WEBTRUST AND ITS SIGNIFICANCE

20 DECEMBER 2022

Digital Age Strategies Pvt Ltd

Business With Wisdom
...Growth With Assurance

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

सी डैक
CDAC

Subhash Rao P B.E , MBA

Associate Director , Sr Auditor

Business With Wisdom
...Growth With Assurance

Digital Age Strategies Pvt. Ltd.

Estt. 2004

~ 30 years of industry Experience, 18 Years in IT /IS security area.

Served as Head of R&D at Sasken Communication Technologies Ltd

Domain of Expertise: HW,SW, Techno commercial Project Management, Cyber security Auditing, Consultancy.

Certification

EC-Council CEH CERTIFIED
EC-Council CHFI CERTIFIED
EC-Council ECIH CERTIFIED
EC-Council CND CERTIFIED
EC-Council CEI CERTIFIED
CDPSE
ISO 27001 Lead Auditor

TOPICS

WebTrust and Browser Forum

Type of Certificates

Implementation

Auditors for WebTrust

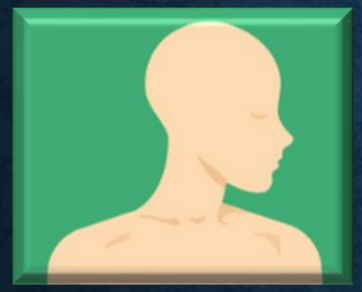
Auditing criteria

Changes required in existing setup/ approach

Business With Wisdom
...Growth With Assurance

TRUSTED CERTIFICATE

Business With Wisdom
...Growth With Assurance



Highly Intellectual

Creative

Identified by face

Identified by voice

Digitally numbered

Identified by biometric

Identified by iris

Trusted Cirtificates

Emotionally weak

Exploitable

Business With Wisdom
...Growth With Assurance

Trusted signature

Digital signature

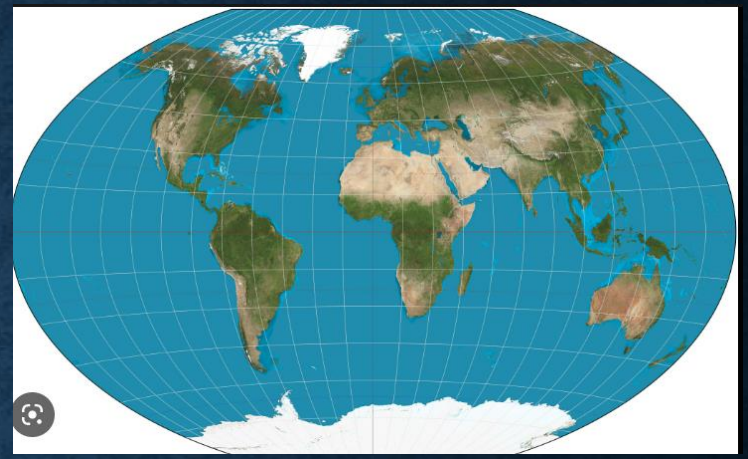
Trusted Organization

Trusted Web Site

Trusted Communication

Trusted Logo

Trusted Document



Certification Authorities

WebTrust

WEBTRUST AUDITORS
Licensed by the CPA, Canada World-Wide Licensing Authority

CCA, Ministry of Information Technology, Govt. of India

Business With Wisdom
...Growth With Assurance

WebTrust Coverage

Business With Wisdom
...Growth With Assurance

WEBTRUST

Business With Wisdom
...Growth With Assurance

WEBTRUST

For Certification Authorities,

program was developed to increase consumer confidence in the Internet as a vehicle for conducting ecommerce,

to increase consumer confidence in the application of PKI technology.

The WebTrust standard is a set of principles designed to follow international information security best practices.

By implementing WebTrust, users of the CA's services can rest assured that their transactions are protected by stringent rules.

Business With Wisdom
...Growth With Assurance

BACKGROUND

- Chartered Professional Accountants of Canada (CPA) reviews and verifies aspects of the web site to ensure that customers transactions are properly completed and billed.
- WebTrust Principles and Criteria for Certification Authorities used as a basis for a practitioner to conduct an engagement on the Issuance and Management of Publicly Trusted Certificates.

Business With Wisdom
...Growth With Assurance

BACKGROUND

- Can be used as a control framework to assess the adequacy of the CA systems, policies and procedures.
- Assessors/auditors can use the framework as a benchmark
- For an internal or independent assessment as an internal auditor,
- For an independent external auditor as supported by the CA/Browser Forum.

Business With Wisdom
...Growth With Assurance

CA/BROWSER FORUM

- Voluntary group of certification authorities (CAs),
- vendors of Internet browser software,
- suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS,
- Code signing, and
- S/MIME (a standard for public key encryption and signing of Multipurpose Internet Mail Extension data).

Business With Wisdom
...Growth With Assurance

BACKGROUND

- The primary goal of the CA/Browser Forum (“CA/B Forum” or the “Forum”)
- Baseline Requirements :
  - to enable efficient and secure electronic communication,
  - addressing user concerns about the trustworthiness of Certificates

Business With Wisdom
...Growth With Assurance

WEBTRUST CERTIFICATES

Business With Wisdom
...Growth With Assurance

SSL BASELINE REQUIREMENT

- In 2011, the CA/Browser Forum introduced its Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates(“BaselineRequirements”, “SSL Baseline Requirements” or “BRs”).
- The WebTrust Principles and Criteria are designed to be used in conjunction with an assurance engagement of a CA as required by the CA/Browser Forum.
- Due to significant overlap ,this engagement should be conducted simultaneously with the WebTrust for CA engagement.

Business With Wisdom
...Growth With Assurance

DIFFERENT TYPES OF SSL CERTIFICATES

- **Domain Validation (DV)**
  - A Domain Validated SSL certificate is issued after proof that the owner has the right to use their domain is established.
  - Because of the minimal checks performed, this certificate is typically issued quicker than other types of certificates.

