TATA CONSULTANCY SERVICES

TATA

Presentation on
Security and Trust for e-Procurement

Global Consulting Practice –
Information Risk Management

Experience certainty.

IT Services
Business Solutions
Outsourcing

e-Procurement – Security and Trust

Agenda

- Introduction to Information Security – Context
- Security Framework (ISO 27001) – Definition and Approach
- Security and Trust – Need
- TCS Certifying Authority (TCS-CA) – Sub- Certifying Authority (Sub-CA)
- Workflow for DSC Issuance and management
- Roles & Responsibilities
- Case Profile

e-Procurement – Security and Trust

Agenda

- Introduction to Information Security – Context
- Security Framework (ISO 27001) – Definition and Approach
- Security and Trust – Need
- TCS Certifying Authority (TCS-CA) – Sub- Certifying Authority (Sub-CA)
- Workflow for DSC Issuance and management
- Roles & Responsibilities
- Case Profile

What is security?

- Protecting the system from viruses and attacks by intruders?
- Firewalls and Intrusion Detection Systems (IDS)?
- Protection of data being transacted?
- No single definition – requires context

Our context is application security

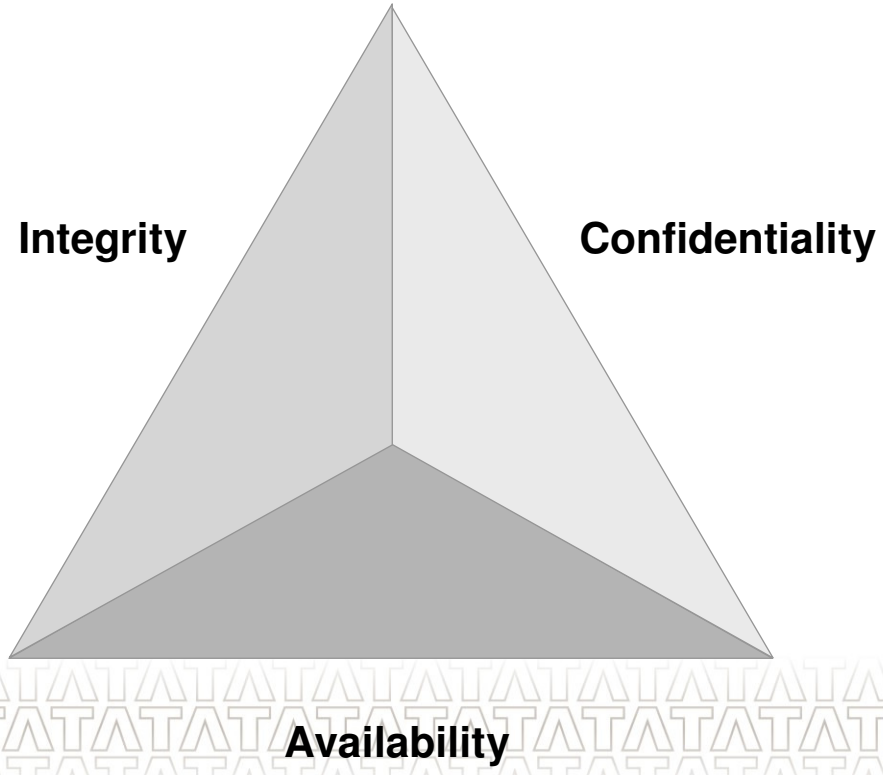
Information Security

Components

"Information is an ***asset*** which, like other important business assets, has ***value*** to an organization and consequently needs to be ***suitably protected.***"

- ISO IEC 17799

- **Privacy and Confidentiality:** protecting sensitive information from unauthorized disclosure
- **Integrity:** safeguarding the accuracy and completeness of information/data
- **Availability:** ensuring that information and associated services are available to users when required



e-Procurement – Security and Trust

Agenda

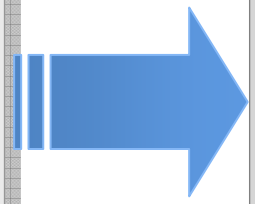
- Introduction to Information Security – Context
- Security Framework (ISO 27001) – Definition and Approach
- Introduction to Security and Trust – Need
- TCS Certifying Authority (TCS-CA) – Sub- Certifying Authority (Sub-CA)
- Workflow for DSC Issuance and management
- Roles & Responsibilities
- Case Profile

Information Security

Global Standard

BS7799

- Developed by the Department of Trade and Industry (DTI) in cooperation with British Standards Institute (BSI).
- Code of practice for Information Security management accepted as a British standard in 1995 as BS7799 (BS7799-1:1995)
- Second part of the standard accepted a few years later as BS7799-2:1998 (10 Domains, 127 Controls)
- BS 7799-2 include PDCA (Plan-Do-Check-Act) Cycle



ISO IEC 27001

- ISO 27001, the replacement for BS7799-2 (11 domains,133 Key controls)
- Its an "Information Security Management Specification With Guidance for Use".
- Basic objective to help establish & maintain an effective ISMS, using a continual improvement approach
- Use of PDCA
- Published in October 2005

Information Security

BSI Transition Statement

- Organizations can choose between BS 7799:2002 part 2 or ISO/IEC 27001:2005 till ***23 July 2006***
- From 23 July 2006 organizations will be assessed to the ***new international standard ISO/IEC 27001:2005***.
- All certificates must be transitioned to ISO/IEC 27001:2005 by the end of the 18 month transition period and any non-conformity must be cleared, which is by ***23 July 2007***.

BS 7799:2002 part 2 will no longer be valid After 23 July 2007

ISO 27001 Standard

What is it?

ISO 27001 – *Information Security Management Systems – Requirements:*

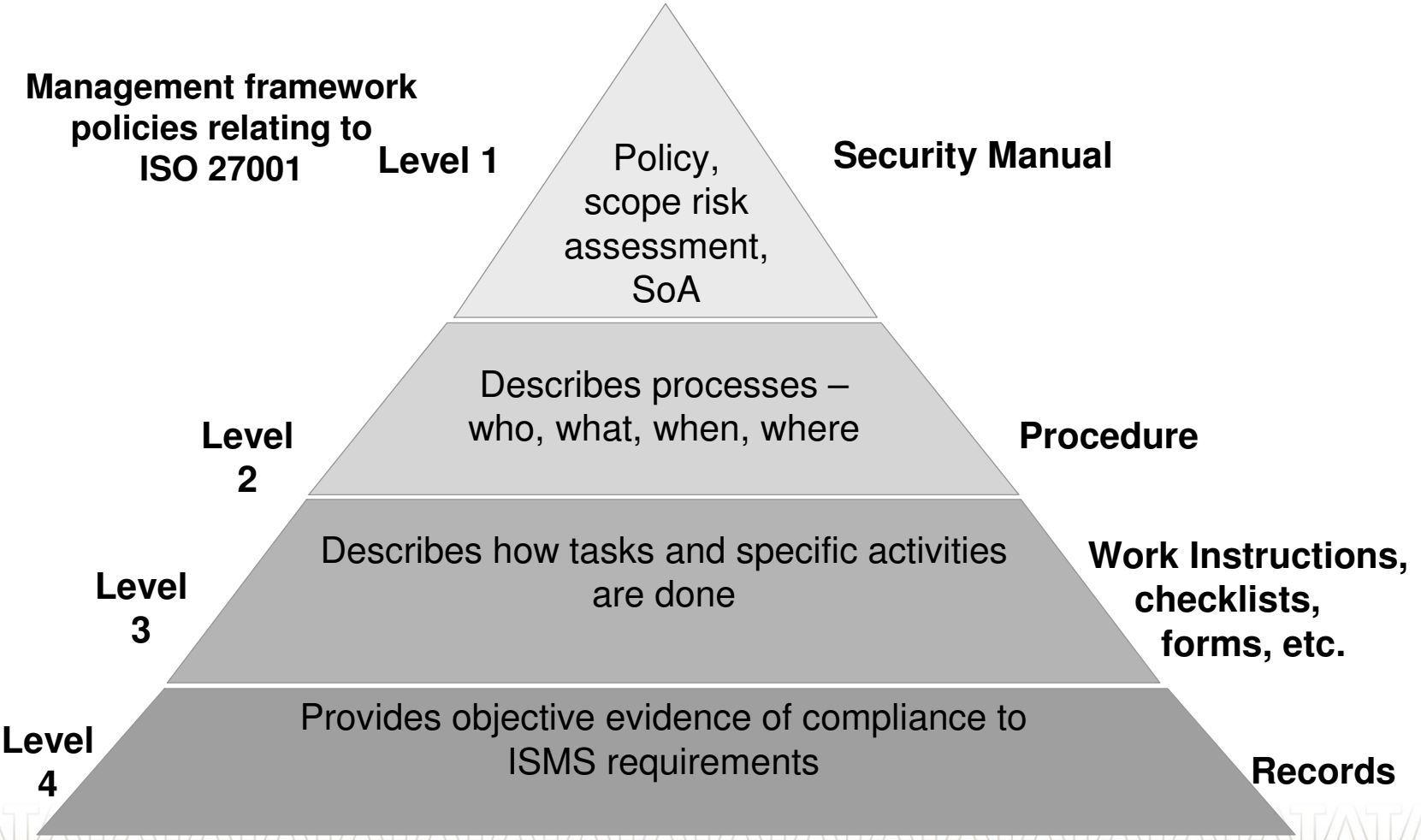
- A standard specification for Information Security Management Systems (ISMS), which is the process by which Senior Management can control their security, minimizing the residual business risk and ensuring that security continues to fulfill corporate, customer and legal requirements
- The means an organization is certified to a quality system of implementing best practice security controls (i.e., ISO 17799)
- Organized around a "Plan-Do-Check-Act" cycle for ensuring continuous review and improvement
- Based on the original British Standard BS 7799-2
- Aligned with ISO 9000 and 14000
- Anticipated to be the de facto international security certification

ISO 27001 is NOT:

- A mandate for ALL the controls in ISO 17799
- Prescriptive in the procedures to follow to ensure compliance (that is, it tells you the "What", but not the "How")

ISO 27001

Documentation



ISO 27001 Standard

The Future

ISO 27000 series has been reserved for information security standards

The following ISO 27000-series standards are already planned:

- **IS0 27000** - vocabulary and definitions (terminology for all of these standards).
- **ISO 27001** - the main Information Security Management System requirements standard (specification), currently known as BS 7799:Part 2, against which organizations will be certified. The final draft of ISO 27001 was published at the start of July.
- **ISO 27002 -** currently known as ISO 17799 - this is the Code of Practice describing a comprehensive set of information security control objectives and outlines a menu of best-practice security controls. The 2005 version of ISO 17799 was published in June and will probably transition to #27002 in 2007.
- **ISO 27003** - will contain implementation guidance.
- **ISO 27004** - will be a new Information Security Management Metrics and Measurement standard to help measure the effectiveness of information security management system implementations.
- **ISO 27005** - will be a new Information Security Risk Management standard to replace BS 7799:Part 3.

