$ ps | Enable

RAIDERS of the LOST CERTIFICATE

Paul Suh
paul.suh@ps-enable.com
http://ps-enable.com

$ ps | Enable

RAIDERS of the LOST CERTIFICATE

Paul Suh
paul.suh@ps-enable.com
http://ps-enable.com

$ ps | Enable

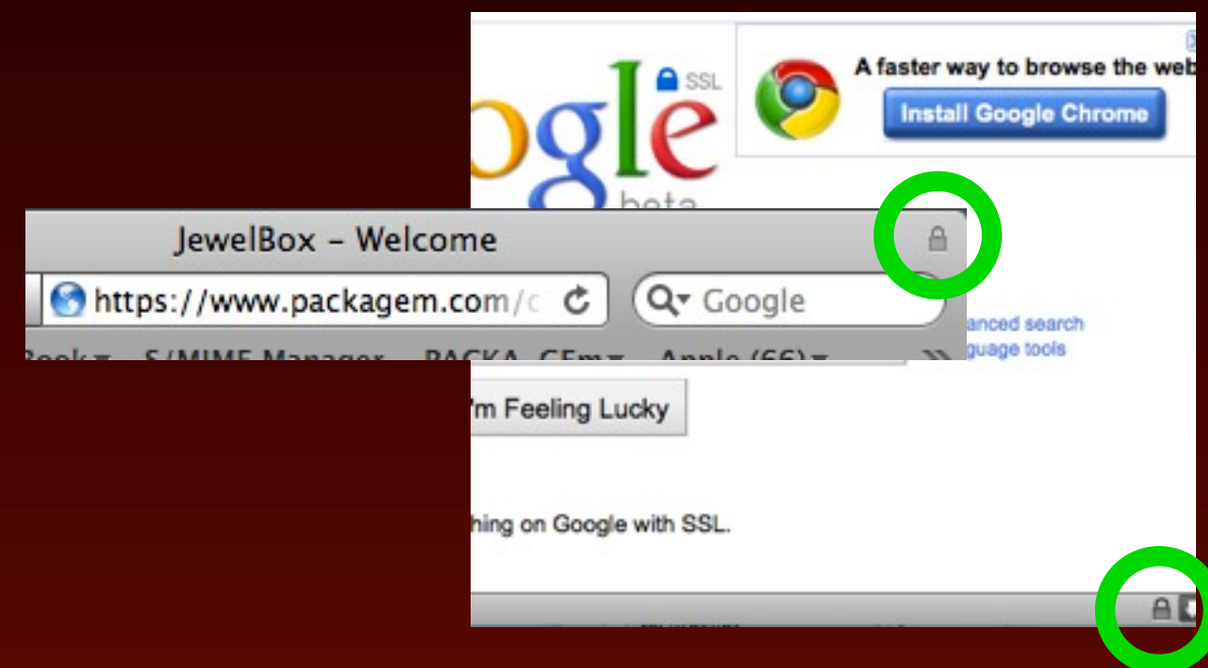
Where do we see certificates?

Browser lock icons

S/MIME e-mail encryption

$ ps | Enable

Where do we see certificates?

