NEW IVG Guidelines and WebTrust

Subhash Rao P

Associate Director Digital Age Strategies Pvt Ltd

PROFILE

Subhash Rao P B.E , MBA

Associate Director , Sr Auditor at Digital Age

30+ years of industry Experience, 20 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 Audit, Forensic Audit, Certifying Authority Audit, WebTrust Audit, Consultancy.

Certification

EC-Council C|EH CERTIFIED

EC-Council C|HFI CERTIFIED

EC-Council E|CIH CERTIFIED

EC-Council C|ND CERTIFIED

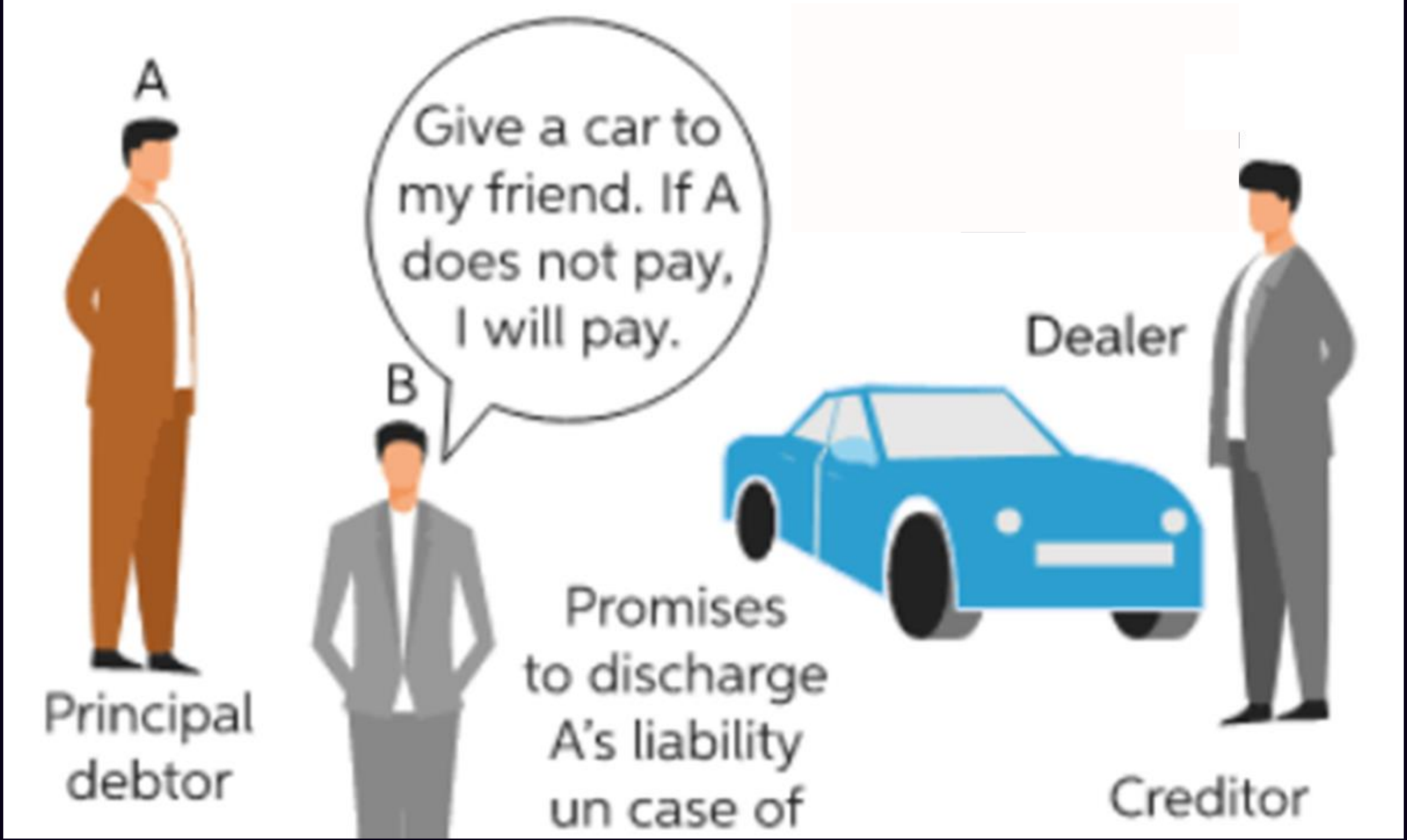
