Time Stamping

Need for Timestamping

- To support assertions of proof
  - Certificates or Messages can be signed after a signing key has expired or been revoked and could be "back-dated"
- Required for documents meant for wide distribution or for long term storage and archiving purposes
- Generally operated as a Trusted Third Party Service

Applications

- Office automation workflows
- Financial Transactions
- E-filing
- Share trading
- E-mails, Contracts
- Medical records
- E-tendering, E-procurement
- Patent, Trademark & Geographical Indicators (GI) filing
- Code Signing etc.,

How Time stamping is done?

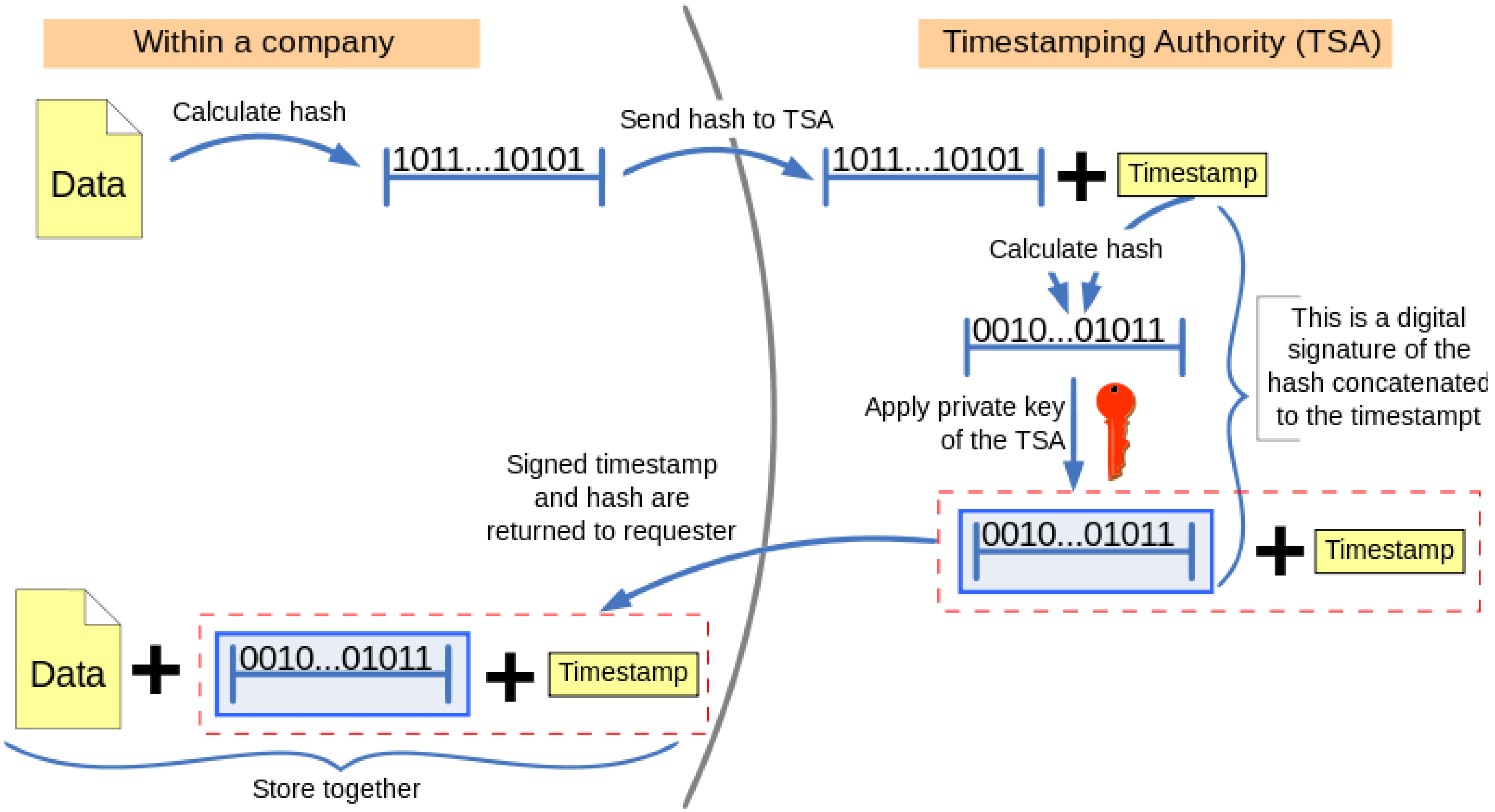
- Time stamping Client
  - Your application
- Time stamping Server
  - Time stamping Authority (TSA)
  - Ex: Verisign, GlobalSign etc…

How Time stamping is done?

