Public Key Infrastructure

Yan Huang

Credit: David Evans (UVA)

Using RSA to Encrypt

- Use 2048-bit modulus (recommended)
- Encrypt 1MB file
  - 4096 2048-bit messages
  - Each $\mathbf{M}^e$ requires $\log_2(e)$ 1024-bit number modular multiplications (unless e is fixed to some small numbers)
- Why does not one use RSA like this?
  - About 100-1000 times slower than DES
  - Need to be careful not to encrypt particular $\mathbf{M}$s
  - Can speed up encryption by choosing e that is an easy number to multiply by (e.g., 3 or $2^{16} + 1$)
  - But, decryption must use non-easy d (~2048 bits)

Hybrid Encryption

- Use RSA to establish a shared secret key for symmetric cipher (e.g., AES)
  - Encrypt the secret key with OAEP padding
- Sign (encrypt with private key) a hash of the message
  - A short block that is associated with the message

RSA Paper

"The need for a courier between every pair of users has thus been replaced by the requirement for a single secure meeting between each user and the public file manager when the user joins the system."

Key Management

Public keys only useful if you know:

1. The public key matches the entity you think it does (and no one else).
2. The entity is trustworthy.

Approach 1: Public Announcement

- Publish public keys in a public forum
  - USENET groups
  - Append to email messages
  - New York Time classifieds
- Easy for rogue to pretend to be someone else

Approach 2: Public Directory

- Trusted authority maintains directory mapping names to public keys
- Entities register public keys with authority in some secure way
- Authority publishes directory
  - Print using watermarked paper, special fonts, etc.
  - Allow secure electronic access

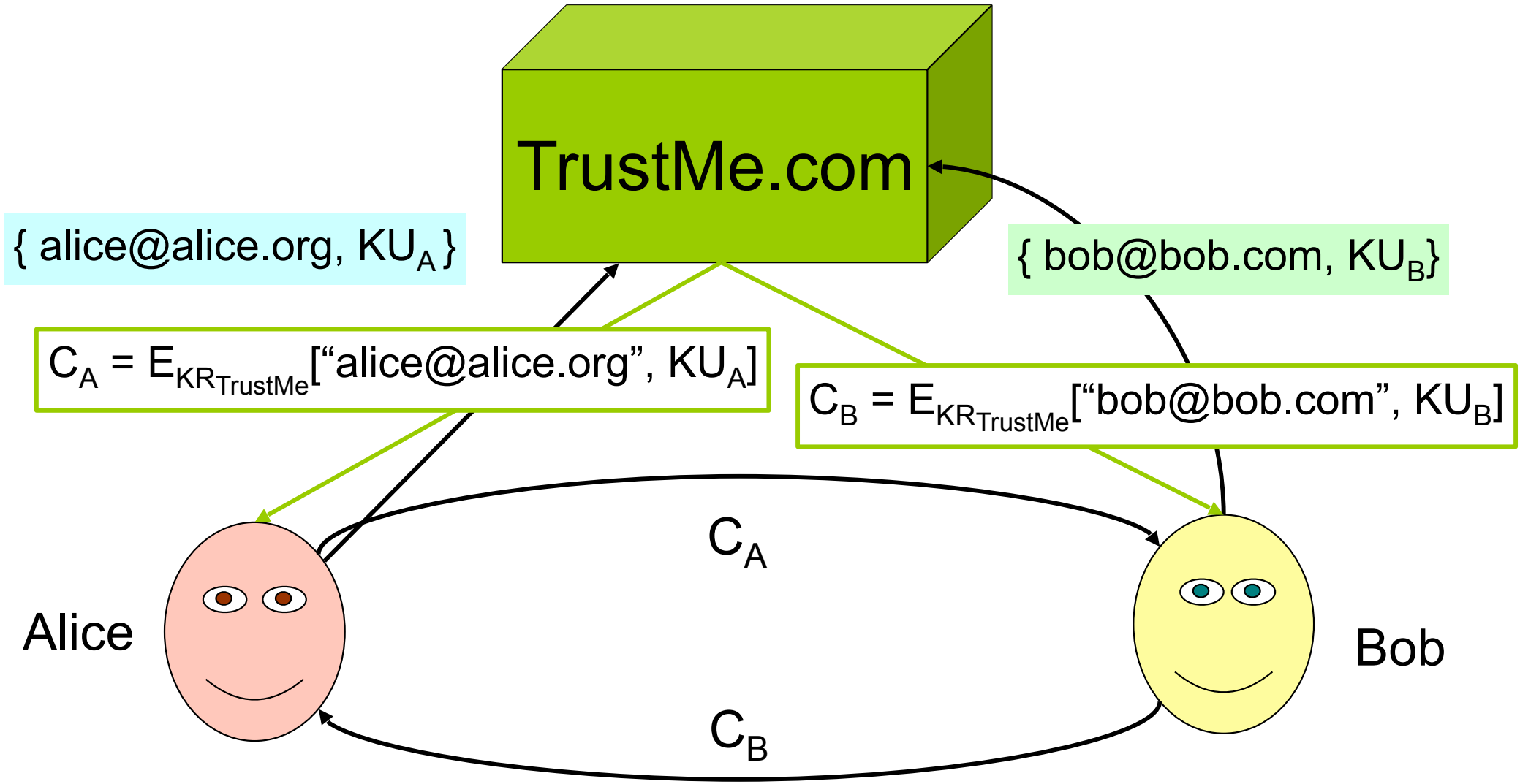
Can we avoid needing an on-line directory?