EC-Council C|EI CERTIFIED

CDPSE

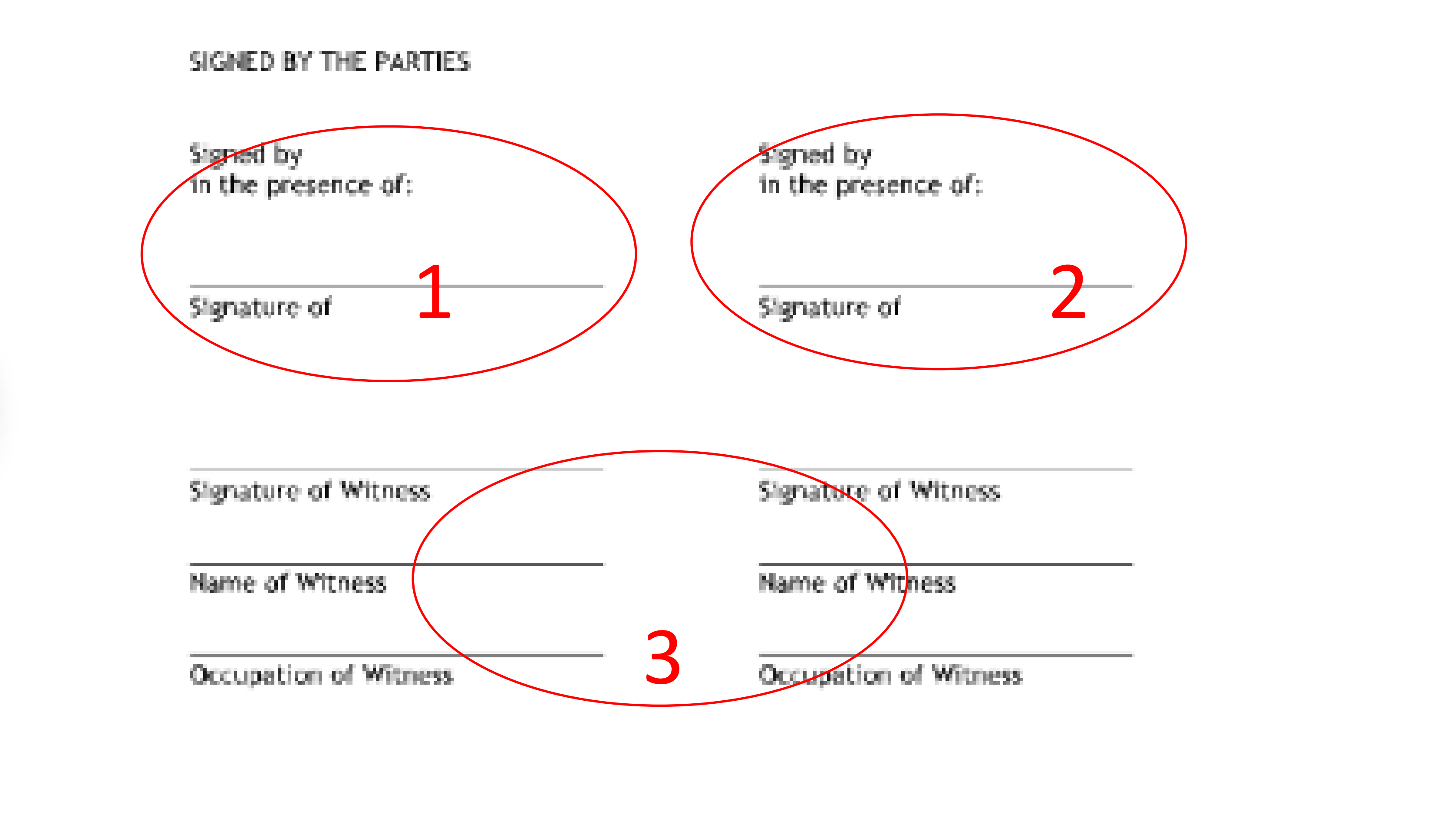
ISO 27001 Certified Lead Auditor

Business With Wisdom
...Growth With Assurance

Certified for ISo27001: 2022 LA


A
Give a car to my friend. If A does not pay, I will pay.
B
Dealer
Principal debtor
Promises to discharge A's liability un case of
Creditor

Trust Model



SIGNED BY THE PARTIES

Signed by
in the presence of:

Signature of

Signature of Witness

Name of Witness

Occupation of Witness

Signed by
in the presence of:

