Rapport
ECB Recommendation on Security for Internet Payments

Swedbank Response
Specification/version: v 1.0
2012-06-19

1. Introduction

Swedbank welcomes the ECB initiative to set a minimum standard for security in internet payments to enhance consumer and web merchant experience. However we would like to stress that security cost money and to change existing solutions into new, different ones with similar level of protection will be expensive and this is accelerated by the short time between the time when these recommendations are finalized and the 30th of June 2014. This will punish PSPs that already are providing secure payments but in a way that needs updating investments to meet the Securepay objectives with duplicate investment burden and indirectly therefore benefit the PSPs that have not made such investments.
In addition we want to point out that ***security on the internet must be ensured by all participants to the internet ecosystem; Internet Service Providers, web-Merchants, Payment Service Providers, Law Enforcement and Governments in general etc.*** Commitment and participation of all players in the effort to secure internet would bring a far better result than a PSP effort alone.
The ECB initiative need to be enlarged both when it comes to the scope of participant's involvement and when it comes to the geographical scope.
The present Swedbank Position paper has been structured as follows;

- First general remarks on the Recommendations
- Secondly comments on specific Recommendations and the underlying key considerations and best practices.

2. General Remarks

Swedbank is in favour of setting a basic level of security for internet payments if the scope is to ensure a level playing field for service providers in the internet payment processing and a minimum security level for both consumers and merchants. The goal of developing recommendations on security for internet payments must be to increase consumer confidence in web-services and encouraging consumers to see web-service as a valid alternative way of doing business.
For this to take place the consumer experience must be the same regardless of web-merchant and of which PSP is providing the web-merchant payment solutions. In addition the consumer experience must be pleasant i.e. the web merchant must provide an attractive and interesting web service combined with an easy to access and use payment service. These two achievements are necessary to reach set goals.

Will the Recommendations result in these two achievements? Partly but not fully and in some cases they may even prevent them from being reached.
It is of utmost importance that ECB understand that web services and internet payments are without geographical boundaries, contradictory to payments in the "old face2face world" internet payments are truly global. Seldom does the consumer know exactly where in the world the web-merchant is located or to what regulation/recommendations the merchant and its PSP adhere. This means that even though EU PSP:s abide to the Recommendations and implement proposed security levels and payment instruments consumers may still experience fraudulent behaviour in their web purchase activities should they shop at a EU located web-merchant using non-EU PSP payment services or from a web-merchant located outside the EU jurisdiction. The introduction of EU only instead of Global Recommendations could easily lead to a non level playing field where PSP:s outside of EU jurisdiction offer easier to use but less secure means of payments to EU web-merchants and even to that a non-EU web-merchant is preferred by the consumer as is offers easier to use and less complex payment services in comparison to the EU web-merchant.
To avoid a situation where requirements are significantly different on EU web-merchants and PSP:s in comparison with their direct competitors located outside of EU Swedbank propose that the Recommendations are introduced in a two step approach; 2014 as Recommendation on EU wide Business practices and at a later stage, based on a wide geographical implementation as Business practices, as Recommendation in a more global area. In parallel with the implementation of the Recommendations as business practice in EU ECB should take the initiative to ensure Global implementation by approaching Central Banks and equivalent outside of the EU.

As an alternative solution, should ECB not accept the proposal to implement the Recommendations as business practices, Swedbank proposes that the

Recommendations are implemented over a period of time, giving all participants to e-Commerce payments ample time to adjust and develop suitable measures and tools. The conversion of bank customers and suppliers from existing security applications into new ones will be a risky and costly operation ultimately paid for by the users in higher cost and thus pricing and risk of service disruptions when this major change takes place. In our opinion there should be a window of change from date of publication of Rules and finalized conversion of at least four years giving banks time to develop new solutions and migrate the large customer bases in orderly manner. Furthermore several regulatory activities are going on in Europe and these Rules should be phased into such a regulatory change package in order to make banks and other PSPs able to combine all changes asked for into one development process to avoid disturbing the merchant and customer markets multiple times with change demands in a few years time.
The ECB should also consider introducing a certification process to ensure that all providers are meeting the requirements. This certification could be complemented with a labelling of ECB approved stamp on such web services.

,
However should the Recommendations come into force in 2014 they raise some areas of concern;

3. Comments on specific recommendations and their KC/BP

3.1 Recommendations – level of detail

Using the setting of recommendations as the tool to ensure security in internet payments requires that the recommendation are structured as to brings clarity on the scope and objective yet leaving it up to the market to develop solutions and services. Unfortunately some of the recommendations are far too detailed and goes from being a recommendation to becoming a description of a solution to be implemented. When the development of solution and services are left to the market it encourages innovation in contradiction when the recommendation becomes too detailed which stifles innovation. For instance one recommendation points at 3Dsecure as suitable for this purpose. 3DS is a proprietary software solution owned by Visa Inc, USA, with some 10 years of operations already. Therefore it can be assumed that this solution does not fit everybody and future security requirements may need improved solutions.