Business With Wisdom
...Growth With Assurance

BACKGROUND

- While the browser displays a padlock, examination of the certificate will not show the company name as this was not validated.
- Many CAs perform additional fraud checks to minimize issuance of a certificate to a domain which may be similar to a high value domain.
- Because of the minimal checks performed, this certificate is typically issued quicker than other types of certificates.

Business With Wisdom
...Growth With Assurance

DIFFERENT TYPES OF SSL CERTIFICATES

- **Organizational Validation (OV)**
  - For OV certificates, CAs must validate the company name, domain name and other information through the use of public databases.
  - CA's may also use additional methods to insure the information inserted into the certificate is accurate.
  - The issued certificate will contain the company name and the domain name for which the certificate was issued for.

Business With Wisdom
...Growth With Assurance

DIFFERENT TYPES OF SSL CERTIFICATES

- **Extended Validation (EV)**

  - EV Certificates are only issued once an entity passes a strict authentication procedure.
  - These checks are much more stringent than OV certificates.
  - The objectives of EV Certificates are twofold:
  - **Identify the legal entity that controls a Web site:**
  - **Enable encrypted communications with a Web site:**

Business With Wisdom
...Growth With Assurance

BACKGROUND

- The secondary purposes of an EV Certificate
- to help establish the legitimacy of a business claiming to operate a Web site
- distribute executable code
- to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud.

Business With Wisdom
...Growth With Assurance

BACKGROUND

- The growth of internet transactions has emphasized the importance of strong authentication of the identity of websites, domain owners, online servers, and software code.
- Certificates that have been issued under stronger authentication controls, processes and procedures are called Extended Validation Certificates (“EV Certificates”).

Business With Wisdom
...Growth With Assurance

BACKGROUND

- EV Certificates are currently differentiated by their intended use as
  - Certificates intended to ensure the identity of a remote computer (“EV SSL Certificates”); and
  - Certificates intended to ensure the identity of a software publisher and the integrity of software code (“EV Code Signing Certificates”).

Business With Wisdom
...Growth With Assurance

DIFFERENT TYPES OF SSL CERTIFICATES

- Code Signing Certificates :
  - the process of digitally signing executables and scripts
  - to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.
  - The process employs the use of a cryptographic hash to validate authenticity and integrity.

Business With Wisdom
...Growth With Assurance

CONT..

- A Code Signature created by a Subscriber may be considered valid for a period not exceeding 39 months. (3Yr 3 months)
- However, the life of a Code Signature may be extended for up to 135 months (11 Yr 3 months)

Business With Wisdom
...Growth With Assurance

CONT..

- a) Signing Service Method:
  - the Subscriber submits the code, or a digest of the code, to a Signing Service for Code Signature.
  - The resulting Code Signature is valid up to the expiration time of the Signing Service certificate
- b) Timestamp Method:
  - the Subscriber signs the code, appends its Code Signing Certificate and submits it to a Timestamp Authority to be time-stamped.
  - The resulting package can be considered valid up to the expiration time of the timestamp certificate (that may be up to 135 months)

VERIFIED MARK CERTIFICATE

- A digital certificate issued by a certificate authority that verifies logo ownership.
- Your logo must be a registered trademark before receiving a VMC.
- Assurance engagement based on the Verified Mark Certificate Requirements (VMCR)
- to describe an integrated set of technologies, protocols, and identity and mark proofing requirements that are necessary for the issuance and management of Verified Mark Certificates (VMCs)

Business With Wisdom
...Growth With Assurance

IMPLEMENTATION

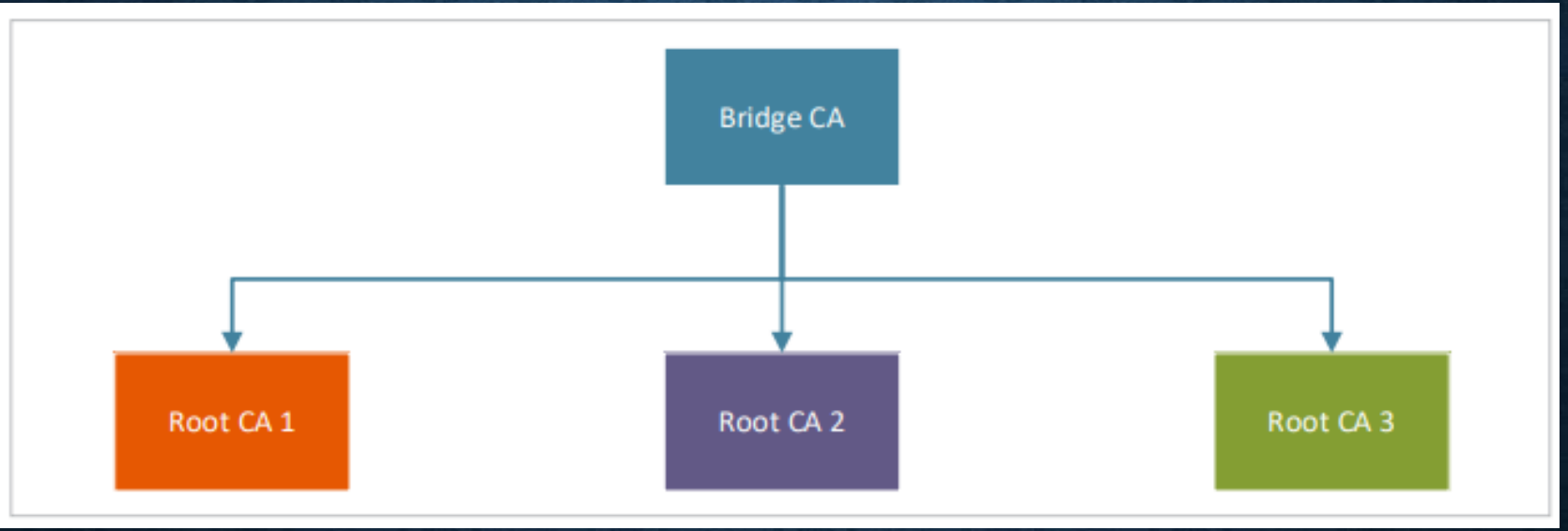
Business With Wisdom
...Growth With Assurance

