SEM Agreed Procedure

Title	**Agreed Procedure 5: Data Storage and IT Security**
Version	**3.0a**
Date	**11th May 2007**

TABLE OF CONTENTS

DOCUMENT HISTORY

VERSION	DATE	AUTHOR	COMMENT
2.0	03/11/2006	SEM Implementation Team	Issue to Regulators
2.1	21/02/2007	Regulatory Authorities	Updated with comments from review of Terminology across all APs and TSC
2.2a	23/03/2007	Regulatory Authorities	Updated with consistency check comments against System Baseline Code
2.9	23/04/2007	SEMIT and Regulatory Authorities	Final version for final review prior to drafting of change control
3.0	25/04/2007	SEMIT and Regulatory Authorities	Tidied up Party/Participant issue, removed Participant User removal to AP1
3.0a	11/05/2007	Regulatory Authorities	Consultation Version

RELATED DOCUMENTS

DOCUMENT TITLE	VERSION	DATE	BY
Trading and Settlement Code	V1.3	30/03/2007	Regulatory Authorities
To be completed following consultation			

1. INTRODUCTION

1.1. BACKGROUND AND PURPOSE

This Agreed Procedure describes the specific procedures and directives for data storage and IT security with which Parties to the Trading and Settlement Code (the "Code") must comply.

1.2. SCOPE OF AGREED PROCEDURE

This Agreed Procedure defines the operational, physical and technical requirements for IT security of the Market Operator's Isolated Market System and the minimum IT security requirements for Type 2 Channel and Type 3 Channel with the Market Operator's Isolated Market System. It also defines the data back-up requirement and data repudiation measures.

In addition it specifies IT security guidelines for Parties' Isolated Market Systems.

This Agreed Procedure forms an annexe to, and is governed by, the Code. This document is a statement of process and procedure. Parties' rights and obligations are set out in the Code.

1.3. DEFINITIONS AND INTERPRETATION

Save as expressly defined, words and expressions defined in the Code shall have the same meanings when used in this Agreed Procedure.

References to particular sections relate internally to this Agreed Procedure unless specifically noted.

There are a number of functional roles described and used in this Agreed Procedure. These are functional roles and do not necessarily reflect the organisation of the Market Operator or the job titles of any member of its staff. A member of the Market Operator staff may perform one or more of these roles.

1.4. COMPLIANCE WITH AGREED PROCEDURE

Compliance with this Agreed Procedure is required under the terms as set out in paragraph 1.7 of the Code.

Sections 2.2 Data Storage and Data Access and 2.3 IT Security Standard for Isolated Market System applies to the Market Operator and the Market Operator's Isolated Market System. These sections should be considered as guidelines for Parties for their Isolated Market System(s). Where a Party has registered as more than one Participant, each Participant having a separate Isolated Market System, this Agreed Procedure applies to all Isolated Market Systems owned or ultimately controlled by the Party, although the compliance with this procedure may be carried out on a Participant level.

2. PROCEDURE DEFINITION

This section 2 provides an overview of the procedure provided for in the main Sections of the Code, for explanatory purposes and to set the context for this Agreed Procedure only. The overview contained in this section is not legally binding and is not intended to create rights or impose obligations on any Party.

2.1. IT SECURITY STANDARD FOR DATA COMMUNICATION

The Code provides for three types of Communication Channel. The IT security standard for data communications applies to the Type 2 Channel and the Type 3 Channel.

2.1.1. Security for Type 2 Channel and Type 3 Channel

Each Participant wishing to communicate using Type 2 Channel or Type 3 Channel shall obtain a Digital Certificate. The process for acquiring a Digital Certificate is set out in Agreed Procedure 3 "Communication Channel Qualification". Digital Certificates will provide the following security facilities.

2.1.1.1 Encryption

All data communication will be encrypted according to the ITU-T X.509 standard. Asymmetric encryption will be adopted using 1024 bit keys.

