Trading and Settlement Code

Agreed Procedure 5: Data Storage and IT Security

April 7

2017

Version 1.0

Contents

DOCUMENT HISTORY

Version	Date	Author	Comment
Draft	07/04/2017	I-SEM Project Team	

RELATED DOCUMENTS

Document Title	Version	Date	By
Trading and Settlement Code			
Agreed Procedure 1 "Registration"			
Agreed Procedure 3 "Communication Channel Qualification".			
Agreed Procedure 6 “Data Publication and Data Reporting”			
Agreed Procedure 11 “Market System Operation, Testing, Upgrading and Support”			
Agreed Procedure 12 “Modifications Committee Operation”			

1. INTRODUCTION

1.1 Background and Purpose

This Agreed Procedure supplements the rules in relation to data storage and IT security set out in the Trading and Settlement Code (hereinafter referred as the "**Code**"). It sets out procedures with which Parties to the Code must comply.

1.2 Scope of Agreed Procedure

This Agreed Procedure sets out:

(a) the operational, physical and technical requirements for IT security of the Market Operator's Isolated Market System;

(b) the minimum IT security requirements for Type 2 Channel and Type 3 Channel with the Market Operator's Isolated Market System;

(c) data back-up requirement and data repudiation measures; and

(d) IT security guidelines for Parties' Isolated Market Systems.

This Agreed Procedure forms an annex to, and is governed by, the Code. It is a statement of process and procedure. Parties' rights and obligations are set out in the Code. In the event of any conflict between a Party's obligations set out in the Code and this Agreed Procedure, the Code shall take precedence.

1.3 Definitions and Interpretation

Words and expressions defined in the Code shall, unless the context otherwise requires or unless otherwise defined herein at Appendix 1 "(Definitions and Abbreviations"), have the same meanings when used in this Agreed Procedure.

References to particular paragraphs relate internally to this Agreed Procedure unless otherwise specified.

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 members of its staff.

1.4 Compliance with Agreed Procedure

Compliance with this Agreed Procedure is required under the Code.

Section 2.4 and section 2.5 of below apply 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). In the event that a Party has registered more than one Participant with 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. ~~PROCEDURES~~DATA STORAGE AND IT SECURITY

2.1 IT Security Standard for Data Communication

The Code provides for three types of Communication Channel. The IT security standard for data communications set out in this Agreed Procedure applies to both Type 2 Channel and Type 3 Channel, with the exception of two factor authentication which only applies to the Type 2 Channel.

2.2 Security for Type 2 Channel and Type 3 Channel

Each Participant intending to use Type 2 Channel and Type 3 Channel shall obtain a Digital Certificate. A Participant using Type 2 Channel shall also have a valid User password. The process for acquiring a Digital Certificate is set out in Agreed Procedure 3 "Communication Channel Qualification". Digital Certificates will provide the security facilities set out below.

2.2.1 Encryption

All data communication ~~will~~ shall be encrypted ~~according to~~in accordance with the ITU-T X.509 standard. Asymmetric encryption ~~will~~ shall be adopted using 2048 bit keys.

2.2.2 Authentication and Non-Repudiation

Digital Signatures utilising a "hash" ~~will~~ shall 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~~shall 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 in accordance with chapter C of the Code.

2.2.3 Keys

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

2.2.4 Certificate Authority

The Market Operator ~~will~~ shall provide, or procure, Certificate Authority services for the purposes of data communication between the Market Operator's Isolated Market System and Participants. These services must include:

(a) Digital Certificate creation

(b) Digital Certificate issuance

(c) Digital Certificate ~~revocation~~cancellation

2.3 Communication Links

Data communication to the Market Operator's Isolated Market System ~~will~~ shall 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.

2.3.1 Type 2 Channel and Type 3 Channel

Where a Participant has initiated a Type 2 Channel and / or Type 3 Channel session, 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 longer than the period ~~set out~~specified in the ~~Interface~~ Technical Specification.

2.3.2 Denial of Service

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

2.3.3 Change Control of Security Standard for Data Communication

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

2.4 Data Storage and Data Access

This section 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 in respect of their Isolated Market Systems.