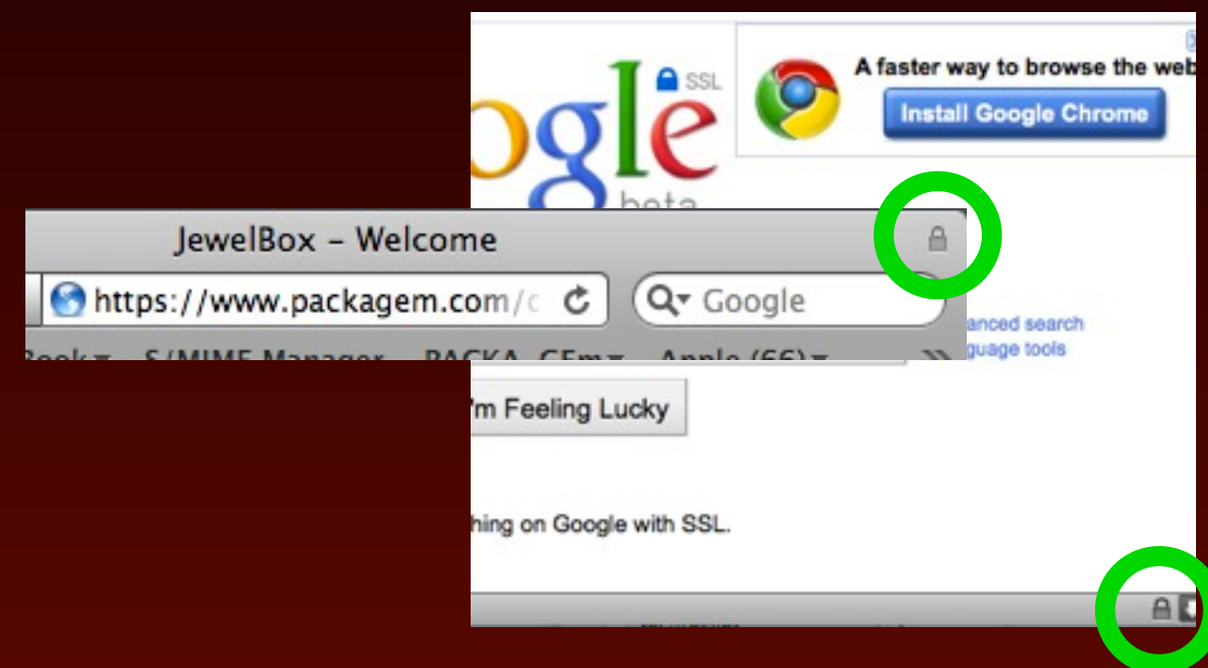


Browser lock icons

S/MIME e-mail encryption

$ ps | Enable

Where do we see certificates?



Browser lock icons

S/MIME e-mail encryption

$ ps | Enable

What is a Certificate?

$ ps | Enable

What is a Certificate?


```
-----BEGIN CERTIFICATE-----
MIIDNDCCAp2gAwIBAgIDDG3kMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
MRAwDgYDVQQKEwdFcXVpZmF4MS0wKwYDVQQLEyRFcXVpZmF4IFNlY3VyZSBDZXJ0
aWZpY2F0ZSBBdXRob3JpdHkwHhcNMDkwODE0MTIyODI1WhcNMTAwOTE1MDgzNjU0
WjCBvjELMAkGA1UEBhMCVVMxGjAYBgNVBAoTEW1haWwuZ29vZGVhc3QuY29tMRMw
EQYDVQQLEwpHVDE1MjczNTkzMTEwLwYDVQQLEyhTZWUgd3d3LnJhcGlkc3NsLmNv
bS9yZXNvdXJjZXMvY3BzIChjKTA5MS8wLQYDVQQLEyZEb21haW4gQ29udHJvbCBW
YWxpZGF0ZWQgLSBSYXBpZFNTTChSKTEaMBgGA1UEAxMRbWFpbC5nb29kZWFzdC5j
b20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALfkfK1/GXjZ9ElME5FBRAic
ELomSkAyLSf7lJkoizNx9TjmQxvhKOOOY4BZha7Ppu65gf561MpUPmpnE+NvJCyP
h0jdZOLniovAAVJAyy6gCb7XnzPYPXR7ei8OVqX+NSxl4Wvl1GD2Cda4Uvg7A949
3s5Dpo8ufWd9A+Lmz8RdAgMBAAGjga4wgaswDgYDVR0PAQH/BAQDAgTwMB0GA1Ud
DgQWBBRdSbSgosLIWuz1Yk48krPNNaMa9zA6BgNVHR8EMzAxMC+gLaArhilodHRw
Oi8vY3JsLmdlb3RydXN0LmNvbS9jcmxzL3NlY3VyZWNhLmNybDAfBgNVHSMEGDAW
gBRI5mj5K9KylddH2CMgEE8zmJCf1DAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYB
BQUHAwIwDQYJKoZIhvcNAQEFBQADgYEAb83ueDKHAUQ2kKx85OjkZJLm7fI5Ah59
z+Qe3uO+2bXQmjfTKXZvFspNN03ffBYsroqrKF6PnJOGRSDaqX5E6OINbG23hoiu
phCk7Clcq6JFMGwXPFJIdJEP3g3/8bJQLMgsODNCEOKyNWlAwEJFw33lJ4+suXHK
```


