	Status	Ingenico comments
GENERAL CONTROL AND SECURITY ENVIRONMENT		
Recommendation 1: Governance		
The internet payment services security policy should be properly documented, and regularly reviewed and approved by senior management. It should define security objectives and the PSP's risk appetite.	KC	Will there be any template provided by the Supervisers to be able to match the compliance of the differents PSPs with the appropriate measurement tools?
The internet payment services security policy should define roles and responsibilities, including an independent risk management function, and the reporting lines for internet payment services, including management of sensitive payment data with regard to the risk assessment, control and mitigation.	KC	no comment
The internet payment services security policy could be laid down in a dedicated document.	BP	no comment
Recommendation 2: Risk identification and assessment		
PSPs, through their risk management function, should carry out and document detailed risk identifi cation and vulnerability assessments, including the assessment and monitoring of security threats relating to the internet payment services the PSP offers or plans to offer, taking into account: i) the technology solutions used by the PSP, ii) its outsourced service providers and, iii) all relevant services offered to customers. PSPs should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines both on the side of the PSP (Such as the susceptibility of the system to payment session hijacking, SQL injection, cross-sitescripting, buffer overfl ows, etc.) and the customer. (Such as risks associated with using multimedia applications, browser plug-ins, frames, external links, etc.)	KC	no comment
On this basis and depending on the nature and significance of the identifi ed security threats, PSPs 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 should take into account the time required to implement the changes (including customer roll-out) and take the appropriate interim measures to minimise disruption.	KC	How the signifiance of the identified security threats is concretely measured? Who will define that the vulnerability is soo high that changes should be operated?
The assessment of risks should address the need to protect and secure sensitive payment data, including: i) both the customer's and the PSP's credentials used for internet payment services, and ii) any other information exchanged in the context of transactions conducted via the internet.	KC	no comment
PSPs should undertake a review of the risk scenarios and existing security measures both after major incidents and before a major change to the infrastructure or procedures. In addition, a general review should be carried out at least once a year. The results of the risk assessments and reviews should be submitted to senior management for approval.	KC	Should this general review be carried out according to the risk related attitude of the PSPs or based on a common policy to all internet payments PSPs? If the answer is the 2nd option, then who will be legitimate to issue this policy?
Recommendation 3: Monitoring and reporting		
PSPs should have a process in place to centrally monitor, handle and follow up on security incidents and security-related customer complaints and report such incidents to the management.	KC	no comment
PSPs and card payment schemes should have a procedure for notifying the competent authorities (i.e. supervisory, oversight and data protection authorities) immediately in the event of major incidents with regard to the services provided.	KC	Does it mean that the PSPs will manage the security related incidents on scheme by scheme basis? Is there any common basis for such incident management would be envisageable among payment schemes?
PSPs and card payment schemes should have a procedure for cooperating on all data breaches with the relevant law enforcement agencies.	KC	no comment
Recommendation 4: Risk control and mitigation		
In designing, developing and maintaining internet payment services, PSPs should pay special attention to the adequate segregation of duties in information technology (IT) environments (e.g. the development, test and production environments) and the proper implementation of the "least privileged" principle as the basis for a sound identity and access management.	KC	no comment
Public websites and backend servers should be secured in order to limit their vulnerability to attacks. PSPs should use fi rewalls, proxy servers or other similar security solutions that protect networks, websites, servers and communication links against attackers or abuses such as "man in the middle" and "man in the browser" attacks. PSPs should use security measures that strip the servers of all superfluous functions in order to protect (harden) and eliminate vulnerabilities of applications at risk. Access by the various applications to the data and resources required should be kept to a strict minimum following the "least privileged" principle. In order to restrict the use of " fake" websites imitating legitimate PSP sites, transactional websites offering internet payment services should be identified by extended validation certifi cates drawn up in the PSP's name or by other similar authentication methods, thereby enabling customers to check the website's authenticity	KC	There is any initative to standardise the key principles of the authetification methdologies? In order to have a common level of protection of the autenticity control of the websites?

PSPs should have processes in place to monitor, track and restrict access to: i) sensitive data, and ii) logical and physical critical resources, such as networks, systems, databases, security modules, etc. PSPs should create, store and analyse appropriate logs and audit trails.	KC	no comment
Security measures for internet payment services should be tested by the risk management function to ensure their robustness and effectiveness. Tests should also be performed before any changes to the service are put into operation. On the basis of the changes made and the security threats observed, tests should be repeated regularly and include scenarios of relevant and known potential attacks.	KC	How will be defined the frequency of tests? How to be sure that the PSPs would be checked by similar methodologies?
