

PKI and Business Issues

Agenda



- Need for a Digital Signature Certificate
- Case Studies – E-Procurement, E-Shopping
- Getting a Digital certificate
- Procedures for Getting Certificates for Members of Government Agencies
- Some Risks and Precautionary Measures

DSC - Where do you need ?



- Individuals / Members on behalf of Companies
 - E-Filing
 - Individuals, All companies, filing their IT returns online
 - E-Procurement
 - Supplier/Vendors participating in E-procurement process
 - E-Ticketing
 - Accredited agents of IATA, for booking tickets in IRCTC
 - E-Payments
 - E-Transfer – through/between banks;
 - E-Voting
 - Already adopted in some countries!
- Servers / Machines
 - E-Trading / E-Shopping
 - Web Servers hosted by Merchants

Case 1: E-Procurement

Digital Signature Certificates used
by Vendors and Issuers of a
Tender

- Benefits
 - Cartel formation, rigging, information leakages, modifications etc... can be avoided
 - Provide privacy and confidentiality to the documents within the tenders
 - Keep the information regarding vendors confidential

E-Procurement - Process



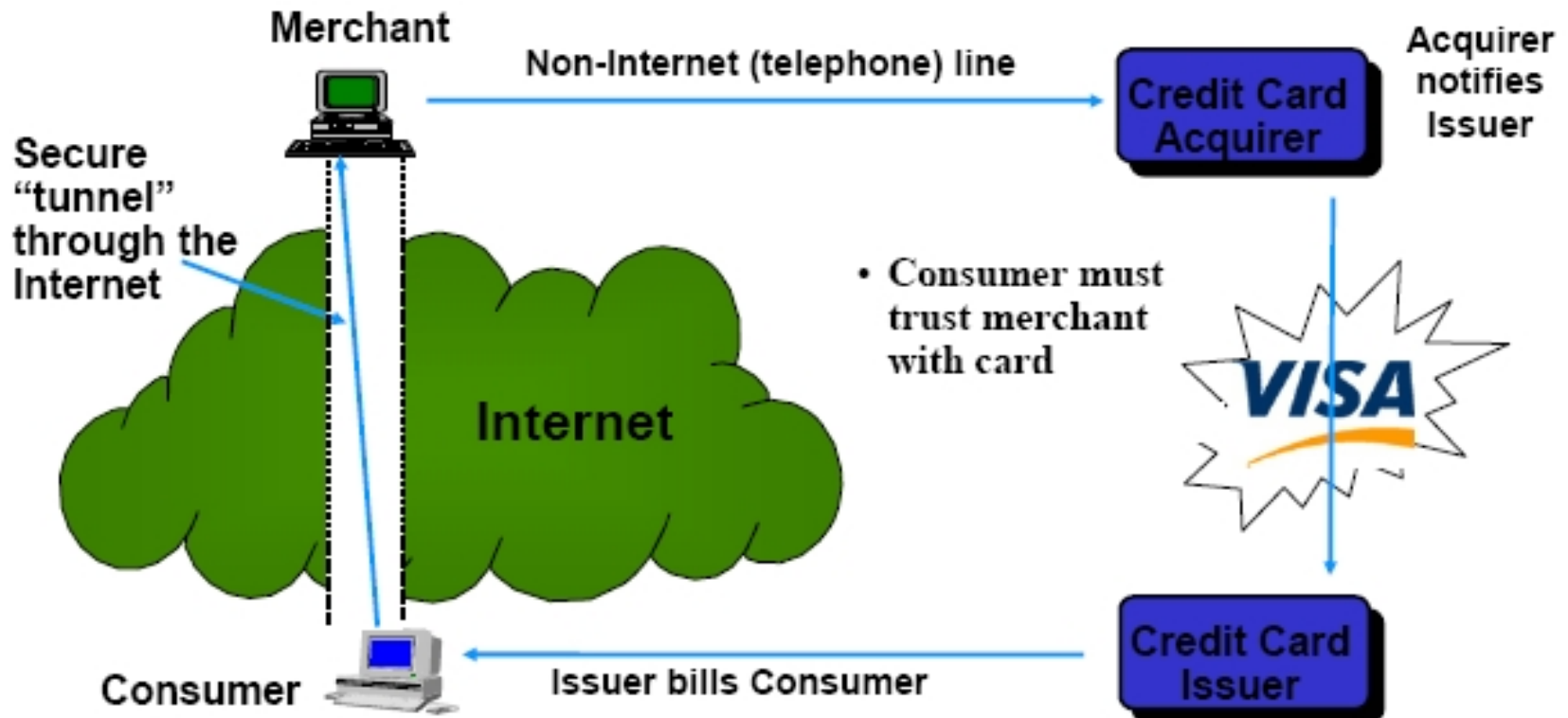
- Issuer of the Tender needs to have a Digital Signature Certificate
 - The public key of the issuer of the tender is required for the vendors
- Each vendor logs on to a online system and provides his digital certificate
- A vendor prepares and digitally signs his document
 - Vendor uses his private key to sign it
- A vendor then uploads his document
 - A vendor uses the public key of the issuer of the tender to encrypt data
 - Now, only the issuer of the tender can decrypt it, using his private key
 - At the server side, the digital signature and data is verified before storing it for further processing

