EUROPEAN PAYMENTS COUNCIL
Towards our Single Payment Area

EPC397-08v1.1 March 15th 2009

CUSTOMER-TO-BANK
SECURITY GOOD PRACTICES GUIDE

Document History

Version	Date	Status
Version 0.1.0	November 20th 2007	First draft
Version 0.2.0	November 30th 2007	Second draft for discussion at the Dec 2007 SPTF meeting
Version 0.3.0	February 15th 2008	Third draft based on comments provided by SPTF for review at the 22nd February 2008 C2B ad hoc meeting
Version 0.4.0	April 29th 2008	Fourth draft based on contributions provided by SPTF C2B WB
Version 0.5.0	June 26th 2008	Fifth draft based on contributions provided by SPTF C2B WB
Version 0.6.0	August 10th 2008	Sixth draft based on comments provided by SPTF – July 2008
Version 0.7.0	December 7th 2008	Final draft based on comments provided by SPTF – October-November 2008
Version 1.0.0	December 9th 2008	Final version for EPC Plenary approval incorporating final ISSG comments
Version 1.1.0	March 15th 2009	Final version incorporating minor comments provided with EPC Plenary voting

TABLE OF CONTENTS

1 MANAGEMENT SUMMARY

E-channels provide outstanding efficiency for both banks and their customers. To build on this efficiency it is obvious that trust, availability and usability of e-channels must be safeguarded. Harmonization of payment instruments, rules and juridical framework encourages the use of cross-border services. New institutions, also non-banks, are expected to enter into the market of payment services. To gather the benefits of SEPA, insurance needs to be provided that the trust in e-banking is not hampered by inconsistent security practices or by "race to the bottom" competition with reduced security costs. Hence, the European payment industry is requested to commit itself to follow the security good principles and practices for the remote initiation of transactions for SEPA instruments in their operations as specified in the present document. In its 4th SEPA Progress Report (February 2006) the Eurosystem welcomed the activity started by EPC, as it is important that the end-to-end security of payment transactions undertaken with SEPA instruments is ensured in a harmonized way, on the basis of good practices and standards.

As a first step EPC has conducted a *survey on security solutions and practices* in use by the banks in Europe for the protection of their Customer-to-Bank (C2B) communications related to SEPA debit and credit transfers. The results of the survey ([9], see Annex 3) found a wide range of different and diverse security practices.

Therefore, a direct derivation of a common list of good security practices for SEPA payment instruments, seemed somewhat challenging. As a consequence a *threat assessment study* was executed as an intermediate step. The outcome of this study [10], see Annex 4) will now serve as input for the present document: the security good practices guide. The development of these principle-based security guidelines will further be based on the security principles contained in ECBS TR 411v2: *Security Guidelines for E-Banking* [7] relative to the Customer-to-Bank area. This TR 411 is based on the report issued by the Basel Committee on Banking Supervision: *Risk management principles for electronic banking* [3], and the subsequent report *"Management and Supervision of Cross-Border Electronic Banking Activities"* [4], issued in July 2003.

Information is one of the most important elements in the banking business today. It represents a valuable asset, which needs to be protected. The protection of information aims primarily at avoiding direct financial losses and reputational damage. A number of technical and organisational security measures are required to protect the authenticity, integrity and confidentiality of information. In online banking these include secure authentication procedures adapted to deal with the latest threats. The challenge will continue to be to strike a commercially viable balance between monetary and reputational damage and expenditure on security.

The present document aims to provide good practice principles and guidelines on the Customer-to-Bank security relative to the remote initiation of electronic transactions for SEPA Direct Debit and SEPA Credit Transfer Schemes. It is further relevant for any e- or m-payment channel solution in Europe and could as well apply to participants in e-invoicing systems. These principles are not put forth as the 'absolute" requirements nor do they try to set specific technical solutions or standards. However, they are recommended to be used as tools by banks, e-banking service providers or any party acting on their behalf, referred to as *financial institutions* in the sequel of this document. As such, they aim to set a common security baseline across all remote Customer to Bank (C2B) SEPA transactions. The document may also help inform the work of national supervisors. They should assist the financial industry to implement a consistent industry level security framework for the delivery of remote banking services to customers. Financial institutions may measure themselves against these principles as a baseline. This common framework aims to protect the finance industry's reputation and should be included as an integral element of any remote banking strategy. Clearly, the principles might need to be adapted when implemented to reflect specific national requirements and individual risk profiles.

The introduction of this document which provides the background and scope is followed by chapter 3 on the classification of the banking services related to remote transaction with respect to their risk profiles. The next section deals with the selection of the controls. Chapter 5 which is the main section of this document specifies the principles in the following areas: board management oversight, customer registration, entity authentication, transaction security and secure operations. Each principle defined, is followed by supporting guidelines which are supplemented with additional information as appropriate. Chapter 6 provides on high level mapping of the principles onto the external threats in the C2B area as specified in [10]. Finally, some conclusions are defined in section 7.

As remote banking is becoming increasingly important for the delivery of financial services to customers it is important that these services are delivered in a secure and safe way. Indeed, this is key for the creation of trust amongst customers in these new services and the customer acceptance of these new payment channels. The principles and guidelines in this document aim to be generic for the C2B area and to provide an overview of the security measures that need to be implemented in this ecosystem. This also means that in their implementation care must be taken to what specific demands or risks the stakeholders are faced to in particular markets and to which specific product offering they relate to. Eventually, a proactive based approach to the various risks and threats associated with remote banking is necessary in order to protect the business and the customer.

2 INTRODUCTION

2.1 BACKGROUND

E-channels provide outstanding efficiency for both banks and their customers. To build on this efficiency it is obvious that trust, availability and usability of e-channels must be safeguarded. To gather the benefits of SEPA, insurance needs to be provided that the trust in e-banking is not hampered by inconsistent security practices or by "race to the bottom" competition with reduced security costs. Therefore EPC has taken the initiative to specify security good principles and practices for the remote initiation of transactions for SEPA instruments. In its 4th SEPA Progress Report (February 2006) the Eurosystem welcomed the activity started by EPC, as it is important that the end-to-end security of payment transactions undertaken with SEPA instruments is ensured in a harmonized way, on the basis of good practices and standards.

The results of the survey [9] conducted by EPC in 2006 found a wide range of different and diverse security practices (see Annex 3). Therefore, a direct derivation of a common list of good security practices for SEPA payment instruments, seemed somewhat challenging. Following the methodology specified in the ISO series 2700x on “Information Security Management Systems” [15] which has been adopted by all industry sectors worldwide, including the financial industry, to constitute a model for establishing, implementing and maintaining Information Security Management Systems, EPC has decided to conduct a Risk and Threat assessment in the C2B environment as an intermediate step towards Security Good Practices Guidelines. Since a complete risk assessment as described in ISO 2700x, could not be conducted within the specific scope and authority of EPC, the study was limited to a threats and vulnerabilities assessment. The recommendations resulting from this study ([10], Annex 4) will be used in the present document.