The PSP's security measures for internet payment services should be periodically audited to ensure their robustness and effectiveness. The implementation and functioning of the internet services should also be audited. The frequency and focus of such audits should take into consideration, and be in proportion to, the security risks involved. Trusted and independent experts should carry out the audits. They should not be involved in any way in the development, implementation or operational management of the internet payment services provided.	KC	The audit should be done by accredited auditors currently in the ecosystem or do the Eurosysteme envisage a new framework with recommendation for accreditation of security auditors by an Independent Entity created for this purpose?
Whenever PSPs and card payment schemes outsource core functions related to the security of the internet payment services, the contract should include provisions requiring compliance with the principles and recommendations set out in this report	KC	no comment
PSPs offering acquiring services should require e-merchants to implement security measures on their website as described in this recommendation.	KC	no comment
Recommendation 5: Traceability		
PSPs should ensure that their service incorporates security mechanisms for the detailed logging of transaction data, including the transaction sequential number, timestamps for transaction data, parameterisation changes and access to transaction data.	KC	no comment
PSPs should implement log files allowing any addition, change or deletion of transaction data to be traced.	KC	no comment
PSPs should query and analyse the transaction data and ensure that any log files can be evaluated using special tools. The respective applications should only be available to authorised personnel.	KC	no comment
[cards] It is desirable that PSPs offering acquiring services require e-merchants who store payment information to have these processes in place.	BP	This should be a KC instead of a BP

	Status	Ingenico comments
SPECIFIC CONTROL AND SECURITY MEASURES FOR INTERNET PAYMENTS		
Recommendation 6: Initial customeridentification, information		
PSPs should ensure that the customer has undergone the necessary identification procedures and provided adequate identity documents and related information before being granted access to the internet payment services.	KC	No comment
PSPs should ensure that the prior information 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. antivirussoftware, firewalls); – guidelines for the proper and secure use of personalised security credentials; – a step-by-step description of the procedure for the customer to submit and authorise a payment, including the consequences of each action; – guidelines for the proper and secure use of all hardware and software provided to the customer; – the procedures to follow in the event of loss or theft of the personalised security credentials or the customer's hardware or software for logging in or carrying out transactions; the procedures to follow if an abuse is detected or suspected; – a description of the responsibilities and liabilities of the PSP and the customer respectively with regard to the use of the internet payment service.	KC	This seems quite heavy for the final customer.
PSPs should ensure that the framework contract with the customer includes compliance related clauses enabling the PSP to fulfil its legal obligations relating to the prevention of money laundering, which may require it to suspend execution of a customer's payment transaction pending the necessary regulatory checks and/or to refuse to execute it. The contract should also specify that the PSP may block a specific transaction or the payment instrument on the basis of security concerns. It should set out the method and terms of the customer notification and how the customer can contact the PSP to have the service "unblocked", in line with the Payment Services Directive.	KC	no comment
PSPs should also ensure that customers are provided, on an ongoing basis and via appropriate means (e.g. leaflets, website pages), with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service.	KC	no comment
It is desirable that the customer signs a dedicated service contract for conducting internet payment transactions, rather than the terms being included in a broader general service contract with the PSP.	BP	What is the goal of this best practice? Would a harmonised methodology in terms of merchant contract for the internet payment be fruitful?
Recommendation 7: Strong customer authentication		What is the Eurosysteme recommendation in terms of authentication methodology? Could a standardisation initative in this domain make sense?
[CT/e-mandate] Credit transfers (including bundled credit transfers) or electronic direct debit mandates should be initiated by strong customer authentication. PSPs could consider adopting less stringent customer authentication for outgoing payments to trusted benefi ciaries included in previously established "white lists", i.e. a customer-created list of trusted counterparties and benefi ciary accounts with strong authentication	KC	no comment
Obtaining access to or amending sensitive payment data requires strong authentication. Where a PSP offers purely consultative services, with no display of sensitive customer or payment information, such as payment card data, that could be easily misused to commit fraud, the PSP may adapt its authentication requirements on the basis of its risk analysis.	KC	no comment
[cards] For card transactions, all PSPs offering issuing services should support strong authentication of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication (e.g. for 3-D Secure, registered in the 3-D Secure Directory) and the customer must have given prior consent to participating in such services. (See Annex 3 for a description of authentication under the cards environment.)	KC	no comment
[cards] All 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.	KC	no comment
[cards] PSPs offering acquiring services should require their e-merchant to support strong authentication of the cardholder by the issuer for card transactions via the internet. Exemptions to this approach should be justifi ed by a (regularly reviewed) fraud risk analysis. In the case of exemptions, the use of the card verifi cation code, CVx2, should be a minimum requirement.	KC	In this point, you propose to accept in some cases the CVx2, which is today considered as not secure enough. It will be difficult to asks PSPs to require their e-merchant implement strong authentication (e.g. 3-D secure) and in the same time allow lower athentication
[cards] All card payment schemes should promote the implementation of strong customer authentication by introducing liability shifts (i.e. from the e-merchant to the issuer) in and across all European markets.	KC	no comment
[cards] For the card payment schemes accepted by the service, providers of wallet solutions should support technologies allowing the issuer to perform strong authentication when the legitimate holder first registers the card data. Providers of wallet solutions should support strong user authentication when executing card transactions via the internet. Exemptions to this approach should be justifi ed by a (regularly reviewed) fraud risk analysis. In the case of exemptions, the use of CVx2 should be a minimum requirement.	KC	In a wallet solution there is no use of CVx2, because the wallet principle is not using card data at the moment of the payment, but only wallet identification/authentication modules (username/password). Card data are encrypted at the moment of the enrolment in the wallet, but after they are never used again. So this requirement couldn't function with wallet for the payment. Authentication is important when the legitimate holder first registers the card data.
