This document is classified as **Green** in accordance with the Panel Information Policy. Information can be shared with other SEC Parties and SMIP stakeholders at large, but not made publicly available.

MP104
'Security Improvements'

Modification Report

Version 0.4

12 February 2021

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

This document also has three annexes:

- **Annex A** contains the business requirements for the solution (**Green**)
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution (**Green**)
- **Annex C** contains the full Data Communications Company (DCC) Preliminary Assessment response (**Green**)

Contact

If you have any questions on this modification, please contact:

Ali Beard

0203 970 1105

alison.beard@gemserv.com

1. Summary

This proposal was raised by Gordon Hextall on behalf of the Security Sub-Committee (SSC).

Users are required to Digitally Sign Extensible Markup Language (XML) format Service Requests and Signed Pre-Commands with a User Role Signing Private Key. That Key must be a separate dedicated Key and must not be used for communication with Devices.

The SSC is concerned that Keys could be used incorrectly. However, without the means to validate the use of separate Keys there is no way to monitor if or how frequently this occurs and no way to advise Users to enable them to ensure they are compliant with the SEC.

The Proposed Solution seeks to mandate, alongside the Enduring Change of Supplier (ECoS) changes, the requirement for Service Users to use a dedicated Private Key to sign XML format Service Requests and Pre-Signed Commands whilst continuing to use their Digital Signing Private Key for GBCS commands.

In addition, the DCC is required to provide a monthly report of Service Users who are not using the new XML User Role Signing Private Key to sign XML format messages.

This modification has an impact on all SEC Parties that are DCC Users, and the DCC Systems. The cost to make the changes to the DCC System will be approximately £170,000-£280,000. This is a Self-Governance modification and the DCC System changes are targeted for implementation in the June 2022 SEC Release alongside the implementation of the ECoS arrangements. The DCC reporting requirements will be in place approximately six months before (around December 2021).

2. Issue

What are the current arrangements?

SEC Appendix AD 'DCC User Interface Specification' (DUIS) section 3.3.1 states that Users shall Digitally Sign every XML format Service Request and Signed Pre-Command sent to the DCC using a User Role Signing Private Key.

That User Role Signing Private Key must be a separate dedicated Key that must not be used for communication with Devices (i.e. different to the Digital Signing Private Key that is used to sign the GB Companion Specification (GBCS) Payload held within Signed Pre-Commands), and a separate User Role Signing Private Key must be used per User Id in use for each User.

Alongside the November 2020 SEC Release the Department for Business, Energy & Industrial Strategy (BEIS) designated new functionality which introduced a new type of Organisation Certificate with the Remote Party Role of xmlSign. The associated Private Key is dedicated for Users to Digitally Sign the XML format Service Requests and Signed Pre-Commands.

What is the issue?

The SSC is concerned that Users could use the same Private Key to sign both the DUIS XML format Service Requests as well as the GBCS Payloads. To ensure the proper application of the SEC

security arrangements, and to help support the Security Controls Framework, the SSC believes a requirement for the DCC to validate the use of separate Keys should be introduced.

What is the impact this is having?

Without the means to validate the use of separate Keys, there is no way to monitor how frequently this might occur and no way to advise Users to enable them to ensure they are compliant with the SEC.

Impact on consumers

This issue has no impact on consumers.

3. Solution

Proposed Solution

The Proposed Solution seeks to validate that Users have used an XML User Role Signing Private Key to sign XML format Service Requests and Signed Pre-Commands that is different to the Digital Signing Private Key used to sign GBCS commands.

The solution can be broken into two sections:

- Reporting Usage of XML wrappers Digitally Signed with Keys different from the XML User Role Signing Private Key
- Cease processing of XML wrappers which are not Digitally Signed with the XML User Role Signing Private Key

The Proposed Solution requires changes to the Data Services Provider (DSP).

Reporting usage of XML wrappers not using XML User Role Signing Private Keys

As part of the reporting changes, the DSP will build a mechanism to track the Key used by the Service Users to sign the XML format Service Requests and Signed Pre-Commands. This will be used to generate a monthly report that contains the list of any Service Users who incorrectly use the Keys not associated with XML Signing Certificates to sign the XML format Service Requests and Signed Pre-Commands during a given month. The monthly report will be generated and manually transferred to the DCC's SharePoint. Parties that can access this report will be specified in the DCC's Impact Assessment. The monthly report will contain:

- Service User ID
- Certificate used (for each Certificate)
- Latest time of use

The reporting capability of the Proposed Solution needs to be made available in advance of the enforcement part of the solution; this will enable the reporting to be used to identify and help Users comply with the SEC.

