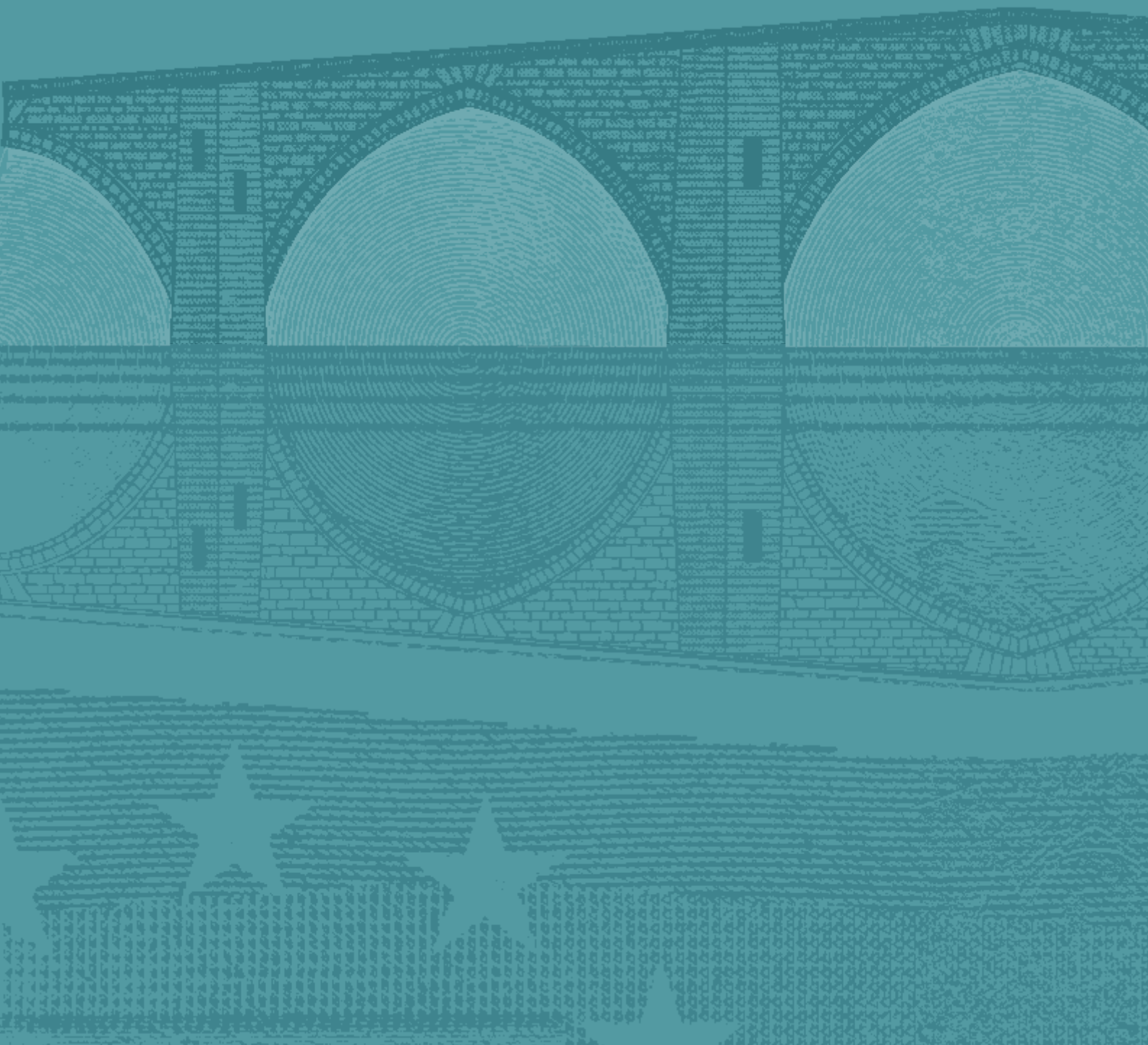
EUROPEAN CENTRAL BANK

EUROSYSTEM

ASSESSMENT GUIDE FOR THE SECURITY OF INTERNET PAYMENTS

FEBRUARY 2014



EUROPEAN CENTRAL BANK

EUROSYSTEM

In 2014 all ECB publications feature a motif taken from the €20 banknote.

ASSESSMENT GUIDE FOR THE SECURITY OF INTERNET PAYMENTS

FEBRUARY 2014

Address
Kaiserstrasse 29
60311 Frankfurt am Main
Germany

Postal address
Postfach 16 03 19
60066 Frankfurt am Main
Germany

Telephone
+49 69 1344 0

Website
http://www.ecb.europa.eu

Fax
+49 69 1344 6000

ISBN: 978-92-899-1159-7 (online)
EU Catalogue number: QB-04-14-051-EN-N (online)

CONTENTS

I INTRODUCTION

This assessment guide has been developed by the European Forum on the Security of Retail Payments, SecuRe Pay (the "Forum"), on the basis of the final "Recommendations for the security of internet payments" (the "Recommendations") published on the ECB's websiteon 31 January 2013.

This assessment guide is intended for those supervisory and oversight authority staff of the Member States who are in charge of assessing compliance with the internet recommendations in the respective countries and is aimed at ensuring that assessments are harmonised and efficient throughout the EU/EEA. This shall facilitate the supervisory/oversight authorities in comparing and/or aggregating findings across Member States, without prejudice to the supervisory controls carried out in accordance with their respective responsibilities. While following the general path provided by this guide, the supervisory/oversight staff will exercise professional judgement, looking at the specific features of the context examined, including possible adaptation and integration of any questions, checkpoints or evidence/reference documentation required. In order to facilitate this exercise, this assessment guide shall be published on the ECB's website.

The Recommendations are expected to contribute to fighting and preventing payment fraud, thus enhancing consumer trust in internet payments. They were formulated as generically as possible in order to accommodate continual technological innovation. The Forum is aware that new threats can arise at any time and will therefore review the recommendations and this assessment guide from time to time. Items in this guide could potentially be subject to changes, taking into account the revised Payment Services Directive (PSD), once it has been endorsed by the European Parliament.

The Recommendations do not attempt to set specific security or technical solutions, nor do they redefine, or suggest amendments to, existing industry technical standards or the authorities' expectations in the areas of data protection and business continuity. When assessing compliance with the security recommendations, the authorities may take into account compliance with the relevant international standards. Where the Recommendations indicate solutions, the same result may be achieved through other means. The Recommendations outlined constitute minimum expectations. They are without prejudice to the responsibility of payment service providers (PSPs), governance authorities (GAs) of payment schemes and other market participants to monitor and assess the risks involved in their payment operations, develop their own detailed security policies and implement adequate security, contingency, incident management and business continuity measures that are commensurate with the risks inherent in the payment services provided.

The Recommendations include key considerations (KCs) and best practices (BPs) that further specify the content of each recommendation. This guide lists assessment questions for each KC and BP, and, where necessary, complements them by illustrative checkpoints which provide further guidance on how to ensure that a question is answered in sufficient detail and interpreted in a consistent way. Furthermore, examples are given of potentially relevant supporting documents (the list is not exhaustive) which could be used to gain reasonable assurance when assessing compliance with the Recommendations.

The assessment questions shall help to ensure a harmonised interpretation of the recommendations. However, they should not be considered prescriptive. Instead, different options could be equally satisfactory in terms of reaching an acceptable level of compliance for each recommendation. The assessment guide describes generic situations, so it may be that not all aspects are of relevance for all PSPs or GAs. This needs to be taken into account throughout the assessment process.

SCOPE AND ADDRESSEES

Unless stated otherwise, the recommendations, key considerations and best practices specified are applicable to all PSPs providing internet payment services, as defined in the PSD,[1] as well as to GAs of payment schemes[2] (card payment schemes, credit transfer schemes, direct debit schemes, etc.) The purpose of the Recommendations is to define common minimum requirements for the internet payment services listed below, irrespective of the access device used:

- [Cards] The execution of card payments on the internet, including virtual card payments, as well as the registration of card payment data for use in "wallet solutions".
- [Credit transfers] The execution of credit transfers on the internet.
- [E-mandates] The issuance and amendment of direct debit electronic mandates.
- [E-money] Transfers of electronic money between two e-money accounts via the internet.

Payment integrators[3] offering payment initiation services are considered to be either acquirers of internet payment services (and thus PSPs) or external technical service providers of the relevant schemes. In the latter case, the payment integrators should be contractually required to comply with the recommendations.

The following are excluded from the scope of the recommendations, key considerations and best practices:[4]

- other internet services provided by a PSP via its payment website (e.g. e-brokerage, online contracts);
- payments where the instruction is given by post, telephone order, voicemail or using SMS-based technology;
- mobile payments other than browser-based payments;[5]
- credit transfers where a third party accesses the customer's payment account;
- payment transactions made by an enterprise via dedicated networks;
- card payments using anonymous and non-rechargeable physical or virtual pre-paid cards where there is no ongoing relationship between the issuer and the cardholder;
- clearing and settlement of payment transactions.

1 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, p. 1.

2 The GA is accountable for the overall functioning of the scheme that promotes the payment instrument in question and ensures that all the actors involved comply with the scheme's rules. Moreover, it is responsible for ensuring the scheme's compliance with oversight standards. See European Central Bank (2009), *Harmonised oversight approach and oversight standards for payment instruments*, February.

3 Payment integrators provide the payee (i.e. the e-merchant) with a standardised interface to payment initiation services provided by PSPs.

4 Some of these items may be the subject of a separate report at a later stage.

5 Specific recommendations applying to the release and maintenance of software applications are subject to the recommendations on mobile payments.

CORE DEFINITIONS

The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication. For the purpose of this report, **sensitive payment data** are defined as data which could be used to carry out fraud[6]. These include (i) data enabling a payment order to be initiated, (ii) data used for authentication, (iii) data used for ordering payment instruments or authentication tools to be sent to customers, as well as (iv) data, parameters and software which, if modified, may affect the legitimate party's ability to verify payment transactions, authorise e-mandates or control the account, such as "black" and "white" lists, customer-defined limits, etc.

