AIRHEADS
2013

Practical Cryptography, Certificates, and 802.1X

Jon Green
Rich Langston
November 2012

ARUBA networks

#airheadsconf

Today's Goals

- **Give a *basic* background in cryptography and public key infrastructure**
  - What is symmetric key crypto?
  - What is asymmetric key crypto?
  - What are certificates and PKI?
- **Show how to use public certs with our controller**
- **Show how these two come together to create 802.1x**

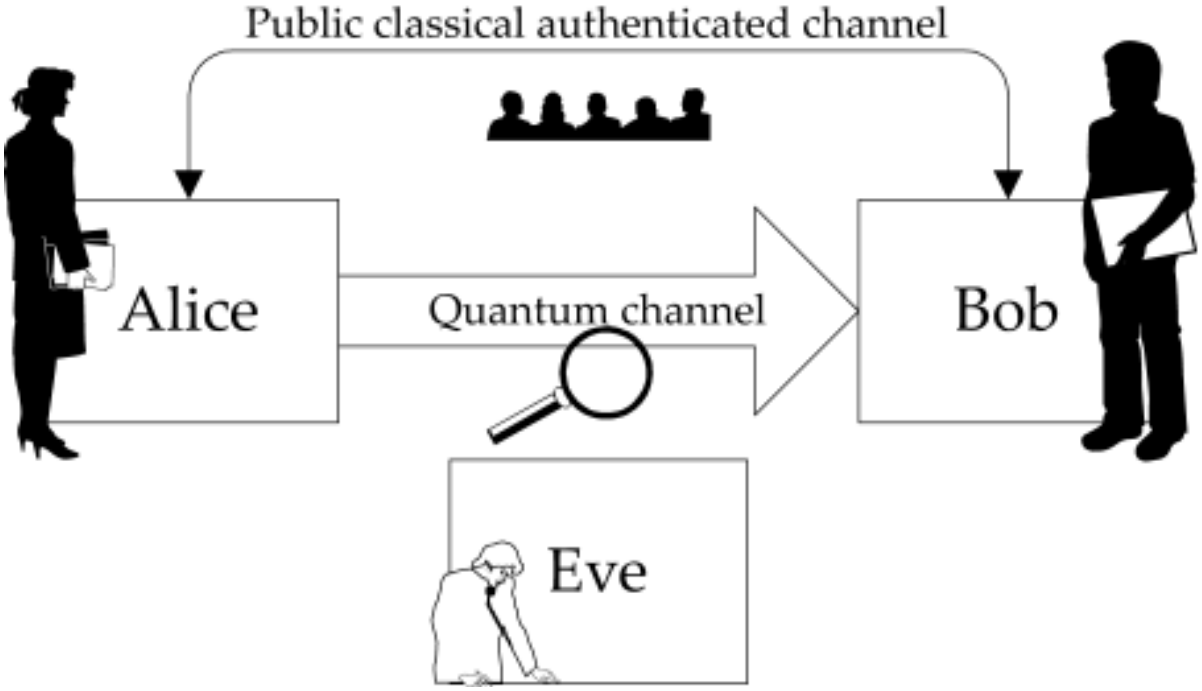
Cryptography Primer

Terminology

- ***Plain text*** **is normal, unencrypted text**
- **A *Cipher* is an encryption technique**
- ***Cipher Text*** **is the unreadable output on the Cypher**

Meet Bob and Alice

- **Bob and Alice are traditionally used in examples of cryptography**



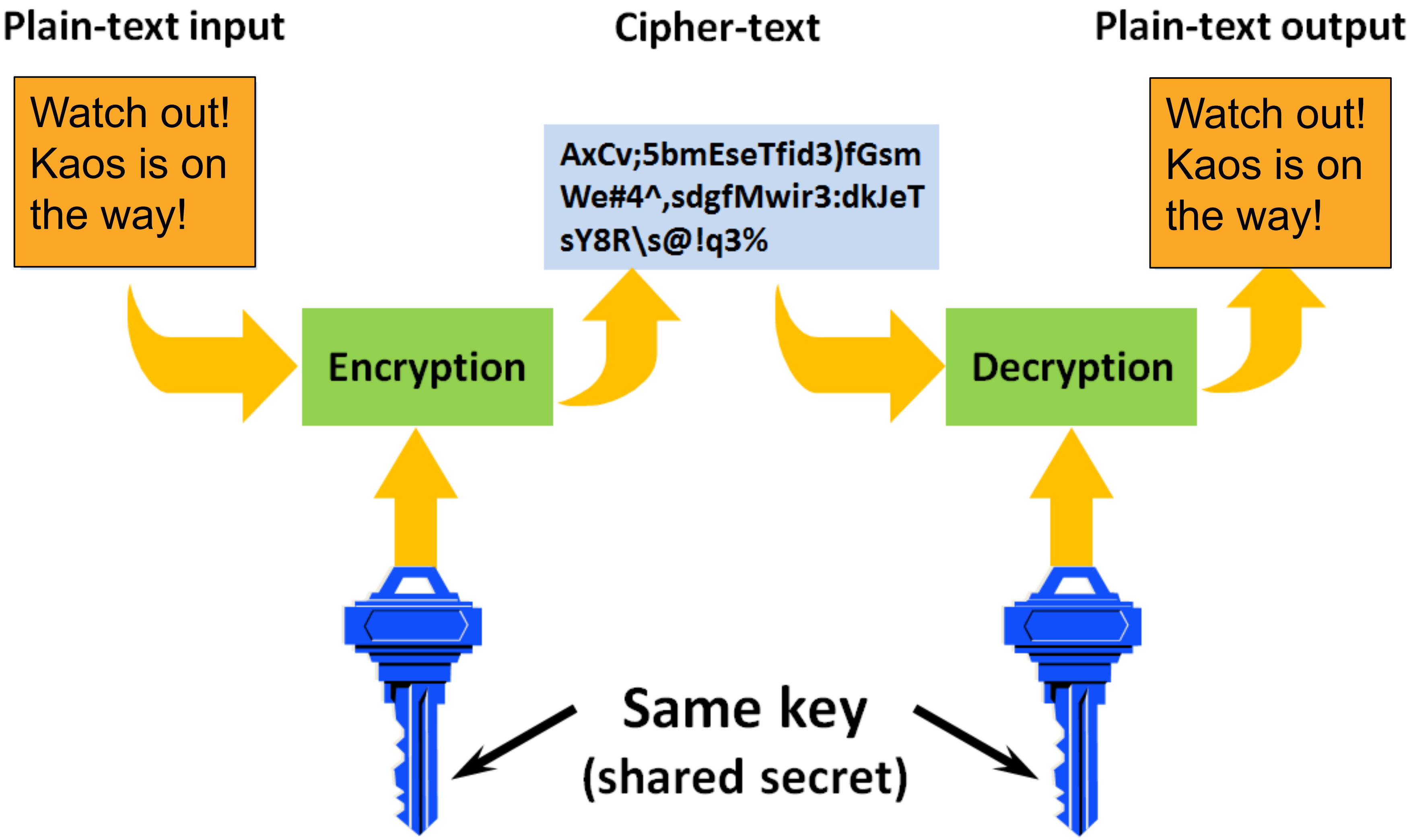
Meet The New Bob, Alice, and Eve

Max, aka “Bob”

Agent 99, aka “Alice”

Konrad of Kaos, aka “Eve”

Symmetric Key Cryptography



Plain-text input

Cipher-text

Plain-text output

Watch out! Kaos is on the way!

AxCv;5bmEseTfid3)fGsm
We#4^,sdgfMwir3:dkJeT
sY8R\s@!q3%

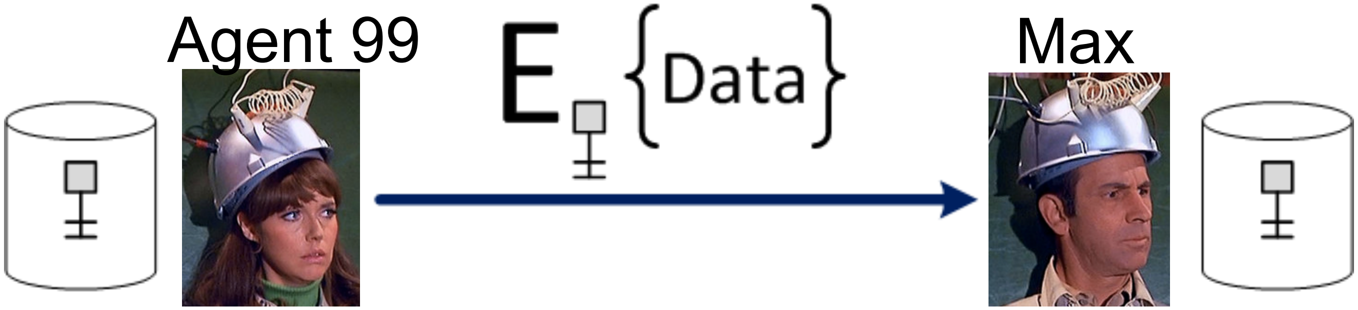
Watch out! Kaos is on the way!

Encryption

Decryption

Same key
(shared secret)

Symmetric Key Cryptography (2)



Agent 99

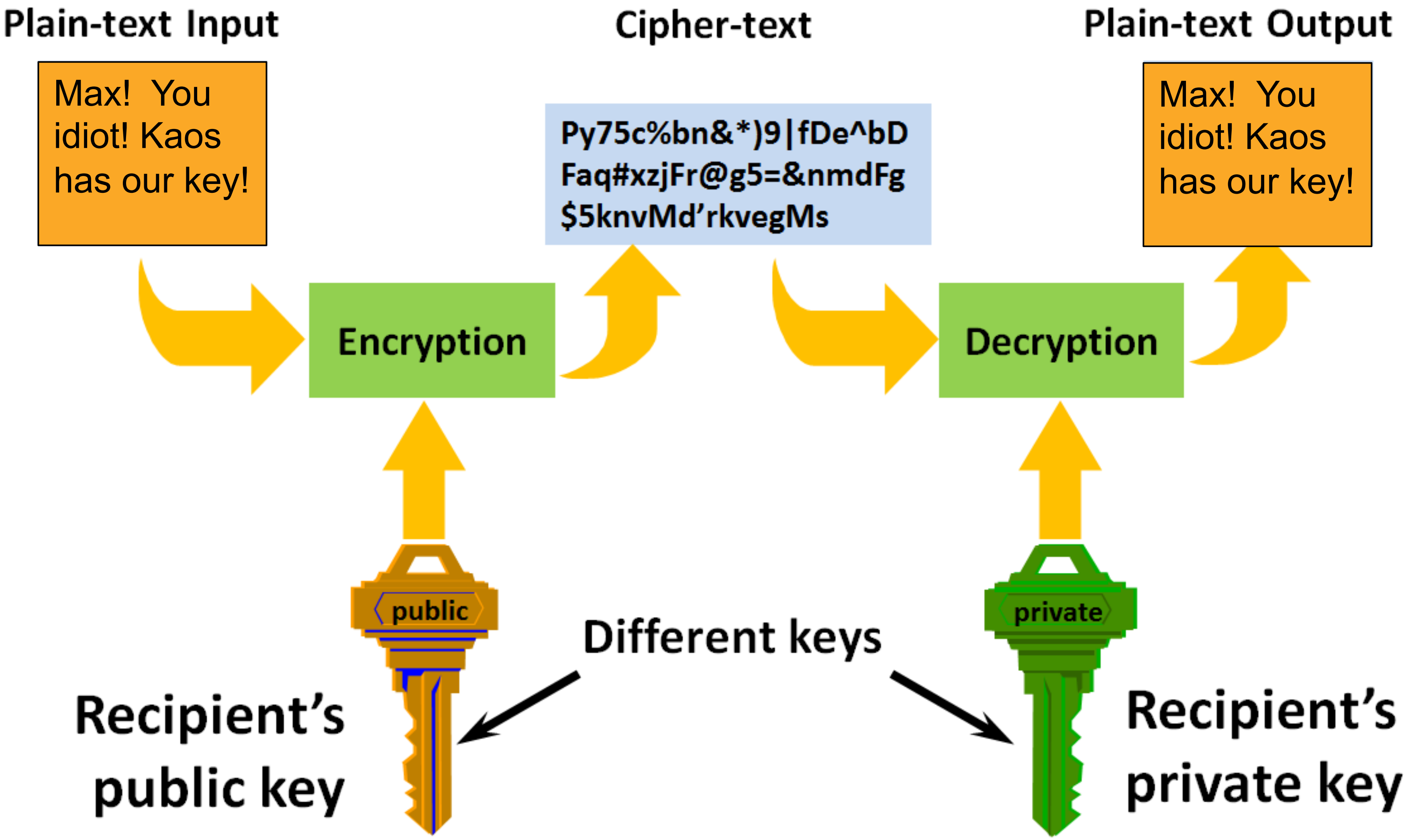
E {Data}

Max

- Strength:
  - Simple and very fast (order of 1000 to 10000 faster than asymmetric mechanisms)
- Weakness:
  - Must agree the key beforehand
  - How to securely pass the key to the other party?
- Examples: AES, 3DES, DES, RC4
- AES is the current “gold standard” for security

Public Key Cryptography (Asymmetric)

AIRHEADS 2013



Plain-text Input

Max! You idiot! Kaos has our key!