Signature of

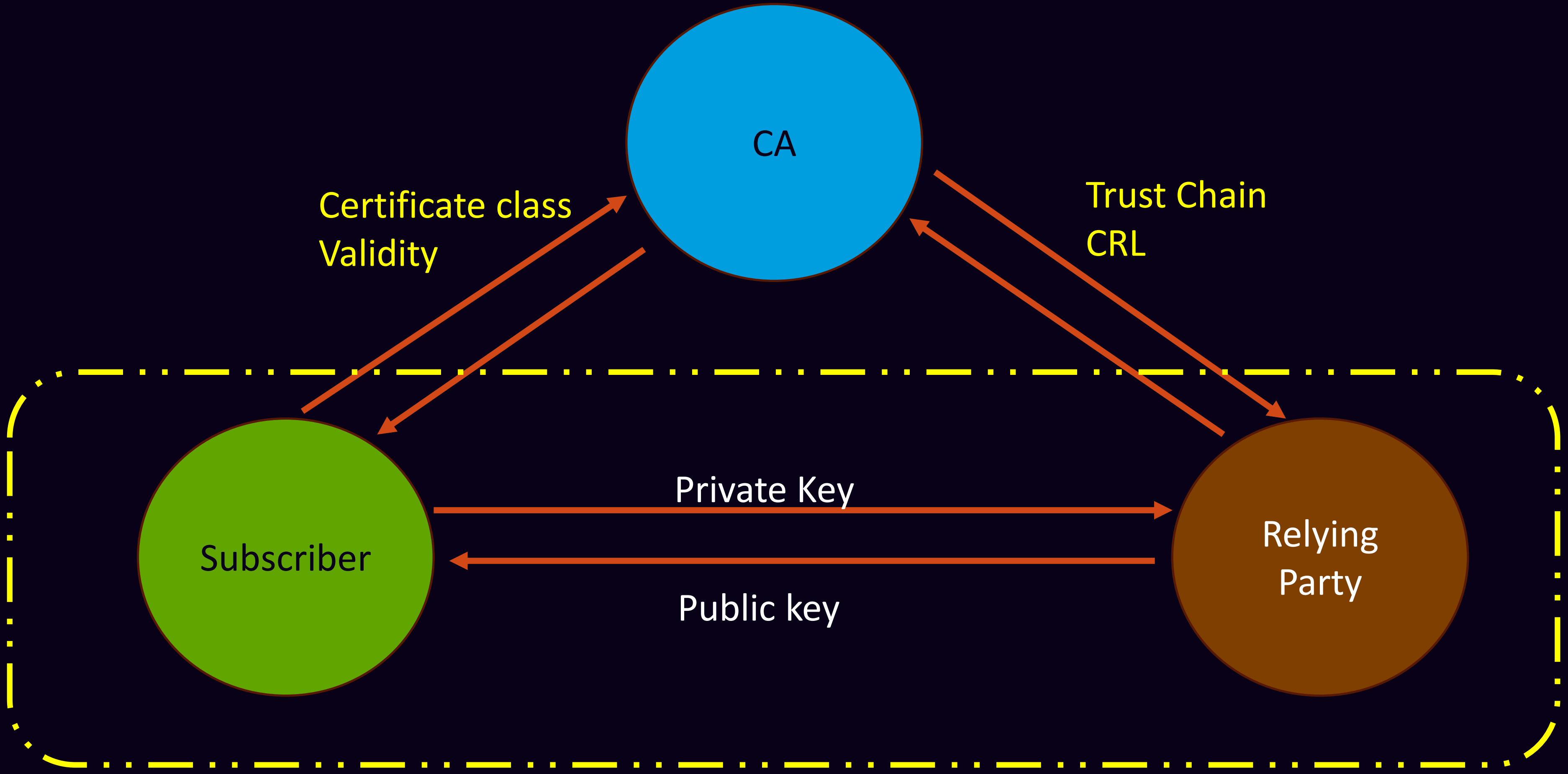
Signature of Witness

Name of Witness

Occupation of Witness

Business With Wisdom
...Growth With Assurance

Trust Model


CA
Certificate class
Validity
Trust Chain
CRL
Subscriber
Private Key
Public key
Relying
Party

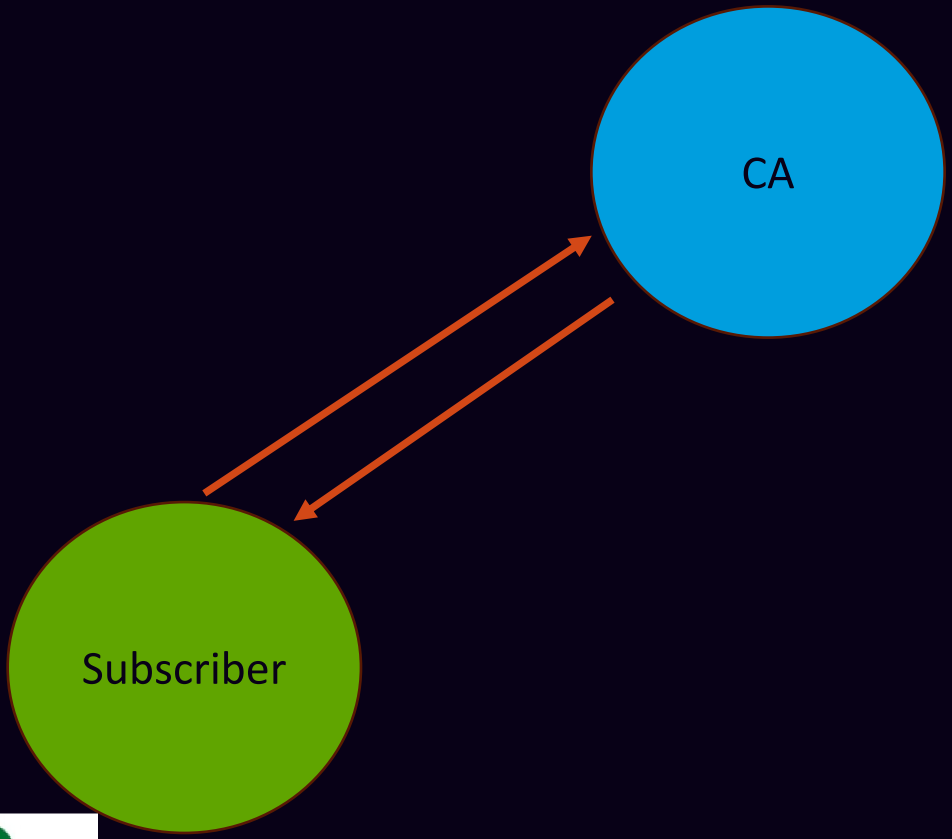
Trust model

- One important question must be answered.
- How will we know in the digital world that an individual’s public key actually belongs to that individual?
- A digital certificate, which is an electronic document containing information about an individual and his or her public key, is the answer.
- The digitally signed document by a trusted organization referred to as a Certification Authority (CA).
- The basic premise is that the CA is vouching for the link between an individual’s identity and his or her public key.
- The Certification Authority provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate.

WebTrust and CA browser forum

- WebTrust engagement by those practitioners enrolled by CPA Canada.
- The CA/Browser Forum was formed among certification authorities (CAs), vendors of Internet browser software and other applications.
- These voluntary organization has worked collaboratively in defining guidelines and means of implementation for PKI as used on the Internet and in certain applications.

What is expected



- Controls are applied for information collection at Subscriber side.
- Controls are applied at CA for the data verification.

