Computer security: authentication of principals and cryptographic protocols

Frans Kaashoek

6.033 Spring 2007

MASSACHUSETTS
INSTITUTE OF
TECHNOLOGY

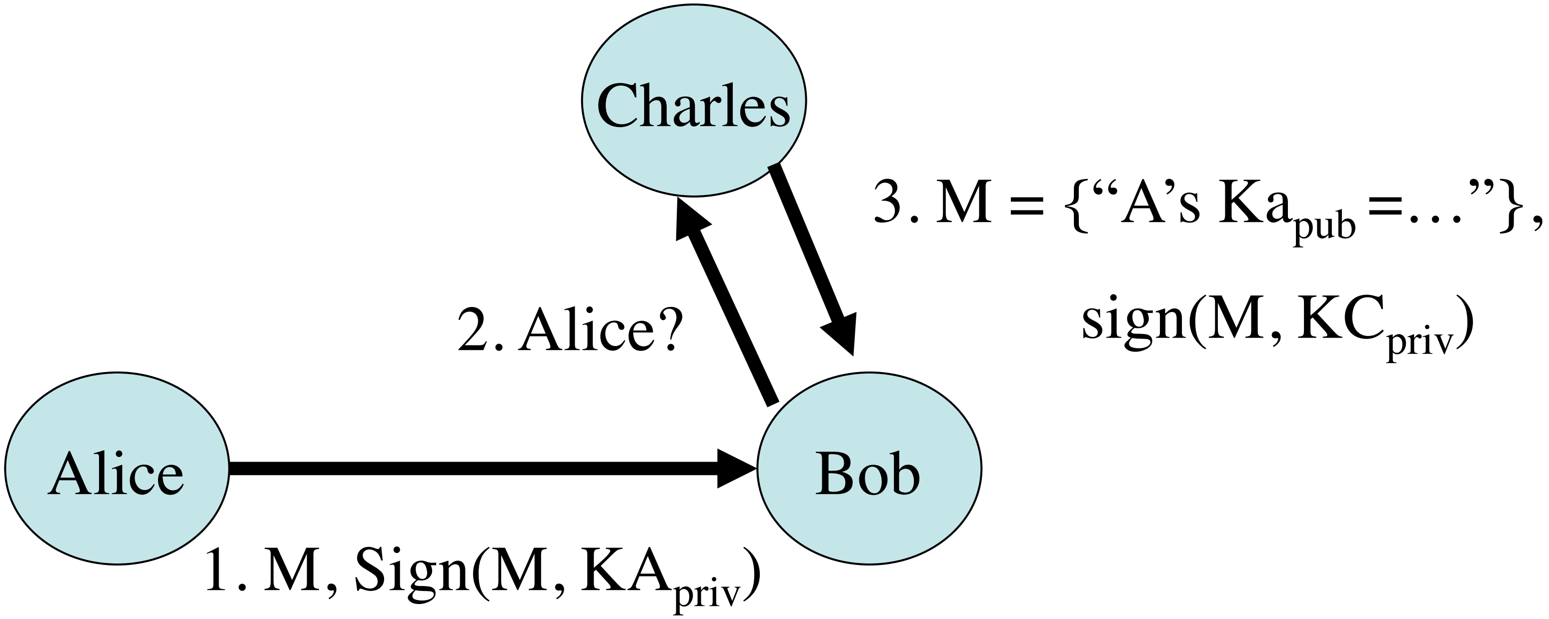
HKN Underground Guide

https://sixweb.mit.edu/student/evaluate/6.033-s2007

Link posted on 6.033 home page

Deadline: May 20

key distribution



Charles

3. $M = \{$“A’s $Ka_{pub} = \ldots$”$\}$,

sign(M, KC_{priv})

