Public Key Applications & Usage A Brief Insight

Scenario

:: Identification, Authentication & Non-Repudiation [illegible] transaction

:: Authenticity, e-business transaction assurance

:: Confidentiality and Integrity requirements

:: Secure access

- by individuals and by other applications.

:: Protection from Man-in-the Middle and replay attacks

:: Mutual authentication

- between each components –

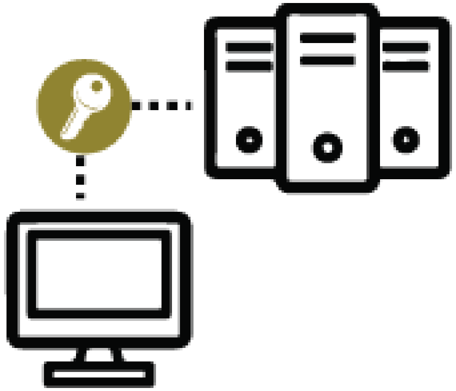
– and others issues such as Eavesdropping, Tampering, Impersonation, Spoofing, Misrepresentation

Public Key 101
- A Revision

How many have wondered just what is Public Key Cryptography, PKI, PKCS, and PKIX are?

Public Key Cryptography

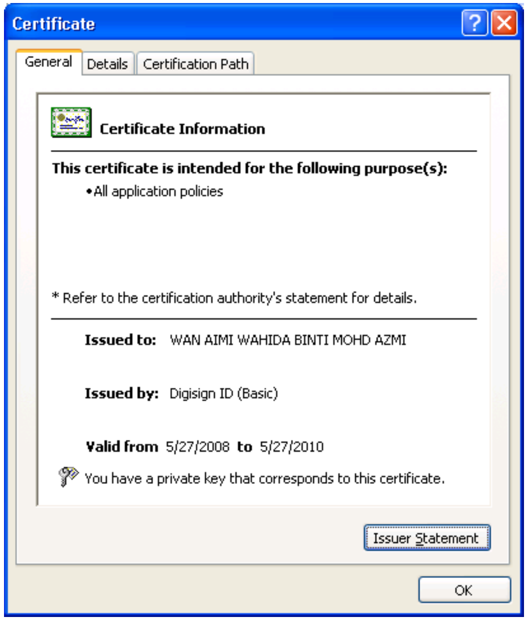
-Encryption algorithms, Message digest functions, Hashed Message Authentication Code (HMAC) functions, Secret key exchange algorithms, Digital signatures



PKI

- framework of services, technology, protocols, and standards . Basic Components - digital certificates, certificate revocation lists, and certification authorities.

Digital Certificates, X.509



Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

* Refer to the certification authority's statement for details.

Issued to: WAN AIMI WAHIDA BINTI MOHD AZMI

Issued by: Digisign ID (Basic)

Valid from 5/27/2008 **to** 5/27/2010

You have a private key that corresponds to this certificate.

Things That We Already Know

- Public Key Technology

An enabling technology to provide security and to provide truly paperless, digital environments.

Potential in applications that involve communications or movement of information over communications or computer networks.

PK techniques along with PKI allow secure communication between parties without prior agreement or arrangement.

