

■ MP268 'Certificate rotation and expired Certificates'

Liz Woods

Raised by Brad Baker from the DCC
Progress to Report Phase

HIGH

Issue

- Devices manufactured after the 2024 Manufacturing Pack release may contain information from an Organisation Certificate with a Validity Period exceeding ten years.
- SMKI PMA deems that Certificates with a Validity Period longer than ten years are an increased security risk
- There is no explicit SEC requirement for post-commissioning replacement of Organisation Certificate information by the DCC.

Impact

- Anticipated that Devices will be installed in 2026 and beyond which contain expired Certificates which will need to be replaced.

Proposed Solution

- Clear guidelines within the SEC mandating Post-Commissioning replacement of Organisation Certificates by the DCC.
- Guidelines will provide explicit instructions and timelines for replacing any Organisation Certificate which has a Validity Period longer than ten years, or is revoked or expired.

■ Proposed Solution Summary

Automatic Organisation Certificate replacement

- Daily automatic initiation of ACB Certificate replacement by DSP
- This automation will prioritise Devices commissioned within the last 48 hours
- If replacement fails, the system retries every 7 days for up to three attempts (21 days total)

Backlog management

- Newly commissioned Devices (within the last 23 days) are prioritised for ACB Certificate replacement
- This allows newer Devices to be updated promptly while the system manages the backlog

Exclusion

- Prepayment Interface Devices (PPMID) will be excluded from automatic ACB Organisation Certificate replacement due to known limitations.
- Many legacy firmware versions of PPMIDs do not support Certificate rotation. In addition, there are a large number of PPMIDs not supported by SECMP0007.

■ Proposed Solution - Reporting

Reporting detail

- Validity Period exceeding ten years
- Are revoked or expired
- Expiring within 18 months
- Are incorrectly assigned in Trust Anchor Cells

Data Points

- GUID
- Device ID
- Device type
- Operational status
- Key location
- Certificate details
- Expiration dates

This additional reporting will be part of the existing monthly Post Commissioning Obligations

Service Users and CSP Service Provider receives a weekly report detailing all their Devices which are currently failing the PCO checks as introduced under MP183 'Post Commissioning Obligations Reporting'

Impact Assessment Impacts

Key Management

- Data Management will be called periodically (e.g. every 15 mins between 8am-10pm)
- Passing through a list of manufacturer ACB certificates.

Data Management

- To limit the worklist size to a configurable value
- Devices will be selected and added to the replacement worklist
- If there is still capacity (N):
 - A further N Devices will be selected
 - Added to the replacement worklist

ECOS Provider (Accenture)

- Changes will be part of existing ECOS solution
- Config change is planned to be in place within 12 weeks of the Private Key Transfer Programme going live
- Production version of the config is referred to as Config File 2.0

DS&A

- Will continue to use the Device Key Mapping table delivered to obtain information of Device Key rotation
- Will provide a regular feed of SMKI certificate details from the DSP to the DS&A. this is already included in phase 2 of MP239
- No extra effort, just makes reporting mandatory

No impact to Tech Specs, infrastructure or any other DSP changes

Additional processing and storage are likely to be required. However, they are not sufficiently large to warrant the procurement of additional compute power or storage.

■ Refinement Consultation key points

Respondent comments

This change relates to the Organisation Certificates which the DCC is responsible for managing and has no direct effect on Suppliers.

From a purely Supplier perspective, this is a beneficial change. It increases the time before Certificate expiry, and therefore reduces the risk of loss communications to a Device, were an expired Certificate to result in a meter becoming non comms.

This change will not place any extra requirements on Suppliers. It will also reduce the frequency of future Certificate replacements, which will have a longer-term reduction on Supplier workload.

We agree with the proposed implementation approach because it ensures the modification is implemented soon after it is approved and before expiry of the original Certificates.

