Data Communications Company

SEC Modification Proposal, SECMP0129, DCC CR4386

Allowing the use case of CNSA Variant for ECDSA

Preliminary Impact Assessment (PIA)

Version:	**0.4**
Date:	**22nd September, 2021**
Author:	**DCC**
Classification:	**DCC Public**

Data Communications Company

Contents

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to complete the Full Impact Assessment of £19,787
- The timescales to complete the Full Impact Assessment of 30 days
- ROM costs for SECMP0129, up to the end of Pre-Integration Testing (PIT) of between £0 and £150,000

Problem Statement and Solution

Cryptographic signing is an important element in the securing and transmission of Critical Commands. However, the Great Britain Companion Specification (GBCS) only refers to the Elliptic Curve Digital Signature Algorithm (ECDSA) cryptographic algorithm for Critical Command signing. The Commercial National Security Algorithm (CNSA) variant is recognised as a more cost-effective and more widely used variant than the ECDSA variant.

The SEC Technical Specifications shall be updated so that they clearly permit the use of the CNSA variant, but must remain optional and not replace the ECDSA variant.

Modification Benefit

Suppliers as well as the Data Services Provider (DSP), routinely carry out Critical Command Signing and they could significantly benefit from this modification, should they choose to use the CNSA variant.

Moving to the standard CNSA variant for ECDSA signing is expected to improve the performance of the Hardware Security Modules, reduce ongoing maintenance effort, and reduce DSP Operational Support charges. A corresponding reduction in the DSP ongoing service charge is anticipated.

DCC notes that related, specific DSP certificate-based functions such as SMKI Recovery, Transitional Change of Supplier (TCoS) to Enduring Change of Supplier (ECoS) migration, and Hardware Security Module performance would show significant performance improvements. The current version can process about 30 certificates per second, while implementing the CNSA variant is expected to accelerate this processing to between 300 and 500 certificates/second.

DCC notes that the legal text should be changed to permit the use of the CNSA variant, but must remain optional.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
23/08/2021	0.1	Initial DCC Review with Service Providers
25/08/2021	0.3	Internal review
22/09/2021	0.4	Amended following SECAS feedback

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP129 Modification Report v0.5	SECAS	23/12/2020
2	MP129 Business Requirements v0.1	SECAS	12/07/2021

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is David Rollason of Smart DCC.

The Preliminary Impact Assessment was requested of DCC on 12th July 2021, and accepted on the 16th July 2021.

3 Context and Requirements

In this section, the context of the Modification, assumptions, and the requirements are stated.

The requirements have been provided by SECAS, the Proposer, and the Working Group.

3.1 Context

The GBCS Section 4.3.3.2 defines how a Smart Metering Entity should create a “Per-Message Secret Number ‘k’ with respect to Elliptic Curve Digital Signature Algorithm (ECDSA)” when applying Digital Signatures to meter communications. The ‘k’ is a Random Number Generator used in the algorithm to create a unique digital signature.

Smart Metering Entities are defined as, “An entity that is either a Device or a Remote Party”. A Remote Party is defined as “An entity which is remote from a Device and is able to either send Messages to or receive Messages from a Device, whether directly or via a third party. Suppliers Parties, the DSP are both Remote Parties and carry out Critical Command signing activities. The Communication Service Providers (CSPs) could also be considered Remote Parties.

3.2 Problem Statement

The Data Services Provider (DSP) considers itself to be a ‘Remote Party’ in the context of Smart Energy Code (SEC) Schedule 8 ‘GB Companion Specification’ (GBCS) Section 4.3.3.2. The DSP interpreted the GBCS as mandating the GBCS variant of Elliptic Curve Digital Signature Algorithm (ECDSA) for all Device Critical Command signing operations, rather than the more common Commercial National Security Algorithm (CNSA) Suite variant, which is approved by the National Institute of Standards and Technology (NIST).

The CNSA variant is recognised as a more cost-effective and more widely used variant for cryptographic signing than the ECDSA. However, the GBCS only refers to the ECDSA for Critical Command signing.

The Department for Business, Energy and Industrial Strategy (BEIS) advised that the DSP could have used the CNSA variant and remained compliant. The Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) agreed that the GBCS wording in Section 4.3.3.2 lacked clarity and would need to be updated to explicitly permit the use of CNSA by Remote Parties.

In terms of current issues, the main concern is that the GBCS wording is unclear whether the more common CNSA Suite variant is permitted. It should be noted that the CNSA Suite variant is easier for Users to implement and makes the process more efficient, and has very clear performance improvements associated with its use.

3.3 Business Requirement

There is one Requirement for this Modification.

Requirement 1: Parties shall be permitted to use the CNSA variant for Critical Command signing.

The CNSA variant is recognised as a more cost-effective and more widely used variant for cryptographic signing than the ECDSA variant. However, the GBCS only refers to the ECDSA variant for Critical Command signing.

