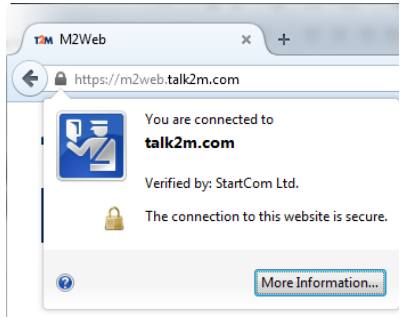
Back to Internet Security Basics

Serge WAUTIER

HMS Connecting Devices™

Internet Security Basics



How do secure
web sites work?

What is *encryption*?
How does it work?

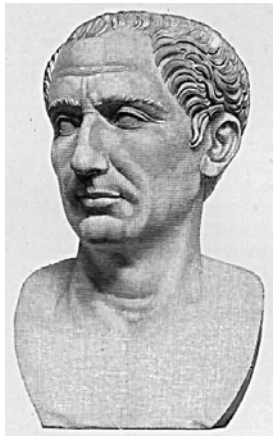
What is a digital certificate?

What about public and private keys?

HMS Connecting Devices™

History

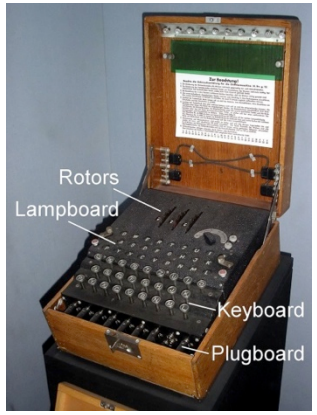
2000 years ago, Julius Caesar



WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

- Secret algorithm
- No key
- Encryption: Someone who steals the message can't understand it



1920 – WorldWar II : Enigma

- Electro-mechanical machine
- Key = mechanical setup of the machine

History

More recently

- 1970- : DES encryption algorithm
- The algorithm is a published standard.

Kerckhoffs's principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

The problem

How to exchange the key?

Assymetric Cryptography

Principle (1976 – Diffie-Hellman)

- Public key: Encrypts the message
- Private key: Decrypts the message

- Find an algorithm that cannot be easily reversed.
- The public key can encrypt but cannot decrypt.

- Implementation (1977 – Rivest, Shamir, Addleman)

  It is easy to prove that a number is prime. But it is difficult to find its factors.

  n = 146429944120587116605887419783692084105576633854587917829657

  Is this a prime number? Easy to find out!
  What are its factors? Much more difficult!

  p = 52141962285665768942387261377 1

  q = 28082936986213471939003661706 7

Connecting Devices™

Assymetric Cryptography

Encryption - Alice sends a message to Bob

- Alice finds Bob's public key in a directory.
- Alice encrypts her message and sends it to Bob.
- Bob decrypts the message using his private key.

- Everybody can send messages to Bob.
- Only Bob can decrypt those messages.

Authentication

- How does Bob know that the message indeed comes from Alice?

- Alice *decrypts* some clear text using her private key.
- Bob *encrypts* the result and finds the original clear text.
- Only Alice could do it since she needed her private key!

Assymetric Cryptography

- How does Alice find Bob's public key?
  - Is there a directory of public keys?
  - Should she ask Bob directly?

- How can Alice be 100% sure she is talking to Bob?
  - Is she talking to the real Bob?
  - Or is it a bad guy who says he's Bob?