Section G

- Two new clauses
- Reference for Appendix AC

Appendix AC

- 4 new clauses
- New clause to introduce obligation on Certificate replacement
- Revoked and Expired Certificate obligations

Forum views

Working Group

Supports the modification

Agreed there is a lack of explicit instruction to replace Certificates

Should not impact I&C – Highlighted Certificate replacement should take place after 7 WD

TABASC

Believe Certificate replacement should take place after 48 hours but before 7 days

Most Suppliers have completed I&C after 48 hours and before 7 days to better align to PCO

Part of DCC License Condition, why is this a mod

SSC

Remained neutral

Updated no sooner than 48 hours & no later than 23 days after I&C

Reporting requirement is captured within current PCO reporting

DCC currently does this & new DSP has requirement to do it

SMKI PMA

Supposed to be included in the new DSP

Why this mod is needed to 'cover' until new DSP is ready

Certificate Rotation and Expired Certificates, SECMP0268

SMETS2 Certificate Post-Commissioning

Current as is Post Commissioning

- SEC Obligation on Energy Suppliers & Network Operators to rotate ES & DNO credentials only
- SEC Obligation on DCC to rotate WANProvider credentials, managed by CSPs
- Manual and ad-hoc ACB certificate rotation by DSP, no obligation



MP268

To be Post Commissioning

- SEC Obligation on DCC to ensure DSP & ECOS providers rotate ACB & COS certificates.
 - ECOS Technical detail – as per SSC requirements to move away from OCA manufacturing certificates within 7 days the rotation is done after 2 days and within 7 day for ECOS.
 - ACB ECOS Technical detail – as per SSC requirements to move away from OCA manufacturing certificates within 23 days the rotation is done after 2 days and within 23 day for ACB DS & ACB KA.
- Apply certificate prioritization ensuring expiring, expired and revoked certificates are prioritized for all OCA certificates managed by DCC excluding Recovery & Root but including WANProvider, ECOS, ACB KA & DS.
- SEC Obligation on DCC to capture data & monitor certificate management.

Changes

1. Align legal text across all DCC service providers
2. Automate rotation & increase efficiency
3. Test automate changes
4. Apply cert prioritization & data reporting.

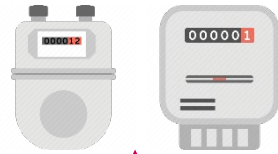
How do DCC know post commissioning is not enough today?

High number of Devices are still using 2016 certs: for capacity management, a plan will be implemented by DCC, its service providers and wider industry to enable a coordinated certificate rotation approach.

We need an immediate plan & push to move away from 2016 & 2017 certificates. Industry will become non-SEC compliant if we don't.

trust anchor cell	Certificate	2016 certs	2017 certs	2018 certs	2019 certs	2020 certs	2021 certs	2022 certs	2023 certs	2024 certs	Total Devices
1	Root	47,172,566									
2	Recovery DS	47,184,938									
3	Supplier DS	55,215	4,743,566	2,598,657	1,508,795	7,759,139	16,516,473	4,278,289	4,392,636	1	41,852,771
4	Supplier KA	55,080	5,994,394	2,582,864	1,710,008	7,838,308	20,373,853	5,214,536	6,718,042	2	50,487,087
5	Supplier prepay KA	9,098	2,545,798	836,474	806,618	3,349,533	4,633,925	440,510			12,621,956
6	Network Operator DS	9,319,679	12,562,286	194,796	56,085	1,128,991					23,261,837
7	Network Operator KA	6,952,824	14,183,180	387,955	11,336	1,048,728	350,939	274,149			23,209,111
8	ACB Certs DS	5,637,132		2,895,417				1,089,568			9,622,117
9	ACB Certs KA	11,660,729		27,730,635				12,533,670			51,925,034
10	CoS DS	1,167,008		10,332					41,267,531		42,444,871
11	WAN Provider DS	4,664,021			3,648,941		1,979,137	1,452,740			11,744,839
12	SAPC DS										
13	SAPC KA										
	Total Devices	133,878,290	40,029,224	37,237,130	7,741,783	21,124,699	43,854,327	25,283,462	52,378,209	3	361,527,127