3.2 All Participants to an Internet Payment

The recommendations aims at shifting the liability in Internet Payments to the issuing payment service provider or payer provider, payment instrument issuer (card, internetbank token etc.) and a clear understanding of where the liability lay in all sequence of an internet payment is valuable to all participants. However the recommendations fail to include all participants to an Internet Payment as Overlay service providers are not addressed at all. For the Recommendations to contribute to increased security in internet payments it is of essence that Overlay services are included. In some cases Overlay services invites the consumer to

give away their credentials and offer to act in their place towards the PSP. This can even be without knowledge to the consumer and provided on request of the Merchant. The Recommendation also neglects the importance of consumers being responsible in their usage of the payment instruments they have been provided with by their PSP:s. For the recommendation to fairly distribute liability without creating a non-level playing these two participants, their activities and responsibilities must be included in the Recommendation.

3.2.1 Overlay Services

As the recommendations fail to include so called Overlay Services the liability is shifted without taking into consideration that the bearer of the liability often has no control over such a service provider; procedure for authentication or level of security. If the purpose of the recommendations is to ensure a minimum level of security for Internet Payments it is of utmost importance that also Overlay Service providers are identified as possible participants to an Internet payment and regulated accordingly. Otherwise the liability will be shifted without allowing the bearer of liability to implement measures that balance the risk they will be carrying.

3.2.2 Merchants

In some areas the Recommendations declare the compliant behaviour of the web-merchant to be the responsibility of the PSP, for example KC 4.7, 7.5, 7.6 and BP 7.1. This can only be relevant when merchant compliance can be included in the service agreement between the merchant and the PSP and be monitored by the PSP. However many activities that can be related to a consumer purchase and the payment for it are handled well before the payment is initiated and is without control or reach for the PSP. The Recommendation must impose such requirements directly on the web-merchant and not on the PSP. In case monitoring as required it must be performed by relevant government bodies and not by PSP: s that lack policing powers.

3.2.3 Consumers

The purpose of the recommendations is to ensure consumer trust in internet payments which is a mutual goal for overseers, PSP:s and web-merchants. However consumers are a vital part of the security measures taken by merchants and PSP:s. A consumer that is provided with a payment instrument and is well informed of their obligations vis-à-vis the payment instrument should carry the liability for acting according to the agreement they have made with their PSP and/or the web-merchant. To create a balance that encourages all participants to contribute to security in internet payment the Recommendations needs to also include consumer responsibility.

3.3 Type of authentication

The recommendation only talks about strong authentication when more modern types of attacks on internet payments are largely unaffected by the strength of the authentication. Modern attacks (e.g. Trojans) changes the receiver account, the amount etc. on “the fly” after the authentication has been done by the consumer. These types of attacks should also be addressed in the recommendations otherwise the recommendations will not lead to the desired goal; consumer and merchant trust in internet payments.

3.4 Glossary of Terms - Definitions - clarifications

The recommendations refer to a variety of terms that may lead to confusion if not clearly defined in the paper. For example “strong authentication” is mentioned several times in the Recommendations but there is only a definition for “authentication”. Another example is that “mutually independent” is used but there is not clear definition on what is meant by “mutually independent”. On the same note “real time” is often mentioned and as “real time” has several definitions depending on in what situation it is used the paper need to clarify what is meant by “real time” in the relation to security for Internet payments.
To allow the recommendations to become market guidelines the glossary of terms needs to be enlarged to include all relevant and necessary definitions.

4. Recommendations - Comments and question marks

Recommendation 1: Governance

All providers should be covered by this document – not only PSPs.
A clarification is needed for the meaning of INDEPENDENT RM FUNCTION – our experience give at hand that RM should be a part of the business landscape

Recommendation 2: Risk identification and assessment

The recommendation lacks a statement that customers and merchants should be held accountable to the adherence of the user terms issued by the PSP when entering into an agreement of internet payment services. Protection should encompass all payment related data and not only “sensitive data”.

Recommendation 3: Monitoring and reporting

The security measures should apply to all participants in the value chain and not only affect PSP:s. In addition, to avoid unnecessary and costly administrative requirements, any new reporting should be incorporated in existing PSP reports to appropriate authorities.

Recommendation 4: Risk control and mitigation.

To ensure merchant adherence of for example 4.7 and other similar requirements there need to be a distribution of liability from PSP:s to merchants. It would be a strong incentive for Merchants to adhere to the requirement if it is connected to liability for the merchant This practice already exists in the insurance industry – if you break security rules, compensation can be withheld.

Recommendation 5: Traceability

This recommendation should be changed to give a high level security policy for traceability. AT the moment the recommendation is far to detailed and is actually regulating in detail how PSP:s should set up their operation, Recommendations on too detailed a level and, as in this case, regulating operation procedures etc. is contra-productive. Operations need to be possible to adopt at all times based on changes in the market such as risk, customer behaviour etc.