REFERENCE

- WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – VERIFIED MARK CERTIFICATES Release Date 1 December 2021 Version 1.0
- WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES Release Date 1 June 2021
- WebTrust for CA Criteria with Controls Version 2.2.2
- WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – CODE SIGNING BASELINE REQUIREMENTS Release Date 31 January 2022 Version 2.7
- WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES — SSL BASELINE WITH NETWORK SECURITY Release Date 31 January 2022 Version 1.7
- WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – EXTENDED VALIDATION SSL Release Date 31 January 2022 Version 1.7.8
- WEBTRUST PRINCIPLES AND CRITERIA FOR REGISTRATION AUTHORITIES Release Date: 1 November 2020 Version 1.1
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Version 1.8.5

IMPLEMENTATION

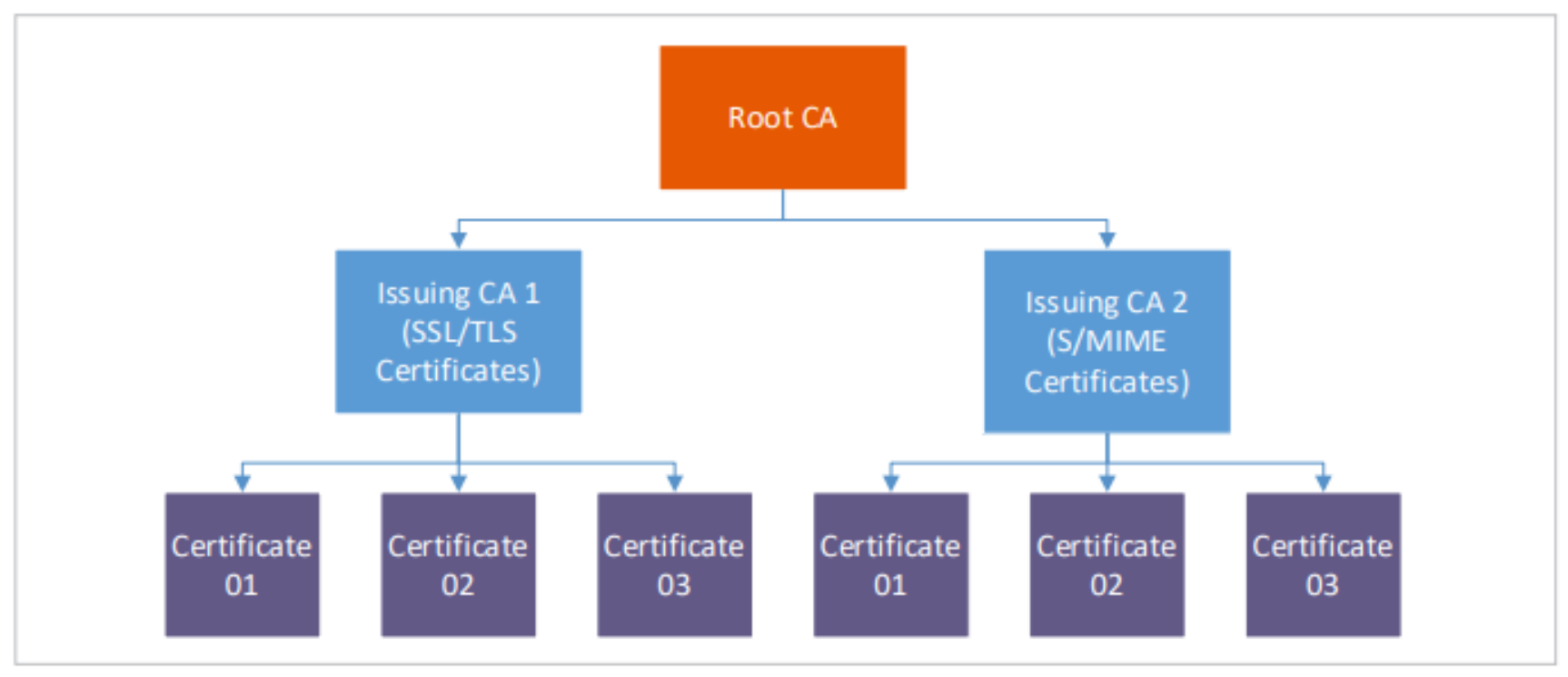
Bridge CA



Business With Wisdom
...Growth With Assurance

IMPLEMENTATION

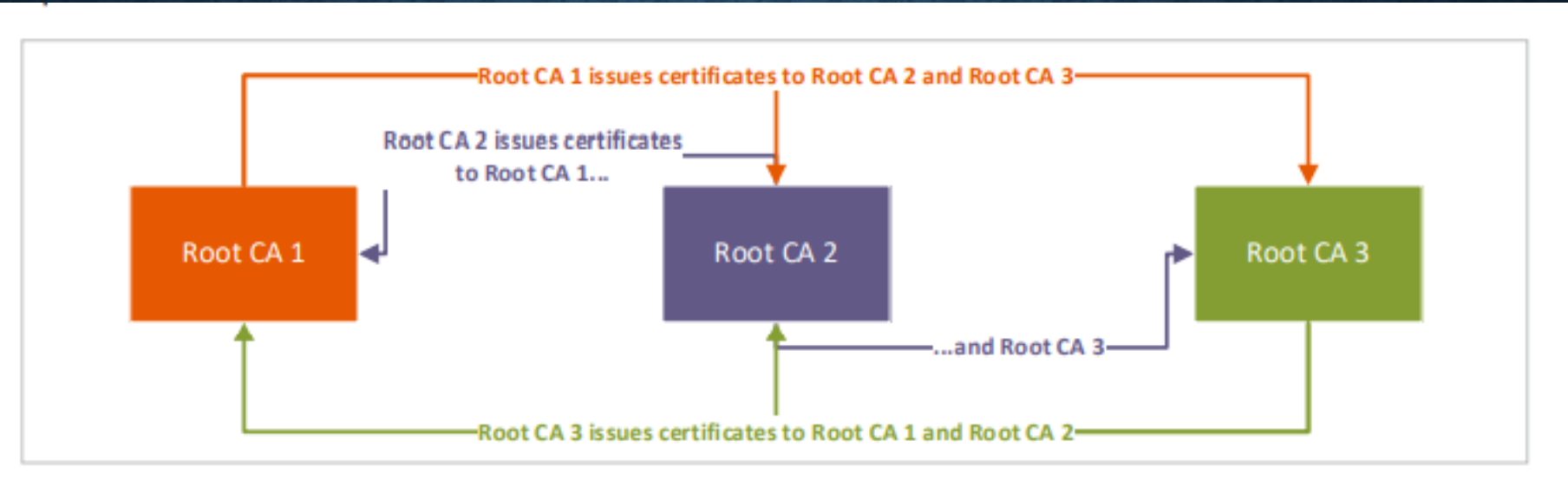
Standard Hierarchical Model



Business With Wisdom
...Growth With Assurance

IMPLEMENTATION

Cross Certification



Business With Wisdom
...Growth With Assurance

IMPLEMENTATION

The CA maintains controls to provide reasonable assurance that certificate **Systems are segmented into networks based on their functional, or logical relationship.**

The CA maintains controls to provide reasonable assurance that Security Support Systems are implemented and configured to **protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks.**

The CA maintains **local network components (e.g., firewalls and routers) in a physically secure environment** and audits their configurations periodically for compliance with the CA's configuration requirements.

