CANADIAN PAYMENTS ASSOCIATION

ASSOCIATION CANADIENNE DES PAIEMENTS

STANDARD 018

PAYMENT ITEM INFORMATION SECURITY STANDARD

Standard 018 – Payment Items Information Security Standard

Implementation and Revisions

Implemented

Amendments

Standard 018 – Payment Item Information Security Standard

Table of Contents

Standard 018 – Payment Item Information Security Standard

1. Introduction and Scope

This Standard sets out the minimum security requirements for the handling of electronic and Cheque Image Payment Items ("Items"), that are Exchanged, Cleared or Settled through the Automated Clearing Settlement Systems (ACSS), with respect to their confidentiality, integrity, availability and non-repudiation.

This Standard applies to Items whenever such information is used by or on behalf of a Member for any of the Process Areas defined in Section 4, below. As such, where a Member has a third party or other agent perform any process or transmit data that Member is accountable for ensuring that the third party or other agent adheres to the requirements set out in this Standard.

This Standard relies on authoritative sources for the creation, management, and examination of a security infrastructure such as:

- Federal Financial Institutions Examination Council (FFIEC) Information Security IT Examination Handbook, July 2006
- ISO/IEC 27002:2013 Code of Practice for Information Security Controls
- ISO/IEC 27015:2012 Information Security Management Guidelines for Financial Institutions
- OSFI Cyber Security Self-Assessment Guidance

2. Definitions

In this standard,

2.1 "Degaussing" refers to the application of magnetic force of sufficient power to erase all data on a given magnetic data storage device.

2.2 "Originating Institution" means the Member originating the Item to another Member for the purpose of Exchange, Clearing or Settlement.

2.3 "Principle of Least Privilege" means the minimum possible privileges to permit a legitimate action, in order to enhance the protection of data and functionality from faults and malicious behaviour.

2.4 "Receiving Institution" means the Member receiving the Item from another Member for the purpose of Exchange, Clearing and Settlement.

2.5 "Secure Environment" means a system which implements controlled and protected storage and use of information.

2.6 "Security Overwriting" refers to overwriting the storage media, including unused portions thereof, with random and patterned data, with the intent of making the recovery of the original data virtually impossible.

2.7 "Security Perimeter" refers to the area bounded by physical area in which a Member can exert complete control over its computer hardware, network hardware, premises, and Images including areas where Members use third party processors.

2.8 "Replay" refers to the repeat of an item that has already been processed.

2.9 "Transmission" means the exchange of Items between physical locations (e.g. between Direct Clearer sites, between regional and central sites, between Direct Clearers and Indirect Clearers, and between CPA Member Institutions and clients.)

Standard 018 – Payment Item Information Security Standard

3. Security Principles

Each Member who originates or purports to originate, transmit or Exchange, or store Items shall ensure such origination, transmission or Exchange, and storage takes place in a Secure Environment and that adequate controls and processes are in place to maintain the integrity, confidentiality, non-repudiation, and availability of Items.

In particular, the following security principles shall be adhered to in the handling of Items:

a) Least Privilege – Access to information shall be based on a need-to-know basis appropriate for the position in the organization.

b) Audit Information – All security significant event information shall be retained to preserve a record of activities to provide future accountability and proof of any decisions and actions.

c) Hostility – The organization and its systems operate and interact in a hostile environment. Unless proven otherwise, systems and networks should be assumed to be non-secure and should not be trusted.

d) Protect against Insider as well as outsider threat – Equal level of protections shall be applied to threats, regardless of the threat origination vector (e.g., insider or outsider).

e) Fail-Safe – Systems should fail in such a way that they deny access rather than grants access.

f) Consistent Security Functions – Members require that externally provided critical services, such as data processing, transaction handling, network services, and software generation, receive the same level of control and information protection as those activities processed within the institution itself.

g) Default to the highest data sensitivity classification – If an Item, document, file or database contains various sensitivity classifications, it shall be treated according to the highest classification category of the information it contains.

h) Segregation of duties – Responsibilities in relation to origination, receiving, storage, transmission, retrieval, and deletion of Items shall be allocated to separate individuals.

i) Dual Control – The organization shall, at a minimum, ensure a dual control position in handling of Items according to its risk tolerances (e.g., that the processing of financial information or transaction and the verification of the outcome would be performed by different personnel, or by a person and an automated process, respectively).

j) Responsibility – All Members are responsible for the security of information systems and networks under their control.

k) Response – Where possible, Members shall act in a timely and co-operative manner to prevent, detect and respond to security incidents.