An indicative list of elements is outlined below that could, depending on the circumstances under which the data are used, be considered as sensitive payment data. In line with the recommendations, the entity being overseen/supervised should provide the supervisor/overseer with a list of those elements it considers to be sensitive payment data. On the basis of this, the overseer/supervisor will decide the sensitivity of the following on a case-by-case basis, taking into account the respective business model:

a) the set of data enabling a payment order to be initiated, e.g.:
- payment account identifiers of the customer stored at the PSP (IBAN[7] or equivalent); the BIC should not be considered sensitive data;
- payment card data (PAN, expiry date, CVx2);

b) data used for authentication (when applicable and used in this context), such as:
- customer identifiers (e.g. client number/log-in name);
- passwords, codes, personal identification numbers (PINs), secret questions, reset passwords/codes;
- phone number (mobile or landline, when applicable);
- certificates;

c) data used for ordering payment instruments or authentication tools to be sent to customers (offering this functionality online in the case of PSPs, otherwise those data that are not considered sensitive), e.g.
- client's postal address;
- phone number, e-mail address;

d) data, parameters and software stored in the PSP's systems which, if modified, may undermine the security of the delivery of payment instruments or authentication tools to the customer or may affect the latter's ability to verify payment transactions, authorise e-mandates or control the account, e.g.
- "black" and "white" lists, customer-defined limits, etc.
- data outlined in (a), (b) and (c), depending on applicability and methods used.

6 The PSP/GA might need to take a broader approach in order to comply with other requirements, such as data protection or privacy laws.
7 If confirmed by the Euro Retail Payments Board.

Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.

Further guidance on strong customer authentication solutions is provided under Recommendation 7. From the Forum's perspective, PSPs with no or only weak authentication procedures cannot, in the event of a disputed transaction, provide proof that the customer has authorised the transaction.

IMPLEMENTATION

As stated in the Recommendations, addressees are expected to comply with both the Recommendations and the KCs or to be able to explain and justify any deviation from them on request of the relevant competent authority ("comply or explain" principle). Furthermore, PSPs, GAs of payment schemes and the relevant market participants are encouraged to adopt best practices.

In order to demonstrate compliance, assessment questions (as outlined in this guide) need to be answered. Once an assessment is initiated by the authority, PSPs/GAs should submit all answers and background documentation in electronic form as far as possible. Contractual agreements can be submitted as scanned copies showing the date and signatures. Specific or personalised information, such as the exact value of an agreed fee or personal details, can be blacked out.

2 RECOMMENDATIONS

GENERAL CONTROL AND SECURITY ENVIRONMENT

Recommendation 1: Governance

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

1.1 KC The security policy should be properly documented, and regularly reviewed (in line with KC 2.4) and approved by senior management. It should define security objectives and the risk appetite.

1.1.1 Does the PSP/GA have a formal security policy in place regarding internet payment services (e.g. in the ambit of an entity's broader information security policy, or of a policy concerning the security of IT systems and services)?

- The PSP/GA has defined security policies regarding the relevant domains of internet payment services (e.g. security management, protection of sensitive data or devices, initiation and operation of transactions and outsourcing).
- The security policies define at least the following elements:

a) objectives and organisation of information security;
b) principles for the secure use and management of information and ICT resources;
c) role and responsibilities, security activities and processes;
d) human resource security;
e) logical/physical security controls;
f) security arrangements for outsourced information/services;
g) the security policies are documented and a procedure is in place to make the relevant parties aware of the security policies and procedures.

- With reference to the GA's security policy sections that are applicable to all payment scheme members, the GA has defined regulations and/or contractual agreements which:

a) require all payment scheme members to comply with the GA's security policy (e.g. the scheme's rules and provisions);
b) allow the GA to check whether payment scheme members are acting accordingly (e.g. assessments, on-site inspections, etc.) and, in the case of non-compliance, give it the power to restore compliance (e.g. action plan, sanctions and penalties, licence revocation)

Applies to: All

Supporting documents: Security policy

1.1.2 Does the policy define security objectives and risk appetite as applicable to internet payment services?

- The PSP/GA's security policies define the security objectives with reference to internet payment services.

- The security objectives are defined on the basis of the PSP/GA's risk appetite coming from its capacity to absorb the relevant loss (e.g. financial loss, reputation damage) and predisposition towards risk-taking (cautious or aggressive in this field).

Applies to: All

Supporting documents: Security policy

1.1.3 Has the security policy been approved by the board or an adequate management body and communicated and made available on a "need-to-know" basis to all relevant employees and external parties?

Applies to: All

Supporting documents: Records of management decisions (e.g. circulars)

1.1.4 Has the PSP/GA documented the criteria that drive the updating of the policy?
Do these criteria ensure that the policy is regularly reviewed and kept up to date?

- The security policy review is carried out at least once a year on the basis of a formal and well-documented procedure which clearly defines:

a) the frequency of, and criteria for, its activation (e.g. major changes in the risk assessment results, business models or technologies adopted), the role and responsibilities of the entities involved, and the time schedule for its execution;

b) inputs for the review (e.g. risk assessment results, audit results, effective measurements and the status of corrective actions, recommendations from authorities, any changes that could affect internet payment services, etc.);

c) review outputs (e.g. risk treatment plan, resources needs, etc.).

- The results of the reviews are clearly documented and records are maintained.

Applies to: All

Supporting documents: Risk assessment report

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

1.2.1 Does the security policy include a clear definition of all roles and responsibilities related to the security of internet payment services?

- The security policy assigns specific roles and responsibilities for information security across the organisation.

- The security roles and responsibilities of employees, contractors and third party providers are defined and documented in accordance with the organisation's information security policy.
- Security roles and responsibilities include the requirement to:

a) implement and act in accordance with the security policies;
b) protect assets from unauthorised access, disclosure, modification, destruction or interference;
c) execute particular security processes or activities;
d) ensure responsibility is assigned to the individual for actions to be taken;
e) report actual or potential security events or other security risks to the organisation;
f) monitor new developments in technology and security (e.g. through participation in special security forums and professional associations), as well as reviewing the security policies accordingly.

- The management ensures that all personnel who are assigned responsibilities defined in the security policies are sufficiently competent to perform the tasks required.

Applies to: All

Supporting documents: Security policy, job profiles and sample curricula

1.2.2 Do these roles and responsibilities comprise the risk management function?[8] Is there a direct reporting line between those responsible for risk management and the board?

Applies to: All

Supporting documents: Security policy

1.2.3 Does the policy define clear reporting lines for internet payment services?

Applies to: All

Supporting documents: Security policy

1.2.4 Does the security policy include specific roles and responsibilities, risk assessment activities, control and mitigation concerning the management of sensitive payment data?

Applies to: All

Supporting documents: Security policy

1.1 BP The security policy could be laid down in a dedicated document.

8 I.e. coordinated activities to direct and control the organisation with regard to risk; it typically includes risk assessment, risk treatment, risk acceptance and risk communication.

1.1.1 BP Is the security policy for internet payment services laid down in a dedicated document? If not, are the provisions applicable to the internet payment services easily identifiable?

Applies to: All

Supporting documents: Security policy

Recommendation 2: Risk assessment

PSPs and payment schemes should carry out and document thorough risk assessments with regard to the security of internet payments and related services, both prior to establishing the service(s) and regularly thereafter.

2.1 KC PSPs and payment schemes, through their risk management function, should carry out and document detailed risk assessments for internet payments and related services. PSPs and payment schemes should consider the results of the ongoing monitoring of security threats relating to the internet payment services they offer or plan to offer, taking into account: i) the technology solutions used by them, ii) services outsourced to external providers and, iii) the customers' technical environment. PSPs and payment schemes should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines both on their side[9] and the side of their customers,[10] as well as the results of the security incident monitoring process (see Recommendation 3).

2.1.1 Has the PSP/GA conducted and documented a detailed risk assessment for internet payments and related services, taking into account the risk profiles of the actors involved in the service provision (based, for example, on risk management methodologies that are up to date and recognised throughout the industry, such as those developed by the ISO, the Project Management Institute and the National Institute of Standards)?

Applies to: All

Supporting documents: Risk assessment/Audit report and risk assessment methodology

2.1.2 Does the risk assessment cover all the PSP/GA's possible areas of responsibility (e.g. organisational, personnel, infrastructural and technical), possible security threats (internal and external) and their magnitude (impact and likelihood), existing or potential safeguards (e.g. technical controls and insurance), vulnerabilities and residual risks?

Applies to: All

Supporting documents: Risk assessment report

9 Such as the susceptibility of the system to payment session hijacking, SQL injection, cross-site scripting, buffer overflows, etc.
10 Such as risks associated with using multimedia applications, browser plug-ins, frames, external links, etc.

2.1.3 Does the risk assessment take into account:

- *(on the PSP/GA side) the services outsourced to external providers, as well as results of the security incident monitoring;*
- *(both on the side of the PSP/GA and on the side of their customers) the technology solutions and platforms used, application architecture, programming techniques and routines?*

Applies to: All

Supporting documents: Risk assessment/Audit report and risk assessment methodology

2.1.4 Do the contracts with the external providers for outsourced services (e.g. operation of accepting devices, communication network facilities, acquiring of transactions) include provisions which:

- *require those service providers to conduct a risk assessment, take appropriate actions and report the results of both to the outsourcer;*
- *give the outsourcer the ability to check, if any through on site visits, the effective implementation of the risk assessment and the related taken actions?*

Applies to: All

Supporting documents: Risk assessment report and contracts

2.2 KC On this basis, PSPs and payment schemes 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. PSPs and payment schemes should take into account the time required to implement the changes (including customer roll-out) and take the appropriate interim measures to minimise security incidents and fraud, as well as potential disruptive effects.

2.2.1 Has the PSP/GA put in place a process for assessing and deriving the necessary changes to existing security measures, the technologies used and the procedures implemented or services offered based on the results of the risk assessment, including any necessary adaptation of the risk assessment methodology itself?

Applies to: All

Supporting documents: Risk assessment and change management policy

2.2.2 Does the assessment of changes lead to a formal implementation plan, including interim measures where necessary, with specific milestones, procedures and contingency measures to facilitate service transition, eliminate the introduction of new vulnerabilities to the services and minimise potential availability incidents?

Applies to: All

Supporting documents: Change management policy and Implementation plan

2.2.3 Has the PSP/GA put in place a process to monitor the implementation of the planned changes that has led to appropriate action being taken?

Applies to: All

Supporting documents: Risk assessment and change management policy

2.3 KC The assessment of risks should address the need to protect and secure sensitive payment data.

2.3.1 Does the PSP have appropriate processes in place to identify sensitive payment data? Does this include operational activities relating to the protection of sensitive payment data and specific controls applying to their management?

Applies to: All

Supporting documents: Risk assessment report

2.3.2 Does the risk assessment address requirements for protecting sensitive payment data (e.g. encryption), as well as the definition and implementation of access policies for sensitive operational activities and the data they involve?