DCC Certificate Management Lifecycle



Ensuring OCA man pack impacts to industry are minimum

Introducing new certificates installed on devices during manufacturing (pre-install)

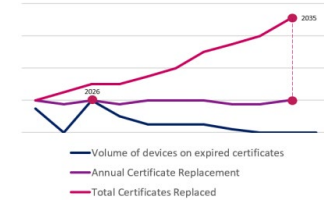
Manufacturing Certificates

- Config files on production lines
- Built into device at manufacturing
- Sits on device at point of install
- Lifetime from point of generation = Maximum 17 years

BAU Production Certificates

- Used as part of post commissioning
- Requires diversification
- Placed on devices remotely
- Lifetime from point of generation = 10 years

Introducing new obligations on DCC SPs to enable post commissioning rotation (Man to BAU)



Introducing a method of smoothing cert rotation demand over time (20% per year – BAU to BAU)

ECOS Programme Code Uplift

MP261 'Extending the Organization Certificate Validity Period'

ECOS Work off (PKT, TCOS Decom, Migration)

OCA Manufacturing Programme

CR5147 (Remote Key Custodian)

MP268 'Certificate rotation and expired Certificates'

CR5392 (Certificate Diversification - Enduring OCA Certificate Management)

DSP2.0 Programme Migration / PKT

2022: ECOS code uplift has gone live

Feb 2024: Reuse of keys mod has gone live

July 2024: ECOS work off complete

April 2025: OCA Man Pack go live

2024 – 2025: Remote key ceremonies go live

November 2025: Mandatory post commissioning, certificate prioritization & reporting go lives

February 2026: Mandatory certificate diversification & associated code changes go live.

2026-2028 DSP2.0 certificate management goes live

DCC E2E Cert Management Policy
(Published October 2024)

Why are PPMIDs not in scope of MP268?

Action:

1. Question to DCC from PPMID vendor x – Why are PPMIDs not in scope for cert rotation within MP268.

Why do the change?

- There are historical defects across all PPMID providers that limit how many firmware versions of PPMIDs support certificate rotation.
- There is no impact to PPMID functionality if manufacturing certificates expire.
- PPMID vendors have will defects open within DCCs OCA manufacturing pack programme that are linked to certificate rotation.
- The timeline and cost of MOD will change + testing scope will be much larger if we add PPMIDs in scope now.
- DCC does not test certificate rotation in PPMIDs in its system integration or user integration testing – therefore does not have evidence of success.
- PPMID firmware is not managed as pro-actively as meters / comms hub firmware

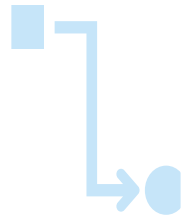
DCC Suggestion:

1. Let MP268 continue with its current proposal and then industry explore if they want to support a post-commissioning change that includes PPMIDs after MP268 go live acceptance or rejection.

Stuart Drinan

Lead E2E Architect

■ Assessment of Change



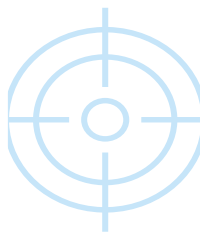
Impacted Parties

- Suppliers
- Electricity Network Operators
- DCC



Costs

- SECAS costs
- £289,000 + Post PIT costs



Target Release

- Nov 2025 SEC Release
- Will be included in the new DSP



Benefits

- Explicit instructions and criteria when Certificate replacement should occur

SEC Objective (f)

(f) To ensure the protection of Data and the security of Data and Systems in operation of this Code

■ Recommendations

- **DETERMINE** whether that MP268 should be progressed to the Report Phase
- **APPROVE** the Modification Report
- **APPROVE** the implementation approach
- **AGREE** that MP268 should be progressed as a Self-Governance Modification

SEC Objective (f)

(f) To ensure the protection of Data and the security of Data and Systems in operation of this Code