

X.509 Public Key Infrastructure

Tim Gable

Why Use a PKI?

- Millions of transactions per day
 - Who are you doing business with?
 - Is your information safe?
 - Is the data accurate?
- A PKI can solve all of these problems

X.509 PKI Background

- Secure transactions
 - Privacy
 - Authentication
 - Integrity
 - Non-repudiation
- Public/private key pairs
 - RSA
 - Use primes and relative primes with modular arithmetic
 - $T^e \bmod n$ -- encryption (T is plaintext)
 - $C^d \bmod n$ -- decryption (C is ciphertext)
- Certificates
 - X.500 database
 - X.509 certificates
 - Certificate Revocation List

X.509 Certificate

```

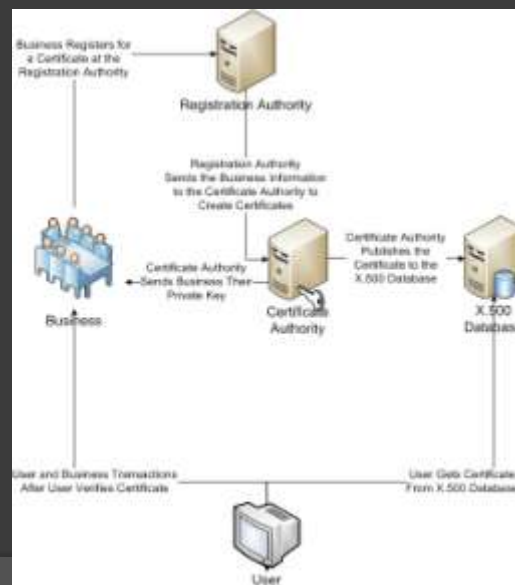
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 7829 (0x1e99)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=US, ST=Western, CN=Cape Town, O=Thawte Consulting cc,
    OU=Certification Services Division,
    CN=Thawte Server CA/emailAddress=server-cert@thawte.com
    Validity
      Not Before: Jul  3 16:04:02 1998 GMT
      Not After : Jul  3 16:04:02 1998 GMT
    Subject: C=US, ST=Maryland, L=Pasadena, O=Scant Baccala,
    OU=FreeSoft, CN=www.FreeSoft.org/emailAddress=baocala@freesoft.org
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:b4:31:88:0a:c4:bc:62:c1:c8:aa:dc:b0:c8:bb:
        83:96:19:d5:09:64:b5:98:41:b0:58:fc:f9:31:e1:
        86:36:d0:8e:54:12:64:ba:75:eb:ea:1c:9c:bb:46:
        70:93:02:1e:08:ea:4f:91:81:70:39:0e:53:8b:17:
        14:94:6e:ee:f4:d5:8f:d5:ca:b3:47:5e:1b:0a:7f:
        05:00:2b:40:01:80:0b:15:31:8d:bf:7a:c7:47:7f:
        8fa:0:21:c7:4c:d0:16:05:00:c1:0f:d7:b8:50:e5:
        d1:75:4b:01:ea:19:50:50:ea:7d:c1:a1:10:1b:88:
        e8:3c:1c:9e:27:52:7e:41:92
      Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
    93:5f:2f:1f:06:a5:d7:0e:ab:a3:6a:f8:24:cf:2b:4:59:5d:9d:
    92:2e:4a:1b:0b:ae:7d:99:17:5d:cd:19:56:ad:ef:03:2f:92:
    ab:2f:4b:0f:0a:12:90:ee:2c:0e:45:03:0e:f6:ee:8e:9c:67:
    d8:ed:40:03:27:ed:6a:15:09:78:a8:06:ee:b7:1e:1b:41:7e:
    0d:13:aa:ad:8d:9e:df:ab:97:50:65:f5:5e:85:a4:ef:13:01:
    5a:de:3d:ea:63:cd:c8:cc:6d:5d:01:05:b5:6d:cc:f3:d0:27:
    87:0e:fc:ba:1f:34:e9:84:6e:6c:0f:22:ef:9b:bb:1e:1d:5:22:
    81:22
  
```

<http://en.wikipedia.org/wiki/X.509>

PKI Basics

- Registration Authority
 - Registration Process
- Certificate Authority
 - Examples
 - VeriSign
 - DigiCert
 - Distribution
- Clients
 - Doing business with certificates

PKI Diagram



PKI Benefits

- ⦿ Versatile
 - Banks
 - E-commerce
 - Government
 - NIST SP 800-32
- ⦿ Privacy
 - Encryption

PKI Benefits (cont)

- ⦿ Authentication
 - Certificates
- ⦿ Integrity
 - Signed Hash
- ⦿ Non-repudiation
 - Digital Signature

PKI Problems

- ⦿ Registration and Distribution Problems
 - 2001-Microsoft Certificates given to the wrong people by VeriSign
- ⦿ Trust
 - CA is just a company that people trust
 - How did they earn that trust?
- ⦿ Non-repudiation
 - Security of your private key

PKI Problems (cont)

- ⦿ Certificate Revocation Lists
 - Back Dating Invalid Certificates
 - Certificates have already been used while invalid
 - CRL cache
 - Clients can download the CRL and use it until it expires
 - Emergency updates are not downloaded

X.509 PKI Overview

- Securing online transactions
- RSA encryption
- X.509 Certificates
- Registration Authority/Certificate Authority
- Benefits
 - Privacy
 - Authentication
 - Integrity
 - Non-repudiation
- Problems
 - Registration and Distribution
 - Trust
 - Non-repudiation
 - Certificate Revocation List