ECB Recommendations for the Security of Internet Payments

GENERAL PART

Scope
General Principals
Implementation
Outline of the Report

This document is an excellent initiative, although its approach is at a very high level. In the future, to accomplish the objectives, it's necessary to clarify some definitions, scope (for instance Mobile Payments), timings and identify all activities.

- Payment Cards, Virtual Cards, Wallet, Credit Transfers, DD (only e-mandates)
  This response is mainly concerning Card Business, please take into consideration that all PCI-DSS compliant entities comply to most of the KCs in this document.

- July 2014, deadline for recommendations implementation
  The deadline established for the implementation of the KCs, may be harmful for the European players in terms of competition with other regions and may have a negative impact in current customer experience.

- Risk assessment and provisions
  It's an important aspect of this analysis. Portuguese PSPs have made a thorough work considering risk assessment. These will have a follow up and updates by the community. Its revision will be done on a regular base.

- Strong customer authentication (Guiding Principles II)
  - It is necessary to clarify the classification of present day instruments in regard to something you know/ have/ are.
  - It is possible that not all have an harmonized interpretation of these classifications (e.g the credit card number or matrix card is something you know or something you have?; an OTP received via an SMS sent to a Mobile is it considered simultaneously something you know and you have?).
  - The combination of concepts of non-reusable and non-replicable may eliminate valuable secure solutions.
  - Exception should be considered for strong authentication, for instance, in recurring payments, frequent users or low value operations.

  Notes:
  The current implementations of 3DS with static passwords will not comply with this principle (this is a concern linked to July 2014 deadline).
  Secure concepts like virtual cards may not accomplish strictly some of these requirements.

- Authorization and Monitoring
  Currently a significant percentage of Portuguese PSPs shared a centralized system for fraud prevention and detection guaranteeing high effectiveness against fraud.

- Customer awareness
  Customer awareness is considered an important aspect for the Portuguese PSPs. Portuguese PSPs, are currently in a process of publication of best practices for all participating agents on internet payments.

Additional Note:
By using the term "No Comment", Portuguese PSPs mean that we are completely aligned with the recommendations and there are several initiatives taking place in the Portuguese community that respond to them.

GENERAL CONTROL AND SECURITY ENVIRONMENT

Recommendation 1: Governance

PSPs should implement and regularly review a formal internet payment services security policy.

1.1 KC The internet payment services security policy should be properly documented, and regularly reviewed and approved by senior management. lt should define security objectives and the PSP's risk appetite.

No Comments, as per additional note at page 1

1.2 KC The internet payment services security policy should define roles and responsibilities, including an independent risk management function, and the reporting lines for internet payment services, including management of sensitive payment data with regard to the risk assessment, control and mitigation.

No Comments, as per additional note at page 1

1.1 BP The internet payment services security policy could be laid down in a dedicated document

Consider to integrate on a overall policy document

Recommendation 2: Risk identification and assessment

PSPs should regularly carry out and document thorough risk identification and vulnerability assessments with regard to internet payment services,

2.1 KC PSP's, through their risk management function, should carry out and document detailed risk identification and vulnerability assessments, including the assessment and monitoring of security threats relating to the internet payment services the PSP offers or plans to offer, taking into account: i) the technology solutions used by the PSP, ii) its outsourced service providers and, iii) all relevant services offered to customers. PSP's should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines both on the side of the PSP and the customer

No Comments, as per additional note at page 1

2.2 KC On this basis and depending on the nature and significance of the identified security threats, PSP's should determine whether and to what extent changes may be necessary to the existing security measures, the technologies used and the procedures or services offered. PSP's should take into account the time required to implement the changes (including customer roll-out) and take the appropriate interim measures to minimise disruption.

No Comments, as per additional note at page 1

2.3 KC The assessment of risks should address the need to protect and secure sensitive payment data, including: i) *both the customer's and the PSP's credentials used for internet payment services, and ii) any other information exchanged in the context of transactions conducted via the internet.*

No Comments, as per additional note at page 1

2.4 KC PSP's should undertake a review of the risk scenarios and existing security measures both after major incidents and before a major change to the infrastructure or procedures. ln addition, a general review should be carried out at least once a year. The results of the risk assessments and reviews should be submitted to senior management for approval.

No Comments, as per additional note at page 1

Recommendation 3: Monitoring and reporting

PSP's should ensure the central monitoring, handling and follow-up of security incidents, inc1uding security-related customer complaints. PSP's should establish a procedure for reporting such incidents to management and, in the event of major incidents, the competent authorities.