Applies to: All

Supporting documents: Risk assessment report

2.4 KC PSPs and payment schemes should undertake a review of the risk scenarios and existing security measures after major incidents affecting their services, before a major change to the infrastructure or procedures and when new threats are identified through risk monitoring activities. In addition, a general review of the risk assessment 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.

2.4.1 Does the PSP/GA review the risk scenarios, updating the related risk assessment results, after major incidents affecting their services and in the case of major changes to their infrastructures or relevant operational procedures? Has the PSP/GA appropriately defined major incidents and major changes?

Applies to: All

Supporting documents: Risk assessment methodology

2.4.2 Does the PSP/GA, as part of its risk monitoring activities, monitor the developments and trends relevant for the functioning and security of the payment service, especially with regard to technological vulnerabilities and new fraud techniques? Do the new threats, which may have been identified through PSP/GA's risk monitoring activities, trigger the review of risk scenarios, in accordance with 2.4.1?

Applies to: All

Supporting documents: Risk assessment methodology

2.4.3 Does the PSP/GA perform a periodic general review of the risk assessment at least once a year? Is it ensured that the method to generate the risk assessments is standardised and reproducible? Are the results of the risk assessment submitted to senior management for approval?

Applies to: All

Supporting documents: Risk assessment methodology

Recommendation 3: Incident monitoring and reporting

PSPs and payment schemes should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. PSPs and payment schemes should establish a procedure for reporting such incidents to management and, in the event of major payment security incidents, the competent authorities.

3.1 KC PSPs and payment schemes should have a process in place to monitor, handle and follow up on security incidents and security-related customer complaints and report such incidents to the management.

3.1.1 Does the PSP have a procedure in place to monitor, handle and follow up on security incidents?

- *This procedure includes a classification for security incidents according to their criticality.*
- *Do the monitoring procedures have up-to-date information on the status of, for example, the systems, components, operational functions and administrative and technical procedures with regard to physical and information security incidents? Are they able to identify early warnings of possible security incidents by detecting anomalies?*

Applies to: All

Supporting documents: Incident management policy

3.1.2 Does the PSP have a procedure in place to inform the respective scheme's GA about major security incidents?

Applies to: All

Supporting documents: Incident management policy

3.1.3 Does the PSP/GA have a procedure in place to monitor,handle and follow up on security-related customer complaints?

Applies to: All

Supporting documents: Complaints management policy

3.1.4 Does the follow-up on security incidents and security-related customer complaints include a process to evaluate, report to the board and take into account the lessons learnt from the relevant incidents/complaints, incorporating this into the security policies and incident management of the PSP/GA?

Applies to: All

Supporting documents: Incident and complaints management policy

3.2 KC PSPs and payment schemes should have a procedure for notifying immediately the competent authorities (i.e. supervisory, oversight and data protection authorities), where they exist, in the event of major payment security incidents with regard to the payment services provided.

3.2.1 Does the PSP/GA have a procedure in place to immediately notify the competent authorities in the event of major payment security incidents with regard to the payment services provided?

Applies to: All

Supporting documents: Compliance/incident and management policy

3.2.2 Has the PSP/GA defined who is in charge, how information is conveyed in a secure manner and how it is ensured that the respective contacts are up to date?

Applies to: All

Supporting documents: Compliance/incident and management policy

3.3 KC PSPs and payment schemes should have a procedure for cooperating on major payment security incidents, including data breaches, with the relevant law enforcement agencies.

3.3.1 Does the PSP/GA have a procedure in place to cooperate with the relevant law enforcement agencies on major payment security incidents, including data breaches?

Applies to: All

Supporting documents: Incident management policy

3.3.2 Has the PSP/GA defined who is in charge, how information is conveyed in a secure manner and how it is ensured that the respective contacts are up to date?

Applies to: All

Supporting documents: Incident management policy

3.4 KC Acquiring PSPs should contractually require e-merchants that store, process or transmit sensitive payment data to cooperate on major payment security incidents, including data breaches, both with them and the relevant law enforcement agencies. If a PSP becomes aware that an e-merchant is not cooperating as required under the contract, it should take steps to enforce this contractual obligation, or terminate the contract.

3.4.1 Has the acquiring PSP contractually required its e-merchants that store, process or transmit sensitive payment data to cooperate with itself and the relevant law enforcement agencies on major security incidents and all data breaches?

Applies to: PSP

Supporting documents: E-merchant contract

3.4.2 Has the acquiring PSP established a procedure to take steps to enforce the contractual obligation of the e-merchant if the PSP becomes aware that an e-merchant is not cooperating as required under the contract?

Applies to: PSP

Supporting documents: Letters of intent

3.4.3 Has the acquiring PSP included the reason "no cooperation on major payment security incidents" in the termination clauses of the respective e-merchant contracts?

Applies to: PSP

Supporting documents: E-merchant contract

Recommendation 4: Risk control and mitigation

PSPs and payment schemes should implement security measures in line with their respective security policies 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, PSPs and payment schemes 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 privilege" principle [11] as the basis for sound identity and access management.

4.1.1 Has it been ensured that IT environments (e.g. the development, test and production environments) are adequately segregated, both on an organisational and a technical level? With reference to environment segregation, the following non-exhaustive list of issues could be considered:

- rules for the transfer of software from development to operational status should be defined and documented;
- software under development, software under test and operational code should be isolated on different IT environments to respectadequate segregation;
- only executable code should be stored in the production environment; compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required;
- the test system environment should emulate the (live) operational system environment as closely as possible;
- users should use different user profiles for operational and test systems, and menus should display appropriate system identification messages to mitigate the risk of error;
- the transfer of sensitive payment data to the development and test system environment should be avoided or, if necessary, allowed temporarily but subject to specific control measures.

Applies to: All

Supporting documents: Security policy, service operating rules, application specifications, solution architecture specifications and audit reports

4.1.2 Has it been ensured that the identity and access management conform to the "least privilege" principle?

With reference to user privileges, the following non-exhaustive list of issues could be checked:

11 "Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job." See Saltzer, J.H. (1974), "Protection and the Control of Information Sharing in Multics", *Communications of the ACM,* Vol. 17, No 7, pp. 388.

- the access privileges (including administrator, super user/root, dba, etc.) associated with each system product (e.g. operating system, database management system and each application) and the users to which they need to be allocated should be identified and reviewed on a regular basis;
- privileges should be allocated to users on a need-to-use basis and, whenever feasible, on an event-by-event basis in line with the access control policy, i.e. the minimum requirement for their functional role only when needed;
- an authorisation process and a record of all privileges allocated should be maintained, with privileges not being granted until the authorisation process is complete;
- an effective recertification process for assessing and, if necessary, revoking privileges should be in place and carried out at regular intervals;
- the development and use of system routines should be promoted to avoid the need to grant generalised privileges to users;
- administrative privileges should be assigned to users through a different user ID from that used for normal business use;
- the scope and complexity of processes, architecture and infrastructure may necessitate role-based access control or at least equivalently strong access control models.

Applies to: All

Supporting documents: Security policy, service operating rules, application specifications, solution architecture specifications and audit reports

4.2 KC PSPs and payment schemes should have appropriate security solutions in place to protect networks, websites, servers and communication links against abuse or attacks. PSPs and payment schemes should strip the servers of all superfluous functions in order to protect (harden) them and eliminate or reduce 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 privilege" 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 [12] drawn up in the PSP's name or by other similar authentication methods.

4.2.1 Does the PSP/GA have appropriate security solutions in place to protect networks, websites, servers and communication links against abuse or attacks? Below is a non-exhaustive list of possible controls that could be checked:

- *Does the PSP/GA have an effective patch management process in place that ensures that systems are at a sufficiently late patch state?*
- *Do all critical systems have, as required, the most recently released, appropriate software patches to protect against exploitation and sensitive data being compromised by malicious individuals and malicious software?*
- *Has the PSP/GA set up the firewalls with appropriate rules to allow only legitimate connections?*

12 An Extended Validation Certificate (EV) is an X.509 public key certificate issued according to a specific set of identity verification criteria. These criteria require extensive verification of the requesting entity's identity by the certificate authority (CA) before a certificate is issued (wikipedia).

- *Has the PSP/GA taken measures to prevent or mitigate (distributed) denial of service attacks?*
- *Does the PSP/GA use intrusion detection and prevention systems to signal and avert attacks identified by a heuristic analysis or by a known pre-set pattern?*
- *Does the PSP/GA use tamperproof communication channels and secure authentication methods (such as VPN) to manage the servers?*
- *Has the PSP/GA enabled full session encryption?*
- *Does the PSP/GA have controls in place to ensure the quality of the software architecture of relevant applications?*
- *Does the PSP/GA have a policy in place regarding secure application-developing techniques?*
- *Has the PSP/GA ensured that relevant source codes were subject to code review by independent reviewers before releases and changes went into production in order to minimise software vulnerabilities, backdoors and manipulation?*
- *Does the PSP/GA have controls in place to ensure that any applications and IT systems are appropriately documented?*
- *Has the PSP/GA ensured that software releases and changes were subject to appropriate tests by testers other than the developers before going into production?*
- *Has the PSP/GA set up an effective change management process?*
- *Does the PSP/GA regularly perform vulnerability scans?*
- *Does the PSP/GA perform penetration tests run by certified auditors?*

Applies to: All

Supporting documents: Security policy, service operating rules, application specifications, solution architecture specifications and audit reports

4.2.2 Has the PSP/GA stripped the servers of all superfluous functions and unused services (hardening)? The PSP could consider:

- *industry-accepted system-hardening standards (e.g. CICS, ISP, SANS, NIST, etc.);*
- *changing user ID and credentials defaults (e.g. administrators' passwords) before installing a product;*
- *enabling only necessary services and protocols;*
- *removing all unnecessary functionality, such as scripts, drivers, features, subsystems and file systems, as well as unnecessary server applications.*

Applies to: All

Supporting documents: Security policy, solution architecture specifications and audit reports

4.2.3 Does the PSP/GA ensure secure communication according to current best practices, including the use of extended validation certificates (e.g. key length, TLS version, encryption cipher, etc.) configured for the PSP's name, or does the PSP use other similar authentication methods?

Applies to: All

Supporting documents: Security policy and Extended validation certificate (or comparable)

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

4.3.1 Does the PSP/GA have appropriate processes in place to monitor, track and restrict logical and physical access to sensitive payment data and critical resources? Has it been ensured that access is only given to authorised users and programs?