Recommendation 6: Initial customer identification, information

KC 6.1 implies that physical identification of customer is necessary prior to allowing into service – is this really the intent of the Recommendations?
This would limit consumer possibility to take advantage of offerings from a wider range of PSP:s as physical present is always required.
KC6.2 Technology, especially on the consumer side, evolves with the very high pace. Defining requirements on consumers equipment, software or other necessary tools (e.g. antivirus software, firewalls) with specific details might have negative consequences on consumer after technology changes. In our opinion the Recommendation should provide possibility to PSPs setting such requirements, in the detail level they deem appropriate
BP 6.1 – will burden customer with an additional contract including general terms and conditions – Any contractual relationship related to Payment services should be included into what is regulated and stated in the Payment Services Directive and not be regarded as a separate service. In many countries e-Commerce payments are mainstream payment services.

Recommendation 7: Strong customer authentication
7.1 KC At this moment of time strong authentication benefits cannot justify its costs in some countries. We suggest having other risk mitigation possibilities, such as low cumulative transaction limits, subject to risk analysis. Furthermore there are risks for other fraud attacks post authorisation but prior to final payment to consider.
KC 7.3 . 3DSecure is a 10 years old proprietary Visa Inc property and should not be mentioned here. Nor should there be a need for prior customer consent for internet payments from all cardholders in Europe. The recommendation mentions the necessity to pre register all cardholders in a 3DS directory when cards are issued assuming that all cards/card holders should be connected to internet payment services. It must however be possible for a PSP to offer cards without internet payment capability and it must also be possible for cardholders to opt not to use cards on the internet. If so, there is no need to pre-register ALL cards in a directory for internet purposes
7.6 KC. Liability shifts were very effective measure to ensure stronger authentication in payment schemas around the world. However it is important to understand that liability shifts do not work in global markets due to the fact that some regions do not implement them. ECB should call for ensuring similar liability shifts in other, non-European markets. Anyway this requirement on liability shift should state from issuer to acquirer since normally the merchant does not have any relation to the issuer of the card.

Recommendation 8: Enrolment for and provision of strong authentication tools
KC 8.1 The requirement on cards registration in connection to shopping is clunky and service disruptive for customers and experience shows that many customers will abandon the purchase when forced to register in a purchase session and therefore merchants tend to be against such practices.

Recommendation 9: Log-in attempts, session time-out, validity of authentication
KC.9.2 De blocking of blocked card – (Swedbank comment applies to Cards) this is a new principle and new routines have to be developed and implemented. In addition the entire value chain issuer.- scheme – acquirer will be affected – costly and cumbersome and not of importance to consumer. Existing procedures are sufficient and should be preserved.

Recommendation 10: Transaction monitoring and authorisation
KC 10.1 – Transaction monitoring is a vital part of business risk assessment and is of the utmost interest to all participants to the e-payment process, PSP:s, consumers, web-merchants alike. However the monitoring requirement should be proportionate to the level of security required taking into account amount, authentication used etc. I.e. lower value payments may be done with lesser monitoring whereas high value payments may require a more stringent real time monitoring in order to prevent fraudulent single transactions.
Differentiation is needed as real time monitoring may lead to a delay of payment completion to the detriment of merchants and customers which is only justifiable for consumers under specific circumstances such as high value payment
KC 10.1 - the requirement on merchant categories seems to be an operational rule and too detailed in a secure internet payment Recommendation. Furthermore schemes need to compete with each other and therefore may adopt different categories.

Recommendation 11: Protection of sensitive payment data
KC 11.2 – this will require banks to encrypt all internet related payment data in the main frame environment – very costly and difficult to achieve. The requirement should be for transportation between PSP:s only.

Recommendation 12: Customer education and communication
12.4KC. Swedbank acknowledge that the responsibility to inform and communicate secure and correct usage of payment instruments to consumers is the responsibility of the issuing PSP. However the requirements stated in KC 12.4 are on education and communication on secure usage of Internet as such and of Internet access device maintenance and security and not on usage of Payment Instrument. To educate EU citizens on how to use Internet in a secure way cannot be responsibility of PSP:s ONLY. Instead it must be a society wide responsibility and handled outside of the subject of Secure Payment Instruments etc.

Recommendation 13: Notifications, setting of limits
13.1KC. To request that the consumer must set a spending limit on his account and/or payment instrument before being able to use it for web-services is contra-productive if the scope of the Recommendations is to encourage consumers to see web-services as a valuable business alternative.
To not to be able to use the payment instrument the consumer already has in his hands to its full extent will hamper the usage and push consumers in the direction of using other means of payments or even other less regulated web-merchant services.
It would be sufficient and less cumbersome for the consumer if they are allowed to set spending limits rather than requested to do so. Such a service would allow a customer to increase security through spending limits should they want to do so without imposing it on all consumers.

Recommendation 14: Verification of payment execution by the customer
KC 14.1 The card payment system with authorisation on day 1 and financial transaction on day 1 + 1 means that there is no way in the card systems to show balance including same day purchases. Instead there will be information on blocked amounts due to approved authorisation request. This should be taken into account on this requirement.