RETAIL ENERGY CODE

This document is classified as **WHITE**.
Information is for public, unrestricted dissemination and publication.

01	Initial Assessment Report
02	Preliminary Change Report
03	Final Change Report

INITIAL ASSESSMENT REPORT

R0151 - IMPLEMENTATION OF ONLINE CERTIFICATE STANDARD PROTOCOL (OCSP) IN ADDITION TO CERTIFICATE REVOCATION LIST (CRL)

DOCUMENT VERSION	V2.0
DATE ISSUED	06/02/2024
DOCUMENT APPROVAL STATUS	APPROVED

RESPONSIBLE COMMITTEE	CHANGE PANEL	CHANGE PATH	SELF GOVERNANCE
PRIORITY STATUS	MEDIUM	URGENCY	STANDARD

DEADLINE FOR ALTERNATIVE CHANGE PROPOSALS	21/06/2024

LEAD CHANGE ANALYST



James Hardy

Click to send an email

020 3922 0757

CHANGE OVERVIEW

This Change seeks to make improvements to the Microsoft Azure Application Gateway module. A defect has been identified which requires the implementation of a manual/ customer workaround when checking the Certificate Revocation Lists (CRLs) systems within the Central Switching Service (CSS) to ensure certificates are revoked. This change seeks to remove the need to complete a manual workaround and implement a real-time certification validation capability.

	High Impact: **N/A**
	Medium Impact: **N/A**
	Low Impact: **CSS Provider and Users**

1 BACKGROUND

A Certificate Revocation List is a list of revoked certificates that is issued and maintained by the Certificate Authority. CRLs are made publicly available by the CSS Certificate Authority (CA) and the URL for the relevant CRL is contained within the certificate metadata. When a connection is established to CSS by a connecting system, the CRL will be downloaded, and the connecting Transport Layer Security (TLS) certificates, or JSON Web Signature (JWS) certificates, are not on the CRL for every connection made and store the CRL as a cached version and periodically update the cached version.

Online Certificate Standard Protocol (OCSP) is a technique where the OCSP server, upon interrogation by the systems attempting the TLS connection (TLS handshake), will respond with the status of the certificate. The status response will be one of “Good”. A certificate status of “Good” shows that the certificate is valid for use.

A similar set of interactions to the above also happens during message signing/validation with the JWS Certificates, where the OSCP responder will also return the status of the certificate.

At a minimum this shows that a certificate with corresponding serial number and validity period hasn’t been revoked. The “Revoked” status indicates that the certificate has been revoked, either temporarily or permanently. If the CA has no record of ever having issued a certificate with the certificate serial number in the request, then this status may also be returned. The “Unknown” status indicates that the responder doesn’t know about the certificate being requested, usually because the request indicates an unrecognised issuer that is not served by this responder.

2 PROBLEM STATEMENT

There is currently a Microsoft Azure Application Gateway module defect against the checking of Certificate Revocation Lists (CRLs), with Microsoft stating that the CRL related defect will not be fixed. Consequently, any system within the CSS ecosystem, systems that use Switching Key Infrastructure (SWIKI), that have incorporated the Azure Application Gateway module to manage the TLS connection will have been required to implement a manual/custom workaround to ensure that certificates that are revoked are not allowed to establish a connection.

3 USER STORIES

REF.	USER STORIES
CONSUMER USER STORIES	
C1	As a consumer, I want to ensure that my data is handled securely.
MARKET PARTICIPANT USER STORIES	
M1	As the CSS Provider, I want to have a robust and automated process for checking revoked certificates from the CRL.
M2	As the CSS Provider, I want to be able to implement the OCSP following the expiry of the current JSON Web Signature (JWS) and TLS Certificates.

M3	As the CSS Provider, I want to ensure OCSP is optional for service users to ensure there is no disruption to certificate validity.

4 IMPACTS

REC SERVICE PROVIDERS	REC PARTIES AND SERVICE USERS	REC DOCUMENTS AND PRODUCTS
Central Switching Service	CSS Users	Schedule 25 – Central Switching Service Schedule CSS Security and API Supporting Information

The table above outlines the expected REC Service Providers, Parties, Service Users, and Documents and Products that are expected to be impacted. These will be reviewed as part of the Service Provider Impact Assessment.

This change will allow the removal of any workarounds that have been introduced to mitigate the Microsoft Azure Application Gateway defect and will have no direct impact to Energy Consumers.

This change will also introduce the advanced features that OCSP brings over the CRL into Switching Key Infrastructure (SWIKI). The OCSP functionality for the whole SWIKI certificate estate will mean that the TLS Certificates and JWS Certificates status can be queried with the OCSP server.

CSS will be impacted through the implementation of the new OCSP server/responder. The change will be optional for REC Parties/Service users, although the Code Manager strongly encourages this change to be implemented, and as this is an internal system change for those who wish to switch to, and utilise, the OCSP system, the impact will be negligible as the only difference will be additional OCSP data on their certificates.

A further Category 3 Change will be required at time of implementation to update the document, CSS Security and API supporting Information, to include the OCSP server/responder address.

This change will have no consumer impact since this is an internal system change.

