Capacity Market Code

Agreed Procedure 4: Communication Channel Qualification

June 2

2017

Version 1.0

Contents

Document History

Version	Date	Author	Comment
1.0	31/05/2017	I-SEM Project Team	Issued to the Regulatory Authorities

Related Documents

Document Title	Version	Date	By
Capacity Market Code			
Agreed Procedure 1 "Registration"			
Agreed Procedure 6 "System and Communication Failures"			

1. INTRODUCTION

1.1 Background and Purpose

This Agreed Procedure supplements the rules set out in the Capacity Market Code (hereinafter referred as the "**Code**") relating to the qualification, setup and maintenance of Communication Channels. It sets out procedures with which Parties to the Code must comply.

1.2 Scope of Agreed Procedure

This Agreed Procedure sets out procedures in relation to:

(a) Obtaining a Digital Certificate;

(b) Communication Channel Qualification testing;

(c) Digital Certificate cancellation; and

(d) Communication Channel suspension.

This Agreed Procedure forms an annex to, and is governed by the Code. It sets out procedures to be followed, subject to the rights and obligations of Parties under 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.

It is not intended that there be any inconsistency or conflict between section 2 "Overview" and section 3 "Procedural Steps". However, in the event of any inconsistency or conflict, section 3 "Procedural Steps" shall take precedence.

In section 3 "Procedural Steps" a corresponding process flow diagram is included for each procedural steps table. Process flow diagrams are for illustrative purposes. It is not intended that there be any inconsistency or conflict between any procedural steps table and process flow diagram however, in the event of any inconsistency or conflict, a procedural steps table 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", have the same meanings when used in this Agreed Procedure.

References to sections refer to sections of this Agreed Procedure unless otherwise specified.

1.4 Compliance with Agreed Procedure

Compliance with this Agreed Procedure is required under the terms of the Code.

2. OVERVIEW

2.1 Communication Channels

The System Operators shall establish and maintain two types of Communication Channel in accordance with paragraph L.2.3.1 of the Code, namely Type 1 Channel and Type 2 Channel.

Type 1 Channel (manual communication) shall be used:

(a) during the initial registration procedure as set out in Agreed Procedure 1 "Registration";

(b) when submitting an Application for Qualification;

(c) where there is an issue with the use of Type 2 Channel as set out in Agreed Procedure 6 "System and Communication Failures";

(d) in the event that Type 2 Channel has been suspended in accordance with section 3.4 below; and

(e) for all Data Transactions not supported by Type 2 Channel.

Type 2 Channel shall be used in the circumstances set out in paragraph L.3.1.1 of the Code. In order to qualify for access to the Capacity Market Platform through Type 2 Channel a Party shall:

(a) obtain a Digital Certificate for the Party Certification Environment (Test Environment) and successfully complete a series of data transfer tests in the Test Environment using Type 2 Channel;

(b) obtain a Digital Certificate for the production environment; and

(c) obtain full access to the production Capacity Market Platform.

2.2 Communication Channel Qualification Testing

The procedural steps in relation to Communication Channel Qualification testing are set out at section 3.1 below. The System Operators shall provide the Party with security access credentials (including a Digital Certificate) for the Party Certification Environment to perform testing.

As part of the procedure, the Party connects to the System Operator's Party Certification Environment. This involves accessing a web-based portal. Note that this Party Certification Environment is a Test Environment distinct from the Capacity Market Platform.

A number of tests must be successfully performed. Where appropriate these may include:

(a) uploading / submitting Capacity Auction Offers, Secondary Auction Bids and Secondary Auction Offers;

(b) downloading / requesting data in relation to Capacity Auction Offers, Secondary Auction Bids and Secondary Auction Offers; or

(c) downloading a report.

2.3 Guidelines Governing Communication Channel Qualification Testing

The Communication Channel Qualification testing procedure set out at section 3.2 below shall only be conducted once per Party for Type 2 Channel, unless a re-test is required in accordance with sections 2.7 or 3.4 below. If a User is added at a later date, Communication Channel testing shall not be repeated.

2.4 Obtaining a Digital Certificate

The procedural steps in relation to obtaining a Digital Certificate are set out at section 3.2 below. This procedure applies to Parties, via Users, seeking to access the Capacity Market Platform through Type 2 Channel.

One Digital Certificate is required for access to both the Balancing Market and Capacity Market. A Digital Certificate obtained under the Trading and Settlement Code for access to the Balancing Market shall also provide certification for access to the Capacity Market Interface. A Digital Certificate obtained in accordance with this Agreed Procedure for access to the Capacity Market Platform shall also provide certification for access to the Balancing Market. For the avoidance of doubt, separate Communication Channel testing is required for the Capacity Market and Balancing Market as described in section 2.2 above.

A Digital Certificate may be cancelled in accordance with the procedure set out at section 3.3 below.

Digital Certificates issued by the System Operators for the purposes of Communication Channel Qualification testing (section 3.1 below) relate only to the System Operators' Party Certification Environment.

