Certificates and Certification Authorities

Wason Liwlompaisan
wason@blognone.com

Two Type of Encryption

- Symmetric Key
  - Same Key to Encrypt/Decrypt
- Asymmetric Key
  - Public/Private Key
  - Encrypted with Private Key, decrypted with Public Key
  - Encrypted with Public Key, decrypted with Private Key

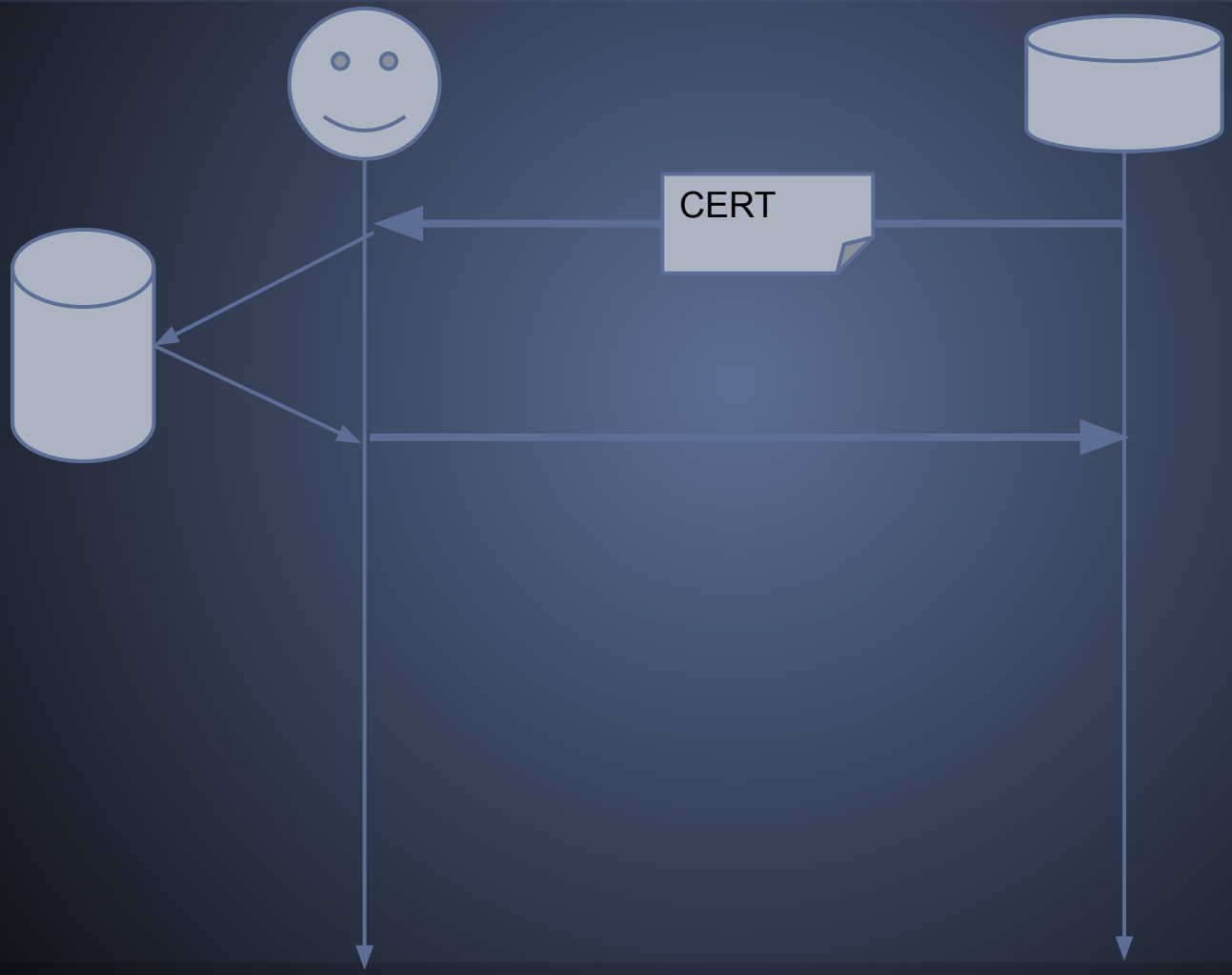
Asymmetric Key

- Public Key == Publicly Announced
- Private Key == Keep with owner only
- Signing
  - Approved by the private key owner
  - Could be checked with public key

