the opportunity for interception by attackers.
73	KC 14.1	Clarification	• Which balances does this refer to?