The development of these principle-based security guidelines will further be based on the security principles contained in ECBS TR 411v2: *Security Guidelines for E-Banking* [7] relative to the Customer-to-Bank area. This TR 411 is based on the report issued by the Basel Committee on Banking Supervision: *Risk Management Principles for Electronic Banking*, originally published in May 2001, followed by a final version in July 2003 [3] and the subsequent report *“Management and Supervision of Cross-Border Electronic Banking Activities”* [4], issued in July 2003.

The present document aims to provide good practice principles and guidelines on the Customer-to-Bank security relative to the remote initiation of electronic transactions for SEPA Direct Debit and SEPA Credit Transfer Schemes. It is further relevant for any e- or m-payment channel solution in Europe and could as well apply to participants in e-invoicing systems. These principles are not put forth as the ‘absolute” requirements nor do they try to set specific technical solutions or standards. However, they are recommended to be used as tools by banks, e-banking service providers or any party acting on their behalf, referred to as *financial institutions* in the sequel of this document. As such, they aim to set a common security baseline across all remote Customer to Bank (C2B) SEPA transactions. The document may also help inform the work of national supervisors. They should assist the financial industry to implement a consistent industry level security framework for the delivery of remote banking services to customers. Financial institutions may measure themselves against these principles as a baseline. This common framework aims to protect the finance industry’s reputation and should be included as an integral element of any remote banking strategy.

Some European banking associations have developed their own national recommendations. EPC has been greatly helped in the preparation of this report by these documents which are included in the references (see [1], [2] and [11]).

2.2 PURPOSE AND SCOPE

The business focus for the present document is where customers interact *remotely* with their financial institutions in order to access financial services, the so-called e-banking services. Hereby "financial institution" should be interpreted in the broadest sense, including banks, service providers or any third party processor acting on their behalf. Banking products and services become accessible and delivered to retails and wholesale customers through electronic distribution channels. This means that the financial institution and the customer communicate at a distance (not involving face-to-face physical presence of the parties) which might involve the usage of a remote e-banking service provider and a device physically operated by the customer. This document is aimed primarily at financial institutions supplying services to personal customers. However most of the principles and guidance given are irrespective of the customer type. The document will mainly concentrate on the new (open) environments, that typically include non-bank controlled access systems and networks, and less on the payment products involved. Indeed, the security related to payment products and the related payment transactions in bank controlled environments such as card based transactions at ATMs or POS or self-banking in bank branches have already been extensively covered in others EPC publications.

The document aims to define security principles and guidelines to address the enhanced security challenges posed by e-banking. This include establishing appropriate authorisation privileges and authentication measures, logical and physical access controls, adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities and data integrity of transactions, records and information. In addition, the existence of clear audit trails for all e-banking transactions should be ensured and measures to preserve confidentiality of key e-banking information should be appropriate with the sensitivity of the information.

Although customer protection and privacy regulations vary from jurisdiction to jurisdiction, banks generally have a clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data and business availability that approaches the level they can expect when using traditional banking distribution channels. To minimise legal and reputational risk associated with e-banking activities conducted both domestically and cross-border, financial institutions should make adequate disclosure of information on their web sites and take appropriate measures to ensure adherence to customer privacy requirements applicable in the jurisdictions to which they are providing e-banking services.

The main purpose of this report is to help financial institutions to implement security controls in their e-banking services based on best practices in relation to specific risk profiles. It is evident that different e-banking services and transactions constitute different risks to the financial institutions and consequently must be treated accordingly. This report identifies six different classes of e-banking services as six risk profiles (Chapter 3). Some of the low risk areas require none or only few security principles implemented. This report focuses on a specific risk profile for customer originated transactions, and recommends guidelines and best practices for this specific risk profile.

Whereas the Basel Committee document contains minimal security requirements agreed upon by all represented countries, this EPC report rather gives guidelines and refers to best practices which the financial institutions should aim for in their future implementation of e-banking services. These guidelines and best practices are not necessarily currently implemented, but will be used by EPC members for evaluation and future development of e-banking services.

Chapter 4 provides some guidance on the selection of controls and the critical success factors in the implementation of a control framework.

Chapter 5 is structured in five areas where specific security principles have been defined: board management oversight, customer registration, entity authentication, transaction security and secure operations. For each area next to the principles, supporting guidelines and additional information as appropriate are provided. In this way the document attempts to develop the general requirements from the Basel report into specific Guidelines and Best Practices which should guide financial institutions in the implementation of the best security controls in their e-banking services.

For the purposes of this report, “e-banking” is defined as remote banking services provided by licensed, regulated financial institutions through devices operated by the customer, excluding automated teller machines because they are under the direct control of financial institutions and management. A “remote banking service” is defined as a:

- dedicated banking service for which the customer has explicitly registered;
- which requires the authentication of the customer;
- using devices and/or software which may be supplied by the financial institution but are under the control of the customer when using this banking service (e.g., home PC, mobile phone, TV,...)

Individual communications such as e-mail (digitally signed or otherwise) received by the financial institutions from a customer, outside the context of a remote banking service, are not included within the scope of this report.

3 CLASSIFICATION OF C2B REMOTE BANKING SERVICES INTO RISK PROFILES

This report classifies e-banking services in the Customer-to-Bank area according to the level of security required to perform the service, and according to the contractual requirement associated with the service.

a. General Information (e.g., brochures, advertising, etc…)

This profile presents the lowest risk. It is concerned with the provision of data which is not related to any account or individual. The presentation of information such as product descriptions, exchange rates, interest rates and contact details for the bank requires only that the information is not corrupted.

b. Customer Related Information (e.g., statements)

This profile deals with information related to customers or their accounts. Examples include statements and account balances. Within this profile, no transactions which transmit funds or change data are allowed, so here the additional risk is the exposure of existing confidential data.

c. Customer Originated Transactions between own accounts

This profile relates to the provision of transactions, where the customer can transfer money between its own accounts, hereby specifying the amount and the date without prior arrangement.

d. Customer Amendment of Pre-Mandated Instructions

This profile relates to financial transactions (direct debit or credit, including standing orders) which have been previously authorised using other channels. Typically, these transactions only allow the customer to vary the amount to be paid, or the date to perform the transaction.

e. Customer Originated Transactions (individual transactions)

This profile relates to the provision of transactions, where the customer can specify the beneficiary, the amount and the date without prior arrangement or subsequent additional authorisation. It is this profile which is the main focus of this report. Financial institutions may decide to sub-divide this profile depending on the transaction amount, or other parameters of the transaction. It further includes remote subscription of known customers to new services provided by financial institutions

f. Customer Acquisition (sign on)

This is the highest-risk profile. Customer recruitment and registration form the basis upon which all future security relies and hence must be treated with the greatest care. Included in this profile is the ability to (remotely) alter the registration information, authentication data or to renew an authentication device.

4 SECURITY CONTROL AREAS

4.1 SELECTING CONTROLS

In [10] EPC has identified and analysed the threats in the C2B area relative to remote transactions as well as their business impact for the banking industry. There are different ways of treating risks associated to these threats. The starting point however is to select a number of control areas.