→ Public Key Infrastructure

Digital certificates

- Contains owner identity and public key.
- It's a standard: X.509

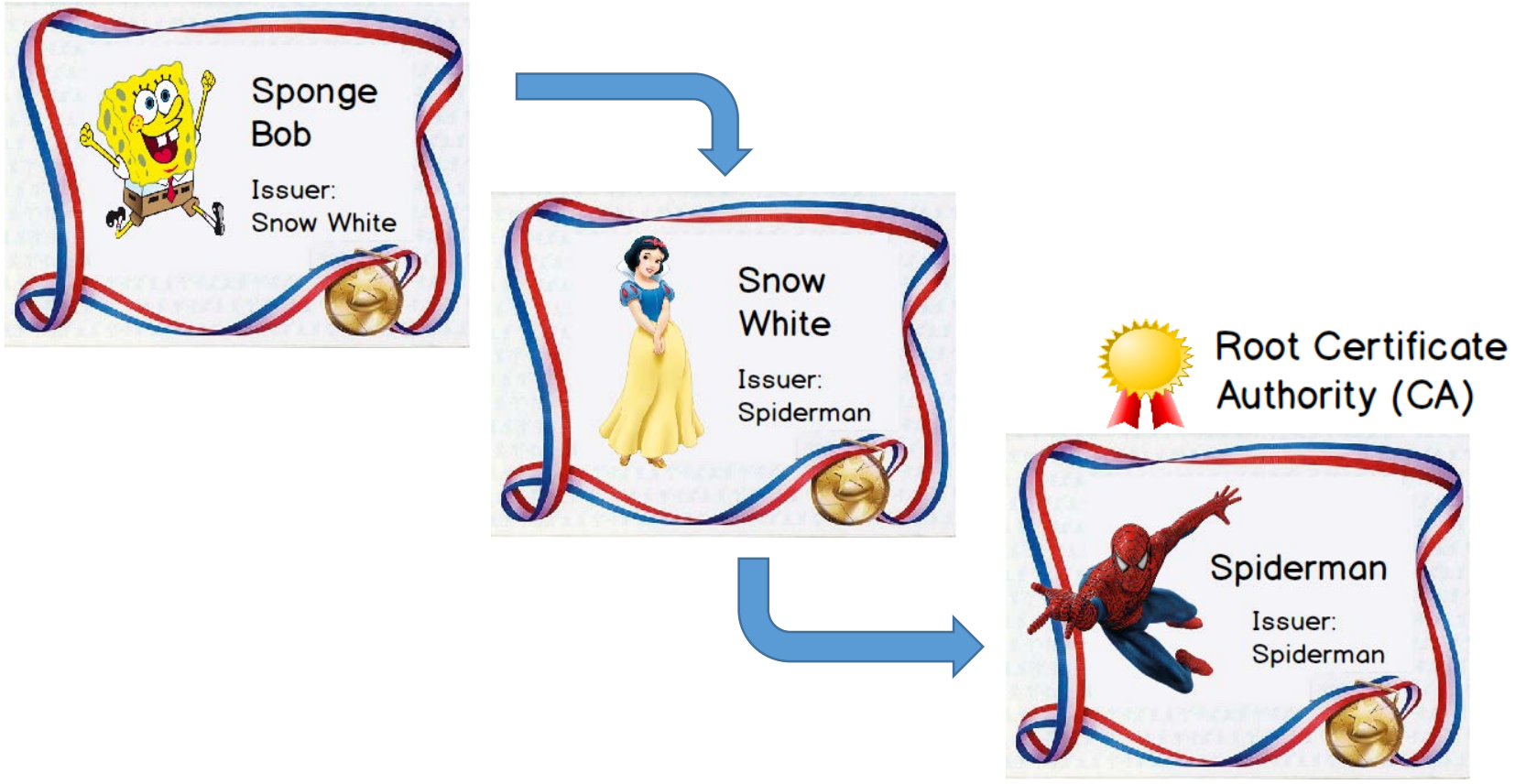
- Certifies the identity of the owner.
- How? Because it is signed by someone we trust.

- It is all based on **trusted** *root certificate authorities*.
- Chain of trust