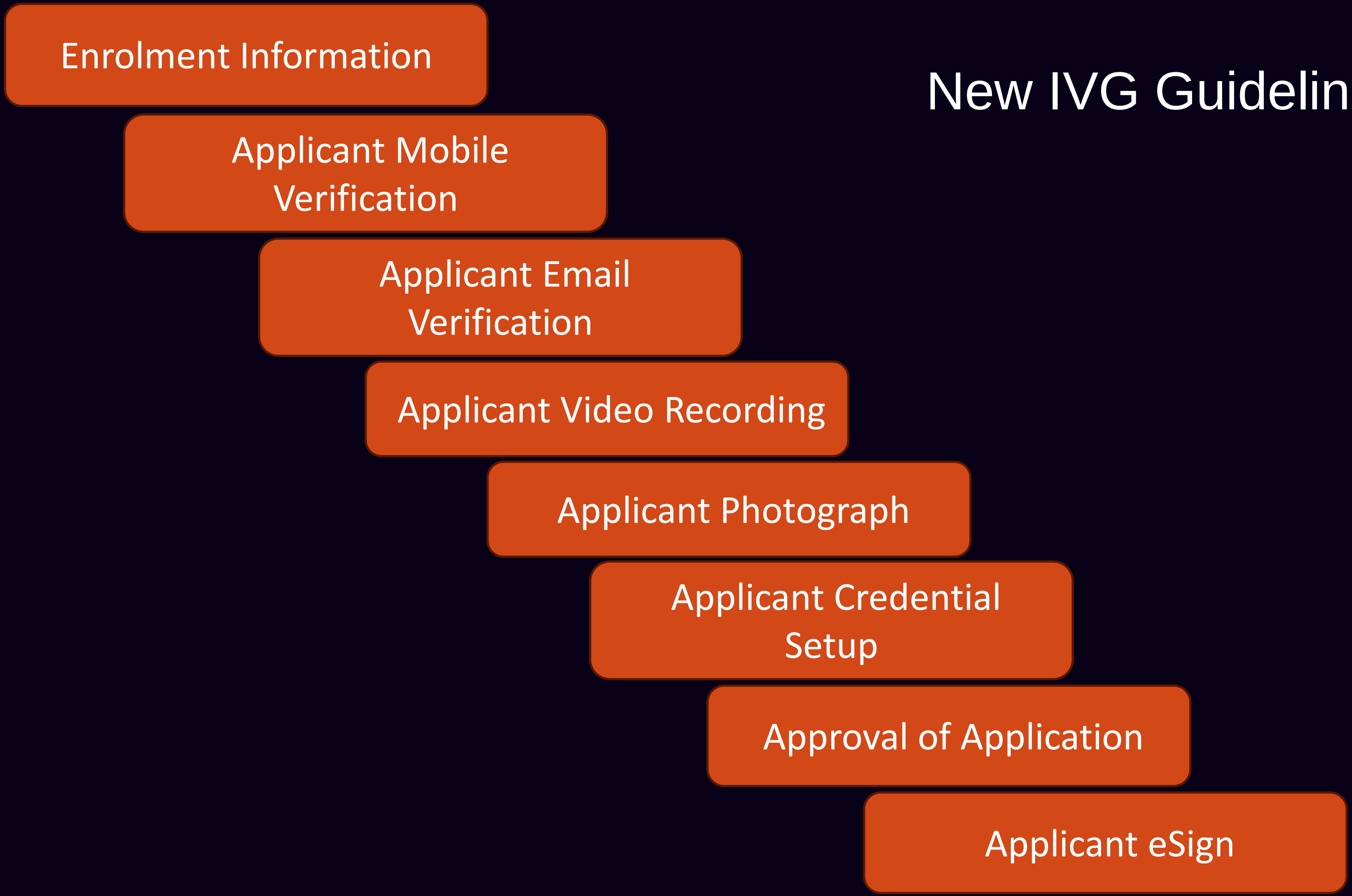
WebTrust controls : Subscriber Registration

- The CA maintains controls to provide reasonable assurance that:
- subscribers are accurately identified in accordance with the CA's disclosed business practices;
- subscribers' domain names and IP addresses are accurately validated in accordance with the CA's disclosed business practices; and
- subscribers' certificate requests are accurate, authorized and complete.
- CA's disclosed business practices;

Business With Wisdom
...Growth With Assurance

How to implement Trust model

New IVG Guidelines



Enrolment Information

Applicant Mobile Verification

Applicant Email Verification

Applicant Video Recording

Applicant Photograph

Applicant Credential Setup

Approval of Application

Applicant eSign

Business With Wisdom
...Growth With Assurance

How to implement Trust model: IVG Guideline

Controller of Certifying Authorities

- Collect information “ KYC”
  - Organization
  - Pan
  - Aadhaar
  - Direct
- Create account
- Authenticate the applicant using the applicant’s mobile number.
- Same mobile number shall be used in the subsequent authentication

Why IVG plays major role in Trust model

- CA provides assurance to relying party
  - Subscriber having private key for the disclosed public key
- CA plays role of witness
- To provide assurance, CA has verified the subscriber
- “Under the Information Technology Act, Digital Signature Certificates (DSC) are issued by Certifying Authorities (CA) upon successful verification of the identity and address credentials of the applicant”

Business With Wisdom
...Growth With Assurance

What is required in Trust model

- WebTrust control
- 5.4.8: Subscriber Agreements describe the required processes to be followed by the Subscriber of any use of the cryptographic mechanism

- "Section 71 of the IT Act stipulates that if anyone makes a misrepresentation or suppresses any material fact from the CCA or CA for obtaining any DSC such person shall be punishable with imprisonment up to 2 years or with a fine up to one lakh rupees or with both"

- This shall be displayed to subscriber.

Business With Wisdom
...Growth With Assurance

What is required in Trust model

- IT Act for protecting the information specifically Rules 33 and 34 of IT CA Rules
- “Information collected from applicant by CA shall be protected and shall not be shared.
    - video, photo, ID cards, phone number, PAN/Aadhaar”
- “Information retention by anybody other than CA, as applicable under the provisions of the IT Act, shall be liable for a penalty for breach of confidentiality and privacy under section 72 of the IT Act.”

Business With Wisdom
...Growth With Assurance

How to secure the data collection

- If someone is sniffing subscriber when login, they will be able to pretend they are subscriber and be logged in as well.
- If the session id is changed, it offers another layer of security, making it harder for the perpetrator to hijack your session.
- Upon successful authentication of the applicant, start a new session for all the associated with the eKYC account creation process and continue the session till its completion.

