Mobile OTPK Technology for Online Digital Signatures

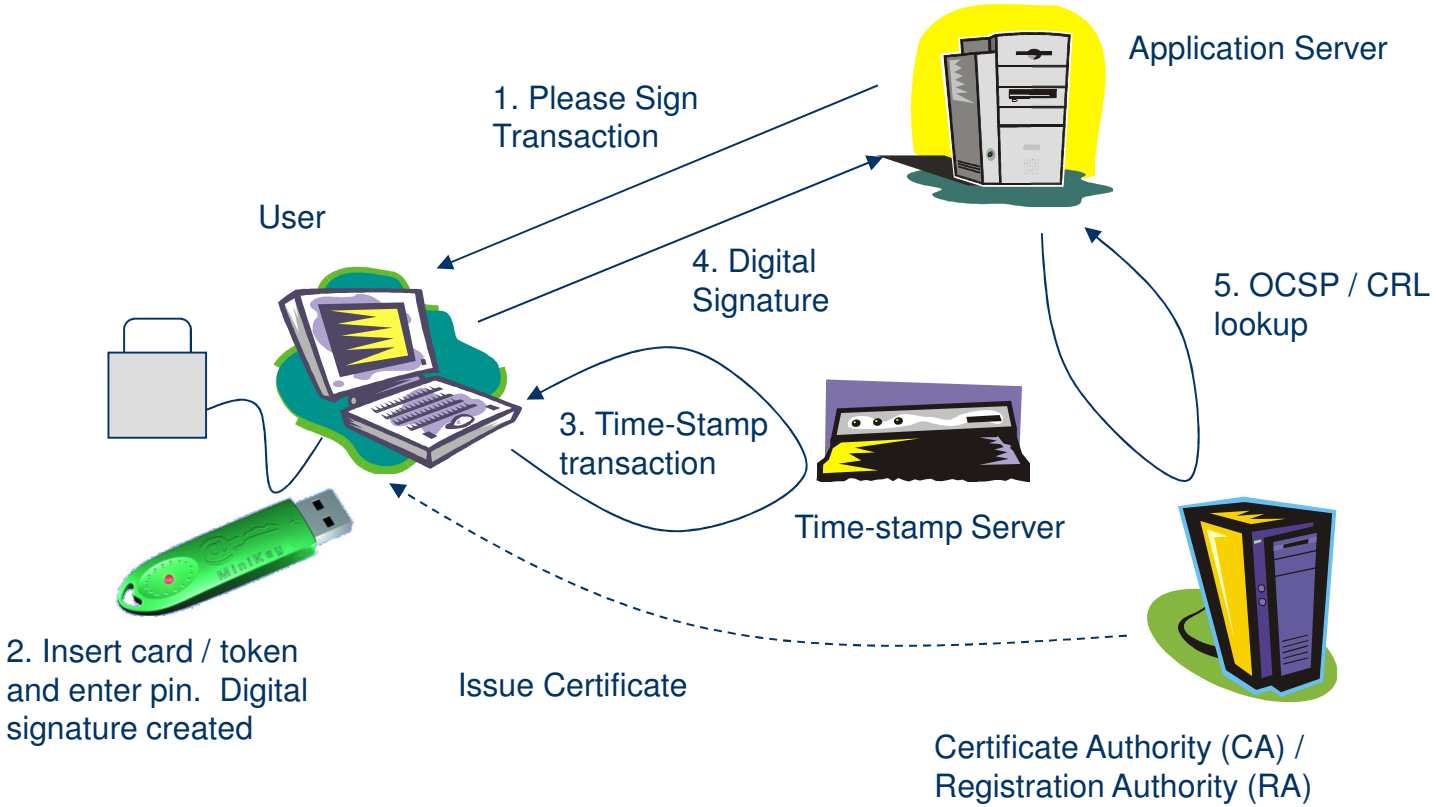
Dec 15, 2015

Presentation Agenda

- The presentation will cover
  - Background
    - Traditional PKI – What are the issued faced ?
    - Alternative technology
  - Introduction to OTPK
  - Comparing OTPK vs PKI
  - Issues surrounding OTPK
  - Demo
  - Future of OTPK

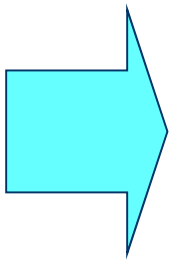
Background

- Traditional PKI



Background

- Problems with Traditional PKI
  - Cost of issuance
    - Cost of Smartcard / USB Token
    - Card personalization
  - Cost of deployment
    - Massive Logistics
    - Helpdesk support
  - Cost of Certificates
    - High upfront and recurrent certificates
  - Lack of mobility
    - Client installation



> Rs1000 per user

Background

- Existing solutions
  - Microsoft CSP
    - Microsoft CSP exists in all machines using Windows OS.
    - Addresses cost of issuance and cost of deployment
    - Introduces problem: key stored in software makes it easy for hackers to steal
  - HSM-backend signing / Virtual smartcard
    - Solutions on SafeNet, nCipher, Thales HSM to implement a “smartcard on the network” which hosts and signs transactions on behalf of user
    - Solutions by RSA Keon, ARX CoSign extend the HSM-signing solution to implement a PKCS#11/CAPI layer to communicate seamlessly with the HSM to sign the transactions.
    - Addresses cost of issuance and cost of deployment + keeping key secure
    - Introduces problem: Signing key not in possession of user. Not in accordance with legislation

Background

- Motivation for new solution – Addressing the problems
  - Addressing cost of issuance and deployment
    - Can we remove the prohibitive cost of PKI without compromising on the legality of the digital signatures ?
    - Cost of 2-factor authentication (2FA)
      - The use of OTP (One-time password) for 2FA is growing very significantly. Already, countries in Singapore and Hong Kong require 2FA for Internet Banking
      - The cost of deploying 2FA using OTP works out to less than Rs 400 per user.
  - Addressing cost of certificates
    - Cost of certificates is not aligned to cost of business / transactions. Can we reduce the upfront certificate costs ?
  - Need for Mobile PKI
    - Can users perform digital signatures on mobile phones ?

Introducing OTPK

- OTPK is NOT a new PKI platform.
- It is about making PKI
  - Easier to use
  - Cheaper to implement & deploy
  - Faster to adopt

Introducing OTPK

- Basis
  - One-time use, short-lived certificate
  - Each time a signature is needed, the key is generated, certified, used to sign the transaction, and then deleted
  - Key always remains in client possession throughout the short lifetime, and never stored on a permanent basis.
  - Main security lies in the online certification process where the user would use strong (2-factor) authentication to the CA/RA.
  - Compatible to existing PKI application architectures
  - In its current form, only usable for authentication and digital signatures.

Introducing OTPK

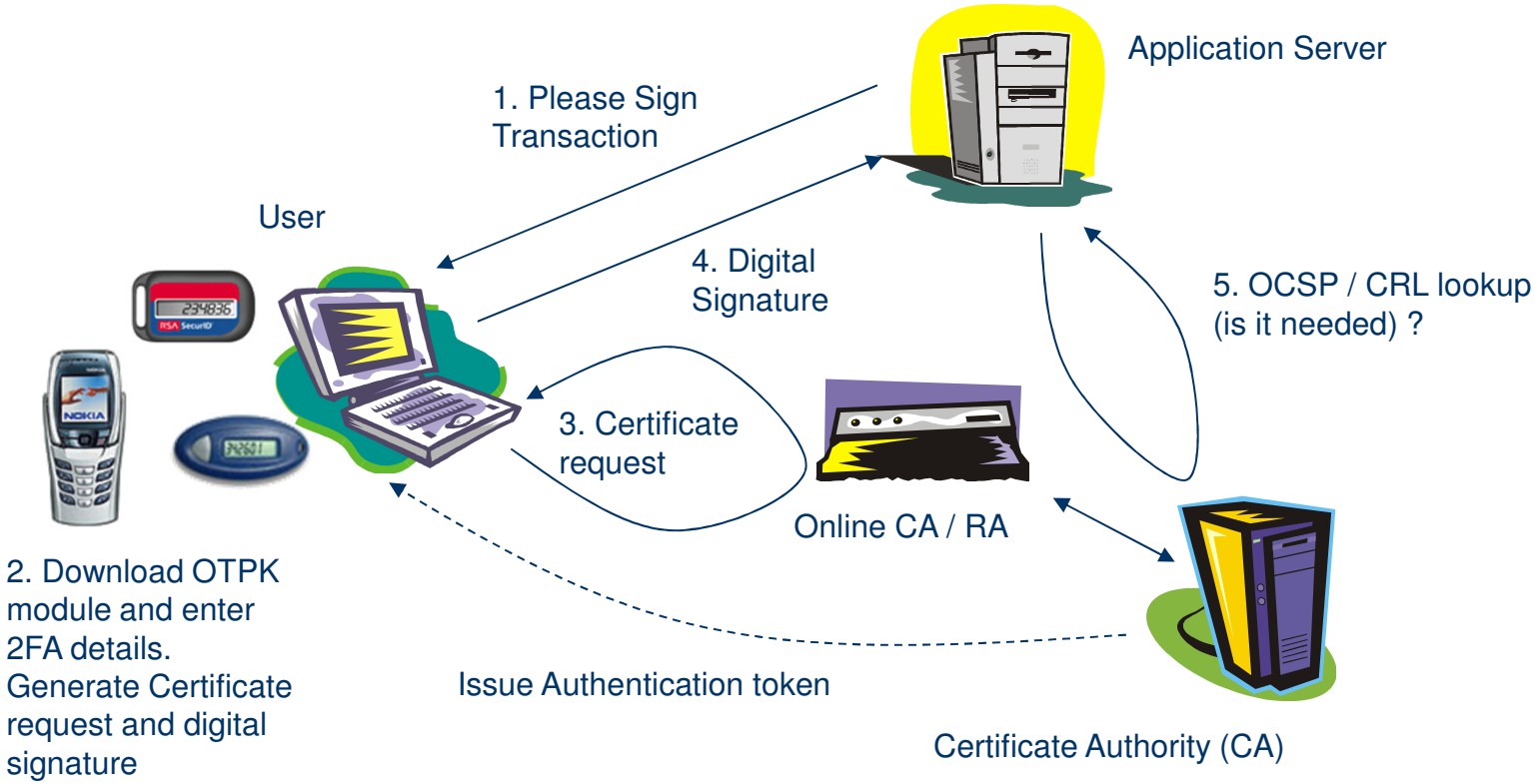
- 2 Phases
  - Registration
    - User is issued a 2FA OTP token, e.g. RSA SecurID, VASCO, Aladdin. Alternative forms of 2FA such as software tokens on J2ME phones, OTP sent through SMS, email, etc can be considered but will impact security.
    - Face to face verification, if required, will take place at this stage.
    - The 2FA OTP token will allow the user to authenticate to the CA/RA during the online certification process.
    - Biometric authentication can be utilized under circumstances where remote biometric authentication is secure. i.e. OTPK is not restricted to 2FA OTP, although authentication credentials should be time-bound to ensure freshness of certificate request.
  - Signing

Introducing OTPK

- 2 Phases (con't)
  - Signing
    - When a digital signature (an asymmetric decrypt operation) on a transaction is required, the user has to download an OTPK module.
    - OTPK module will
      - Generate public-private key pair.
      - Prompt the user to provide the 2FA OTP credentials
      - Embed the 2FA OTP credential and transaction hash (for time-stamping) within certificate request.
      - Certificate request is end-to-end encrypted for the CA/RA
    - Certificate request is sent to CA/RA
    - CA/RA verifies 2FA OTP credentials, and issues short term (e.g. 5 min) certificate. Certificate contains transaction hash for time-stamping purpose
    - OTPK module will return the digital signature of transaction and delete the private key.
    - User now has the certificate and signature, without private key.

Introducing OTPK

- OTPK PKI



Comparing OTPK with PKI

- The advantages of OTPK over Traditional PKI are:
  - No need for smartcards for users
    - Lower cost of issuance from smartcard to OTP levels
  - Much smaller window of compromise
    - Private Key is now valid for only short time (e.g. 5 minutes) as compared to 1-3 years.
  - No need for large LDAP systems
    - Strong of OTPK certificates in LDAP is no feasible. Instead, certificate should be attached with signature.
  - No CRLs or OCSP for certificates
    - Short certificate lifetime ensures CRLs/OCSPs not relevant.
  - Low learning curve
    - All complexities abstracted for users to presenting 2FA OTP.