Business With Wisdom
...Growth With Assurance

IMPLEMENTATION

The CA maintains controls to provide reasonable assurance that **Root CA Systems are located in a High Security Zone and in an offline state or air-gapped from all other networks.**

The **CA's private (signing and confidentiality) keys are stored and used within a secure cryptographic device meeting the appropriate ISO 15408 protection profile or FIPS 140-2 level requirement based on a risk assessment** and the business requirements of the CA and in accordance with the CA's CPS and applicable Certificate Policy(s).

The CA issues CRLs at regular intervals, as specified in the CP, even if no changes have occurred since the last issuance.

Business With Wisdom
...Growth With Assurance

IMPLEMENTATION

The Parent CA makes Sub-CA and cross certificate status information available to Relying Parties using an established mechanism (e.g., CRL, OCSP, etc.) in accordance with the Parent CA's CP.

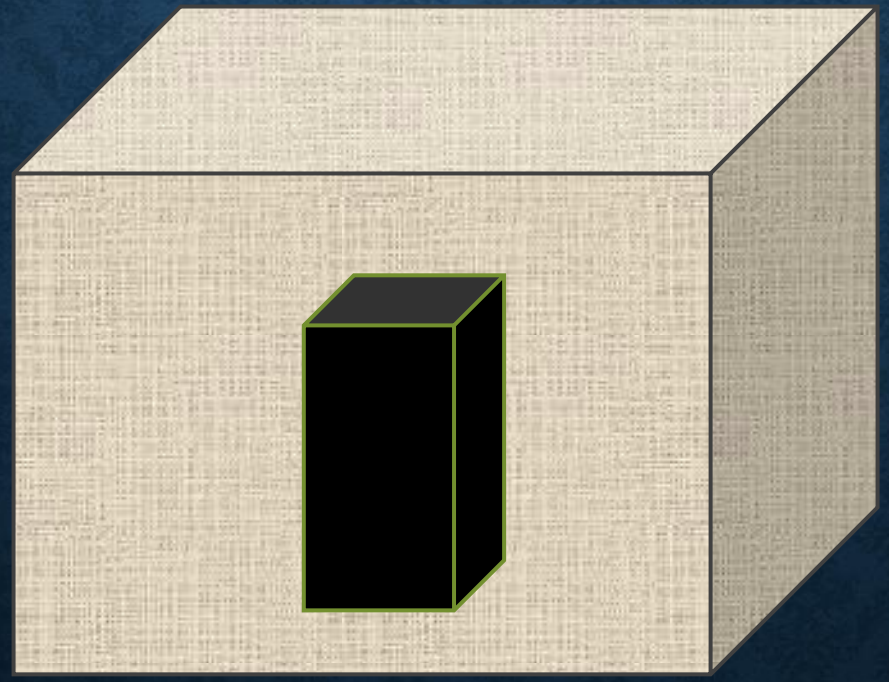
The CA maintains controls to provide reasonable assurance that:

- Code Signing Certificates issued to a Subscriber are valid for a period not exceeding 39 months;
- Non-EV Code Signing Certificates issued to a Signing Service that fully complies with the CS BRs are valid for a period not exceeding 39 months ;
- **Time Stamping Certificates issued to a Timestamp Authority that fully complies with the CS BRs are valid for a period not exceeding 135 months.**
- **Time Stamping Certificates issued to a Timestamp Authority are replaced with a new certificate and a new private key no later than every 15 months**