3.1 KC PSP's should have a process in place to centrally monitor, handle and follow up on security incidents and security-related customer complaints and report such incidents to the management.

No Comments, as per additional note at page 1

3.2 KC PSP's and card payment schemes should have a procedure for notifying the competent authorities (i.e. supervisory, oversight and data protection authorities) immediately in the event of major incidents with regard to the services provided.

No Comments, as per additional note at page 1

3.3 KC PSPs and card payment schemes should have a procedure for cooperating on all data breaches with the relevant law enforcement agencies.

No Comments, as per additional note at page 1

Recommendation 4: Risk control and mitigation

PSP's should implement security measures in line with their internet payment services security policy in order to mitigate identified risks. These measures should incorporate multiple layers of security defences, where the failure of one line of defence is caught by the next line of defence ("defence in depth").

4.1 KC In designing, developing and maintaining internet payment services, PSP's should pay special attention to the adequate segregation of duties in information technology (IT) environments (e.g. the development, test and production environments) and the proper implementation of the "least privileged" principle as the basis for a sound identity and access management.

No Comments, as per additional note at page 1

4.2 KC Public websites and backend servers should be secured in order to limit their vulnerability to attacks. PSP's 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. PSP's should use security measures that strip the servers of all superfluous functions in order to protect (harden) and eliminate vulnerabilities of applications at risk: Access by the various applications to the data and resources required should be kept to a strict minimum following the "least privileged" principle. In order to restrict the use of "fake" websites imitating legitimate PSP sites, transactional websites offering internet payment services should be identified by extended validation certificates drawn up in the PSP's name or by other similar authentication methods, thereby enabling customers to check the website's authenticity.

No Comments, as per additional note at page 1

4.3 KC PSP's should have processes in place to monitor, track and restrict access to: i) sensitive data, and ii) logical and physical critical resources, such as networks, systems, databases, security modules, etc. PSP's should create, store and analyse appropriate logs and audit trails.

No Comments, as per additional note at page 1

4.4 KC Security measures for internet payment services should be tested by the risk management function to ensure their robustness and effectiveness. Tests should also be performed before any changes to the service are put into operation. On the basis of the changes made and the security threats observed, tests should be repeated regularly and include scenarios of relevant and known potential attacks.

No Comments, as per additional note at page 1

4.5 KC The PSP's security measures for internet payment services should be periodically audited to ensure their robustness and effectiveness. The implementation and functioning of the internet services should also be audited. The frequency and focus of such audits should take into consideration, and be in proportion to, the security risks involved. Trusted and independent experts should carry out the audits. They should not be involved in any way in the development, implementation or operational management of the internet payment services provided.

We agree in general but it should be clear what is the scope of audits to be performed, not to overlap with current audits already performed (eg PCI; 3DS).

4.6 KC Whenever PSP's and card payment schemes outsource core functions related to the security of the internet payment services, the contract should include provisions requiring compliance with the principles and recommendations set out in this report

No Comments, as per additional note at page 1

4.7 KC PSPs offering acquiring services should require e-merchants to implement security measures on their website as described in this recommendation.

No Comments, as per additional note at page 1

Recommendation 5: Traceability

PSP's should have processes in place ensuring that all transactions can be appropriately traced.

5.1 KC PSPs should ensure that their service incorporates security mechanisms for the detailed logging of transaction data, including the transaction sequential number, timestamps for transaction data, parameterisation changes and access to transaction data.

No Comments, as per additional note at page 1

5.2 KC PSPs should implement log files allowing any addition, change or deletion of transaction data to be traced.

No Comments, as per additional note at page 1

5.3 KC PSPs should query and analyse the transaction data and ensure that any log files can be evaluated using special tools. The respective applications should only be available to authorised personnel.

No Comments, as per additional note at page 1

5.1 BP [cards] It is desirable that PSPs offering acquiring services require e-merchants who store payment information to have these processes in place.

No Comments, as per additional note at page 1

Specific Control and Security measures for Internet Payments

Recommendation 6: Initial customer identification, information

Customers should be properly identified and confirm their willingness to conduct internet payment transactions before being granted access to such services. PSPs should provide adequate "prior" and "regular" information to the customer about the necessary requirements (e.g. equipment, procedures) for performing secure internet payment transactions and the inherent risks.

6.1 KC PSPs should ensure that the customer has undergone the necessary identification procedures and provided adequate identity documents and related information before being granted access to the internet payment services.