- Vendor can be sure that:
 - Except for the issuer of the tender, none can open his quote document
- Issuer of the tender can be sure that:
 - That the quote that has been received from a given vendor, has indeed come from the same vendor
 - That the quote given by the vendor has not been tampered on the way

Case 2: E-Shopping

Digital Signature Certificate used
by an Online Merchant's Web
server

E-Shopping



E-Shopping Process



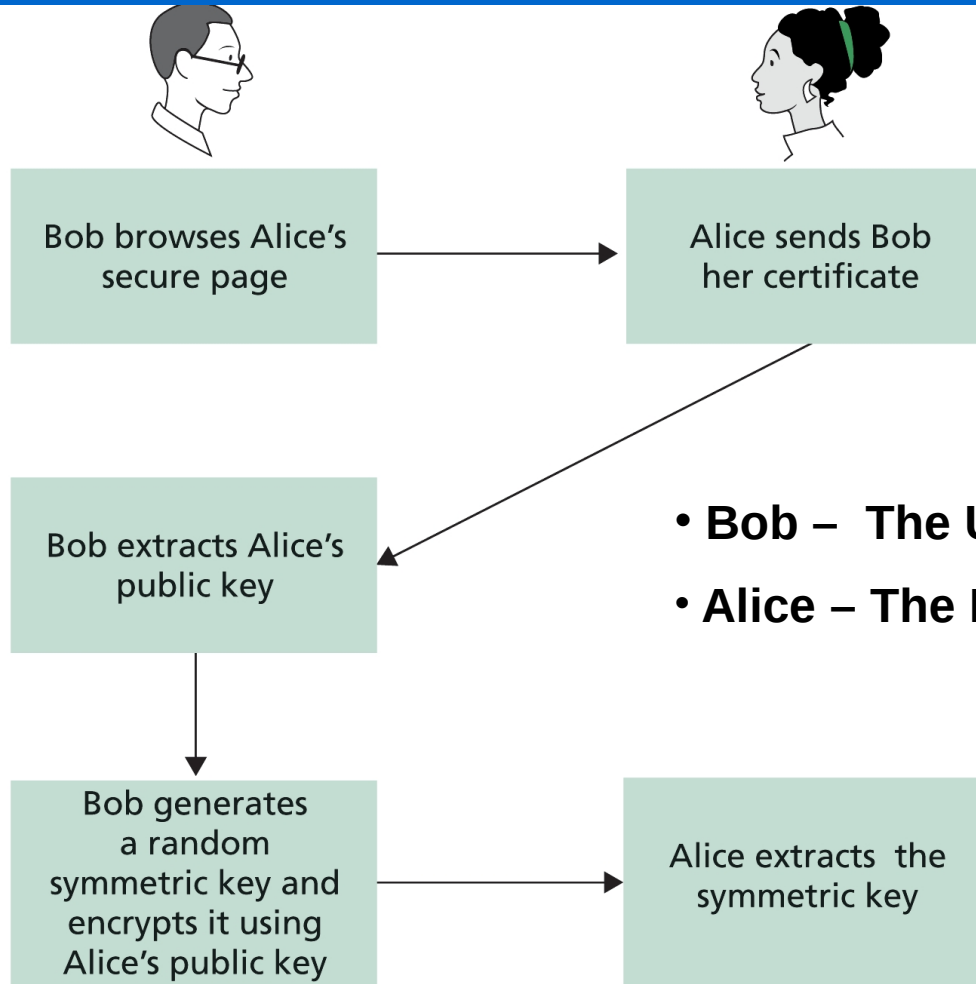
- Traditional E-Shopping
 - Machine (Server) – Machine (Client) Authentication
 - You are @ Client side; Merchant is @ Server side;
 - Client (Browser) will receive a digital certificate from the Server (Web Server), signed by a CA
 - If the CA is not in the list of 'Trusted CAs', Client will ask you, whether to trust this CA, and go forward
 - On trusting the CA, Client will then extract the Public Key, associated with the Domain Name of that Web Server

E-Shopping Process



- Client will then generate a random symmetric key and encrypts the key with the server's public key and sends it to the server
- Server will decrypt the message using its private key, and will find the key to be used for encrypting and decrypting messages, thus establishing a secure communication channel
- This is how **SSL** Works!