2.5 Guidelines Governing Digital Certificate Use

One Digital Certificate is required for each User and is associated with that User's profile.

A single Digital Certificate can allow the User to access any or all of the Functional Areas specified when the User is set-up for access to the Capacity Market Platform.

A User is given system access at a Participant level. A User can be associated with the Units of one Participant or multiple Participants, depending on their allocated system access.

Digital Certificates are environment specific i.e. a separate Digital Certificate is required when accessing Test Environments and production environments.

2.6 Accessing the Capacity Market Platform

In order to obtain full access to the Capacity Market Platform, the System Operators shall verify:

(a) that Communication Channel testing has been completed successfully; and

(b) that the Party has demonstrated compliance through self-certification with the IT security guidelines set out in the Code.

The System Operators shall allow access to the Capacity Market Platform once it is satisfied that these steps are complete. The Party shall be notified by email that they are granted access to the Capacity Market Platform via the Communication Channel for which testing has been successfully completed.

2.7 Maintaining Type 2 Channel

Parties shall ensure that interfaces to their Type 2 Channels comply with any IT security requirements specified in the Code and this Agreed Procedure (see sections 2.10 and 2.11). Any deviation from these requirements may result in a Communication Channel suspension in accordance with section 3.4 below.

In order for a Party to maintain a Type 2 Channel, the Party shall comply with the Technical Specification and satisfy the following requirements:

(a) there must be a valid User per Functional Area, with access to administer the required functionality;

(b) a valid Digital Certificate is required for each User;

(c) each User shall obtain a valid Capacity Market Interface password (as enforced by the Capacity Market Platform);

(d) adequate and resilient internet access is required;

(e) each User shall access the production Capacity Market Platform using their assigned Digital Certificate and Capacity Market Interface username and password; and

(f) Parties are required to notify the System Operators, via the Helpdesk in accordance with Agreed Procedure 5 "System Operation, Testing, Upgrading and Support", of transaction malfunction issues due to Communication Channel failure.

A Party is obliged to remain qualified for Type 2 Channel for the duration of its participation in the Capacity Market. The System Operators may instruct a Party to perform a Communication Channel Qualification re-test at any time in accordance with the IT security guidelines set out in the Code and this Agreed Procedure.

2.8 Communication Channel Suspension

The procedural steps in relation to Communication Channel suspension are set out at section 3.4 below.

A Party may be suspended from using Type 2 Channel by the System Operators. This shall be a temporary measure that shall be reversed once the System Operators are satisfied that appropriate action has been taken to resolve the issues that led to suspension. The following circumstances may lead to Communication Channel suspension:

(a) The Party requests for a particular Communication Channel to be temporarily suspended. This could arise when the Party becomes aware of a security breach.

(b) The Party does not have valid Users with the appropriate access rights to operate in the SEM.

(c) The Party Type 2 Channel password has expired.

(d) The Party Digital Certificate has expired.

(e) The Party is deemed by the System Operators to be non-compliant with the required IT standards as specified in the Code and this could affect the security / performance of the Capacity Market Platform.

(f) The System Operators have evidence of an IT security breach in the Party's systems and this could affect the security / performance of the Capacity Market Platform.

(g) The System Operators have evidence that a Party's interaction with the Capacity Market Platform is having a performance impact.

Where the System Operators have suspended a Communication Channel for a particular Party, the Party shall be immediately notified by email and provided with the reason(s) for the suspension. The System Operators may specify the steps for that Party to take to resolve the issue. Due to the time restrictions involved it is not possible to make the suspension dependent on an appeals process. Any disagreement in relation to a temporary suspension must be dealt with through the Dispute Resolution Process under the Code. A Party shall inform the System Operators of any security breach of its systems as soon as it becomes aware of such breach.

2.9 Authorised Persons

2.9.1 Nomination of Authorised Persons

Where Parties communicate with the System Operators via Type 1 Channel or any other communication required under the Code or Agreed Procedures, that communication must be from an authorised member of staff referred to as an Authorised Person. To be an Authorised Person, Party staff must first be registered as a User via the Capacity Market Interface. A User can then be authorised under one or more of the authorisation categories set out at Appendix 2 “Authorisation Categories”.

A Party Administrative User is permitted to nominate and change the authorisations of other staff from the relevant Party. As this role is administered via the Capacity Market Interface, no other type of User is permitted to perform this function. At least one Party Administrative User must be registered during the process of Party registration (see Agreed Procedure 1 “Registration”). Where a Party does not have any valid Party Administrative User(s) then a new nomination must be submitted on the Party Administrative User form provided by the System Operators and signed by a director or company secretary for the company.

2.9.2 Authentication of Information

As part of the authorisation process for performing the tasks set out at Appendix 2 “Authorisation Categories”, authentication information is required by the System Operators to verify the Authorised Person. When a communication is received from the Authorised Person the authentication information provided is dependent on the method of communication and is described in the table below.

Table 1: Details for Authentication

Mode of Communication	Authentication information
Post	Full Name, Signature
Facsimile	Full Name, Signature
Email	Full Name, Originate from registered email address

To authenticate the communication from an Authorised Person, the System Operators shall request, via telephone, their authentication code or answers to confidential questions specific to the User as provided as part of the User registration process.