This information is unofficial at present: the details may well change when the ISO 27000-series standards are issued by ISO.

ISO 27001 Compliance

Benefits

ISO 27001 Compliance

PDCA Model applied to ISMS

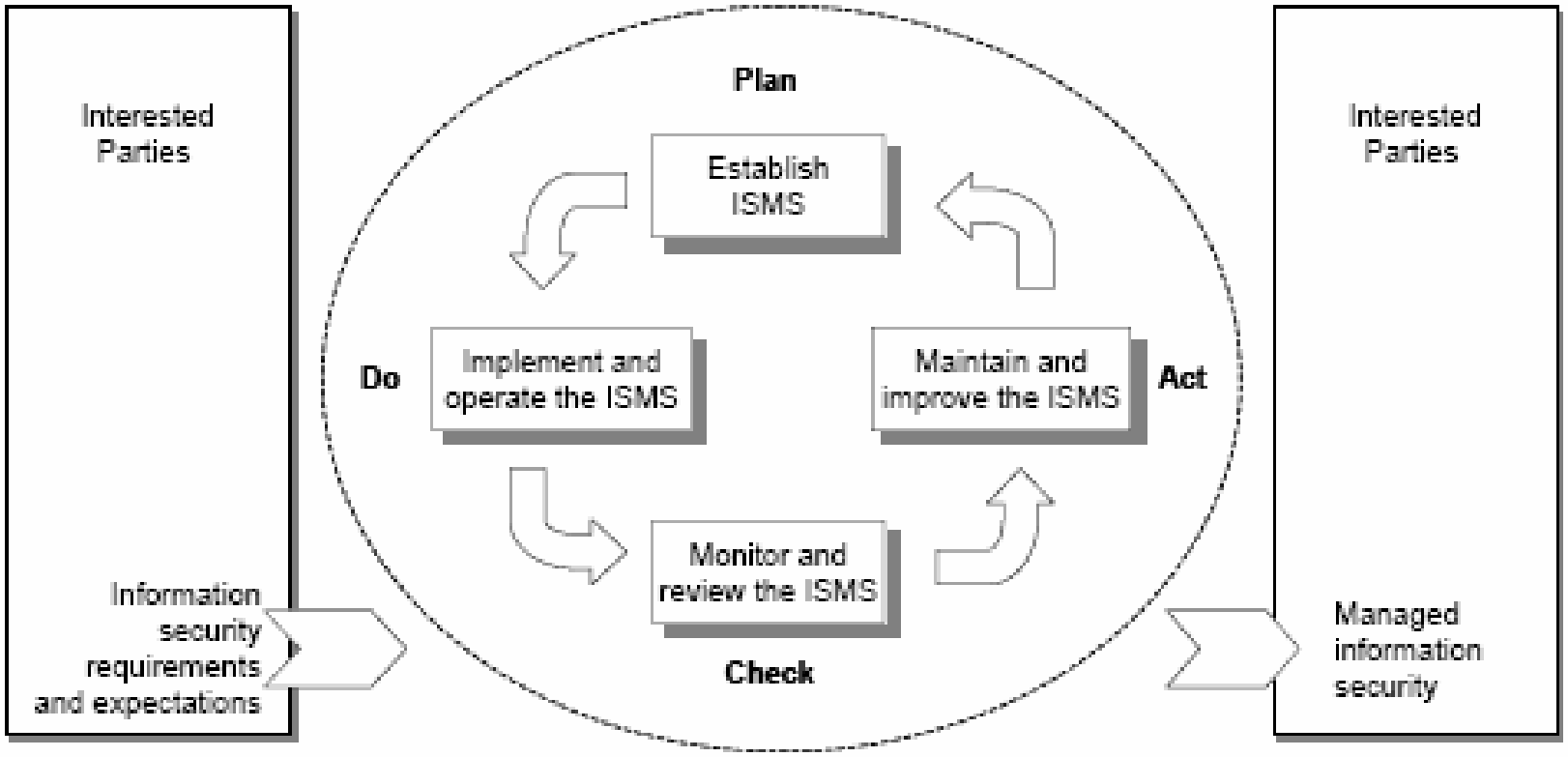
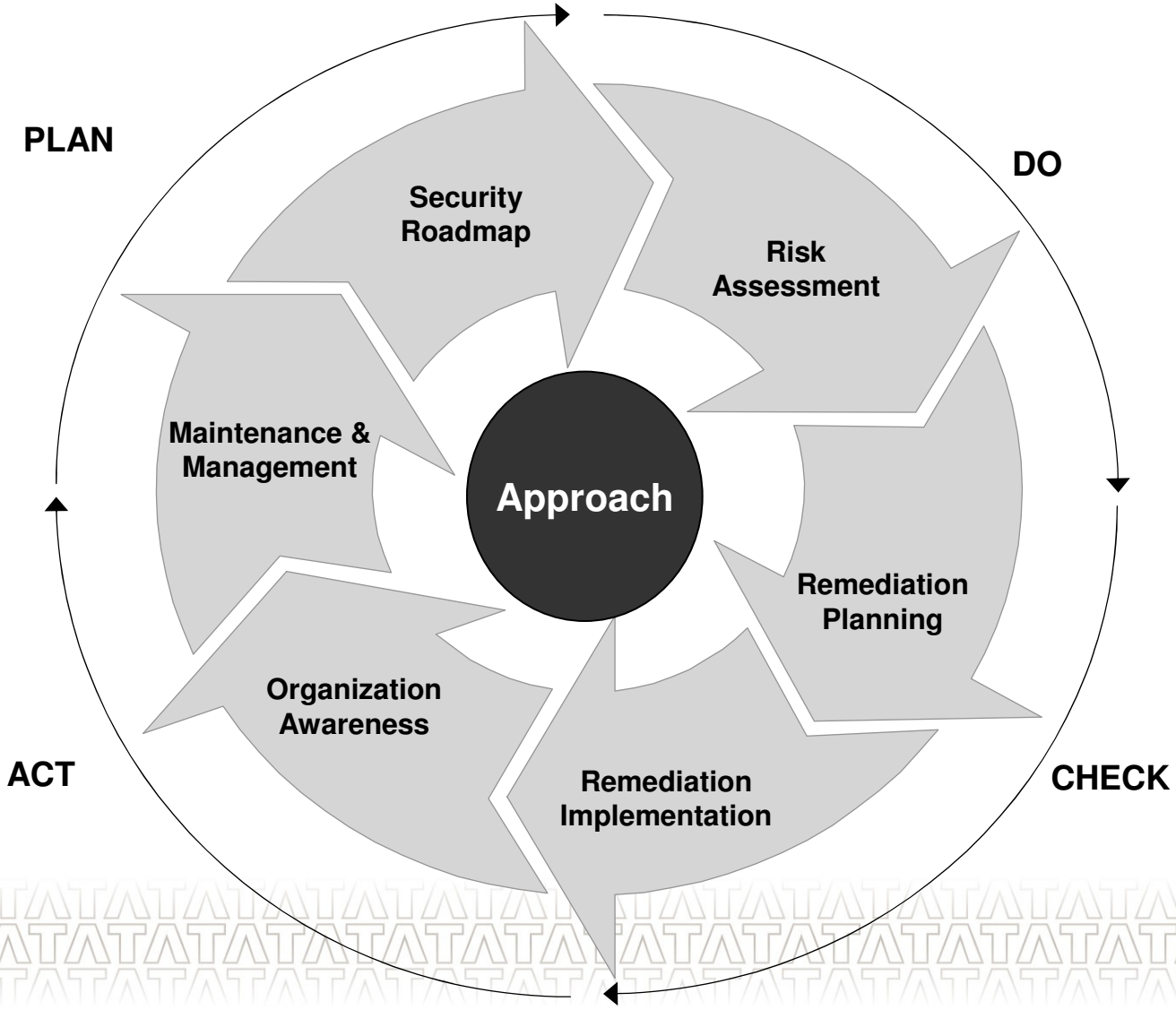