5 CROSS CODE IMPACTS

No Cross Code Impacts have been identified.

6 CHANGE PATH AND RESPONSIBLE COMMITTEE

CHANGE PATH	Self-Governance	RESPONSIBLE COMMITTEE	Change Panel

This change will impact the CSS which is governed under Schedule 25 – Central Switching Service Schedule – of the REC. Therefore, since the impacted documents come under the responsibility of the Change Panel, they should be the Responsible Committee for this change.

7 PRIORITY STATUS AND URGENCY

Category	Significance / Resource impacts / Urgency	Further selection / breakdown	Score (0-3)	Weighting	Weighted Score
Impacts	Consumer Impact	Indirect	1	27	27
	Retail Markets Impact	Innovation and Market Arrangements	1	17	17
	RECCo / REC Party / REC Service Provider Impact	Operational Effectiveness and Efficiencies	1	7	7
		Legal and Regulatory Compliance	1	14	14
Resource	Complexity / Effort / Duration		3	9	28
Strategic Alignment	Contribution to/ Alignment with the objectives of the REC		1	17	8
	Contribution to/ Alignment with RECCo's Forward Work Plan		0		0
Urgency *(The need to progress a change to meet a targeted date)*		Other Planned Activity	1	10	10
				Overall Priority Score (rounded)	110

Priority Status	MEDIUM
Change Proposal Type	STANDARD

This change has been determined as having a medium priority score of 110. This is primarily driven by the high resource impact, due to the complexity of this change.

Consumer and Retail Impact – a score of 1 due to the minor, indirect impact this will have on customers through ensuring that customer's data is continued to be handled securely. Retail Markets also receive a score of 1 under innovation and market arrangements because of ensuring data is being securely handled.

Operational Effectiveness and Efficiencies - a score of 1 to reflect that the current defect prevents the efficiency when checking Certificate Revocation Lists, but this change will restore operational efficiency by providing an alternative method.

Legal, Regulatory and Compliance – a score of 1 since the CSS has a requirement to protect customer data, and this change will increase the security of the REC Central Systems to do so.

Complexity/Effort/Duration – a score of 3 to reflect the levels of expertise required due to the technical aspects of this change. A period of Solution Development will be required to find and test an alternative option (the implementation of OCSP), this will be complex and will require a long duration due to the multiple impact assessments that will have to be completed by Service Providers.

Contribution to/Alignment with the REC Objectives – a score of 1 to reflect the solution to an error that could prevent the effectiveness of the REC's Central Systems. This change does not impact RECCo's Forward Work Plan.

Urgency – a score of 1 to reflect only a small number of incidents being caused by the Microsoft Azure Application Gateway Module defect, and this change being optional for CSS users.

8 SUMMARY OF CHANGE PROPOSAL PLAN

A Change Proposal Plan has been developed that includes time for Analysis, Solution Development, Assessment, and Consultation. The Solution Analysis and Development period has been set to allow time for the Solution to be considered during Technical Change Workshops, and for a Preliminary Impact Assessment and a Detailed Impact Assessment to take place.

Following the completion of the Solution Development, the plan includes a standard 15 Working Day (WD) Party Impact Assessment and a standard 15 WD Consultation period.

The Preliminary Change Report will be published on 21 June 2024 before the Consultation on 05 July 2024, with the Final Change Report being issued on 09 August 2024 for the Responsible Committee decision on 20 August 2024.

	FROM	TO
SOLUTION ANALYSIS AND DEVELOPMENT	01/11/2023	26/01/2024
SERVICE PROVIDER IMPACT ASSESSMENT PERIOD	02/02/2024	24/04/2024
PARTY IMPACT ASSESSMENT	10/05/2024	04/06/2024
PRELIMINARY CHANGE REPORT ISSUED	21/06/2024	21/06/2024
RESPONSIBLE COMMITTEE REVIEW	02/07/2024	02/07/2024
CONSULTATION	05/07/2024	26/07/2024
FINAL CHANGE REPORT ISSUED	09/08/2024	09/08/2024
RESPONSIBLE COMMITTEE DECISION	20/08/2024	20/08/2024
APPEAL WINDOW CLOSURE	04/09/2024	04/09/2024

9 GLOSSARY

TERM	DEFINITION
Azure Application Gateway	means the web traffic load balance enabling the management of traffic to web applications, providing an application delivering controller as a service.
Central Switching Service (CSS)	means the Systems and processes provided or procured by the CSS Provider for the purpose of providing the Address Management Service and the Registration Service.
Certificate Authority	means the CSS Provider in its role as Security Certificate Authority for the Central Switching Service.
Certificate Revocation List (CRL)	means the list of revoked security certificates maintained by the CSS Certificate Authority
Online Certificate Status Protocol	means the scheme used to maintain the security of a server and other network resources and is an Internet Protocol that Certificate Authorities use to determine the status of Transport Layer Security certificates to help web browsers check the status and validity of HTTPS websites.
TLS Certificate	means a security certificate required in accordance with the CSS Schedule to secure either end of the network connection to ensure the transfer of Market Messages across the communication channel is via a secure encrypted channel.
Transport Layer Security (TLS)	means the encryption protocol that protects data when it moves between computers.