HTTPS

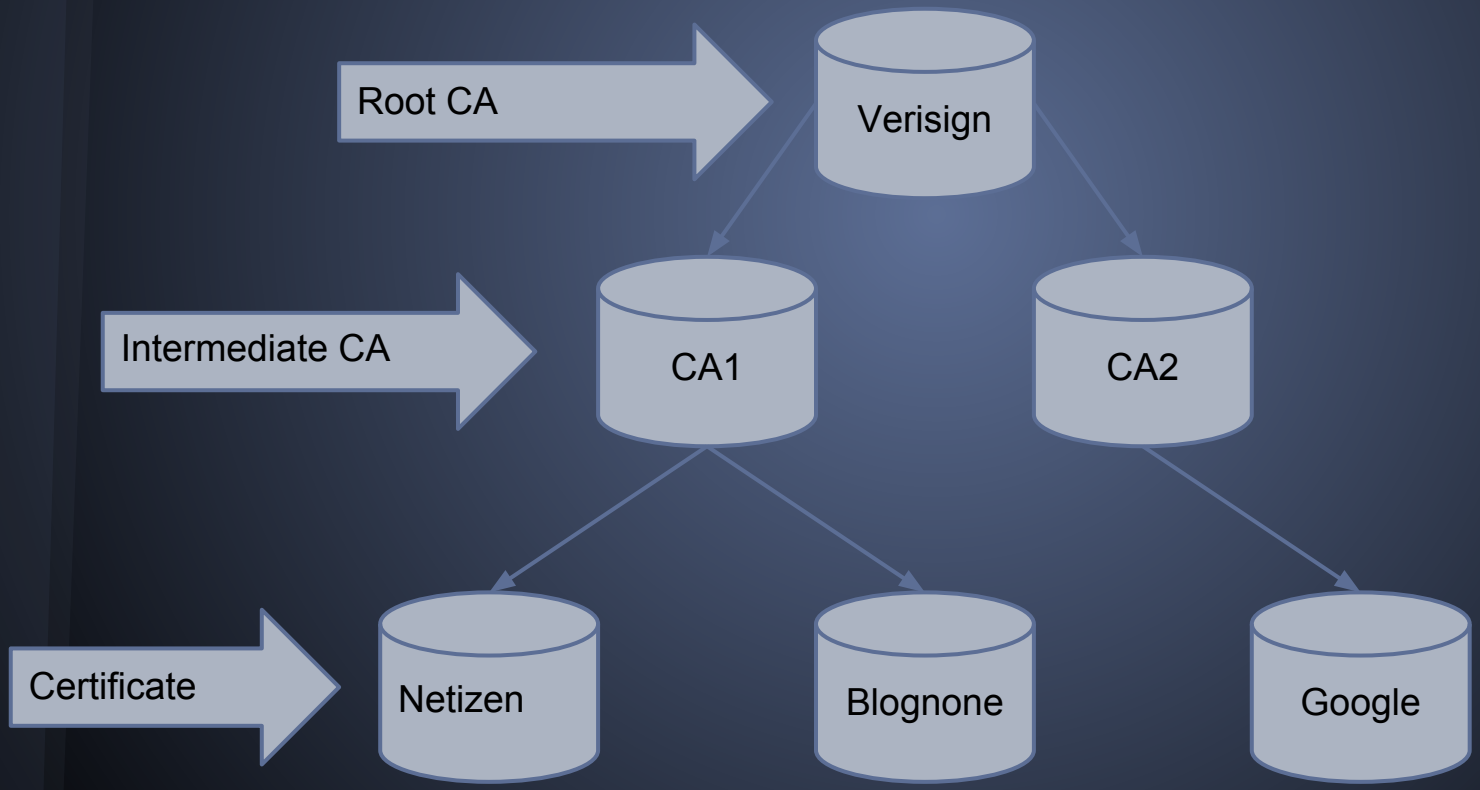
- Secured HTTP
- Ensure you're talking with the domain owner
- Nobody else know the message

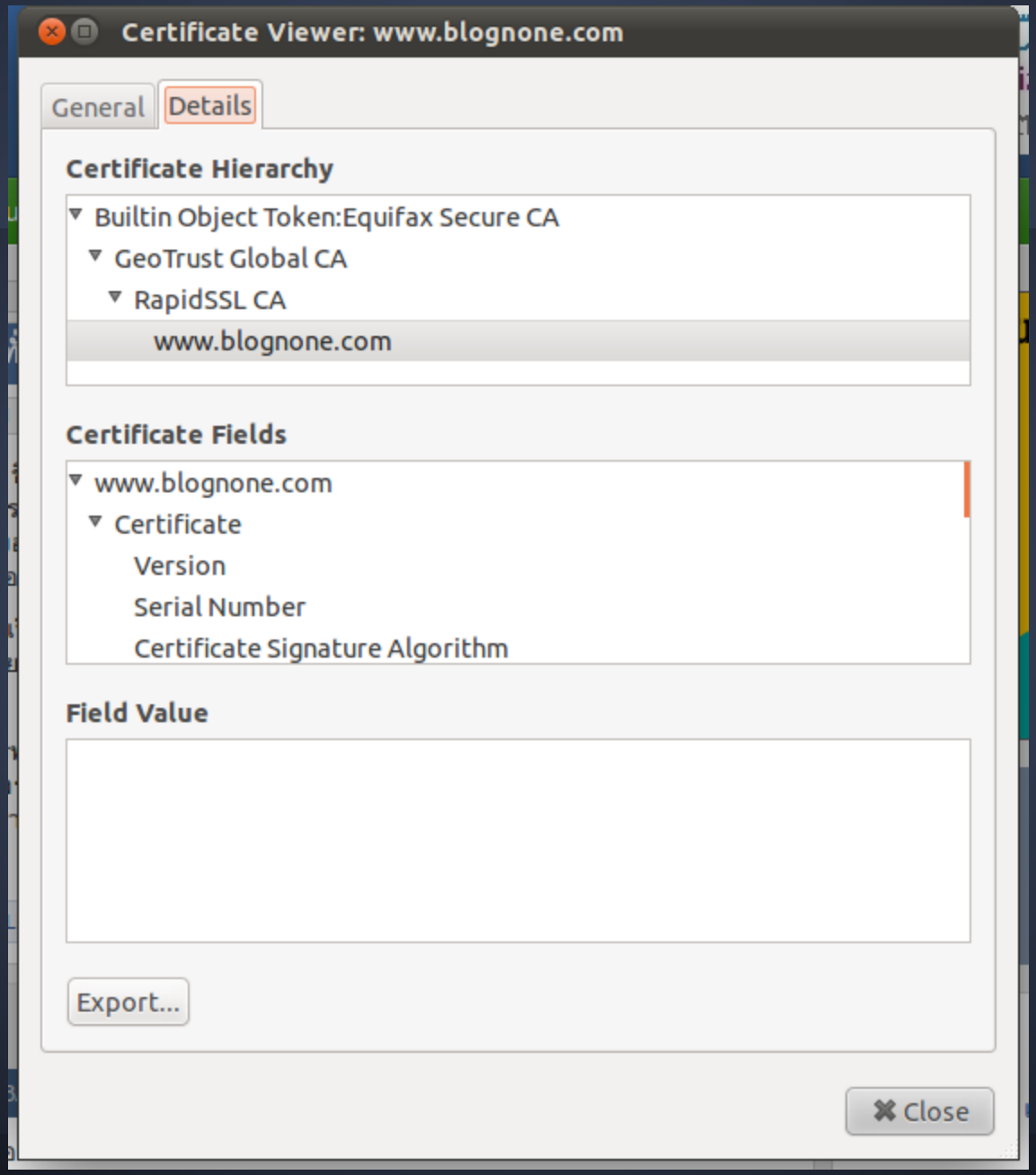
HTTPS



PKI

- Public Key Infrastructure




Certificate Viewer: www.blognone.com
General
Details
Certificate Hierarchy
Builtin Object Token:Equifax Secure CA
GeoTrust Global CA
RapidSSL CA
www.blognone.com
Certificate Fields
www.blognone.com
Certificate
Version
Serial Number
Certificate Signature Algorithm
Field Value
Export...
Close

Mozilla (Firefox) Root CA

A-Trust
ACCV
AffirmTrust
Buypass
Camerfirma
CATCert
Certicamara S.A.
Certigna of Dhimyotis
Certinomis
certSIGN
Chunghwa Telecom
CNNIC
Comodo
ComSign
DigiCert
DigiNotar (DISABLED)
Disig
E-Guven
E-TUGRA
EDICOM
Entrust
Firmaprofesional
GlobalSign
Go Daddy
Government of France
HARICA
Hongkong Post
IdenTrust
Izenpe
Japanese GPKI
JCSI
Kamu SM
Keynectis / Certplus
Microsec e-Szignó
NetLock
Network Solutions
QuoVadis
S-TRUST
SECOM Trust
Sertifitseerimiskeskus AS
Staat der Nederlanden / Logius
StartCom
SwissSign
Symantec / GeoTrust
Symantec / TC TrustCenter
Symantec / thawte
Symantec / VeriSign
T-Systems
Trustwave
TURKTRUST
TWCA
Unizeto Certum
Verizon / Cybertrust
Wells Fargo
WISeKey

The site's security certificate is not trusted!

