

SUMMARY OF UPDATES - CPS v 3.0 (Amendment from CPS v.2.1)

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
1.0 Preface	1.4 <i>Publication and Notification</i>	DIGICERT Sdn Bhd Lot 2-1 Enterprise 1 Technology Park Malaysia, Bukit Jalil 57000 Kuala Lumpur, Malaysia Tel: +603 8996 1600 Fax: +603 8996 1054	Changed Digicert's address: DIGICERT Sdn Bhd (457608-K) No. 3-20 & 3-22, Jalan 14/155B Aked Esplanad, Bukit Jalil 57000 Kuala Lumpur, Malaysia Tel: +603 8992 8800 Fax: +603 8992 8810	Moved to new premise
	1.7.2 <i>Customer Service Contact Details</i>	DIGICERT Sdn Bhd Lot 2-1 Enterprise 1 Technology Park Malaysia, Bukit Jalil 57000 Kuala Lumpur, Malaysia Tel: +603 8996 1600 Fax: +603 8996 1054	Changed Digicert's address: DIGICERT Sdn Bhd (457608-K) No. 3-20 & 3-22, Jalan 14/155B Aked Esplanad, Bukit Jalil 57000 Kuala Lumpur, Malaysia Tel: +603 8992 8800 Fax: +603 8992 8810	Moved to new premise
2.0 DIGICERT certification infrastructure	2.1 <i>Trust Infrastructure</i>	The initial Root key length is 1024 bits and it is created using a trustworthy device complying with the requirement of the DSA.	Removed text - "The initial Root key length is 1024 bits and it is created using a trustworthy device complying with the requirement of the DSA."	Misleading to subscriber that Digicert root key is 1024.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
	2.1 <i>Trust Infrastructure – Digicert Sdn Bhd (Licensed CA)</i>		Amended Digicert's PKI Hierarchy	<ul style="list-style-type: none"> • Digisign Server ID (Enrich) has been rooted under GTE Cyber Trust Class Global Root • Added text "Refer to App 6.2 for List of Certificates" on Enterprise CA box
	2.1 <i>Trust Infrastructure – (End-Entities)</i>	End-entity need not necessarily be a natural <u>person</u> ; it could also be a certificate using system such as a secure web server.	Added text - " <u>or any organization.</u> " "End-entity need not necessarily be a natural <u>person</u> ; it could also be a certificate using system such as a secure web server <u>or any organization.</u> "	For BNM project, we do issue certificates bearing the organization name, but not used in web server.
	2.2 <i>Certificate Classes</i>	This is done through the physical presentation of the identification documents	Edited statement of assurance for Class 2 certificate "This is done through the physical presentation of the identification documents <u>or confirmed against reliable third party database</u> ".	LHDNM e-Filing digital certificate online verification is performed against LHDNM database. No identification documents are required during online application.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
	2.2 <i>Certificate Classes</i>	Strict verification and authentication by the CA, RA or its appointed agents is required for certificates issued in smart card, virtual smart card (floppy disk) or any other applicable tokens. Confirmation is based upon the official identification document issued by government agencies. The reliability of the information is determined at the sole discretion of the CA, RAs or Enterprise CA.	Edited statement of validation for Class 2 certificate "Strict verification and authentication by the CA, RA or its appointed agents or <u>reliable database</u> is required for <u>soft certificates and certificate</u> issued in smart card, virtual smart card (floppy disk) or any other applicable tokens. Confirmation is based upon the official identification document issued by government agencies. The reliability of the information is determined at the sole discretion of the CA, RAs or Enterprise CA <u>or database owner</u> ".	LHDNM e-Filing digital certificate online verification is performed against LHDNM database.
	2.3 <i>Certificate Profile</i>	None	Updated Figure 3 X.509 v3 Certificate format. CA signature : MD5/ SHA-1	CA signature field is empty. There are 2 algorithms in DigiCert's CA signature, MD5 or SHA-1.