Business With Wisdom
...Growth With Assurance

How to secure the data collection

- Provide the interface only to the applicant.
- CA shall not provide any provision to submit the applicant's details other than the applicant.
- Allow submission only through website interface
    - No link based access.

Business With Wisdom
...Growth With Assurance

How to implement Trust model – Mobile number

- For the proof of possession of the mobile number, CA shall send an SMS OTP
- The same shall be verified by capturing through the interface provided by CA

How to implement Trust model – eMail

- Email ID of the applicant is mandatory for issuance of DSC based on the eKYC account activated by CA
- For email verification, the CA shall send an email OTP or challenge response or verification URL
- No disposable email (fast temporary email without registration) shall be accepted by CA

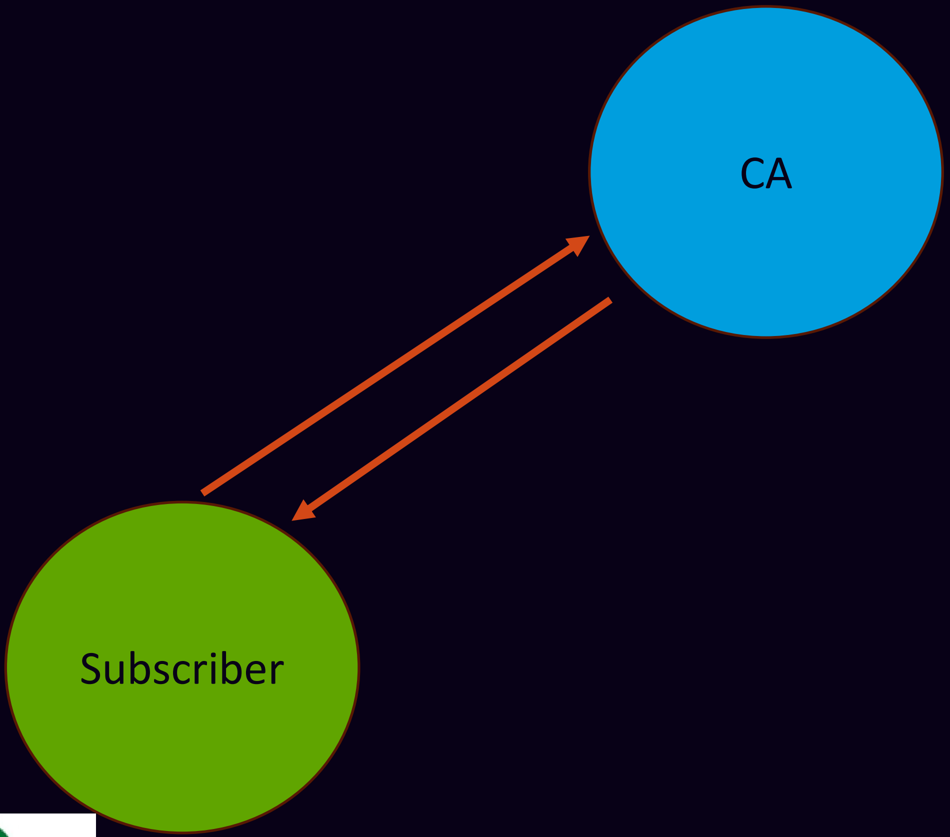
Business With Wisdom
...Growth With Assurance

How to implement Trust model – Verification

- CA shall allow only the automatic population of digitally signed information received from the source of eKYC like Aadhaar or Bank in the electronic application form
- verification of the DSC applicant shall be carried out using online interactive video verification
- the originals of the identity and address proof shall be verified during the video verification.

Business With Wisdom
...Growth With Assurance

How to implement Trust model



- Provide validity for the thrust
- The validity of the eKYC account shall not be more than 2 years.
- Conduct fresh eKYC verification.
- The applicant shall have the option to activate, deactivate and close the account at any point.

Business With Wisdom
...Growth With Assurance

How to implement Trust model

- The PIN shall be created along with the eKYC account ID.
- eKYC account user ID change is not allowed after creation.
- The PIN reset shall be with mobile OTP and email verification.
- In the absence of email, it shall be mobile OTP and video verification.
- In the case of banking where email is not captured earlier, the PIN reset shall be allowed only after successful matching of fresh eKYC with the registered eKYC details.

Business With Wisdom
...Growth With Assurance

How to implement Trust model

- eKYC account access only through 2 factor authentication.
  - Something you have: Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token
  - Something you know: This could be a personal identification number (PIN), a password, answers to “secret questions” or a specific keystroke pattern
  - Something you are: This category is a little more advanced, and might include biometric pattern of a fingerprint, an iris scan, or a voice print

Business With Wisdom
...Growth With Assurance

How to implement Trust model WebTrust

- For individual end entity certificates, the CA or RA verifies the identity of the person whose name is to be included in the subscriber distinguished name field of the certificate.
- An unauthenticated individual name is not included in the subscriber distinguished name.
- For organisational certificates containing a domain name of an organisation, the CA or RA verifies the organisation’s ownership, control, or right to use the domain name and the authority of the requesting party included in the common name attribute of the subscriber distinguished name field of the certificate.
- An unauthenticated domain name is not included in a certificate.

Business With Wisdom
...Growth With Assurance

How to implement Trust model - Name

- If both PAN and Aadhaar are involved in the KYC process, CA should provide an option to select the name as it appears in either PAN or Aadhaar.
- name match should be verified by CA during the CA verification process.

Business With Wisdom
...Growth With Assurance

How to implement Trust model - Address

- The address of the DSC applicant shall be residential or organizational.
- address proof required

Business With Wisdom
...Growth With Assurance

How to implement Trust model – subscriber agreement

- WebTrust control
- 6.1.12 : The certificate request is treated as acceptance of the terms of conditions by the requesting entity to use that certificate as described in the Subscriber Agreement.
- CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.