[cards] For virtual cards, the initial registration should take place in a safe and trusted environment (as defi ned in Recommendation 8). Strong authentication should be required for the virtual card data generation process if the card is issued in the internet environment.	KC	no comment
[cards] It is desirable that e-merchants support strong authentication of the cardholder by the issuer in card transactions via the internet. In the case of exemptions, the use of CVx2 is recommended.	BP	same remark as in line 15
For customer convenience purposes, PSPs providing multiple payment services could consider using one authentication tool for all internet payment services. This could increase acceptance of the solution among customers and facilitate proper use.	BP	no comment
Recommendation 8: Enrolment for and provision of strong authentication tools		

Enrolment for and provision of strong authentication tools should fulfil the following requirements. – The related procedures should be carried out in a safe and trusted environment (e.g. face-to-face at a PSP's premises, via an internet banking or other secure website offering comparable security features, or via an automated teller machine). – Personalised security credentials and all internet payment-related devices and software enabling the customer to perform internet payments should be delivered securely. Where tools need to be physically distributed, they should be sent by post or delivered with acknowledgement of receipt signed by the customer. Software should also be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with. Moreover, personalised security credentials should not be communicated to the customer via e-mail or website. – [cards] For card transactions, the customer should have the option to register for strong authentication independently of a specifi c internet purchase. In addition, activation during online shopping could be offered by re-directing the customer to a safe and trusted environment, preferably to an internet banking or other secure website offering comparable security features.	KC	no comment
[cards] Issuers should actively encourage cardholder enrolment for strong authentication. Cardholders should only be able to bypass strong authentication in exceptional cases where this can be justified by the risk related to the card transaction. In such instances, weak authentication based on the cardholder name, personal account number, expiration date, card verifi cation code (CVx2) and/or static password should be a minimum requirement.	KC	At least the circumstances under which the cardholder can bypass the strong athentication must be very limited and cautiously defined (e.g. low-value payment)
Recommendation 9: Log-in attempts, session time-out, validity of authentication		
When using a one-time password for authentication purposes, PSPs should ensure that the validity period of such passwords is limited to the strict minimum necessary (i.e. a few minutes).	KC	no comment
PSPs should set down the maximum number of failed log-in or authentication attempts after which access to the internet service is (temporarily or permanently) blocked. They should have a secure procedure in place to re-activate blocked internet services	KC	no comment
PSPs should set down the maximum period after which inactive payment sessions are automatically terminated, e.g. after ten minutes.	KC	no comment
Recommendation 10: Transaction monitoring and autorisation		
PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules (such as black lists of compromised or stolen card data), abnormal behaviour patterns of the customer or the customer's access device (change of Internet Protocol (IP) address 12 or IP range during the internet payment session, sometimes identified by geolocation IP checks (A "Geo-IP" check verifies whether the issuing country corresponds with the IP address from which the user is initiating the transaction), abnormal transaction data or e-merchant categories, etc.) and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions should be commensurate with the outcome of the fraud risk assessment.	KC	Could the Eurosysteme provide treshold recommendation for fraud detection?
Card payment schemes in cooperation with acquirers should elaborate a harmonised definition of e-merchant categories and require acquirers to implement it accordingly in the authorisation message conveyed to the issuer. (Currently the e-merchant categories are not yet standardised across card payment schemes and not always conveyed in the authorisation message. The harmonised classifi cation of e-merchant categories would help PSPs to analyse the fraud risk of a transaction.)	KC	agree
It is desirable that PSPs perform the screening and evaluation procedure within an appropriate time period, in order not to unduly delay execution of the payment service concerned.	BP	What do you mean by "appropriate time period"? This time should be harmonised and should apply to all PSPs according to a deep knowledge of the market expectations about it.