The GBCS and any other SEC Technical Specifications shall be updated so that they clearly permit the use of the CNSA variant, but must remain optional and not replace the ECDSA variant.

Suppliers also routinely carry out Critical Command Signing and they could significantly benefit from this modification, should they choose to use the CNSA variant.

The CNSA variant must be implemented with a Federal Information Processing Standard (FIPS)-approved random number generator. This increases processing requirements, but has a higher level of security associated with the full implementation.

3.4 Proposed Solution

The Proposed Solution is to modify the GBCS so it clearly shows the CNSA variant is permitted for use as well as the ECDSA variant. This modification will not directly impact any Parties as it is not changing any obligations and only seeks to make the GBCS clearer. The legal text implementation costs will be limited to the Smart Energy Code Administrator and Secretariat (SECAS) time and effort.

System changes would be required by the DSP and any other Service Provider that wishes to adopt the CNSA variant.

As directed by SECAS, this solution should be applied to Smart Metering Equipment Technical Specifications (SMETS)1 and SMETS2 Devices. However SMETS1 does not use Critical Commands and the benefits would be minimal in applying this solution, such that SMETS1 usage has been discounted in this document.

4 Description of Technical Solution

Changes to the DSP are required for implementing the CNSA Variant solution. It should be noted that while the Communications Service Providers could implement the CNSA variant, the number of Critical commands sent to Communications Hubs is low, performance gains would be minimal, and the reduction in memory on the devices would have a negative effect and would most likely require Comms Hub changes.

4.1 DSP Solution

The existing GBCS variant of ECDSA is supported in the DSP using a custom library (named Phase2 API) provided by the Hardware Security Module (HSM) vendor, Thales. The solution would change this to the standard CNSA variant for ECDSA signing for (Access Control Broker) ACB and Recovery operations. Moving to the standard CNSA variant for ECDSA signing is expected to improve the performance of the HSMs and reduce ongoing maintenance effort. It is also expected to deliver performance improvement for the Recovery application.

It shall be noted that TCoS signing will continue to use the existing ECDSA variant, as TCoS will eventually be replaced by the ECoS service.

To change to the standard CNSA variant for ECDSA signing, DSP would make the following changes.

1. Modify the DSP implementation to use the standard ECDSA signing mechanism rather than using the Thales Phase2 API.
2. Modify the DSP implementation to support JCE/PKCS[1]11 keys, which are usable outside of the SEE (Secure Execution Engine) of HSMs.
3. Copy the existing digital signature keys and convert the copies to be usable by JCE such that the certificates in the Devices can remain unchanged. This will require DSP to upgrade the HSM client software.
4. Remove the SEE machines that are no longer required. The SEE machines are used to hold the existing keys. The associated Access Control Lists (ACL) shall also be removed.

The revised application code that supports the use of Standard CNSA shall be subject to a feature switch to allow for phased deployment and provide fail back if required. Item 4 above (Removal of the SEE machines) will only occur after the feature switch has been activated in each environment and successful operation has been confirmed.

It should also be noted that the recovery application is a special case function that is not updated via standard release processes as it is not network connected to core DSP in normal state. Its update will need to be subject to manual code deployment and specific testing.

[1] JCE is the Java Cryptography Extension, PKCS relates to Public-Key Cryptography Standards

5 Impact on Systems, Processes and People

This section describes the impact of SECMP0129 on Services and Interfaces that impact Users and/or Parties.

5.1 Security Impact

The implementation will be security assured throughout. This assurance includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

The DSP Security Team will be involved with each aspect of this change and activities will include, but are not limited to, development team support, key conversion, regression testing, reconfiguration of HSM for each environment and update of all security documentation reflecting the new Design. The Security Team will also be directly involved in supporting testing of the recovery function.

A more detailed Security impact will be carried out as part of the Full Impact Assessment.

The Security libraries will need to be modified to use the standard CNSA variant for ECDSA signing as described above.

5.2 Hardware Security Module

The SEE machines that are no longer required shall be removed from the HSMs. It shall be noted that a minimum of one SEE per environment is needed for supporting the Certificate Signing Request (CSR) for GMAC (Galois Message Authentication Code).

5.3 Infrastructure Impact

There will be no change to the infrastructure design as a result of this change. Additional processing and storage will be required; however, they are not sufficiently large to warrant the procurement of additional compute power or storage. The change does not impact the DSP resilience or DR implementation.

5.4 Service Impact

It is not thought that the change in behaviour of the DSP system from this Modification will have a material ongoing service impact. No changes to SLAs or reporting are expected as a result of this change. However, a more detailed service impact will be completed as part of the FIA.

5.5 Solution Benefits

The benefits of this Modification are operational in nature.

Moving to the standard CNSA variant for signing is expected to improve the performance of the HSMs and reduce ongoing maintenance effort and Operational Support charges. When implemented, there is expected to be a corresponding reduction in the DSP ongoing service charge.

Using the CNSA variant is also expected to deliver performance improvement for the SMKI Recovery application. The current version can process about 30 certificates per second, while implementing the CNSA variant is expected to accelerate this processing to between 300 and 500 certificates/second. This will benefit large scale certificate replacement activities

such as TCoS to ECoS Migration, and also any use of the SMKI Recovery application to replace compromised certificates.

6 Implementation Timescales and Approach

This change is expected to be included in a future SEC Release. Design, Build, and PIT is expected to take about three months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA. As noted in section 4.1, the HSM client software upgrade could be carried out as part of the DSP Technical Refresh activity. Since this version upgrade is a prerequisite for implementing this Modification, this Modification could be part of a release that includes the Tech Refresh activity or a later major release.

It is likely that the testing and deployment of updates to the recovery function will be aligned to extant recovery function activities (the regular (annual) SMKI Recovery testing that takes place) in order to minimise costs. However, this would act as a major timeline dependency for the delivery of this Modification and alternative plans might be developed in the FIA.

6.1 Testing and Acceptance

There will be an impact to Systems Integration Testing (SIT) as a result of this change. SIT activities will include test preparation, execution and reporting as required, as well as Service Request Variant (SRV) testing to verify the use of critical commands on selected devices.

The System Integrator will be required to manage the testing. It should be noted that the additional costs for SIT are likely to be similar to Design, Build, and PIT costs, and the scale of the costs is due to testing certificates with the HSM. These costs will be included in the Full Impact Assessment (FIA).

There is no perceived requirement to test this Modification in User Integration Testing (UIT).

7 Costs and Charges

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional requirements. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change during discussions with the DCC. As a result the final offer price may result in a variation.

The table below details the cost of delivering the changes and Services required to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

	Design, Build and PIT	Days to Create FIA	Cost to Create FIA
DSP	£0 to £150,000	30	£19,787

Table 2: SECMP0129 Standalone Cost

The phases included are as follows.

Design	The production of detailed System and Service designs to deliver all new requirements.
Build	The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented. It includes Unit Testing (also referred to as System Testing), Performance Testing and Factory Acceptance Testing by the Service Provider or supplier.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.

Based on the existing requirements, the fixed price cost for a Full Impact Assessment is **£19,787** and would be expected to be completed in 30 days.

7.1 Legal Text Changes

For the legal text change, SECAS recommends this be a Self Governance Modification.

Legal text implementation costs will be limited to the Smart Energy Code Administrator and Secretariat (SECAS) time and effort.

Appendix A: Glossary

The table below provides definitions of the terms used in this document.

Acronym	Definition
ACB	Access Control Broker
ACL	Access Control List
CAN	Contract Amendment Note
CNSA	Commercial National Security Algorithm
CR	DCC Change Request
CSP	Communication Service Provider
CSR	Certificate Signing Request
DCC	Data Communications Company
DSP	Data Service Provider
ECDSA	Elliptic Curve Digital Signature Algorithm
ECoS	Enduring Change of Supplier
FIA	Full Impact Assessment
FIPS	Federal Information Processing Standard
GBCS	Great Britain Companion Specification
GMAC	Galois Message Authentication Code
HSM	Hardware Security Module
JCE	Java Cryptography Extension
NIST	National Institute of Standards and Technology
PIA	Preliminary Impact Assessment
PKCS	Public-Key Cryptography Standards
PIT	Pre-Integration Testing
ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SEE	Secure Execution Engine
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMETS	Smart Metering Equipment Technical Specification
SMKI	Smart Meter Key Infrastructure
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SRV	Service Request Variant
TCoS	Transitional Change of Supplier
UIT	User Integration Testing

Appendix B: Risks, Assumptions, Issues, and Dependencies

The tables below provide a summary of any Risks, Assumptions, Issues, and Dependencies (RAID) observed during the production of this PIA. Scope exclusions are also noted.

Assumptions

Ref	Description	Status/Mitigation
MP129-DA1	To avoid incurring additional charges for SMKI Recovery testing, there is a dependency on the delivery of this Modification being scheduled at a suitable date to allow the Annual SMKI Recovery Testing to take place	Open
MP129-DA2	TCoS signing will continue to use the existing ECDSA variant, as TCoS will eventually be replaced by the ECoS service. It is assumed that the current HSM setup can achieve the required processing rates for ECoS migration	Open
MP129-DA3	It is assumed that there will be a requirement for Performance testing and benchmarking of the Recovery application before and after the implementation of this CR4386	Open

Dependencies

Ref	Description	Status/Mitigation
MP129-DD1	To avoid incurring additional charges for SMKI Recovery testing, there is a dependency on the delivery of this CR4386 being scheduled at a suitable date to allow the Annual SMKI Recovery Testing to take place	Open

Scope Exclusions

TCoS is excluded from the scope of this Modification on the basis that it is soon to be replaced and in order to keep charges as low as possible.

The Install & Commission (I&C) of new devices is not required for this change and is therefore excluded, on the basis that SIT testing will be undertaken against existing device sets.