No Comments, as per additional note at page 1

6.2 KC PSPs should ensure that the prior information [11] supplied to the customer contains specific details relating to the internet payment services. These should include, as appropriate:

- *clear information on any requirements in terms of customer equipment, software or other necessary tools (e.g. antivirus software, firewalls);*
- *guidelines for the proper and secure use of personalised security credentials;*
- *a step-by-step description of the procedure for the customer to submit and authorise a payment, including the consequences of each action;*

- *guidelines for the proper and secure use of all hardware and software provided to the customer;*

- *the procedures to follow in the event of loss or theft of the personalised security credentials or the customer's hardware or software for logging in or carrying out transactions;*
- *the procedures to follow if an abuse* is *detected or suspected;*

- *a description of the responsibilities and liabilities of the PSP and the customer respectively with regard to the use of the internet payment service.*

No Comments, as per additional note at page 1

6.3 KC PSPs should ensure that the framework contract with the customer includes compliance-related clauses enabling the PSP to fulfil its legal obligations relating to the prevention of money laundering, which may require it to suspend execution of a customer's payment transaction pending the necessary regulatory checks and/or to refuse to execute it. The contract should also specify that the PSP may block a specific transaction or the payment instrument on the basis of security concerns. It should set out the method and terms of the customer notification and how the customer can contact the PSP to have the service "unblocked", in line with the Payment Services Directive.

No Comments, as per additional note at page 1

6.4 KC PSPs should also ensure that customers are provided, on an ongoing basis and via appropriate means (e.g. leaflets, website pages), with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service.

No Comments, as per additional note at page 1

6.1 BP It is desirable that the customer signs a dedicated service contract for conducting internet payment transactions, rather than the terms being included in a broader general service contract with the PSP.

We do not agree. The client general contract should also include Internet payments (no segregation is recommended because it might increment the complexity and confusion to the customer).

Recommendation 7: Strong customer authentication

Internet payment services should be initiated by strong customer authentication.

7.1 KC [CT/e-mandate] Credit transfers (including bundled credit transfers) or electronic direct debit mandates should be initiated by strong customer authentication. PSPs could consider adopting less stringent customer authentication for outgoing payments to trusted beneficiaries included in previously established "white lists", i.e. a customer-created list of trusted counterparties and beneficiary accounts with strong authentication.

No Comment, as per additional note at page 1

7.2 KC Obtaining access to or amending sensitive payment data requires strong authentication. Where a PSP offers purely consultative services, with no display of sensitive customer or payment information, such as payment card data, that could be easily misused to commit fraud, the PSP may adapt its authentication requirements on the basis of its risk analysis.

Conditioned by comments included on guiding principle two

7.3 KC [cards] For card transactions, all PSPs offering issuing services should support strong authentication of the cardholder. 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. (See Annex 3 for a description of authentication under the cards environment.)

Conditioned by comments included on guiding principle two

7.4 KC [cards] All PSPs offering acquiring services should support technologies allowing the issuer to perform strong authentication of the ca rdho lde r for the card payment schemes in which the acquirer participates.

Conditioned by comments included on guiding principle two

7.5 KC [cards] PSPs offering acquiring services should require their e-merchant to support strong authentication of the cardholder by the issuer for card transactions via the internet. Exemptions to this approach should be justified by a (regularly reviewed) fraud risk analysis. In the case of exemptions, the use of the card verification code, CVx2, should be a minimum requirement.

Conditioned by comments included on guiding principle two.
There is one aspect that must be taken into consideration. We agreed on CVx2 as a minimum requirement, but recurring payments should be considered and detailed.

7.6 KC [cards] All card payment schemes should promote the implementation of strong customer authentication by introducing liability shifts (i.e. from the e-merchant to the issuer) in and across all European markets.

Great care has to be taken in order not to harm European merchants, acquirers PSPs and ultimately cardholders.

7.7 KC [cards] For the card payment schemes accepted by the service, providers of wallet solutions should support technologies allowing the issuer to perform strong authentication when the legitimate holder first registers the card data. Providers of wallet solutions should support strong user authentication when executing card transactions via the internet. Exemptions to this approach should be justified by a (regularly reviewed) fraud risk analysis. In the case of exemptions, the use of CVx2 should be a minimum requirement.

Conditioned by comments included on guiding principle two

7.8 KC [cards] For virtual cards, the initial registration should take place in a safe and trusted environment (as defined in Recommendation 8). Strong authentication should be required for the virtual card data generation process if the card is issued in the internet environment.