Figure 1 — PDCA model applied to ISMS processes

Source: ISO IEC 27001

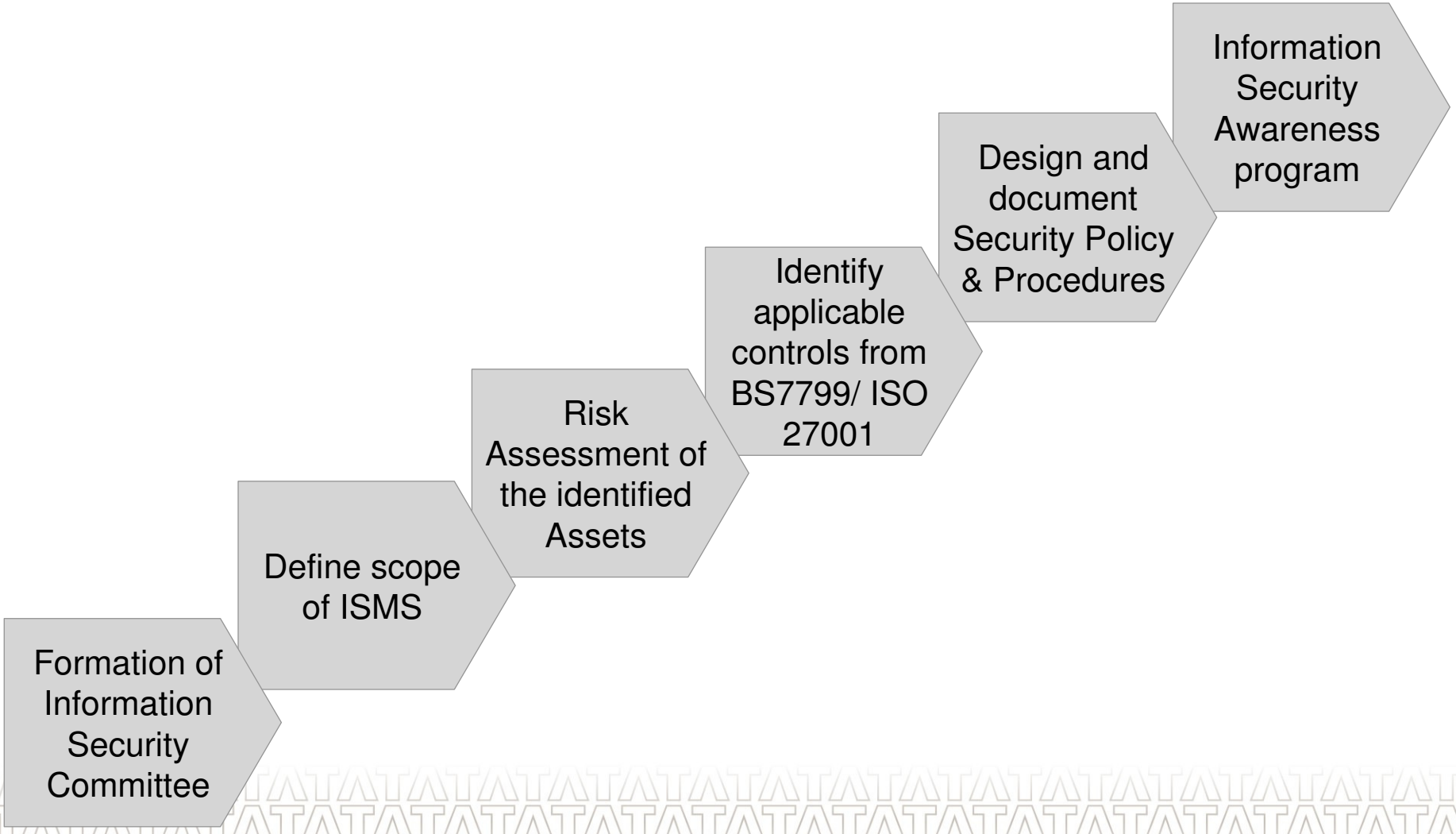
ISO 27001 Approach

Road to Maturity



ISO 27001 Approach

Compliance

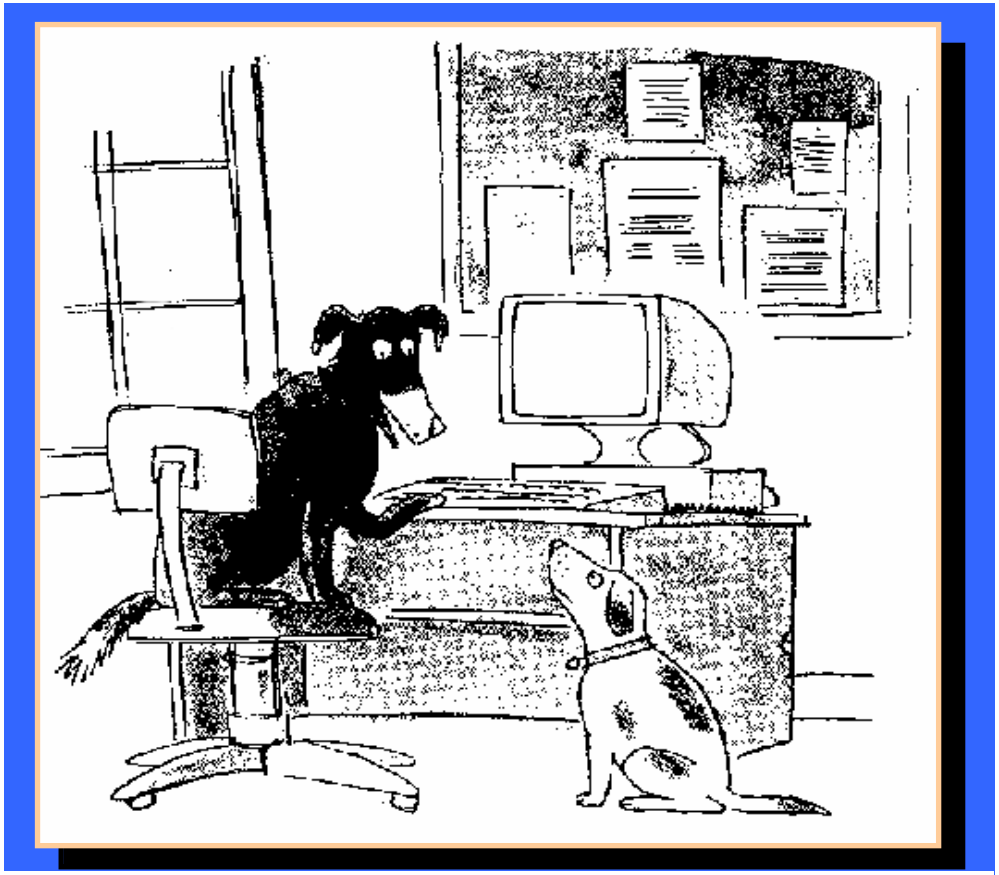


e-Procurement – Security and Trust

Agenda

- Introduction to Information Security – Context
- Security Framework (ISO 27001) – Definition and Approach
- Security and Trust – Need
- TCS Certifying Authority (CA) – Sub- Certifying Authority (Sub-CA)
- Workflow for DSC Issuance and management
- Roles & Responsibilities
- Case Profile

The issues: Security and Trust



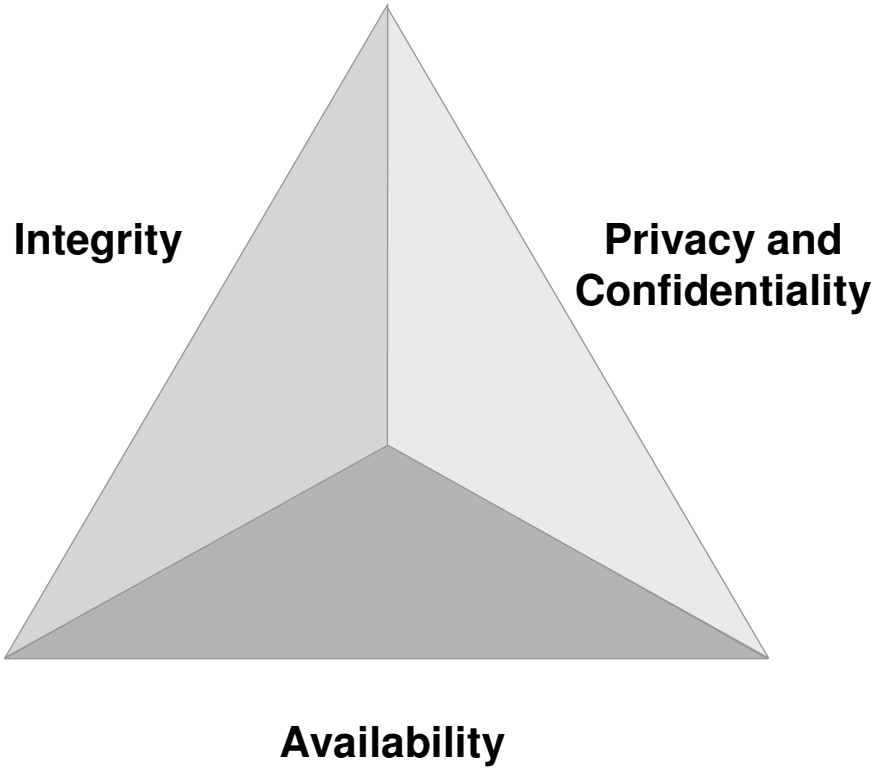
“ On the Internet, no one knows, Who I am ”

- Who is at the other end of the wire?
- Who can see the data?
- Was anything altered in passing?
- When was it executed?
- Who signed the document?