2. Alice?

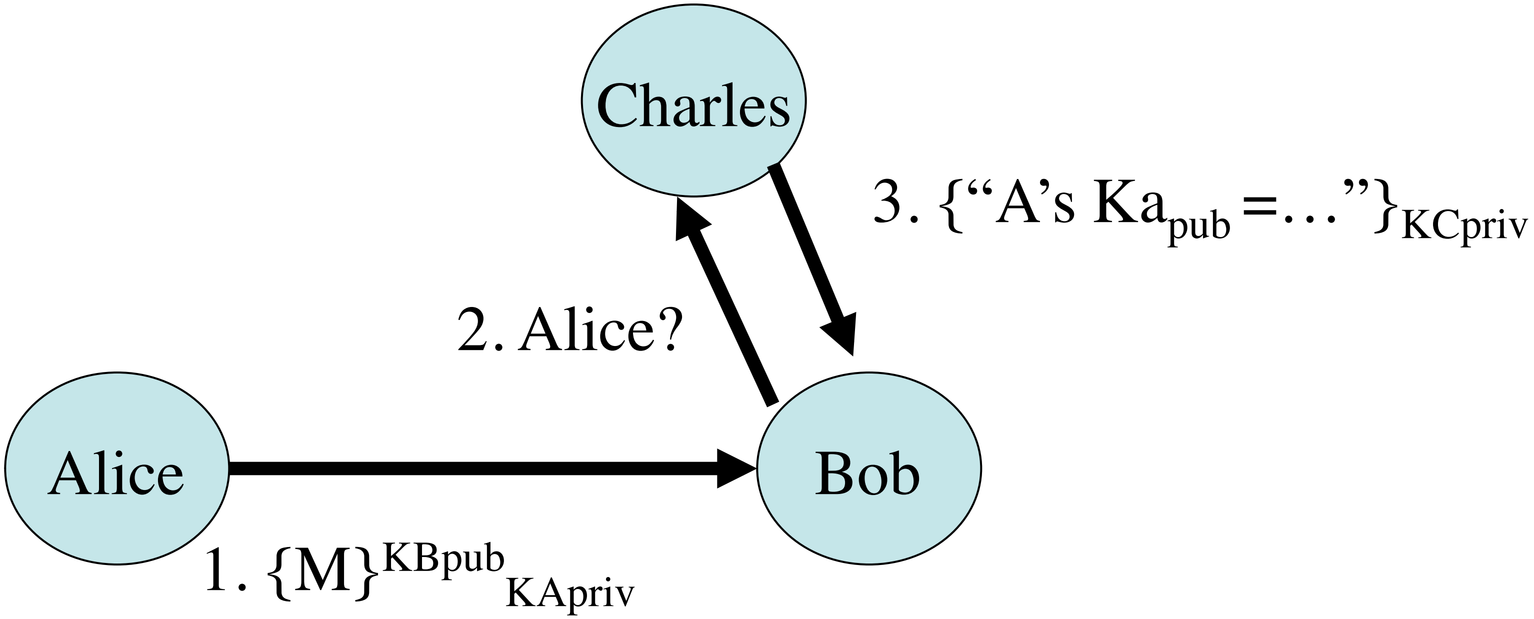
Alice

Bob

1. M, Sign(M, KA_{priv})

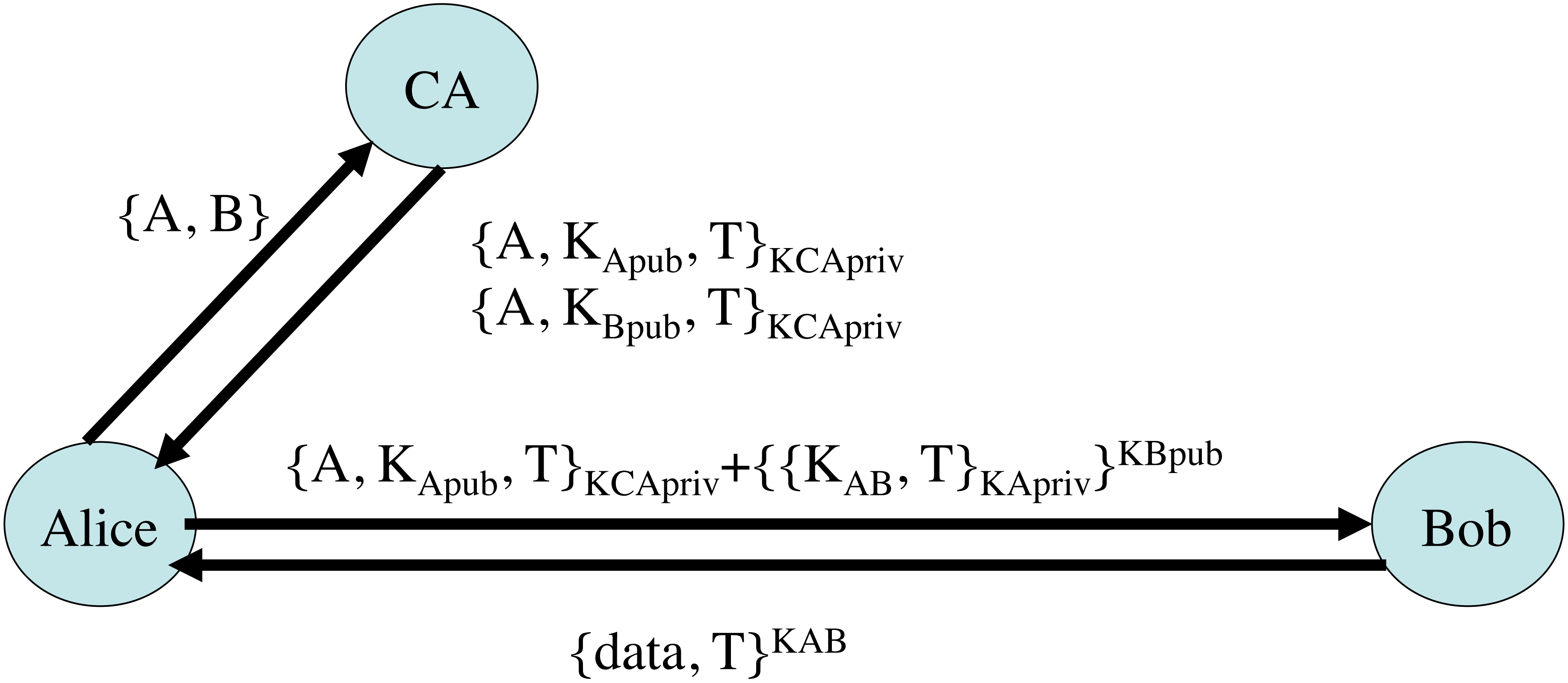
- 3 is a *certificate* for Alice’s public key
- Charles is called a *certificate authority*
- The interaction is an example of a *cryptographic protocol*

Shorter notation


Charles
3. $\{$“A’s Ka_{pub} =…”$\}_{KCpriv}$
2. Alice?
Alice
Bob
1. $\{M\}^{KBpub}_{KApriv}$