2.1.1.2 Authentication and Non Repudiation

Digital signatures utilising a “hash” will be implemented to ensure authentication of message senders and to provide a basis for the non-repudiation of messages. Validation of message “hash” values will be performed by de-encryption using the sender’s Public Key and comparison with a locally generated “hash”. Validation failure signifies an authentication issue or corruption of message contents and the cause must be investigated by the Market Operator and Participant concerned following the process described in Section 3 of the Code.

2.1.1.3 Keys

The Market Operator and each Participant are required to create and exchange a Public Key. Corresponding Private Keys must be protected against theft or use by unauthorised persons, viruses or trojans. The creation and exchanging of Public Keys will be performed at the time of creation of the Digital Certificate by the Certificate Authority (CA).

2.1.1.4 Certificate Authority

The Market Operator will provide, or procure, CA services for the purposes of data communication between the Isolated Market System and Participants. The services provided must include:

- Digital Certificate creation
- Digital Certificate issuance
- Digital Certificate revocation

2.1.2. Communication Links

Data communication will be achieved utilising the public internet. Each Party is responsible for their individual connection(s) to the internet. The Market Operator is responsible for connection of the Market Operator’s Isolated Market System to the internet.

All Parties must maintain a redundant and fault-tolerant network configuration of sufficient capacity to meet their peak communication needs.

2.1.3. Type 2 Channel

Where a Participant has initiated a Type 2 Channel session then the Market Operator's Isolated Market System shall monitor the duration of the session and may terminate the session if there has been no activity for more than 10 minutes.

2.1.4. Denial of Service

Participants shall not engage in activities that may be reasonably construed as Denial of Service Attacks on the Market Operator's Isolated Market System or the Market Operator's connection to the internet. If the Market Operator reasonable construes that a Participant is acting in a manner that negatively impacts on the availability or functionality of the Market Systems then they are entitled to take any action in relation to Communication Channels necessary to remedy the situation, including, but not limited to, the restriction of Type 3 access for the Participant in question.

2.1.5. Change Control of Security Standard for Data Communication

If the Market Operator requires a change to the security standard or the implementation of that security standard for data communications then it shall follow the processes in Agreed Procedure 12 "Modifications Committee Operation" and/or Agreed Procedure 11 "Market System Operation, Testing, Upgrading and Support".

2.2. DATA STORAGE AND DATA ACCESS

2.2.1. Data Storage and Data Access Overview

This section on data storage and data access sets out the standards that the Market Operator shall apply to its Isolated Market System. These standards should also be used by Parties as guidelines for data storage and data access for their Isolated Market Systems. In this section, the term "MO Users" refers to Market Operator staff and other contracted individuals procured by the Market Operator, and not other Parties staff.

The Market Operator's IT security policies shall detail the specific requirements for data storage and data access for the Market Operator's Isolated Market System, including, without limitation, the items prescribed under the following sections.

2.2.2. Controlling Access to Information

The Market Operator shall implement three levels of data confidentiality in its systems namely:

- Public Data– data freely available to all Parties and the general public;
- Private Data – data restricted to the Participant relevant to that data;
- Market Private Data – data restricted to the Market Operator.

To control access to information:

- Private Data is restricted to the relevant Participant and Market Operator staff.
- Market Private Data is restricted to Market Operator staff.

2.2.3. User Access Management

2.2.3.1 Market Operator Staff

To help prevent unauthorised access to systems all MO User access requires a level of authorisation prior to access being given. The Market Operator shall implement an authorisation process to ensure only the appropriate level of access is granted to individual MO Users to enable them to fulfil their roles.

2.2.3.2 User Access

Digital Certificates are obtained in accordance with Agreed Procedure 3 "Communication Channel Qualification".

Each Party is then responsible for authorising access for each of its Participant Users, or removing access for Participant Users which are no longer relevant to a Party's organisation, to the specific Functional Areas as described in Agreed Procedure 1.