Business With Wisdom
...Growth With Assurance

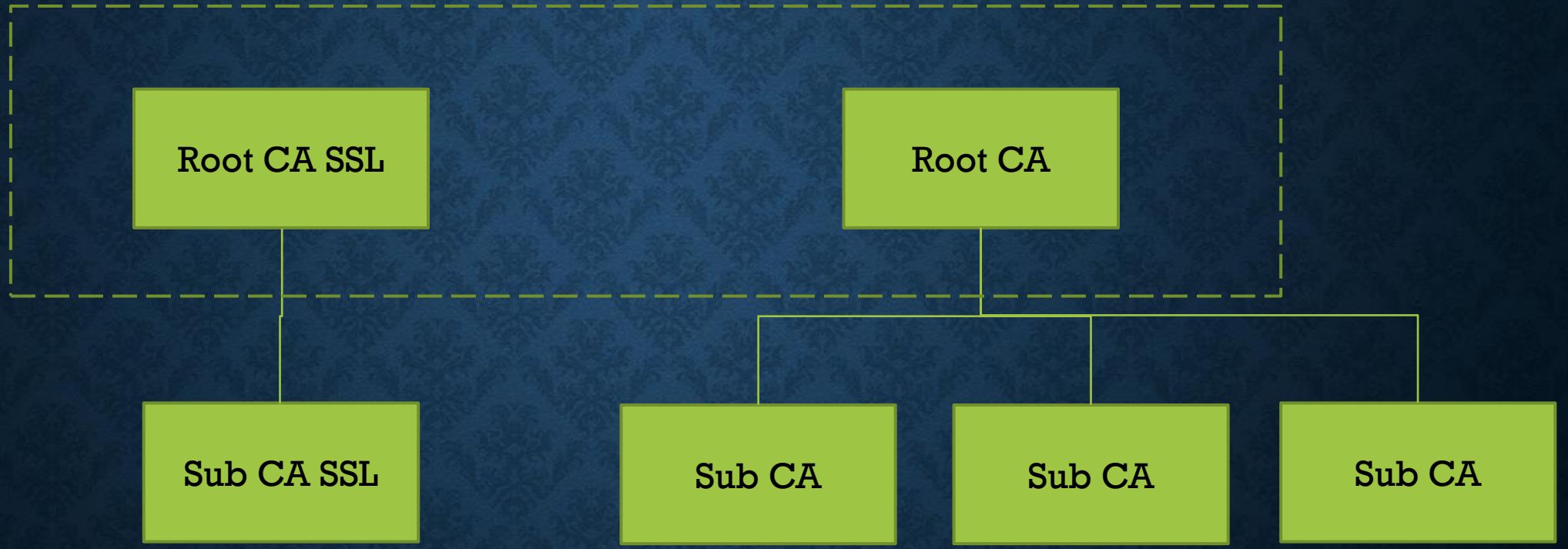
IMPLEMENTATION

Physical barriers are in place (e.g., Faraday cage) to prevent electromagnetic radiation emissions for all Root CA operations (e.g., key generation and certification of CA Certificates) as disclosed in CP and/or CPS