3.0 DigiCert operational requirements	3.1 .1 <i>Key Generation and Protection</i>	When DIGICERT creates subscriber key pairs, DIGICERT warrants that it will not keep or escrow a copy of the subscriber's private key.	Edited text - When DIGICERT creates subscriber key pairs, DIGICERT warrants that it will not keep or escrow a copy of the subscriber's private key <u>unless with consent by subscriber</u> .	In LHDNM e-Filing, user have the options to backup certificate and password in DigiCert database.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
	3.1.1 <i>Key Generation and Protection</i>	CA generates key	Edited text - Key generations for Class 2 (Digisign ID Basic): CA <u>or subscriber</u> generates key.	In LHDNM e-Filing, certificate issued is under Class 2 where subscriber browser will generate the private key.
	3.1.1 <i>Key Generation and Protection</i>	Subscriber generates server key pairs.	Edited text - Key generations for Class 2 (Digisign Server ID): <u>CA</u> <u>or</u> subscriber generates server key pairs.	For iVest server certificate in smart card, certificate key pairs from smart card are generated by CA during smart card pre-personalisation.
	3.1.2 <i>Certificate Applications</i>	None	Added statement "Online registration at web service provider, the identification documents and information required are set forth by the web service provider and CA" at Class 2 Digisign ID Basic/Enhanced.	Online application providers might require additional information / documents e.g. tax reference number in e-Filing, Certificate of Incorporation in BPFK Quest 2.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
	3.1.3 <i>Validations of Certificate Applications</i>	None	<p>Added the following statement in Class 2 Digisign ID Basic/ Enhanced Validation requirements:</p> <p>The data of the applicant for online enrolment is verified against reliable database. Automated online system will compares the applicant Identification Card/ Passport Number and other personal information against the database.</p>	Tax payer in e-Filing system when applying for digital certificate, information such as IC and Tax Reference Number is validated against LHDNM database.
	3.1.3 <i>Validations of Certificate Applications</i>	The subscriber shall receive the certificate and the related private key in his preferred media (smart card, USB token, floppy disk or any other applicable tokens).	<p>Edited the following statement in Nature of communication in applying Digisign ID Basic:</p> <p>The subscriber shall receive the certificate and the related private key in <u>softcert</u>, smart card, USB token, floppy disk or any other applicable tokens.</p>	E-Filing certificate is in software certificate format.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
3.2 Certificate Issuance	3.2.1 <i>Certificate Acceptance</i>	Subscriber indicates acceptance by receiving the smart card, virtual smart card or any other applicable tokens from DIGICERT or its RAs and usage of the digital certificate	<p>Edited the following statement in Nature of communication in acceptance of Digisign ID Basic/Enhanced:</p> <p>Subscriber indicates acceptance by receiving/<u>downloading</u> the certificate from DIGICERT or its RAs and/or usage of the digital certificate whichever come first.</p>	Subscriber indicate acceptance by downloading certificate as well. To cater for online certificate application i.e. e-Filing, BCB online renewal.