2.2.4. User Responsibilities

The Market Operator shall implement suitable access arrangements to help prevent unauthorised MO User access to the Market Operator's Isolated Market System. Where these access arrangements require the use of passwords by the MO Users then suitable constraints and procedures shall be applied to promote security of the passwords and access to MO Users' workstations whilst the MO User is connected to the Market Operator's Isolated Market System.

2.2.5. System and Application Access Control

MO Users will have restricted access to specific areas of the system according to their level of authority and access requirements.

2.2.6. Monitoring System Access

To assist in the detection of unauthorised activities within the Market Operator's Isolated Market System, the Market Operator shall monitor system access. The Market Operator shall implement procedures to deal with incidents of unauthorised activities.

2.2.7. Data Storage

To maintain the integrity and availability of information processing and communication services data will be stored at least two sites. The Market Operator shall employ an off-line electronic back-up solution of market data which will allow recovery of data in the short-term (less than one week) for disaster recovery and also facilitate the requirement to store market data over the long term.

Market data will be stored for a period of not less than seven years.

Market data relates to the Market Operator's fulfilment of its rights and obligations where interaction with Parties and Participants, or Publication is involved. Market data does not include internal communications within the Market Operator, email with Parties or Participants (important functions are backed up by Type 1 communications), except where defined explicitly as required for reporting purposes on an ongoing basis under the terms of the Market Auditor Report.

2.3. IT SECURITY STANDARD FOR ISOLATED MARKET SYSTEM

2.3.1. IT Security Standard Overview

This section on IT security standard sets out the standards that the Market Operator shall apply to its Isolated Market System. These standards should also be used by Parties as guidelines for security standards for their Isolated Market System.

The Market Operator's IT security policies shall detail the specific requirements for IT security standards for the Market Operator's Isolated Market System, including, without limitation the following provisions.

2.3.2. Security Organisation

The following roles will be designated to manage the security of the Market Operator's Isolated Market System:

- A Quality role will set out specific responsibilities for quality and security audit, system maintenance, technical authoring, familiarisation training and the security incident report procedure;
- A Technical Operations role will set out responsibilities for computer/network security and database security;
- A Facilities role will set out responsibilities for building security;
- A Personnel Officer role will set out responsibilities for the training of staff on security matters;

2.3.3. Change Control

To ensure any patches to existing software or development updates to software or supporting documentation are managed in a secure and controlled manner the Market Operator will follow a change control process. All changed software and/or documentation will be held within a configuration management system. The change management process is detailed in Agreed Procedure 11 "Market System Operation, Testing, Upgrading and Support".

2.3.4. Security of System Files

To ensure that development projects and support activities are conducted in a secure manner all access to server directories and files required for the maintenance of the Market Operator's Isolated Market System will be restricted to staff working in the development team and other approved staff and contractors procured by the Market Operator. The development team will be provided access to development, test and quality assurance systems; support staff will be provided access to development, test, quality assurance and production systems.

2.3.5. Security in Development and Support Processes

To maintain the security of system software and information held on the Market Operator's Isolated Market System changes can only be implemented under the authority of the approved change control process. System source files and application build instructions will be maintained in a configuration management system.

2.3.6. Security of Data against Loss, Modification or Misuse

To prevent loss, modification or misuse of data the Market Operator shall procure that only authorised MO Users will be given access to specific areas of the system in which those MO Users are managed and trained to operate.

The Market Operator shall use reasonable endeavours to ensure that its Isolated Market System is protected from accidental or deliberate access from unauthorised persons. This shall include implementation of suitable firewall protection and anti-virus protection to protect its Isolated Market System from unauthorised access via the internet or other external network connections. Firewall protection may be provided using hardware and software firewall solutions as appropriate for the system being protected.