Business With Wisdom
...Growth With Assurance

How to implement Trust model – DSC issuance

- DSC shall be issued only upon satisfying the verification requirements specified in the respective eKYC sections in this document.
- The maximum time limit for the download of DSC shall be 30 days from the date of completion of verification/approval.

Business With Wisdom
...Growth With Assurance

How to implement Trust model – SSL Certificate

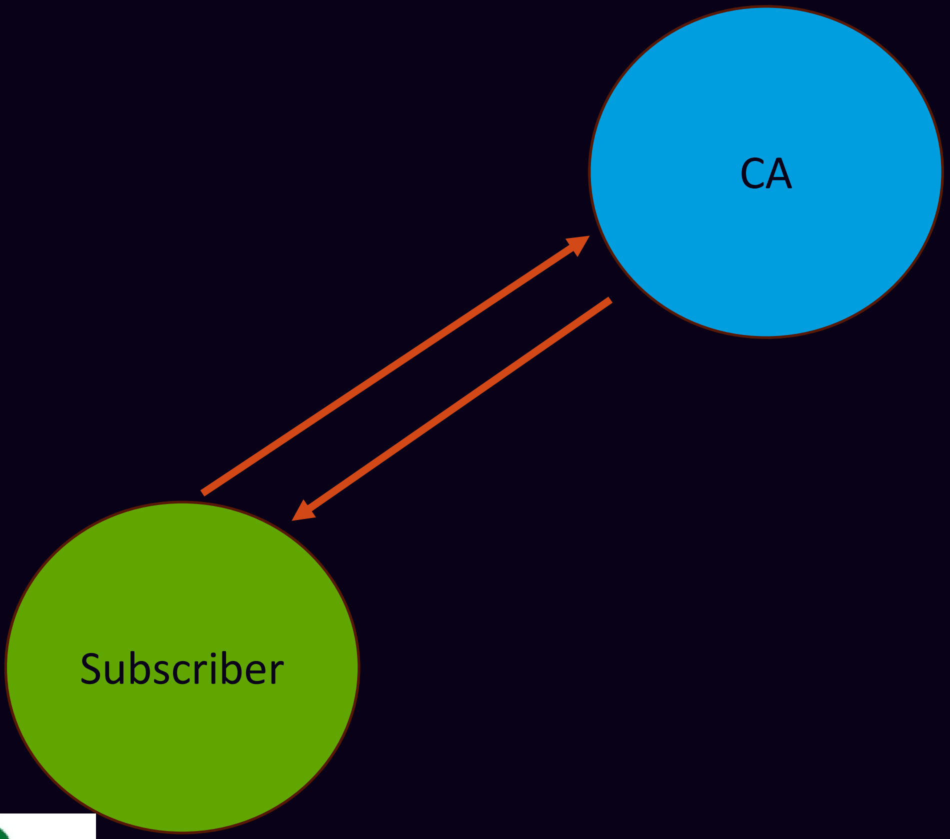
- The issuances limited only to .IN domain.
- Only organizational persons are eligible to apply for SSL certificates on behalf of their organizations.
- The application to the CA in a digitally signed application form.
- Request shall contain
  - the domain name(s) to be certified,
  - the Certificate Signing Request (CSR) and
  - the information of the requestor and the organization.
  - accompanied by necessary supporting documents.

Business With Wisdom
...Growth With Assurance

How to implement Trust model – SSL Certificate

- The minimum set of documents to be submitted includes:
  - DSC Application Form
  - Applicant ID Proof
  - Authorization Letter by Organization Authorized Signatory
  - Authorized Signatory Proof
  - Proof of Organizational Existence

How to implement Trust model – Web Trust requirement



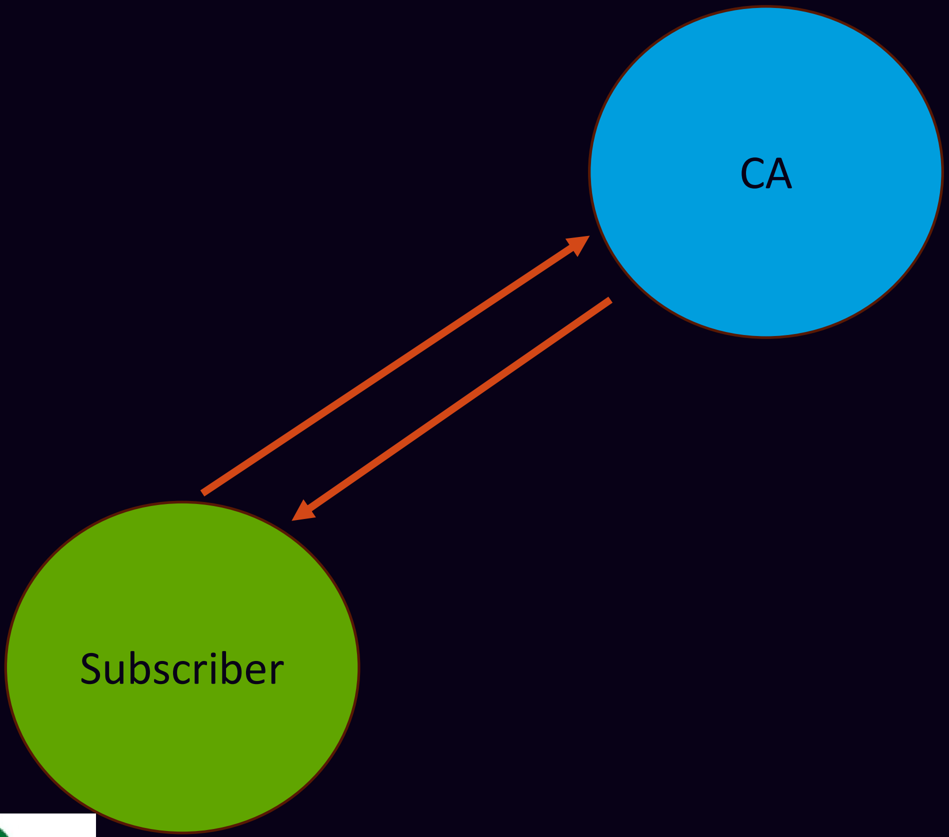
- WebTrust Criterion 2.1.2:
- The CA maintains controls to provide reasonable assurance that for Subscriber certificates issued:
- The subject AltName extension is present and contains at least one entry
- Each entry MUST be either: A dNSName containing the Fully-Qualified Domain Name (Wildcard FQDNs permitted); or
- An iPAddress containing the IP address of a server.