$ ps | Enable

No, really…

$ ps | Enable

No, really…

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 814564 (0xc6de4)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Equifax, OU=Equifax Secure Certificate Authority
        Validity
            Not Before: Aug 14 12:28:25 2009 GMT
            Not After : Sep 15 08:36:54 2010 GMT
        Subject: C=US, O=mail.goodeast.com, OU=GT15273593, OU=See
www.rapidssl.com/resources/cps (c)09, OU=Domain Control Validated -
RapidSSL(R), CN=mail.goodeast.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b7:e4:7c:ad:7f:19:78:d9:f4:49:4c:13:91:41:
                    44:08:9c:10:ba:26:4a:40:32:2d:27:fb:94:99:28:
```

$ ps | Enable

A Little More Basic, Please?

$ ps | Enable

A Little More Basic, Please?

1. Choose two distinct prime numbers p and q.
2. Compute $n = pq$.
3. Compute $\phi(n) = (p - 1)(q - 1)$, where ϕ is Euler's totient function.
4. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e,\phi(n)) = 1$ (i.e., e and $\phi(n)$ are coprime).
5. Determine $d = e^{-1} (\mathrm{mod}\ \phi(n))$. (i.e., d is the multiplicative inverse of $e (\mathrm{mod}\ \phi(n))$).

An alternative, used by PKCS#1, is to choose d matching with , where is the least common multiple. Using λ instead of $\phi(n)$ allows more choices for d. λ can also be defined using the Carmichael function, $\lambda(n)$.

$ ps | Enable