Applies to: All

Supporting documents: Security policy and application specifications

4.3.2 Does the PSP/GA create, store and analyse appropriate logs and audit trails?

- The PSP/GA's applications are capable of providing audit trails, including log-in, error and warning messages as well as other information messages in log files.
- The PSP/GA ensures that the timestamps included in log files and audit trails remain accurate, e.g. by regularly synchronising its servers with one or more trusted time sources (such as time server or GPS).
- The PSP/GA regularly analyses log files and audit trails and takes correctional and/or preventive measures.

Applies to: All

Supporting documents: Application specifications and audit reports

4.4 KC In designing,[13] developing and maintaining internet payment services, PSPs should ensure that data minimisation[14] is an essential component of the core functionality: the gathering, routing, processing, storing and/or archiving, and visualisation of sensitive payment data should be kept at the absolute minimum level.

4.4.1 Has the PSP performed an analysis of the types of personal information required for the operation of the payment service and defined the minimum level of information required?

Applies to: PSP

Supporting documents: Risk assessment report

13 Privacy by design.
14 Data minimisation refers to the policy of gathering the least amount of personal information necessary to perform a given function.

4.4.2 Does the PSP ensure that data minimisation is an essential component of the core functionality during the design, development and maintenance phases? *(For example, the PSP describes the protection measures put in place, as well as outlining both automated and manual controls that ensure data minimisation is adhered to in the design, development and maintenance phase so that the gathering, routing, processing, storing and/or archiving, and visualisation of sensitive payment data achieved through the application is minimised.)*

Applies to: PSP

Supporting documents: Security policy, application specifications, design and development methodology documentation

4.5 KC Security measures for internet payment services should be tested under the supervision of the risk management function to ensure their robustness and effectiveness. All changes should be subject to a formal change management process ensuring that changes are properly planned, tested, documented and authorised. 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.

4.5.1 Does the PSP/GA test security measures for internet payment services under the supervision of the function responsible for risk management?

Applies to: All

Supporting documents: Security policy and risk management function approval document

4.5.2 Does the PSP/GA ensure that all changes are subject to a formal change management process for planning, testing, documenting and authorising changes?

Applies to: All

Supporting documents: Change request document and plan

4.5.3 Does the PSP/GA conduct regular tests against relevant and known potential attacks to ensure that changes are implemented correctly and that possible vulnerabilities to any security threats observed are identified?

Applies to: All

Supporting documents: Security policy, test scenarios and test reports.

4.6 KC Security measures of PSPs and GAs for internet payment services should be periodically audited to ensure their robustness and effectiveness. The implementation and functioning of the internet payment 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 (internal or external) 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.

4.6.1 Are the implementation and functioning of the internet payment services, as well as the PSP/GA's security measures, periodically audited in order to ensure their robustness and effectiveness? (The audit at the initial implementation is considered a one-off audit, and further functional audits should be performed for major changes.)

Applies to: All

Supporting documents: Audit management policy, audit report and auditor certification

4.6.2 Does the PSP take into consideration the security risks involved to determine the frequency and focus of the audits in proportion to the security risks?

Applies to: All

Supporting documents: Audit management policy

4.6.3 Does the PSP/GA ensure that the auditors are trusted and independent experts (i.e. not in any way involved in the development, implementation or operational management of its internet payment services)?

Applies to: All

Supporting documents: Audit management policy

4.6.4 Does the PSP/GA have procedures in place to report the results of such audits to the board?

Applies to: All

Supporting documents: Report to the board/audit committee

4.6.5 Has the PSP/GA defined the concept of "major change" (as used in 4.6.1)?

Applies to: All

Supporting documents: Audit management policy

4.7 KC Whenever PSPs and payment schemes outsource 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.

4.7.1 Does the PSP/GA contractually require outsourcing companies to comply with the principles and recommendations set out in the "Recommendations for the security of internet payments" whenever functions related to the security of internet payment services are outsourced?

Applies to: All

Supporting documents: Security policy and outsourced contracts

4.8 KC PSPs offering acquiring services should contractually require e-merchants handling (i.e. storing, processing or transmitting) sensitive payment data to implement security measures in their IT infrastructure, in line with KCs 4.1 to 4.7, in order to avoid the theft of those sensitive payment data through their systems. If a PSP becomes aware that an e-merchant does not have the required security measures in place, it should take steps to enforce this contractual obligation, or terminate the contract.

4.8.1 When offering acquiring services, does the PSP contractually require those e-merchants who handle sensitive payment data to implement security measures in their IT infrastructure, in line with KCs 4.1-4.7?

Applies to: PSP

Supporting documents: E-merchant contracts

4.8.2 Has the PSP set up a procedure to monitor compliance with this contractual obligation, detailing the steps to take in case any breaches are detected, up to the termination of the e-merchant contract?

Applies to: PSP

Supporting documents: Policy document

4.1 BP PSPs could provide security tools (e.g. devices and/or customised browsers, properly secured) to protect the customer interface against unlawful use or attacks (e.g. "man in the browser" attacks).

4.1.1 BP Does the PSP provide security tools to protect the customer interface against unlawful use or attacks (e.g. secure interface provided by custom software running from a secured USB device[15], dedicated security software for screening the customer's PC)?

Applies to: PSP

Supporting documents: Security policy

15 E.g. portable "secure browser", available on a USB key and running outside the normal PC operating system.

Recommendation 5: Traceability

PSPs should have processes in place ensuring that all transactions, as well as the e-mandate process flow, are appropriately traced.

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

5.1.1 Does the PSP/GA ensure that its service incorporates security mechanisms for the detailed logging of transaction and e-mandate data?

Applies to: All

Supporting documents: Security policy

5.1.2 Do the transaction and e-mandate logs contain the correct transaction sequential numbers and timestamps?

Applies to: All

Supporting documents: Application specifications

5.1.3 Are parameterisation changes, access and attempts to access transaction and e-mandate data accurately logged?

Applies to: All

Supporting documents: Application specifications

5.1.4 Does the PSP/GA ensure that log files are tamperproof and can only be accessed by authorised personnel or applications?

Applies to: All

Supporting documents: Application specifications, security testing report and audit report

5.1.5 Does the PSP/GA ensure that log files are stored for an adequate time frame, in line with local regulation?

Applies to: All

Supporting documents: Security policy

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

5.2.1 Has the PSP/GA set up a file-logging application allowing any addition, change or deletion of transaction and e-mandate data to be traced?

Applies to: All

Supporting documents: Application specifications

5.3 KC PSPs should query and analyse the transaction and e-mandate data and ensure that they have tools to evaluate the log files. The respective applications should only be available to authorised personnel.

5.3.1 Does the PSP have software tools and processes to evaluate the log files?

Applies to: All

Supporting documents: Security policy

5.3.2 Does the PSP have an access control policy in place that allows only authorised personnel to have access to the log file evaluation tools and to be able to parameterise them?

Applies to: All

Supporting documents: Security policy

5.3.3 Does the PSP periodically query and analyse the logged transaction and e-mandate data for inconsistencies, signs of tampering and unauthorised access?

Applies to: All

Supporting documents: Security policy

5.3.4 Are there other events, besides the regular check, that trigger queries and analysis of operations?

Applies to: All

Supporting documents: Security policy

5.1 BP PSPs offering acquiring services could contractually require e-merchants who store payment information to have adequate processes in place supporting traceability.

5.1.1 BP When offering acquiring services, does the PSP contractually require e-merchants who store payment information to have adequate processes in place to support traceability and to report respective issues to the PSP/GA (all the KCs listed above)?

Applies to: PSP

Supporting documents: E-merchant contracts

SPECIFIC CONTROL AND SECURITY MEASURES FOR INTERNET PAYMENTS

Recommendation 6: Initial customer identification, information

Customers should be properly identified in line with the European anti-money laundering legislation[16] and confirm their willingness to make internet payments using the services before being granted access to such services. PSPs should provide adequate "prior", "regular" or, where applicable, "ad hoc" 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 customer due diligence procedures, and has provided adequate identity documents[17] and related information before being granted access to the internet payment services.[18]

6.1.1 Where there are official guidelines and legal requirements on remote identification, does the PSP comply with them?

Applies to: PSP

Supporting documents: Security policy

6.1.2 Does the PSP use an appropriate identification concept for internet payments?

- If the customer is not identified in a face-to-face environment, is the customer's information checked with, and confirmed by, reliable third party information (which could, depending on the respective national legislation, be telephone or electricity bills or identification by third parties) or information gathered on the basis of a bank transfer of a small amount of money?

16 For example, Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. OJ L 309, 25.11.2005, p. 15-36. See also Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis. OJ L 214, 4.8.2006, p. 29-34.

17 For example, passport, national identity card or advanced electronic signature.

18 The customer identification process is without prejudice to any exemptions provided in existing anti-money laundering legislation. PSPs need not conduct a separate customer identification process for the internet payment services, provided that such customer identification has already been carried out, e.g. for other existing payment-related services or for the opening of an account.

- Are the PSP's procedures on customer due diligence reviewed periodically by an internal/external auditor and reported to the board and the competent authority?

Applies to: PSP

Supporting documents: Security policy

6.1.3 Does the identification process take place prior to granting the customer access to the internet payment services?

Applies to: PSP

Supporting documents: Security policy

6.2 KC PSPs should ensure that the prior information[19] 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 transaction and/or obtain information, 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.

6.2.1 Is the PSP supplying its customer with the prior information in accordance with the points mentioned above?[20]

Applies to: PSP

Supporting documents: Contract/terms of service

19 This information complements Article 42 of the Payment Services Directive which specifies the information that the PSP must provide to the payment service user before entering into a contract for the provision of payment services.
20 Potentially subject to changes taking into account the revised Payment Services Directive, once endorsed.

6.2.2 If the completeness and validity (over time) of the information furnished to customers by PSPs has to be certified by a competent authority, does the PSP comply with this requirement?

Applies to: PSP

Supporting documents: Policy

6.2.3 Does the PSP require customers to formally acknowledge the receipt of this information?

Applies to: PSP

Supporting documents: Contract/terms of service

6.3 KC PSPs should ensure that the framework contract with the customer specifies that the PSP may block a specific transaction or the payment instrument[21] 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 internet payment transaction or service "unblocked", in line with the Payment Services Directive.

6.3.1 Does the framework contract between the PSP and the customer include clauses related to internet payments and, in particular:

- the possibility for the PSP to block specific transactions or the payment instruments on the basis of predefined security concerns;
- methods and terms of the customer notification by the PSP about the blocking;
- the communication modalities between the customer and the PSP for solving the blocking case?