4. Process Areas

The process areas set out in this Standard are:

4.1 Origination

The origination process speaks to the creation of an Item (e.g., an ISO 20022 Item in the ISO 20022 format is described in the ISO AFT Usage Guidelines.)

4.2 Receiving

The receiving process speaks to the retrieval and processing of an Item (e.g. an EDI Item in the format described in Standard 023).

4.3 Storage

The storage process involves recording Items on media for short-term use.

4.4 Transmission

The transmission process is the exchange of Items between physical locations.

4.5 Archival

The archival process moves or copies Items to a repository used for long-term storage and indexing of the messages or files and associated information at a Member branch or data centre. The archival process ends when an Item is deleted.

4.6 Retrieval

The retrieval process involves a request for the retrieval of a specific Item from an archive, which is received and authorized for processing. The retrieval process ends when the Item is retrieved and delivered to the entity requesting the retrieval.

4.7 Deletion

The deletion process involves the erasure of Items. The deletion process is complete when no further access to the Item is possible.

4.8 Back-up / Removable Storage

The back-up process creates and retains copies of Items.

5. Security Requirements

The requirements regarding processes for Items in this section are organized under the following security headings:

A. Logical and administrative access control;
B. Malicious Code;
C. Logging;
D. Incident Detection and Response;

Standard 018 – Payment Item Information Security Standard

E. Third Parties;
F. Network Security; and
G. Audit.

Members are accountable for ensuring adherence to the security requirements outlined below at all sites including respective back-up and recovery sites. These requirements apply to a Member even in situations where the services are performed by a third party or another Member on behalf of that Member.

Note: Bracketed references following the security requirements listed below are provided for **information purposes only**, and to indicate comparable requirements within common industry standards.

A. Logical and administrative access control

Process Area	Security requirement – Logical and administrative access control
General	i) Items shall be protected from unauthorized access and tampering via documented access control policy and mechanisms. This protection is to be in effect from the point of origination by Member or receipt from corporate client to the point of deletion. (ISO/IEC 27002:2013 9.4.1) ii) Access to items and permissions shall be managed, incorporating the principles of least privilege, least functionality, and separation of duties. (ISO/IEC 27002:2013 9.1.2) iii) Access rights shall be subject to regular reviews (annually, at a minimum). When access is granted, changed, or revoked it shall be verified against approvals. Removal of rights, where no longer required, shall be done in a timely manner. (ISO/IEC 27002:2013 9.2.5) iv) Information used to authenticate users shall be assigned and controlled through a formal process. (ISO/IEC 27002:2013 9.2.4) v) Access to systems and applications handling the Item shall be controlled through a secure logon procedure. (ISO/IEC 27002:2013 9.4.2) vi) A password or authentication policy shall be in place that establishes, at a minimum, password controls for users. (ISO/IEC 27002:2013 9.4.3) vii) Users shall be required to follow the Member's practices to protect information used for authentication. (ISO/IEC 27002:2013 9.3.1)
Origination	i) The software used in the origination of Items shall be protected from unauthorized access. (ISO/IEC 27002:2013 14.2.4) ii) Activities performed by maintenance or repair personnel, at branch, ABM, Data Centre or other systems used in the origination of Items, shall be authorised and logged in accordance with the Member's security risk profile. (ISO/IEC 27002:2013 15.1.1)
Transmission	i) All transmission of Items shall take place in a Secure Environment. (ISO/IEC 27002:2013 14.1.2)