OK, You’ve Really Lost Me

$ ps | Enable

OK, You’ve Really Lost Me

1. Allows two sides to communicate securely without exchanging secret codes beforehand

$ ps | Enable

OK, You’ve Really Lost Me

1. Allows two sides to communicate securely without exchanging secret codes beforehand
2. Assures the identity of the certificate holder

$ ps | Enable

OK, You’ve Really Lost Me

1. Allows two sides to communicate securely without exchanging secret codes beforehand
2. Assures the identity of the certificate holder

$ ps | Enable

Cyrptography

cryptography |kripˈtägrəfē|

noun

the art of writing or solving codes.

$ ps | Enable

The Ancient Greeks

$ ps | Enable

Demonstration: Scytale

$ ps | Enable

Symmetric Ciphers

Both sides must have the same secret key

Keys can be simple or complex

Scytale

Enigma

JN-25

One-time pad

$ ps | Enable

Use of a Symmetric Key

$ ps | Enable

Use of a Symmetric Key

$ ps | Enable

Use of a Symmetric Key

$ ps | Enable

Use of a Symmetric Key

$ ps | Enable

The Trouble with Symmetric Ciphers

Making sure all of the users of a code have the same key

A.k.a., the “Key Distribution Problem”

More complex ciphers are more secure but make the Key Distribution Problem worse

$ ps | Enable

Submarine I-1 and JN-25

- Submarine I-1 sunk with copies of codes
- Salvaged by Allied forces
- All Japanese Naval codes considered compromised in 1943

