Mini Conference
Ensuring Legally Significant Trusted Transboundary Electronic Interaction

29 March 2017

Indian Initiatives on Electronic Signature and Mutual Recognition

T.A. Khan
takhan@meity.gov.in

Securing electronic transactions

Authentication	Reliable identification of sender/recipient of data
Confidentiality	Protection of data from undesired disclosure
Integrity	Prevention of undesired creation, modification or deletion of data
Non-repudiation	Committed transactions cannot be denied

Applications and Considerations

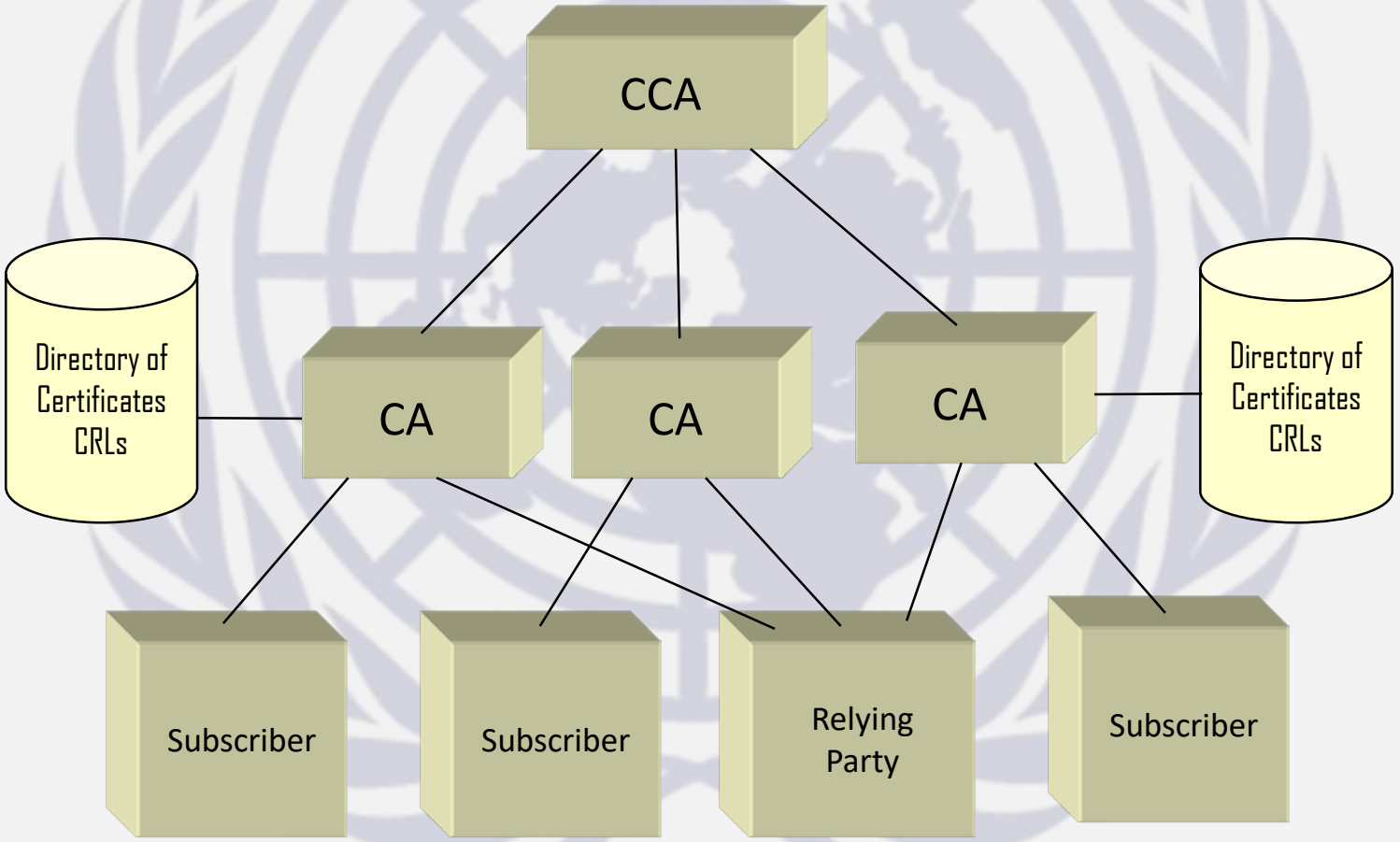
Data filing, eLICENSE,eCOUNCELLING: User-Password/Secure Channel/Supporting Documents

Return Filing: Two Factor Authentication

ePAYMENT: Two factor Authentication(Low Value), Electronic Signature(High Value)

ePROCUREMENT: eSIGNATURE + Multi factor Authentication+ Encryption + Multi location Audit Trail

Indian PKI Model



CCA regulates, licenses CAs and operates Root Certifying Authority for India

PKI in India : A Brief Overview

The Information Technology Act, 2000 provides legal sanctity to Digital Signatures

Office of Controller of Certifying Authorities (CCA) has been established for licensing and regulating the work of Certifying Authorities

Office of CCA has established the Root Certifying Authority of India (RCAI) for signing certificates of licensed CAs, who issue DSCs to the subscribers or operate sub-CAs for issuing DSCs to subscribers

Areas of Applications : e-Licencing , e-Procurement , e-Banking ,e-Governance, e-Mail Signing and Encryption, etc.