- Process
  - Compute hash of your data
  - Send your hash to TSA
    - TSA generally ask you to sign to your hash
  - TSA concatenates a timestamp to the hash and calculates hash of this concatenation. This hash is then digitally signed by TSA.
  - This signed hash + timestamp is sent back to your application which appends it to the original data, and could be sent to the receiver.

How Timestamping is done?

Trusted timestamping

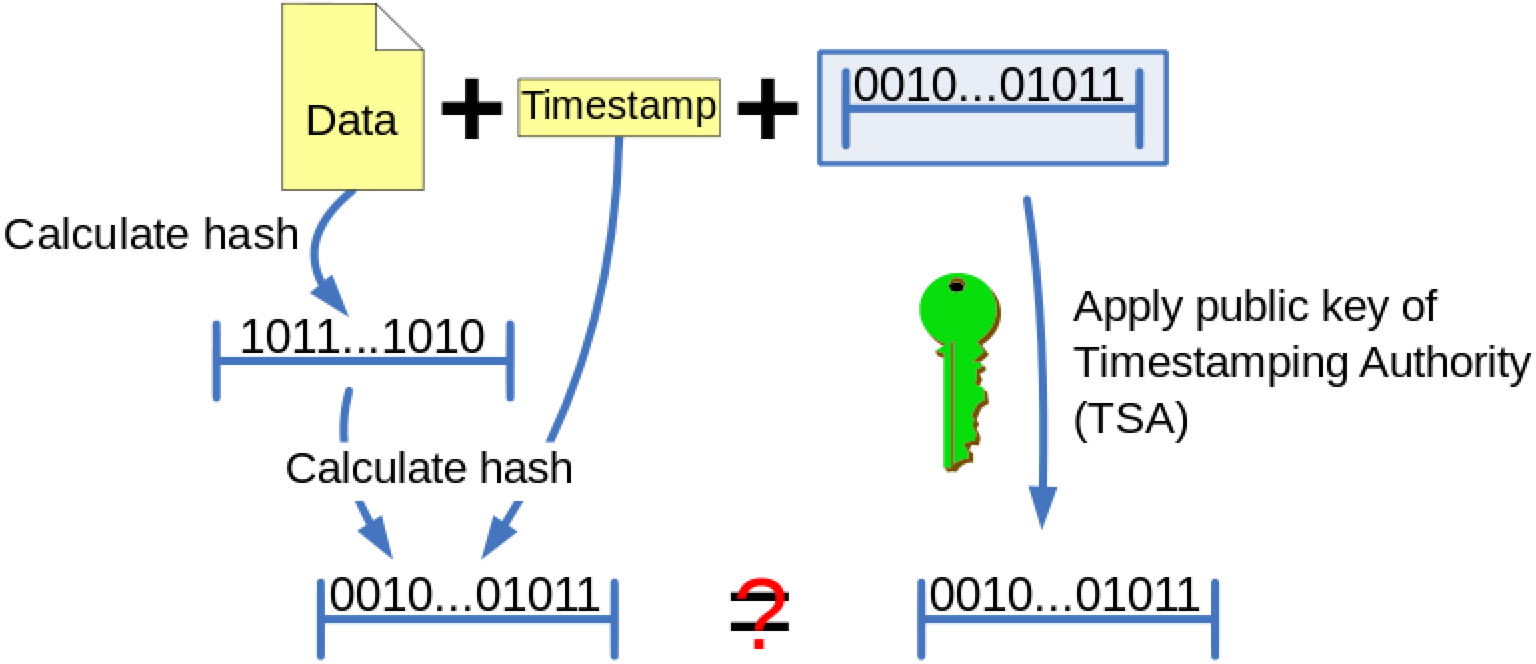

Within a company
Timestamping Authority (TSA)
Data
Calculate hash
1011...10101
Send hash to TSA
1011...10101
Timestamp
Calculate hash
0010...01011
Apply private key of the TSA
This is a digital signature of the hash concatenated to the timestampt
0010...01011
Timestamp
Signed timestamp and hash are returned to requester
Data
0010...01011
Timestamp
Store together