$ ps | Enable

VENONA Project

- High demand for code pads caused Soviets to re-use some one-time pads
- US was able to read some Soviet message traffic encrypted with the re-used pads

$ ps | Enable

Ron Rivest, Adi Shamir, Leonard Adleman

$ ps | Enable

Ron Rivest, Adi Shamir, Leonard Adleman

R S A

$ ps | Enable

Ron Rivest, Adi Shamir, Leonard Adleman

R S A

- Originally discovered by James H. Ellis, Clifford Cocks, and Malcolm Williamson at GCHQ in the UK in 1973

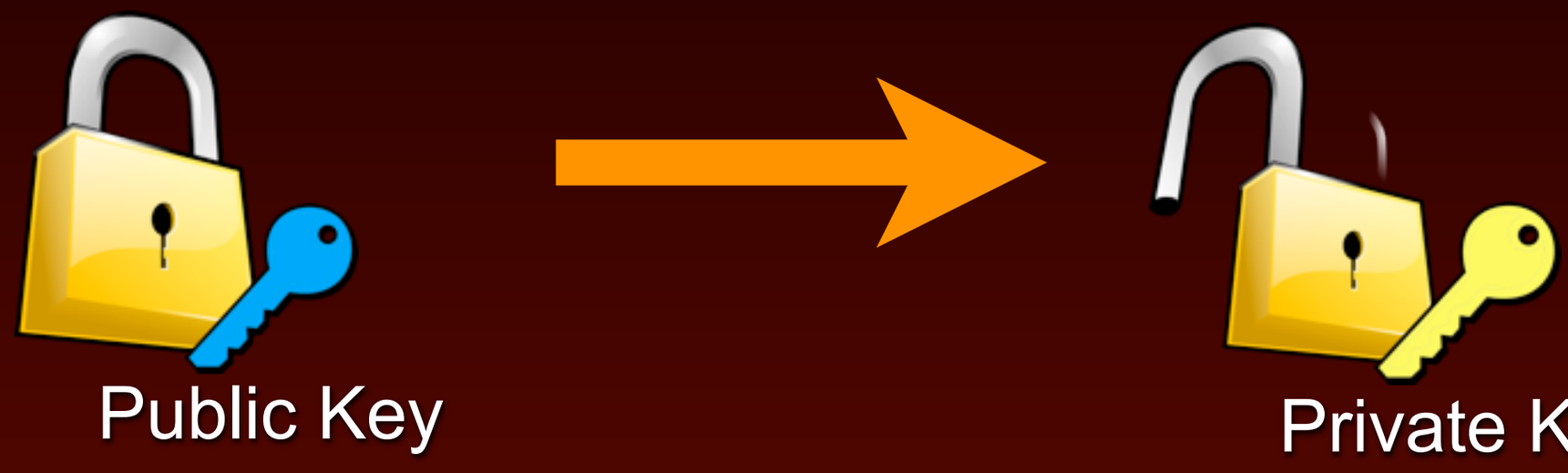
$ ps | Enable

How Does RSA Work?

Public Key

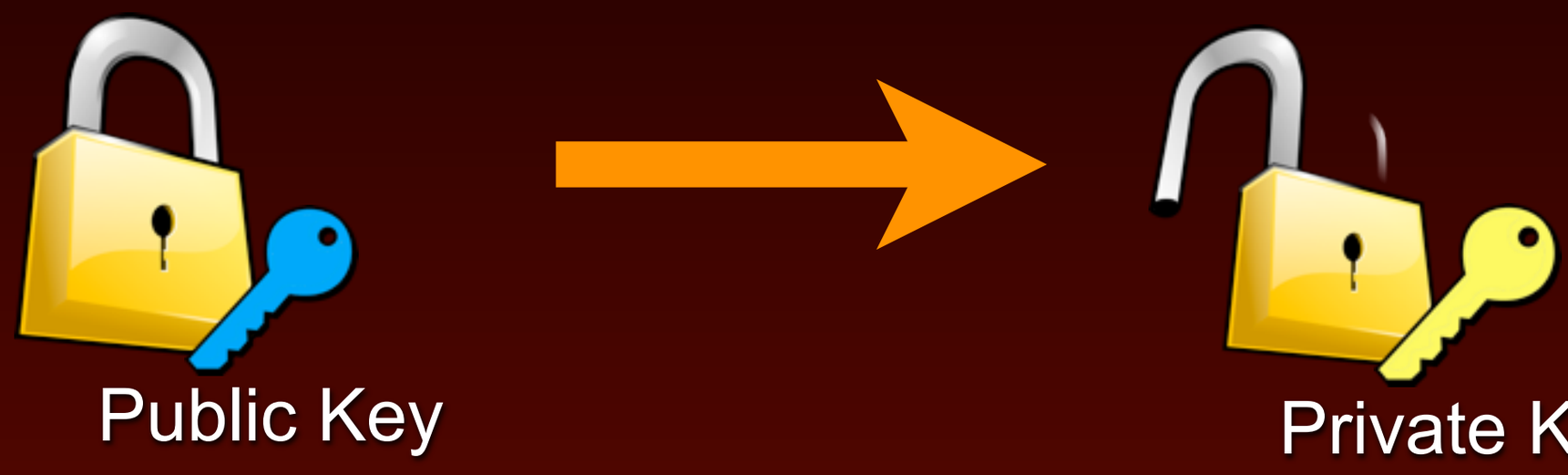
$ ps | Enable

How Does RSA Work?



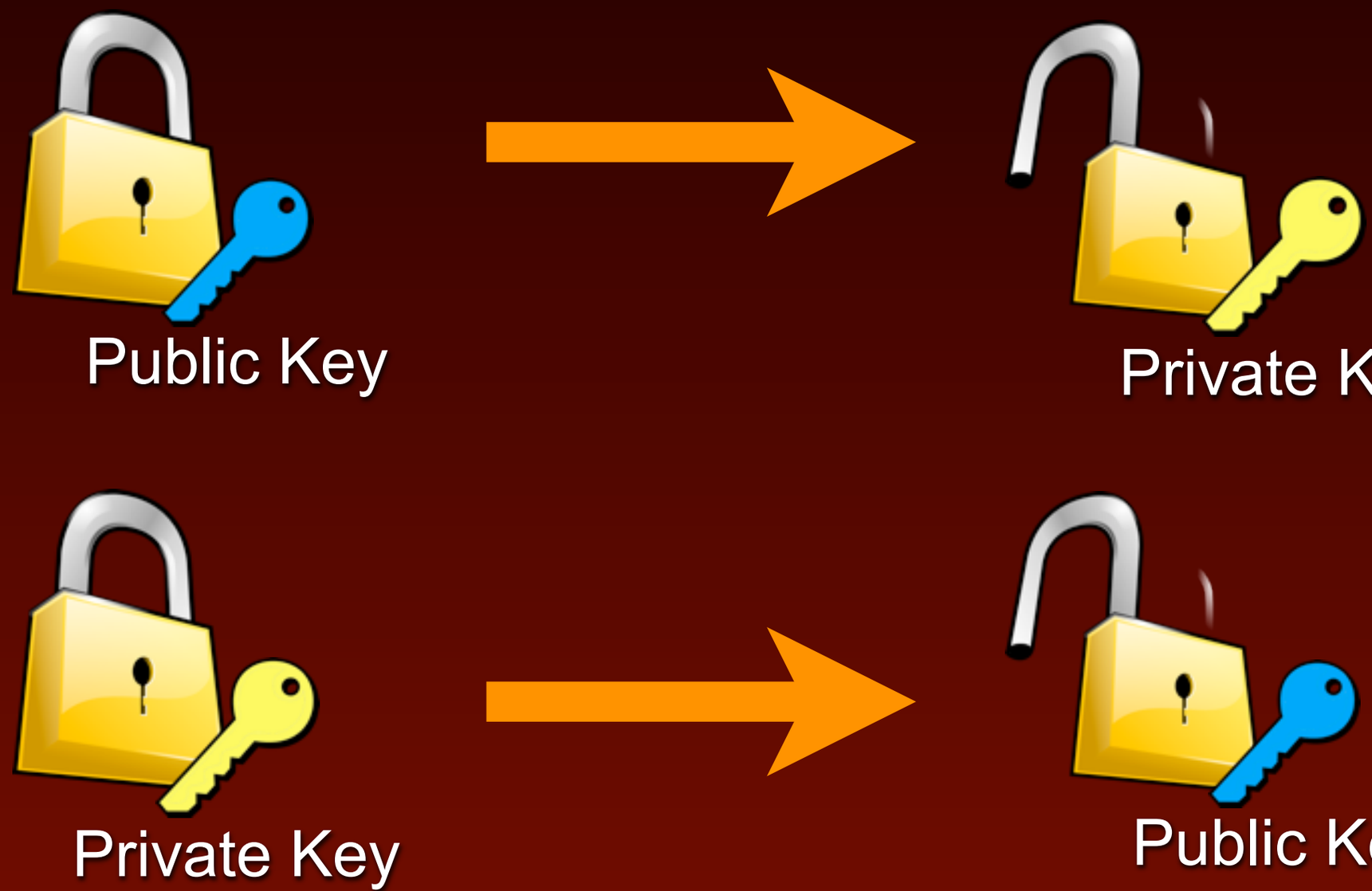
$ ps | Enable

How Does RSA Work?



$ ps | Enable

How Does RSA Work?



$ ps | Enable

Public Key Encryption

Public Key
Alice

$ ps | Enable

Public Key Encryption

Public Key
Alice

$ ps | Enable

Public Key Encryption

Public Key
Alice

Public Key
Alice

$ ps | Enable

Public Key Encryption

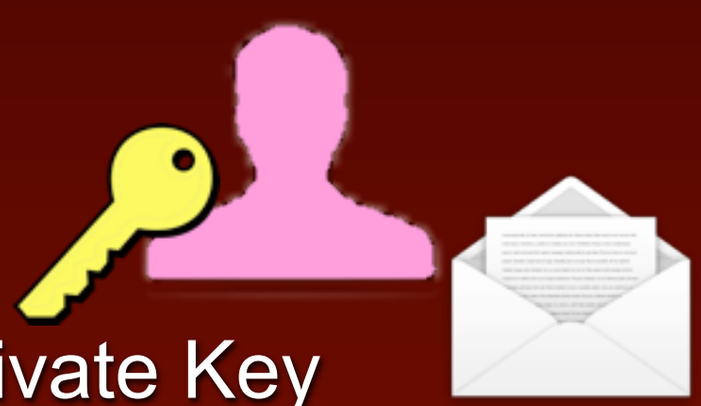
Public Key
Alice

Public Key
Alice

$ ps | Enable

Public Key Encryption

Public Key
Alice



Private Key
Alice

Public Key
Alice

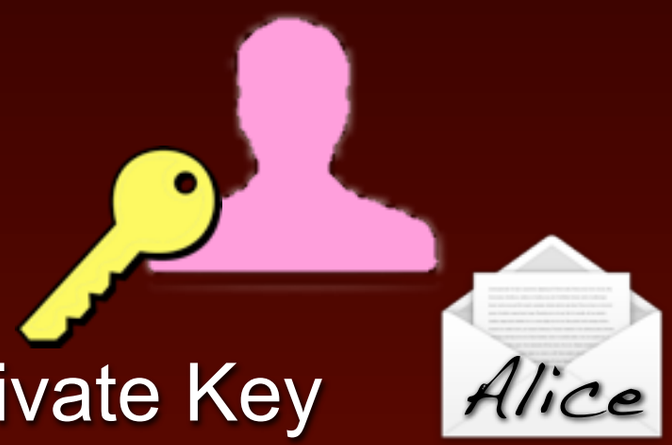
$ ps | Enable

Digital Signature

Private Key
Alice

$ ps | Enable

Digital Signature



Private Key
Alice

$ ps | Enable

Digital Signature

Private Key
Alice

$ ps | Enable

Digital Signature