Cease processing of XML wrappers which are not Digitally Signed with the XML User Role Signing Private Key

The DSP will amend the Service User validation checks to verify that every XML format Service Request and Signed Pre-Command submitted by a Service User has been signed using the XML User Role Signing Private Key. Once implemented, if the validation check is failed, the DSP will reject the XML format Service Request or Signed Pre-Command using a new Response Code specifically for this scenario. This new Response Code will be available as part of a new DUIS version. If Service Users use a version of the DUIS that does not support the new Response Code, they will be notified using the existing Response Code E100.

All Service Users will be required to use the XML User Role Signing Private Key for Digitally Signing XML format Service Request and Signed Pre-Command. They must obtain a new Smart Metering Key Infrastructure (SMKI) Organisation Certificate with the Remote Party Role of xmlSign.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
✓	Electricity Network Operators	✓	Gas Network Operators
✓	Other SEC Parties	✓	DCC

Breakdown of Other SEC Party types impacted			
✓	Shared Resource Providers	✓	Meter Installers
✓	Device Manufacturers		Flexibility Providers

This modification has an impact on all Service Users as they will be required to use a new SMKI Certificate to Digitally Sign XML format Service Request and Signed Pre-Command. There is also an impact on Parties as a new Response Code for non-compliant Digitally Signed XML format Service Request and Signed Pre-Command will be added to the DUIS.

DCC System

System changes will be made to the Service User validation checks to verify that all XML format Service Requests and Signed Pre-Commands submitted by a Service User have been signed using the XML User Role Signing Private Key.

The full impacts on DCC Systems and DCC's proposed testing approach can be found in the DCC Preliminary Assessment response in Annex C.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section A 'Definitions and Interpretation'
- Appendix AB 'Service Request Processing Document'
- Appendix AD 'DCC User Interface Specification' (DUIS)

The changes to the SEC required to deliver the proposed solution can be found in Annex B.

Technical specification versions

The ECoS changes are targeted for implementation alongside the June 2022 SEC Release and will require an uplift of the DUIS. Therefore, the implementation approach of this modification will be aligned with the ECoS changes to prevent needing a separate DUIS uplift within the same calendar year.

Consumers

There are no impacts to consumers in this modification.

Other industry Codes

This modification has no impact on other industry Codes.

Greenhouse gas emissions

This modification has no impact on greenhouse gas emissions.

5. Costs

DCC costs

The estimated DCC implementation costs to implement this modification is £170,000-£280,000. As this change only impacts one Service Provider the cost has been provided as a range to preserve commercial confidentiality. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Cost**
Design, Build and Pre-Integration Testing (PIT)	£170,000-£280,000
Systems Integration Testing (SIT)	TBC
User Integration Testing (UIT)	TBC
Implement to Live	TBC
Application Support	TBC

More information can be found in the DCC Preliminary Assessment response in Annex C.

SECAS costs

The estimated SECAS implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **30 June 2022** (June 2022 SEC Release) if a decision to approve is received on or before 31 July 2021; or
- **3 November 2022** (November 2022 SEC Release) if a decision to approve is received after 31 July 2021 but on or before 31 December 2021.

This is a DCC System impacting change. The system changes in this modification are targeted for implementation in the June 2022 SEC Release. The DCC plans to implement the reporting requirements of this modification in late 2021/early 2022, as the reporting capability being delivered earlier will allow the reporting to identify and ensure DCC Users are compliant with the SEC before the enforced use of the signing certificate and subsequent rejection of incorrectly signed commands. Full functionality would ideally be aligned with the ECoS changes going live in June 2022.

7. Assessment of the proposal

Observations on the issue

The Change Sub-Committee (CSC) recognised the need for the proposal and that the issue it seeks to address is clear. The Technical Architecture and Business Architecture Sub-Committee (TABASC) and the SSC were supportive of the change to ensure the security of the system. No other comments were received.

Solution development

On 14 January 2020 BEIS published a consultation[1] seeking stakeholder views; part of this consultation was around XMLSigning Certificates and associated Private Signing Keys. The consultation advised that discussion had taken place with the SMKI Policy Management Authority (PMA) and the SSC. The consultation proposed to introduce an XML Signing Certificate as a new type of Organisation Certificate. This would allow the DCC to validate that Users are using a dedicated Private Key to sign XML format Service Requests and Pre-Signed Commands whilst continuing to use their Digital Signing Private Key for GBCS commands. The consultation proposed changes to the SEC to introduce the use of these new types of Certificates and associated Private Signing Key.