Generally, controls should be selected and taking into account:

a) legal and regulatory requirements and constraints;

b) business and operational requirements and constraints;

c) the cost of implementation in relation to the risks being reduced, and remaining proportional to the organisation’s requirements and constraints;

and

d) the potential losses if a security breach occurs.

Factors such as loss of reputation should also be taken into account. It should be ensured that controls are selected and implemented in compliance with all applicable laws and regulations. Implemented controls should be able to deliver one or more of the following aspects: protection, detection, response and recovery from security incidents.

Furthermore, security controls should be considered at the systems and products requirements specification and design stage. Failure to do so may result in additional costs and less effective solutions, and maybe, in the worst case, inability to achieve adequate security.

A number of controls can be considered as a good starting point for implementing (information) security principles. They are either based on essential legislative requirements or considered to be common practice for (information) security.

Controls considered to be essential to an organisation from a legislative point of view include, depending on applicable legislation:

a) data protection and privacy of personal information;

b) safeguarding of organisational records;

c) intellectual property rights.

Controls considered to be common practice for information security include:

d) information security policy document;

e) data classification;

f) allocation of information security responsibilities;

g) information security awareness, education and training;

h) the secure development, (security) testing and maintenance of infrastructures, devices, applications and processes.

i) vulnerability management;

j) business continuity management;

k) management of information security incidents and improvements;

4.2 CRITICAL SUCCESS FACTORS

Experience has shown that the following factors are often critical to the successful implementation of a (information) security management framework within an organisation:

1. information security policy, objectives and activities that reflect business objectives;
2. an approach and framework to implementing, maintaining, monitoring and improving information security that is consistent with the organisational culture;
3. visible support and commitment from all levels of management;
4. a good understanding of the information security requirements, risk assessment and risk management;
5. effective marketing of information security to all managers, employees and other parties to achieve awareness;
6. translation of information security policies into operational standards and guidelines to be used by managers, employees and other parties;
7. provision to fund information security management activities;
8. establishing an effective information security incident management process;
9. implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

.

More guidance on the selection of controls and critical success factors in the implementation thereof can be found in the ISO series 2700x [15].

5 SECURITY PRINCIPLES AND GUIDELINES

This chapter focuses on security principles upon which the provision of secure e-banking services by financial institutions is based. Although based on the principles specified by the Basel documents, this document refines some of the principles and guidelines as the current and future implementation of e-banking services is the focus. Each of the principles is developed into specific guidelines to which e-banking systems should try to adhere, unless there are good reasons for alternative practices. Most of the guidelines are followed by additional information with the aim to provide further support in implementing them.

5.1 APPLICATION OF SECURITY PRINCIPLES

This document is designed to give financial institutions and their customers a clear view of the financial industry's position on securing e-banking services. Financial institutions should take these principles and incorporate them into local procedures, standards and guidelines applicable to their business function. It should be noted that the provision of secure services in a distributed systems environment requires all partners to maintain effective control of the devices, software and security tokens. Therefore the principles and guidelines are not only addressing financial institutions but some are also dealing with the customers of e-banking services. Indeed, customer responsibility and due diligence with regard to devices and software under their sole control (e.g., specifically to protect credentials used in the authentication mechanism) is an area which demands increasing attention and education in view of the emerging threats in the C2B environment. Customers should also be made aware that they have responsibilities as defined in the terms and conditions of service, to ensure that they may use remote e-banking services with confidence.

5.2 BOARD AND MANAGEMENT OVERSIGHT

Principle 1: The board of directors and senior management of financial institutions providing e-banking services should establish effective management oversight over the risks associated with these activities, including the establishment of specific accountability, policies and controls to manage these risks. More in particular, prior to engaging in cross-border e-banking activities, they should conduct appropriate risk assessment and due diligence.

Purpose: An adequate management oversight on the risk and security management associated to e-banking services is a prerequisite to allow an adequate handling of the threats and vulnerabilities inherent to these services. Senior management should actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment and acknowledgement of security responsibilities.

Implementation Guidelines:

Guideline 1.1: Financial institutions should have a framework of information security controls (e.g., an Information Security Management System (ISMS) or equivalent process) to manage risks. The Board of Directors or senior management should approve and monitor key aspects of the security control process.

Additional information: An Information Security Management System (ISMS) should be established based on a risk management. This approach will ensure a cost-balanced approach to effectively address the threats in view of the potential business impact for e-banking services. Guidance on the establishment of a ISMS is for instance provided in ISO 27000x (see [15]. Also [16] provides further guidance on a risk management based approach.

Guideline 1.2: Financial institutions should adhere to the relevant Code of Practice as established by (national) regulations.

Additional information: Financial institutions should adhere in their offering of cross-border services to all (national) regulations which might be applicable to internet services next to the overall banking regulations. This includes data protection laws, (tele)communication regulations, internet security, money laundering, cybercrime regulations, etc…

Guideline 1.3: Financial institutions should have a comprehensive due diligence and management oversight process for outsourcing relationships and other third party dependencies. The board of directors or senior management should approve and monitor key aspects of this process.

Additional information: The security of the information hold by the financial institutions related to e-banking services (including customer information) and the information processing facilities that are accessed, processed, communicated or managed by external parties should be managed and maintained appropriately. Where there is a business need to work with external parties that may require access to the financial institution's information and information processing facilities, or in obtaining or delivering a product or service from an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement (e.g., contract, SLA,…) with the external party.

5.3 CUSTOMER REGISTRATION

Principle 2: Financial institutions providing e-banking services should take appropriate measures to identify and register customers with whom they conduct business remotely.

Purpose: It is essential in banking to confirm that a particular communication, transaction, or access request is legitimate. Accordingly, financial institutions should use reliable methods for verifying the identity and authorisation of new customers, as well as authenticating the identity and authorisation of established customers seeking to register for remote banking services.

Implementation Guidelines:

Guideline 2.1: Financial institutions should be compliant to national requirements to execute 'Know your Customer' (KYC) processes and verify the customer's credentials in the opening and operation of an account.

Additional information: KYC processes are set out by national regulatory authorities and are based on robust customer identification and authentication processes in the registration of customers. These are particularly important in the cross-border e-banking context given the additional difficulties that may arise from doing business electronically with customers across national borders, including the increased risk for identity impersonation and the greater difficulty in conducting effective credit checks on potential customers.

Guideline 2.2: Customers should explicitly register for an e-banking service to manage their bank account(s) from a remote location.

Additional information: This explicit registration aims to raise customer awareness and stresses the trust factor involved in accessing e-banking systems.

Guideline 2.3: Financial institutions should ensure that, during the registration process the identification of the customer takes place using identity credentials commensurate with achieving confidence in the identity of the customer. The guideline remains valid in case of a re-registration process if the customer's authentication mechanism has been compromised,

Additional information: Financial institutions should determine which identification methods to use, based on national regulatory requirements to KYC, and management's assessment of the risk posed by the e-banking system as a whole or by the various subcomponents. This risk analysis should evaluate the transactional capabilities of the e-banking system (e.g., funds transfer, bill payment, loan origination, account aggregation, etc...), and the sensitivity and value of the stored e-banking data.