Simplify security and identity management with a single security infrastructure

Digital Certificates

Mechanism establish for others can Trust

verify

Provide & Verify your identity

certificate authority (CA), a trusted third party

with a reliable means to check your identity

Digital Certificates add value to public key cryptography

Digital Management & Scalability

The public key is vouched for by a

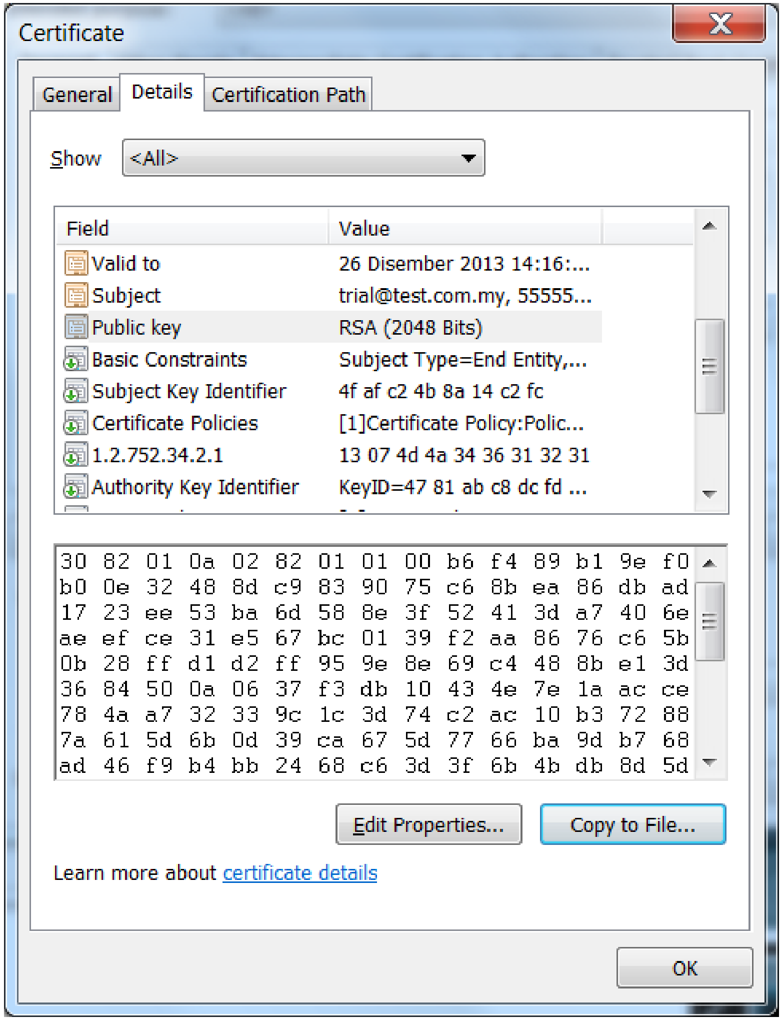
An important network for transactions.

- Users
- Machine /Devices

- Managing Public Key and usage of certificates.
- Certificates & network of trust certificates authorities (CAs), allow PK to scale - meet the needs to enterprise and inter enterprise usage

Verifying the authenticity of an entity's purported public key.

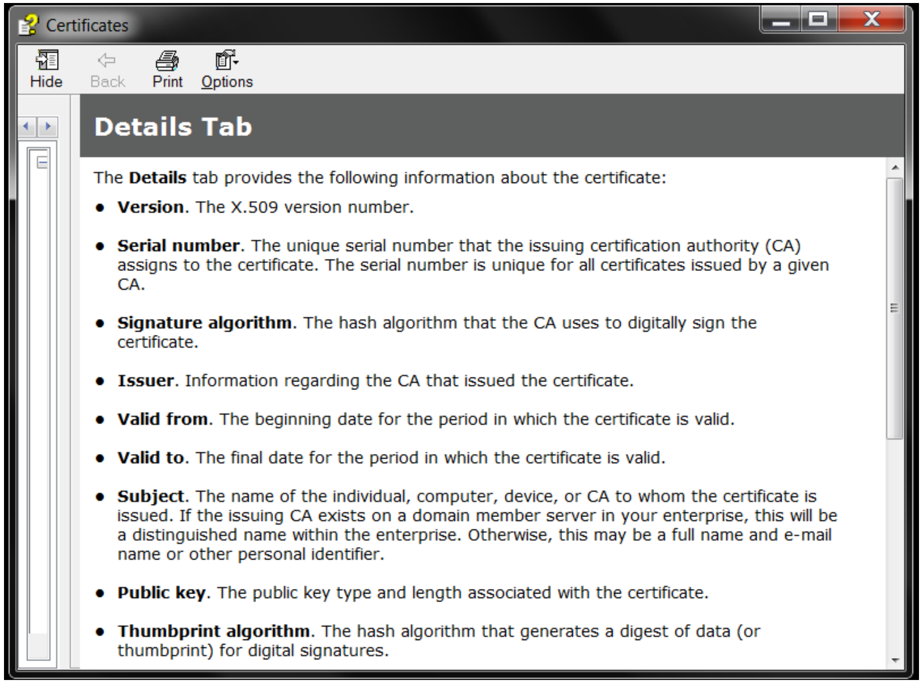
X.509 Format



Field	Value
Valid to	26 Disember 2013 14:16:...
Subject	trial@test.com.my, 55555...
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity,...
Subject Key Identifier	4f af c2 4b 8a 14 c2 fc
Certificate Policies	[1]Certificate Policy:Polic...
1.2.752.34.2.1	13 07 4d 4a 34 36 31 32 31
Authority Key Identifier	KeyID=47 81 ab c8 dc fd ...

```
30 82 01 0a 02 82 01 01 00 b6 f4 89 b1 9e f0
b0 0e 32 48 8d c9 83 90 75 c6 8b ea 86 db ad
17 23 ee 53 ba 6d 58 8e 3f 52 41 3d a7 40 6e
ae ef ce 31 e5 67 bc 01 39 f2 aa 86 76 c6 5b
0b 28 ff d1 d2 ff 95 9e 8e 69 c4 48 8b e1 3d
36 84 50 0a 06 37 f3 db 10 43 4e 7e 1a ac ce
78 4a a7 32 33 9c 1c 3d 74 c2 ac 10 b3 72 88
7a 61 5d 6b 0d 39 ca 67 5d 77 66 ba 9d b7 68
ad 46 f9 b4 bb 24 68 c6 3d 3f 6b 4b db 8d 5d
```

Learn more about certificate details



Details Tab

The **Details** tab provides the following information about the certificate:

- **Version**. The X.509 version number.
- **Serial number**. The unique serial number that the issuing certification authority (CA) assigns to the certificate. The serial number is unique for all certificates issued by a given CA.
- **Signature algorithm**. The hash algorithm that the CA uses to digitally sign the certificate.
- **Issuer**. Information regarding the CA that issued the certificate.
- **Valid from**. The beginning date for the period in which the certificate is valid.
- **Valid to**. The final date for the period in which the certificate is valid.
- **Subject**. The name of the individual, computer, device, or CA to whom the certificate is issued. If the issuing CA exists on a domain member server in your enterprise, this will be a distinguished name within the enterprise. Otherwise, this may be a full name and e-mail name or other personal identifier.
- **Public key**. The public key type and length associated with the certificate.
- **Thumbprint algorithm**. The hash algorithm that generates a digest of data (or thumbprint) for digital signatures.

-----BEGIN CERTIFICATE-----
MIICKzCCAZSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGEwJV
UzER
MA8GA1UEChMITmV0c2NhcGUxFTATBgNVBAsTDFN1cHJpeWEncyBDQTAeFw05
NzEw
MTgwMTM2MjVaFw05OTEwMTgwMTM2MjVaMEgxCzAJBgNVBAYTAlVTMREwDwY
DVQQK
EwhOZXRzY2FwZTENMAsGA1UECxMEUHViczEXMBUGA1UEAxMOU3Vwcml5YSB
TaGV0
dHkwgZ8wDQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAMr6eZiPGfjX3uRJgEjmKiqG
7SdATYazBcABu1AVyd7chRkiQ31FbXFOGD3wNktbf6hRo6EAmM5/R1AskzZ8AW7L
iQZBcrXpc0k4du+2Q6xJu2MPm/8WKuMOnTuvzpo+SGXelmHVChEqooCwfdiZywyZ
NMmrJgaoMa2MS6pUkfQVAgMBAAGjNjA0MBEGCWCGSAGG+EIBAQQEAwIAgDAf
BgNV
HSMEGDAWgBTy8gZZkBhHUfWJM1oxeuZc+zYmyTANBgkqhkiG9w0BAQQFAAOBg
QBt I6/z07Z635DfzX4XbAFpjlRl/AYwQzTSYx8GfcNAqCqCwaSDKvsuj/vwbf91o3j3
UkdGYpcd2cYRCgKi4MwqdWyLtpuHAH18hHZ5uvi00mJYw8W2wUOsY0RC/a/IDy84
hW3WWehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfpRqjd1A== -----END CERTIFICATE--
---

