This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

MP129 'Allowing the use of CNSA variant for ECDSA'

Conclusions Report – version 1.0

About this document

This document summarises the responses received to the Modification Report Consultation and the decision of the Change Board regarding approval or rejection of this modification.

Summary of conclusions

Change Board

The Change Board voted to **approve** MP129. It believed the modification better facilitated SEC Objective (g)[1].

Modification Report Consultation

SECAS received one response to the Modification Report Consultation. The respondent believed that the modification should be approved. They considered the modification better facilitated SEC Objective (g).

[1] Facilitate the efficient and transparent administration and implementation of this Code.

Modification Report Consultation responses

Summary of responses

The respondent believed that the modification would provide greater clarity on which variants of the Elliptic Curve Digital Signature Algorithm (ECDSA) are permissible for use by SEC Parties.

Following the Modification Report Consultation, the legal text drafting for this modification was amended slightly to ensure the relevant sections were aligned with the updated external document which they reference.

Change Board vote

Change Board vote

The Change Board voted to **approve** MP129 under Self-Governance.

The vote breakdown is summarised below:

Change Board vote				
Party Category	**Approve**	**Reject**	**Abstain**	**Outcome**
Large Suppliers	6	0	0	**Approve**
Small Suppliers	1	0	0	**Approve**
Network Parties	3	0	0	**Approve**
Other SEC Parties	2	0	0	**Approve**
Consumer Representative	1	0	0	**Approve**
			Overall outcome:	**APPROVE**

Views against the General SEC Objectives

The Change Board believe that MP129 will better facilitate SEC Objective (g) as the modification will provide greater clarity on which variants of the ECDSA are permissible for use.

Change Board discussions

An Other SEC Parties representative queried the statement in the Modification Report that MP129 will have no impact on Devices. SECAS clarified that changing the ECDSA variant only changes the way in which the secret number '*k*' for the digital signature is generated; it doesn't change the composition of the signature itself. Using the Commercial National Security Algorithm (CNSA) Suite variant therefore makes no difference to how Devices receive Critical Commands.