2.10 Security for Type 2 Channel (Digital Certificates)

Digital Certificates shall provide the security facilities set out below.

2.10.1 Encryption

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

2.10.2 Authentication and Non-Repudiation

Digital Signatures utilising a "hash" 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 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 System Operators and Participant concerned.

2.10.3 Keys

The System Operators 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 shall be performed at the time of creation of the Digital Certificate by the Certificate Authority.

2.10.4 Certificate Authority

The System Operators shall provide, or procure, Certificate Authority services for the purposes of data communication between the Capacity Market Platform and Participants. These services must include:

(a) Digital Certificate creation;

(b) Digital Certificate issuance; and

(c) Digital Certificate cancellation.

2.10.5 System Operators User Access Management

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

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

2.10.6 Authorised User Access

Once Digital Certificates and User passwords are obtained each Party is responsible for authorising access for each of its Users, or removing access for Users to the Functional Areas which are no longer relevant to a Party's organisation.

It is the responsibility of the Party to ensure that its Digital Certificates and User passwords are valid for any Trading Day, for each relevant User.

2.10.7 User Responsibilities

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

2.11 Communication Links

2.11.1 Internet Connection

Data communication to the Capacity Market Platform shall be achieved using the internet. Each Party is responsible for their individual connection(s) to the internet.

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

2.11.2 Type 2 Channel

Where a Participant has initiated a Type 2 Channel session, the Capacity Market Platform shall monitor the duration of the session and may terminate the session if there has been no activity for longer than the period specified in the Technical Specification.

2.11.3 Denial of Service

Participants shall not engage in activities that may reasonably be construed as denial of service attacks on the Capacity Market Platform or the System Operators' connection to the internet. If the System Operators reasonably construe that a Participant is acting in a manner that negatively impacts on the availability or functionality of the Capacity Market Platform then they are entitled to take any action in relation to Communication Channels that is necessary to remedy the situation.

2.11.4 Change Control of Security Standard for Data Communication

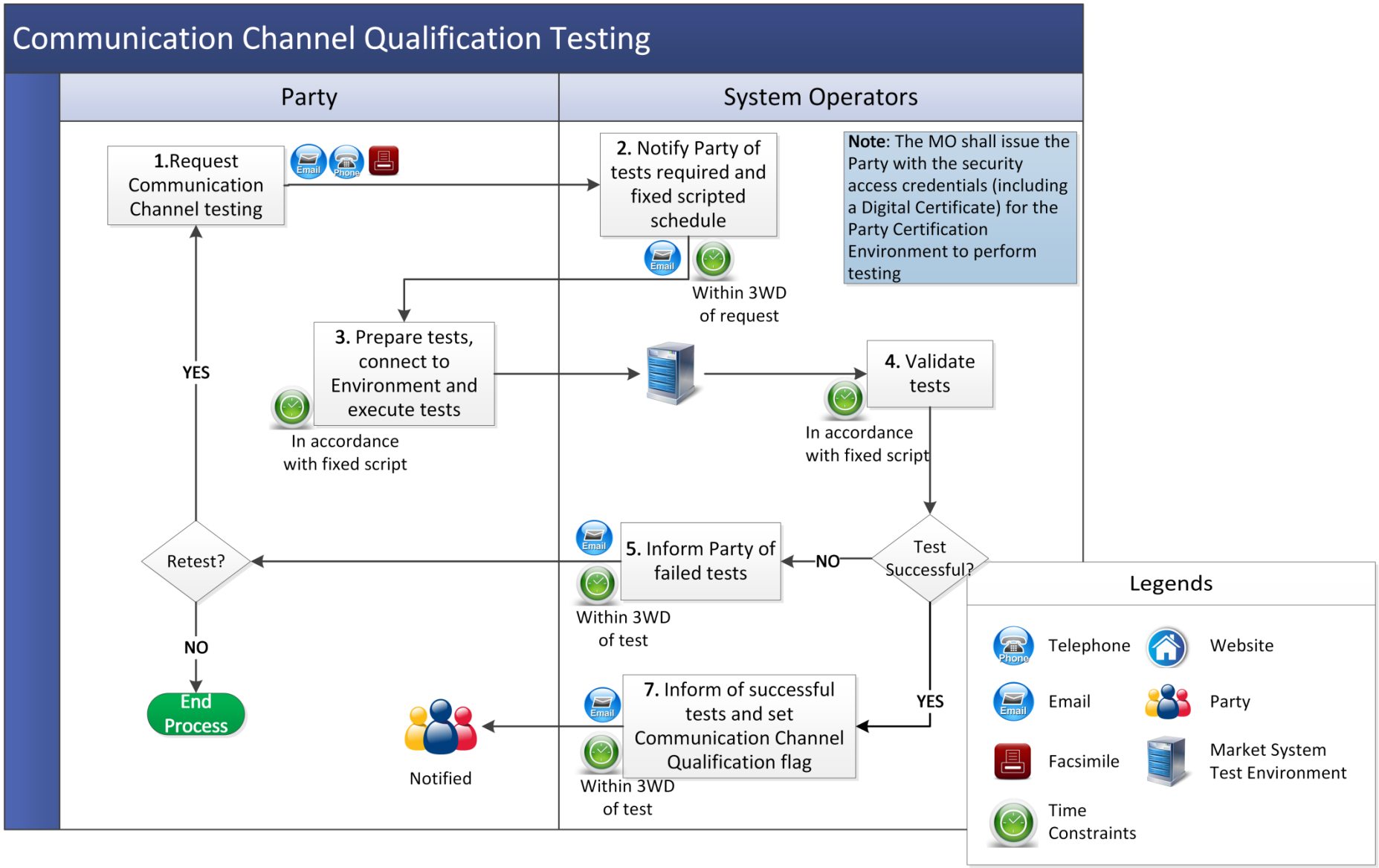
If the System Operators require the implementation of the security standard for data communications or a change to that standard, they shall follow the procedure set out in Agreed Procedure 5 "Market System Operation, Testing, Upgrading and Support".