PKI

Public Key Infrastructure

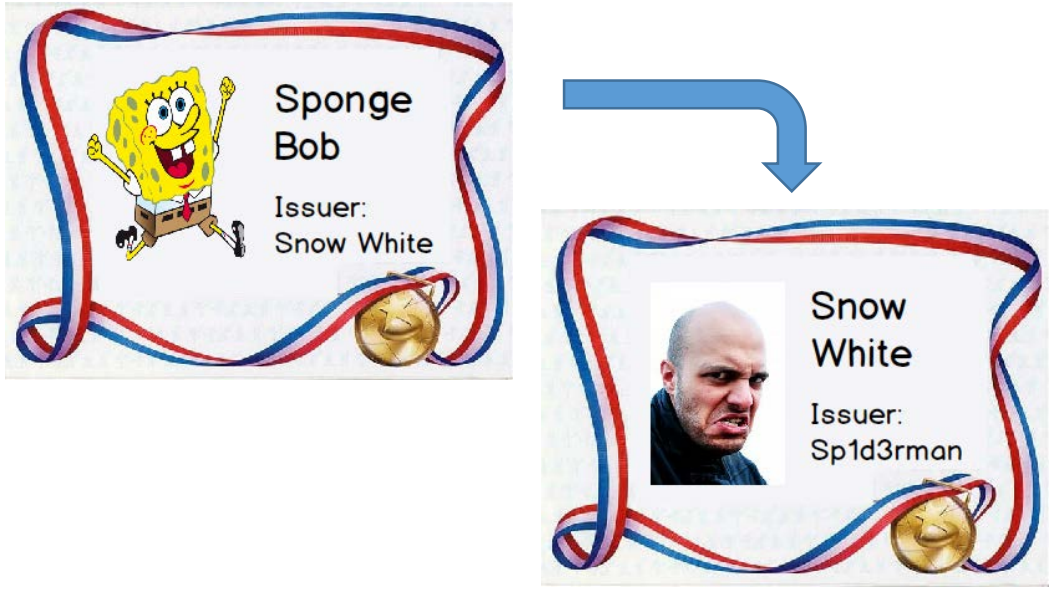
Can I trust the certificate sender?



PKI

Public Key Infrastructure

Typical threat: *Man-in-the-middle*

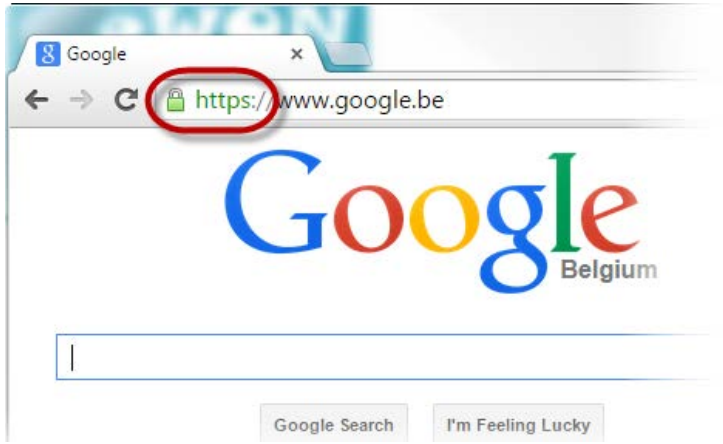


HTTPS

Secure Website

HTTPS = Secure HTTP

- eBanking & eCommerce
- Where you enter a password
- Where you enter data
  - e.g.: google
- Just everywhere!