It is desirable that PSPs notify the customer of the eventual blocking of a payment transaction, under the terms of the contract, and that the block is maintained for as short a period as possible until the security issues have been resolved.	BP	Let us be careful not to ease phishing attacks.
Recommendation 11: Protection of sensitive payment data		
All data or files used to identify and authenticate customers (at log-in and when initiating internet payments or other sensitive operations), as well as the customer interface (PSP or e-merchant website), should be appropriately secured against theft and unauthorised access or modifi cation.	KC	Why not link this requirement with the European Data privacy requirements?
PSPs should ensure that when transmitting sensitive payment data, a secure end-to-end communication channel is maintained throughout the entire duration of the internet payment service provided in order to safeguard the confi dentiality of the data, using strong and widely recognised encryption techniques.	KC	no comment
[cards] PSPs offering acquiring services should encourage their e-merchants not to store any sensitive payment data related to card payments. In the event e-merchants handle, i.e. store, process or transmit sensitive data related to card payments, such PSPs should require the e-merchants to have the necessary measures in place to protect these data and should refrain from providing services to e-merchants who cannot ensure such protection.	KC	Would PCI DSS be enough for the e-merchants?
[cards] It is desirable that e-merchants handling sensitive cardholder data appropriately train their dedicated fraud management staff and update this training regularly to ensure that the content remains relevant to a dynamic security environment.	BP	no comment

	Status	Ingenico comments
CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION		
Recommendation 12: Customer education and communication		
PSPs should provide at least one secured channel for ongoing communication with customers regarding the correct and secure use of the internet payment service. PSPs should inform customers of this channel and explain that any message on behalf of the PSP via any other means, such as e-mail, which concerns the correct and secure use of the internet payment service, is not reliable. The PSP should explain: - the procedure for customers to report to the PSP (suspected) fraudulent payments, suspicious incidents or anomalies during the internet payment session and/or possible social engineering 16 attempts; – the next steps, i.e. how the PSP will respond to the customer; – how the PSP will notify the customer about (potential) fraudulent transactions or warn the customer about the occurrence of attacks (e.g. phishing e-mails).	KC	no comment
Through the designated channel, PSPs should keep customers informed about updates in procedures and security measures regarding internet payment services. Any alerts about significant emerging risks (e.g. warnings about social engineering) should also be provided via the designated channel	KC	no comment
Customer assistance should be made available by PSPs for all questions, complaints, requests for support and notifi cations of anomalies or incidents regarding internet payments, and customers should be appropriately informed about how such assistance can be obtained.	KC	agree
PSPs and, where relevant, card payment schemes should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need: – to protect their passwords, security tokens, personal details and other confi dential data; – to manage properly the security of the personal device (e.g. computer), through installing and updating security components (antivirus, fi rewalls, security patches); – to consider the signifi cant 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.	KC	agree
[cards] It is desirable that PSPs offering acquiring services arrange educational programmes for their e-merchants on fraud prevention.	BP	It would be good if it could take place in association with European e-commerce federation (EDIMA)
Recommendation 13: Notifications, setting of limits		
Prior to providing internet payment services, PSPs should agree with each customer on spending limits applying to those services (e.g. setting a maximum amount for each individual payment or a cumulative amount over a certain period of time), and on allowing the customer to disable the internet payment functionality.	KC	agree
Within the agreed limits, e.g. taking into account overall spending limits on an account, PSPs could provide their customers with the facility to manage limits for internet payment services in a secure environment.	BP	What does it mean exactly to manage the limit fo internet payment? Like in the physical word? The definition of the spending limit on a bilateral basis?
PSPs could implement alerts for customers, such as via phone calls or SMS, for fraud-sensitive payments based on their risk management policies	BP	no comment
PSPs could enable customers to specify general, personalised rules as parameters for their behaviour with regard to internet payments, e.g. that they will only initiate payments from certain specific countries and that payments initiated from elsewhere should be blocked.	BP	no comment
Recommendation 14: Verifi cation of payment execution by the customer		
PSPs should provide customers with a facility to check transactions and account balances at any time in a secure environment	KC	agree
Any detailed electronic statements should be made available in a secure environment. Where PSPs periodically inform customers about the availability of electronic statements (e.g. when a new monthly e-statement has been issued, or on an ad hoc basis after execution of a transaction) through an alternative channel, such as SMS, e-mail or letter, sensitive payment data should not be included in such statements or, if included, they should be masked.	KC	agree