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~~below.

2.4.1 Controlling Access to Information

The Market Operator shall implement the following levels of data confidentiality in its Isolated Market System~~s namely~~:

(a) Public Data: data available, without access restriction, via public website

(b) Private Data:

i. Member Public Data: data available to all Participants only; and
ii. Member Private Data: data restricted to the Participant relevant to that data;

(c) Market Private Data: data restricted to the Market Operator staff.

(d) REMIT Data: data restricted to the European Agency for the Cooperation of Energy Regulators and relevant Participants.

2.4.2 Market Operator User Access Management

To help prevent unauthorised access to systems, all Market Operator 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 Market Operator Users and System Operator Users, to enable them to fulfil their roles.

Market Operator Users, System Operator Users and support staff will have restricted access to specific areas of the system according to their level of authority and access requirements.

2.4.3 Authorised User Access

Digital Certificates (along with User password for Type 2 Channel) 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 to the Functional Areas which are no longer relevant to a Party's organisation, as described in Agreed Procedure 1 "Registration".

It is the responsibility of the Party to ensure that its ~~their~~ Digital Certificates and~~/or~~ User passwords are valid for a given Trading Day, for each relevant User.

2.4.4 User Responsibilities

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

2.4.5 Monitoring System Access

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

2.4.6 Data Storage

In order to maintain the integrity and availability of information, processing and communication services data ~~will~~ shall be stored in at least two sites. The Market Operator shall employ an offline electronic back-up solution of market data which ~~will~~ shall allow recovery of market data as soon as reasonably practicable for disaster recovery and shall also facilitate the requirement to store market data over the long term.

Market data shall ~~will~~ be stored for a period of not less than six years.

Reference to market data in this section relates to the Market Operator's fulfilment of its rights and obligations in accordance with the Code which relate to interaction with Parties or publication of market data. Market data does not include internal communications within the Market Operator or emails between the Market Operator and Parties (important functions are backed up by Type 1 Channel), except where specifically required for reporting purposes on an ongoing basis under the terms of ~~the~~ a Market Auditor report.

2.5 IT Security Standard for Isolated Market System

This section sets out the standards that the Market Operator shall apply to its Isolated Market System. These standards should be used by Parties as guidelines for the security standards to be implemented in respect of their Isolated Market Systems.

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.

2.5.1 Security Organisation

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

(a) a~~A~~ Quality role with~~will have~~ specific responsibility~~ies~~ for quality and security audit, system maintenance, technical authoring, familiarisation training and the security incident report procedure;

(b) a~~A~~ technical operations role ~~will have~~with responsibility~~ies~~ for computer / network security and database security;

(c) a~~A~~ facilities role ~~will have~~with responsibility~~ies~~ for building security; and

(d) a~~A~~ personnel officer role ~~will have~~with responsibility~~ies~~ for the training of staff on security matters.

2.5.2 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".

2.5.3 Security of Market Operator Infrastructure, Systems and Applications

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

2.5.4 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~~ may only be implemented under the authority of the approved change control process. System source files and application build instructions shall~~will~~ be maintained in a configuration management system.

2.5.5 Security of Data against Loss, Modification or Misuse

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

The Market Operator shall use reasonable and appropriate measures to ensure that its Isolated Market System is protected from all forms of cyber security threats, including but not restricted to unauthorised access, malicious code, Denial of Service Attack and data leakage.

2.5.6 Compliance

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

2.5.7 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 shall~~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~~ shall be stored in a secure location when not in use and, subject to the data storage provisions set out in section 2.4 above, retained on site.

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

2.5.8 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~~shall comply ~~at all times~~ with the Market Operator security requirements and procedures.

All employees shall~~will~~ be obliged to maintain customer confidentiality.