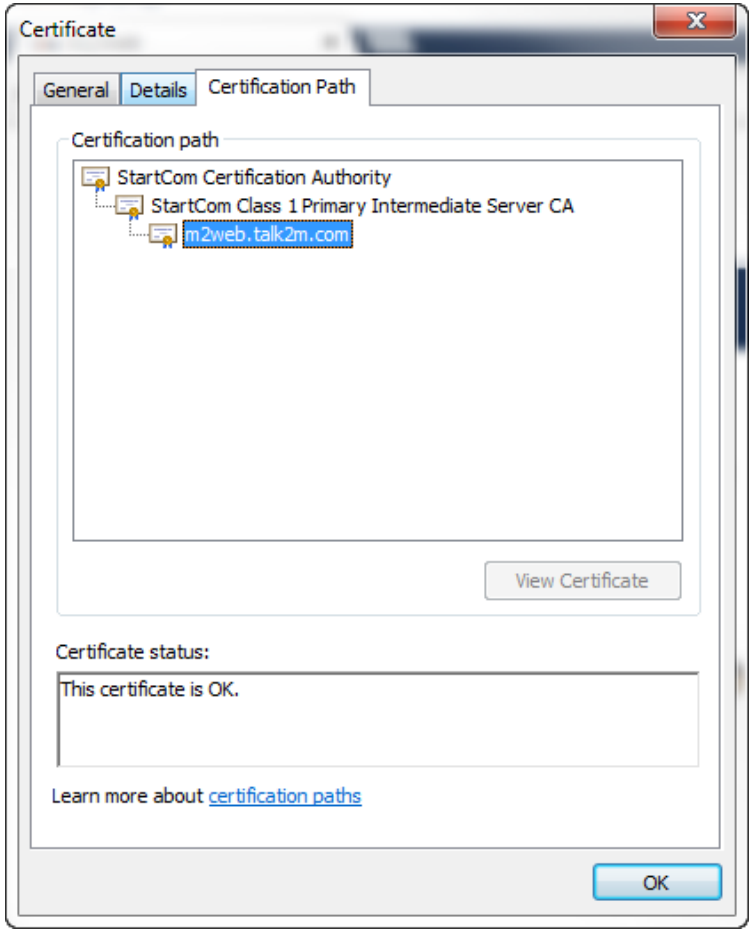


PKI

Public Key Infrastructure

Digital certificates

- Subject
  - Common Name
  - Company
  - …
- Validity period
- Your public key
- Your signature
- Issuer



SSL: The usual security protocol

- HTTPS = Secure HTTP = HTTP using SSL
- OpenVPN = private networking protected by SSL
- SSH = Secure SHell: Remote console access to servers.
- E-mail,…

- SSL invented by Netscape in 1995.
- Soon evolved into a standard (TLS) but remains widely known as *SSL*
- Current version is TLS 1.2.

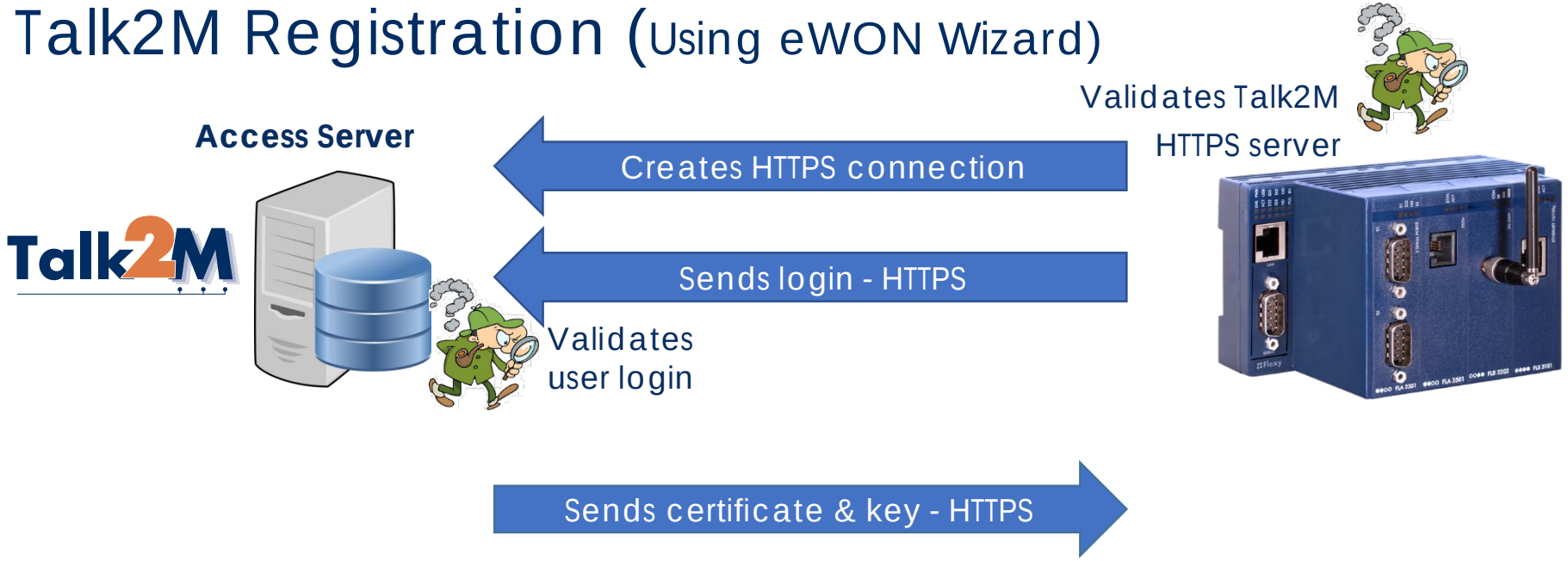
SSL config of Apache Web Server

/etc/httpd/conf.d/mywebsite.conf:

```
<VirtualHost www.example.com:443>
  ServerName www.example.com

  SSLEngine               on

  SSLCertificateFile      /etc/pki/tls/certs/www.example.com.cer
  SSLCertificateKeyFile   /etc/pki/tls/private/www.example.com.key
  SSLCACertificateFile    /etc/pki/tls/certs/ca-bundle.pem

  SSLProtocol             all -SSLv2 -SSLv3
  SSLCipherSuite          ECDHE-RSA-AES128-GCM-SHA256:…
  SSLHonorCipherOrder     on

  DocumentRoot /var/www/www.example.com
  …
```

OpenVPN/eWON

1. Talk2M Registration (Using eWON Wizard)



Talk2M creates the certificate of each eWON (and server)

VPN: Self-signed certificates

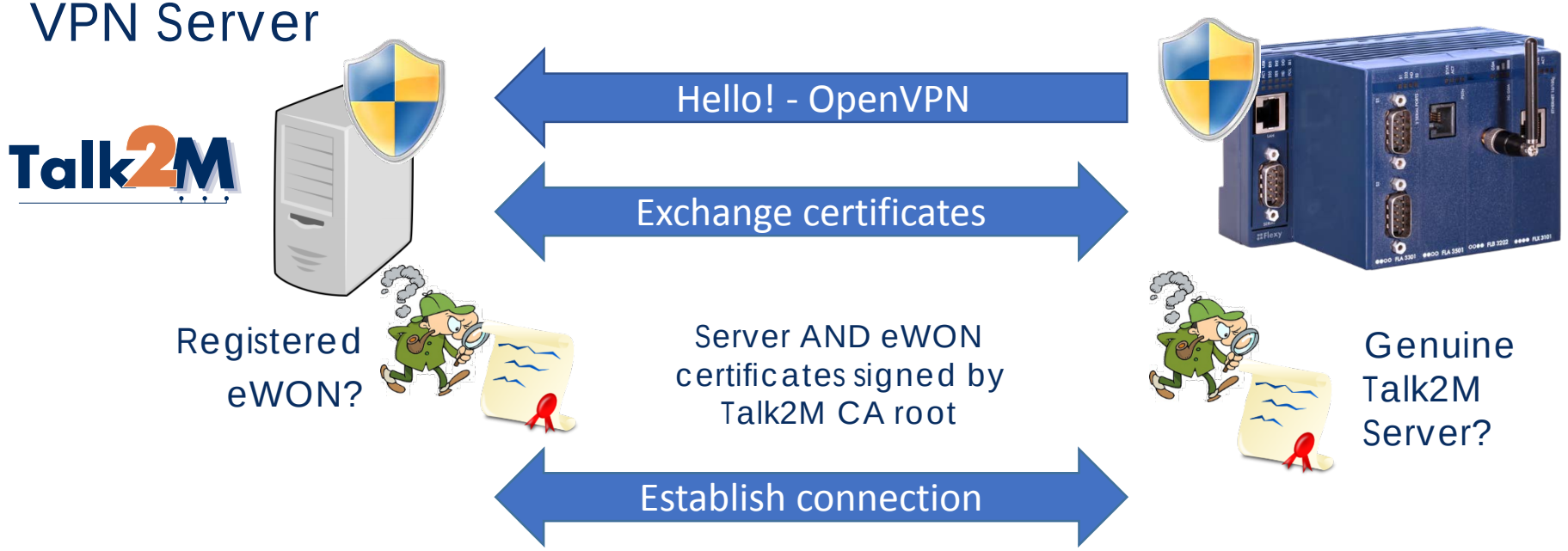
All parties receive their cert from a common authority (Here: Talk2M)

Ensures that all parties are members of the same club!