Cipher-text

Py75c%bn&*)9|fDe^bD
Faq#xzjFr@g5=&nmdFg
$5knvMd’rkvegMs

Plain-text Output

Max! You idiot! Kaos has our key!

Encryption

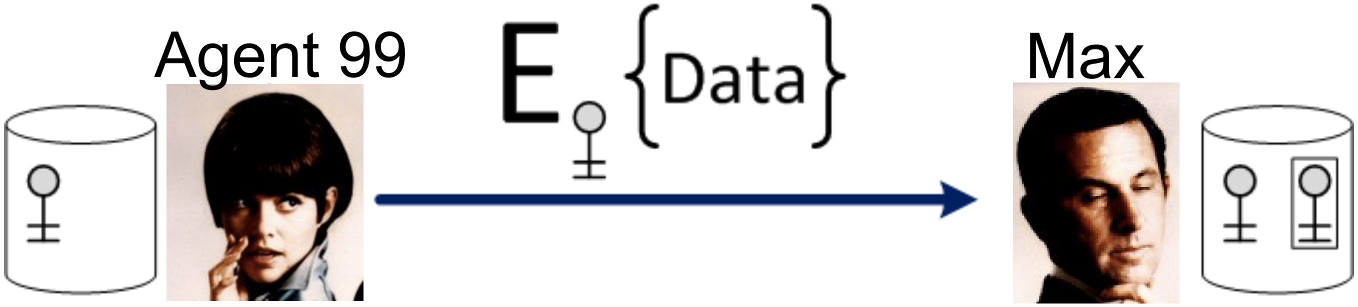
Decryption

Different keys

Recipient’s public key

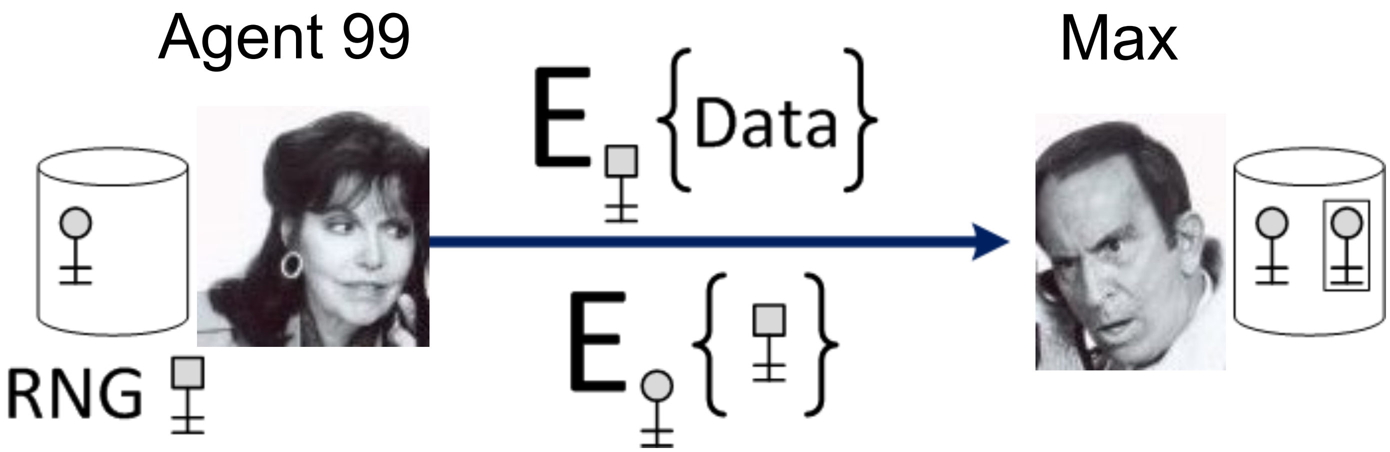
Recipient’s private key

Public Key Cryptography (2)



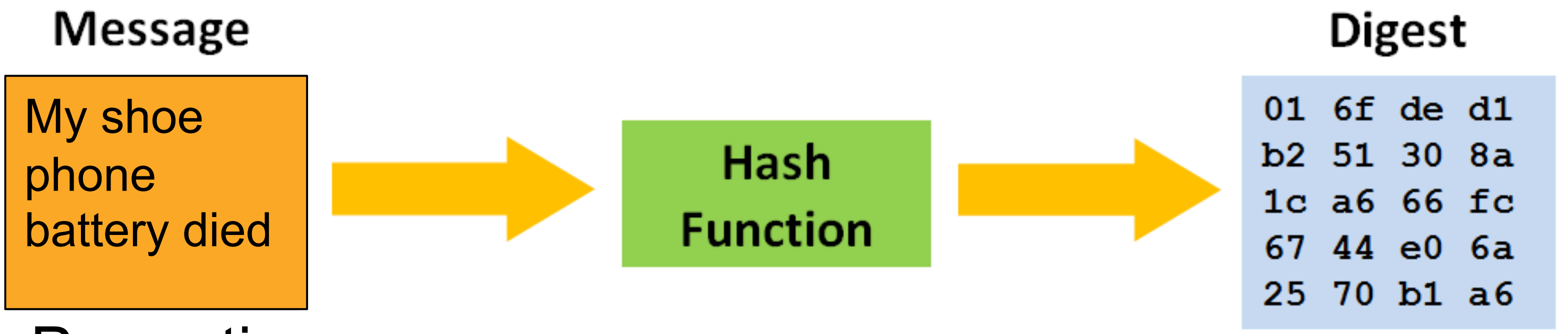
- Strength
  - Solves problem of passing the key – Anyone can use the public key to encrypt a message, but only recipient can decrypt
  - Allows establishment of trust context between parties
- Weakness:
  - Slow (MUCH slower than symmetric)
  - Problem of trusting public key (what if I've never met you?)
- Examples: RSA, DSA, ECDSA

Hybrid Cryptography



- Randomly generate “session” key
- Encrypt data with “session” key (symmetric key cryptography)
- Encrypt “session” key with recipient’s public key (public key cryptography)

Hash Function



Message

My shoe phone battery died

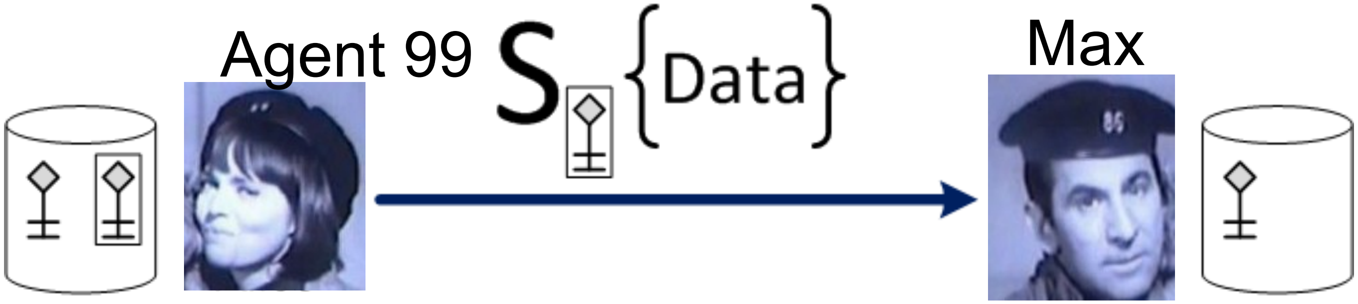
Hash Function

Digest

```
01 6f de d1
b2 51 30 8a
1c a6 66 fc
67 44 e0 6a
25 70 b1 a6
```

- Properties
  - it is easy to compute the hash value for any given message
  - it is infeasible to find a message that has a given hash
  - it is infeasible to find two different messages with the same hash
  - it is infeasible to modify a message without changing its hash
- Ensures message integrity
- Also called message digests or fingerprints
- Examples: MD5, SHA1, SHA2 (256/384/512)

Digital Signature



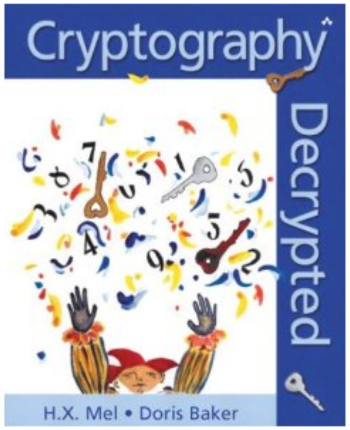
- Combines a hash with an asymmetric crypto algorithm
- The sender's private key is used in the digital signature operation
- Digital signature calculation:

$$S_{\text{⚿}}\{\text{Data}\} == \text{Data} + \underbrace{E_{\text{⚿}}\{H(\text{Data})\}}_{\text{Digital Signature}}$$

Summary: Security Building Blocks

- **Encryption provides**
  - confidentiality, can provide authentication and integrity protection
- **Checksums/hash algorithms provide**
  - integrity protection, can provide authentication
- **Digital signatures provide**
  - authentication, integrity protection, and non-repudiation
- **For more info:**

Buy this Book!



Cryptography Decrypted [Paperback]

H. X. Mel (Author), Doris M. Baker (Author)

★★★★☆ (39 customer reviews)

List Price: ~~$54.99~~

Price: $38.36 & this item ships for **FREE with Super Saver Shipping**. Details

You Save: $16.63 (30%)

Only 15 left in stock (more on the way).

Ships from and sold by **Amazon.com**. Gift-wrap available.

Want it delivered Wednesday, October 31? Order it in the next 21 hours and 46 minutes, ar