3. PROCEDURAL STEPS

3.1 Communication Channel Qualification Testing

Step	Step Description	Timing	Method	By / From	To
1	Request Communication Channel testing. *Note:* The Market Operator shall issue the Party with the security access credentials (including a Digital Certificate) for the Party Certification Environment to perform testing.	As required	Email / Telephone / Facsimile	Party	System Operators
2	Notify Party of tests required and fixed scripted schedule of test.	Within 3 WD of request	Email	System Operators	Party
3	Prepare tests, connect to Party Certification Environment and execute tests.	In accordance with fixed script	Party Certification Environment website	Party	-
4	Validate tests. If acceptable go to step 7, otherwise continue to step 5.	In accordance with fixed script	-	System Operators	-
5	Inform Party of failed tests.	Within 3 WD of test	Email	System Operators	Party
6	If Party requires re-test (after correction of Party's systems is complete) return to step 1, otherwise **end process.**	As required	-	Party	-

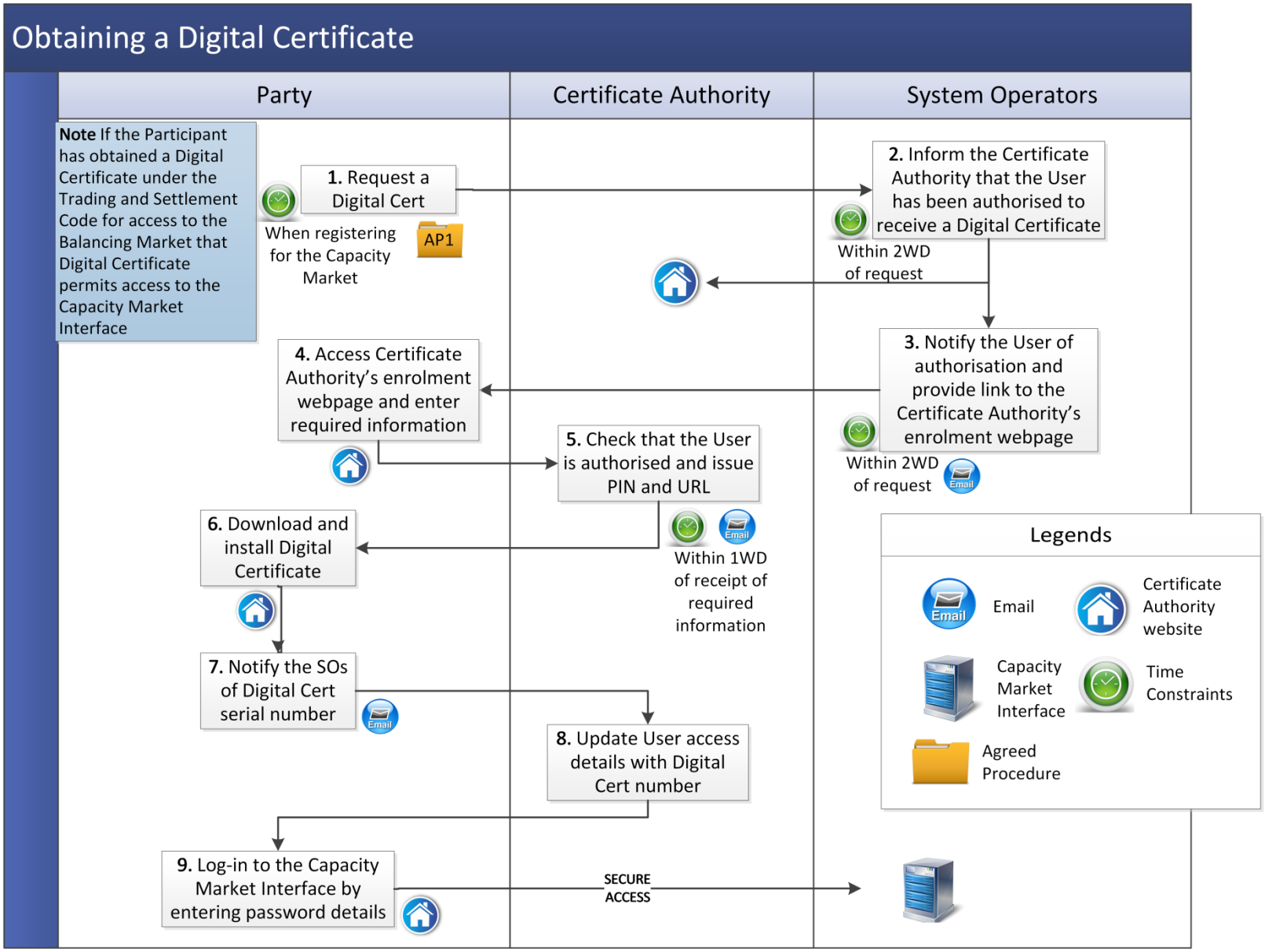
Step	Step Description	Timing	Method	By / From	To
7	Inform of successful tests and set Communication Channel qualification flag.	Within 3 WD of test	Email	System Operators	Party


