Summary of Updates – CPS Revision 11 (Amendment from CPS Revision 10) **4 June 2024**

Section	CPS Revision 10	CPS Revision 11	Reasoning / Notes
1	Root Certificate • Pos Digicert Class 1 Root CA G2 • Pos Digicert Class 2 Root CA G2 • Pos Digicert Class 2 Root CA G3 • Pos Digicert Class 2 Root CA G4 • Pos Digicert Class 2 ECC Root CA R1 • Pos Digicert AATL Root CA • Pos Digicert Time Stamping Root CA • Malaysia Premier CA G2	Updated to: Root Certificate • Pos Digicert Class 1 Root CA G2 • Pos Digicert Class 2 Root CA G3 • Pos Digicert Class 2 ECC Root CA R1 • Pos Digicert AATL Root CA	Alignment with the current business practice.
1.1	POS DIGICERT conforms to the current version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates (the “Baseline Requirements, published at www.cabforum.org. If a discrepancy arises between interpretations of this document and the Baseline Requirements, the Baseline Requirements shall take precedence over this document. Additional assertions on standards used in this CPS can be found under the respective titles / headers in this CPS wherever applicable.	This specific paragraph was omitted.	Alignment with the current business practice.
All sections (where applicable)	The titles of sections 1.5.3, 1.5.4, 4.2.1, 4.2.2, 4.2.3, 4.3.2, and 9.4.6 were not aligned with RFC 3647.	Titles have been revised to align with RFC 3647.	Alignment with RFC 3647
All sections (where applicable)	The usage of the term “Subordinate CA” and “Sub CA” throughout the document.	All references to ‘Subordinate CA’ and ‘Sub CA’ have been updated to ‘Intermediate / Issuing CA’ throughout the document.	Alignment with the current business practice.
All sections (where applicable)	The requirements for Class 3 Certificates were not included in CPS Revision 10 since they were not part of Pos Digicert’s offering.	Requirements for Class 3 has been included. However, all references to ‘Class 3 Certificate’ will be standardised as ‘No stipulation’ throughout the document due to Pos Digicert not offering those services.	Adhering to MCMC Requirement

1.6.3	WebTrust Principle and Criteria for Certification Authorities Version 2.2.1.	Updated to: WebTrust Principle and Criteria for Certification Authorities, Version 2.2.2.	Alignment with the applicable document version.
All sections (where applicable)	Pos Digicert offers the following intermediate certificates: i. Pos Digicert DV SSL G4. ii. Pos Digicert Server ID G2. iii. Pos Digicert DV SSL G4.	All references to 'DV SSL G4', 'Pos Digicert Server ID G2', and 'Pos Digicert DV SSL G4' have been omitted, as these offerings are no longer part of Pos Digicert's services.	Alignment with the current business practice.
All sections (where applicable)	All references are made to 'Pos Digicert Digisign ID G2'.	Updated to: Pos Digicert Digisign ID G3.	Alignment with the current business practice.
4.5.1	The provision concerning unsuccessful subscriber attempts to unlock smart cards or tokens, leading to permanent blocking of the device and necessitating certificate reissuance at the subscriber's expense, was not included in CPS Revision 10.	Included: In the event a subscriber attempts to unlock the smart card or token multiple times which results in the smart card or token being blocked permanently, the unblocking process by Pos Digicert would render the certificate unusable and would require the digital certificate in the devices to be reissued. In this scenario, the Subscriber would bear the cost of the digital certificate reissuance. Subscribers are advised to contact Pos Digicert the moment they can't access their smart card or token. It is discouraged for Subscribers to try to unblock their smart card or token multiple times which may result in permanent blocking of the devices.	Alignment with the current business practice.
4.10.2	POS DIGICERT provides certificate services 24 x 7 without interruption. POS DIGICERT shall publish the revocation status as stipulated in CPS Part 4.9.7.	Updated to: POS DIGICERT shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint. POS DIGICERT shall publish the revocation status as stipulated in CPS Part 4.9.7.	Alignment with the current business practice.
5.4.2	Critical system events, access attempts and CA software operation events are logged on a daily basis. The audit trail is reviewed at least **once per week**.	Updated to: Critical system events, access attempts and CA software operation events are logged on a daily basis. The audit trail is reviewed at least **once a month**.	Alignment with the current business practice.