Validation of Timestamp

- First the hash of the original data is calculated
- Timestamp given by TSA is then appended to the above hash
- Hash of the above is calculated (Let's call it A)
- Digital signature of TSA is validated, which will get the hash of (the original message + timestamp) (Let's call it B)
- If A and B are equal then the timestamp and message has not been altered and timestamp was issued by TSA
- If not either the timestamp was not issued by TSA or the timestamp was altered

Validation of Timestamp

Checking the trusted timestamp



If the calculated hashcode equals the result of the decrypted signature, neither the document or the timestamp was changed and the timestamp was issued by the TTP. If not, either of the previous statements is not true.

Time Stamping Services in India

- In India, time stamping services are provided by CA's and CCA have mandated the CA's to provide the same
- Key points that were mentioned in the Time stamping Guidelines for CAs by CCA are:
    - The CA shall not issue a Time stamping certificate other than for its own time stamping service.
    - The Time stamping service provided by CA should be logically & physically separate from the CA systems.
    - However CA can use the same physical infrastructure and resources.

Time Stamping Services in India

- The Audit of the Time Stamping service shall be included in the audit of CA facilities.
- The OID identifier (i.e., {2.16.356.100.3.0} shall be asserted in every time stamp token.
- The time-stamp token shall be signed using a key generated exclusively for this purpose. The relying parties shall be able to ascertain this by the presence of a critical extended key usage extension of id-kp-time stamping {1 3 6 1 5 5 7 3 8}.

Time Stamp Requirements

- **Time Stamp Token:**
  - Time stamp tokens shall be in compliance with RFC 3161.
  - Each time stamp token shall have a unique identifier.
  - The time included in the time-stamp token shall be synchronized with Standard Time Source within the accuracy defined in this policy and, if present, within the accuracy defined in the timestamp token itself. The accuracy is defined to be ± 1 second.

Time Stamp Token Profile

- The time-stamp token shall include:
  - An identifier for the TSA policy,
  - A time value at which the time-stamp token has been generated,
  - A hash value for the data being time-stamped as provided by the requestor,
  - Information on public key cryptography used,
  - A public key certificate or its issuer relating information, and
  - A signature value.

Time Request Format

Field	Value
Version	V1(1)
Message Imprint	Hash algorithm identifier, Hash message
Time Stamping Services Policy ID	Absent or id-tsp business {2.16.356.100.3.0}
Nonce	Optional
Certificate Request	Optional
Request Extension	Value *
None	None

* No extension is required to be supported

Time Stamp Response Format

Field	Value
Status	As specified in RFC 3161
Time Stamp Token	CMS SignedData content type with encapsulated content type of id-ct-TSTInfo {1.2.840.113549..1.9.16.1.4} – always contains time stamping services certificate in SigningCertificate attribute which is part of signerinfo
	Version : V1 (1)
	Time Stamping Services Policy ID : id-tsp business {2.16.356.100.3.0}
	Message Imprint (same as in the Request)
	Serial Number (Unique, up to 160 bits)
	Time Stamp : Generalized time in UTC
	Accuracy : Optional
	Ordering : Optional
	Nonce : Same as in request; present if and only in request
	TSA : Time Stamping Services Distinguished Name
Response Extension	Value *
None	None