Customers may be registered for remote banking services by one of the following means:

- Physical presence
- Registered letter
- Electronically via a Website.

Identification should be performed by requiring that the customer presents one or more legitimate credentials issued by government or other trusted issuer organisations.

In case of e-registration, appropriate measures should be in place to control the e-banking system connection such that unknown third parties cannot displace known customers.

Guideline 2.4: Where national regulations and financial institutions allow customers to register for banking services through the use of a PKI certificate issued by the government or other trusted issuer organisation, the KYC used to register the customer for the certificate must be no less than that which is used by financial institutions in that country.

Additional information: In case customers use certificates for their identification when registering for a (remote) banking service, the procedure at the registration authority verifying the identity of the customer should be under control of and/or supervised by the financial institution and accepted by the financial supervisory authorities.

Some countries may forbid the delegation of the customer identification to third parties; other countries allow this delegation to certification authorities if they provide the customer with a qualified certificate (or other certificate agreed between the two parties on a commercial basis) and if there has been physical identification at the registration authority before delivery of the certificate.

Guideline 2.5: Financial institutions should have controls to ensure that credentials are distributed to customers in a way that is trustworthy. The level of trust in the customer's identity should be maintained throughout the customer relationship.

Additional information: Financial institutions should keep control of addressing information (physical or e-) which are used for communication with the customer. Call centre staff should be well informed and educated in the procedures that are used for sending out e.g., new passwords or authentication devices. All sending of new passwords or devices should be logged, and the financial institution might consider giving the customer a notification on another communication channel (e.g., sending an SMS when a new OTP-device is going to be sent by mail).

Guideline 2.6: Customers should only have access to their own accounts. In case of an agent acting on behalf of a customer, financial institutions should ensure that the appropriate mandate is in place, and the agent is authenticated and authorisation given, before access to the e-banking services are assigned.

Additional information: Any addition, deletion or change of an individual, agent or system to an authentication database should be duly authorised by an authenticated source. Authenticated e-banking sessions remain secure throughout the full duration of the session or in the event of a security lapse the session should require re-authentication. Authentication databases that provide access to e-banking customer accounts or sensitive systems should be protected from tampering and corruption. Any such tampering should be detectable and audit trails should be in place to document such attempts.

5.4 ENTITY AUTHENTICATION

Principle 3: Financial institutions providing e-banking services should take appropriate measures to provide mutual authentication between themselves and their customers with whom they conduct business remotely.

Purpose: It is essential for banking services, more in particular for remote banking where physical verification is impossible, that "transacting parties" mutually authenticate each other, in other words mutually verify the identity of the entity the other claims to be.

Implementation Guidelines:

Guideline 3.1: Financial Institutions should authenticate registered customers as the first step in a remote banking session. The mechanisms used to authenticate the registered customer should be appropriate to the risks identified.

Additional information: If the customer merely wants to check his/her bank balance, the authentication process does not need to be as sophisticated as is necessary if a credit transfer or securities order is involved. Financial institutions can use a variety of methods to establish authentication, including PINs, passwords, smart cards, biometrics. These authentication methods range from a single factor (e.g., a password) to a dynamic two-factor (e.g., token and a dynamic one-time password for each authentication session). Moreover, in case of two-factor authentication, both factors should be independent such that a compromise of one of them, does not impact the other. Obviously, multi-factor authentication generally provides a higher confidence level.
The decision-making processes for which mechanisms to implement could be guided by the EPC Customer to Bank Security Threat Assessment (see [10]).

Guideline 3.2: Financial Institutions should employ a mechanism which allows their authentication by the customer throughout a remote banking session.

Additional information: It is recommended to use the SSL/TLS/https protocol for establishing a secure network channel. Hereby the usage of extended validation certificates, signed by a recognised, industry standard certification authority, is an emerging good practice.

5.5 TRANSACTION SECURITY

Principle 4: Financial Institutions offering e-banking services should take appropriate measures to provide transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.

Purpose: To ensure that authorisation of remote payment transactions is achieved as evidence to all parties involved in an e-banking transaction (see [5]).

Implementation Guidelines:

Guideline 4.1: Financial Institutions should offer adequate mechanisms to protect the integrity of data and to prove authenticity of the data origin throughout a remote banking session.

Additional information: Financial Institutions should offer to customers a payment mechanism capable of providing data integrity and authenticity of data origin. For instance transactions involving movements of money should be authenticated with strong authentication methods.
Financial Institutions should monitor the usage of the issued payment mechanism and take appropriate action in case anything suspicious happens with respect to the remote transaction. Customers trying to access the e-banking service with software or hardware that cannot fulfil technical or algorithmic requirements should be refused admission and be instructed to upgrade.

Guideline 4.2: Financial institutions should offer adequate mechanisms to prevent replay of transactions.

Additional information: It should not be possible to capture transactions and to re-submit them into the system. Therefore transaction authentication should include a dynamic factor.

Guideline 4.3: Financial institutions should identify transactions with particularly high risk and make more screening/controls before these transactions are accepted to be executed.

Additional information: Examples of situations that might require additional screening include:

- Customer is emptying his/her account (or using his entire credit limit) for a transaction to a beneficiary to whom this customer never has made any payments before;
- Transaction with large amount going to an unusual place;
- Transaction to credit account suspected of being a money mule;
- Indications of session hi-jacking.

Guideline 4.4: Financial institutions should use appropriate logging to provide proof of authenticity and accountability of remote e-banking transactions.

Additional information: To support proof of authenticity and accountability, financial institutions should pay special attention to a reliable audit trail (see also Principles 7 and 8) and auditable procedures. The ECBS TR409 [6] provides further guidance on this matter.

Guideline 4.5: Customers should be informed of security risks when using the e-banking system concerned and should be advised on appropriate security behaviour.

Additional information: Further guidance on customer education may be found in [16].

Principle 5: Financial institutions providing e-banking services should take appropriate measures to protect sensitive data in e-banking transactions.

Purpose: To ensure that sensitive data cannot be compromised or used by unauthorised persons. Sensitive data includes all information listed under b) through f) in the classification provided in chapter 3.

Implementation Guidelines:

Guideline 5.1: Financial institutions should use mechanisms to protect the confidentiality of sensitive information passed between the e-banking customer and the bank.

Additional information: The protection of the confidentiality of sensitive information should be appropriate to the impact of the risk of unauthorised exposure. The requirement for confidentiality should be determined by a “value and risk assessment” of the data – for example, a user’s identification (e.g., account number) is less sensitive than their authentication data (e.g., password). For exchanging sensitive information it is recommended to use the SSL/TLS/https protocol for establishing a secure network channel. In case of highly confidential data, it is recommended to encrypt the data. Guidance on encryption and the usage of algorithms and associated parameters as key lengths may be found in [8].