Subsequently, at the February 2020 SMKI PMA meeting[2], the DCC confirmed that it will be ready to create new XML Signing Roles following the publication of the BEIS consultation response. During the SMKI PMA meeting, a BEIS Representative advised that the Government consultation responses expressed concern that the introduction of new XML Signing Roles will introduce new regulation. The SMKI PMA Chair confirmed that wording has been added into MP104, which, once implemented, will run in parallel with the introduction of the new Roles.

During the March 2020 SSC meeting[3], The SSC Chair informed SSC Members that the proposed SEC legal drafting was available to SSC Members and will be shared with BEIS to ensure a consistent approach with the BEIS proposals for using the XML Digital Signing Key as part of ECoS processes.

The Working Group was provided with an update at the January 2021 meeting. It agreed that the issue was clear, whilst also agreeing that the SSC should be used as a Working Group as the modification progresses, due to the security implications of the modification.

The DCC returned the Preliminary Assessment on 27 January 2021. The solution, impacts, and cost of the modification were presented to the SSC on 24 February 2021. The SSC was generally in agreement and had no further observation or action required regarding the Preliminary Assessment. The SSC discussed who may be authorised to access the DCC SharePoint as part of the monthly reporting capability of the solution. The SSC provided guidance on this, and SECAS consequently recommended to the DCC that the authorised person(s) who can access the DCC SharePoint should be clarified. The DCC advised that this will be highlighted in the full Impact Assessment. The Proposer agreed with this approach.

[1] Consultation on changes to Standard Conditions of Gas and Electricity Supply Licences, conditions of the DCC Licence, the SEC, the UNC and the MRA
[2] SECPMA_66_2502
[3] SSC_97_2503 (**RED**)

The Working Group was updated again in March 2021, following the return of the Preliminary Assessment. One Working Group member questioned if an update was needed to the Security Controls Framework (SCF). The Chair of the SSC, who was present at the meeting confirmed that an update to the SCF was taking place on 3 March to accommodate these changes.

Support for Change

The Working Group, SSC and SMKI-PMA all confirmed that they are supportive of these changes.

Views against the General SEC Objectives

Proposer's views

The Proposer believes this modification will better facilitate SEC Objective (a)[4] as the modification improves the efficiency and operation of smart metering systems, and Objective (f)[5] as the modification will improve the security of data and systems of the SEC.

Views against the consumer areas

Improved safety and reliability

If implemented, this modification will have a neutral impact against this consumer area but will improve the overall safety of the Smart Metering programme.

Lower bills than would otherwise be the case

If implemented, this modification will have a neutral impact against this consumer area.

Reduced environmental damage

If implemented, this modification will have a neutral impact against this consumer area.

Improved quality of service

If implemented, this modification will have a neutral impact against this consumer area.

Benefits for society as a whole

If implemented, this modification will have a neutral impact against this consumer area.

[4] Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

[5] Ensure the protection of Data and the security of Data and Systems in the operation of this Code

Appendix 1: Progression timetable

This modification will be taken issued for Refinement Consultation and an Impact Assessment Requested.

Timetable	
Event/Action	**Date**
Draft Proposal raised	18 Dec 2019
Presented to CSC for final comment and recommendations	28 Jan 2020
Panel converts Draft Proposal to Modification Proposal	14 Feb 2020
Solution Development	16 Mar 2020
Business requirements developed with Proposer, DCC and TABASC chair	13 Oct 2020
Business requirements discussed with SSC	25 Nov 2020
Preliminary Assessment requested	16 Nov 2020
Modification discussed with Working Group	6 Jan 2021
Preliminary Assessment returned	26 Jan 2021
Modification discussed with SSC	24 Feb 2021
Modification discussed with Working Group	3 Mar 2021
Modification discussed with TABASC	4 Mar 2021
Refinement Consultation	29 Mar 2021 – 20 Apr 2021

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
BEIS	Department for Business, Energy and Industrial Strategy
CSC	Change Sub-Committee
DCC	Data Communications Company
DSP	Data Services Provider
DUIS	DCC User Interface Specification
ECoS	Enduring Change of Supplier
GBCS	GB Companion Specification
PIT	Pre-Integration Testing
SCF	Security Controls Framework
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	System Integration Testing

Glossary	
Acronym	**Full term**
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
UIT	User Integration Testing
XML	Extensible Markup Language