Business With Wisdom
...Growth With Assurance

IMPLEMENTATION



Business With Wisdom
...Growth With Assurance

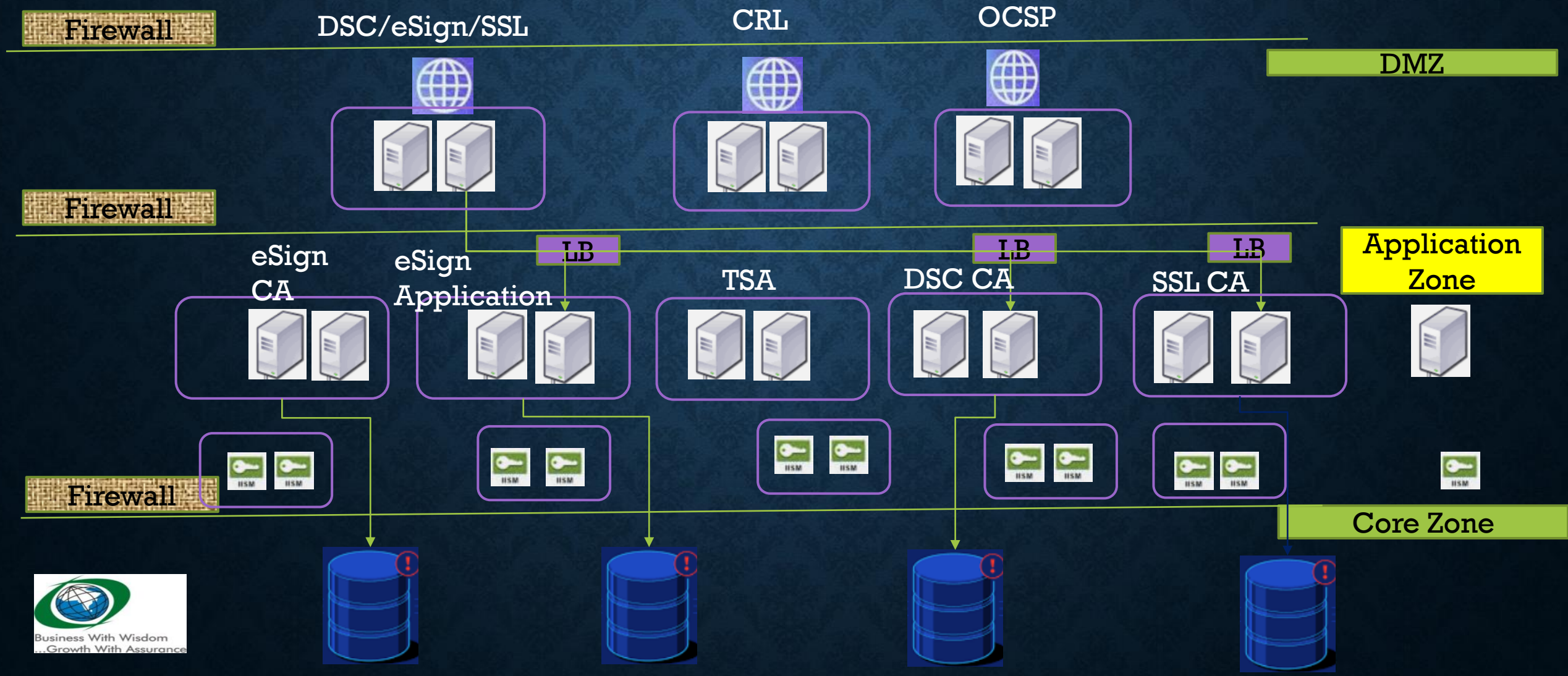
IMPLEMENTATION

Sample CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key algorithm	Key size	Digest algorithm	Not before	Not after	SKI	SHA256 fingerprint
1	1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	6D5A3 34C1BA F569E	rsaEncryption	(4096 bit)	sha256With RSAEncryption	Mar 13 17:13:04 2017 GMT	Dec 31 17:13:04 2030 GMT	02:AE:95:D6: 52:E5:01:87: 40:AD:11:AF: DC:CD:01:EE: 69:A7:D4:77	DB:AF:00:71: 06:47:95:A5: 78:FC:FD:9F: 9E:19:63:BF: E6:D1:3D:D8: FE:8C:47: A0:7E:33:BB: 77:F9:1A:15:19
2	1	C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA – EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	7DAAA F3CF15 F8F45	rsaEncryption	(2048 bit)	sha256With RSAEncryption	Mar 14 01:25:41 2017 GMT	Mar 14 01:25:41 2027 GMT	92:A4:60:D4 :ED:AC:57:3 D:C2:1B:24:0 7:0D:AF:AC :DD:F1:0D:8 A:9A	DF:30:CF:75: 83:21:F7:F6:D0: 08:21:05:AB: CD:BA:A4:59: 38:B3:42:CF: 5D:10:38:27: 92:52:E8:A7: D3:3A:9F
2	2	C=CA O=ABC-CA Inc. CN=ABC-CA Issuing CA – EV	C=CA O=ABC-CA Inc. CN=ABC-CA Root CA – G1	8FABA F6CF45 F884F	rsaEncryption	(2048 bit)	sha256With RSAEncryption	Apr 22 07:41:53 2017 GMT	Apr 22 07:41:53 2027 GMT	92:A4:60:D4 :ED:AC:57:3 D:C2:1B:24:0 7:0D:AF:AC :DD:F1:0D:8 A:9A	DC:25:7D:4E: 09:57:8E:1F: 86:E8:17:95: CA:FF:57:6C: D8:DD:AE:BD: A9:0D:30:23: 3E:24:CA:AC: B4:C6:60:B1

Business With Wisdom
...Growth With Assurance

IMPLEMENTATION



Business With Wisdom
...Growth With Assurance

WEBTRUST EMPANELMENT

Business With Wisdom
...Growth With Assurance

EMPANELLED WEBTRUST PRACTIONER

- *As of December 5, 2022*
  - Anthony Kam & Associates Ltd.
  - AUDIT TRUST SERVICES S.A.S.
  - AUREN
  - Baker Tilly MH Consulting Sdn Bhd
  - BDO
  - Deloitte
  - **Digital Age Strategies Pvt Ltd.**
  - EY
  - Grant Thornton
  - KPMG
  - Moreira Associados Auditores Independentes
  - PKI Contabilidade e Auditoria Ltda
  - PwC
  - Richter LLP
  - RSM Hong Kong Schellman & Company, LLC
  - SUN RISE CPAS' FIRM,
  - MEMBER OF DFK INTERNATIONAL

Business With Wisdom
...Growth With Assurance

WEB TRUST AUDIT : DIGITAL AGE STRATEGIES PVT LTD

- IT Services Company providing services in the area of Information Security
- More than 18 years.
- Certified for ISO 27001:2013 Information Security Management System (ISMS) Standard by RIR Certifications Ltd.
- Certified for ISO 9001:2015 Quality Management System (QMS) Standard by AJA Registrars Ltd., UK.
- Quality of Reporting
- Project Management
- Financial Audit exposure

Business With Wisdom
...Growth With Assurance

VERIFICATION OF DIGITAL AGE SERVICES

- Controller of Certifying Authorities (CCA) Audit for Digital Signature, E-sign.
- Security Audit (Data Centre, DRS, Application, Network, Database)
- VA & PT (Vulnerability Assessment & Penetration Testing)
- Mobile App security audit - Android, IOS, Windows
- Digital Forensic Audit / Investigation
- Application Source Code review
- Anti-Phishing scan , Malware monitoring, WAF Services
- Load testing
- ISO Consultations & Implementation Leading to Certification (ISO 27001-ISMS, ISO 9001-QMS, ISO 22301-BCMS)
- Migration Audit for Application & Data

Business With Wisdom
...Growth With Assurance

VERIFICATION OF DIGITAL AGE EMPANELMENT

CERT-In, Ministry of Information Technology, Govt. of India

CCA, Ministry of Information Technology, Govt. of India

Certification Authorities

WEBTRUST AUDITORS FOR INDIA
Licensed by the CPA, Canada World-Wide Licensing Authority

Data Security Council of India

Reserve Bank of India

National Association of Software and Service Companies

STQC EMPANELED LABORATORIES

EC Council, US Authorized Training Partner

DIT, Government of Maharashtra

Empanelled with several Banks like Corporation Bank, PNB, Indian Bank, South Indian Bank, Federal Bank, Andhra Bank etc. and with ALSTOM for SRLDC, NRLDC, WRLDC

CCA CHECKLIST V/S WEB TRUST

ADDITIONAL REQUIREMENT, PARTIALLY COVERED, UPDATE REQUIRED

PRINCIPLE FOR BASELINE REQUIREMENT

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

- Network and Certificate System Security Requirements (“Network Security Requirements”)

Business With Wisdom
...Growth With Assurance

CONT..

- The principles developed with the relying party in mind and, intended to be practical and nontechnical in nature.
- Certification Authorities Principles
  - CA Business Practices Disclosure
  - The Certification Authority:
  - Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement; and
  - Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control policies in its Certificate Policy

Business With Wisdom
...Growth With Assurance

CONT..

- Principle 2: Signing Service Integrity
  - The CA maintains effective controls to provide reasonable assurance that:
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - The Subscriber information is properly authenticated (for the registration activities performed by ABC-CA); and
  - Subordinate CA certificate and cross certificate requests are accurate, authenticated and approved.

Business With Wisdom
...Growth With Assurance

CONT..

- Principle 3: CA Environmental Controls
  - The Certification Authority maintains effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data is restricted to authorised individuals;
  - The continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance and operations are properly authorised and performed to maintain CA systems integrity

Business With Wisdom
...Growth With Assurance

CONT..

- Principle 3: Extended Validation Service Integrity
  - The Certification Authority maintains effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data is restricted to authorized individuals;
  - The continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

Business With Wisdom
...Growth With Assurance

PRINCIPLE FOR VERIFIED MARK CERTIFICATE REQUIREMENTS

- Principle 1: Policy Management and Business Practices Disclosure
- Principle 2: VMC Service Integrity
- Principle 3: CA Environmental Security
- Principle 4: Network and Certificate System Security Requirements

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Cross certification and meeting browser forum requirement.

• Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue);

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Process update and documentation

- Refer document "WebTrust requirement not covered in CCA checklist"

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Instructions to be published in website for anti-malware organization

The CA provides instructions on its website to Anti-Malware Organization, Subscribers, Relying Parties, Application Software Vendors and other third parties for reporting complaints or suspected private key compromise, CS Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks or other types of fraud, compromise, misuse, or inappropriate conduct related to CS Certificates to the CA

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Extended validation to codesign certificate
- Code Signing Certificate validity not exceeding 39 months
- Time stamping certificate not exceeding 135 months
- Time Stamping Certificates issued to a Timestamp Authority are replaced with a new certificate and a new private key no later than every 15 months

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- For High Risk application maintaining internal data base of all previously revoked certificate to reject subspinous request

> The CA maintains controls to provide reasonable assurance that the CA uses an internal database of all previously revoked Certificates (including those relating to Code Signatures on Suspect Code) and previously rejected certificate requests to identify subsequent suspicious certificate requests.

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- For High risk certificates additional verification

The CA maintains controls to provide reasonable assurance that the CA identifies high risk certificate requests, and conducts additional verification activities, including:

- **Activities in accordance with Section 4.2.1 ofthe SSL Baseline Requirements**
- **Determining whether the entity is identified as requesting a Code Signing Certificate from a High-Risk Region of Concern**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- CA maintains control on malware related incidents

The CA maintains controls to provide reasonable assurance that for incidents involving malware:

- **Within 1 business day of being made aware of the incident, the CA contacts the software publisher and requests a response within 72 hours.**
- **Within 72 hours of being made aware of the incident, the CA determines the volume of relying parties impacted.**
- **If a response is received from the publisher, the CA and publisher determine a 'reasonable date' for revocation**
- **If no response is received from the publisher, the CA notifies the publisher that the CA will revoke the certificate in 7 days unless it has documented evidence that this will cause significant impact to the general public.**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- For High risk certificate verifying delegated third party's process

For High Risk Certificate Requests, the CA maintains controls to provide reasonable assurance that the CA and its Signing Services verify that the Delegated Third Party's processes to identify and further verify High Risk Certificate Requests meets the requirements of the CA's own processes for High Risk Certificate Requests.

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Authority that is available for use by customers of its Code Signing Certificates

The CA maintains controls to provide reasonable assurance that:

It operates a RFC-3161-compliant Timestamp Authority that is available for use by customers of its Code Signing Certificates

It recommends to Subscribers that they use the CA's Timestamping Authority to time-stamp signed code

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- The CA maintains controls to provide reasonable assurance that certificate issuance by the Root CA shall require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation
- Root CA private key not used for EV SSL

The CA maintains controls to provide reasonable assurance that Root CA Private Keys are not used to sign EV SSL certificates.

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Time stamping signing key to be protected by FIPS 140-2 Level 3

The CA maintains controls to provide reasonable assurance that:

- **It protects its Timestamp Authority signing key using a process that is at least to FIPS 140-2 Level 3, Common Criteria EAL 4+ (ALC_FLR.2), or higher.**
- **Any changes to its Timestamp signing process are an auditable event.**
- **The Timestamp Authority ensures that clock synchronisation is maintained when a leap second occurs.**
- **The Timestamp Authority synchronises its timestamp server at least every 24 hours with a UTC(k) time source.**
- **The timestamp server is configured to automatically detect and report on clock drifts or jumps out of synchronisation with UTC.**
- **Clock adjustments of one second or greater are auditable events.**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- EV SSL support in CPS

The CA and its Root CA discloses4 on its website:

- **EV SSL Certificate practices, policies and procedures;**
- **CAs in the hierarchy whose subject name is the same as the EV SSL issuing CA; and**
- **its commitment to conform to the latest version of the Guidelines for Issuance and Management of Extended Validation Certificates issued by the CA/Browser Forum.**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Commercial General Liability Insurance (occurrence form) and Professional Liability/Errors & Omissions insurance as established by the EV SSL Guidelines,

The CA maintains controls and procedures to provide reasonable assurance that:

- **the CA and Root CA maintain the minimum levels of Commercial General Liability Insurance (occurrence form) and Professional Liability/Errors & Omissions insurance as established by the EV SSL Guidelines, and**
- **the providers of the Insurance coverage meet the ratings qualifications established under the EV SSL Guidelines, or**
- **If the CA and/or its root CA self-insures for liabilities, the CA and/or its root CA maintains the minimum liquid asset size requirement established in the EV SSL Guidelines.**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Guidelines to be published by CA
- Instructions to report suspected compromise

The CA provides instructions to Subscribers, Relying Parties, Application Software Vendors and other third parties for reporting complaints or suspected private key compromise, EV SSL Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV SSL Certificates to the CA.

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- EV SSL certificate support for international organization

The CA maintains controls to provide reasonable assurance that it issues EV SSL Certificates to Non-Commercial Entities as defined within the EV SSL Guidelines that meet the following requirements:

• the Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government; • the Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

• the Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- CRLs for an EV SSL Certificate chain can be downloaded in no more than three (3) seconds over an analogue telephone line under normal network conditions.

The CA maintains controls to provide reasonable assurance that CRLs for an EV SSL Certificate chain can be downloaded in no more than three (3) seconds over an analogue telephone line under normal network conditions.