Conditioned by comments included on guiding principle two

7.1 BP [cards] It is desirable that e-merchants support strong authentication of the cardholder by the issuer in card transactions via the internet. In the case of exemptions, the use of CVx2 is recommended

Conditioned by comments included on guiding principle two

7.2 BP For customer convenience purposes, PSPs providing multiple payment services could consider using one authentication tool for all internet payment services. This could increase acceptance of the solution among customers and facilita te proper use.

No Comments, as per additional note at page 1

Recommendation 8: Enrolment for and provision of strong authentication tools

PSPs should ensure that customer enrolment for and the initial provision of strong authentication tools required to use the internet payment service is carried out in a se cure manner.

8.1 KC Enrolment for and provision of strong authentication tools should fuljil the following requirements.

- *The related procedures should be carried out in a safe and trusted environment (e.g. face-to-face at a PSP's premises, via an internet banking or other secure website offering comparable security features, or via an automated teller machine).*

- *Personalised security credentials and all internet payment-related devices and software enabling the customer to perform internet payments should be delivered securely. Where tools need to be physically distributed, they should be sent by post or delivered with acknowledgement of receipt signed by the customer. Software should also be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with. Moreover, personalised security credentials should not be communicated to the customer via e-mail or website.*

- *[cards] For card transactions, the customer should have the option to register for strong authentication independently of a specific internet purchase. ln addition, activation during online shopping could be offered by re-directing the customer to a safe and trusted environment, preferably to an internet banking or other secure website offering comparable security features.*

No Comments, as per additional note at page 1

8.2 KC [cards] Issuers should actively encourage cardholder enrolment for strong authentication. Cardholders should only be able to bypass strong authentication in exceptional cases where this can be justified by the risk related to the card transaction. ln such instances, weak authentication based on the cardholder name, personal account number, expiration date, card verification code (CVx2) and/or static password should be a minimum requirement.

No Comments, as per additional note at page 1

Recommendation 9: Log-in attempts, session time-out, validity of authentication

PSPs should limit the number of authentication attempts, define rules for payment session "time out" and set time limits for the validity of authentication.

9.1 KC When using a one-time password for authentication purposes, PSPs should ensure that the validity period of such passwords is limited to the strict minimum necessary (i.e. a few minutes).

No Comments, as per additional note at page 1

9.2 KC PSPs should set down the maximum number of failed log-in or authentication attempts after which access to the internet service is (temporarily or permanently) blocked. They should have a secure procedure in place to re-activate blocked internet services.

No Comments, as per additional note at page 1

9.3 KC PSPs should set down the maximum period after which inactive payment sessions are automatically terminated, e.g. after ten minutes.

No Comments, as per additional note at page 1

Recommendation 10: Transaction monitoring and authorisation

Security monitoring and transaction authorisation mechanisms aimed at preventing, detecting and blocking fraudulent payment transactions before they are executed should be conducted in real time; suspicious or high risk transactions should be subject to a specific screening and evaluation procedure prior to execution.

10.1 KC PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules (such as black lists of compromised or stolen card data), abnormal behaviour patterns of the customer or the customer's access device (change of Internet Protocol (IP) address 12 or IP range during the internet payment session, sometimes identified by geolocation IP checks." abnormal transaction data or e-merchant categories, etc.) and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions should be commensurate with the outcome of the fraud risk assessment.

No Comments, as per additional note at page 1

10.2 KC Card payment schemes in cooperation with acquirers should elaborate a harmonised definition of e-merchant categories and require acquirers to implement it accordingly in the authorisation message conveyed to the issuer,"

No Comments, as per additional note at page 1

10.1 BP It is desirable that PSPs perform the screening and evaluation procedure within an appropriate time period, in order not to unduly delay execution of the payment service concerned.

No Comments, as per additional note at page 1

10.2 BP It is desirable that PSPs notify the customer of the eventual blocking of a payment transaction, under the terms of the contract, and that the block is maintained for as short a period as possible until the security issues have been resolved.

No Comments, as per additional note at page 1

Recommendation 11: Protection of sensitive payment data

Sensitive payment data should be protected when stored, processed or transmitted.

11.1 KC All data or files used to identify and authenticate customers (at log-in and when initiating internet payments or other sensitive operations), as well as the customer interface (PSP or e-merchant website), should be appropriately secured against theft and unauthorised access or modification.

No Comments, as per additional note at page 1

11.2 KC PSPs should ensure that when transmitting sensitive payment data, a secure end-to-end communication channel is maintained throughout the entire duration of the internet payment service provided in order to safeguard the confidentiality of the data, using strong and widely recognised encryption techniques.