33 new from $30.00 43 used from $14.88

FREE TWO-DAY SHIPPING FOR COLLEGE STUDENTS

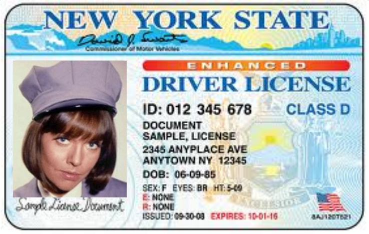
Learn more amazonstudent

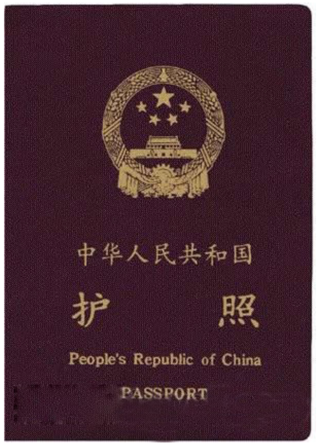
Certificates, Trust & PKI

You have to decide who you trust before you decide what to believe

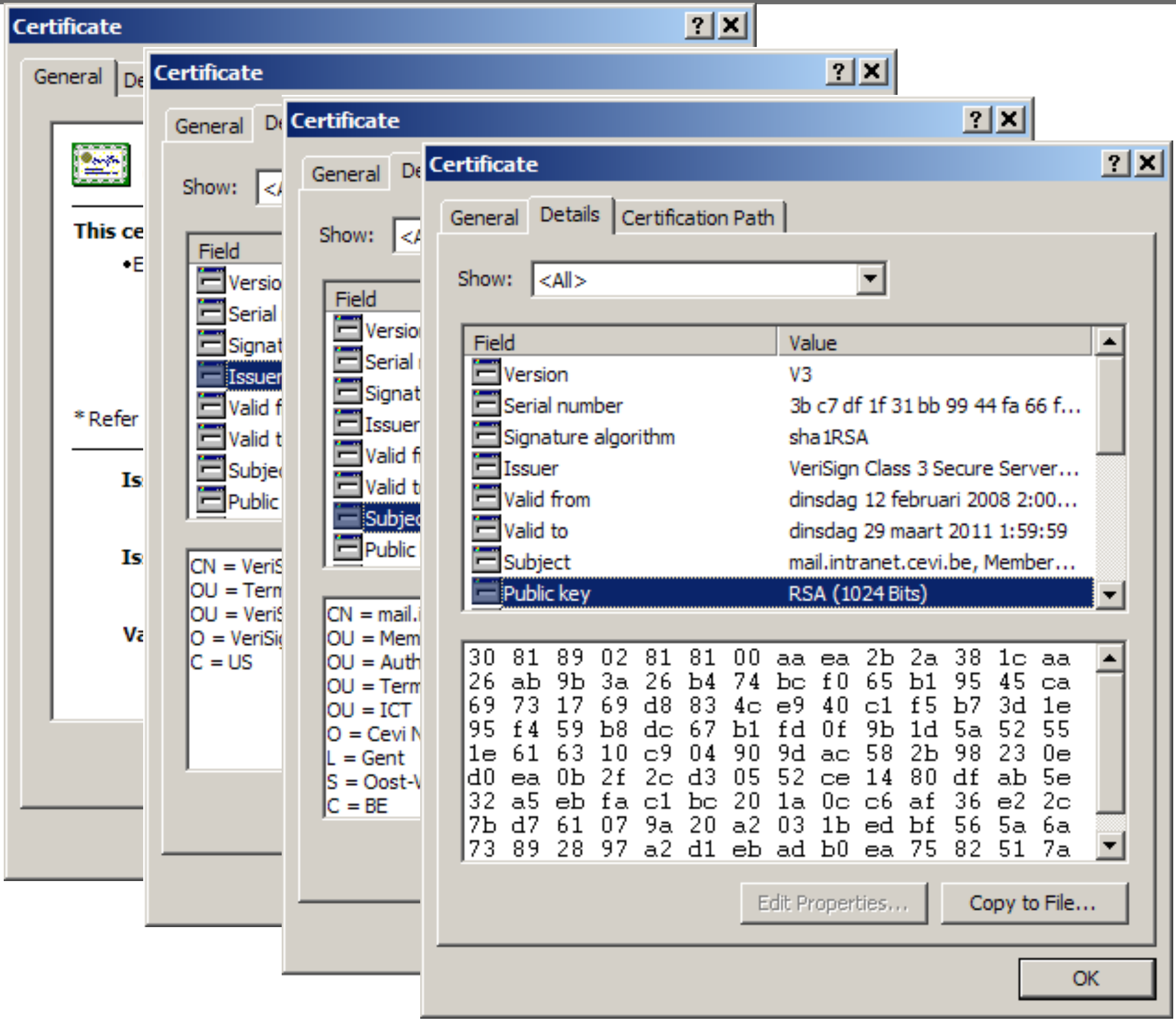
What is a Certificate?

- A certificate is a digitally signed statement that binds a public key to some identifying information
  - The signer of the certificate is called its issuer
  - The entity talked about in the certificate is the subject of the certificate
- Certificates in the real world
  - Any type of license, government-issued ID's, membership cards, ...
  - Binds an identity to certain rights, privileges, or other identifiers





What is a Certificate? (2)



Show: <All>

Field	Value
Version	V3
Serial number	3b c7 df 1f 31 bb 99 44 fa 66 f...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Secure Server...
Valid from	dinsdag 12 februari 2008 2:00...
Valid to	dinsdag 29 maart 2011 1:59:59
Subject	mail.intranet.cevi.be, Member...
Public key	RSA (1024 Bits)

```
30 81 89 02 81 81 00 aa ea 2b 2a 38 1c aa
26 ab 9b 3a 26 b4 74 bc f0 65 b1 95 45 ca
69 73 17 69 d8 83 4c e9 40 c1 f5 b7 3d 1e
95 f4 59 b8 dc 67 b1 fd 0f 9b 1d 5a 52 55
1e 61 63 10 c9 04 90 9d ac 58 2b 98 23 0e
d0 ea 0b 2f 2c d3 05 52 ce 14 80 df ab 5e
32 a5 eb fa c1 bc 20 1a 0c c6 af 36 e2 2c
7b d7 61 07 9a 20 a2 03 1b ed bf 56 5a 6a
73 89 28 97 a2 d1 eb ad b0 ea 75 82 51 7a
```

CN = VeriS
OU = Term
OU = VeriS
O = VeriSig
C = US

CN = mail.i
OU = Mem
OU = Auth
OU = Term
OU = ICT
O = Cevi N
L = Gent
S = Oost-V
C = BE

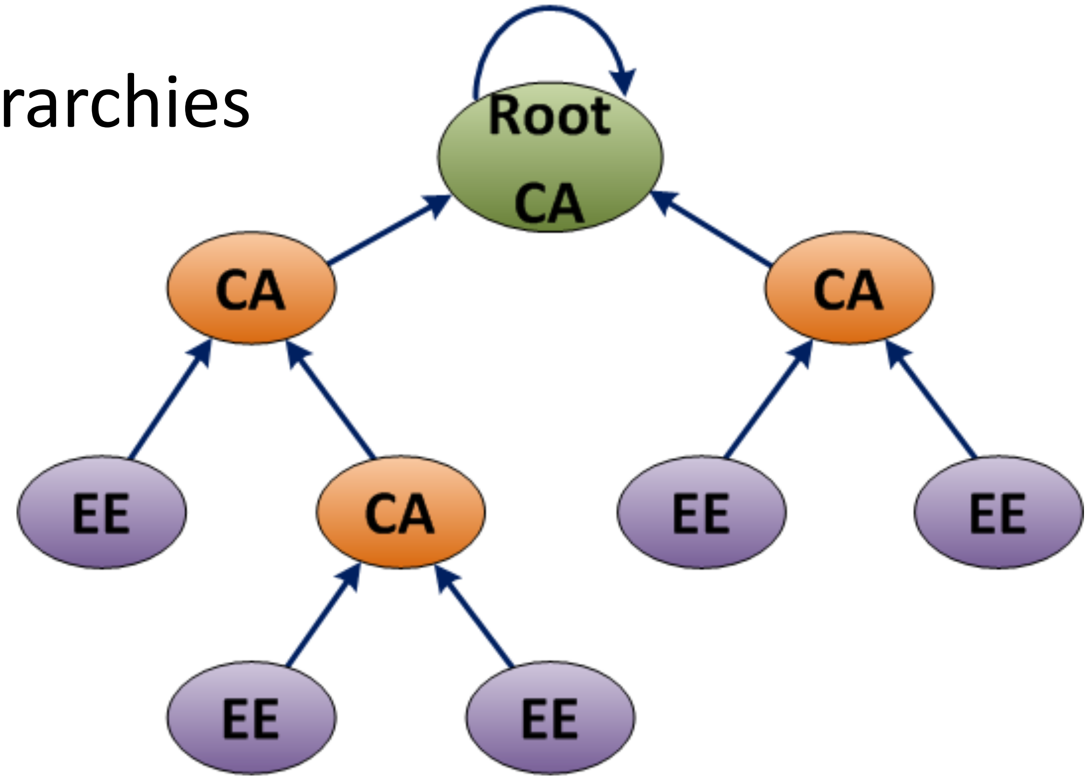
Trust Model

- Agent 99 will believe Max's public key belongs to Max **if** Agent 99 trusts the issuer of Max's certificate to make key-name binding statements
- How can we convince Agent 99 to trust the issuer of Max's certificate?
- Solution: Agent 99 must implicitly trust *some* set of public keys
  - Once she does that, those public keys can introduce other public keys to her (hierarchical model)

Public Key Infrastructure

AIRHEADS 2013

- A Certificate Authority (CA) guarantees the binding between a public key and another CA or an “End Entity” (EE)
- CA Hierarchies



Certificate Authority Best Practice

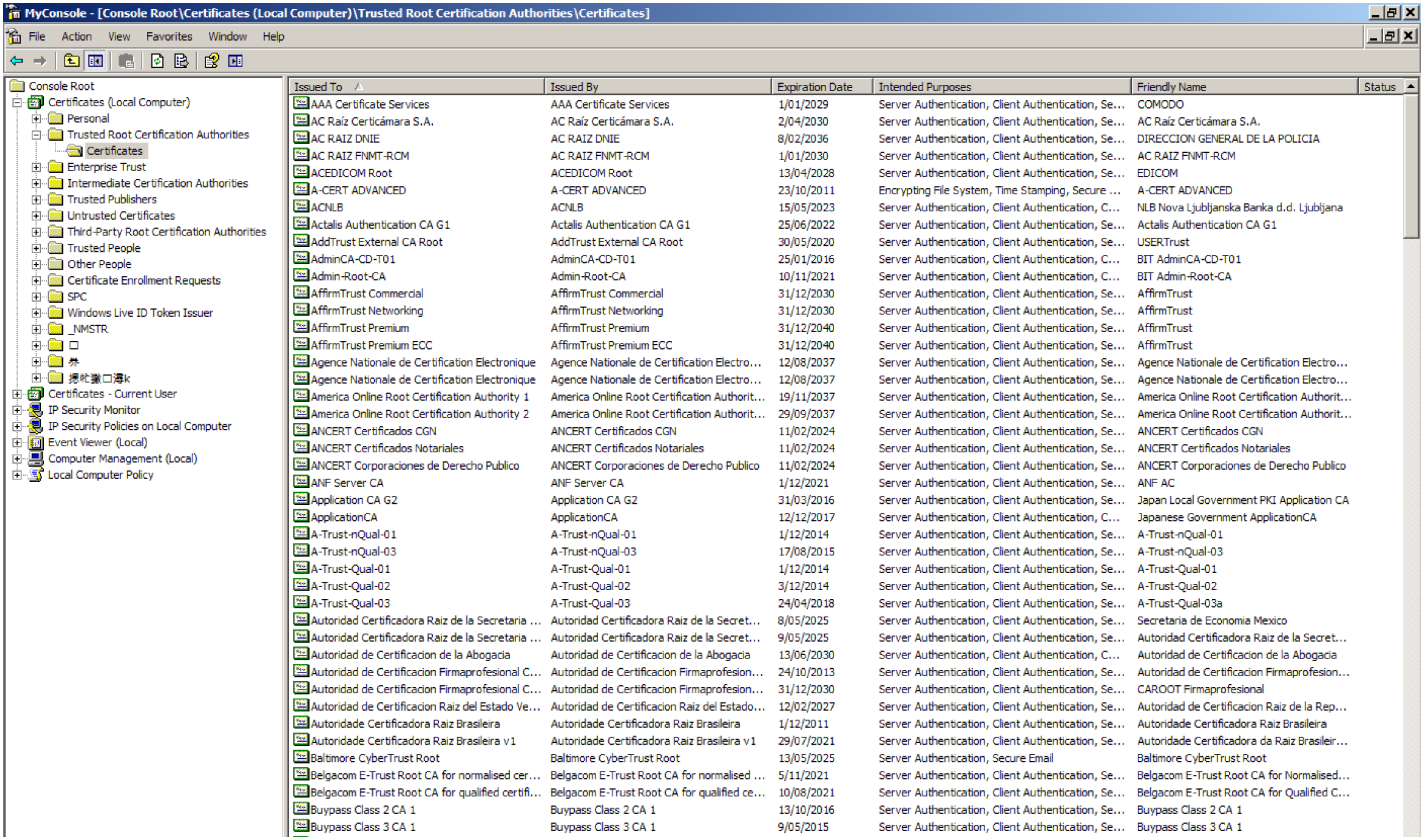
- **Normally, self-signed root CAs are created, then these create subordinate CAs**
- **Once subordinate CAs have been created, the root is taken offline**
  - If the root is compromised, the trust model is broken and the bad guys can fool you into trusting a cert that is bogus

Certificate Authority Best Practices

Symantec/VeriSign Data Center

Who do you trust?