- Subscript for signing
- Superscript for encrypting

Denning-Sacco



CA

$\{A, B\}$

$\{A, K_{Apub}, T\}_{KCApriv}$
$\{A, K_{Bpub}, T\}_{KCApriv}$

Alice

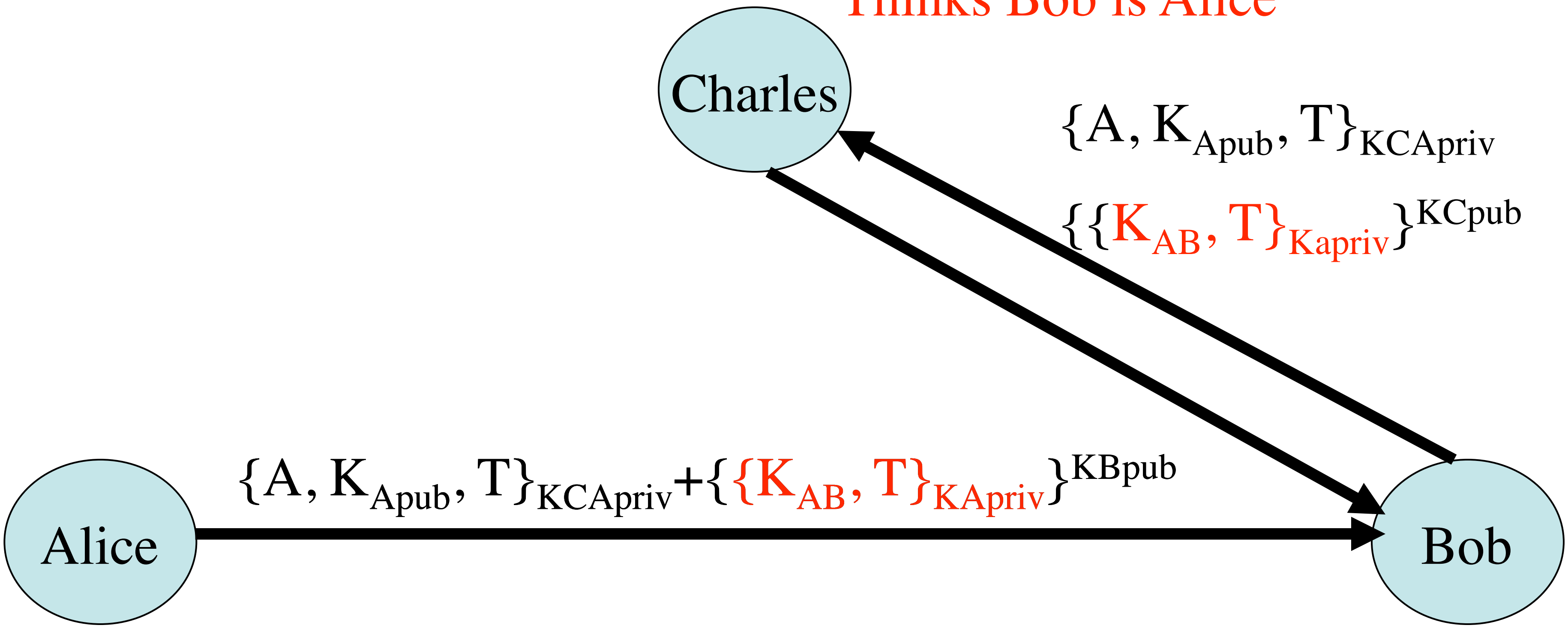
$\{A, K_{Apub}, T\}_{KCApriv}+\{\{K_{AB}, T\}_{KApriv}\}^{KBpub}$