Mutual Recognition

The parties shall provide for mutual recognition of trade-related data and documents in electronic form originating from other parties on the basis of substantially equivalent level of reliability

Electronic Signatures

Indian IT Act is technology-neutral and can cover signatures based on various technologies and methods, however, such technologies and the manner in which these technologies are to be used is to be prescribed by the Central Government

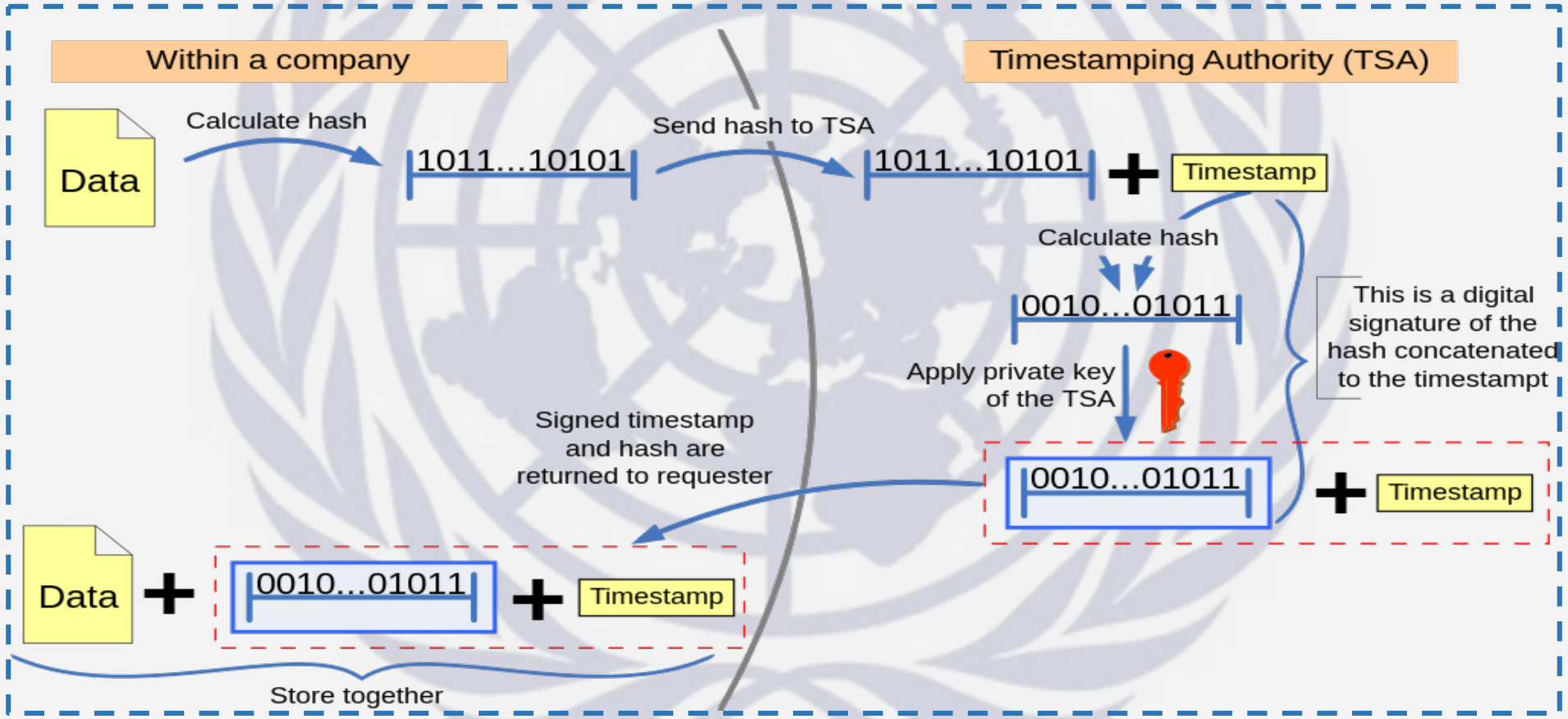
Foreign Certificates

CCA can also recognize Foreign Certifying Authorities operating under a PKI Regulator, if:-

- The level of reliability of PKI environment of the country is at least equal that of India.
- The Controller (CCA) enters into a MoU with the PKI Regulator for Mutual Recognition of CAs.
- The Controller ,with previous approval of the Central Government, publishes the list of recognised CAs and the CA is included in such list.

Foreign CAs not operating under a PKI Regulator need to apply to the CCA for recognition

Trusted Time-stamping



Legally valid proof of existence of a document at a particular time.
User submits hash of the document. TSA adds a Timestamp and signs it.
Privacy is maintained as only the hash of the document is made available to TSA(CA).

THANK YOU