- *It’s all about trust*
- *The key issue in an e-Procurement/ Web based environment is security and trust*
- *Lack of security results in lack of trustworthiness*

Information Security
Missing Component

- **Privacy and Confidentiality**: protecting sensitive information from unauthorized disclosure
- **Integrity**: safeguarding the accuracy and completeness of information/data
- **Availability**: ensuring that information and associated services are available to users when required
- **Non-Repudiation and Authenticity**



Introduction to Security and Trust - Need

e-Procurement requires PAIN

P rivacy and Confidentiality
- *Data can be only be viewed by the target part*

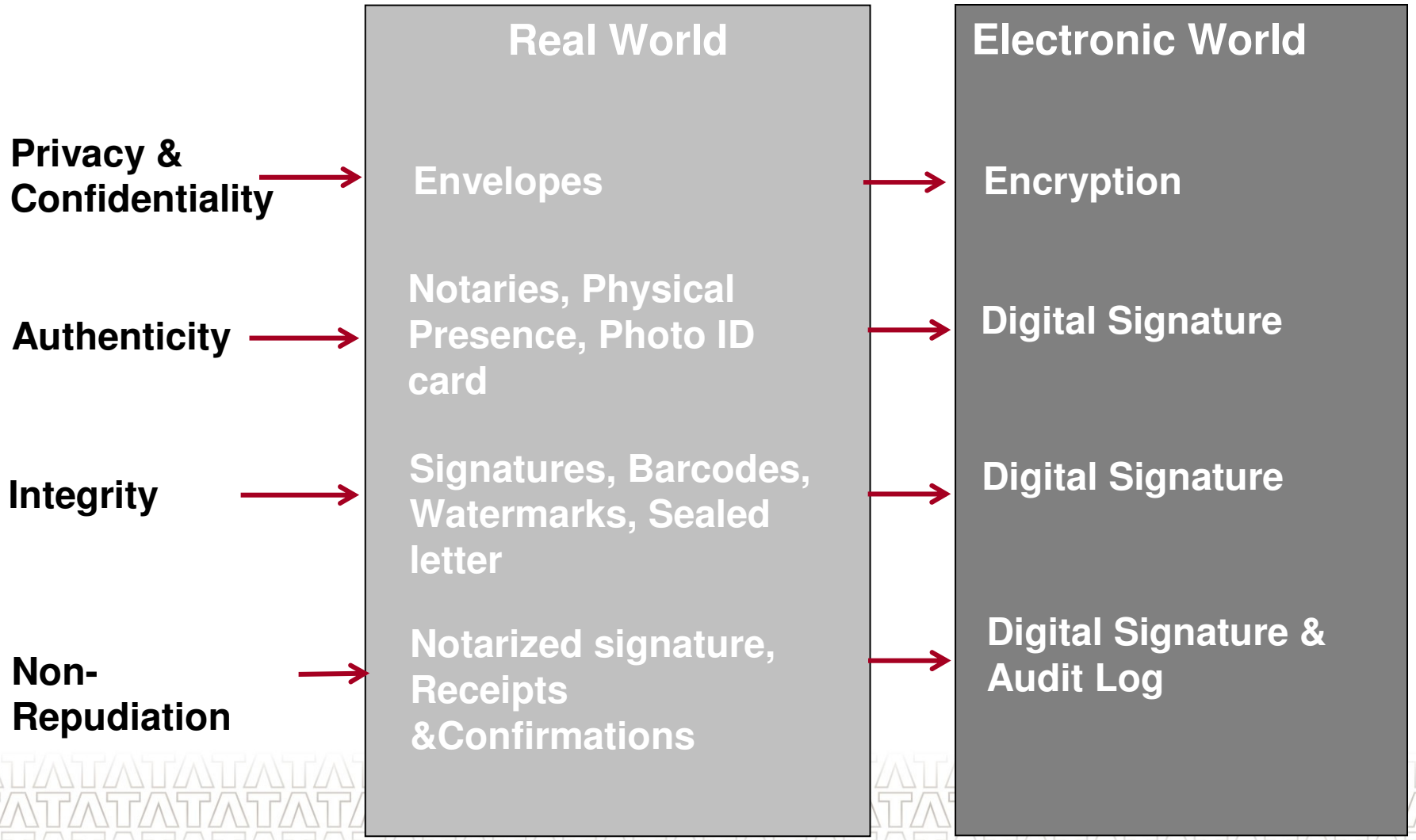
A uthentication
- *Each party is who claims to be*

I ntegrity
- *The data has not been changed*

N on-Repudiation
- *No party can deny the involvement in a transaction*

Introduction to Security and Trust - Need

Traditional Paper based solutions



Introduction to Security and Trust - Need

Disadvantages of existing system – Electronic systems without PKI

- Paper-based processes are **slow** and **expensive**
  - Time taken for the documents to reach through courier / postal service
  - Time taken in processing the documents manually for approval
  - Cost of the paper documents
  - Cost of the courier / postal services

- Paper-based systems lack
  - ***User Authentication*** – as the hand-written signatures can easily be forged
  - ***Data Integrity*** – as the information can easily be altered in transit
  - ***Confidentiality*** – as the information can easily be read in transit

- Paper documents may get lost or misplaced

- Large Physical storage place is required to keep the paper documents

- Retrieval of the paper documents is a cumbersome process

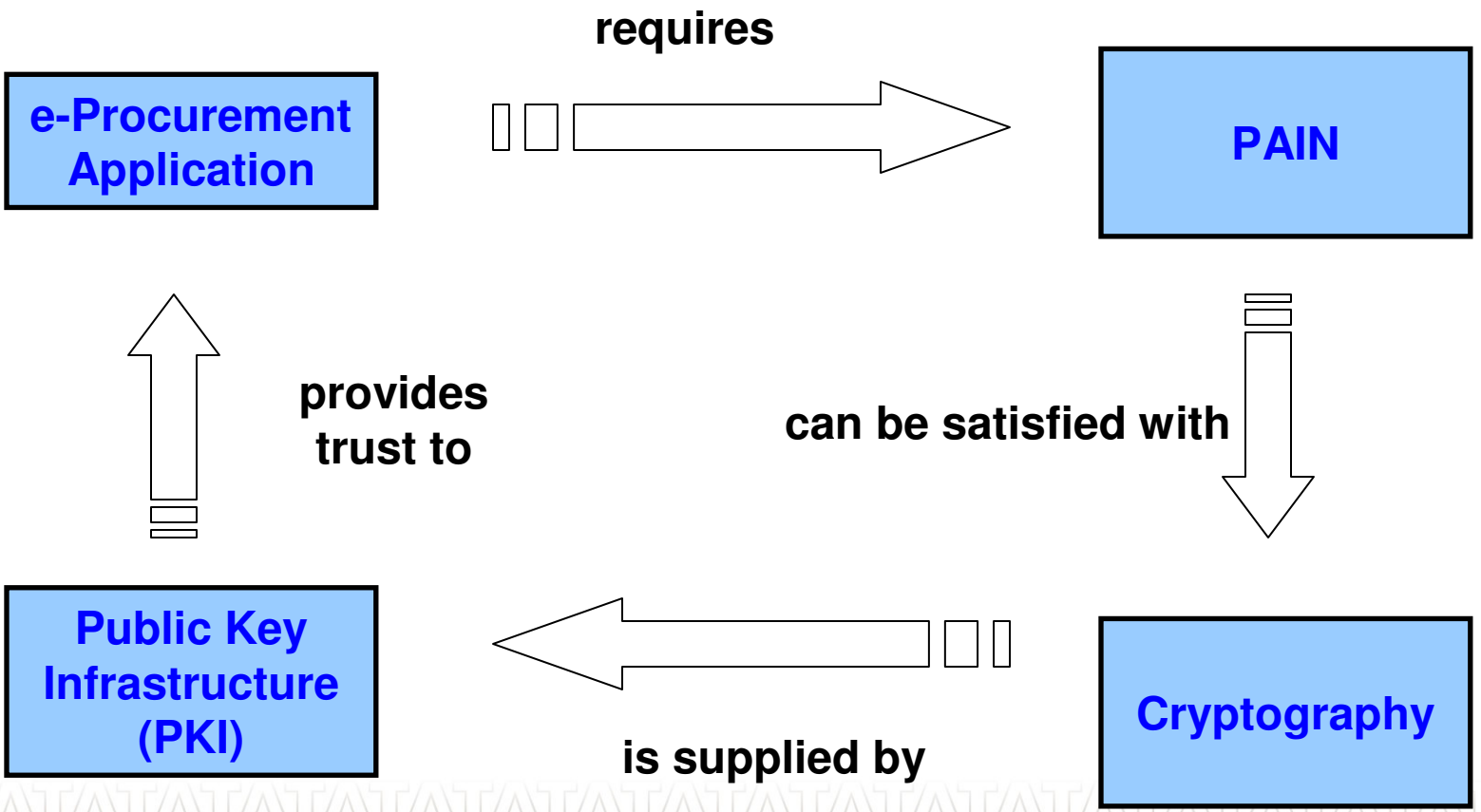
Introduction to Security and Trust - Need

Measures to improve - Using Digital Signatures

- The transactions can be done electronically in a click of a button.
- The details are sent across instantaneously once the information is submitted. Hence there is **no time delay** in communication.
- The processing & approval is done electronically at each level and hence takes less time
- All the official communications can be sent through email, which is fast and cost-effective
- Ensures **PAIN**
- Archival of information is possible. Also retrieval of the archived data is easier
- No physical storage is required for the documents
- **Legal sanctity** in the court of law

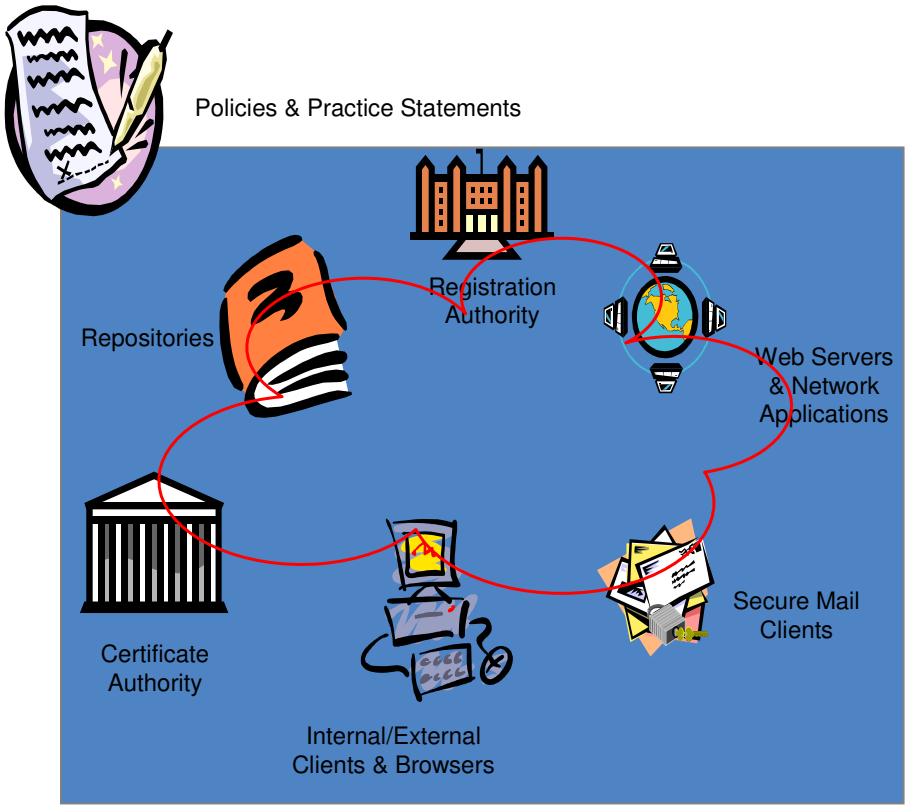
Public Key Infrastructure (PKI)