	ii) Payment related information included in Items shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or unauthorized Replay. (ISO/IEC 27002:2013 14.1.3)
Storage	Logical and physical access to the storage devices and to the software shall be restricted to authorized and authenticated individuals and software. (ISO/IEC 27002:2013 9.1.2)
Archival	Logical and physical access to archived Items shall be restricted to individuals based on the *principle of least privilege.* (ISO/IEC 27002:2013 9.1.2)
Retrieval	Access to Items shall be restricted to authorized and authenticated individuals and software. (ISO/IEC 27002:2013 9.1.2)
Deletion	When removing or retiring media (including paper copies) from an entity's security perimeter that may have been used to store Items, the following rules apply: (ISO 27002:2013 8.3.2) i) If the media can be overwritten it shall be sanitized through secure software overwrite or degaussing. The use of secure software deletion shall follow industry accepted standards such as CSE ITSG-06 - Clearing and Declassifying Electronic Data Storage Devices or NIST SP 800-88 Guidelines for Media Sanitation; or ii) If the media cannot be overwritten it shall be physically destroyed. This involves the physical incineration or shredding of the storage media with the intent of making recovery of original data impossible.
Back-up/ Removable Storage	Logical and physical access to the copies of information containing Items including laptops (e.g., USB devices, CDs/DVDs, memory cards, tapes, etc.) shall be protected and restricted to individuals based on the *principle of least privilege*. Removable media and off-line storage containing payment information shall be managed in accordance with the Member's security risk profile. (ISO/IEC 27002:2013 12.3.1)

B. Malicious Code

Process Area	Security requirement – Malicious Code
General	The systems used for creating, storing, archiving, and transmitting Items shall be guarded against malicious code to prevent unauthorized modifications and security incidents. (ISO/IEC 27002:2013 12.2.1)

Standard 018 – Payment Item Information Security Standard

C. Logging

Process Area	Security requirement – Logging
General	i) Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed in accordance with the Member's security risk profile. (ISO/IEC 27002:2013 12.4.1) ii) Logging facilities and log information shall be protected against unauthorized access and modification. (ISO/IEC 27002:2013 12.4.2) iii) A reference time source shall be used to synchronize all of the clocks supporting all relevant information processing systems within a Member's security domain. (ISO/IEC 27002:2013 12.4.4).

D. Incident Detection and Response

Process Area	Security requirement – Incident Detection and Response
General	i) Processes and procedures shall be in place to identify and respond to unauthorized access attempts or breaches with respect to systems used for transmission of Payment Items or to the Items themselves. (ISO/IEC 27002:2013 16.1.1) ii) Information security events shall be reported through the Member's appropriate management processes as quickly as possible. (ISO/IEC 27002:2013 16.1.2) iii) An incident response team shall be in place with a formal incident response process to investigate possible unauthorized events. (ISO/IEC 27002:2013 16.1.5) iv) Where a breach or other failure of a Member's security safeguards results in an unauthorized party gaining access to another Member's client data, the Member subject to the breach or failure shall notify the other Member and the CPA as soon as possible following the discovery of such unauthorized access.

E. Third Parties

Process Area	Security requirement – Third Parties
General	i) A Member shall consider cyber security risk as part of its due diligence process for material outsourcing arrangements and critical IT service providers, including subcontracting arrangements related to the process areas referred to above. (OSFI 4.26) ii) Members shall require all material outsourcing (including critical IT service providers) involved in the process areas referred to above, to safeguard Member's Payment information. (OSFI 4.27) iii) A Member shall have processes in place to ensure the timely notification of a cyber incident from critical IT service providers or service providers with whom the Member has any material outsourcing arrangements. (OSFI 4.28) iv) Care shall be taken to ensure service providers are able to monitor or cancel Item(s) distributed among several organizations in case there is a doubt in Item legitimacy. (ISO/IEC 27015:2012 6.2.3)

F. Network Security

Process Area	Security requirement – Network Security
General	i) Formal transfer policies, procedures and controls shall be in place to protect the confidentiality and integrity of Items transferred through the use of all types of communication facilities. (ISO/IEC 27002:2013 13.2.1) ii) Telecommunications Networks shall be controlled and managed to protect information across all systems and applications. (ISO/IEC 27002:2013 13.1.1)
Transmission	Information included in electronic Payment Item shall be protected in accordance to the Member's risk tolerance. (ISO/IEC 27002:2013 13.2.3)

G. Audit

Process Area	Security requirement – Audit
General	i) Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with, at a minimum, legislative requirements. (ISO/IEC 27002:2013 18.1.3) ii) The Member shall ensure that relevant legal, regulatory and contractual requirements are regularly checked against their respective information security management framework for ensuring compliance monitoring. (ISO/IEC 27015:2012 15.2.3)