Private Key
Alice

Public Key
Alice

$ ps | Enable

Man in the Middle

Public Key
“Alice”

$ ps | Enable

Man in the Middle

$ ps | Enable

Obtaining a Certificate

Public Key
Private Key

Private Key
CA

$ ps | Enable

Obtaining a Certificate

Public Key
Private Key

CSR

Private Key
CA

$ ps | Enable

Obtaining a Certificate

Public Key
Private Key

CSR

Private Key
CA

$ ps | Enable

Obtaining a Certificate

Public Key
Private Key

CSR

Private Key
CA

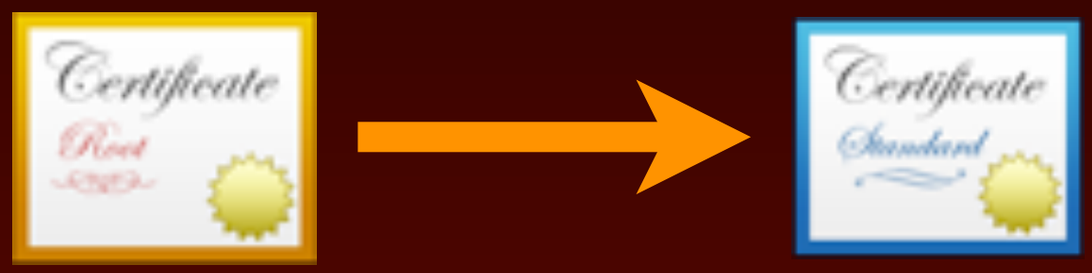
$ ps | Enable

Certificate Chains

Root
Certificate
Authority

$ ps | Enable

Certificate Chains



Root Certificate Authority

Intermediate Certificate Authority

$ ps | Enable

Certificate Chains

Root Certificate Authority

Intermediate Certificate Authority

Leaf Certificate

$ ps | Enable

- A Certificate is a Public Key Digitally Signed by Some Entity That You Trust

$ ps | Enable

Demonstration: Verifying a Certificate

$ ps | Enable

Certificate Elements

X.509 - ITU standard

X.509 v3 - Current version of the standard

$ ps | Enable

Certificate Elements

Version

Serial Number

Algorithm ID

Issuer

Not Valid Before

Not Valid After

Subject

Subject Public Key Info

Public Key Algorithm

Subject Public Key

Extensions (Optional)

Certificate Signature Algorithm

Certificate Signature

$ ps | Enable

Certificate Elements: Subject

Servers: LDAP-style identifier