2.3.7. Compliance

A security policy and security plan will be maintained and reviewed on an annual basis. Input to the review will include the results of an annual security audit and the results of investigations into any incidents since the previous security review. These reviews will be performed by those responsible for the Quality role in the Market Operator.

2.3.8. Physical and Environmental Security

To prevent loss, damage or compromise of assets or interruption to business activities, servers and communication equipment associated with the Market Operator's Isolated Market System will be located in locked rooms within Market Operator offices with access limited to staff that need to work in them. Any paper records or electronic media with sensitive data contained therein will be stored in a secure location when not in use and, subject to the data storage provisions in 2.2.7, retained on site.

All data rooms will be protected by UPS and stand-by generators with these facilities located in locked compounds.

2.3.9. Personnel Security

The terms of reference for all staff involved in delivering services associated with the Market Operator's Isolated Market System will be required to "comply at all times with the Market Operator security requirements and procedures from time to time in force".

All employees will be obliged to maintain customer confidentiality.

2.4. COMPUTATIONAL MACHINE PRECISION AND METHOD OF ROUNDING

The Trading Payments and Trading Charges will be calculated to the levels of precision set out below.

Payment / Charge types	*Unit Type*	*Document*	*Precision (€ decimal places)*
Energy Payments	*Generator*	*Settlement Statement*	*4*
Energy Charges	*Supplier*	*Settlement Statement*	*4*
Capacity Payments	*Generator*	*Settlement Statement*	*4*
Capacity Charges	*Supplier*	*Settlement Statement*	*4*
Constraint Payments	*Generator*	*Settlement Statement*	*4*
Uninstructed Imbalance Payments	*Generator*	*Settlement Statement*	*4*
Imperfections Charges	*Supplier*	*Settlement Statement*	*4*
Energy Payments	*Participant*	*Self-Billing Invoice*	*2*
Energy Charges	*Participant*	*Invoice*	*2*
Capacity Payments	*Participant*	*Self-Billing Invoice*	*2*
Capacity Charges	*Participant*	*Invoice*	*2*
Constraint Payments	*Participant*	*Self-Billing Invoice*	*2*

Make Whole Payments	*Participant*	*Invoice*	*2*
Uninstructed Imbalance Payments	*Participant*	*Self-Billing Invoice*	*2*
Imperfections Charges	*Participant*	*Invioce*	*2*

Arising from the technical implementation of the central market systems, the results of all settlement calculations and settlement variables used within those settlement calculations performed in the Code are rounded to 8 decimal places.

3. APPENDIX 1 – DEFINITIONS AND ABBREVIATIONS

3.1. DEFINITIONS

Active Power	As defined in the Code
Annual Capacity Payment Sum	As defined in the Code
Billing Period	As defined in the Code
Capacity Charge	As defined in the Code
Capacity Payment	As defined in the Code
Capacity Period	As defined in the Code
Certificate Authority	is an entity which issues Digital Certificates for use by other parties. The Certificate Authority validates the data contained in the Digital Certificate and correctly identifies the party to which it issues the Digital Certificate
Certificate Issuer	is an entity which issues Digital Certificates for use by other parties. The Certificate Issuer relies on the party requesting the Digital Certificate to validate that the data contained in the Digital Certificate correctly identifies the party to which the Certificate Issuer issues the Digital Certificate.
Charge	As defined in the Code
Code	As defined in the Code
Communication Channel	As defined in the Code
Constraint Payments	As defined in the Code
Data Transaction	As defined in the Code
Demand	As defined in the Code
Denial of Service Attack	is an attempt to make a computer resource unavailable to its intended users
Digital Certificate	is an electronic credential issued and digitally signed by a certificate authority (CA). The international standard upon which most commercial certificates are based is the ITU-T X.509 certificate. The digital certificate represents the certification of an individual, business, or organizational public key.
Digital Key	A digital key is a number or group of numbers that is carefully chosen to have certain mathematical properties. Depending on the encryption algorithm being used, the key may be a large random number or a set of related numbers
Digital Signature	A digital signature is a digital stamp made with a cryptographic algorithm. The stamp is made using a key, and cannot be forged without access to that key. Usually, you use your Private Key to sign messages and documents – the same Private Key you would use to unlock an encrypted message that someone sent to you
Energy Charges	As defined in the Code