Applies to: PSP

Supporting documents: Framework contract

6.3.2 Is the blocking of transactions supported by well – defined criteria (e.g. risk matrix, taking into account the risk and general profile of a customer and the amounts involved in a particular transaction or the customer's payment behaviour)?

Applies to: PSP

Supporting documents: Security policy and risk assessment report

21 See Article 55 of the Payment Services Directive on limits of the use of the payment instrument.

6.3.3 Does the procedure for unblocking transactions respect the prescriptions of the PSD and inform the customer on costs and contributions as well as on eventual claims reserved to customers in case of an inappropriately blocked transaction?

Applies to: PSP

Supporting documents: Contract/terms of service

6.4 KC PSPs should also ensure that customers are provided, on an ongoing or, where applicable, ad hoc 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.

6.4.1 Does the PSP give the customer clear instructions on their responsibilities with regard to the secure use of the service? Is this done via appropriate communication channels and at an acceptable frequency?

Applies to: PSP

Supporting documents: Contract/terms of service policy

6.4.2 If the instructions have to be validated beforehand by a competent authority, does the PSP comply with this requirement?

Applies to: PSP

Supporting documents: Policy

6.1 BP The customer could sign a dedicated service contract for conducting internet payment transactions, rather than the terms being included in a broader general service contract with the PSP.

6.1.1 BP Does the PSP offer a dedicated service contract for conducting internet payment transactions or are the internet payment modalities included in the general framework contract?

Applies to: PSP

Supporting documents: Contract

6.1.2 BP If these dedicated service contracts have to be validated beforehand by a competent authority, does the PSP comply with this requirement?

Applies to: PSP

Supporting documents: Policy

Recommendation 7: Strong customer authentication

The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication.

Clarification on the strong customer authentication procedure.

7.0.1 Does the authentication procedure make use of two or more elements to prove the authenticity of the user?

- The authentication procedure requires the use of at least two elements.
- These elements are chosen from at least two of the defined categories (i.e. knowledge and ownership is allowed; ownership and ownership is not allowed).

Applies to: PSP

Supporting documents: Technical specifications

7.0.2 For ownership and inherence elements:

Did independent and competent third parties certify or evaluate that the level of security for these devices is sound and that they are tamper-resistant?

- The devices have been certified by certification authorities on the basis of acknowledged standards or methodologies, or they have at least been evaluated (e.g. security report) by, for example, laboratories, university experts or technical consultants.
- The resistance is verified on the basis of penetration tests and vulnerability assessments.

Applies to: PSP

Supporting documents: Certification/evaluation report

7.0.3 Have the security features of the solution been properly defined and implemented (e.g. algorithm specs, key length, information entropy[22])?

- The security features follow publicly available and recognised standards.
- For one-time passwords (OTPs): Is the password value generated using secure devices and procedures based on publicly available and recognised standards? The procedures generate sufficiently complex passwords; the knowledge of one password value does not assist in deriving subsequent values.

Applies to: PSP

Supporting documents: Technical specifications

22 In this context the term "entropy" means: *a measure of the amount of uncertainty that an attacker faces to determine the value of a secret.* This concept has been used in the context of information theory and cryptography as a measure of the difficulty in guessing or determining a password or a key.

7.0.4 If a multi-purpose device (e.g. mobile phone or tablet) is used as the ownership element (e.g. to receive or generate a one-time password or initiate a drop call mechanism), does the PSP apply measures to mitigate the risk of it being used to initiate a fraudulent internet payment at the same time (e.g. via viruses/internet attacks)?

- Do the security features follow recommendations contained in publicly available and recognised standards?
- Is the payment itself initiated via a separate/independent channel?

Applies to: PSP

Supporting documents: Technical specifications

7.0.5 Are the secrets used for the knowledge element based on an appropriate security policy?

- Is there a password policy (information entropy, complexity, length, expiration time, number of characters that cannot be repeated, not guessable)? If so, is it enforced?
- If a non-password-based procedure is adopted, is it ensured that the likelihood of a false positive is comparable or less than the case of a (sound) password?

Applies to: PSP

Supporting documents: Security policy, certification/evaluation report

7.0.6 Are the procedure and the chosen elements designed to ensure independence, e.g. in terms of the technology used, algorithms and parameters?

- The breach of one authentication element leaves the protection offered by the other elements unaffected (e.g. in the case of knowledge + ownership, the theft/misappropriation of one element leaves the effort necessary for the attacker to breach/bypass the other unchanged).
- Alternatively, in the case of co-dependence (e.g. where a PIN is used to initiate the generation of an OTP for a device) the risks are appropriately mitigated, taking the following into consideration:

a) specific security measures to avoid PIN guessing or retrieval from the device;
b) anti-cloning features of the device (e.g. smart card, token, SIM);
c) particularly strong security features of the OTP generated (length, information entropy, random algorithms).

Applies to: PSP

Supporting documents: Security policy, certification/evaluation report

7.0.7 Does the strong customer authentication procedure operate in such a way that:

- the customer has to input all the credentials before receiving a positive or negative result;
- in cases of denied authentication, no information is given about which was the incorrect piece of data input (user ID, first element, second elements etc.)?

Applies to: PSP

Supporting documents: Technical specifications

7.0.8 Does at least one of the selected elements fall into the inherence category or is it/are they non-reusable and non-replicable?

- Authentication codes are not replicable, since authenticator values[23] are accepted only once by the authentication system, allowing the user to perform only a specific operation.
- It is not feasible to forge/clone an exploitable copy of the element (except for inherence), even having the element in availability, and it is also not feasible to steal related confidential information (e.g. cryptographic keys, sensitive software or private keys for digital signatures) via the internet, including when not performing a payment-related transaction (e.g. via malware or advanced persistent threats – APTs).

Applies to: PSP

Supporting documents: Technical specifications

7.0.9 Is the confidentiality of the authentication value protected from the moment it is generated to its verification by the authentication server?

Applies to: PSP

Supporting documents: Technical specifications

7.0.10 Has the security of the whole strong authentication procedure been evaluated (e.g. via a penetration test) and is it subject to regular re-evaluations?

Applies to: PSP

Supporting documents: Certifications/evaluation report and risk management policy

23 The authentication element (e.g. knowledge, ownership, inherence) produces a data string (e.g. password, OTP, biometric value) that is sent remotely to the authentication server, during the payment initiation phase. This data string, the "authenticator value", is transmitted via a protocol, to the authentication server as a proof the user possesses and controls the "authentication element" and, consequently, as a proof of the user's identity.

7.1 KC [CT/e-mandate/e-money] PSPs should perform strong customer authentication for the customer's authorisation of internet payment transactions (including bundled CTs) and the issuance or amendment of electronic direct debit mandates. However, PSPs could consider adopting alternative customer authentication measures for:

– outgoing payments to trusted beneficiaries included in previously established white lists for that customer;

– transactions between two accounts of the same customer held at the same PSP;

– transfers within the same PSP justified by a transaction risk analysis;

– low-value payments, as referred to in the Payment Services Directive[24].

7.1.1 Has the PSP implemented the use of strong customer authentication for the customer's authorisation of internet payment transactions?

- This includes the initiation of credit transfers (single or bundled), the initiation of e-money transfers and the issuance/amendment of electronic mandates.
- Each initiation of single or bundled transactions (single or bundled payment orders) requires strong customer authentication.

Applies to: PSP [CT/e-mandate/e-money]

Supporting documents: Security policy

7.1.2a If the PSP is using one or more of the listed exemptions, has a security evaluation of the alternative authentication measures chosen been performed and documented with respect to the risk of the related payments?

Applies to: PSP [CT/e-mandate/e-money]

Supporting documents: Risk assessment report (analysis for each service offered to customers)

7.1.2b Does the PSP require strong customer authentication for establishing and/or modifying the white list by the customer via the internet?

Applies to: PSP [CT/e-mandate/e-money]

Supporting documents: Security policy

7.1.2c If transfers occur within the same PSP, is a transaction risk analysis used to identify low-risk payments against predefined categories and therefore justifying the use of alternative authentication measures? (If the same customer has two accounts at the same PSP, the PSP is not required to conduct a transaction risk analysis on top of an alternative customer authentication.)

24 See the definition of low-value payment instruments in Articles 34(1) and 53(1) of the Payment Services Directive.

Applies to: PSP [CT/e-mandate/e-money]

Supporting documents: Risk assessment report and security policy

7.1.2d In cases of successive low value payments[25], has the PSP defined a limit for the total amount of payments and the number of transactions without strong customer authentication?

Applies to: PSP [CT/e-mandate/e-money]

Supporting documents: Risk assessment report and security policy

7.1.3 If no PSP is involved in the issuance or amendment of electronic direct debit mandates, the creditor's PSP could encourage merchants to implement a procedure using strong customer authentication.

Applies to: PSP [CT/e-mandate/e-money]

Supporting documents: Creditor PSP's contract with the merchant

7.2 KC Obtaining access to or amending sensitive payment data (including the creation and amending of white lists) requires strong customer 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 assessment.

7.2.1 Has the PSP identified all sensitive data accessible to its customers online (e.g. through its e-banking website(s))? Are access and/or amendment to those data protected with strong customer authentication? Does the risk assessment consider each service offered to customers?

Applies to: PSP

Supporting documents: Risk assessment report

7.2.2 In the case of consultative services with no display of sensitive customer or payment information and where alternative authentication measures are adopted, is there a risk analysis attached to those services so as to justify the adoption and adequacy of such authentication solutions? Does the risk assessment consider each service offered to customers?

Applies to: PSP

Supporting documents: Risk assessment report

25 In line with the definition of the PSD.

7.3 KC [cards] For card transactions, all card issuing PSPs should support strong authentication of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication.

7.3.1 Has the card-issuing PSP implemented strong customer authentication for all its cards that are meant to be used on the internet? Are there known exceptions (e.g. corporate cards) and do they benefit from a risk analysis and proper monitoring if there are any issues?

Applies to: PSP [cards]

Supporting documents: Risk assessment report and security policy

7.3.2 Are all cards (that are issued, activated and internet-enabled) registered within the PSP's IT system that is to be used with strong customer authentication?

Applies to: PSP [cards]

Supporting documents: Risk assessment report, security policy and application/technical specifications

7.3.3 Does the GA require the card-issuing PSPs to strongly authenticate the customer on request of an acquiring PSP or wallet provider?