SSL - Explained



- **Bob – The User @ Client**
- **Alice – The Merchant @ Server**

Courtesy: James F Kurose, Keith W Ross, Computer Networking: A Top-Down approach featuring the Internet

How to get a Digital Signature Certificate?

Getting a Public Key Certificate



- Consists of 2 stages
 - Stage 1: Online Enrollment
 - Stage 2: Validation of Identity
 - Your credentials will be validated before issuing you digital certificate

Stage 1: Online Enrollment



- Visit any of the licensed CA's website and fill in the details
 - Submit the information about yourself
 - Some of the mandatory fields include
 - First name and last name
 - Email Address
 - City, State, Country
 - Permanent Address and Pin Code

- Challenge Phrase
 - You will be asked to provide a “challenge phrase”
 - You will require this pass phrase to renew, replace or revoke your certificate
 - CA does not have access to your challenge phrase
 - Hence it is your responsibility to safeguard it!.
- Your public-private key pair will be generated
 - Private keys will be of 1024 bits in length
 - If you are using IE browser, then you must select the Microsoft Enhanced Cryptographic Provider Option.
 - Remember that, this stores your private key in the IE browser itself

Stage 1: Online Enrollment Cont..



- If you have a smart card or USB token to store your Digital Certificate, you may select the Datakey RSA CSP (Cryptographic Service Provider) from the drop-down list box.
 - These CSP will give you the private keys that are 1024 bits in length
- Your public key will be sent to the CA for creation of the digital certificate
- Make the Payment!, by choosing one of the options.

Stage 2: Validation of Identity



- You need to be present before a trusted third-party who can identify and certify you
 - The third-party could be your banker, performing the authentication function
 - The banker will attest your name, signature and photograph based on the records with the bank
 - Some widely recognized, government-issued Photo-IDs are:
 - Passport, Driving License, PAN card, Voters ID card, Service Identity card issued by any State / Central government to its employee

Stage 2: Validation of Identity



- In short, you must
 - Complete the form
 - Have your banker attest the letter
 - Submit all documentation to the CA
- Your name, Email Id, Address that you enter in the form must be exactly as you have provided in the online enrollment

Certificate Issuance



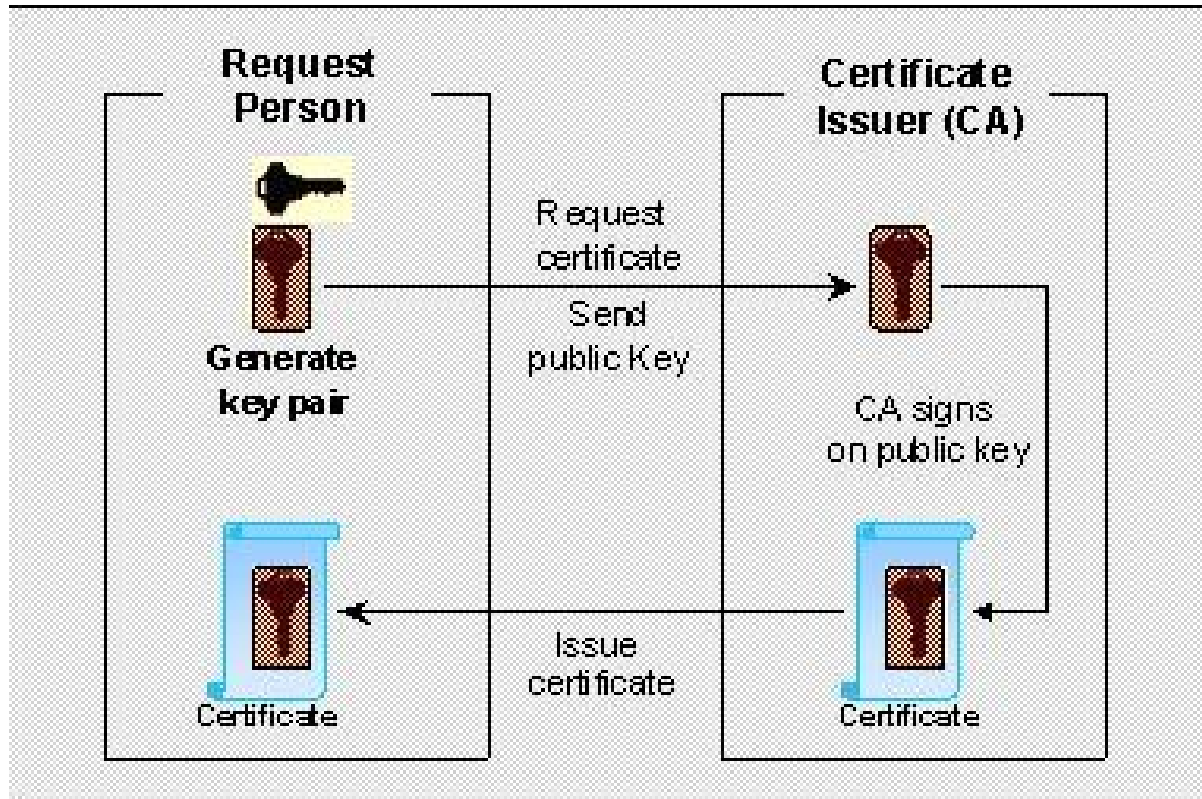
- CA will begin the validation process, after it had received all the duly completed documents
- If there is any discrepancy with the documents submitted, CA will send you an e-mail with the instructions to either re-enroll or to submit corrected documents
- After the validation process is completed, and upon receiving the payment, CA will issue your digital certificate
- You will receive an email with a URL, a PIN number and the instructions to pick your digital certificate