No Comments, as per additional note at page 1

11.3 KC [cards] PSPs offering acqumng services should encourage their e-merchants not to store any sensitive payment data related to card payments. ln the event e-merchants handle, i.e. store, process or transmit sensitive data related to card payments, such PSPs should require the e-merchants to have the necessary measures in place to protect these data and should refrain from providing services to e-merchants who cannot ensure such protection.

No Comments, as per additional note at page 1

11.1 BP [cards] It is desirable that e-merchants handling sensitive cardholder data appropriately train their dedicated fraud management stafJ and update this training regularly to ensure that the content remains relevant to a dynamic security environment.

No Comments, as per additional note at page 1

CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION

Recommendation 12: Customer education and communication

PSPs should communicate with their customers in such a way as to reassure them of the integrity and authenticity of the messages received. The PSP should provide assistance and guidance to customers with regard to the secure use of the internet payment service.

12.1 KC PSPs should provide at least one secured channel " for ongoing communication with customers regarding the correct and secure use of the internet payment service. PSPs should inform customers of this channel and explain that any message on behalf of the PSP via any other means, such as e-mail, which concerns the correct and secure use of the internet payment service, is not reliable. The PSP should explain:

- *the procedure for customers to report to the PSP (suspected) fraudulent payments, suspicious incidents or anomalies during the internet payment session and/or possible social engineering 16 attempts;*
- *the next steps, i.e. how the PSP will respond to the customer;*
- *how the PSP will notify the customer about (potential) fraudulent transactions or warn the customer about the occurrence of attacks (e.g. phishing e-mails).*

No Comments, as per additional note at page 1

12.2 KC Through the designated channel, PSPs should keep customers informed about updates in procedures and security measures regarding internet payment services. Any alerts about significant emerging risks (e.g. warnings about social engineering) should also be provided via the designated channel.

No Comments, as per additional note at page 1

12.3 KC Customer assistance should be made available by PSPs for all questions, complaints, requests for support and notifications of anomalies or incidents regarding internet payments, and customers should be appropriately informed about how such assistance can be obtained

No Comments, as per additional note at page 1

12.4 KC PSPs and, where relevant, card payment schemes should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need:

- *to protect their passwords, security tokens, personal details and other confidential data;*
- *to manage properly the security of the personal device (e.g. computer), through installing and updating security components (antivirus, firewalls, security patches);*
- *to consider the significant threats and risks related to downloading software via the internet if the customer cannot be reasonably sure that the software is genuine and has not been tampered with;*
- *to use the genuine internet payment website.*

No Comments, as per additional note at page 1

12.1 BP [cards] It is desirable that PSPs offering acquiring services arrange educational programmes for their e-merchants on fraud prevention.

No Comments, as per additional note at page 1

Recommendation 13: Notifications, setting of limits

PSPs should provide their customers with options for risk limitation when using internet payment services. They may also provide alert services.

13.1 KC Prior to providing internet payment services, PSPs should agree with each customer on spending limits applying to those services (e.g. setting a maximum amount for each individual payment or a cumulative amount over a certain period of time), and on allowing the customer to disable the internet payment functionality.

No Comments, as per additional note at page 1

13.1 BP Within the agreed limits, e.g. taking into account overall spending limits on an account, PSPs could provide their customers with the facility to manage limits for internet payment services in a secure environment.

No Comments, as per additional note at page 1

13.2 BP PSPs could implement alerts for customers, such as via phone calls or SMS, for fraud-sensitive payments based on their risk-management policies.

No Comments, as per additional note at page 1

13.3 BP PSPs could enable customers to specify general, personalized rules as parameters for their behaviour with regard to internet payments, e.g. that they will only initiate payments from certain specific countries and that payments initiated from elsewhere should be blocked.

No Comments, as per additional note at page 1

Recommendation 14: Verification of payment execution by the customer

PSPs should provide customers in good time with the information necessary to check that a payment transaction has been correctly executed.

14.1 KC PSPs should provide customers with a facility to check transactions and account balances at any time in a secure environment.

No Comments, as per additional note at page 1

14.2 KC Any detailed electronic statements should be made available in a secure environment. Where PSPs periodically inform customers about the availability of electronic statements (e.g. when a new monthly e-statement has been issued, or on an ad hoc basis after execution of a transaction) through an alternative channel, such as SMS, e-mail or letter, sensitive payment data should not be included in such statements or, if included, they should be masked.

No Comments, as per additional note at page 1