Applies to: PSP [cards]

Supporting documents: Policy

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

7.4.1 Has the acquiring PSP, for all card schemes it supports, implemented strong customer authentication in its IT systems and protocols used to communicate with the issuers?

Applies to: PSP [cards]

Supporting documents: Risk assessment report and security policy

7.4.2 Have those implementations been audited or do they benefit from a quality/security review?

Applies to: PSP [cards]

Supporting documents: Audit report/security review

7.5 KC [cards] PSPs offering acquiring services should require their e-merchant to support solutions allowing the issuer to perform strong authentication of the cardholder for card transactions via the internet. The use of alternative authentication measures could be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments, as referred to in the Payment Services Directive.

7.5.1 Has the acquiring PSP required its e-merchants to support strong customer authentication by the issuer for card not present (CNP) transactions over the internet?

- Does the PSP check whether the merchant is complying with this requirement?

Applies to: PSP [cards]

Supporting documents: E-merchant contract and audit report

7.5.2 Is the acquiring PSP able to precisely monitor its e-merchant base when it comes to strong customer authentication implementations? For example:

- *does the PSP maintain a list of its e-merchants having effective strong customer authentication solutions in place;*
- *can the PSP track transactions together with the method of authentication used (e.g. strong/alternative)?*

Applies to: PSP [cards]

Supporting documents: E-merchant contract, e-merchants register and fraud monitoring reports

7.5.3 When the PSP allows alternative authentication measures to be used by e-merchants:

- *is this exemption made for low-value payments in accordance with the PSD, or does the acquirer require the e-merchant to perform a risk analysis to pre-identify categories of lowrisk transactions, taking into account the nature of the products/services sold (e.g. physical vs. digital goods and services), the delivery channel, customer behaviour, the fraud monitoring skills of the e-merchant, etc., and is a transaction risk analysis conducted against those categories;*

- *are those conditions set out in the contractual framework provided by the GA or contracts concluded between the actors concerned (acquiring PSP, e-merchant)?*

Applies to: All [cards]

Supporting documents: Risk assessment report, security policy and e-merchant contract

7.6 KC All payment schemes should promote the implementation of strong customer authentication by introducing a liability regime[26] for the participating PSPs in and across all European markets

7.6.1 Has the GA implemented a liability shift in the payment scheme towards the PSP failing to support strong customer authentication for payments over the internet (i.e. when initiating a credit transfer, e-money transaction or card payment, or when generating a direct debit e-mandate)?

Applies to: GA

Supporting documents: Scheme membership contracts and scheme rules

7.6.2 Is the liability regime transparent, clear and enforceable, and does it include a dispute resolution mechanism?

Applies to: GA

Supporting documents: Scheme membership contracts and scheme rules

7.7 KC [cards] For the card payment schemes accepted by the service, providers of wallet solutions should require strong authentication by the issuer when the legitimate holder first registers the card data.

7.7.1 When the legitimate holder first registers card data or at least when the first transaction with the card is initiated, do PSPs provide wallet solutions requiring strong customer authentication by the issuer?

Applies to: PSP/ Wallet provider and [cards]

Supporting documents: Security policy/customer registration process documentation

7.8 KC Providers of wallet solutions should support strong customer authentication when customers log in to the wallet payment services or carry out card transactions via the internet. The use of alternative authentication measures could be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments, as referred to in the Payment Services Directive.

7.8.1 Does the wallet provider support strong customer authentication in (at least) one of the following cases: i) for the log-in to the wallet service; ii) when initiating a card payment over the internet?

Applies to: PSP

Supporting documents: Security policy/customer payment process documentation

26 The liability regime should provide that a PSP must refund other PSPs for any fraud resulting from weak customer authentication.

7.8.2 When the PSP providing wallet solutions allows for alternative authentication measures to be used by e-merchants:

- *is this exemption made for low-value payments in accordance with the PSD, or has the wallet provider performed a risk analysis to pre-identify categories of low-risk transactions, taking into account the nature of the products/services sold (e.g. physical vs. digital goods and services), the delivery channel, customer behaviour, the fraud monitoring skills of the e-merchant, etc., and is a transaction risk analysis conducted against those categories;*

- *are those conditions set out in the contractual framework provided by the GA or contracts closed between the actors concerned (wallet provider, e-merchant)?*

Applies to: PSP

Supporting documents: Risk assessment report, security policy and e-merchant contract

7.9 KC [cards] For virtual cards, the initial registration should take place in a safe and trusted environment[27]. Strong customer authentication should be required for the virtual card data generation process if the card is issued in the internet environment.

7.9.1 In the case of the implementation of virtual cards, does the initial registration take place in a safe and trusted environment as per the definition provided?

Applies to: PSP [cards]

Supporting documents: Security policy/customer registration process, supporting documents

7.9.2 Is strong customer authentication required when generating virtual card data over the internet?

Applies to: PSP [cards]

Supporting documents: Application specifications

7.10 KC PSPs should ensure proper bilateral authentication when communicating with e-merchants for the purpose of initiating internet payments and accessing sensitive payment data.

7.10.1 Is bilateral (mutual) authentication enforced by the PSP when communicating with e-merchants for the purpose of initiating internet payments and accessing sensitive payment data, e.g. through the use of secure protocols (such as TLS), allowing mutual authentication in accordance with current best practices (such as key length, TLS version, encryption cipher, etc.)?

27 Environments under the PSP's responsibility where adequate authentication of the customer and of the PSP offering the service and the protection of confidential/sensitive information is assured include: i) the PSP's premises; ii) internet banking or other secure website, e.g. where the GA offers comparable security features inter alia as defined in Recommendation 4; or iii) automated teller machine (ATM) services. (In the case of ATMs, strong customer authentication is required. Such authentication is typically provided by chip and PIN, or chip and biometrics.)

Applies to: PSP

Supporting documents: PSP and e-merchant contract and Technical specifications

7.1 BP E-merchants could support strong authentication of the cardholder by the issuer in card transactions via the internet.

7.1.1 BP Already covered under 7.5.1 of the KCs

Applies to: E-merchants [cards]

Supporting documents: E-merchant contract

7.2 BP For customer convenience purposes, PSPs could consider using a single strong customer authentication tool for all internet payment services. This could increase acceptance of the solution among customers and facilitate proper use.

7.2.1 BP Does the PSP offer the same strong customer authentication solution to all its customers and across all internet payment services, including ebanking payment services and card payments over the internet, for example?

Applies to: PSP

Supporting documents: Security policy and technical specifications

7.2.2 BP Has the PSP defined fallback solutions covering the risk of a single point of compromise (regarding the SCA tool)?

Applies to: PSP

Supporting documents: Security policy and technical specifications

7.3 BP Strong customer authentication could include elements linking the authentication to a specific amount and payee. This could provide customers with increased certainty when authorising payments. The technology solution enabling the strong authentication data and transaction data to be linked should be tamper resistant.

7.3.1 BP Does the PSP provide strong customer authentication solutions for which one (or more) of the selected elements entails transaction data signing (specifying the amount and the payee, as well as the time stamp, and ensuring that the transaction cannot be altered)?

Applies to: PSP

Supporting documents: Security policy and technical specifications

7.3.2 BP Have the solutions chosen been audited/reviewed, including for tamper resistance?

Applies to: PSP

Supporting documents: Certification/evaluation report

Recommendation 8: Enrolment for and provision of authentication tools and/or software delivered to the customer

PSPs should ensure that customer enrolment for and the initial provision of the authentication tools required to use the internet payment service and/or the delivery of payment-related software to customers is carried out in a secure manner.

8.1 KC Enrolment for and provision of authentication tools and/or payment-related software delivered to the customer should fulfil the following requirements.

– The related procedures should be carried out in a safe and trusted environment while taking into account possible risks arising from devices that are not under the PSP's control.

– Effective and secure procedures should be in place for the delivery of personalised security credentials, payment-related software and all internet payment-related personalised devices. Software delivered via the internet should also be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with.

– [cards] For card transactions, the customer should have the option to register for strong authentication independently of a specific internet purchase. Where activation during online shopping is offered, this should be done by re-directing the customer to a safe and trusted environment.

8.1.1 Has the PSP implemented a procedure ensuring that the enrolment for and provision of authentication tools and/or payment-related software delivered to the customer takes place in a safe and trusted environment[27]?

Applies to: PSP

Supporting documents: Security policy and technical specifications

8.1.2 Has the PSP taken into account possible risks related to the authentication tools provided and/or software delivered to the customer arising from the devices that are not under the PSP's control?

Applies to: PSP

Supporting documents: Risk assessment report and technical specifications

8.1.3 Does the PSP have effective and secure procedures in place for the delivery of personalised security credentials (e.g. separate delivery of devices and credentials, separate delivery channels)?

Applies to: PSP

Supporting documents: Security policy

8.1.4 Does the PSP have effective and secure procedures in place for the delivery of personalised paymentrelated software?

Applies to: PSP

Supporting documents: Security policy

8.1.5 Does the PSP have effective and secure procedures in place for the delivery of all internet paymentrelated personalised devices?

Applies to: PSP

Supporting documents: Security policy

8.1.6 Does the PSP have a procedure in place to monitor the number of incidents related to the provision of authentication tools and the delivery of software?

Applies to: PSP

Supporting documents: Incident management policy

8.1.7 If software is delivered via the internet, is it ensured that it is digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with?

Applies to: PSP

Supporting documents: Security policy

8.1.8 Does the PSP outline in its contracts or policies that the customer (for card transactions) has the option to register for strong authentication irrespective of a specific internet purchase?

Applies to: PSP [cards]

Supporting documents: Security policy and customer contract

8.1.9 If the PSP offers the activation of strong customer authentication during online shopping, is this done by redirecting the customer to a safe and trusted environment?

Applies to: PSP [cards]

Supporting documents: Technical specifications

8.2 KC [cards] Issuers should actively encourage cardholder enrolment for strong authentication and allow their cardholders to bypass enrolment only in an exceptional and limited number of cases where justified by the risk related to the specific card transaction.

8.2.1 Do issuers actively encourage cardholder enrolment for strong authentication?

Applies to: PSP [cards]

Supporting documents: Customer information material and customer contract

8.2.2 Has the PSP clearly defined, on the basis of a risk analysis, the exceptional and limited number of cases for allowing the enrolment for strong authentication to be bypassed?

Applies to: PSP [cards]

Supporting documents: Risk assessment report

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

PSPs should limit the number of log-in or authentication attempts, define rules for internet payment services 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.