The solution for e-Procurement trust requirements



Introduction to Security and Trust – PKI

combating R.I.S.K



- PKI = Public Key Infrastructure
- It's the capability to issue, manage, distribute and use Digital Certificates
- It includes:
  - Certifying Authorities (CA)
  - Registration Authorities (RA)
  - Security Policies
  - Certificate Distribution System
  - PKI-enabled Applications
  - Subscribers / Relying Parties

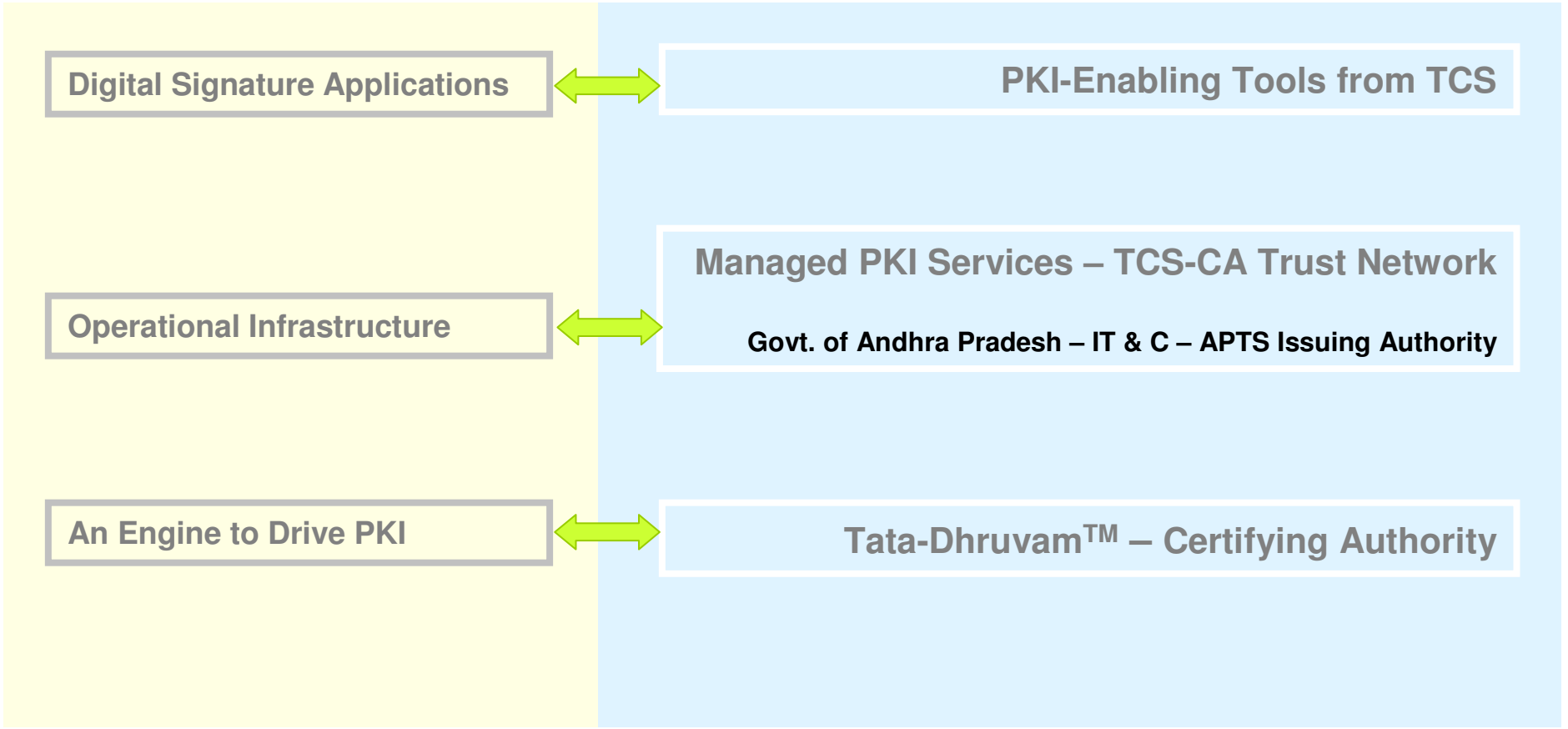
Introduction to Security and Trust – PKI

what it takes

- A PKI Engine
  - To drive the digital certificate lifecycle
- Operational Infrastructure
  - For managing client/user applications for digital certificates
- PKI-enabling Tools
  - For leveraging the benefits of PKI

Introduction to Security and Trust – Problem x Solution

how the cookie crumbles



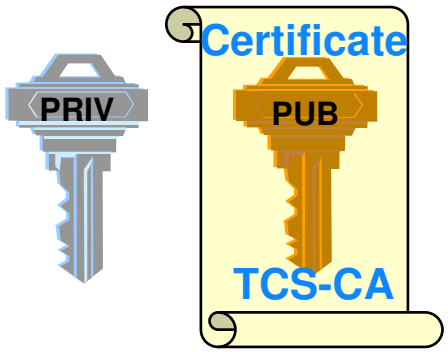
Introduction to Security and Trust

PKI enabling

- Two-factor Authentication
  - Digital Certificate Based Authentication with Smart Card/ USB Token
- Web-based Signing/ Encryption
  - Online Form Signing/ Encryption
- Desktop Signing/ Encryption
- Messaging/ Mailing
  - Lotus Notes mails
  - Lotus iNotes Web Access

Introduction to Security and Trust – DSC

Cryptography basics



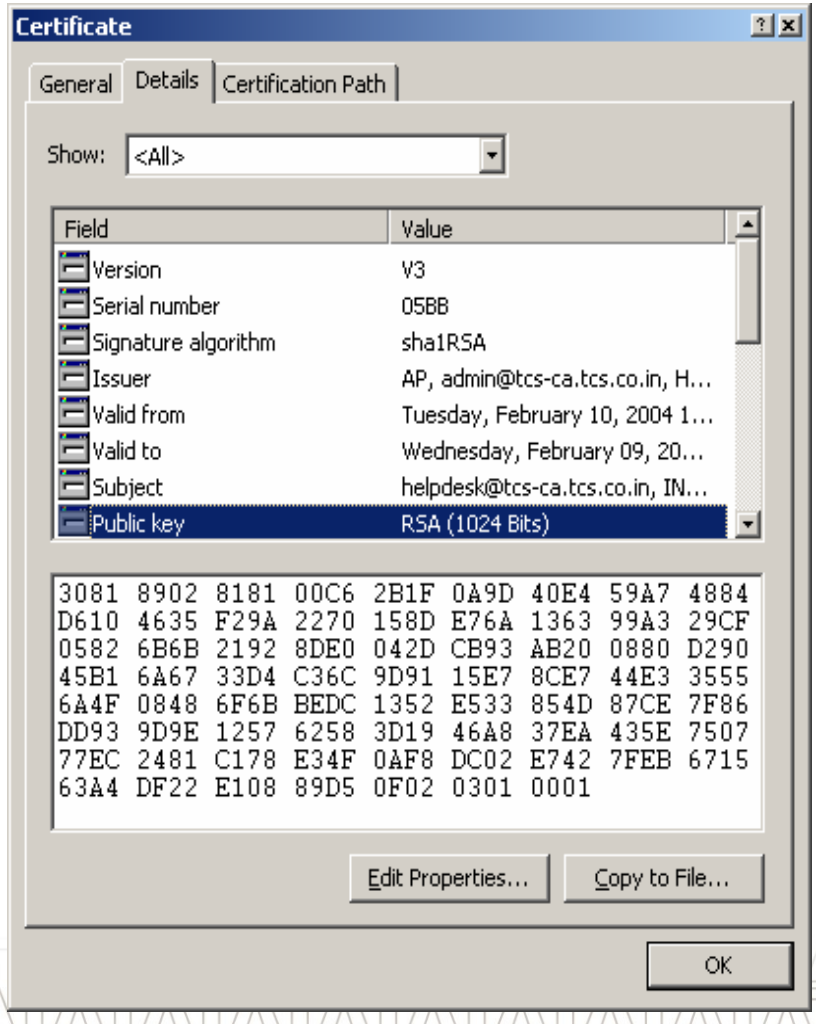
- Based on the science of **Public Key cryptography**
- Uses **Public** and **Private** "**key pairs**", and Digital Certificate

- What is a **Digital Signature Certificate (DSC)**?
  - A Digital Certificate is a digitally signed statement issued by a trusted party, such as Tata Consultancy Services-Certifying Authority (TCS-CA), that binds the identity of a person or entity to a specific public key.
  - Trust inherits from a Certifying Authority

- What does a Digital Signature Certificate contain?
  - Details about the user
    - X.500 distinguished name (DN)
    - E-mail address
  - Details about the certificate issuer (called the Certifying Authority, or CA)
  - User's public key
  - Validity period
  - A digest of the certificate contents
  - The certificate digest is signed by the CA

Introduction to Security and Trust – DSC

How does a DSC look like?