```
o=Company,ou=Department,cn=www.example.com
```

E-mail: E-mail address extension

```
o=Company,ou=Department,cn=Alice Doe/
emailAddress=alice.doe@example.com
```

$ ps | Enable

Certificate Elements: Subject

Servers: LDAP-style identifier

```
o=Company,ou=Department,cn=www.example.com
```

E-mail: E-mail address extension

```
o=Company,ou=Department,cn=Alice Doe/
emailAddress=alice.doe@example.com
```

$ ps | Enable

Certificate Elements: Subject

Servers: LDAP-style identifier

```
o=Company,ou=Department,cn=www.example.com
```

E-mail: E-mail address extension

```
o=Company,ou=Department,cn=Alice Doe/
emailAddress=alice.doe@example.com
```

$ ps | Enable

Certificate Elements: Extensions

Basic Constraints

Key Usage

Extended Key Usage

Subject Alternative Name

$ ps | Enable

Certificate Extensions
Key Usage

Digital Signature

Non-Repudiation

Key Encipherment

Key Certificate Signing

CRL Signing

$ ps | Enable

Certificate Extensions
Extended Key Usage

Client Authentication

Code Signing

E-mail Protection

OCSP Signing

$ ps | Enable

Subject Alternative Name Certificates

Also called Unified Communications Certificate (UCC)

Common with Microsoft Exchange

Has Subject Alternative Name attribute

```
DNS Name=www.example.com

DNS Name=wiki.example.com
```

$ ps | Enable

Certificate Revocation

Certificate Revocation List (CRL)

Online Certificate Status Protocol (OCSP)

$ ps | Enable

Examine a Certificate's Details

$ ps | Enable

Using a Server Certificate

- Obtain chain certificates
- Install certificate via Server Admin
- Configure each service
  - iChat, iCal Server, Mail, Mobile Access, Open Directory, RADIUS, VPN, Web
- Test the connection

$ ps | Enable

Test Certificate Usage

- SSL
  - First exchange is certificate information
  - Most services: HTTPS, IMAPS, XMPP-S
- STARTTLS
  - First exchange is capability information in clear
  - Certificate sent later
  - SMTP-S

$ ps | Enable

Test Certificate Usage