9.1.1 Has the PSP defined a validity period for the OTP in line with the risk analysis? If so, does it result in a limited lifetime?

- The defined validity period results in a limited lifetime that is appropriate for the prevention of attacks (e.g. in some cases, a validity period less than 120 seconds might be appropriate).

Applies to: PSP

Supporting documents: Risk assessment, security policy and technical specifications

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

9.2.2 Has the PSP set down a maximum number of failed log-in or authentication attempts (retry limits) in line with the risk analysis (see recommendation 2), after which access to the internet payment service is (temporarily or permanently) blocked?

Applies to: PSP

Supporting documents: Risk assessment report, security policy and technical specifications

9.2.3 Has the PSP defined specific procedures in order to be able to block (temporarily or permanently) the internet payment service in the event of retry limits being exhausted? Is the customer informed about retry limits and of the procedure to follow to reactivate the internet payment services? Are they promptly served with clear notice of the service being blocked and informed of the procedures to follow to reactivate the internet payment services?

Applies to: PSP

Supporting documents: Security policy and technical specifications

9.2.4 Has the PSP defined specific secure procedures to reactivate blocked internet payment services?

Applies to: PSP

Supporting documents: Security policy

9.2.5 Has the PSP implemented a mechanism to prevent double log-in?

Applies to: PSP

Supporting documents: Security policy

9.3 KC PSPs should set down the maximum period after which inactive internet payment services sessions are automatically terminated.

9.3.1 Has the PSP defined the maximum period after which inactive internet payment service sessions are automatically terminated (i.e. closing both application and network sessions after a defined period of inactivity) in line with the risk analysis (recommendation 2)?

Applies to: PSP

Supporting documents: Risk assessment report and security policy

Recommendation 10: Transaction monitoring

Transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions should be operated before the PSP's final authorisation; suspicious or high risk transactions should be subject to a specific screening and evaluation procedure. Equivalent security monitoring and authorisation mechanisms should also be in place for the issuance of e-mandates.

10.1 KC PSPs should use fraud detection and prevention systems to identify suspicious transactions before the PSP finally authorises transactions or e-mandates. Such systems should be based, for example, on parameterised rules (such as black lists of compromised or stolen card data), and monitor abnormal behaviour patterns of the customer or the customer's access device (such as a change of Internet Protocol (IP) address[28] or IP range during the internet payment services session, sometimes identified by geolocation IP checks,[29] atypical e-merchant categories for a specific customer or abnormal transaction data, etc.). Such systems should also be able to detect signs of malware infection in the session (e.g. via script versus human validation) and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions, while complying with the relevant data protection legislation, should be commensurate with the outcome of the risk assessment.

10.1.1 Does the PSP/GA have fraud detection and prevention solutions in place for identifying suspicious transactions before they are finally authorised?

Applies to: All

Supporting documents: Security policy and technical specifications

10.1.2 If the monitoring is based on parameterised rules (such as black lists of compromised or stolen card data), are they sufficiently defined and updated on a regular basis?

Applies to: All

Supporting documents: Technical specifications

10.1.3 Do the fraud detection and prevention solutions used by the PSP/GA identify abnormal behaviour patterns of the customer (such as the IP or IP range changing during the internet session)?

Applies to: All

Supporting documents: Technical specifications

10.1.4 Are geolocation and/or e-merchant category types used/screened when monitoring the customer's (potentially abnormal) behaviour? If not, are relevant alternative parameters are used?

28 An IP address is a unique numeric code identifying each computer connected to the internet.
29 A "Geo-IP" check verifies whether the issuing country corresponds with the IP address from which the user is initiating the transaction.

Applies to: All

Supporting documents: Technical specifications

10.1.5 Has the PSP/GA put fraud detection and prevention solutions in place in order to detect malware signs and alert for suspicious transactions?

Applies to: All

Supporting documents: Technical specifications

10.1.6 Have the rules covered by the solutions been adopted by PSPs/GA in line with, and linked to, the risk assessment referred to under Recommendation 2?

Applies to: All

Supporting documents: Risk assessment and technical specifications

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 PSP's authorisation message conveyed to the issuer.[30]

10.2.1 Have GAs of card payment schemes developed or adopted a harmonised definition of e-merchant categories?

- Has this definition been agreed in cooperation with acquiring PSPs?
- Do these definitions follow standards established for traditional/physical merchants?
- Are these definitions periodically updated and communicated[31]?

Applies to: All

Supporting documents: Project implementation plan and Harmonised e-merchant categories

10.2.2 Are there procedures in place to ensure acquirers adopt these definitions in the authorisation messages conveyed to the issuers of payment transactions?

Applies to: All

Supporting documents: Contracts and business rules

30 E-merchant categories refer to the classification of merchants according to sector of business activity. Currently the e-merchant categories are not yet standardised across card payment schemes and not always conveyed in the authorisation message. The harmonised classification of e-merchant categories (based, for example, on the European NACE classification) would help PSPs to analyse the fraud risk of a transaction.

31 Given the relative youth of the e-market place in general and its dynamics regarding new types of services being provided/offered.

10.3 KC Acquiring PSPs should have fraud detection and prevention systems in place to monitor e-merchant activities.

10.3.1 Do acquiring PSPs have fraud detection solutions implemented in such a way that allows the monitoring of e-merchant activities on the basis of, for example:

- transaction patterns (types of products/services acquired, related amounts);
- e-merchant categories;
- geolocation?

Applies to: PSP

Supporting documents: Security policy and technical specifications

10.4 KC PSPs should perform any transaction screening and evaluation procedures within an appropriate time period, in order not to unduly delay the initiation and/or execution of the payment service concerned.

10.4.1 Does the PSP use an appropriate time frame for transaction screening procedures (and potential fraud evaluation) which ensures that the initiation and/or execution of the transaction are not unduly delayed (in line with the provisions of the PSD)?

Applies to: PSP

Supporting documents: Security policy and technical specifications

10.5 KC Where the PSP, according to its risk policy, decides to block a payment transaction which has been identified as potentially fraudulent, the PSP should maintain the block for as short a time as possible until the security issues have been resolved.

10.5.1 Has the PSP defined and documented procedures (technical or other) to ensure that blocked transactions are kept in that status for as short a time as possible?

Applies to: PSP

Supporting documents: Risk assessment report, security policy and technical specifications

Recommendation 11: Protection of sensitive payment data

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

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

11.1.1 Has the PSP properly identified and classified all sensitive payment data according to their protection needs?

Applies to: PSP

Supporting documents: Security policy

11.1.2 Does this include all data used to identify and authenticate customers (e.g. at log-in, when initiating internet payments and when issuing, amending or cancelling e-mandates), as well as the customer interface (PSP or e-merchant website)?

Applies to: PSP

Supporting documents: Risk assessment and security policy

11.1.3 Has the PSP set up specific procedures and technical measures (e.g. through the use of cryptography, access control measures or audit trails) to ensure that all sensitive payment data are appropriately secured against theft and unauthorised access or modification?

Applies to: PSP

Supporting documents: Security policy

11.2 KC PSPs should ensure that when exchanging sensitive payment data via the internet, secure end-to-end encryption[32] is applied between the communicating parties throughout the respective communication session, in order to safeguard the confidentiality and integrity of the data, using strong and widely recognised encryption techniques.

11.2.1 Does the PSP ensure that, when exchanging sensitive payment data via the internet, secure end-to-end encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and integrity of the data, using strong and widely recognised encryption techniques? (The encryption should cover the whole communication session "full session encryption".)

Applies to: All

Supporting documents: Technical specifications

11.3 KC PSPs offering acquiring services should encourage their e-merchants not to store any sensitive payment data. In the event e-merchants handle, i.e. store, process or transmit sensitive payment data, such PSPs should contractually require the e-merchants to have the necessary measures in place to protect these data. PSPs should carry out regular checks and if a PSP becomes

32 End-to-end-encryption refers to encryption within or at the source end system, with the corresponding decryption occurring only within or at the destination end system. ETSI EN 302 109 V1.1.1. (2003-06).

aware that an e-merchant handling sensitive payment data does not have the required security measures in place, it should take steps to enforce this contractual obligation, or terminate the contract.

11.3.1 Does the PSP encourage e-merchants not to store any sensitive payment data, e.g. by offering acquiring services where the sensitive payment data would be under the PSP's responsibility?

Applies to: All

Supporting documents: Technical specifications

11.3.2 In the event of e-merchants handling, i.e. storing, processing or transmitting sensitive payment data, does the PSP contractually require the e-merchants to have the necessary measures in place to protect these data?

Applies to: All

Supporting documents: E-merchant contract

11.3.3 Has the PSP carried out regular checks for those e-merchants that handle sensitive payment data (e.g. through audits or by requiring the e-merchant to provide respective audit reports)?

Applies to: All

Supporting documents: Audit reports

11.3.4 In cases of non-compliance by the e-merchant, has the PSP taken measures to enforce the contractual obligation or terminate the contract?

Applies to: All

Supporting documents: Audit reports

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

11.1.1 BP Do PSP contracts require e-merchants handling sensitive payment data to appropriately train their fraud management staff and update this training regularly to ensure that the content remains relevant to a dynamic security environment?

Applies to: E-merchants

Supporting documents: E-merchant contract

CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION

Recommendation 12: Customer education and communication

PSPs should provide assistance and guidance to customers, where needed, with regard to the secure use of the internet payment services. PSPs should communicate with their customers in such a way as to reassure them of the authenticity of the messages received.

12.1 KC PSPs should provide at least one secured channel[33] 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 services session and/or possible social engineering[34] 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 their non-initiation, or warn the customer about the occurrence of attacks (e.g. phishing e-mails).

12.1.1 Has the PSP defined at least one secured channel (e.g. online banking, encrypted and digitally signed e-mail, dedicated secure website, ATM) for ongoing communication with customers regarding the correct and secure use of the internet payment service?

Applies to: PSP

Supporting documents: Security policy

12.1.2 Does the PSP 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?

- This procedure is implemented in practice, e.g. in customer contracts, customer information leaflets, information campaigns or websites.

Applies to: PSP

Supporting documents: Policy document, customer contract and PSP website

33 Such as a dedicated mailbox on the PSP's website or a secured website.
34 Social engineering in this context means techniques of manipulating people to obtain information (e.g. via e-mail or phone calls), or retrieving information from social networks, for the purposes of fraud or gaining unauthorised access to a computer or network.