Some of possible Public Key Technology usage

Secured Online Banking

Date Time Stamping

Signing & Encryption PDF & Document

Secure Email

Watermark PKI

Code Signing

Online File Storage system

Cloud

Network Security - Strong Device Infrastructure [illegible]

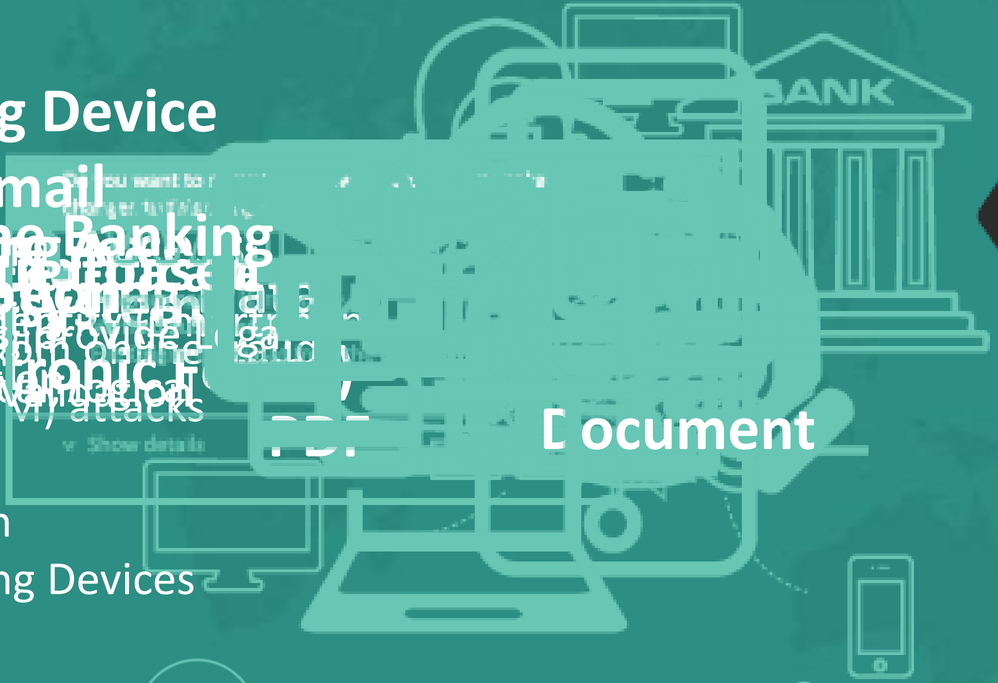
BYOD [illegible]

[illegible]

- Client devices to protect from phishing, man-in-the-middle (MITM) attacks

and mobile access)

- IPSec VPN
- Machine / Device Authentication
- Firewalls, Routers and Networking Devices



User/Enterprise Certificate

Federated Identity and Access Management

Network Security – Strong Device Infrastructure Identities; WiFi, VPN, BYOD, Remote Access

Secure File Transfer (Protecting Data Entered & Stored In Electronic Forms

Secured Authentication Document

Secure Web Form

Mobile Device

PKI Federated Identity

Identity federation streamlines and simplifies IAM processes. By allowing to link, re-use and combine identities across multiple domains, it means users no longer require distinct credentials for each domain.

One particularly flexible incarnation is single sign-on, whereby one-off authentication grants seamless access to a host of federated services.

PKI BYOD

Integrated Multi-Factor Authentication for users and devices

- Identification of User Identity
- Authorization to access application
- Encrypted Connection
- Audit User Activity

Data is not stored locally

- minimizing risk of data leakage if device is lost or stolen

End user convenience through instant secure access to information

Must be compatible with all end devices

New Challenges

Open Organizations - Require Safe Identity
- Firewall & VPN no longer define the border of security domain

Internet of Things
- M2M
-By 2020 more 200 billion devices connected to Internet

Critical Infrastructure

Privacy in Internet
- Protect Identity & Private Data

Anonymity

THANK YOU

ariffuddin@digicert.com.my