Guideline 5.2: Financial institutions should ensure that the logical access control of their host e-banking platforms and their overall security are sufficient to prevent unauthorised access to sensitive data.

Additional information: These logical access controls should be subject to review and tests to ensure that they are operating effectively. A system should also be proven against information leakage, i.e., whether a customer can, intentionally or unintentionally, access information of other customers. A common method used by the industry is to conduct external penetration tests of the e-banking host platform.

Guideline 5.3: Measures should be taken to help prevent the customers themselves disclosing their own sensitive data to third parties.

Additional information: E-banking customers are subject to a wide range of threats including Trojans and phishing attacks (see [10]). Financial institutions should contribute to raising customer awareness on these threats so that they do not fall victim (see also Principle 11). For instance, they should work to make their customers aware of risks related to phishing. Co-operation with consumer protection organisations, or organisations working for information security should be considered. Furthermore, Financial Institutions should not send e-mail to their customers with links to internet addresses (URLs) which may be mistaken for phishing.

Financial institutions should also design their e-banking service offering in such a way that it does not provide inconsistencies that would help an attacker launch a social engineering attack against the Customer (seee [17]).

Financial institutions should further encourage their customers to keep their computers well updated with anti-virus software, anti-spyware, operating system patches etc. They should also consider giving warnings against use of computers located in hostile or rogue environments.

5.6 SECURE OPERATIONS

Principle 6: Financial Institutions providing e-banking services should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.

Purpose: In order to minimise the opportunities for fraud financial institutions need to control authorisation and access privileges. Failure to provide adequate authorisation control could allow individuals to alter their authority, circumvent segregation and gain access to the e-banking system which they are not privileged or qualified for.

Implementation Guidelines:

Guideline 6.1: Financial Institutions should have appropriate authorisation controls and access privileges while ensuring effective segregation of duties for their e-banking services and underlying infrastructures and supporting processes.

Additional information: Systems should be designed to ensure that no employee or outsourced service provider could enter into the e-banking system or authorise/manipulate a transaction. E-banking systems should be tested to ensure that segregation of duties cannot be compromised. As an example segregation should be maintained between developers and administrators of the e-banking systems. Financial institutions should also maintain an up to date register relative to the rights of the users (e.g., when an administrator leaves the function, he/she must be deleted and replaced). A Role Based Access Control (RBAC) offers the appropriate system to address these requirements.

Emergency procedures, required in order to confer authority to different people when the principals are unable to perform their duties, should produce sufficient logs and notifications to ensure that management is aware of the substitution and is able to control or revoke the substitution.

Guideline 6.2: Financial Institutions should educate their business customers on the appropriate segregation of duties within their organisation more in particular to mitigate against fraudulent payments being initiated.

Additional information: Further guidance is provided in IS 2700x which Financial Institutions may use to further educate the business to implement appropriate information security management systems.

Principle 7: Financial institutions providing e-banking services should ensure that appropriate measures are in place to protect the data of e-banking transactions, records and information.

Purpose: To ensure that the long-term storage of transaction data is sufficient to preserve the integrity, confidentiality and availability of these transactions such that they can be used as evidence in dispute resolution processes and both criminal prosecutions of fraudsters.

Implementation Guidelines:

Guideline 7.1: Financial institutions should protect the integrity of stored data.

Additional information: A range of methods are available to support this requirement. Effective methods are for this data to be written to permanent media, which can then be physically protected, or alternatively the data can be protected with the help of hardware and software measures which prevent alterations.

As an example, the compromise of customers personal information or the security information they use to log in to e-banking services, allows fraudsters to access customer accounts to cause financial loss.

Guideline 7.2: Financial institutions should protect the confidentiality of sensitive stored data.

Additional information: Measures taken to preserve confidentiality should be appropriate with the sensitivity of the information being stored. In case of highly confidential data, it is recommended to encrypt the data. Guidance on encryption and the usage of algorithms and associated parameters as key lengths may be found in [8].

Guideline 7.3: Financial Institutions should ensure the availability of the stored data. This also includes the retention of stored data in line with regulatory requirements.

Additional information: The strategy chosen to preserve the integrity of the transaction data must be sufficient to meet the lifetime for which the data should be stored. In the case of cryptographic methods of protection thought should be given to key lengths over the lifetime that the data is expected to be stored and its integrity preserved.

Guideline 7.4: Financial institutions should have appropriate processes and methods in place for their systems and application development, testing and maintenance.

Additional information: Financial Institutions should implement appropriate measures to segregate and protect their systems such as the use of firewalls between the Internet, the e-banking service and the core applications. E-Banking processes are to be designed in a manner that minimizes the amount of sensitive data that is stored/transmitted in vulnerable environments.
Methods used for the secure development and maintenance of web applications should embrace internationally recognized web application development methods such as the ones defined by the Open Web Application Security Project that amongst others address the top ten most common web application security flaws [17]. Financial Institutions are encouraged to regularly evaluate their e-banking applications relative to the vulnerabilities and recommendations stated in the OWASP documentation.

Principle 8: Financial Institutions providing e-banking services should ensure that clear audit trails exist for all e-banking transactions.

Purpose: Accurate and consistent audit trails will help to provide the substantive evidence of how customer payments have been executed within financial institutions. They will provide the necessary additional information to the payment transaction logs in order to provide the complete history of a payment.

Implementation Guidelines:

Guideline 8.1: Financial institutions should retain and protect the integrity of the audit trail of the remote banking transaction interactions. The audit trail records should be kept in line with regulatory requirements and according to the requirements following risks analyses.

Additional information: These should be given the same level of protection as the payment transaction logs, under guideline 7.2 and retained for similar periods to those under guideline 7.2. Consideration should be given to ensuring that the time clocks of systems across the entire payment chain should be synchronised to a common time source in order to support later reconciliation of log and audit trails.

Guideline 8.2: Audit trails should log every remote banking transaction related interaction. This includes every update (or attempt to make an update) of customer data related to e-banking.

Additional information: As an example, when a bank clerk changes the mobile phone number or e-post address of a customer, or requires a new one time password device, there must be an audit trail present which can be traced down to the individual performing the task.

Principle 9: Financial Institutions providing e-banking services should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.

Purpose: Financial institutions should develop and maintain a managed process for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity. They should develop recovery objectives that reflect the risk they represent to the operation of the financial system. As appropriate, such recovery objectives may be established in consultation with, or by, the relevant financial authorities and their suppliers.

Implementation Guidelines:

Guideline 9.1: Business continuity management should be an integral part of the overall risk management programme of financial industry participants and financial authorities. Business continuity management policies, standards and processes should be implemented on an enterprise-wide basis or, at a minimum, embedded in an organisation's critical operations.

Additional information: A framework should be implemented for reporting to the board and senior management on matters related to business continuity, including implementation status, incident reports, testing results and related action plans for strengthening an organisation's resilience or ability to recover specific operations.

Confusion can be a major obstacle to an effective response to an operational disruption. Accordingly, roles, responsibilities and authority to act, as well as succession plans, should be clearly articulated in an organisation's business continuity management policies.

Guideline 9.2: Financial institutions should develop recovery objectives that reflect the risk they represent to the operation of the financial system. As appropriate, such recovery objectives may be established in consultation with, or by, the relevant financial authorities.

Additional information: Events that can cause interruptions (e.g., Denial of Service attacks, see [10]) to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security. Financial institutions should consider the extent to which they pose such a risk and augment their business continuity management where they determine that a disruption of their operations would affect the operation of the broader financial system. Furthermore, they should establish recovery objectives that are proportionate to the risk they pose to the operation of the financial system. Recovery objectives should identify expected recovery levels and recovery times for specific activities.

Guideline 9.3: Financial institutions should include in their business continuity plans procedures for communicating within their organisations and with relevant external parties in the event of a major operational disruption.

Additional information: Accordingly, and also because of the added pressure that is often associated with decision-making during a major operational disruption, the business continuity plans of financial industry participants and financial authorities should incorporate comprehensive emergency communication protocols and procedures. A crisis may require the use of secure communications using specialised "secure" telephones, faxes, and emails. Financial institutions should regular update the calling trees and other contact information and should test the calling trees periodically.

Guideline 9.4: Financial institutions should test their business continuity plans, evaluate their effectiveness, and update their business continuity management, as appropriate.

Additional information: Testing, which can take many forms, should be conducted periodically, with the nature, scope and frequency determined by the criticality of the applications and business functions, the organisation's role in broader market operations, and material changes in the organisation's business or external environment. In addition, such testing should identify the need to modify the business continuity plan and other aspects of an organisation's business continuity management. An independent party, such as internal or external audit, should assess the effectiveness of the organisation's testing programme, review test results and report their findings to senior management and the board. It is important, therefore, that testing programmes should involve all personnel who are likely to be involved in responding to major operational disruptions. In addition to ensuring that business continuity plans are evaluated and updated as necessary, testing is also essential for promoting awareness, familiarity and understanding among key personnel of their roles and responsibilities in the event of a major operational disruption.

Principle 10: Financial Institutions providing e-banking services should develop appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal and external attacks that may hamper the provision of e-banking systems and services.

Purpose: To ensure that information security events and weaknesses associated with e-banking systems and services are managed appropriately in order to allow timely corrective actions in a consistent and effective approach.

Implementation Guidelines:

Guideline 10.1: Providers should ensure that detection and monitoring systems and methods are in place. Moreover, information security events and weaknesses associated with information systems should be reported through appropriate management channels as quickly as possible, to allow timely corrective actions to be taken. Finally, all relevant communication should be organised in a timely manner to limit the damage including customer information as needed.

Additional information: A formal information security event / weakness reporting procedure should be established. All employees, contractors and third parties should be made aware of their responsibility to report to the designated point of contact and according to the procedures the different types of events and weaknesses that might have an impact on the security of the organisation assets. More information about the reporting of information security incidents can be found in ISO/IEC TR 18044.
Further guidance on customer information is provided under principle 11.

Guideline 10.2: Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents or weaknesses.

Additional information: A formal information security incident response and escalation procedure setting out the action to be taken on receipt of a report of an information security event should be established. More information about the management of information security incidents can be found in ISO/IEC TR 18044 [14].

Guideline 10.3: There should be mechanisms in place to enable information security incidents to be quantified and monitored.

Additional information: The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents. The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security guidelines review process.

Guideline 10.4: Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal) evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Additional information: Internal procedures should be developed and followed when collecting and presenting evidence for the purpose of disciplinary actions. In general the rules for evidence cover the admissibility (whether or not the evidence could be used for instance in court) and the weight (the quality and completeness). When an information security event is first detected it may not be obvious whether or not the event will result in a court action Therefore it is advisable to be careful that necessary evidence is not destroyed intentionally or accidentally and to involve professionals (e.g., a lawyer or police) in an early stage. Organisations should also be aware that collecting evidence may transcend their own organisation or jurisdictional boundaries and hence they need to be entitled to do so.

Principle 11: Financial Institutions providing e-banking services should ensure that adequate information is provided on their websites to allow potential customers or customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions. More in particular, financial institutions intending to engage in cross-border activities should provide sufficient disclosure on their web site to allow potential customers to determine next to the bank's identity, also the home country, and regulatory license(s).

Purpose: To protect the customer against fraudulent sites. The provision of information describing the bank is an important safeguard against services provided by organisations which fraudulently adopt the same "look and feel" as the bank's service in order to capture the customer's authentication data and financial information.

Implementation Guidelines:

Guideline 11.1: Information related to e-banking services should be timely and comprehensive enough to allow customers to have a good evaluation of service levels and risks.

Additional information: Financial institutions have the responsibility to provide potential customers or customers with necessary information to identify, control and monitor any risks associated with the e-banking services. On-going customer information and updates on security issues related to electronic channels (e.g., security instructions as part of e-banking agreement, awareness campaigns of threats and means how customers can protect themselves, etc...) should be provided.

Guideline 11.2: A help desk service should be available to potential customers or customers via e-mail or phone during sufficient time frames.

Additional information: Financial institutions should include a Q&A sheet on their web site.

Guideline 11.3: Financial institutions have the responsibility to provide potential customers or customers with appropriate information about risks and liabilities associated with the e-banking services.

Additional information: This includes the responsibility of the financial institutions to inform their customers of e-banking services on their responsibility and due diligence with regard to devices and software under their sole control.

Financial institutions should further inform exposed customers without delay and provide their contribution to the corrective measures to limit the damage.

Furthermore, financial institutions should support and educate their customers to identify and report suspicious situations or behaviour.

Principle 12: Financial Institutions providing e-banking services should take appropriate measures to ensure adherence to the jurisdictions to which they are providing e-banking products and services.

Purpose: Although the Payment Services Directive [5] is generating much greater harmonisation and commonality of approach there will continue to be other important legislation which is different in each jurisdiction. It is essential that the financial institutions respect this legislation in those countries in which they offer e-banking services to their customers and wherever those services are hosted and operated.

Implementation Guidelines:

Guideline 12.1: All relevant statutory, regulatory, and contractual requirements and the organisation’s approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organisation.

Additional information: There are increasingly cooperative arrangements to allow service providers operating in multiple jurisdictions to understand and recognise the nationally relevant legislation and regulation that they will need to comply with. These arrangements will supplement but not replace Financial institutions to adopt their own compliance programmes.

Guideline 12.2: Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

Guideline 12.3: Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

Additional information: It will be essential to ensure that the appropriate obligations are placed on any service providers who might be contracted by a Financial Institution to deliver any component of their e-banking services.

Guideline 12.4: Cryptographic guidelines should be established in compliance with all relevant agreements, laws, and regulations.

Additional information: Appropriate strengths of cryptography (see [8]) should be implemented in all e-banking service offerings which also meet the applicable regulations.