Energy Payment	As defined in the Code
Facilities	relates to building security.
Functional Areas	As defined in Agreed Procedure 1 "Participant and Unit Registration and Deregistration"
Generation	As defined in the Code
Generator	As defined in the Code
Hash Function	A hash function is a computation that takes a variable-size input and returns a fixed-size string, which is called the hash value. One-way hash functions, hash functions that are hard to invert, are used to generate a message digest. Examples of well-known hash functions are MD4, MD5, and SHA-1.
Help Desk	As defined in Agreed Procedure 11 “Market System Operation, Testing, Upgrading and Support”
Imperfections Charge	As defined in the Code
Isolated Market System	As defined in the Code
ITU-T X.509	X.509 is published as ITU recommendation ITU-T X.509 (formerly CCITT X.509) and ISO/IEC/ITU 9594-8 which defines a standard certificate format for Public Key certificates and certification validation.
Loss-Adjusted	As defined in the Code
Make Whole Payment	As defined in the Code
Market Operator	As defined in the Code
Market Operator Licence	As defined in the Code
Market Private Data	As defined in Section 2.2.2
Market Web Interface	As defined in Agreed Procedure 1 "Participant and Unit Registration and Deregistration"
Maximum Demand	summation of Loss Adjusted Net Demand for all Supplier Units in a Trading Period
Net Demand	As defined in the Code (Variables)
Participant	As defined in the Code
Party	As defined in the Code
Personnel Officer	A role within the Market Operator with responsibility for the training of staff on security matters.
Price	As defined in the Code (Variables)
Private Data	As defined in Agreed Procedure 6 “Data Publication”
Public Data	As defined in Agreed Procedure 6 “Data Publication”

Public Key & Private Key	Rather than using the same key to both encrypt and decrypt the data, Public Key encryption uses a matched pair of encryption and decryption keys. Each key performs a one-way transformation on the data. Each key is the inverse function of the other; what one does, only the other can undo. A Public Key is made publicly available by its owner, while the Private Key is kept secret. To send a private message, an author scrambles the message with the intended recipient's Public Key. Once so encrypted, the message can only be decoded with the recipient's Private Key.
Regulatory Authorities	As defined in the Code
SEM	As defined in the Code
Settlement	As defined in the Code
Settlement Day	As defined in the Code
SMP	As defined in the Code
Quality	relates to quality and security audit, system maintenance, technical authoring, familiarisation training and the security incident report procedure.
Supplier	As defined in the Code
Supplier Unit	As defined in the Code
Technical Operations	relates to computer/network security and database security.
Trading Charges	As defined in the Code
Trading Payments	As defined in the Code
Trading Period	As defined in the Code
Type 1 Channel	As defined in the Code
Type 2 Channel	As defined in the Code
Type 3 Channel	As defined in the Code
Uninstructed Imbalance Payment	As defined in the Code
Unit	As defined in the Code
MO User	As defined in section 2.2.1of this Agreed Procedure
Participant	As defined in the Code
Participant User	Means a member of the Participant's staff who has been granted a Digital Certificate under Agreed Procedure 3 "Communication Channel Qualification" and has been authorised by the Participant to access the Functional Areas of the Market Web Interface
Value of Lost Load	As defined in the Code
Working Day	As defined in the Code

Uninterruptible Power Supply	is a device which maintains a continuous supply of electric power to connected equipment by supplying power from a separate source when the normal power source is not available

3.2. ABBREVIATIONS

CA	Certification Authority
CI	Certificate Issuer
UPS	Uninterruptible Power Supply