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Self-Assessment on at least once in 3 months

The CA maintains controls to provide reasonable assurance that:

• it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the EV SSL Certificates issued during the period commencing immediately after the previous self-assessment samples were taken. For all EV SSL certificates where the final cross-correlation and due diligence requirements of Section 11.13 are performed by a Delegated Third Party, the sample size is increased to at least six percent (6%); and

• The CA reviews each Delegated Third Party's practices and procedures to assess that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- VMC issuance in CPS

> **The CA maintains controls to provide reasonable assurance that CRLs for an EV SSL Certificate chain can be downloaded in no more than three (3) seconds over an analogue telephone line under normal network conditions.**

- Limitation on liability in CPS

> **The CA discloses in the CP and/or CPS any limitations on liability, if the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its CP and/or CPS**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- The CA maintains controls to provide reasonable assurance that it issues VMC to Government Entities

The CA maintains controls to provide reasonable assurance that it issues VMC to Government Entities as defined within the VMCR that meet the following requirements:

- **the entity's legal existence was established by the political subdivision in which the entity operates;**
- **the entity is not in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and**
- **the entity is not listed on a government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- VMC to Non-Commercial Entities

The CA maintains controls to provide reasonable assurance that it issues VMC to Non-Commercial Entities, defined within the VMCR as applicants that meet the following requirements:

- **the Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government;**
- **the Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and**
- **the Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Subordinate CA

The CA maintains controls to provide reasonable assurance that it does not archive the Subordinate CA Private Keys. Additionally:

- **If the CA or any of its designated RAs generated the Private Key on behalf of the Subordinate CA, then the CA shall encrypt the Private Key for transport to the Subscriber or Subordinate CA.**
- **If the CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.**
- **The CA only archives a Subordinate CA Private Key if it receives authorisation from the Subordinate CA.**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Operational existence verification

The CA maintains controls to provide reasonable assurance that it verifies Applicant's, or Affiliate/Parent/Subsidiary Company's operational existence by:

- verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;
- verifying that the Applicant, Affiliate, Parent Company, or
- Subsidiary Company is listed in either a current QIIS or QTIS;
- • verifying that the Applicant, Affiliate, Parent Company, or
- Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit
- Account directly from a Regulated Financial Institution; or
- relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current
- Demand Deposit Account with a Regulated Financial Institution.

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- The CA maintains controls to provide reasonable assurance the CA confirms that the Mark Representation submitted by the Subject organization matches the Registered Mark

> **The CA maintains controls to provide reasonable assurance the CA confirms that the Mark Representation submitted by the Subject organization matches the Registered Mark in accordance with Section 3.2.16.1 of the VMCR.**

- Third party delegation

> **The CA maintains controls to provide reasonable assurance that Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are configured by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party.**

Business With Wisdom
...Growth With Assurance

ADDITIONAL REQUIREMENTS COMPARED TO CCA CHECKLIST

- Critical vulnerability mitigation within 96 hrs

The CA maintains controls to provide reasonable assurance that it performs one of the following within ninety-six (96) hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: '• Remediate the Critical Vulnerability;

• If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: — Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and — Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; OR

Business With Wisdom
...Growth With Assurance

PARTIAL UPDATE COMPARED TO CCA CHECKLIST

- Key Generation script

a. definition and assignment of participant roles and responsibilities;

b. management approval for conduct of the key generation ceremony;

c. specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers;

d. specific steps performed during the key generation ceremony, including;

• Hardware preparation;

• Verification of the integrity of the operating system and other software from its source

• Verification of the integrity of the operating system and other software from its source

• When a previously built master operating system image is being used, verification of the integrity of that image;

• Operating system installation;

• CA application installation and configuration;

• CA key generation;

• CA key backup;

e. physical security requirements for the ceremony location

g. sign-off on the script or in a log from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and

h. notation of any deviations from the key generation ceremony script

Business With Wisdom
...Growth With Assurance

PARTIAL UPDATE COMPARED TO CCA CHECKLIST

- 12 chars password for Admin

The CA maintains controls to provide reasonable assurance that Trusted Roles using a username and password to authenticate shall configure accounts to include but not be limited to: • For accounts accessible only within Secure Zones or High Security Zones: — Passwords have at least twelve (12) characters • For authentications which cross a zone boundary into a Secure Zone or High Security Zone: — Require Multi-Factor Authentication • For accounts accessible from outside a Secure Zone or High Security Zone: — Passwords to have at least eight (8) characters, not be one of the user's previous four (4) passwords; and implement account lockout for failed access attempts in accordance with requirement 2.k (Criterion 2.11); • Effective 1 April 2020, routine password changes are completed no more frequently than once every two years.

Business With Wisdom
...Growth With Assurance

PARTIAL UPDATE COMPARED TO CCA CHECKLIST

- System account review once in 3 months

The CA maintains controls to provide reasonable assurance that it reviews all system accounts at least every three (3) months and deactivates any accounts that are no longer necessary for operations.

Business With Wisdom
...Growth With Assurance

PARTIAL UPDATE COMPARED TO CCA CHECKLIST

- Trusted role delegated to third party

> **The CA maintains controls to provide reasonable assurance that Security Support Systems under the control of CA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems.**

- Log review within 31 days

> **The CA maintains controls to provide reasonable assurance that it monitors the integrity of the logging processes for application and system logs through continuous automated monitoring and alerting or through a human review to ensure that logging and log-integrity functions are effective. Alternatively, if a human review is utilized and the system is online, the process must be performed at least once every 31 days**

Business With Wisdom
...Growth With Assurance

PARTIAL UPDATE COMPARED TO CCA CHECKLIST

- Subordinate CA certificate revocation within 7 days

The CA maintains controls to provide reasonable assurance that Subordinate CA Certificates are revoked within 7 days if any of the following events occurs:

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6,

……

Business With Wisdom
...Growth With Assurance

PARTIAL UPDATE COMPARED TO CCA CHECKLIST

- Vulnerability Assessment to be conducted every 3 months

The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following: • Within one (1) week of receiving a request from the CA/Browser Forum; • After any system or network changes that the CA determines are significant; and • At least every three (3) months

Business With Wisdom
...Growth With Assurance

CCA TO UPDATE

- OCSP response using RFC 2560 - it is obsolete and taken over by 6960 from June 2013.

> **The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960 and/or RFC5019, and are signed either:**
>
> **…..**

Business With Wisdom
...Growth With Assurance

X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

RFC 6960

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions:

04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | RFC 6960

Document	**Type**	RFC - Proposed Standard (June 2013) Errata Updated by RFC 8954 Obsoletes RFC 2560, RFC 6277 Updates RFC 5912 Was draft-ietf-pkix-rfc2560bis (pkix WG)
	Authors	Stefan Santesson, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, Dr. Carlisle Adams


Questions


Business
Continuity

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

Partnering For Excellence

Business With Wisdom
...Growth With Assurance

DIGITAL AGE STRATEGIES PVT. LTD.