Communication Channel Qualification Testing
Party
System Operators
1.Request Communication Channel testing
2. Notify Party of tests required and fixed scripted schedule
Within 3WD of request
Note: The MO shall issue the Party with the security access credentials (including a Digital Certificate) for the Party Certification Environment to perform testing
3. Prepare tests, connect to Environment and execute tests
In accordance with fixed script
4. Validate tests
In accordance with fixed script
Test Successful?
NO
5. Inform Party of failed tests
Within 3WD of test
Retest?
YES
NO
End Process
YES
7. Inform of successful tests and set Communication Channel Qualification flag
Within 3WD of test
Notified
Legends
Telephone
Website
Email
Party
Facsimile
Market System Test Environment
Time Constraints

3.2 Obtaining A Digital Certificate

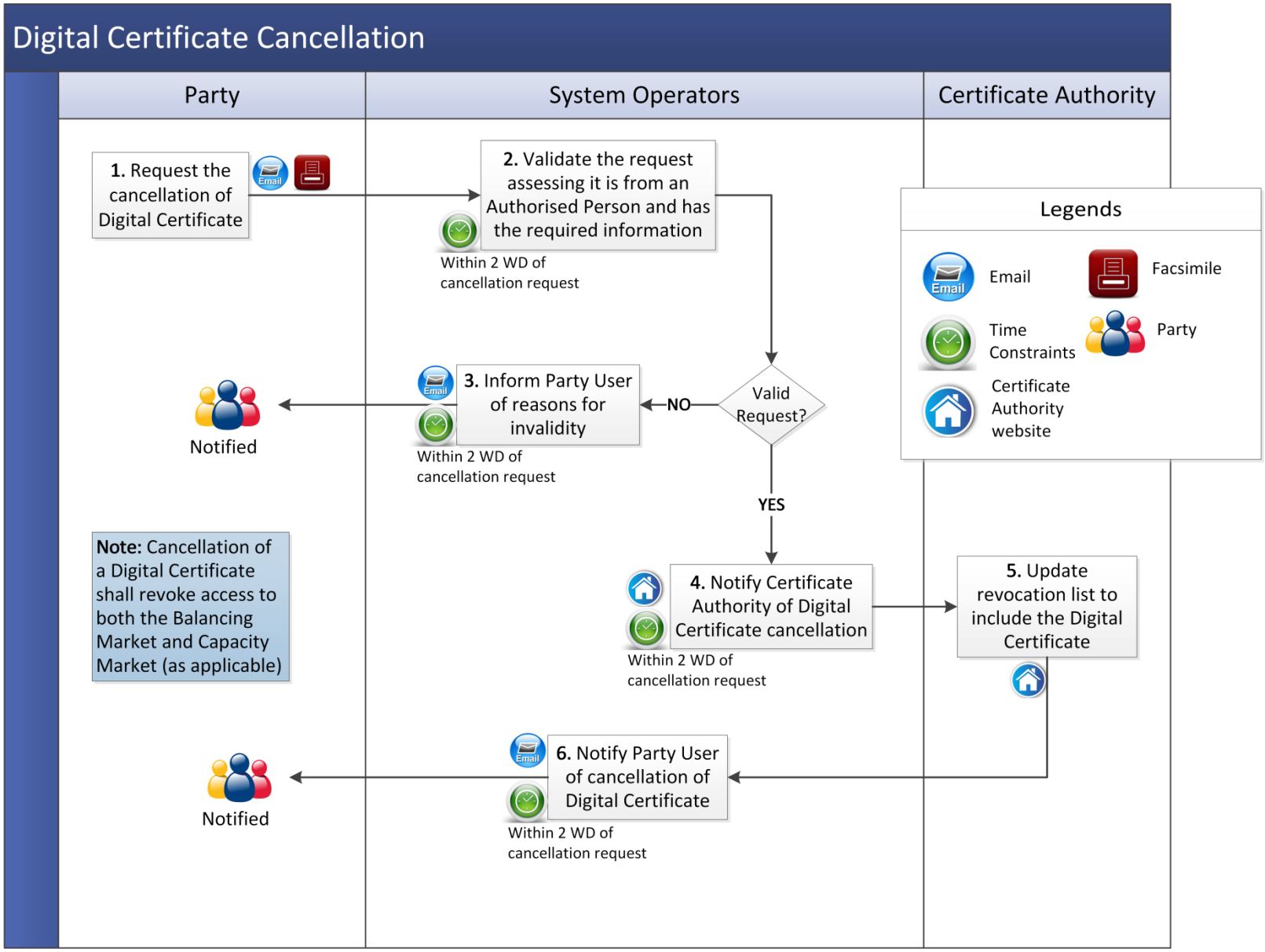
Step	Step Description	Timing	Method	By / From	To
1	A Digital Certificate request is made during registration for the Capacity Market. *Note:* If the Participant has obtained a Digital Certificate under the Trading and Settlement Code for access to the Balancing Market that Digital Certificate permits access to the Capacity Market Interface.	As required	In accordance with Agreed Procedure 1 "Registration"	Party	System Operators
2	Inform the Certificate Authority that the Party User has been authorised to receive a Digital Certificate.	Within 2 WD of request	Certificate Authority website	System Operators	Certificate Authority
3	Notify the Party User of authorisation to obtain a Digital Certificate and provide link to the Certificate Authority's enrolment webpage.	Within 2 WD of request	Email	System Operators	Party
4	Access Certificate Authority's enrolment webpage and enter required information.	As required	Certificate Authority website	Party	-
5	Check that the Party User is authorised and issue PIN and URL.	Within 1 WD receipt of required information	Email	Certificate Authority	Party
6	Download and install Digital Certificate using URL and PIN.	As required	Certificate Authority website	Party	-
7	Notify System Operators of the Digital Certificate serial number.	-	Email	Party	System Operators
8	System Operators update User access details with the	-	-	System Operators	-