Introduction to Security and Trust – DSC

Digital Authentication & Digital Signatures

- What is a **Handwritten Signature**?
  - A signature is a mark made with the present intention to authenticate a writing

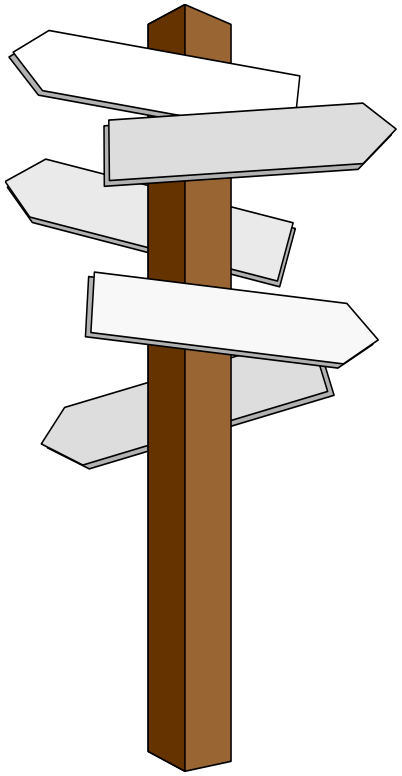
- What is a **Digital Signature**?
  - A message is sealed and signed by the sender of the message
  - A unique code that binds the signer to a specific message.
    - Created by a specific entity (i.e. a person)
    - Can't be forged
  - Only someone possessing the private key could have created the digital signature
  - Anyone with access to the corresponding public key can verify the digital signature
  - Any modification of the signed data (even changing only a single bit in a large file) invalidates the digital signature

- Digital signatures provides:
  - Authentication/ Identification (**Who**)
  - Message Integrity (**What**)
  - Non Repudiation/Non Denial (**Legal Binding**)

Introduction to Security and Trust – DSC

Usage Scenarios

- Any application or process which presently **uses ink** and **paper signature**
- Any business process which requires **authentication** and/ or **privacy**
  - Order processing, e-Procurement, e-Filing, Electronic Tendering, etc
- Any process which requires **access control** or **identification**
  - Web site log in (eliminate user names/ passwords)



Introduction to Security and Trust - DSC

Enablers

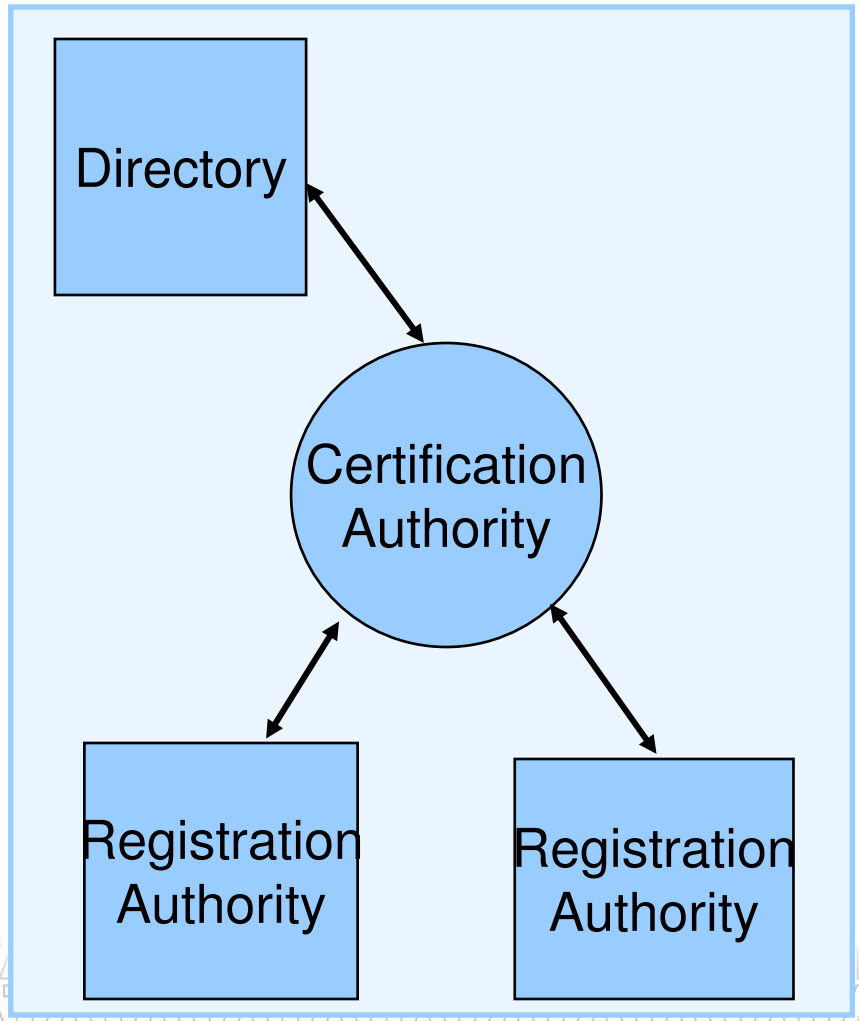
- **Legal framework** - IT Act of India, 2000
  - Enforceable Legal and validity of Digital Signatures at par with Hand written signatures
- **Licensed Third Party Trusted Authorities** - Certifying Authorities
  - A Trusted Third Party (TTP) is an independent enterprise that provides reliability on, and confidence in, the truth and worth of electronic business transactions.
  - For issuance and management of Digital Signature Service (Digital Certificates)

e-Procurement – Security and Trust

Agenda

- Introduction to Information Security – Context
- Security Framework (ISO 27001) – Definition and Approach
- Security and Trust – Need
- TCS Certifying Authority (TCS-CA) – Sub- Certifying Authority (Sub-CA)
- Workflow for DSC Issuance and management
- Roles & Responsibilities
- Case Profile

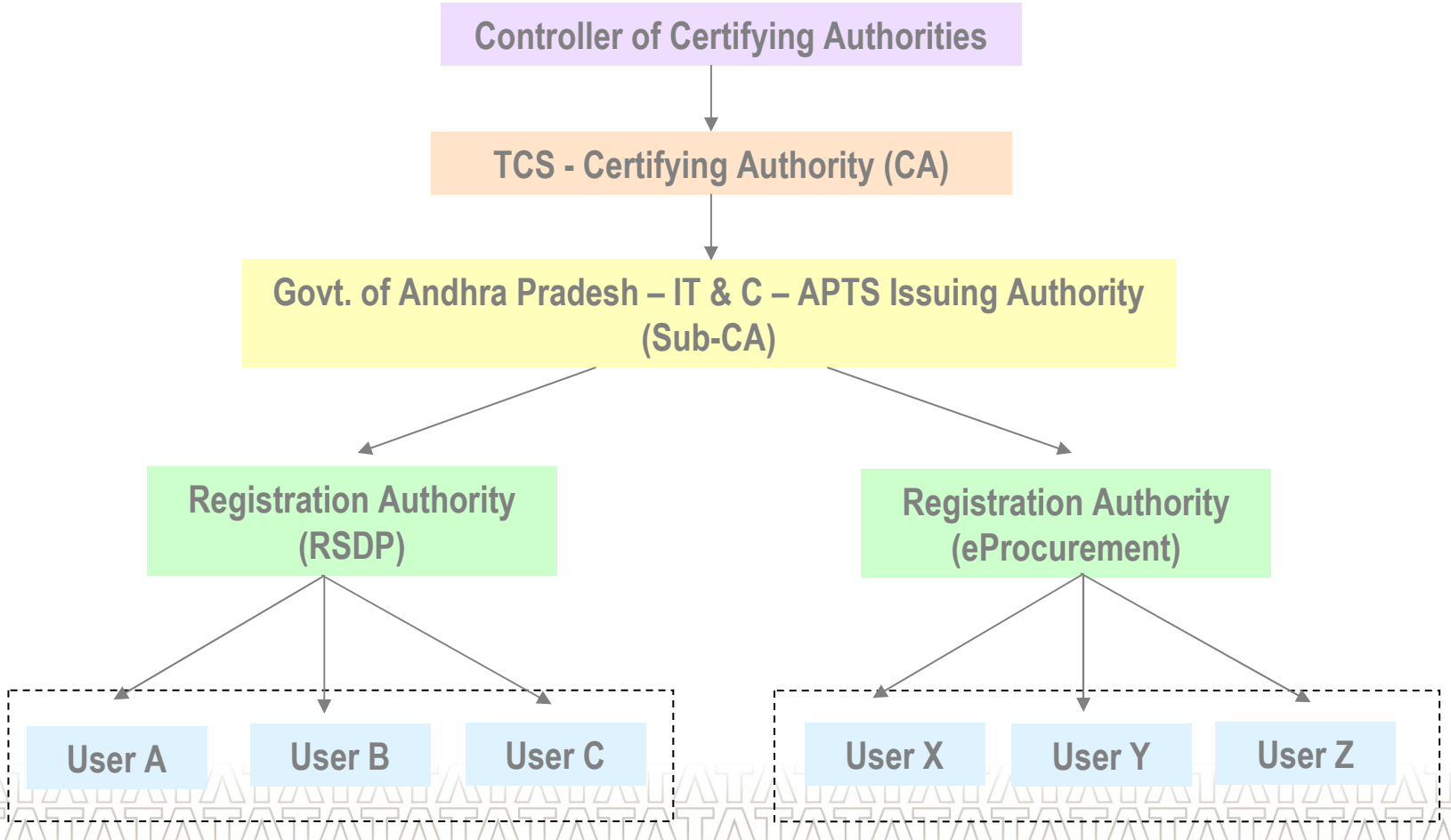
The Components of Public Key Infrastructure (PKI)