Windows: Start->Run->certmgr.msc


MyConsole - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
Certificate Enrollment Requests
SPC
Windows Live ID Token Issuer
_NMSTR
□
Certificates - Current User
IP Security Monitor
IP Security Policies on Local Computer
Event Viewer (Local)
Computer Management (Local)
Local Computer Policy

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
AAA Certificate Services	AAA Certificate Services	1/01/2029	Server Authentication, Client Authentication, Se...	COMODO	
AC Raíz Certicámara S.A.	AC Raíz Certicámara S.A.	2/04/2030	Server Authentication, Client Authentication, Se...	AC Raíz Certicámara S.A.	
AC RAIZ DNIE	AC RAIZ DNIE	8/02/2036	Server Authentication, Client Authentication, Se...	DIRECCION GENERAL DE LA POLICIA	
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	1/01/2030	Server Authentication, Client Authentication, Se...	AC RAIZ FNMT-RCM	
ACEDICOM Root	ACEDICOM Root	13/04/2028	Server Authentication, Client Authentication, Se...	EDICOM	
A-CERT ADVANCED	A-CERT ADVANCED	23/10/2011	Encrypting File System, Time Stamping, Secure ...	A-CERT ADVANCED	
ACNLB	ACNLB	15/05/2023	Server Authentication, Client Authentication, C...	NLB Nova Ljubljanska Banka d.d. Ljubljana	
Actalis Authentication CA G1	Actalis Authentication CA G1	25/06/2022	Server Authentication, Client Authentication, Se...	Actalis Authentication CA G1	
AddTrust External CA Root	AddTrust External CA Root	30/05/2020	Server Authentication, Client Authentication, Se...	USERTrust	
AdminCA-CD-T01	AdminCA-CD-T01	25/01/2016	Server Authentication, Client Authentication, C...	BIT AdminCA-CD-T01	
Admin-Root-CA	Admin-Root-CA	10/11/2021	Server Authentication, Client Authentication, C...	BIT Admin-Root-CA	
AffirmTrust Commercial	AffirmTrust Commercial	31/12/2030	Server Authentication, Client Authentication, Se...	AffirmTrust	
AffirmTrust Networking	AffirmTrust Networking	31/12/2030	Server Authentication, Client Authentication, Se...	AffirmTrust	
AffirmTrust Premium	AffirmTrust Premium	31/12/2040	Server Authentication, Client Authentication, Se...	AffirmTrust	
AffirmTrust Premium ECC	AffirmTrust Premium ECC	31/12/2040	Server Authentication, Client Authentication, Se...	AffirmTrust	
Agence Nationale de Certification Electronique	Agence Nationale de Certification Electro...	12/08/2037	Server Authentication, Client Authentication, Se...	Agence Nationale de Certification Electro...	
Agence Nationale de Certification Electronique	Agence Nationale de Certification Electro...	12/08/2037	Server Authentication, Client Authentication, Se...	Agence Nationale de Certification Electro...	
America Online Root Certification Authority 1	America Online Root Certification Authorit...	19/11/2037	Server Authentication, Client Authentication, Se...	America Online Root Certification Authorit...	
America Online Root Certification Authority 2	America Online Root Certification Authorit...	29/09/2037	Server Authentication, Client Authentication, Se...	America Online Root Certification Authorit...	
ANCERT Certificados CGN	ANCERT Certificados CGN	11/02/2024	Server Authentication, Client Authentication, Se...	ANCERT Certificados CGN	
ANCERT Certificados Notariales	ANCERT Certificados Notariales	11/02/2024	Server Authentication, Client Authentication, Se...	ANCERT Certificados Notariales	
ANCERT Corporaciones de Derecho Publico	ANCERT Corporaciones de Derecho Publico	11/02/2024	Server Authentication, Client Authentication, Se...	ANCERT Corporaciones de Derecho Publico	
ANF Server CA	ANF Server CA	1/12/2021	Server Authentication, Client Authentication, Se...	ANF AC	
Application CA G2	Application CA G2	31/03/2016	Server Authentication, Client Authentication, Se...	Japan Local Government PKI Application CA	
ApplicationCA	ApplicationCA	12/12/2017	Server Authentication, Client Authentication, C...	Japanese Government ApplicationCA	
A-Trust-nQual-01	A-Trust-nQual-01	1/12/2014	Server Authentication, Client Authentication, Se...	A-Trust-nQual-01	
A-Trust-nQual-03	A-Trust-nQual-03	17/08/2015	Server Authentication, Client Authentication, Se...	A-Trust-nQual-03	
A-Trust-Qual-01	A-Trust-Qual-01	1/12/2014	Server Authentication, Client Authentication, Se...	A-Trust-Qual-01	
A-Trust-Qual-02	A-Trust-Qual-02	3/12/2014	Server Authentication, Client Authentication, Se...	A-Trust-Qual-02	
A-Trust-Qual-03	A-Trust-Qual-03	24/04/2018	Server Authentication, Client Authentication, Se...	A-Trust-Qual-03a	
Autoridad Certificadora Raiz de la Secretaria ...	Autoridad Certificadora Raiz de la Secret...	8/05/2025	Server Authentication, Client Authentication, Se...	Secretaria de Economia Mexico	
Autoridad Certificadora Raiz de la Secretaria ...	Autoridad Certificadora Raiz de la Secret...	9/05/2025	Server Authentication, Client Authentication, Se...	Autoridad Certificadora Raiz de la Secret...	
Autoridad de Certificacion de la Abogacia	Autoridad de Certificacion de la Abogacia	13/06/2030	Server Authentication, Client Authentication, C...	Autoridad de Certificacion de la Abogacia	
Autoridad de Certificacion Firmaprofesional C...	Autoridad de Certificacion Firmaprofesion...	24/10/2013	Server Authentication, Client Authentication, Se...	Autoridad de Certificacion Firmaprofesion...	
Autoridad de Certificacion Firmaprofesional C...	Autoridad de Certificacion Firmaprofesion...	31/12/2030	Server Authentication, Client Authentication, Se...	CAROOT Firmaprofesional	
Autoridad de Certificacion Raiz del Estado Ve...	Autoridad de Certificacion Raiz del Estado...	12/02/2027	Server Authentication, Client Authentication, Se...	Autoridad de Certificacion Raiz de la Rep...	
Autoridade Certificadora Raiz Brasileira	Autoridade Certificadora Raiz Brasileira	1/12/2011	Server Authentication, Client Authentication, Se...	Autoridade Certificadora Raiz Brasileira	
Autoridade Certificadora Raiz Brasileira v1	Autoridade Certificadora Raiz Brasileira v1	29/07/2021	Server Authentication, Client Authentication, Se...	Autoridade Certificadora da Raiz Brasileir...	
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Server Authentication, Secure Email	Baltimore CyberTrust Root	
Belgacom E-Trust Root CA for normalised cer...	Belgacom E-Trust Root CA for normalised ...	5/11/2021	Server Authentication, Client Authentication, Se...	Belgacom E-Trust Root CA for Normalised...	
Belgacom E-Trust Root CA for qualified certifi...	Belgacom E-Trust Root CA for qualified ce...	10/08/2021	Server Authentication, Client Authentication, Se...	Belgacom E-Trust Root CA for Qualified C...	
Buypass Class 2 CA 1	Buypass Class 2 CA 1	13/10/2016	Server Authentication, Client Authentication, Se...	Buypass Class 2 CA 1	
Buypass Class 3 CA 1	Buypass Class 3 CA 1	9/05/2015	Server Authentication, Client Authentication, Se...	Buypass Class 3 CA 1	

Public CA versus Private CA

- **Windows Server includes a domain-aware CA – why not just use it?**

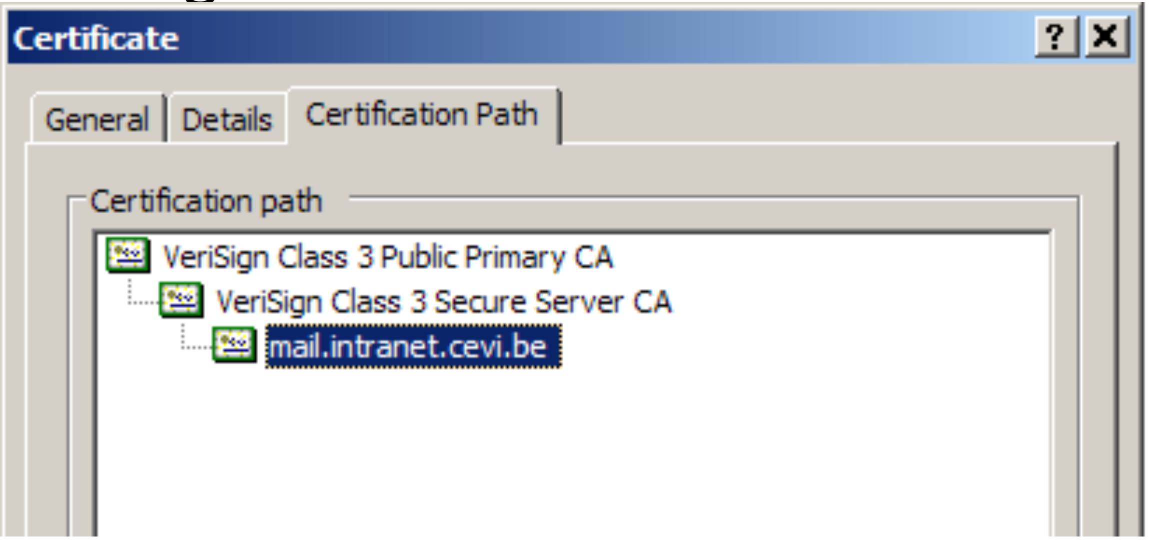
- **Disadvantages:**
  - PKI is complex. Might be easier to let Verisign/Thawte/etc. do it for you.
  - *Nobody outside your Windows domain will trust your certificates*
- **Advantages:**
  - Less costly
  - Better security possible. Low chances of someone outside organization getting a certificate from your internal PKI

ClearPass as a CA

- **Only intended for BYOD – not a general-purpose CA**
  - No Web enrollment interface
  - No manual enrollment interface
  - Limited (BYOD-focused) policy controls
- **Recommendation: Use for deploying BYOD certs which have limited applicability**
  - Valid for WLAN access to a limited access zone
  - Not valid for other enterprise services (email, VPN, app sign-on, etc.)

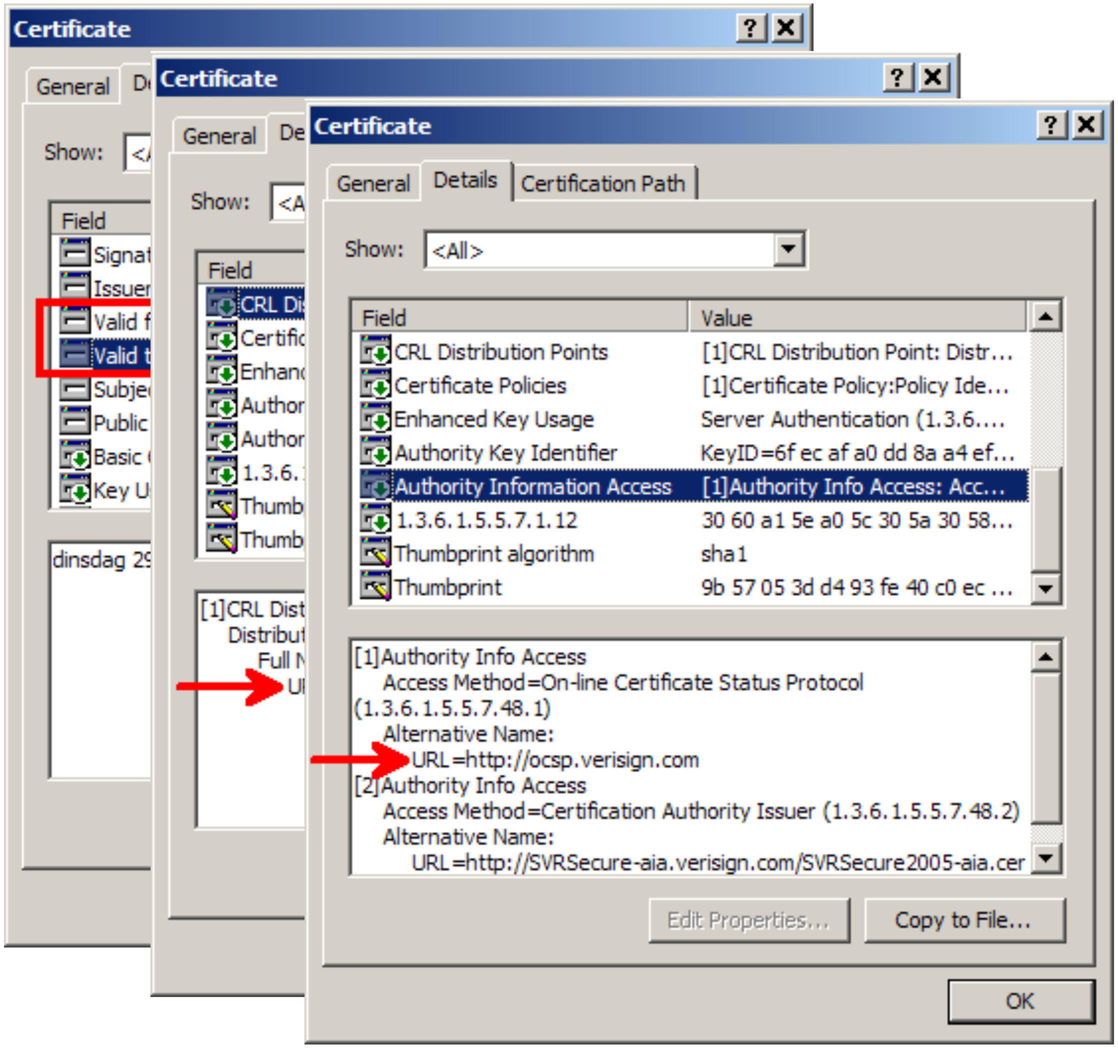
Public Key Infrastructure (3)

- Agent Agent 99 trusts Max's public key if there is a valid chain of certificates from Max's public key to a root CA that Agent 99 implicitly trusts
  - Web browsers also check DNS hostname == certificate Common Name (CN)
- Chain Building & Validation