Bob

$\{data, T\}^{KAB}$

1. Authenticate Alice to Bob and Bob to Alice
2. Set up a shared-secret key

Impersonation Attack



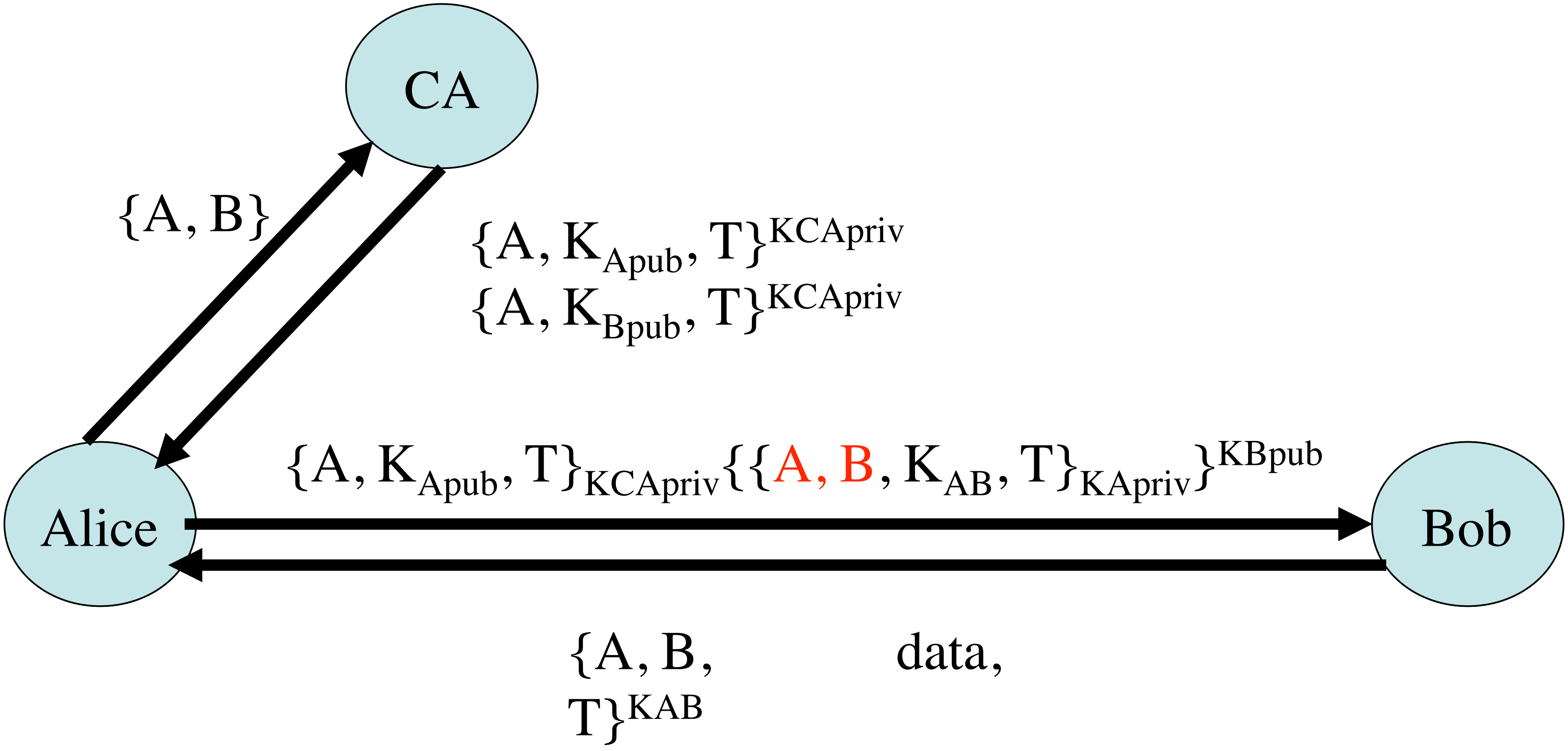
Thinks Bob is Alice

$\{A, K_{Apub}, T\}_{KCApriv}$

$\{\{K_{AB}, T\}_{Kapriv}\}^{KCpub}$

$\{A, K_{Apub}, T\}_{KCApriv}+\{\{K_{AB}, T\}_{KApriv}\}^{KBpub}$

Denning-Sacco (fixed)



$\{A, B\}$

$\{A, K_{Apub}, T\}^{KCApriv}$

$\{A, K_{Bpub}, T\}^{KCApriv}$

$\{A, K_{Apub}, T\}_{KCApriv}\{\{A, B, K_{AB}, T\}_{KApriv}\}^{KBpub}$

$\{A, B,$ data, $T\}^{KAB}$

Be explicit!