Step	Step Description	Timing	Method	By / From	To
	Digital Certificate serial number.				
9	Log-in to the Capacity Market Interface and change password as prompted.		Certificate Authority website / Capacity Market Interface	Party	-


Obtaining a Digital Certificate
Party
Certificate Authority
System Operators
Note If the Participant has obtained a Digital Certificate under the Trading and Settlement Code for access to the Balancing Market that Digital Certificate permits access to the Capacity Market Interface
1. Request a Digital Cert
When registering for the Capacity Market
AP1
2. Inform the Certificate Authority that the User has been authorised to receive a Digital Certificate
Within 2WD of request
3. Notify the User of authorisation and provide link to the Certificate Authority's enrolment webpage
Within 2WD of request
Email
4. Access Certificate Authority's enrolment webpage and enter required information
5. Check that the User is authorised and issue PIN and URL
Within 1WD of receipt of required information
Email
6. Download and install Digital Certificate
7. Notify the SOs of Digital Cert serial number
Email
8. Update User access details with Digital Cert number
9. Log-in to the Capacity Market Interface by entering password details
SECURE ACCESS
Legends
Email
Email
Certificate Authority website
Capacity Market Interface
Time Constraints
Agreed Procedure

3.3 Digital Certificate Cancellation

Step	Step Description	Timing	Method	By / From	To
1	Request the cancellation of Digital Certificate. *Note:* Cancellation of a Digital Certificate shall revoke access to both the Balancing Market and Capacity Market (as applicable).	As required	Email / Facsimile	Party	System Operators
2	Validate the request assessing whether it contains all the required information and is from an appropriate Authorised Person. If valid go to step 4, otherwise continue to step 3.	Within 2 WD of cancellation request	-	System Operators	-
3	Inform Party User of reasons for invalidity, **end process.**	Within 2 WD of cancellation request	Email	System Operators	Party
4	Notify Certificate Authority of Digital Certificate cancellation.	Within 2 WD of cancellation request	Certificate Authority website	System Operators	Certificate Authority
5	Update revocation list to include the Digital Certificate.	-	Certificate Authority website	Certificate Authority	-
6	Notify Party User of cancellation of Digital Certificate.	Within 2 WD of cancellation request	Email	System Operators	Party