VeriSign Class 3 Public Primary CA
VeriSign Class 3 Secure Server CA
mail.intranet.cevi.be

Certificate Validity



Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Enhanced Key Usage	Server Authentication (1.3.6....
Authority Key Identifier	KeyID=6f ec af a0 dd 8a a4 ef...
Authority Information Access	[1]Authority Info Access: Acc...
1.3.6.1.5.5.7.1.12	30 60 a1 5e a0 5c 30 5a 30 58...
Thumbprint algorithm	sha1
Thumbprint	9b 57 05 3d d4 93 fe 40 c0 ec ...

```
[1]Authority Info Access
     Access Method=On-line Certificate Status Protocol
(1.3.6.1.5.5.7.48.1)
     Alternative Name:
          URL=http://ocsp.verisign.com
[2]Authority Info Access
     Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
     Alternative Name:
          URL=http://SVRSecure-aia.verisign.com/SVRSecure2005-aia.cer
```

Good to Know: Apple TV

- With the latest version of Apple TV iOS, WPA2 Enterprise can be used
- However, the Apple TV does not have a clock
- So when it is rebooted, it thinks it is January, 1970, aka the “epoch”
- It will not authenticate successfully because it will not trust the network’s cert is valid
- NTP must complete first to fix the time

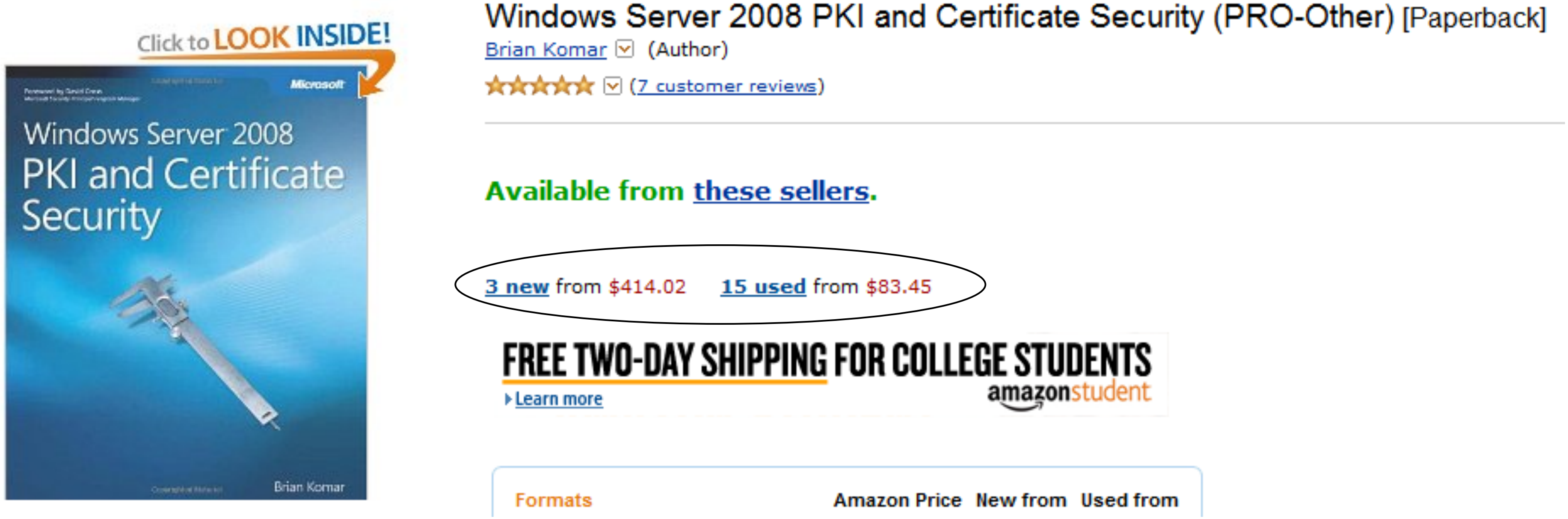
OCSP

- **Can be used by the *client* (e.g. web browser) to verify server's certificate validity**
  - OCSP URL is read from server certificate's AIA field
- **Can be used by the *server* (e.g. mobility controller) to verify client's certificate validity**
  - OCSP URL is most often configured on the server to point to specific OCSP responders
- **OCSP transactions use HTTP for transport protocol**
- **Important: Nonce Extension required for replay prevention**
  - Some public CAs don't like this…

OCSP – Two Variants

- **OCSP Direct Trust Model**
  - Each OCSP responder has an OCSP Responder certificate
  - Each Responder cert must be installed on relying party (controller)
  - ArubaOS only supports a single Responder cert – problem for redundancy
- **OCSP Delegated Trust Model**
  - OCSP responder has an OCSP Responder cert issued by each issuing CA for which it can respond
  - Relying party checks to see that OCSP response is signed by a known cert
  - Requires each issuing CA cert to be installed on relying party (controller) because chaining is not supported
  - Requires ArubaOS 6.1.4.1-FIPS or ArubaOS 6.3+

For More Info



Windows Server 2008 PKI and Certificate Security (PRO-Other) [Paperback]

Brian Komar (Author)

★★★★★ (7 customer reviews)

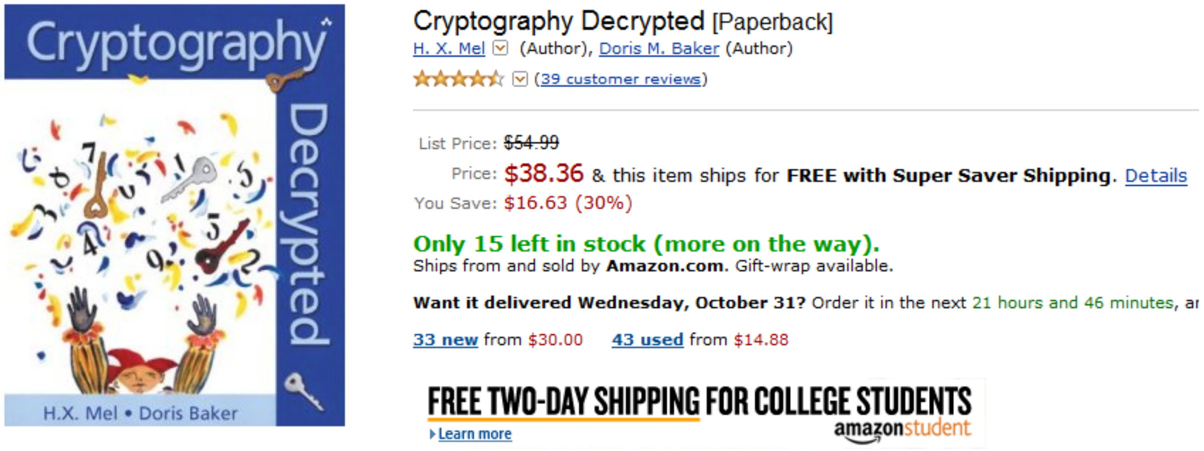
Available from these sellers.

3 new from $414.02   15 used from $83.45

FREE TWO-DAY SHIPPING FOR COLLEGE STUDENTS

Learn more   amazonstudent

Formats   Amazon Price   New from   Used from



Cryptography Decrypted [Paperback]

H. X. Mel (Author), Doris M. Baker (Author)

★★★★☆ (39 customer reviews)

List Price: ~~$54.99~~

Price: $38.36 & this item ships for FREE with Super Saver Shipping. Details

You Save: $16.63 (30%)

Only 15 left in stock (more on the way).

Ships from and sold by Amazon.com. Gift-wrap available.

Want it delivered Wednesday, October 31? Order it in the next 21 hours and 46 minutes, ar

33 new from $30.00   43 used from $14.88

FREE TWO-DAY SHIPPING FOR COLLEGE STUDENTS

Learn more   amazonstudent

Buy this Book!

Aruba Certificate Operations

Relevant Certificate Types

- **Server Certificate**
  - Used by controller to authenticate to the client (EAP-TLS, PEAP, Web)
- **CA Certificate**
  - Used by controller to validate client certificate (EAP-TLS only)
- **Client Certificate**
  - Used by client to authenticate to the network (EAP-TLS only)

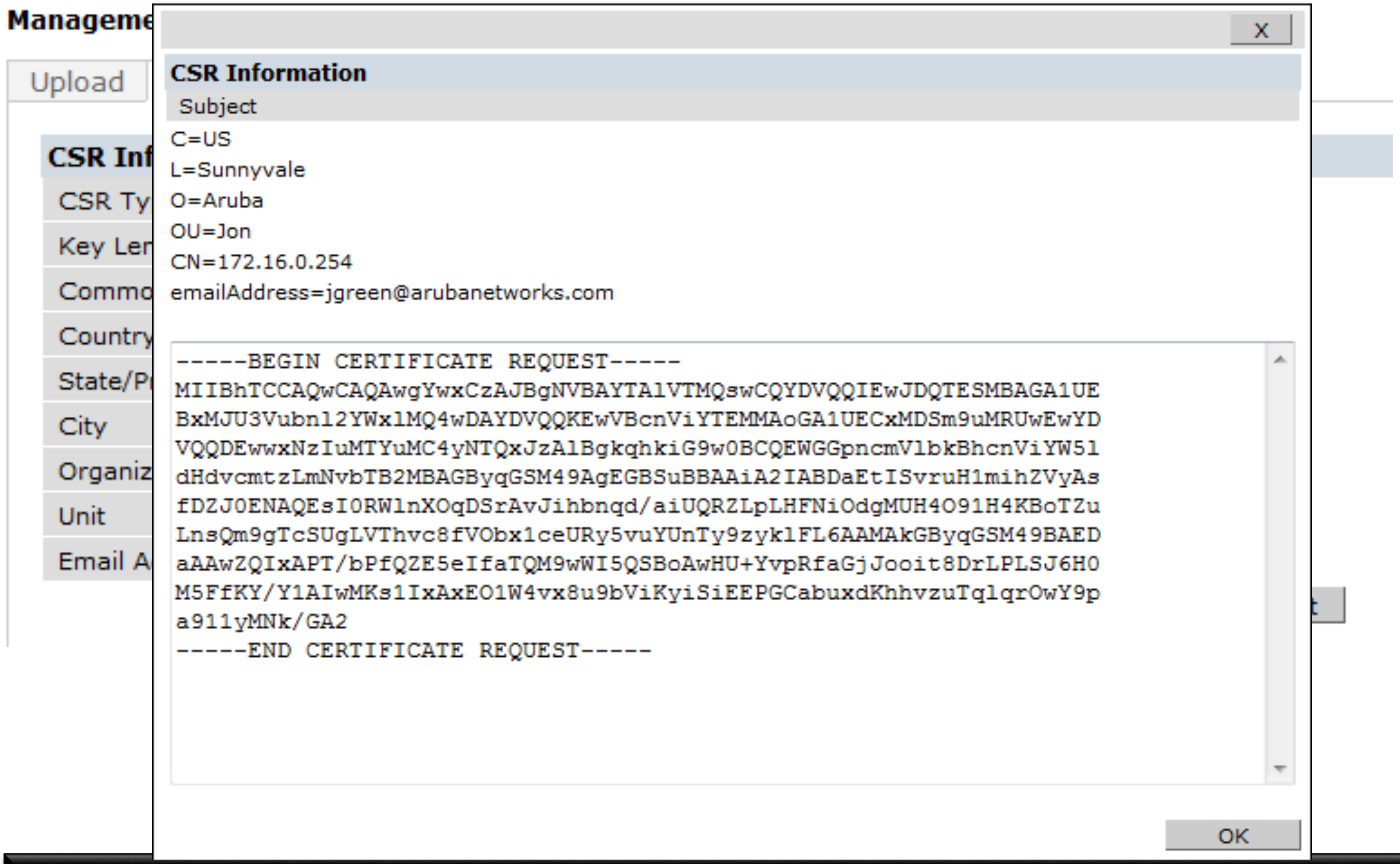
Certificate Formats

- **PEM / PKCS#7**
  - Contains a certificate in base64 encoding (open in a text editor)
- **DER**
  - Contains a certificate in binary encoding
- **PFX / PKCS#12**
  - Contains a certificate AND private key, protected by a password

Using Certificate Signing Request

- **Private key stays on controller**
- **CSR is sent to CA**
  - How this works depends on the CA type
- **CA issues certificate in PEM/CER or DER format**
- **Certificate is uploaded to controller**
- **Controller puts certificate back together with private key automatically**