6 MAPPING SECURITY THREATS ON SECURITY PRINCIPLES

This section aims to provide a high level mapping of the principles in relation to their circumvention of the threats as identified in EPC publication "*Customer to Bank Security Threat Assessment* [10], related to remote e-banking services. Clearly, this mapping is only a high level view of the most important matching without dealing with any detail. Moreover, it should be noted that the document on the threats mentioned above mainly focuses on external threats while some of the principles in the present document are broader in scope since they also address internal threats of financial institutions. As such, the matrix below should be regarded as a subset of the full mapping of principles against threats, namely limited to the external threats identified in [10].

Threats/ **Principles**	**Phishing**	**Pharming**	**Trojan horse**	**Man-in-the-middle**	**Denial of service**	**Data Attacks***
Principle 1	X	X	X	X	X	X
Principle 2	X	X	X	X		
Principle 3	X	X	X			
Principle 4	X	X	X	X		X
Principle 5	X		X	X		X
Principle 6						X
Principle 7						X
Principle 8						X
Principle 9					X	
Principle 10	X	X	X	X	X	X
Principle 11	X		X	X		
Principle 12	X	X	X	X	X	X

Table 1: Mapping the principles on the "external" threats

*The original threat "Botnets" as described in [10] has been replaced by Data Attacks in this table for botnets allow a combination of attacks on sources of (customer) data.

7 CONCLUSIONS

Remote banking is becoming increasingly important for the delivery of banking services to customers. Bank customers today expect to be able to interact with their bank on a remote basis at almost any time and trust that the banks provide the services in a safe way. These guidelines provide an overview of the security measures that need to be implemented by a financial institution (bank or service provider) on a remote basis. When using such guidelines, care must betaken to what specific demands or risks financial institutions are faced to in particular markets or to the specific product offering. Eventually, a proactive based approach to the various risks and threats associated with remote banking is necessary in order to protect the business and the customer.

8 REFERENCES

[1] APACS (UK)**:** *Secure Remote Banking Services: Principles*, Version 1.0, August 2002.

[2] APACS (UK)**:** *Secure Remote Banking Services: Generic Practices*, Version 1.0, December 2002.

[3] Basel Committee on Banking Supervision: *Risk Management Principles for Electronic Banking*, July 2003.

[4] Basel Committee on Banking Supervision: *Management and Supervision of Cross-Border Electronic Banking Activities*, July 2003.

[5] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on *Payment Services in the Internal Market.*

[6] ECBS TR 409: *The Use of Audit Trails in Security Systems, Guidelines for European Banks*, 2001.

[7] ECBS TR 411: *Security Guidelines for E-Banking - Application of Basel risk Management Principles*, Version 2, August 2004.

[8] EPC 342-08v1.1: *Guidelines on Algorithm Usage and Key Management*, November 2008 (former ECBS TR 406)

[9] EPC 281-06v1.0: *Customer to Bank Security Survey: Summary of Results*, August 2006.

[10] EPC 052-08v1.2: *Customer to Bank Security Threat Assessment*, February 2008.

[11] Finansrådet (DK): *Draft Codex on IT-security in self-service systems*, November 2002.

[12] FFIEC: *E-Banking, IT Examination Handbook*, August 2003.

[13] ISO TR 13569: *Banking and related financial services – Information Security Guidelines,* 2006.

[14] ISO/IEC TR 18044: *Information technology - Security techniques - Information security incident management,* 2004.

[15] ISO/IEC 27001 – 27007: *Information Technology - Security Techniques - Information Security Management Systems*, 2005-2008.

[16] Monetary Authority of Singapore (MAS): *Internet banking and technology risk management guidelines*, Version 3.0, June 2008.

[17] OWASP: http://www.owasp.org

9 ANNEX 1: ABBREVIATIONS

Abbreviation	Term
CERT	Computer Emergency Response Team
C2B	Customer to Bank
DoS	Denial of Service
ECB	European Central Bank
EPC	European Payment Council
ESTF	Eurosystem Task Force
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICAO	International Civil Aviation Organisation
ISMS	Information Security Management System
KYC	Know Your Customer
OTP	One Time Password
OWASP	Open Web Application Security Project
PIN	Personal Identification Number
RBAC	Role Based Access Control
SEPA	Single Euro Payments Area
SLA	Service Level Agreement
SMS	Short Message Service
SSL	Secure Socket Layer
TAN	Transaction authentication number
TLS	Transport Layer Security
URL	Uniform Resource Locator

10 ANNEX 2: TERMINOLOGY

Banking Services: means services provided by licensed regulated financial institutions or their agents. Typically this may be interpreted as management of accounts (e.g., current, credit card, savings) and communication with financial institutions including, but not necessarily limited to:

- brochure distribution
- marketing literature distribution
- registration or application form distribution
- terms and conditions literature distribution and where an authentication method has been established:
- account opening
- balance and transaction reporting
- account management enquiries
- setting up and management of mandated payment Instructions including direct debit instructions and standing orders
- generation of pre-mandated payment instructions, including bill payment services
- ad hoc instructions including payments
- purchase, exchange and clearing of electronic cash
- issuing, depositing and clearing of electronic cheques
- purchase and sale of currency
- issuing of banker's credit references
- electronic signature verification services.

Compromised: the authentication credentials have been lost or are suspected of having become known to, or available for use by, an unauthorised third party – thereby undermining any authentication based on those credentials.

Confidentiality: only the intended recipient(s) and sender are able to apply or use the banking transaction or related information. An intercepted message should remain meaningless to any interceptor.

Customer: means an entity (person or organisation) with an account with a financial institution providing (e-)banking services.

Customer Authentication: reasonable assurance to the financial institution that the individual undertaking a banking transaction is the correct registered user.

Financial institution: a bank as a supplier of remote e-banking services or any third parties specifically employed by the financial institution in the provision of those services.

Financial institution Authentication: a reasonable assurance to a customer or relying party that the e-banking system being accessed or addressed is under the control of the intended organisation.

Integrity: information has not been amended, corrupted, lost or duplicated.

Registration: the process where a customer enters into a contractually binding arrangement with a financial institution for remote banking services.

Registered Customer: a user who has successfully completed the registration process with a financial institution. In the corporate environment it is construed as a person or persons communicating on behalf of their employer with a financial institution where no contractual relationship exists between the financial institution and the individual, but between the financial institution and the individual's employer.

Remote: an interaction between a financial institution and a device physically operated by the customer. It means the customer and their financial institution communicate at a distance not involving face-to-face physical presence of the parties (internet, mobile, phone, TV,…).

Remote e-Banking Services: are services provided by licensed, regulated financial institutions through devices operated by the customer, excluding automated teller machines because they are under the financial institution's direct control and management. For the purposes of this document, a Remote e-Banking Service is construed as:

- a dedicated banking service for which the customer has explicitly registered;
- which requires the authentication of the customer;
- using devices and/or software which may be supplied by the financial institution but are under the control of the customer when using this banking service (e.g., home PC, mobile phone, TV,...).

Remote Banking Session: a communication interaction commencing with the mutual authentication process and terminating with either the user explicitly logging off the remote e-banking service or a termination in the interactive session. Other forms of electronic communication such as e-mail, although not interactive, should be interpreted as a single complete remote e-banking session when it is within the context of a remote e-banking service.