Getting the Certificate



- Visit the URL given in your email, and enter the PIN number into the field on the page, and then 'Submit' it.
- Pick up the Digital certificate using the same computer and browser that you used for enrolling for the digital certificate
- The next option will lead to the installation of the certificate in the browser.

Process - Explained



- Applicant generates his/her own key pair and sends the public key to the CA with some proof of his/her identification
- CA will put the public key in a new certificate, digitally sign the certificate using its private key and then send the certificate to the applicant

Procedures for Getting Certificates for Members of Government Agencies

NIC-CA



- NIC – Certifying Authority
- Type of Applicant/Subscriber
 - Government / PSU & Statutory Bodies / Registered Companies
- Issues Signing Certificate and Encryption Certificate
- Maximum validity period of 2 years
- 3 Classes of Certificates
 - Class – I Certificate
 - Assurance Level: Minimum level of assurance; Subscriber identity is proved only with the help of Distinguished Name – DN
 - Suggested Usage: Signing certificate primarily be used for signing personal emails and encryption certificate is to be used for encrypting digital emails and SSL certificate to establish secure communication through SSL
 - Category: Issued to the individuals of Govt bodies and to Web servers within NIC domain

Classes of Certificates



– Class – II Certificate

- Assurance Level: Conforms the details submitted in the form including photograph and documentary proof
- Suggested Usage: Signing certificate may also be used for digital signing, code signing, authentication for VPN client, Web form signing, user authentication, Smart Card Logon, Single sign-on and signing involved in e-procurement / e-governance applications, in addition to Class-I usage
- Category: Issued to the individuals from Govt bodies and web servers in open domain

Classes of Certificates



– Class – III Certificate

- Assurance Level: Highest level of Assurance; Proves existence of name of the organization, and assures applicant's identity authorized to act on behalf of the organization.
- Suggested Usage: Signing certificate may also be used for digital signing for discharging his/her duties as per official designation and also encryption certificate may also be used for encryption requirement as per his/her official capacity
- Category: Issued to Govt entities / Head of the Institutions, Govt Companies and Autonomous bodies

Process for Obtaining DSC



- User/Individual has to fill-up the DSC (Digital Signature certificate) form and submit it to NIC-CA
- A user-id, password is created for the user, based on the details given in the application
- Then the applicant has to login with the details and has to generate key pairs request and download certificate within 90 days, after the user-id has been created
- DSC will be issued on a smart card that allows only a maximum of 10 incorrect entries, for entering the pass phrase/pin, after which the card gets blocked and hence the DSC has to be revoked and reissued.

Process for Obtaining DSC



- NIC-CA will publish the certificate in the NIC-CA repository after acceptance of the DSC (Digital Signature Certificate) by the individual
- On cessation of employment, the certificate will be revoked

Important points to note



- Keep the private key safe and do not share it with others
- If in case the private key is compromised, applicant should immediately inform NIC-CA office and send a request for suspension
- Key Escrow / Key Archiving is not done by NIC-CA, and hence recovery of private encryption key is not possible
- Individual owning the Certificate / Tokens / Technology are fully responsible for their actions with the keys

References



- <http://nicca.nic.in> – CA website of NIC
- <http://www.cca.gov.in/LicencedCer.jsp> -
List of CA Certificates

Thank You