* No extension is required to be generated, no extension shall be critical

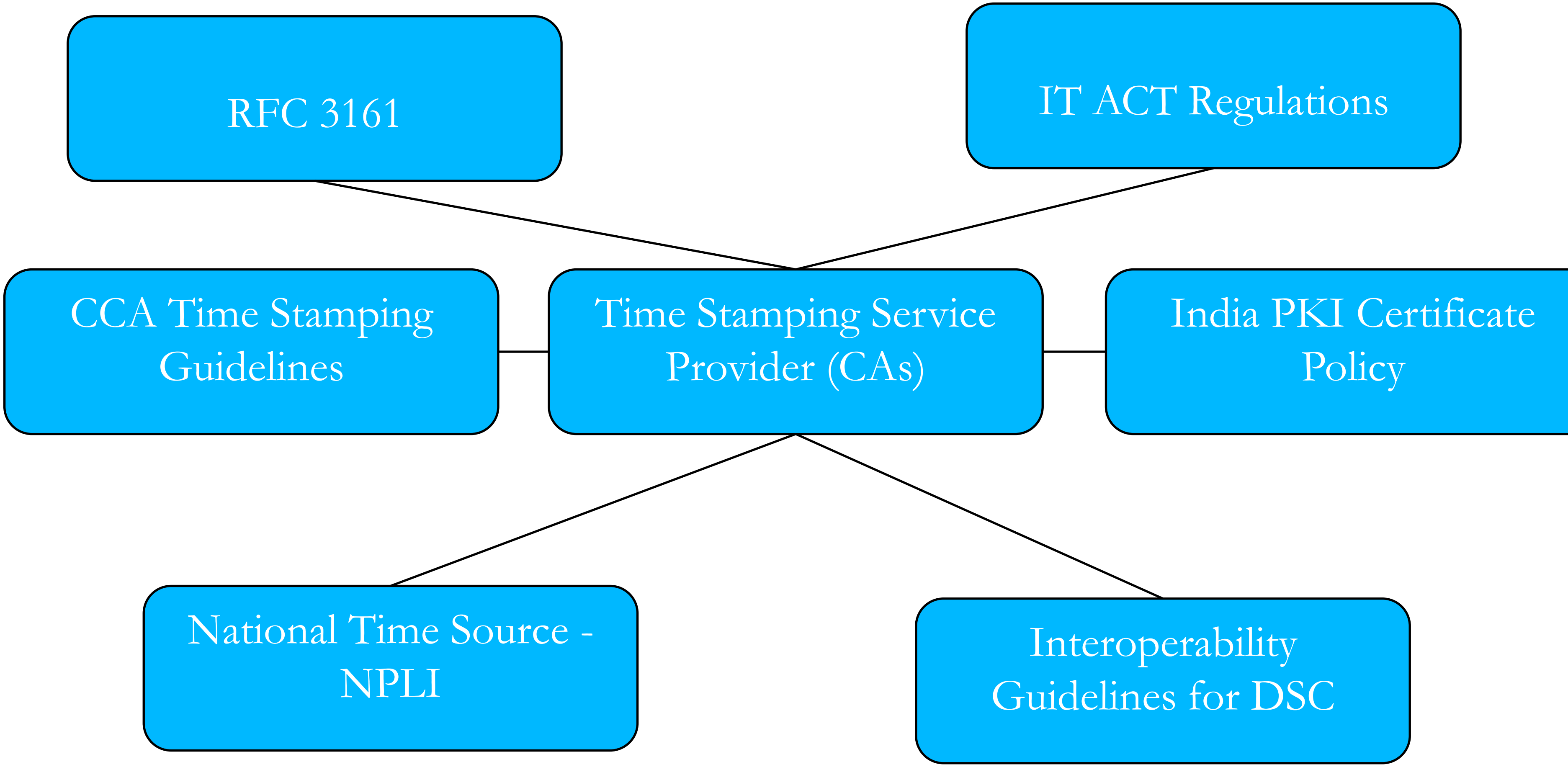
Time Stamp Requirements

- **Time Stamping Services Clock:**
  - The time values the Time Stamping services uses in the time-stamp token shall be traceable to a Standard Time Source in India.
  - When the Time Stamping services clock is detected as being out of the accuracy specified in this guidelines, the event shall be audited and time-stamp tokens shall not be issued. Furthermore, this non-issuance shall be audited.

Time Stamp Requirements

- The National Physical Laboratory, India (NPLI), is responsible for maintenance and development of the Indian Standard Time (IST) .
- NPLI maintains the time scale of Indian Standard Time (IST) with the help of a commercial cesium atomic clock.
- The time scale maintained by NPLI is designated as UTC.
- All the TSAs should synchronize their master clocks with the NPLI based time scale with in the accuracy.

Time Stamping Policy &Time source framework



RFC 3161

IT ACT Regulations

CCA Time Stamping Guidelines

Time Stamping Service Provider (CAs)

India PKI Certificate Policy

National Time Source - NPLI

Interoperability Guidelines for DSC

Key Benefits

- Accurate time in conformance with Government Guidelines
- Digitally Signed timestamps
- Verifiable in future
- Assured Integrity and Non-repudiation
- Fraud Detection
- Electronic Notary
- Content to be time stamped is protected from public exposure

References

- www.cca.gov.in
- www.ietf.org/rfc/rfc3161.txt
- https://en.wikipedia.org/wiki/Trusted_timestamping

Thank You