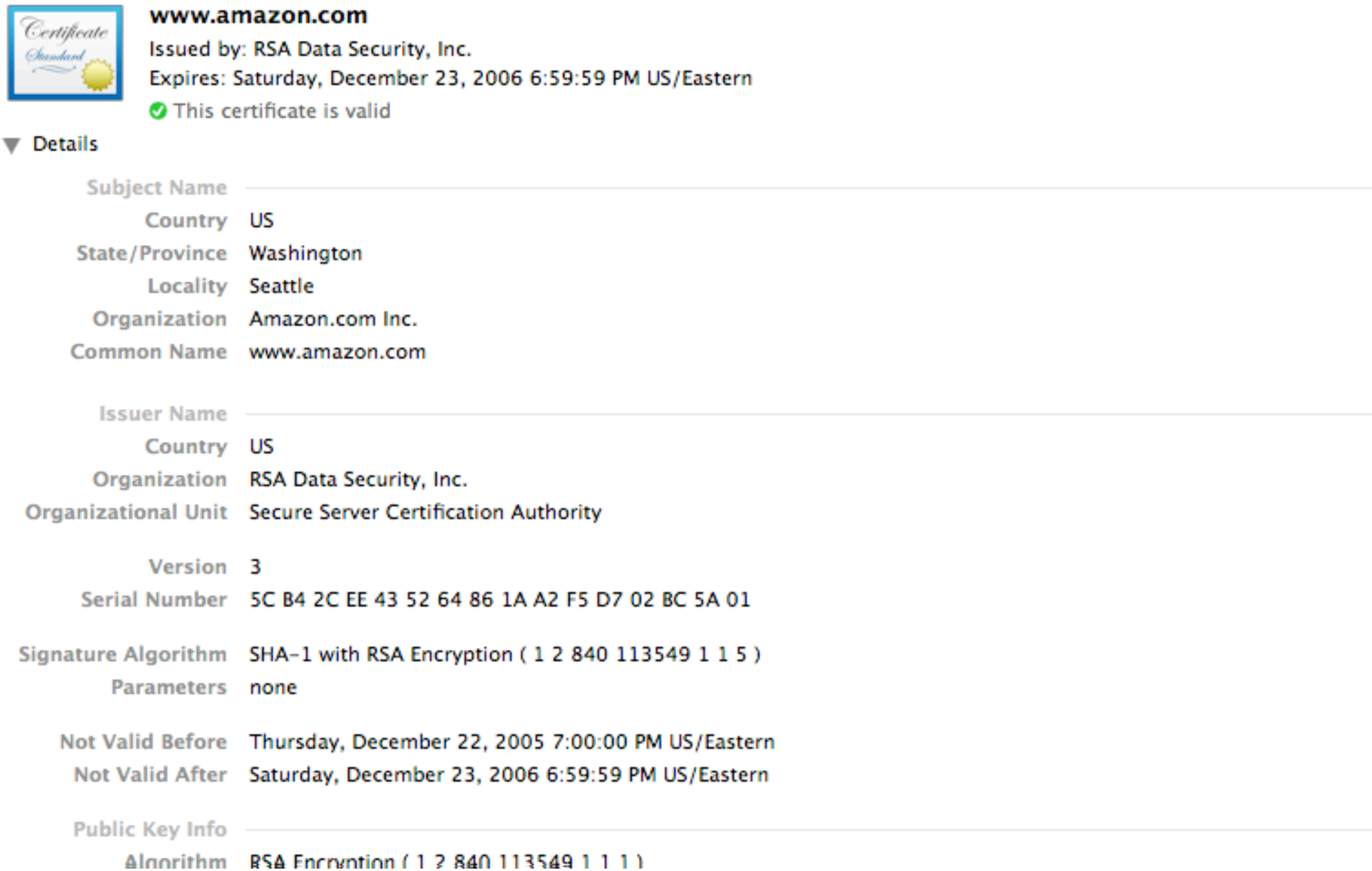
Example: Web (SSL simplified)

- U: https://www.amazon.com
- B →W: {random_{c}, session-id, ciphersuites}
- B ← W: {random_{s}, session-id, $\{\text{amazon.com}, K_{\text{pub-amazon}}\}_{\text{Kversign}}$}
- B: verify($\{\text{amazon.com}, K_{\text{pub-amazon}}\}_{\text{Kversign}}$, $K_{\text{pub-verisign}}$)?
- B →W: $\{\text{pre-master-secret}\}^{\text{Kpub-amazon}}$
- ……

X509 certificate

- struct X509_certificate {

```
unsigned version;
unsigned serial;
signature_cipher_identifier;
issuer_signature;
issuer_name;
subject_name;
subject_public_key_cipher_identifier;
subject_public_key;
validity_period;
};
```



www.amazon.com

Issued by: RSA Data Security, Inc.

Expires: Saturday, December 23, 2006 6:59:59 PM US/Eastern

✓ This certificate is valid

▼ Details

Subject Name

Country US

State/Province Washington

Locality Seattle

Organization Amazon.com Inc.

Common Name www.amazon.com

Issuer Name

Country US

Organization RSA Data Security, Inc.

Organizational Unit Secure Server Certification Authority

Version 3

Serial Number 5C B4 2C EE 43 52 64 86 1A A2 F5 D7 02 BC 5A 01

Signature Algorithm SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)