Comparing OTPK with PKI

- The advantages of OTPK over Traditional PKI are: (cont')
  - Easy Interface into 2FA / Biometric authentication
    - Traditional PKI has 2 different points of authentication – point of issuance & point of signing. Only single point of authentication exists for OTPK
  - Private Key always in possession of user
    - As compared to software / HSM alternatives. OTPK is closer to the PKI legislation around the world.
  - Protocol is interchangeable for all asymmetric algorithms
    - OTPK can be used for RSA, DSA, ECDSA. If algorithm is not suitable e.g. broken, insufficient key length, licensing, platform incompatibility, it can be changed quickly by replacing the OTPK module. This contrasts with a total recall smartcards/tokens which is highly infeasible.
  - Solution is very scalable
    - OTPK Backend handles only 1 asymmetric operation (key certification). This can be spread over several sub-CAs in a horizontal scaling infrastructure.

Comparing OTPK with PKI

- The advantages of OTPK over Traditional PKI are: (cont')
  - Efficient Pricing model for CA
    - Since each certificate is tied to a transaction, CAs can charge on a pay-per-use basis.
    - Differentiation can be :
      - Mode – online vs batch processing, per transaction or per authentication session
      - Timing – peak hour vs off-peak hours
      - Loyalty – more usage => cheaper certificates
      - Branding – Different classes of certificates
      - Algorithm – Different pricing for different certificates
      - Level of Insurance / liability
    - OTPK certificates can be supported on applications that are expecting traditional PKI certificates since OTPK also uses X.509 certificates, barring a possible X.509 extension indicating that status information is not published.
    - CAs can support both traditional and OTPK PKI and allow both systems to interoperate.

Issues surrounding OTPK

- Issues surrounding OTPK
  - Online CA Key
    - As compared to traditional PKI, the OTPK CA key is online and certificates are issued in real-time.
    - Mitigating controls:
      - Stolen CA Key - Use of FIPS certified HSM to house CA key
      - Fake certificate requests – Use of strong 2FA with end-to-end encryption for certificate requests.
  - User Registration
    - In traditional PKI, key is generated once during the registration process. The registration process may require a face-to-face verification.
    - In OTPK PKI, the authentication token is issued during the registration process. The face-to-face verification step is complied with.

Issues surrounding OTPK

- Issues surrounding OTPK (con't)
  - Secure Time-stamping
    - Time stamping is a deliberate process in traditional PKI where the user or server will send the hash for time-stamping.
    - For OTPK, the transaction hash should be included in the certificate request so that the CA can also provide time-stamping services at no extra procesing costs.
  - Secure Private key deletion
    - The deletion of the key, when the certificate has expired is important. For traditional PKI, proof of private key destruction can be the destruction of the smartcard / token.
    - For OTPK, besides using properly designed software with FIPS certification, the indirect way is to ensure that the key cannot be used for any other operation. This is similar to the Secure Time-stamping approach where the transaction hash is included in the certificate, ensuring that improper use will result in a signature verification failure.

To be discussed

- Strong authentication
  - While we have advocated the use of hardware OTP tokens for user authentication in OTPK, the use of very simple and inexpensive 2-factor authentication solutions such as challenge-response “bingo cards” can be used. While it may make OTPK more compelling, what is its implication with the legality of digital signatures ?
- CAs issuing more certificates
  - In OTPK, the CAs will potentially issue certificates at much higher volume and speed. Is the CA infrastructure at risk ?
- Interoperating traditional PKI with OTPK PKI
  - Does it make sense to CAs ?
  - Can we simply introduce new extensions to make traditional PKI operate with OTPK PKI ? What else is needed ?

Future of OTPK

- C-DAC is planning the following:
  - Building an OTPK toolkit with HSM providers
  - Operating OTPK pilots in various industries including:
    - Government
    - Banking
    - Internet transactions
    - Healthcare
- Build an OTPK-adoption community.
  - All support welcome. Email: saquib@cdac.in

Thank you

Questions ?

saquib@cdac.in