Certificates

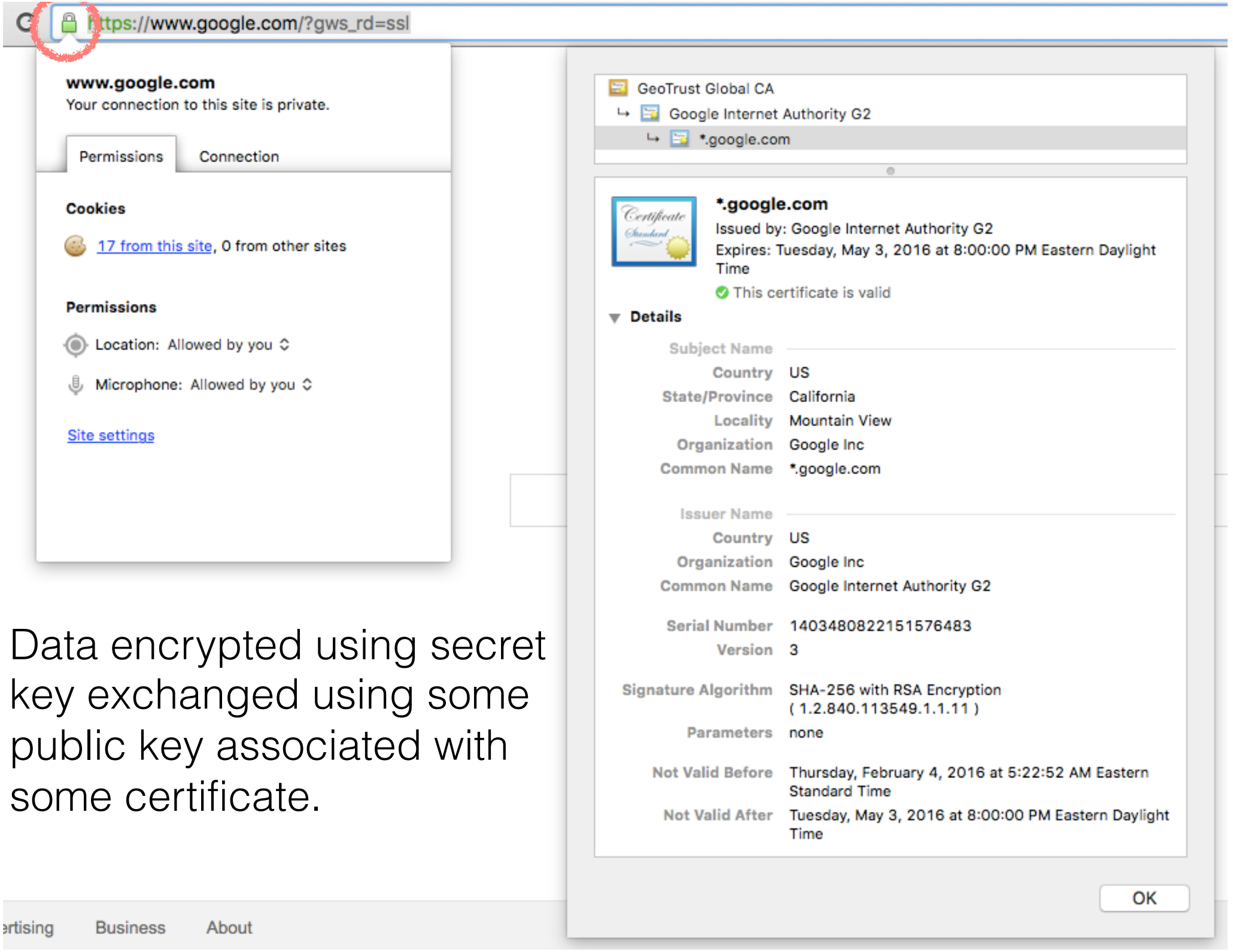
Loren Kohnfelder, MIT 4th year thesis project, 1978: Towards a Practical Public-key Cryptosystem