- **Certification Authority** (CA): *An entity or service that issues certificates. Acts as a guarantor of the binding between the subject public key and the subject identity information contained within the certificates it issues and manages.*
- **Registration Authority** (RA)/ Sub-CA: *An entity or service that registers users, validates its identity and is trusted by the Certification Authority.*
- **Certificate Repository/Directory**: *A public directory/database in which certificates and their status (e.g. validity) is published.*

TCS - Certifying Authority (TCS-CA)

Sub-CA – Operational Infrastructure



The components: Analogies

In a PKI	Issuance of a passport
Certification Authority	➔The Indian state
Sub-CA/ Registration Authority	➔Passport registration office
Directory	➔List of all passports
Certificates	➔Passport

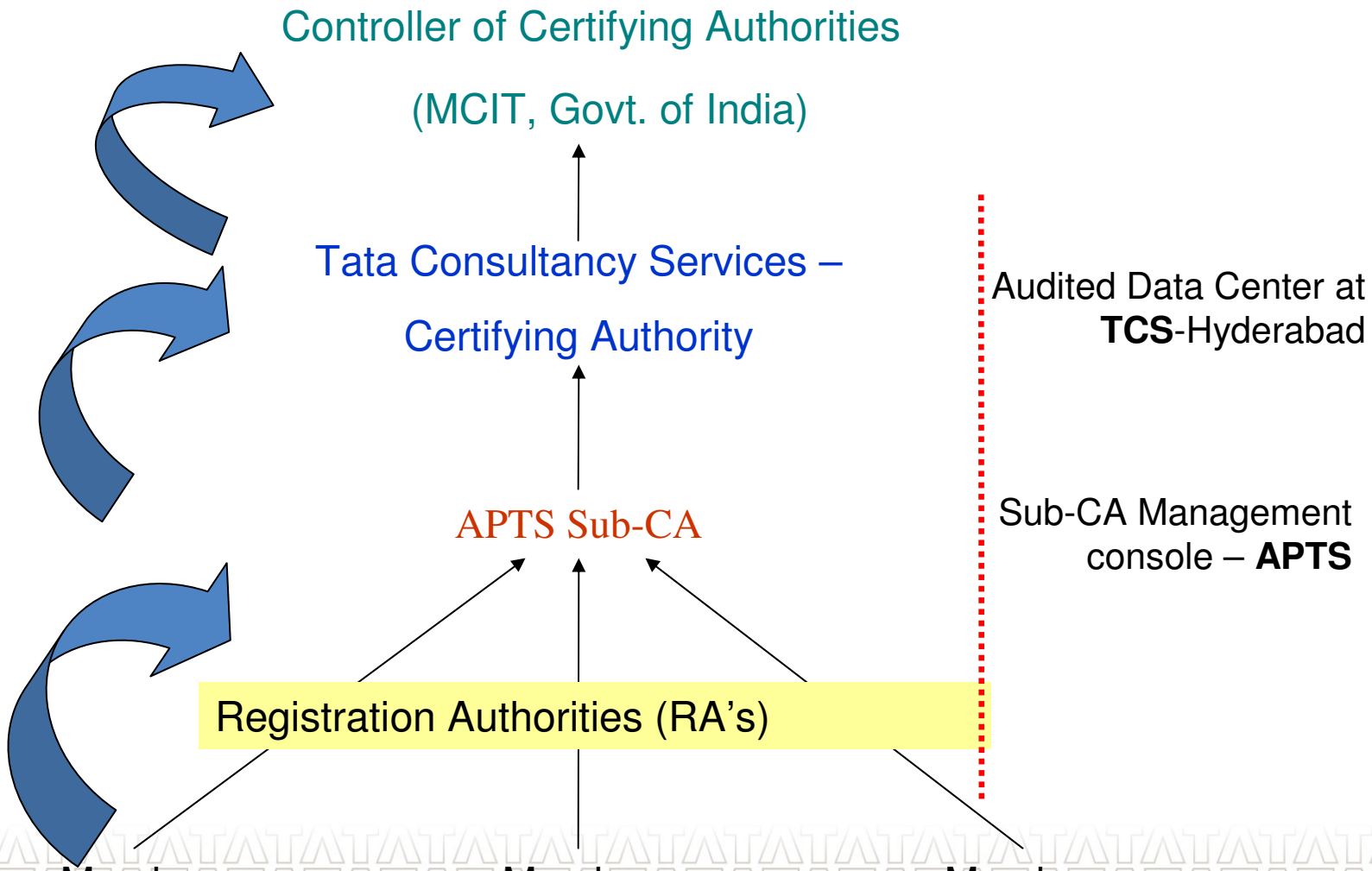
Managed PKI Services

Sub-CA

- TCS-CA Managed PKI Services : Subordinate – Certifying Authority (Sub-CA) solution
- APTS : Sub-CA to TCS-CA
- APTS issues Digital Certificates to its
  - members/ employees/ partners/ affiliates throughout the enterprise
  - without investing on Physical/ Hardware/ Software infrastructure.
- Outsourced Model
- Legally valid Digital Certificates as per the Indian IT Act, 2000
- Exercise full control over Certificate Issuance
- Closed user group
- Cost benefit