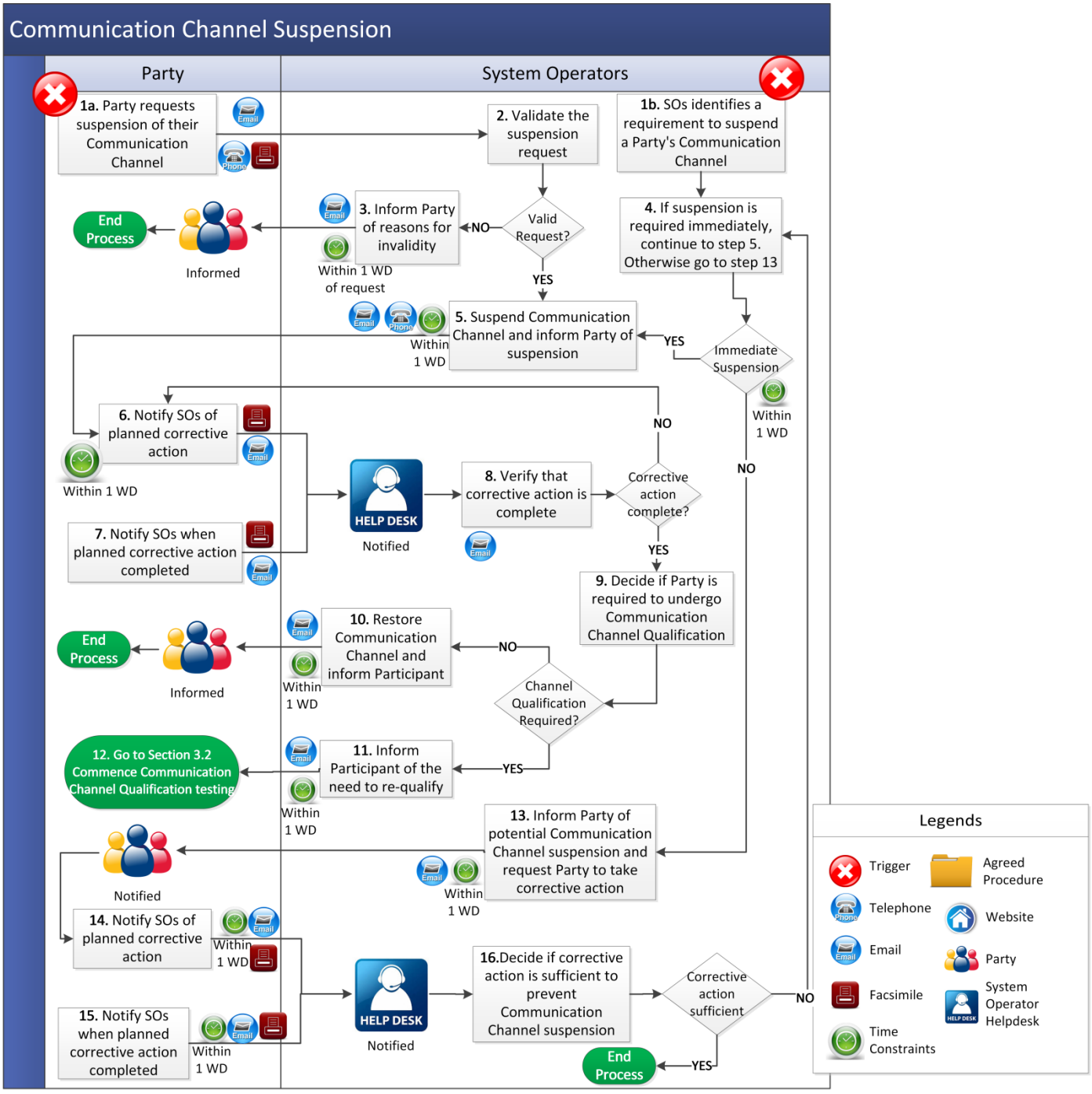

Digital Certificate Cancellation
Party
System Operators
Certificate Authority
1. Request the cancellation of Digital Certificate
2. Validate the request assessing it is from an Authorised Person and has the required information
Within 2 WD of cancellation request
Valid Request?
NO
3. Inform Party User of reasons for invalidity
Within 2 WD of cancellation request
Notified
YES
4. Notify Certificate Authority of Digital Certificate cancellation
Within 2 WD of cancellation request
5. Update revocation list to include the Digital Certificate
6. Notify Party User of cancellation of Digital Certificate
Within 2 WD of cancellation request
Notified
Note: Cancellation of a Digital Certificate shall revoke access to both the Balancing Market and Capacity Market (as applicable)
Legends
Email
Facsimile
Time Constraints
Party
Certificate Authority website

3.4 Communication Channel Suspension

Step	Step Description	Timing	Method	By / From	To
1	If: (a) a Party requests suspension of Communication Channel, go to step 2; or (b) the System Operators identify a requirement to suspend a Party's Communication Channel, go to step 4.	As required	Email and Telephone / Facsimile	Party System Operators	System Operators
2	Validate the suspension request assessing whether it has the required information is from an appropriate Authorised Person. If valid go to step 5, otherwise continue to step 3.	-	-	System Operators	-
3	Inform Party of reasons for invalidity, **end process.**	Within 1 WD	Email	System Operators	Party
4	If suspension is required immediately, continue to step 5. Otherwise go to step 13.	-	-	System Operators	-
5	Suspend Communication Channel and inform Party of suspension.	Within 1 WD	Email and Telephone	System Operators	Party
6	Notify System Operators of planned corrective action.	Within 1 WD	Email / Facsimile	Party	System Operators
7	Notify System Operators when planned corrective action completed.	Within timelines notified to the System Operators in	Email / Facsimile	Party	System Operators