	3.2.3 <i>Time of Issuance</i>	None	<p>Added the following statement in Class 2 certificate:</p> <p>For online application, issuance is immediate where the PIN is set by the subscriber.</p>	To cater for online certificate application i.e. e-Filing, MyKad, where PIN is set by user during certificate downloading. Also to cater for future online application.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
3.4 Certificate Revocation and Suspension	3.4.2 <i>Revocation by Subscriber</i>	Walk-in to DIGICERT or its RA Subscriber shall fill in Revocation Request Form upon the request for revocation with following details: <input type="checkbox"/> NRIC/Passport <input type="checkbox"/> Smart card / floppy disk / certificate serial number <input type="checkbox"/> Reason for revocation is required	<i>Edited</i> the following statement in verification procedure for Digisign ID Basic/ Enhanced: <u>Walk-in to DIGICERT or its RA</u> Subscriber shall fill in Revocation Request Form or <u>Online Form (if applicable)</u> upon the request for revocation with following details: <ul style="list-style-type: none">• NRIC/Passport• Reason for revocation is required• <u>Challenge Pass Phrase</u> <u>or any submitted</u> <u>enrolment information (if</u> <u>applicable).</u>	To cater for online revocation.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason				
<p>3.5 <i>Certificate Expiration</i></p>	<p>3.5.1 <i>Notice of Expiration</i></p>		<p>Removed the following column:</p> <p>DIGICERT will provide notice to the subscriber on the expiry date as follows :</p> <table border="1" data-bbox="1384 520 1641 735"> <tr> <td>Enterprise CA</td> </tr> <tr> <td>Two months</td> </tr> <tr> <td>-</td> </tr> <tr> <td>-</td> </tr> </table>	Enterprise CA	Two months	-	-	<p>Bumiputra Bank Commerce Enterprise CA will be changed to CIMB Enterprise CA. There will be a review on the current Standard Operating Procedure and the time frame for Digicert to send expiry notice might differ accordingly to the new request.</p> <p>The statement "The expiry notice time frames for certificate issued by RA and Enterprise CA are similar to Class 2 (Basic / Enhanced) unless indicated in the agreement between DIGICERT and the RA/Enterprise CA" is sufficient.</p>
Enterprise CA								
Two months								
-								
-								

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
	3.5.3 <i>Renewal of Certificate</i>	The certificate renewal process is similar to an application for a new certificate.	Added text “unless agreed upon the relying parties between the Certification Authority and the Enterprise CA subscriber.” text: “The certificate renewal process is similar to an application for a new certificate <u>unless agreed upon the relying parties between the Certification Authority and the Enterprise CA subscriber.</u> ”	The online renewal for CIMB does not enforce subscriber to submit his/her details regardless of whether it has changed or otherwise. Renewal may be approved based on the presentation of valid certificates issued under CIMB Enterprise CA.
3.6 Security Audit Procedures	3.6.2 <i>Frequency of Processing Log</i>	Critical system events, access attempts and CA operation events are logged on a daily basis.	Added text - “software”: Critical system events, access attempts and CA software operation events are logged on a daily basis.	Added “software” to make sure it reflects to our CA engine software which is Nexus Certificate Manager.
	3.6.4 <i>Protection of Audit Log</i>	Audit trail for CA operation events is digitally signed to ensure integrity. Each log record contains the time stamp the type of log entry and the identity of log event.	Added text - “software”: Audit trail for CA software operation events is digitally signed to ensure integrity. Each log record contains the time stamp the type of log entry and the identity of log event.	Added “software” to make sure it reflects to our CA engine software which is Nexus Certificate Manager.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
	3.6.5 <i>Audit Log Backup Procedures</i>	All files including the latest audit trail file are stored either in a magneto optical or DAT tape and kept in a secure archive facility	Changed “magneto optical” to “LTO 4 cartridge”: All files including the latest audit trail file are stored either in a LTO 4 cartridge or DAT tape and kept in a secure archive facility.	No longer using magneto optical due to obsolete technology and support.
	3.6.6 <i>Audit Collection System</i>	The audit trail accumulation system is part of the CA operating system. The log can be viewed using a standard NT event viewer.	Changed “operating” to “software”, change “NT event viewer” to “CA software administrative module”: The audit trail accumulation system is part of the CA software system. The log can be viewed using a standard CA software administrative module .	Added “software” to make sure it reflects to our CA engine software which is Nexus Certificate Manager. Audit trails of CA software systems can only be viewed by Security Officer (SO) by using CA software administrative module provided for integrity and security.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
3.7 Records Archival	3.7.4 <i>Archive Collection System (Internal or External)</i>		Removed text - “The archive for CA database and audit trails is stored onto separate media.”: The archive collection system (backup facility) for the audit trail files is described in CPS Part 3.6.6.	Archive for CA database and audit trails store in one media for easy restoration based on new backup software solution - VERITAS Backup Exec
4.4 Key Management Controls	4.4.1. <i>Usage Periods for the Public and Private Keys</i> 10	The validity period of the CA key pairs is five years.	Added text - “The validity period of the CA key pairs is five years unless agreed by the subscriber of Enterprise CA and Digicert.” text: The validity period of the CA key pairs is five years <u>unless agreed by the subscriber of Enterprise CA and Digicert.</u>	There is Enterprise CA which has 10 years validity.