Generating Certificate Signing Request



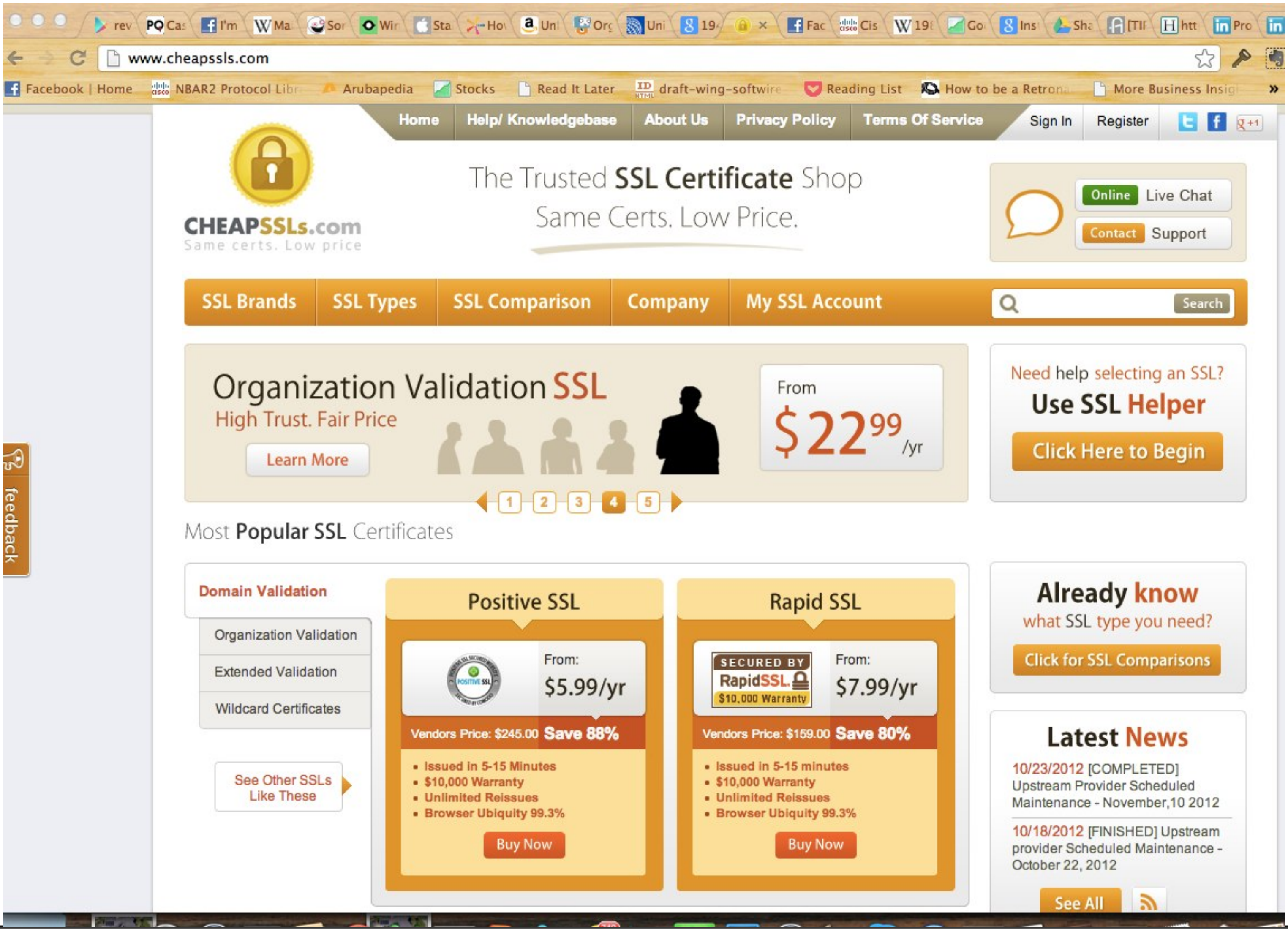
CSR Information

Subject

C=US
L=Sunnyvale
O=Aruba
OU=Jon
CN=172.16.0.254
emailAddress=jgreen@arubanetworks.com