Step	Step Description	Timing	Method	By / From	To
		step 6			
8	Verify that corrective action is complete. If corrective action is not complete, notify Party and return to step 6. If corrective action is complete continue to step 9.	As soon as practicable following notification at step 7	Email	System Operators	Party
9	Decide if Party is required to undergo Communication Channel Qualification. If re-qualification is not necessary continue to step10. If qualification is required, go to step 11.	-	-	System Operators	-
10	Restore Communication Channel and inform Party, **end process**	Within 1 WD	Email	System Operators	Party
11	Inform Party of the need to re-qualify for Communication Channel.	Within 1 WD	Email	System Operators	Party
12	Commence Communication Channel Qualification testing procedure at section 3.2, **end process**.	-	-	Party	-
13	Inform Party of potential Communication Channel suspension and request Party to take corrective action.	Within 1 WD	Email	System Operators	Party
14	Notify System Operators of planned corrective action.	Within 1 WD	Email / Facsimile	Party	System Operators
15	Notify System Operators when planned corrective action completed.	As specified in step 14	Email / Facsimile	Party	System Operators

Step	Step Description	Timing	Method	By / From	To
16	Decide if Party corrective action is sufficient to prevent Communication Channel suspension. If corrective action sufficient, **end process**. If corrective action is insufficient return to step 4.	-	-	System Operators	-


Communication Channel Suspension
Party
System Operators
1a. Party requests suspension of their Communication Channel
2. Validate the suspension request
1b. SOs identifies a requirement to suspend a Party's Communication Channel
3. Inform Party of reasons for invalidity
NO
Valid Request?
YES
Within 1 WD of request
End Process
Informed
4. If suspension is required immediately, continue to step 5. Otherwise go to step 13
5. Suspend Communication Channel and inform Party of suspension
Within 1 WD
YES
Immediate Suspension
Within 1 WD
NO
NO
6. Notify SOs of planned corrective action
Within 1 WD
7. Notify SOs when planned corrective action completed
HELP DESK
Notified
8. Verify that corrective action is complete
Corrective action complete?
YES
9. Decide if Party is required to undergo Communication Channel Qualification
End Process
Informed
10. Restore Communication Channel and inform Participant
Within 1 WD
NO
Channel Qualification Required?
YES
11. Inform Participant of the need to re-qualify
Within 1 WD
12. Go to Section 3.2 Commence Communication Channel Qualification testing
13. Inform Party of potential Communication Channel suspension and request Party to take corrective action
Within 1 WD
Notified
14. Notify SOs of planned corrective action
Within 1 WD
15. Notify SOs when planned corrective action completed
Within 1 WD
HELP DESK
Notified
16.Decide if corrective action is sufficient to prevent Communication Channel suspension
Corrective action sufficient
NO
YES
End Process
Legends
Trigger
Agreed Procedure
Telephone
Website
Email
Party
Facsimile
System Operator Helpdesk
Time Constraints

APPENDIX 1: DEFINITIONS

Authorised Person	means the representative of a Party who is authorised by that Party to communicate with the System Operators.
Capacity Market Interface	means the function within the Capacity Market Platform that interfaces to the Type 2 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.
Digital Certificate	means an electronic credential issued and digitally signed 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 organizational public key.
Functional Area	means the different parts of the Capacity Market Platform that Users may be provided access to as set out in in Agreed Procedure 1 "Registration".
Party Certification Environment	means a Test Environment which allows a Party to test their ability to interact with Capacity Market Platform functionality.
Party Administrative User	means the person who creates and maintains the User information pertaining to a Party.
Test Environment	means a non-production version of a Capacity Market Platform used for test purposes prior to an update to the Capacity Market Platform.
User	means: (a) in relation to a Party, a nominated member of a Party staff who is authorised to utilise qualified Communication Channels that interact with the Capacity Market Platform; and (b) in relation to the System Operators, a member of the System Operators' staff who has been authorised to access

	specific parts of the Capacity Market Platform. The procedure in relation to registration of User access rights is set out in Agreed Procedure 1 “Registration”.
Web Services	means the automated communication consisting of an XML-based programmatic interface.

APPENDIX 2: AUTHORISATION CATEGORIES

Authorised Categories A

Category	Description	Agreed Procedure
A	Declare Limited Communication Failure request	Agreed Procedure 5, Agreed Procedure 6

Authorised Categories B

The following Authorised Categories list is not covered under the User Authorisations section of the Capacity Market Interface. However, these processes can be activated by Users that have sufficient access privileges to normally perform these tasks via the Capacity Market Interface, but due to a Limited Communications Failure are unable to do so.

Category	Description	Agreed Procedure	Authorised Person
1	Submit/Modify Unit Registration and/or Interconnector Data	Agreed Procedure 1	Registration User
2	Request Capacity Auction Bid/Offer Data	Agreed Procedure 3	User with trading access
3	Ad hoc Report request	-	As per requester Capacity Market Interface access
4	Requesting Digital Certificates	Agreed Procedure 4	Party Administrative User
5	Requesting Qualification Data		User with Trading Access