Remote Banking Transaction: a request for information or an instruction issued by the registered customer, and the response from the financial institution.

Two-factor authentication: a reasonable assurance about the identity of an entity based on a combination of something this entity has with something this entity knows.

11 ANNEX 3: CUSTOMER TO BANK SECURITY SURVEY

This European country survey [9] focused on the authentication of customers and the authentication of the credit transfers and direct debits payments. Hereby following payment types and services by banks were deemed out of scope for this survey:

- Card payments and card payments security.
- Paper and cheque-based channels.
- Phone banking (as far as this is not migrating to internet banking).
- Online cheque payments.

This security inventory mainly dealt with the authentication issues of the customer to bank dialogue and on the bank to customer dialogue with the focus on the customer's access to the information provided by the bank. The bank-to-bank dialogue was considered to be sufficiently well defined and under control of oversight departments and was not in scope.

The survey has found many common themes in how customers are authenticated across all the countries surveyed, the most striking of which is the degree and depth of attention being given by all countries surveyed to both current authentication methods and for future customer authentication strategies to migrate – if necessary - to stronger solutions.

There are however distinct differences at the detailed level. Many of these differences emerge from the way banking services are offered to customers in differing domestic regions, and how banks segment their market and the way the customer proposition and experience for authentication for each segment is presented in each country. These differences are compounded by very different obligations placed on the banks within each country by national banking associations and/or regulatory authorities.

The additional factor giving rise to differences in both approaches to authentication and/or the speed of migration is the very differing perceptions of the currently prevailing solutions, threats and the actual consequences in terms of fraud losses and customer experience within each country. These factors shape the risk appetite and risk assessment within each country and within each bank on migration strategies and timelines and specific solutions.

At the consumer level static user credentials are still the most common method of authentication across the survey respondents; although these are often submitted in partial form or through methods other than direct keyboard entry, or supplemented by other simple 2-factor methods such as iTANs. In all cases where static credentials are currently the primary authentication strategy plans are being drawn up for a migration to methods solutions based on 2-factor authentication. Here the EMV based CAP architecture has a strong degree of support amongst several countries/banks.

There is as yet no wide scale interoperability of authentication strategies in the consumer market. This is because the primary relationship between the bank and their customer is bilateral, with each bank accepting the liability for knowing its own customers. This is unlikely to change in the near future. This is true even in the case of the EMV based CAP solution where there is scope for much greater interoperability through the use of common readers and common authentication application on EMV payment cards. However, even in this case the dynamic authentication provided by the EMV payment card issued to the customer by their bank that is read in the EMV compliant reader can only be validated by the bank issuing the card to the customer.

It is not yet clear what the future impact on customer authentication will be in those countries whose citizens are/will be issued with an electronic ID card with a digital signature capability. There remain many issues to resolve (for example: customers may need a card reader and/or software installed; lack of European harmonisation; agreeing liability arrangements, etc.) if banks were to consider accepting these credentials as a form of authentication to their services.

There is evidence from the survey that business and corporate requirements for authentication are met by a wide range of solutions in what is a very competitive market. There is much closer alignment between countries in the selection of solutions adopted for the large enterprises which are strongly characterised by the adoption of PKI solutions. The method of use and issue of these PKI credentials to customers and the degree of standardisation varies across Europe. In several countries there is a high degree of standardisation through domestic standards and/or architecture frameworks allowing solutions offering a relation between corporate customers and a number of banks (multilateral relationships). In other countries there is a much less uniformity. The bank to enterprise in these countries is a bilateral commercial relationship not dissimilar to that which pertains in the consumer market.

The survey concludes that a number of countries provided information on future plans. Most commonly, these involve a migration toward a hardware-based two-factor authentication solution. The use of EMV cards with the MasterCard CAP architecture seems to be a popular choice. Also the fact that the SEPA Cards Framework requires migration to debit cards with an EMV-chip will strengthen the opportunities for migration.

12 ANNEX 4: CUSTOMER TO BANK SECURITY THREAT ASSESSMENT

Although the report [10] aimed to provide a business impact per threat type it proved to be very difficult to get an overall appreciation of the business impact today caused by attacks based on the threats described in the Customer-to-Bank environment.

The main reasons for this were twofold:

- The amount of data which is available on significant losses to financial institutions is very limited and difficult to access;
- There is hardly any info available on the kind and number of customer attacks, the methods used, the type of customers targeted.

Hence what follows is to be conceived as the overall perception of the contributors to this report and aimed to highlight the overall potential consequences to the business over time.

It is clear that the threat environment in the C2B area remains significant more in particular in the customer space. However, it is also very important to notice that there are a number of limiting factors which help to contain the potential problems caused by the threats described. Those factors can be listed as follows:

- Although some of the attacks described are technical feasible, the difficulty remains for the attackers to actually extract value out of these attacks because of the difficulty in recruiting sufficient “Money Mules” to launder the proceeds of successful attacks;
- There is a tradition and long-term expertise in the financial industry of fraud monitoring and detection which makes this environment less attractive to potential attackers compared to some others;
- Increasing awareness about the threats within the banking environment.

To address C2B threats in an efficient way it is recommended to apply a broad range and combination of strategies as follows:

- Education/awareness of all parties involved in the C2B area but with a special focus to customers;
- Encourage customers to implement all possible measures which are advised by banks;
- Strong authentication methods including out of band transaction signing that survive the “dirty” environments[1];
- Appropriate secure good practices and standards to provide reasonable assurance of the availability of C2B services;

[1] A “dirty” environment is one in which it is assumed that it could have been compromised with stealthy undetectable Trojan and key stroke loggers, or one in which one should have no confidence in its level of security and protection

- Strong management and control of operations and services offered by third party processors;
- Enhanced fraud detection and monitoring techniques;
- Strong international co-operation of CERTs and law enforcement bodies.

Finally, it is recommended to use this threat and vulnerability assessment as a basis to guide the implementation and design of any new European wide internet based payment scheme.

13 ANNEX 5: MAPPING EPC C2B PRINCIPLES ON ISO/IEC 27002

This annex aims to provide a high level mapping of the EPC C2B principles specified in the present document onto the security controls defined in ISO/IEC 27002 [15]. It shows at a glance for which principles it is useful to consult the ISO standard to receive further guidance and indirectly via Table 1 how the ISO standard helps to address the threats identified.

EPC Principles **ISO 27002 Principles**	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**
Security Policy	X											
Organising Information Security	X											
Asset Management		X				X	X	X				
Human Resources Security						X						
Physical and Environmental Security	X											
Communications and Operations Management	X	X	X	X	X	X	X	X			X	
Access Control		X	X			X						
Information Systems Acquisition, Development and Maintenance	X	X	X	X	X	X	X	X			X	
Information Security Incident Management										X		
Business Continuity Management									X			
Compliance	X	X									X	X

Table 2: Mapping the EPC C2B principles on the ISO/IEC 27002 principles