You attempted to reach **jusci.net**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway | Back to safety

▸ Help me understand

Attacks

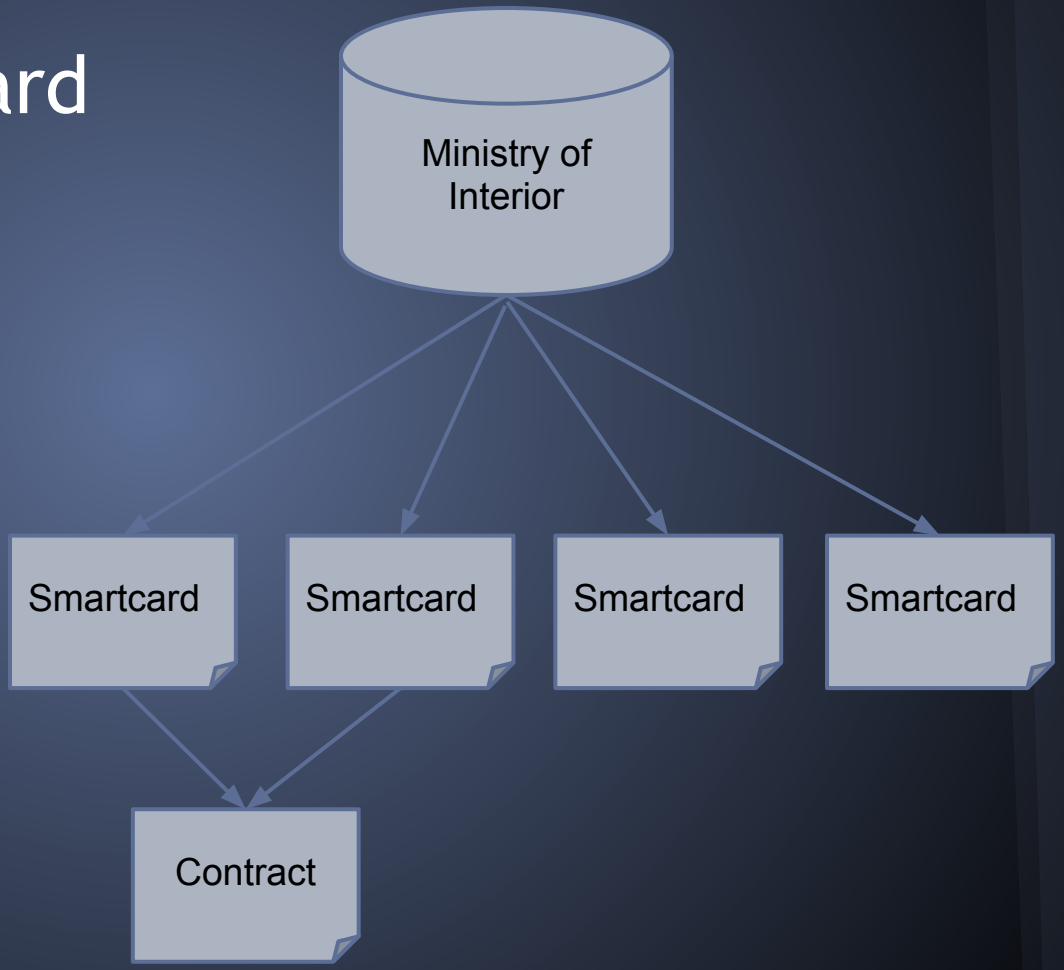
- One CA compromised, all web compromised
- CA in non-free jurisdiction
- Etisalat, an ISP in UAE
  - Update Blackberry with Snooping program
  - Now it's an intermediate CA
- Comodo SSL hacked in 2011

Thailand

- No CA in Thai jurisdiction
- National Root CA is in Thailand's master plan
- TOR announced in March 2012

Smartcard

- Computer in a card
- PKCS #11
  - Sign documents
- Internal CA



Problems with Smartcard

- CA's security
- Card Loss
- https://www.blognone.com/news/12414/