12.1.3 Has the PSP explained: (i) the procedure for customers to report to the PSP (suspected) fraudulent payments, suspicious incidents or anomalies during the internet payment services session and/or possible social engineering attempts; (ii) the next steps, i.e. how the PSP will respond to the customer; (iii) how the PSP will notify the customer about (potential) fraudulent transactions or their non-initiation, or warn the customer about the occurrence of attacks (e.g. phishing e-mails)?

- These procedures are secure, efficient and understandable for the customer.

Applies to: PSP

Supporting documents: Policy document and customer contract

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

12.2.1 Does the PSP have a procedure to ensure that customers are informed through the secure channel about updates in security procedures regarding internet payment services and of any alerts concerning any significant risks that are emerging (e.g. warnings about social engineering)?

- The procedure is clearly defined.
- The procedure is secure, efficient and understandable for the customer.

Applies to: PSP

Supporting documents: Policy document

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 related services, and customers should be appropriately informed about how such assistance can be obtained.

12.3.1 Is customer assistance available 24/7 for notifications of anomalies or incidents regarding internet payments and related services, and during normal business hours for all questions, complaints or requests for support regarding internet payments and related services?

Applies to: PSP

Supporting documents: Policy for customer assistance

12.3.2 Does the PSP have a procedure in place that ensures that, even if there is a major incident, appropriate information is communicated to the customers?

- Customer assistance is appropriately skilled.
- Customer assistance has appropriate measures and sufficient resources.

Applies to: PSP

Supporting documents: Human Resource policy and policy for customer assistance

12.3.3 Does the PSP have a procedure in place to communicate how the customer can obtain assistance?

- This might include initial information when signing the contract, indications on the PSP's website, emergency numbers on payment instruments or authentication tools.

Applies to: PSP

Supporting documents: Policy for customer assistance, customer contract and PSP website

12.4 KC PSPs, and, where relevant, 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 properly manage 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 of the PSP.

12.4.1 Has the PSP initiated customer education and awareness programmes designed to ensure that customers understand, at a minimum, the need:

- to protect their passwords, security tokens, personal details and other confidential data;
- to properly manage 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 of the PSP.

Applies to: All

Supporting documents: Policy document and awareness programme material

12.4.2 Does the PSP have a procedure in place to ensure that the content and documentation is relevant, complete, understandable and readily available?

- The procedure includes customer feedback loops in order to measure the effectiveness (i.e. important messages are understood by the recipients) and reach of the programs (e.g. number of clients).

Applies to: All

Supporting documents: Policy document, awareness programme and statistics / evaluation report

12.5 KC Acquiring PSPs should require e-merchants to clearly separate payment-related processes from the online shop in order to make it easier for customers to identify when they are communicating with the PSP and not the payee (e.g. by re-directing the customer and opening a separate window so that the payment process is not shown within a frame of the e-merchant).

12.5.1 Do acquiring PSPs contractually require e-merchants to clearly separate payment-related processes from the online shop in order to make it easier for customers to identify when they are communicating with the PSP and not the payee (e.g. by redirecting the customer and opening a separate window so that the payment process is not shown within a frame of the e-merchant)?

Applies to: PSP

Supporting documents: E-merchant contract, technical specifications and audit reports

12.5.2 Do acquiring PSPs monitor and enforce this?

- The acquiring PSP has the right to audit the e-merchant on the compliance with rulebooks and contracts.
- The acquiring PSP raises awareness of this issue with the e-merchant and has a procedure to ensure compliance (e.g. fines, decline of contract.)

Applies to: PSP

Supporting documents: Audit reports

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

12.1.1 BP Has the PSP established/offered physical or virtual educational programmes on fraud prevention for its e-merchants?

Applies to: PSP

Supporting documents: Educational programme material

12.1.2 BP Is content and documentation is relevant and can merchants easily access this information (e.g. protected websites, regular circulars)?

Applies to: PSP

Supporting documents: Educational programme material

12.1.3 BP Can the PSP prove that training programs are attended on a regular basis by a significant number of merchants?

- The PSP has a procedure to track the number of merchants that attended courses and completed the programmes.
- The PSP has defined risk categories for merchants and ensures that high risk merchants are in particular involved in the educational programmes.

Applies to: PSP

Supporting documents: Educational programme statistics/evaluation reports

Recommendation 13: Notifications, setting of limits

PSPs should set limits for internet payment services and could provide their customers with options for further risk limitation within these limits. They may also provide alert and customer profile management services.

13.1 KC Prior to providing a customer with internet payment services, PSPs should set limits[35] applying to those services, (e.g. a maximum amount for each individual payment or a cumulative amount over a certain period of time) and should inform their customers accordingly. PSPs should allow customers to disable the internet payment functionality.

13.1.1 Are the PSP's limits clearly defined (e.g. the maximum amount for each individual payment or a cumulative amount over a certain period of time)?

- The PSP has defined limits specific to its internet payments services or otherwise applied globally to all payment instruments. Limits including other remote payments (e.g. mail and telephone order) would also be acceptable.
- Are the limits proportionate to the risk involved in the services provided (e.g. the PSP has analysed the risks involved and has a procedure to ensure that the limits are proportionate to the risk)?

Applies to: PSP

Supporting documents: Risk assessment report and policy document

35 Such limits may either apply globally (i.e. to all payment instruments enabling internet payments) or individually.

13.1.2 Does the PSP have a procedure to explicitly inform the customer about these limits and their handling through an understandable and transparent procedure? Does this information take place prior to providing the customer with internet payment services?

Applies to: PSP

Supporting documents: Security policy and customer information material

13.1.3 Has the PSP informed the customer in a transparent way that he/she may disable the internet payment functionality? Is the relevant procedure efficient and clearly explained?

Applies to: PSP

Supporting documents: Security policy and technical specifications

13.1 BP Within the set limits, PSPs could provide their customers with the facility to manage limits for internet payment services in a safe and trusted environment.

13.1.1 BP Does the PSP provide its customers with the facility to manage limits for internet payment services in a safe and trusted environment?

Applies to: PSP

Supporting documents: Policy document and technical specifications

13.1.2 BP Has the PSP established a procedure which is appropriate, secure and not misleading?

- *The procedure has been clearly explained to customers, including all relevant aspects (e.g. when changes of limits become effective).*
- *Changes to the user limits are kept track of and made available to the customer.*

Applies to: PSP

Supporting documents: Policy document and technical specifications

13.2 BP PSPs could implement alerts for customers, such as via phone calls or SMS, for suspicious or high risk payment transactions based on their risk-management policies.

13.2.1 BP Does the PSP provide alerts for customers, e.g. via phone calls or SMS, for suspicious or high-risk payment transactions?

- The procedure set a default amount limit that triggers an alert, giving the option to lower that limit.

Applies to: PSP

Supporting documents: Policy document and technical specifications

13.2.2 BP Are the alerts secure, clear and in line with the PSP's risk-management policies?

Applies to: PSP

Supporting documents: Policy document, technical specifications

13.3 BP PSPs could enable customers to specify general, personalised rules as parameters for their behaviour with regard to internet payments and related services, e.g. that they will only initiate payments from certain specific countries and that payments initiated from elsewhere should be blocked, or that they may include specific payees in white or black lists.

13.3.1 BP Does the PSP enable customers to specify, in a safe and trusted environment, general, personalised rules as parameters for their behaviour with regard to internet payments and related services (e.g. that they will only initiate payments from specific countries and that payments initiated from elsewhere should be blocked, or that they may include specific payees in white or black lists)?

Applies to: PSP

Supporting documents: Policy document and technical specifications

13.3.2 BP Can the customer change the personalised rules and parameters above in a secure and convenient manner?

- A track of the changes to the personalised rules is maintained and made available to the customer via online banking.
- Customers are notified by the PSP about the changes of limits via an out-of-the-band channel, e.g. SMS alerts.

Applies to: PSP

Supporting documents: Policy document and technical specifications

Recommendation 14: Customer access to information on the status of payment initiation and execution

PSPs should confirm to their customers the payment initiation and provide customers in good time with the information necessary to check that a payment transaction has been correctly initiated and/or executed.

14.1 KC [CT/e-mandate] PSPs should provide customers with a near real-time facility to check the status of the execution of transactions as well as account balances at any time[36] in a safe and trusted environment.

14.1.1 Does the PSP provide the customers with a near real-time facility 24/7 to check the status of the execution of transactions, as well as account balances, at any time?

Applies to: PSP [CT/e-mandate]

Supporting documents: Policy document

14.1.2 Is this facility operated in a safe and trusted environment?

Applies to: PSP [CT/e-mandate]

Supporting documents: Policy document

14.2 KC Any detailed electronic statements should be made available in a safe and trusted environment. Where PSPs inform customers about the availability of electronic statements (e.g. regularly when a periodic 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 communications or, if included, they should be masked.

14.2.1 Does the PSP have a procedure to ensure that any detailed electronic statement is only made available in a safe and trusted environment?

Applies to: PSP

Supporting documents: Business Practice Handbook

14.2.2 Does the PSP have a procedure to ensure that, where customers are informed about the availability of electronic statements (e.g. regularly when a periodic e-statement has been issued, or on an ad hoc basis after execution of a transaction) through an alternative channel,

36 Excluding exceptional non-availability of the facility for technical maintenance purposes, or as a result of major incidents.

such as by SMS, e-mail or letter, that sensitive payment data are not to be included or masked?

Applies to: PSP

Supporting documents: Business Practice Handbook

GLOSSARY OF TERMS

The following terms are defined for the purpose of this Assessment Guide.

Term	Definition
Authentication	A procedure that allows the PSP to verify a customer's identity.
Authorisation	A procedure that checks whether a customer or PSP has the right to perform a certain action, e.g. the right to transfer funds, or to have access to sensitive data.
Credentials	The information – generally confidential – provided by a customer or PSP for the purposes of authentication. Credentials can also mean the physical tool containing the information (e.g. one-time-password generator, smart card), or something the user memorises or represents (such as biometric characteristics).
Major payment security incident	An incident which has or may have a material impact on the security, integrity or continuity of the PSP's payment-related systems and/or the security of sensitive payment data or funds. The assessment of materiality should consider the number of potentially affected customers, the amount at risk and the impact on other PSPs or other payment infrastructures.
Transaction risk analysis	Evaluation of the risk related to a specific transaction taking into account criteria such as, for example, customer payment patterns (behaviour), value of the related transaction, type of product and payee profile.
Virtual cards	A card-based payment solution where an alternative, temporary card number with a reduced validity period, limited usage and a pre-defined spending limit is generated which can be used for internet purchases.
Wallet solutions	Solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants.