MP104 ‘Security Improvements’ Business requirements – version 1.0

About this document

This document contains the business requirements that support the solution for this Modification Proposal. It sets out the requirements along with any assumptions and considerations. The Data Communications Company (DCC) will use this information to provide an assessment of the requirements that help shape the complete solution.

1. Business requirements

This section contains the functional business requirements. Based on these requirements a full solution will be developed.

Business Requirements	
Ref.	**Requirement**
1	The DCC shall check that the User has used an XML User Role Signing Private Key that is associated with a Public key that is contained within an Organisation Certificate that has a Remote Party Role of “xmlSign”, to Digitally Sign the XML wrapper of each Service request and Signed Pre-Command.
2	The DCC shall cease processing the communication if the User has not complied with Ref 1.
3	The DCC shall notify the User if the DCC ceases to process a communication as per Ref 2.
4	In advance of the implementation of Ref 1-3, the DCC shall provide a monthly report to the Security Sub-Committee of: • Users who are not using the private keys associated with a public key that is contained within an Organisation Certificate that has a Remote Party Role of “xmlSign” to Digitally Sign the XML Wrapper as will be required when Ref 1 is implemented. • Once Ref 1-3 is implemented, there are no further requirements for this report to be produced.
5	The Implementation of Ref 1-3 is expected to align with the start of the operation of the Enduring Change of Supplier (ECoS) function to reduce implementation complexity for Users and DCC. DCC should manage the communication of the requirement for Users to use keys associated with XML Signing certificates alongside communications already planned for ECoS implementation.

2. Considerations and assumptions

This section contains the considerations and assumptions for each business requirement.

2.1 General

This solution will be applied to SMETS1 and SMETS2 Devices.

This business requirement is to be aligned with the Department for Business, Energy & Industrial Strategy (BEIS) requirements that will require DCC system changes. Specifically:

- changes involving XML Signing Certificates for DCC Users that BEIS consulted on in January 2020; and
- changes proposed by BEIS related to how Change of Supplier (CoS) Update Security Credentials Service Requests should be processed as part of the Enduring Change of Supplier (ECoS) arrangements.

Part of the BEIS ECoS proposals is for MPIDs to be included within the subject common name field of XML signing certificates issued to suppliers. These MPIDs are planned to be used as part of the processing checks applied to CoS requests under ECoS.

This is to enable the relationship between supplier and an MPID to be capable of being defined based solely on whether an MPID (Market Participant) is included within the XML signing certificate of a supplier.

One of the BEIS requirements is that where the DCC receives a Certificate Signing Request for an XML Signing Organisation Certificate from a Supplier Party which seeks to include an MPID in the relevant field, the DCC shall reject the Certificate Signing Request if there exists another Organisation Certificate that has been Issued by the Organisation Certification Authority (OCA) to a different Supplier Party that:

- has not expired;
- has not been revoked; and
- contains the MPID that is included within the Certificate Signing Request.

The business requirement set out below has similar characteristics and the DCC system design changes would be most economically achieved by the impact assessment being conducted in parallel.

2.2 Requirement 1:

The DCC shall check that the User has used separate XML User Role Signing Private Keys to Digitally Sign each Service request and Signed Pre-Command.

2.3 Requirement 2:

The DCC shall cease processing the communication if the User has not used separate XML User Role Signing Private Keys to Digitally Sign each Service request and Signed Pre-Command.

2.4 Requirement 3:

The DCC shall notify the User if the DCC ceases to process a communication because the User has not used separate XML User Role Signing Private Keys to Digitally Sign each Service request and Signed Pre-Command.

2.5 Requirement 4:

The DCC shall provide a monthly report to the Security Sub-Committee (SSC) of Users who have not used separate XML User Role Signing Private Keys to Digitally Sign each Service request and Signed Pre-Command.

2.6 Requirement 5:

The Implementation of Ref 1-3 is expected to align with the start of the operation of the Enduring Change of Supplier (ECoS) function to reduce implementation complexity for Users and DCC. DCC should manage the communication of the requirement for Users to use keys associated with XML Signing certificates alongside communications already planned for ECoS implementation.

3. 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 & Industrial Strategy
CoS	Change of Supplier
DCC	Data Communications Company
ECoS	Enduring Change of Supplier
MPID	Market Participant ID
OCA	Organisation Certification Authority
SSC	Security Sub-Committee