Managed PKI Services

Sub-CA - Trust Hierarchy



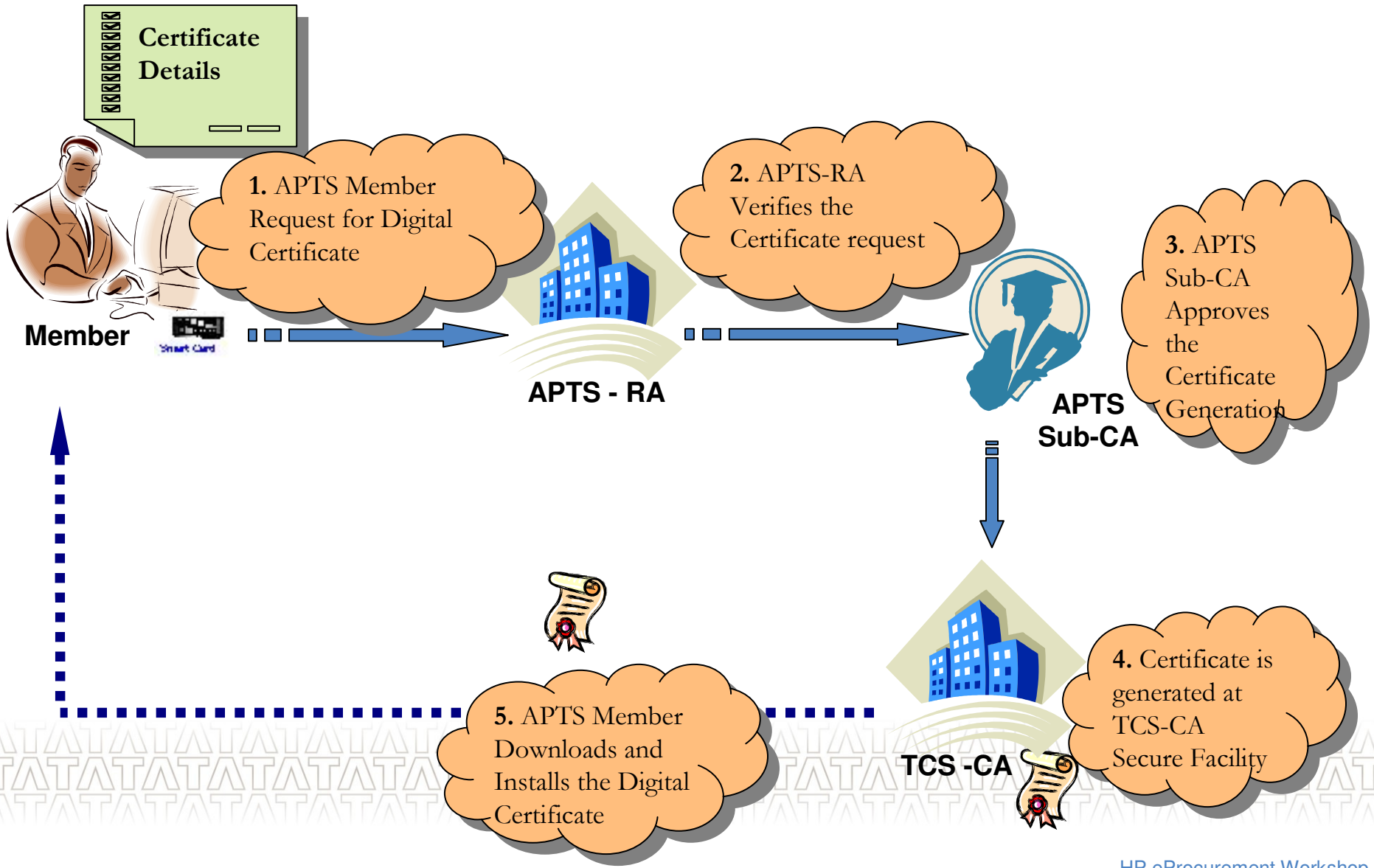
e-Procurement – Security and Trust

Agenda

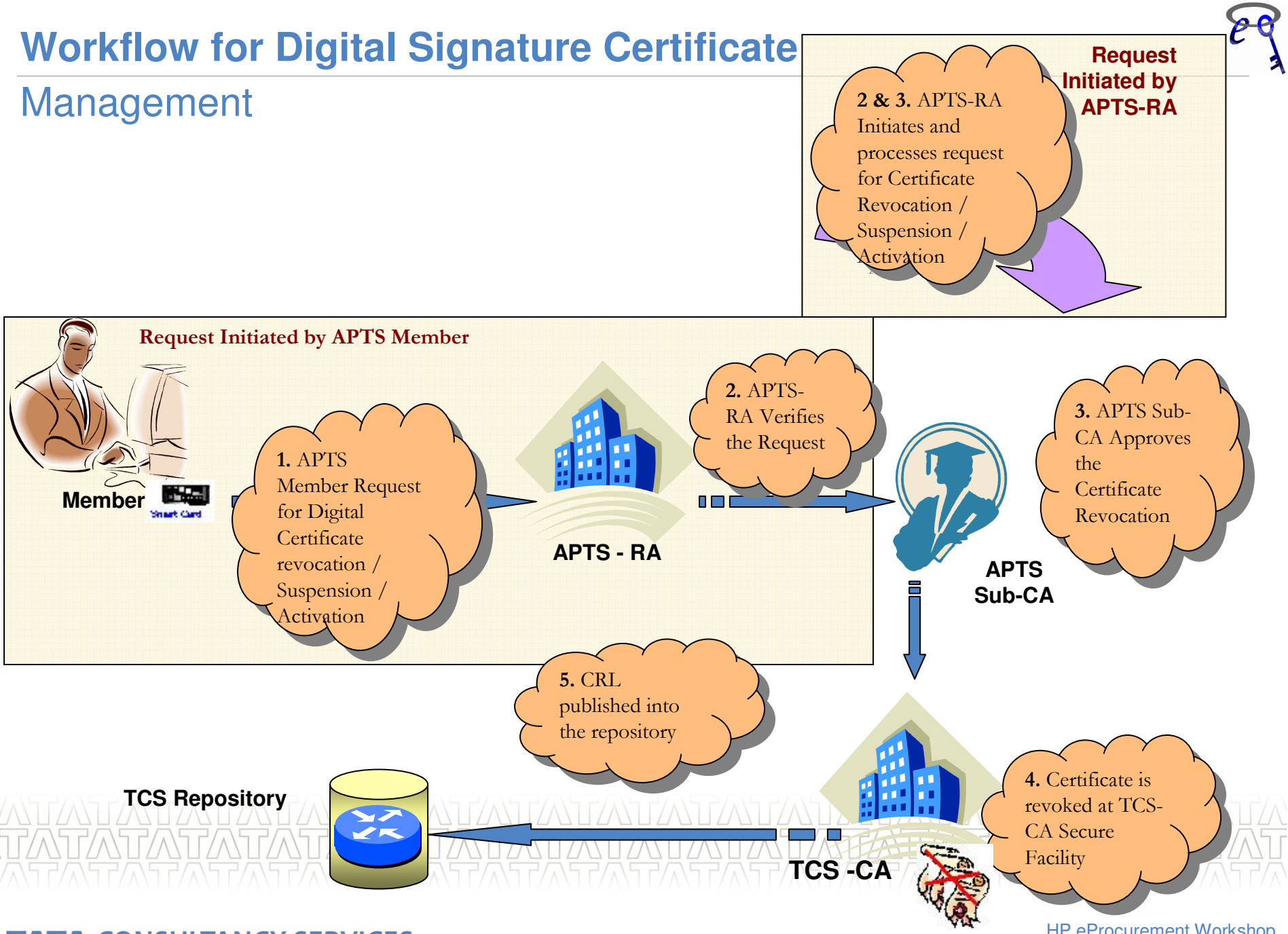
- Introduction to Information Security – Context
- Security Framework (ISO 27001) – Definition and Approach
- Security and Trust – Need
- TCS Certifying Authority (TCS-CA) – Sub- Certifying Authority (Sub-CA)
- Workflow for DSC Issuance and management
- Roles & Responsibilities
- Case Profile

Workflow for Digital Signature Certificate

Issuance



Workflow for Digital Signature Certificate Management



e-Procurement – Security and Trust

Agenda

- Introduction to Information Security – Context
- Security Framework (ISO 27001) – Definition and Approach
- Introduction to Security and Trust – Need
- TCS Certifying Authority (CA) – Sub- Certifying Authority (Sub-CA)
- Workflow for DSC Issuance and management
- Roles & Responsibilities
- Case Profile

Roles & Responsibilities

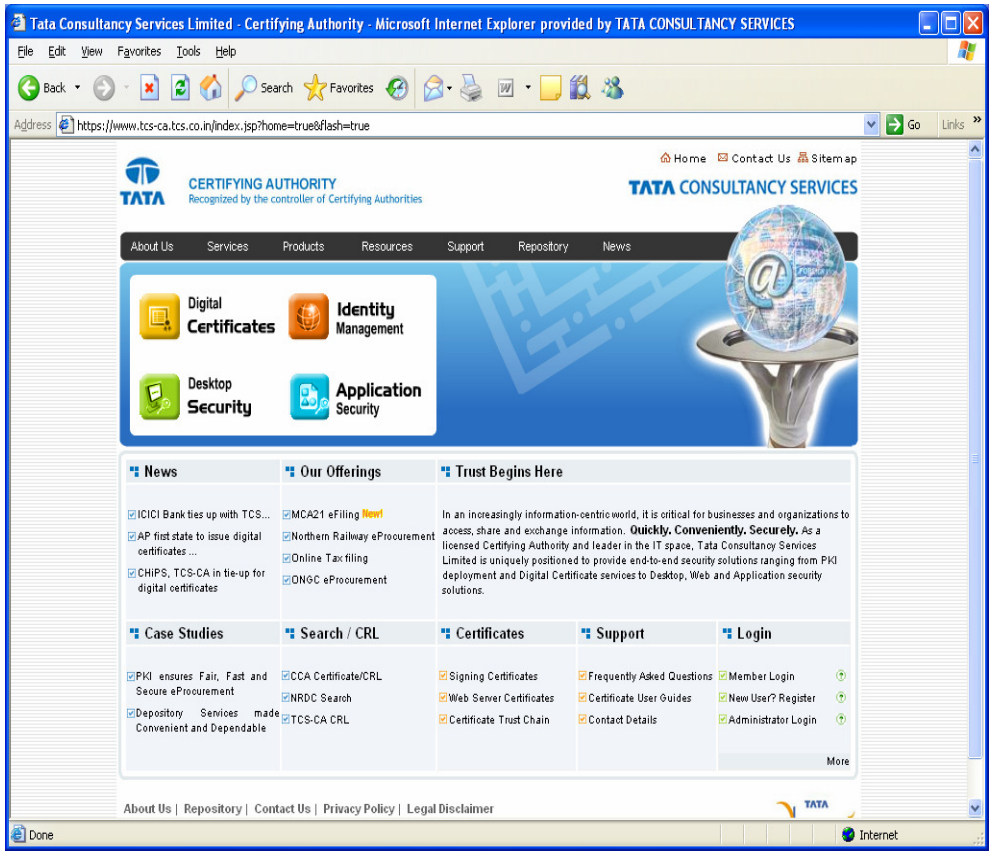
APTS Member - Request for Certificate

- Go through the Digital Certificate Registration Centre from APTS website
- Register with TCS-CA and enroll for a Digital Certificate through the APTS Digital Certificate Registration Centre
- Download the Certificate request form and submit the same to APTS-RA after filling. Also submit the validation documents as per the checklist
- Once the certificate is generated, login to the TCS-CA website through APTS Digital Certificate Registration Centre and download the certificate

Roles & Responsibilities

APTS-RA - Processing the Certificate Request

- Login to TCS-CA website (www.tcs-ca.tcs.co.in) using User ID and Certificate (installed in the USB token)
- Check for the new requests
- Collect the Certificate Request Form and validation documents from the APTS Members who has applied for the certificate
- Process the certificate online once the documents are in place



Roles & Responsibilities

APTS Sub-CA - Processing/ Approving the Certificate Request

- Login to TCS-CA website (www.tcs-ca.tcs.co.in) using User ID and Certificate (installed in the USB token)
- Check for the new requests
- Collect the Certificate Request Form and validation documents from the APTS-RA
- Process/ Approve the certificate request online
- Once the Sub-CA approves the request, the Certificate will be generated at the TCS-CA Secure facility and the same will be available for download by the APTS Members

e-Procurement – Security and Trust

Agenda

- Introduction to Information Security – Context
- Security Framework (ISO 27001) – Definition and Approach
- Introduction to Security and Trust – Need
- TCS Certifying Authority (CA) – Sub- Certifying Authority (Sub-CA)
- Workflow for DSC Issuance and management
- Roles & Responsibilities
- Case Profile

Case Profile

eProcurement – Government of Andhra Pradesh

- Requirement
  - Authenticity and non-repudiation for bid submission
  - Confidentiality of the financial data and technical documents
  - Assurance of time of bid submission
  - Legal sanctity for all the above transactions

- TCS Solution
  - Digital Signature Enabling tool – FormSigner
  - Encryption/ Decryption tool – FormCipher
  - Time Stamping/ digital Notarization tool – TATA-Saakshi
  - Managed PKI Services for issuing legally valid DSC

Case Profile

eProcurement – Government of Andhra Pradesh

Solution Workflow

- All the bidders are issued Digital Signature Certificates prior to bid submission
- For each tender, authorized officials at GoAP are identified and they are issued DSC
- Bidding Process
  - Bidder logs into GoAP eProcurement site with User ID/ DSC stored in USB token (Two factor Authentication)
  - Bidder fills-in the financial data and uploads the required documents
    - The financial data captured in HTML form and the attachments are digitally signed by the client at the client side
  - The digitally signed data comes to the eProcurement server
    - At the eProcurement site, the data is encrypted for the identified officials
    - The encrypted data is stored into the database
  - GoAP official logs into the admin module of the eProcurement site with User ID/ DSC stored in USB token (Two factor Authentication)
  - While viewing the financial data and attachment, the GoAP official inserts his/ her USB token with DSC, and the data is decrypted at the client side
  - GoAP official can also verify the signature of the data and attachments

TATA CONSULTANCY SERVICES

TATA

Thank you

Raj Kumar Singh
rajk.singh@tcs.com

Contact: TCS-CA Helpdesk
Mail: helpdesk@tcs-ca.tcs.co.in
Phone: 1800-425-1922 (Toll-free), +91-40-66673524/5
Web: www.tcs-ca.tcs.co.in / www.tcs.com

Experience certainty.

IT Services
Business Solutions
Outsourcing