3. ~~COMPUTATIONAL MACHINE PRECISION AND METHOD OF ROUNDING~~PROCEDURES

~~3.~~ Computational Machine Precision and Method of Rounding

Formatted: AP Heading2, Indent: Left: 0 cm, Hanging: 1.5 cm

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	Invoice	2
Energy Charges	Participant	Invoice	2
Capacity Payments	Participant	Invoice	2
Capacity Charges	Participant	Invoice	2
Make Whole Payments	Participant	Invoice	2
Uninstructed Imbalance Payments	Participant	Invoice	2
Imperfections Charges	Participant	Invoice	2

Arising from the technical implementation of the Central Market Systems, the following rounding is applied to Settlement calculations and Settlement variables:

a) the results of all Settlement calculations are rounded to 8 decimal places;

b) all Settlement variables used within settlement calculations that are initialised within the Settlement system of the Central Market Systems are rounded to 8 decimal places; and

c) all Settlement variables used within Settlement calculations that are not initialised within the Settlement system of the Central Market Systems shall be rounded in accordance with the Code.

d) a~~A~~ll Settlement variable shall be published in accordance with numerical rounding as specified in Chapter C “Data and Information Systems”, of the Code.

APPENDIX 1: DEFINITIONS ~~AND ABBREVIATIONS~~

Balancing Market Interface	means the function within the Market Operator's systems that interfaces to the Type 2 Channel and Type 3 Channel communications in accordance with the Code.
Certificate Authority	means 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.
Denial of Service Attack	means an attempt to make a computer resources and~~&~~ systems unavailable to its intended users.
Digital Certificate	means an electronic credential issued and ~~digitally signed~~signed with a Digital Signature by a Certificate Authority. 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 organis~~z~~ational P~~p~~ublic K~~k~~ey.
Digital Signature	means 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, a Private Key is used to sign messages and documents (the same Private Key used to unlock an encrypted message that someone sent to you).
Functional Area	means the different parts of the Balancing Market Interface that Users may be provided access to in accordance with the Code.
ITU-T X.509	means X.509 which 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.
Market Private Data	means the class of m~~M~~arket d~~D~~ata that is only accessible by Market Operator staff.
Member Private Data	means the class of Private Data for which individual reports are generated for individual Participants only and made available by the Market Operator via the Balancing Market Interface.
Member Public Data	means the class of Market Data for which individual reports are generated for all Participants and made available by the Market Operator via the Balancing Market Interface.
Quality	means quality and security audit, system maintenance, technical authoring, familiarisation training and the security incident report procedure.

Private Key	means the key used to decode a private message. The author of a message 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. It is confidential. In relation to Public Keys and Private Keys, each performs a one-way transformation on the data and each is the inverse function of the other i.e.~~;~~ what one does, only the other can undo.
Private Data	~~means reports generated for individual Participants only ("Member Private") or all of them ("Member Public") and made available by the Market Operator via the Balancing Market Interface.~~means Member Private Data and Member Public Data.
Public Data	means market information, market prices and volumes, forecasted data, and any ~~other system~~other system data required by the Code to be published by the Market Operator targeted for the general public.
Public Key	means encryption using a matched pair of encryption and decryption keys. In relation to Public Keys and Private Keys, each performs a one-way transformation on the data and each is the inverse function of the other i.e.~~;~~ what one does, only the other can undo. A Public Key is made publicly available by its owner, while the Private Key is confidential. 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.
~~**Interface**~~ **Technical Specification**	means interface documentation, to include technical and functional details and data definitions. ~~It shall be under Market Operator version control.~~ The listing shall not include the items' version numbers but shall be under Market Operator version control.
User	means: (a) in relation to a Party, a nominated member of a Party's staff who is authorised to utilise qualified Communication Channels that interact with the Market Operator's Isolated Market System; and ~~(a) in relation to a Participant: a nominated member of the Participant staff who is authorised to utilise qualified communication facilities that interact with the Market Operator's Isolated Market System; and~~ (b) in relation to the Market Operator: a member of the Market Operator staff who has been authorised to access specific parts of the Market Operator Isolated Market System.

Comment [A1]: Note: wording of definition updated to include corresponding definitions (it has the same meaning.

Formatted: Indent: Left: 0.07 cm, Hanging: 0.79 cm