"Public-key communication works best when the encryption functions can reliably be shared among the communicants (by direct contact if possible). Yet when such a reliable exchange of functions is impossible the next best thing is to trust a third party. Diffie and Hellman introduce a central authority known as the Public File… Each individual has a name in the system by which he is referenced in the Public File. Once two communicants have gotten each other's keys from the Public File then can securely communicate. **The Public File digitally signs all of its transmission so that enemy impersonation of the Public File is precluded."**

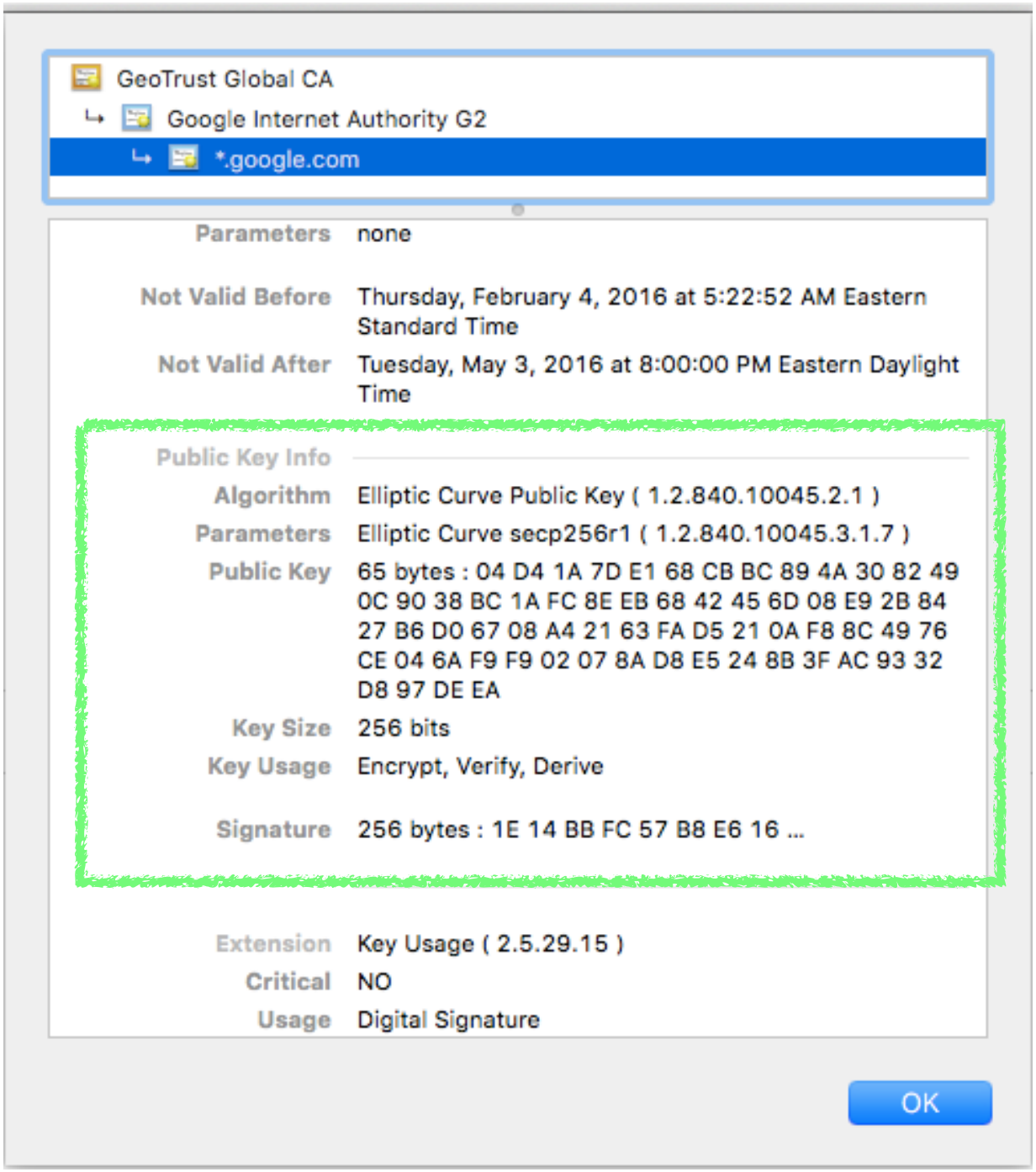
Certificates



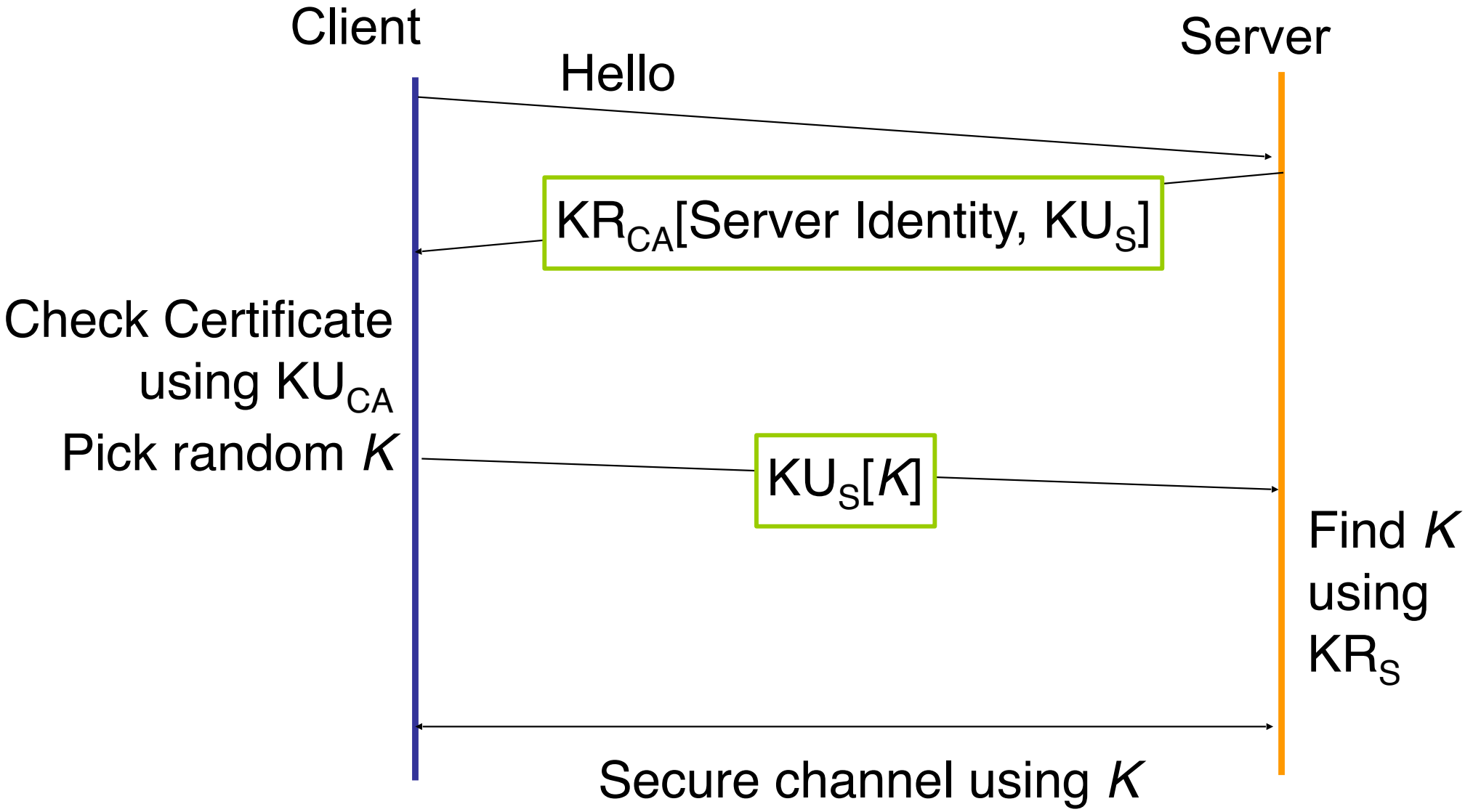
KU — Public Key
KR — Private Key



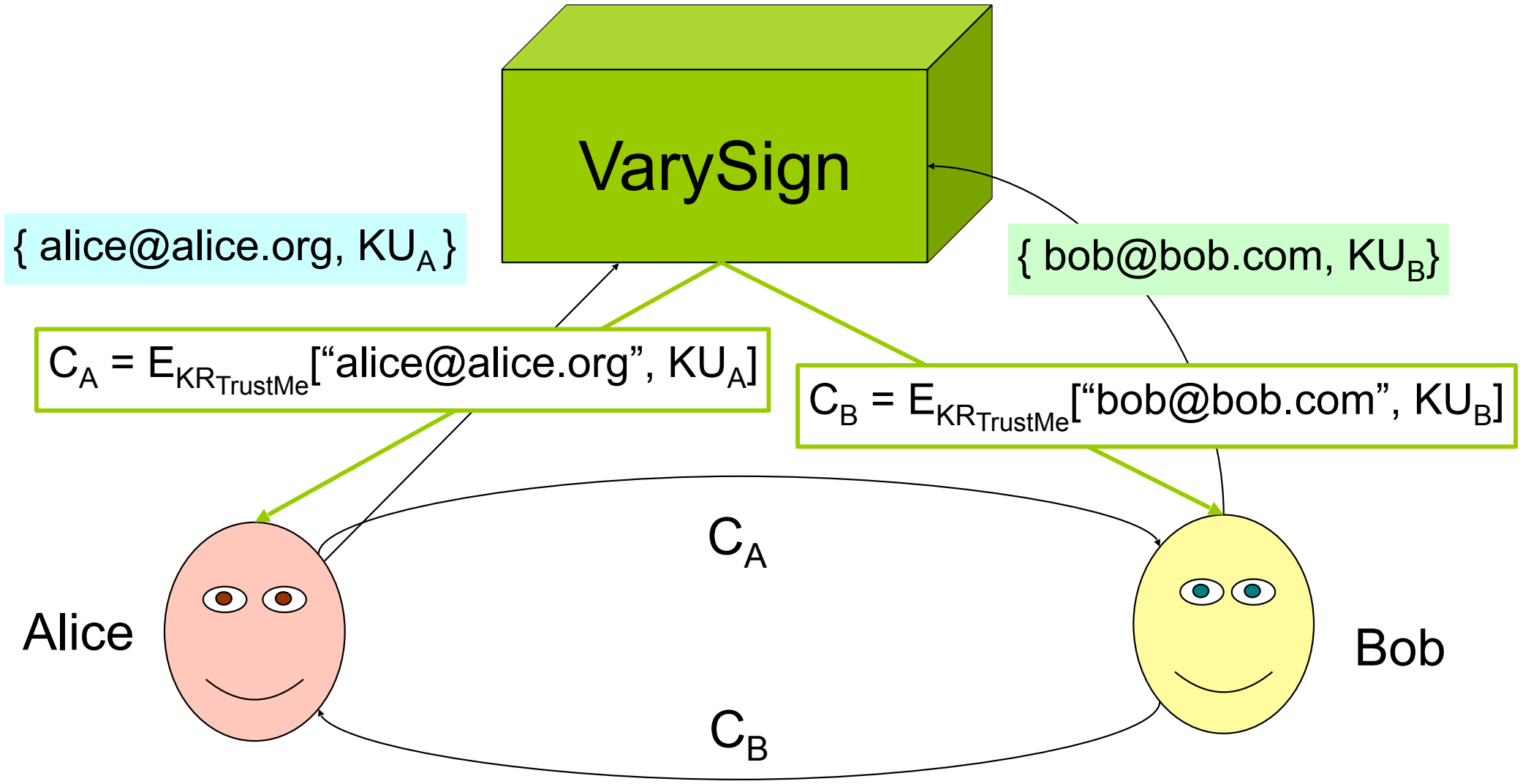
Data encrypted using secret key exchanged using some public key associated with some certificate.