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBhTCCAQwCAQAwgYwxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTESMBAGA1UE
BxMJU3Vubnl2YWxlMQ4wDAYDVQQKEwVBcnViYTEMMAoGA1UECxMDSm9uMRUwEwYD
VQQDEwwxNzIuMTYuMC4yNTQxJzAlBgkqhkiG9w0BCQEWGGpncmVlbkBhcnViYW5l
dHdvcmtzLmNvbTB2MBAGByqGSM49AgEGBSuBBAAiA2IABDaEtISvruH1mihZVyAs
fDZJ0ENAQEsI0RWlnXOqDSrAvJihbnqd/aiUQRZLpLHFNiOdgMUH4O91H4KBoTZu
LnsQm9gTcSUgLVThvc8fVObx1ceURy5vuYUnTy9zyklFL6AAMAkGByqGSM49BAED
aAAwZQIxAPT/bPfQZE5eIfaTQM9wWI5QSBoAwHU+YvpRfaGjJooit8DrLPLSJ6H0
M5FfKY/Y1AIwMKs1IxAxEO1W4vx8u9bViKyiSiEEPGCabuxdKhhvzuTqlqrOwY9p
a911yMNk/GA2
-----END CERTIFICATE REQUEST-----
```

Send CSR to your CA of choice



The Trusted SSL Certificate Shop
Same Certs. Low Price.

Organization Validation SSL
High Trust. Fair Price

From $22.99/yr

Need help selecting an SSL?
Use SSL Helper

Most Popular SSL Certificates

Positive SSL
From: $5.99/yr
Vendors Price: $245.00 Save 88%
- Issued in 5-15 Minutes
- $10,000 Warranty
- Unlimited Reissues
- Browser Ubiquity 99.3%

Rapid SSL
SECURED BY RapidSSL $10,000 Warranty
From: $7.99/yr
Vendors Price: $159.00 Save 80%
- Issued in 5-15 minutes
- $10,000 Warranty
- Unlimited Reissues
- Browser Ubiquity 99.3%

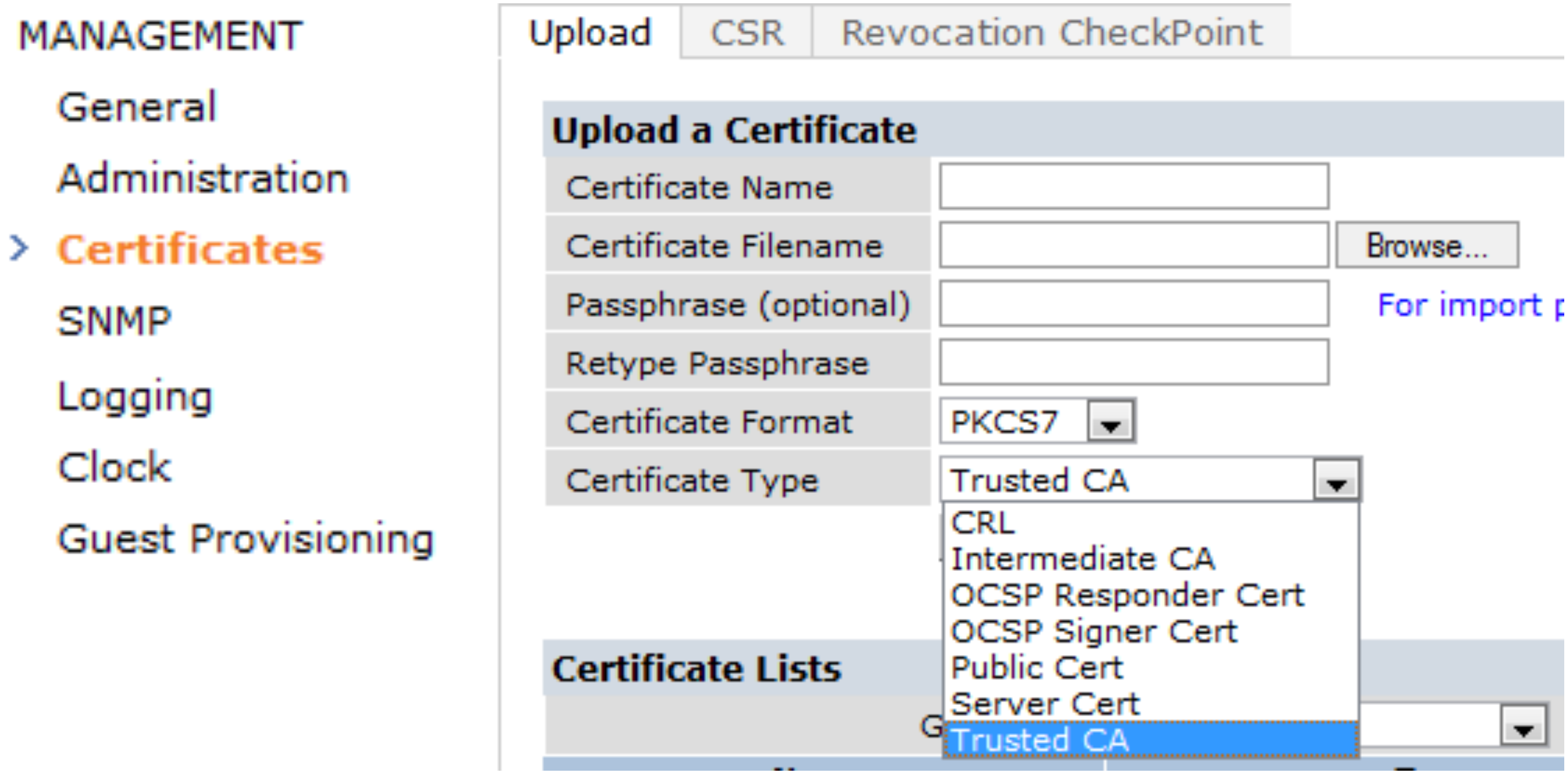
Already know what SSL type you need?

Latest News

10/23/2012 [COMPLETED] Upstream Provider Scheduled Maintenance - November,10 2012

10/18/2012 [FINISHED] Upstream provider Scheduled Maintenance - October 22, 2012

Uploading Certificates



MANAGEMENT

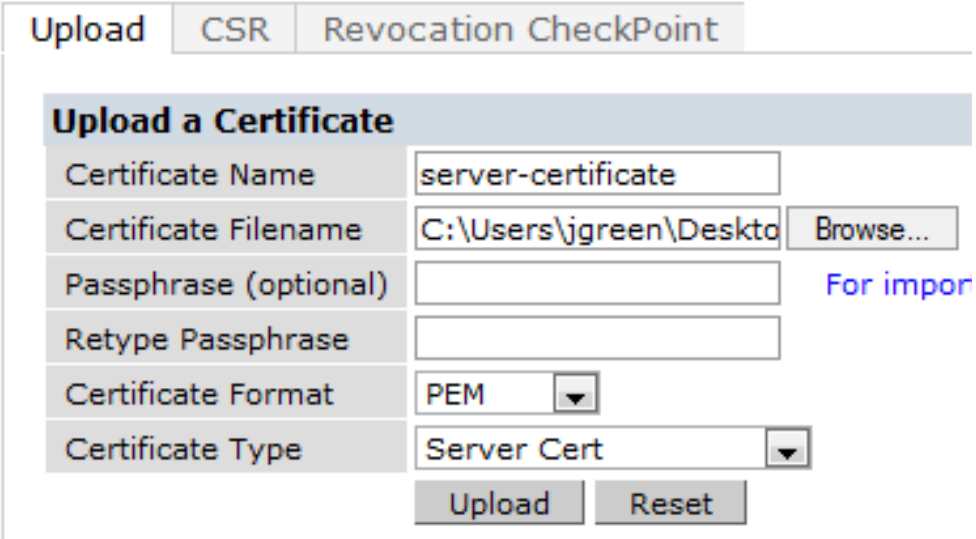
- General
- Administration
- › Certificates
- SNMP
- Logging
- Clock
- Guest Provisioning

Upload a Certificate

Certificate Name	
Certificate Filename	Browse...
Passphrase (optional)	For import p
Retype Passphrase	
Certificate Format	PKCS7
Certificate Type	Trusted CA

Certificate Lists

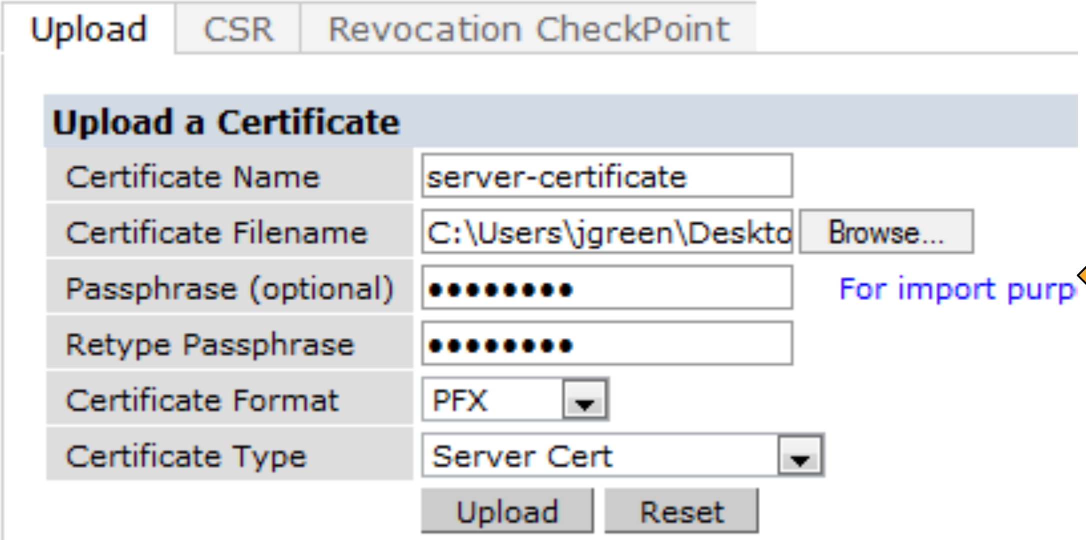
Uploading Certificate



Upload a Certificate

Certificate Name	server-certificate
Certificate Filename	C:\Users\jgreen\Deskto Browse...
Passphrase (optional)	For impor
Retype Passphrase	
Certificate Format	PEM
Certificate Type	Server Cert

Certificate only (PEM format)



Upload a Certificate

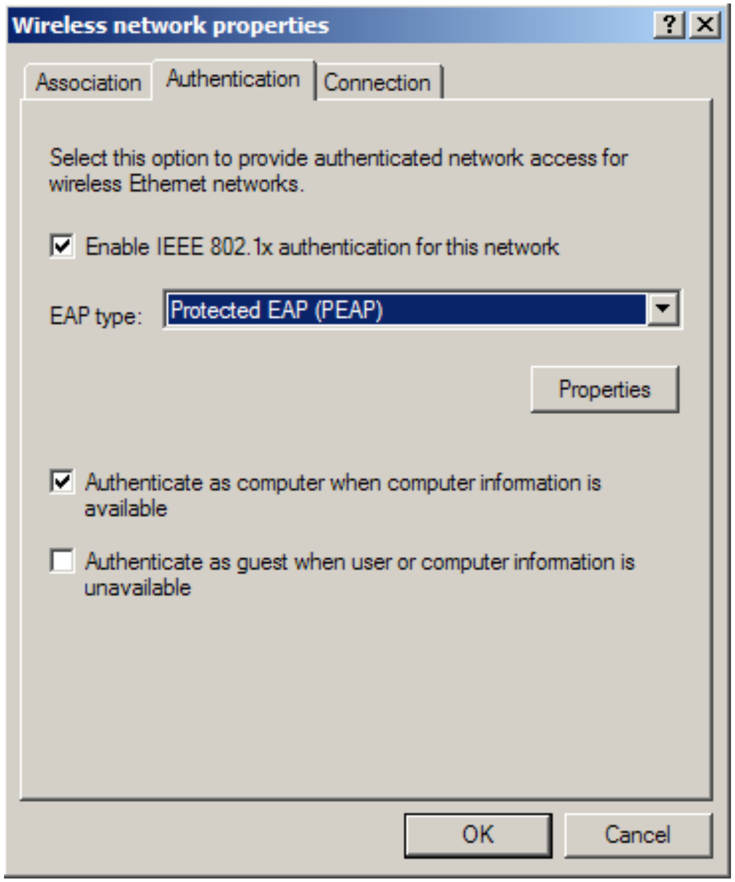
Certificate Name	server-certificate
Certificate Filename	C:\Users\jgreen\Deskto Browse...
Passphrase (optional)	●●●●●●●● For import purp
Retype Passphrase	●●●●●●●●
Certificate Format	PFX
Certificate Type	Server Cert

Certificate and private key in PFX format

Putting it all together: 802.1X

Authentication with 802.1X

- Authenticates users before granting access to L2 media
- Makes use of EAP (Extensible Authentication Protocol)
- 802.1X authentication happens at L2 – users will be authenticated before an IP address is assigned



Select this option to provide authenticated network access for wireless Ethernet networks.

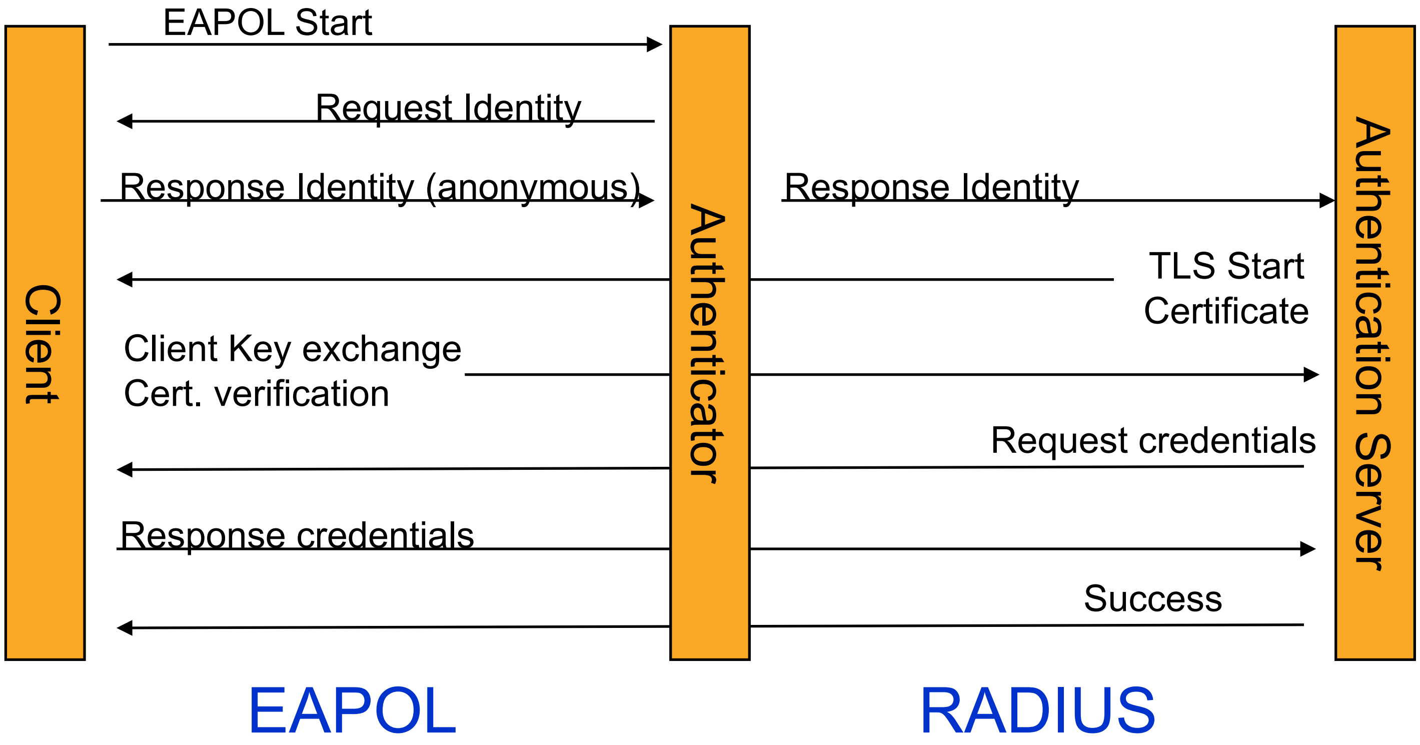
☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

Sample EAP Transaction



2-stage process

- Outer tunnel establishment
- Credential exchange happens inside the encrypted tunnel

802.1X Acronym Soup

PEAP (Protected EAP)

- Uses a digital certificate on the network side
- Password or certificate on the client side

EAP-TLS (EAP with Transport Level Security)

- Uses a certificate on network side
- Uses a certificate on client side

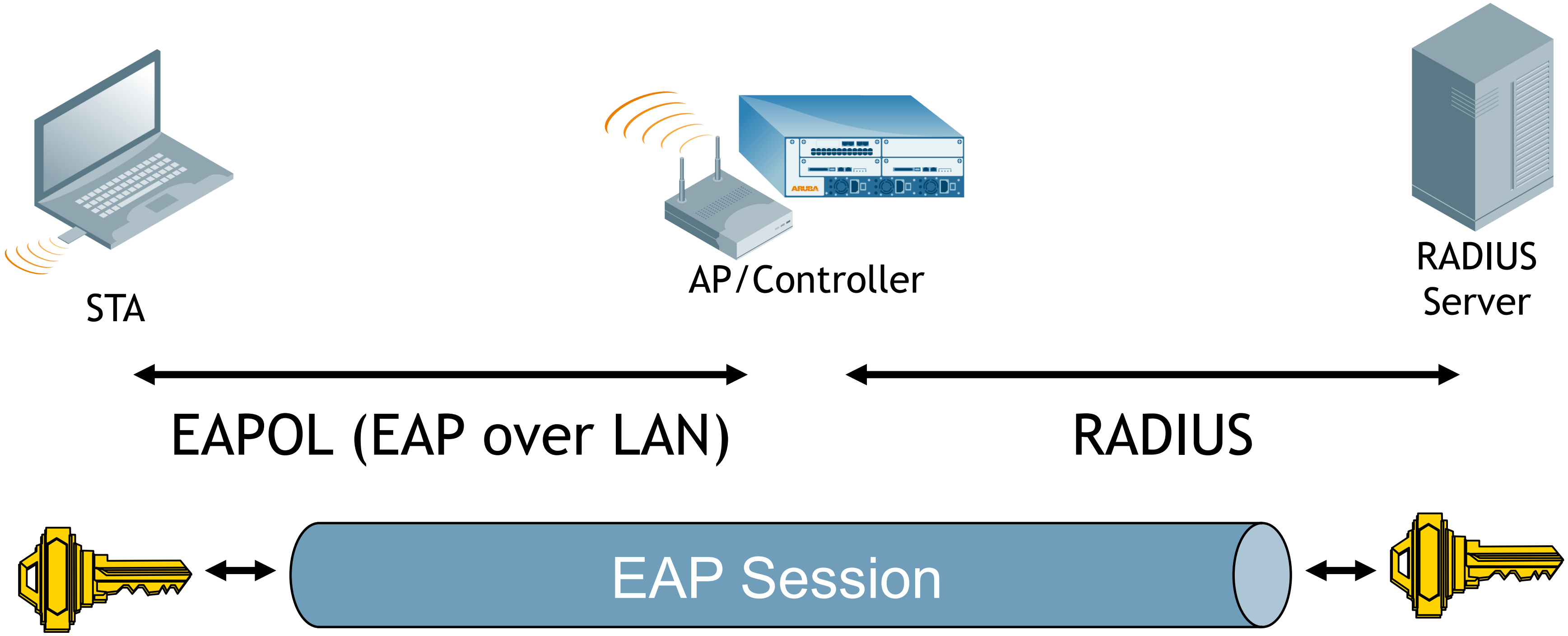
TTLS (Tunneled Transport Layer Security)