```
openssl s_client -connect host:port
    <-servername name>

openssl s_client -connect host:port
    -starttls smtp
```

$ ps | Enable

Open Directory CA

Automatically generated

- “<Organization name> Open Directory Certification Authority”
- “IntermediateCA_<servername>_1”
- “IntermediateCA_<servername>_2”
- …
- <servername> Code Signing Certificate

$ ps | Enable

Trust Profiles

Install "Trust Profile for ps Enable, Inc."?

This device profile will configure your Mac for the following: Certificate.

Trust Profile for ps Enable, Inc.

Unverified

Description	Configures your device to trust the Profile Manager s...
Signed	mainserver.pretendco.com Code Signing Certificate
Received	Sep 13, 2012

Settings	Certificate ps Enable, Inc. Open Directory Certification Au...

DETAILS

Certificate

Description	Root certificate for ps Enable, Inc.
Certificate	ps Enable, Inc. Open Directory Certification Authority
Expires	Sep 13, 2017
Issuer	ps Enable, Inc. Open Directory Certification Authority

$ ps | Enable

Sources of Trust

$ ps | Enable

Sources of Trust

/System/Library/Keychains/

$ ps | Enable

Sources of Trust

/System/Library/Keychains/

SystemRootCertificates.keychain

$ ps | Enable

Sources of Trust

/System/Library/Keychains/

SystemRootCertificates.keychain

SystemCACertificates.keychain (intermediates)

$ ps | Enable

Sources of Trust

/System/Library/Keychains/

SystemRootCertificates.keychain

SystemCACertificates.keychain (intermediates)

EVRoots.plist

$ ps | Enable

Sources of Trust

/System/Library/Keychains/

SystemRootCertificates.keychain

SystemCACertificates.keychain (intermediates)

EVRoots.plist

X509Anchors

$ ps | Enable

Sources of Trust

/System/Library/Keychains/

- SystemRootCertificates.keychain
- SystemCACertificates.keychain (intermediates)
- EVRoots.plist
- X509Anchors

/Library/Keychains/System.keychain

Sources of Trust

/System/Library/Keychains/

SystemRootCertificates.keychain

SystemCACertificates.keychain (intermediates)

EVRoots.plist

X509Anchors

/Library/Keychains/System.keychain

~/Library/Keychains/login.keychain

Browsers and Trust

$ ps | Enable

Browsers and Trust

Safari and Chrome use Keychain

$ ps | Enable

Browsers and Trust

Safari and Chrome use Keychain

Firefox does not!

$ ps | Enable

Demonstration: Certificate Trust

$ ps | Enable

Problems with PKI

$ ps | Enable

Problems with PKI

How many Certificate Authorities in System Roots?

$ ps | Enable

Problems with PKI

How many Certificate Authorities in System Roots?

182

Google for “Diginotar”

$ ps | Enable

Problems with PKI

- How many Certificate Authorities in System Roots?
  - 182
  - Google for “Diginotar”
- Certificate revocation
  - OCSP off due to privacy leaks
  - CRL is too big

$ ps | Enable

Problems with PKI

- Proliferation of private roots
  - Profile Manager / MDM
  - Active Directory PKI
- Domain validation vs. Extended validation

$ ps | Enable

Problems with PKI

- Recent attacks on implementations
  - Null-terminated strings
  - BEAST / CRIME
- Weaknesses in underlying crypto
  - MD5 is dead
  - SHA-1 is fading

$ ps | Enable

Problems with PKI

No I'm not going to talk about running as an admin

$ ps | Enable

RAIDERS of the LOST CERTIFICATE

Q & A

Paul Suh
paul.suh@ps-enable.com
http://ps-enable.com

$ ps | Enable