|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **MODIFICATION PROPOSAL FORM** | | | | | |
| **Proposer** | **Date of receipt** | | **Type of Proposal** | | **Modification Proposal ID** |
| **SEMO** | **21 November 2013** | | **Standard** | | **Mod\_11\_13** |
| **Contact Details for Modification Proposal Originator** | | | | | |
| **Name** | | **Telephone number** | | **Email address** | |
| **Mike Harrington** | | **(01) 23 70445** | | **Michael.Harrington@sem-o.com** | |
| **Modification Proposal Title** | | | | | |
| **Amendment of AP5 to update the encryption key standard from 1024 bit to 2048 bit** | | | | | |
| **Documents affected** | | **Section(s) Affected** | | **Version number of T&SC or AP used in Drafting** | |
| **AP5** | | **2.1.1.1** | | **V13.0** | |
| **Explanation of Proposed Change**  *(mandatory by originator)* | | | | | |
| Section 2.1.1.1 of Agreed Procedure 5 (AP5) details that Digital Certificates using the ITU-T X.509 1024-bit asymmetric encryption standard are required for Type 2 and Type 3 Channel Communication with the Market Operator Isolated Market System.  Given developments in internationally accepted internet communication security standards it is has been necessary to move from 1024-bit encryption keys to 2048 bit keys for Type 2 and Type 3 Channel Communication.  The Certificate Authority (CA) used by the Market Operator has actually adopted a 2048-bit standard for all new and renewed Digital Certificates issued to Market Participants since 2010. In general, Market Participants would not have noticed the change as all the major internet browsers (e.g. Microsoft Internet Explorer) are compatible with 2048-bit keys. Any Market Participant that renewed or installed a certificate since 2010 will be at 2048-bit level.  This modification proposal would update the encryption level detailed in Section 2.1.1.1 of AP5 from 1024-bit to 2048-bit. This would reflect the current encryption standard being used by the Market Operator. Market Participants would continue to obtain and renew digital certificates in the usual way and this modification proposal would not impact on any other areas of the Code. | | | | | |
| **Legal Drafting Change**  *(Clearly show proposed code change using* ***tracked*** *changes, if proposer fails to identify changes, please indicate best estimate of potential changes)* | | | | | |
| 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 2048 bit keys. | | | | | |
| **Modification Proposal Justification**  *(Clearly state the reason for the Modification)* | | | | | |
| As a pre-emptive action against security threats and in compliance with Certification Authority/Browser forum requirements based on NIST Special Publication 800-131A, at the end of 2013 all web browsers and Certification Authorities (CAs) will no longer sell or support 1024-bit RSA certificates.  The Certificate Authority used by the Market Operator has adopted a 2048-bit standard for all new and renewed Digital Certificates issued to Market Participants since 2010.  The proposed change to Section 2.1.1.1 of Agreed Procedure 5 would ensure that it is correctly aligned with the current security standard used by the Market Operator. The update to 2048-bit keys is required by the Certificate Authority and adheres to current internationally accepted standards on secure internet communication.  Encryption technology and standards evolve to meet security demands. It is possible that the encryption standard could change again in the future, which may require another change to AP5. A more general description could be used in Section 2.1.1.1 of AP5, but it is considered important to give clear details of the current encryption standard being used so that Participants can ensure their technology is compatible.  It is in the interest of all Parties to the Code that secure Communications Channels are maintained. Market Participants will continue to obtain and renew Digital Certificates in the usual way outlined in the Code. | | | | | |
| **Code Objectives Furthered**  *(State the Code Objectives the Proposal furthers, see Section 1.3 of T&SC for Code Objectives)* | | | | | |
| 1.3.1. To facilitate the efficient discharge by the Market Operator of the obligations imposed upon it by its Market Operator Licences  1.3.5. To provide transparency in the operation of the Single Electricity Market | | | | | |
| **Implication of not implementing the Modification Proposal**  *(State the possible outcomes should the Modification Proposal not be implemented)* | | | | | |
| Should this modification not be implemented, then Agreed Procedure 5 will not accurately reflect the latest Encryption standard that is used for Type 2 and Type 3 communication with the Market Operator Isolated Market System. | | | | | |
| **Working Group**  *(State if Working Group considered necessary to develop proposal)* | | | **Impacts**  *(Indicate the impacts on systems, resources, processes and/or procedures)* | | |
| No. | | | No systems change is required. | | |
| ***Please return this form to Secretariat by email to*** [***modifications@sem-o.com***](mailto:modifications@sem-o.com) | | | | | |

**Notes on completing Modification Proposal Form:**

1. **If a person submits a Modification Proposal on behalf of another person, that person who proposes the material of the change should be identified on the Modification Proposal Form as the Modification Proposal Originator.**
2. **Any person raising a Modification Proposal shall ensure that their proposal is clear and substantiated with the appropriate detail including the way in which it furthers the Code Objectives to enable it to be fully considered by the Modifications Committee.**
3. **Each Modification Proposal will include a draft text of the proposed Modification to the Code unless, if raising a Provisional Modification Proposal whereby legal drafting text is not imperative.**
4. **For the purposes of this Modification Proposal Form, the following terms shall have the following meanings:**

**Agreed Procedure(s): means the detailed procedures to be followed by Parties in performing their obligations and functions under the Code as listed in Appendix D “List of Agreed Procedures”.**

**T&SC / Code: means the Trading and Settlement Code for the Single Electricity Market**

**Modification Proposal: means the proposal to modify the Code as set out in the attached form**

**Derivative Work: means any text or work which incorporates or contains all or part of the Modification Proposal or any adaptation, abridgement, expansion or other modification of the Modification Proposal**

**The terms “Market Operator”, “Modifications Committee” and “Regulatory Authorities” shall have the meanings assigned to those terms in the Code.**

**In consideration for the right to submit, and have the Modification Proposal assessed in accordance with the terms of Section 2 of the Code (and Agreed Procedure 12), which I have read and understand, I agree as follows:**

**1. I hereby grant a worldwide, perpetual, royalty-free, non-exclusive licence:**

* 1. **to the Market Operator and the Regulatory Authorities to publish and/or distribute the Modification Proposal for free and unrestricted access;**
  2. **to the Regulatory Authorities, the Modifications Committee and each member of the Modifications Committee to amend, adapt, combine, abridge, expand or otherwise modify the Modification Proposal at their sole discretion for the purpose of developing the Modification Proposal in accordance with the Code;**
  3. **to the Market Operator and the Regulatory Authorities to incorporate the Modification Proposal into the Code;**

**1.4 to all Parties to the Code and the Regulatory Authorities to use, reproduce and distribute the Modification Proposal, whether as part of the Code or otherwise, for any purpose arising out of or in connection with the Code.**

**2. The licences set out in clause 1 shall equally apply to any Derivative Works.**

**3. I hereby waive in favour of the Parties to the Code and the Regulatory Authorities any and all moral rights I may have arising out of or in connection with the Modification Proposal or any Derivative Works.**

**4. I hereby warrant that, except where expressly indicated otherwise, I am the owner of the copyright and any other intellectual property and proprietary rights in the Modification Proposal and, where not the owner, I have the requisite permissions to grant the rights set out in this form.**

**5. I hereby acknowledge that the Modification Proposal may be rejected by the Modifications Committee and/or the Regulatory Authorities and that there is no guarantee that my Modification Proposal will be incorporated into the Code.**