Business With Wisdom
...Growth With Assurance

How to implement Trust model – Domain Name Verification:

- Each value provisioned for subject alternative names (dnsNames) shall undergo domain name verification to prove the ownership / control of the domain by the requestor of the certificate.
- communication to:
  - webmaster@domainname.com,
  - administrator@domainname.com,
  - admin@domainname.com,
  - hostmaster@domainname.com,
  - postmaster@domainname.com, or
  - any email ID listed in the technical, registrant, or administrative contact field of the domain's Registrar record;

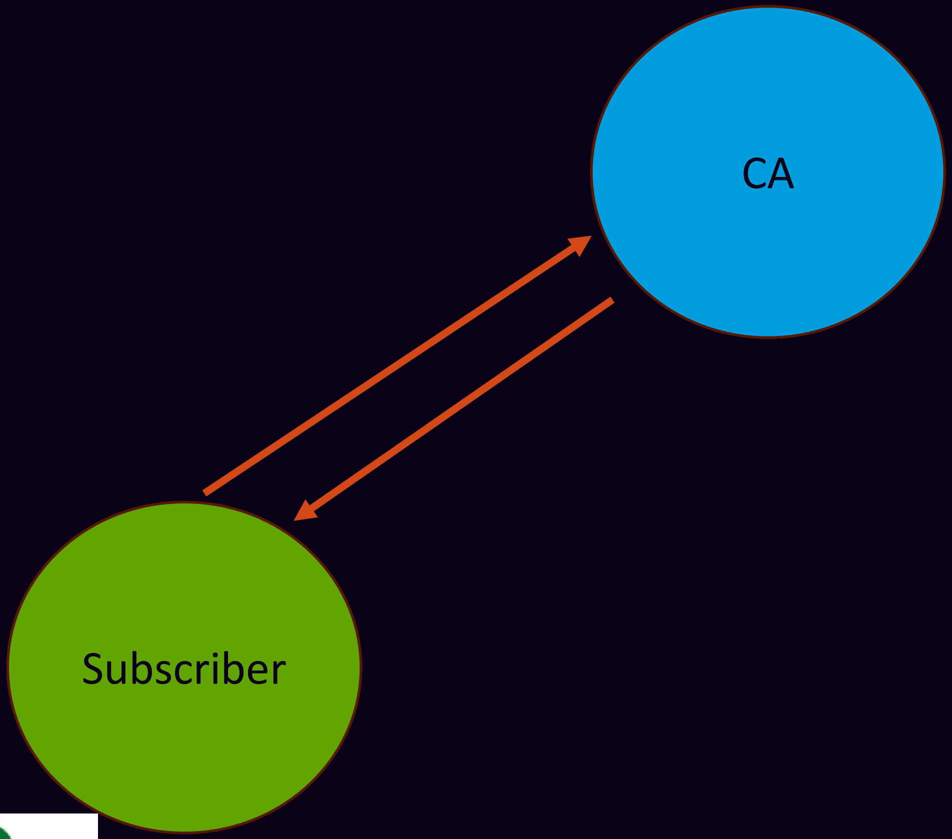
How to implement Trust model – Domain Name Verification:



- Requiring a practical demonstration of domain control (Eg: making changes to the DNS zone file or adding a unique file/filename on the domain under verification);
- This is achieved by CA sharing a unique Request Token or a Random Value, valid for a short duration, with the applicant and validating this data against the content of the file name provided or the DNS value (CNAME, TXT or CAA record) of the domain.

Business With Wisdom
...Growth With Assurance

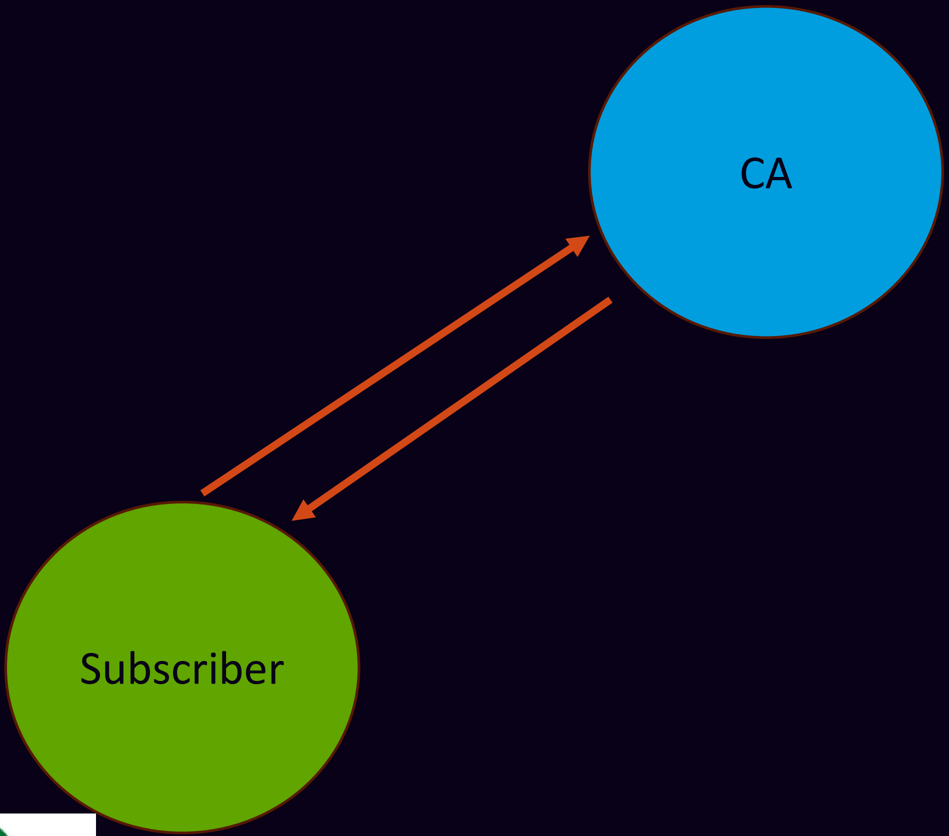
How to implement Trust model – Domain Name Verification:



- In the case of wildcard domains, these shall undergo additional checks, to not to wrongly issue, for a domain listed in the public suffix list (PSL).
- The Public Suffix List (PSL) is a community-maintained list of rules that describe the internet domain name suffixes under which independent organisations can register their own sites.
- If the domain is listed in PSL, the application shall be refused, unless the applicant proves ownership of the entire domain namespace.

Business With Wisdom
...Growth With Assurance

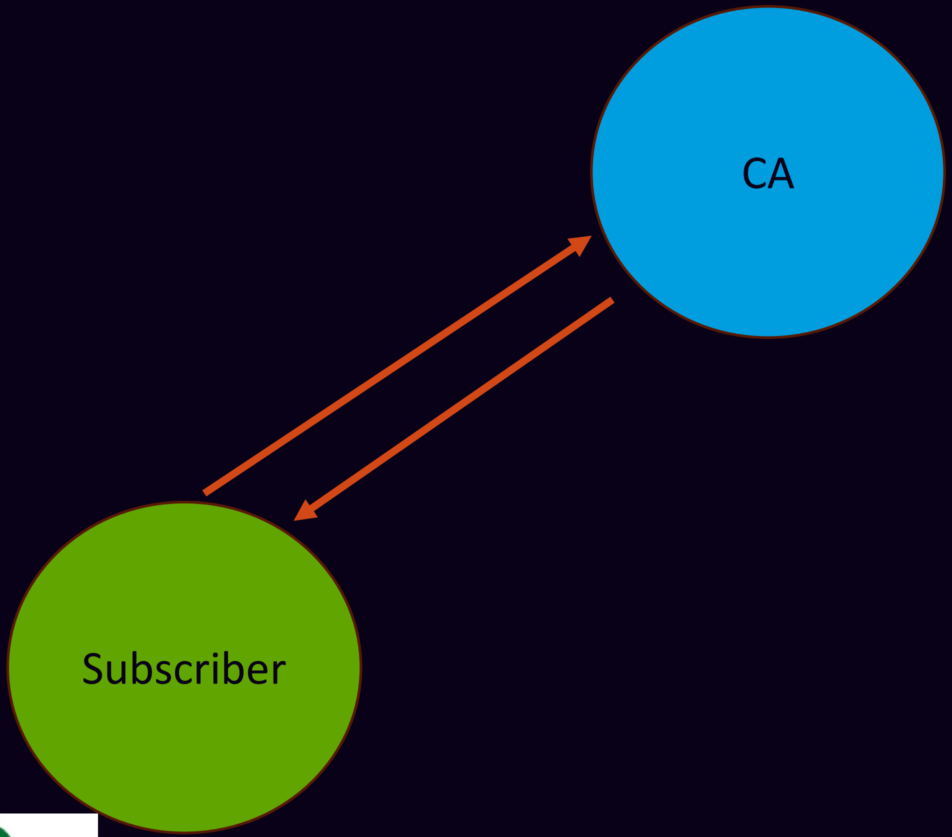
How to implement Trust model – IP:



- it shall be verified to have the applicant’s control over the IP, by means of
  - a change in agreed information in a URL containing the IP address, OR
  - IP assignment document of IANA or Regional Internet Registry, OR
  - performing r-DNS lookup resulting in a domain name verified by above procedure.

Business With Wisdom
...Growth With Assurance

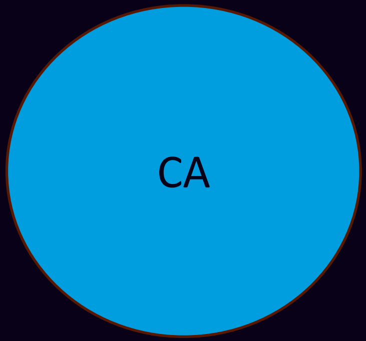
How to implement Trust model – Web Trust



- The CA maintains controls to provide reasonable assurance that it does not issue certificates containing a Reserved IP Address or Internal Name in the subjectAltName extension or subject:commonName field.

Business With Wisdom
...Growth With Assurance

How to implement Trust model – CA



- Disclose practice statement
- Implement secure environment
- Develop policy and implement procedure
- Provide access only to trusted person
- Log all events at CA
- Record verification logs
- Record 6 sec video of verification officer
- Review logs for anomalies
- Train the Trusted persons
- Preventive maintenance of equipment
- Conduct periodic vulnerability assessment
- Conduct periodic compliance audit

Business With Wisdom
...Growth With Assurance

Partnering For Excellence

Business With Wisdom
...Growth With Assurance

DIGITAL AGE STRATEGIES PVT. LTD.