GeoTrust Global CA
Google Internet Authority G2
*.google.com
Parameters none
Not Valid Before Thursday, February 4, 2016 at 5:22:52 AM Eastern Standard Time
Not Valid After Tuesday, May 3, 2016 at 8:00:00 PM Eastern Daylight Time
Public Key Info
Algorithm Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key 65 bytes : 04 D4 1A 7D E1 68 CB BC 89 4A 30 82 49 0C 90 38 BC 1A FC 8E EB 68 42 45 6D 08 E9 2B 84 27 B6 D0 67 08 A4 21 63 FA D5 21 0A F8 8C 49 76 CE 04 6A F9 F9 02 07 8A D8 E5 24 8B 3F AC 93 32 D8 97 DE EA
Key Size 256 bits
Key Usage Encrypt, Verify, Derive
Signature 256 bytes : 1E 14 BB FC 57 B8 E6 16 ...
Extension Key Usage (2.5.29.15)
Critical NO
Usage Digital Signature
OK

SSL (Secure Sockets Layer)
Simplified TLS Handshake Protocol

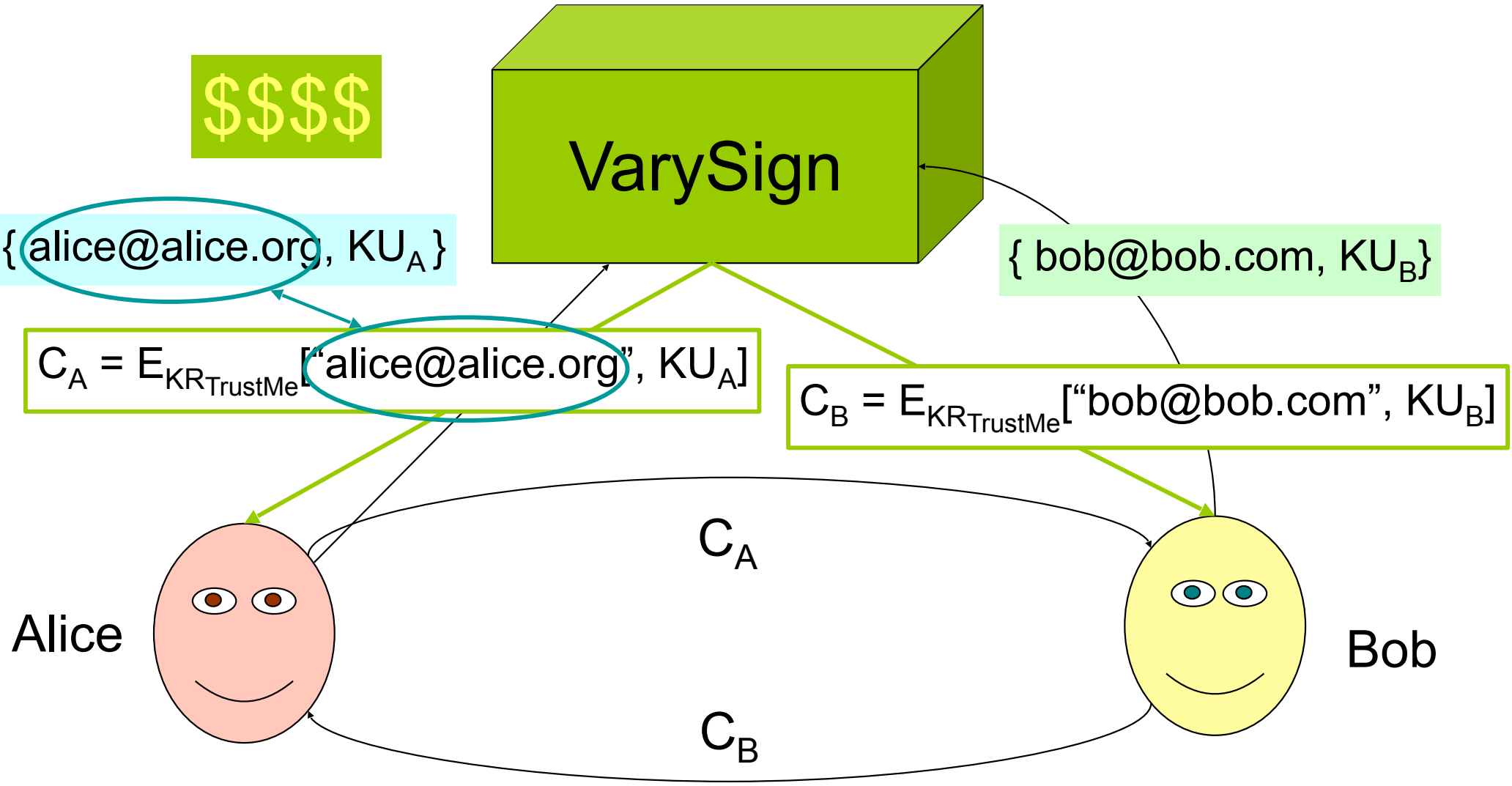


Certificates



How does TrustMe.com decide whether to provide Certificate?

Verifying Identities



http://www.verisign.com - Compare All SSL Certificates from VeriSign, Inc. - Mozilla Firefox

VeriSign

Compare All SSL Certificates

Close Window

Option	Secure Site SSL Certificates	Secure Site Pro True 128-Bit SSL	Commerce Site SSL Certificates	Commerce Site Pro True 128-bit SSL	Managed PKI for SSL Standard Edition	Managed PKI for SSL Premium Edition	Managed PKI for Intranet SSL Standard Edition	Managed PKI for Intranet SSL Premium Edition
View Product Description	Product Info	Product Info	Product Info	Product Info	Product Info	Product Info	Product Info	Product Info
Ready to Buy?	Buy Now	Buy Now	Buy Now	Buy Now	Contact Sales	Contact Sales	Contact Sales	Contact Sales
Price: 2-Year Certificate	$598	$1,790	$1,798	$2,795	Contact Sales	Contact Sales	Contact Sales	Contact Sales
Price: 1-Year Certificate	$349	$995	$949	$1,495	$249/certificate for 10	$695/certificate for 10	$179/certificate for 10	$489/certificate for 10
Number of certificates	Single	Single	Single	Single	5, 10, 25, 50, 100, more	5, 10, 25, 50, 100, more	5, 10, 25, 50, 100, more	5, 10, 25, 50, 100, more
Free SSL Trial	Free SSL Trial	-						
Minimum SSL Encryption	40-bit	128-bit						
Issuance	Standard	Express delive						by
Online Payment Processing	-	-						
VeriSign NetSure Protection Warranty	$100,000	$250,000						