4.7 Cryptographic Module Engineering Controls	4.7 <i>Cryptographic Module Engineering Controls</i>	Digicert CA hardware cryptographic module is designed to comply with international standards (FIPS 1-140 lenz)	Changed the word - “lenz” to “Level 2”: Digicert CA hardware cryptographic module is designed to comply with international standards (FIPS 1-140 <u>Level 2</u>)	Typo error, no such thing as “lenz”.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason												
5.2 Liability	5.2.1 CA Liability	<p>Reliance limit</p> <p>RM500.00</p> <p>RM2,000.00 (Basic)</p> <p>RM25,000.00 (Enhanced)</p> <p>RM50,000.00 (Server)</p> <p>Up to RM25,000 (Enterprise CA)</p>	<p>Edited the following title:</p> <p>DIGICERT shall only be liable for the issued certificates to an amount not exceeding the following</p> <table border="0"> <thead> <tr> <th data-bbox="1355 512 1478 536">of certificate</th> <th data-bbox="1509 512 1758 536">Reliance limit/ Liability C.</th> </tr> </thead> <tbody> <tr> <td data-bbox="1355 560 1411 584">Class 1</td> <td data-bbox="1509 560 1610 584">RM500.00</td> </tr> <tr> <td data-bbox="1355 608 1411 632">Class 2</td> <td data-bbox="1509 608 1700 632">RM2,000.00 (Basic)</td> </tr> <tr> <td data-bbox="1355 655 1411 679">Class 2</td> <td data-bbox="1509 655 1749 679">RM25,000.00 (Enhanced)</td> </tr> <tr> <td></td> <td data-bbox="1509 703 1722 727">RM50,000.00 (Server)</td> </tr> <tr> <td></td> <td data-bbox="1509 751 1760 775">Up to RM25,000 (Enterpris</td> </tr> </tbody> </table>	of certificate	Reliance limit/ Liability C.	Class 1	RM500.00	Class 2	RM2,000.00 (Basic)	Class 2	RM25,000.00 (Enhanced)		RM50,000.00 (Server)		Up to RM25,000 (Enterpris	To indicate the reliance limit is Liability Cap by CA.
of certificate	Reliance limit/ Liability C.															
Class 1	RM500.00															
Class 2	RM2,000.00 (Basic)															
Class 2	RM25,000.00 (Enhanced)															
	RM50,000.00 (Server)															
	Up to RM25,000 (Enterpris															

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
	5.2.1 <i>CA Liability</i>	None	<p>Added the following statement: The reliance limit on each certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall Digicert Sdn Bhd be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of liability cap.</p>	To further explain the reliance limit of the certificate.
5.4 Interpretation and Enforcement	5.4.3 <i>Dispute Resolution Procedures</i>		<p>Removed the following statement in Dispute resolution procedures: The Office of the Controller is the arbitrator for these disputes.</p>	Advised by MCMC to remove this statement.

Main Clause	Sub Clause	CPS v2.1	CPS v3.0	Reason
5.5 Fees	5.5.1 <i>Certificate Issuance or Renewal Fees</i>	Certificate fees shall be officially published on DIGICERT's website and other printed materials deemed necessary and copyrighted by DIGICERT.	Amended/added text – “or” and “and”: Certificate fees shall be officially published on DIGICERT's website and <u>or</u> other printed materials deemed necessary and copyrighted by DIGICERT.	Certain fees are not officially published on website, e.g. certificate fees for BNM Sub CA.
6.0 Appendices	6.2 <i>List of Certificates for Enterprise CA</i>	None	Newly inserted page	To simplify the diagram in Figure 2 Digicert PKI Hierarchy; hence grouped all certificates under Enterprise CA.