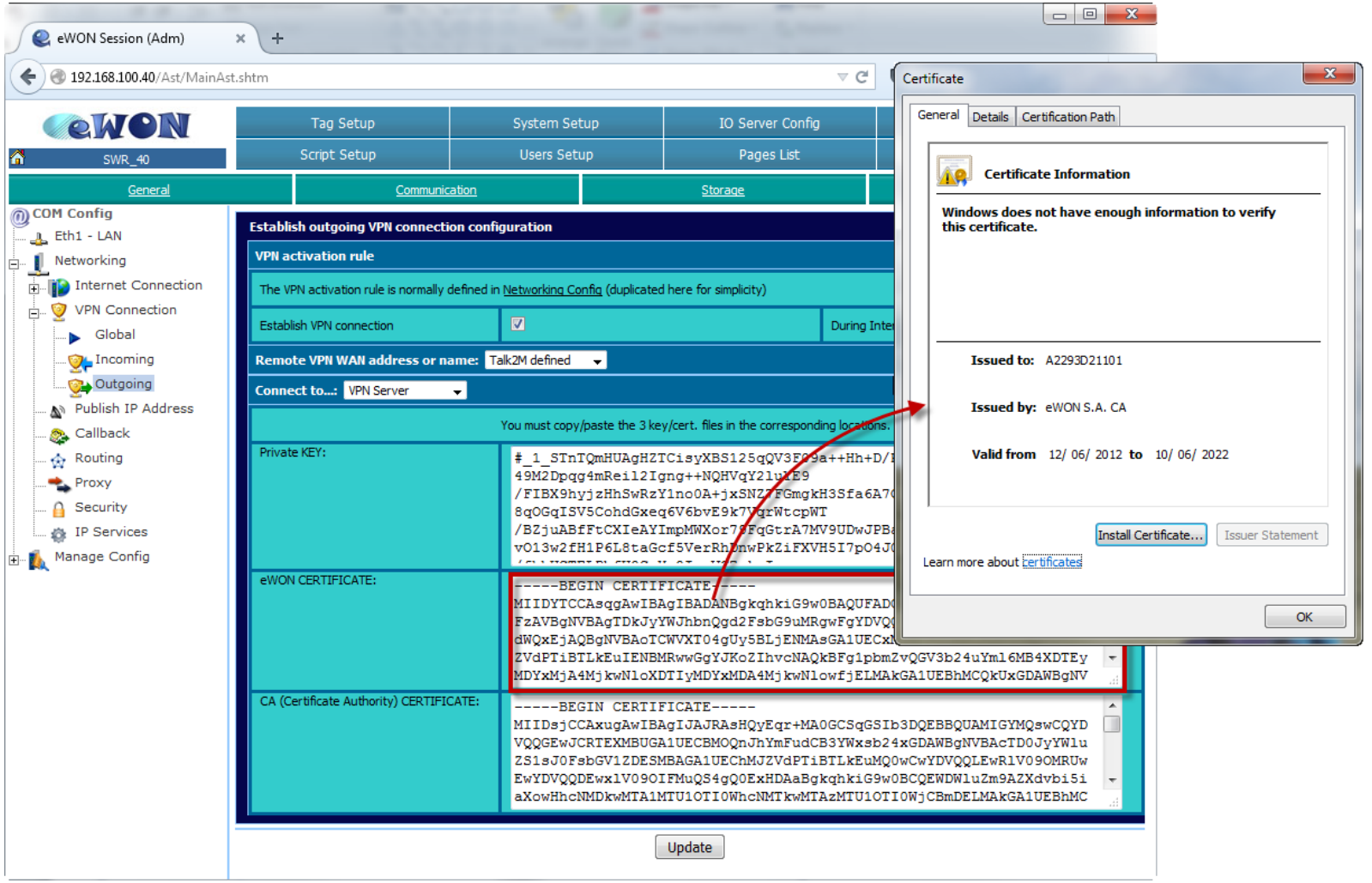
The certificate is the membership card of the Talk2M club

2. VPN Connection

eWON connects to Talk2M



OpenVPN/eWON



Connecting Devices™

Secure Connections

- Encryption : Hide the message from the bad guys
- Authentication : Make sure who you talk to

- Digital certificates for your secure website:
  - Buy from Verisign, Thawte, GoDaddy, StartSSL,...

- Protect your passwords!
- Do not keep default passwords
  - adm/adm

Thank you!

Connecting Devices™