- Uses a certificate on the network side
- Password, token, or certificate on the client side

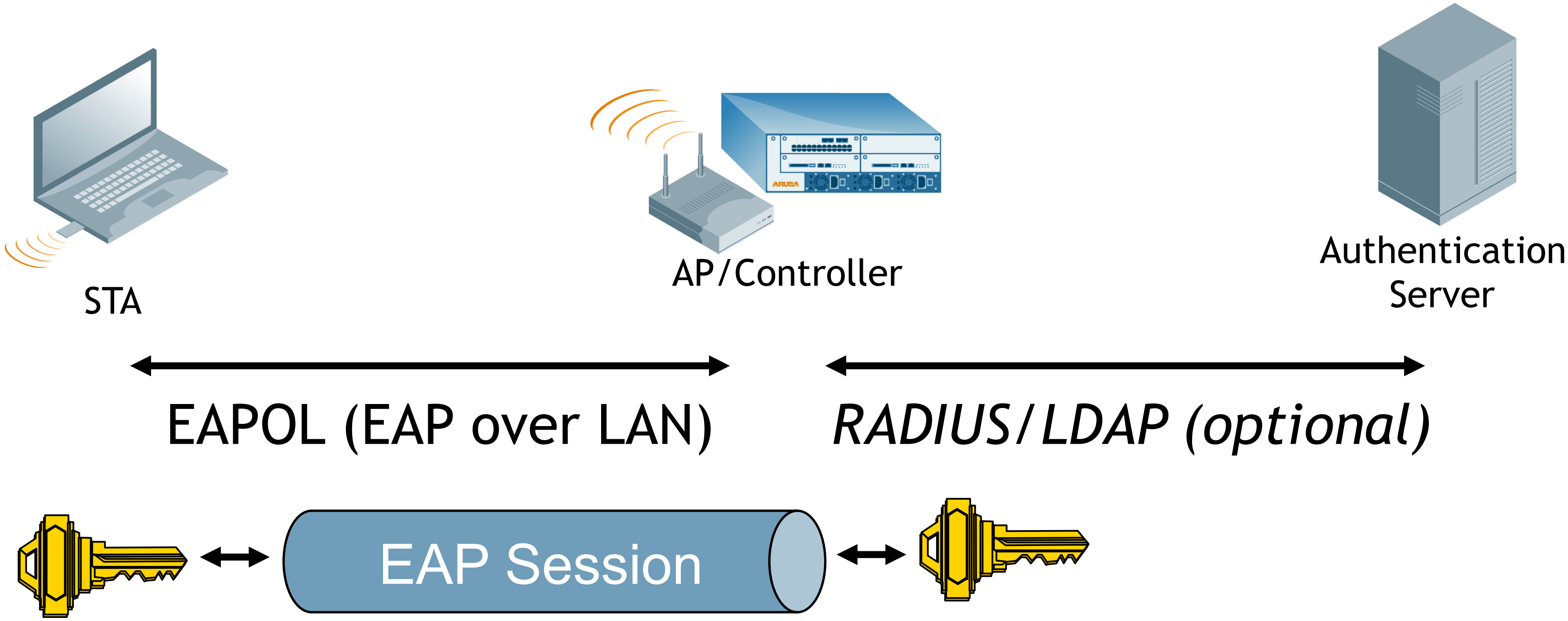
EAP-FAST

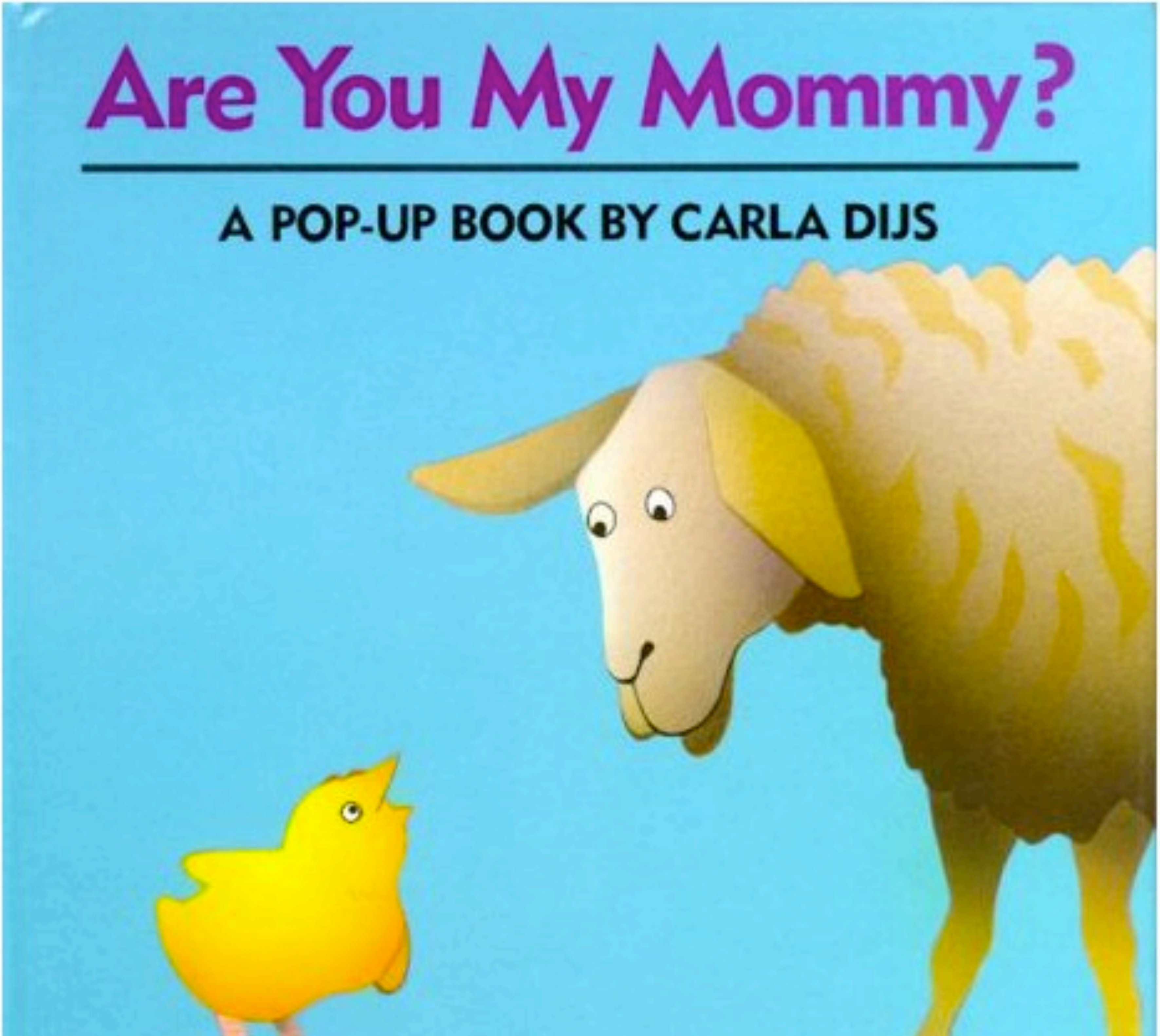
- Cisco proprietary
- Do not use – known security weaknesses

EAP to RADIUS Server



Local EAP Termination

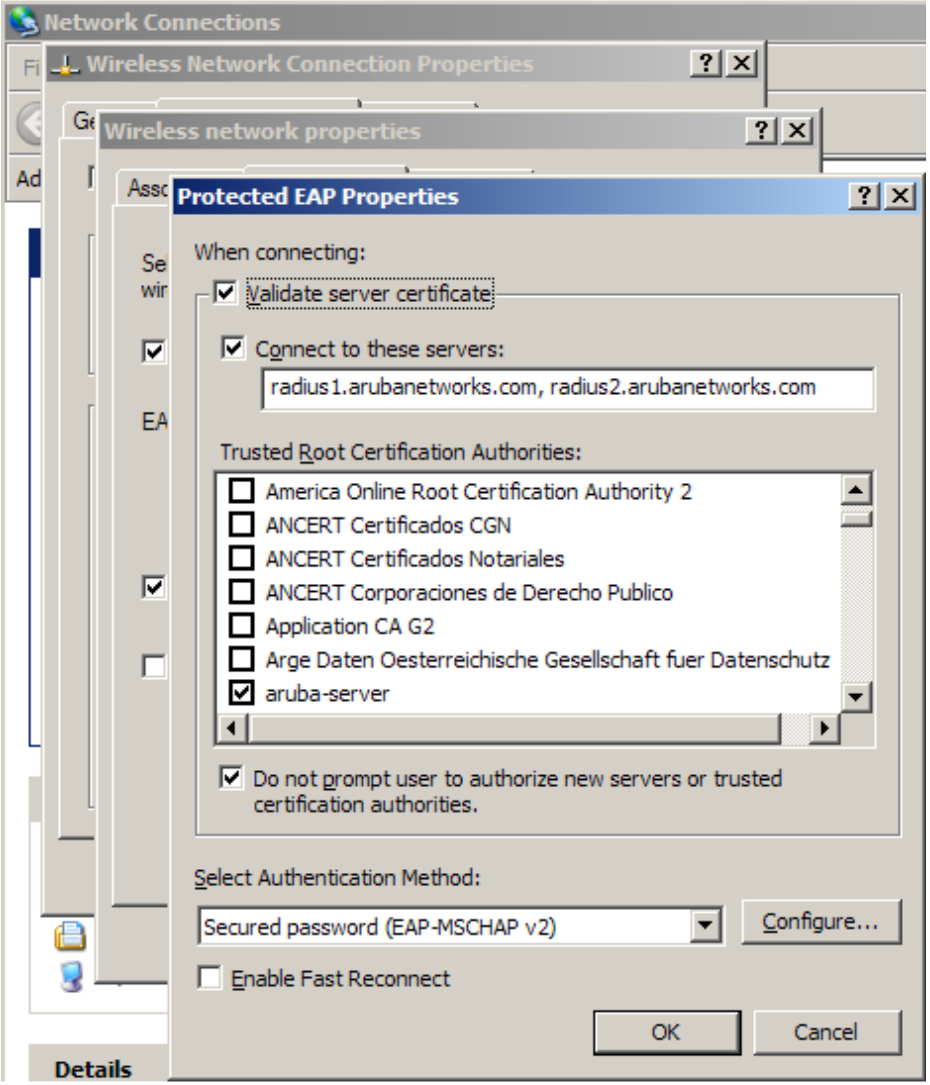




Are You My Mommy?

A POP-UP BOOK BY CARLA DIJS

Configure Supplicant Properly


Network Connections
Wireless Network Connection Properties
Wireless network properties
Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

radius1.arubanetworks.com, radius2.arubanetworks.com

Trusted Root Certification Authorities:

- ☐ America Online Root Certification Authority 2
- ☐ ANCERT Certificados CGN
- ☐ ANCERT Certificados Notariales
- ☐ ANCERT Corporaciones de Derecho Publico
- ☐ Application CA G2
- ☐ Arge Daten Oesterreichische Gesellschaft fuer Datenschutz
- ☑ aruba-server

☑ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

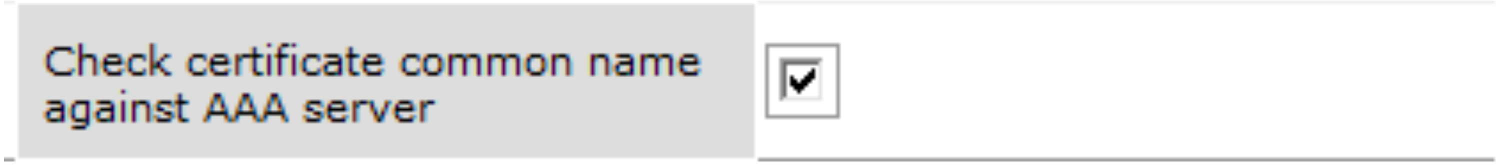
Secured password (EAP-MSCHAP v2)

☐ Enable Fast Reconnect

- Configure the Common Name of your RADIUS server (matches CN in server certificate)
- Configure trusted CAs (an in-house CA is better than a public CA)
- ALWAYS validate the server certificate
- Do not allow users to add new CAs or trust new servers
- Enforce with group policy

Authentication Sources

- **PEAP Termination**
  - Authentication against whatever AAA server has been configured (RADIUS, internal DB, LDAP)
  - If LDAP is used, use GTC as the inner EAP method
- **EAP-TLS Termination**
  - If client certificate is valid and not revoked, client will be authenticated
  - Optional: Look up certificate name in RADIUS/LDAP (configure ‘aaa authentication dot1x cert-cn-lookup)



Check certificate common name against AAA server ☑

Multi-Factor 802.1X Authentication?

- **Sequenced authentication**
  - Machine credential followed by user credential
  - Sequencing must be tracked by auth server (CPPM)
  - Supported in Windows domain environment…. but nowhere else
  - Timing / user behavior dependencies
- **Hardware tokens**
  - Viable option, but users don't like them…
  - Use EAP-GTC, EAP-POTP
  - RSA supplicant available
- **Stacked authentication**
  - Machine and user credential in same EAP transaction
  - Theoretically possible, but not supported by any known supplicant

Isn't MSCHAPv2 broken?

- Short answer: Yes – because of things like rainbow tables, distributed cracking, fast GPUs, etc.
- This is why we use MSCHAPv2 *inside* a TLS tunnel for Wi-Fi
- Still using PPTP for VPN? Watch out…

Future directions: EAP-PWD

- The problem: Today's password-based auth exposes password hashes to a possibly unknown entity
- Goal of PWD: Mutual authentication using a password
- Both sides prove they possess the password without actually *exposing* the password or a password derivative
- Developed by Dan Harkins of Aruba Networks – standardized in RFC xxx

Credits

- **Some slides stolen from: http://cevi-users.cevi.be/Portals/ceviusers/images/default/Userdag-20101125-Certs.pptx**
- **Some others stolen from: http://acs.lbl.gov/~mrt/talks/secPrimer.ppt**
- **Get Smart images used without permission**

The Airheads Challenge

Use Unlock Code “CRYPTO”

To get the quiz for this session

Login to play at

community.arubanetworks.com

AIRHEADS
LAS VEGAS 2013

JOIN: community.arubanetworks.com

FOLLOW: @arubanetworks

DISCUSS: #airheadsconf