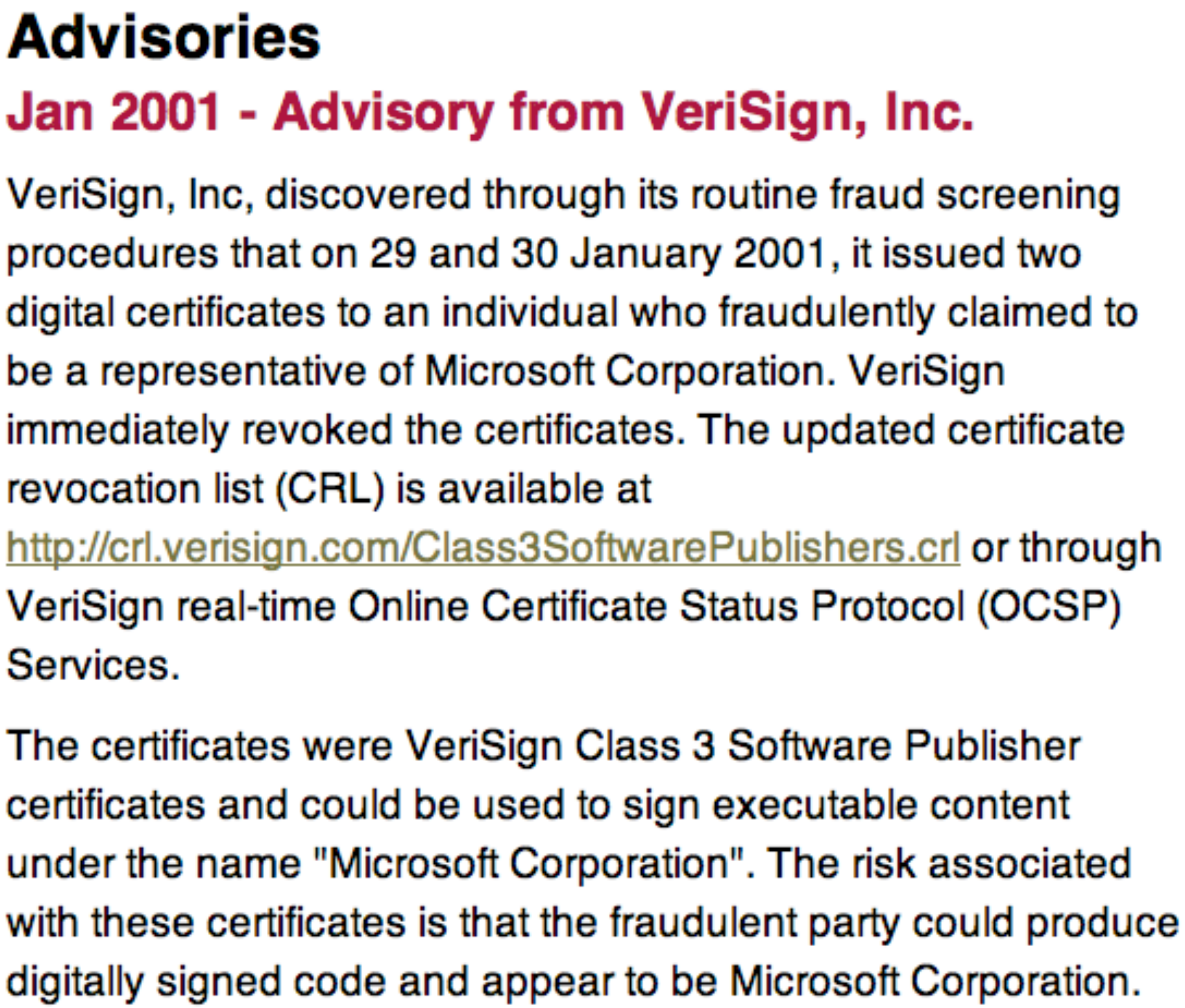
Parameters none

Not Valid Before Thursday, December 22, 2005 7:00:00 PM US/Eastern

Not Valid After Saturday, December 23, 2006 6:59:59 PM US/Eastern

Public Key Info

Algorithm RSA Encryption (1 2 840 113549 1 1 1)



Advisories

Jan 2001 - Advisory from VeriSign, Inc.

VeriSign, Inc, discovered through its routine fraud screening procedures that on 29 and 30 January 2001, it issued two digital certificates to an individual who fraudulently claimed to be a representative of Microsoft Corporation. VeriSign immediately revoked the certificates. The updated certificate revocation list (CRL) is available at http://crl.verisign.com/Class3SoftwarePublishers.crl or through VeriSign real-time Online Certificate Status Protocol (OCSP) Services.

The certificates were VeriSign Class 3 Software Publisher certificates and could be used to sign executable content under the name "Microsoft Corporation". The risk associated with these certificates is that the fraudulent party could produce digitally signed code and appear to be Microsoft Corporation.