Qualys Guard	-	Free						
Netcraft	-	Free *$1,000 value*	Free *$1,000 value*	Free *$1,000 value*	-	-	-	-
Keynote Red Alert	-	Free	Free	Free	-	-	-	-
VeriSign Secured Seal	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured
Authentication	2 factor authentication	2 factor authentication	2 factor authentication	2 factor authentication	Class 3 organizational authentication	Class 3 organizational authentication	Class 3 organizational authentication	Class 3 organizational authentication

With over half a million businesses authenticated, VeriSign follows a rigorous and independently audited authentication process. All involved VeriSign employees pass stringent background checks, and each authentication is split between multiple individuals. We maintain physically secure facilities, including biometric screening on entry.

VeriSign's Certificate Classes

- "Secure Site" SSL Certificate
  - Supports 40-bit session key
  - Proves: you are communicating with someone willing to pay VeriSign $598 (or with ~$1000 to break a 40-bit key)
  - Except they have a free 14-day trial (but it uses a different Trial CA key)


http://www.verisign.com - Why SGC-Enabled Certificates? - SGC SSL Certificates f...
VeriSign
Why SGC-Enabled Certificates?
Without an SGC-enabled certificate in place, site visitors using certain older browsers and many Windows 2000 users will only receive 40- or 56-bit encryption.
VeriSign (including its affiliates, resellers, and subsidiaries) is the only leading SSL provider with SGC-enabled SSL Certificates that can provide true 128- or 256-bit encryption to the most Web site visitors.
128-bit encryption offers 2^{88} times as many possible combinations as 40-bit encryption. That's over a trillion times a trillion times stronger.
Isn't your customer's trust worth it?
Close Window
Transferring data from server.iad.liveperson.net...
Adblock

“Secure Site Pro” Certificate

- $995 per year
- “true 128-bit key”

  “128-bit encryption offers 2^{88} times as many possible combinations as 40-bit encryption. That’s over a trillion times a trillion times stronger.”

  trillion = 10^{12} trillion * trillion = 10^{24}

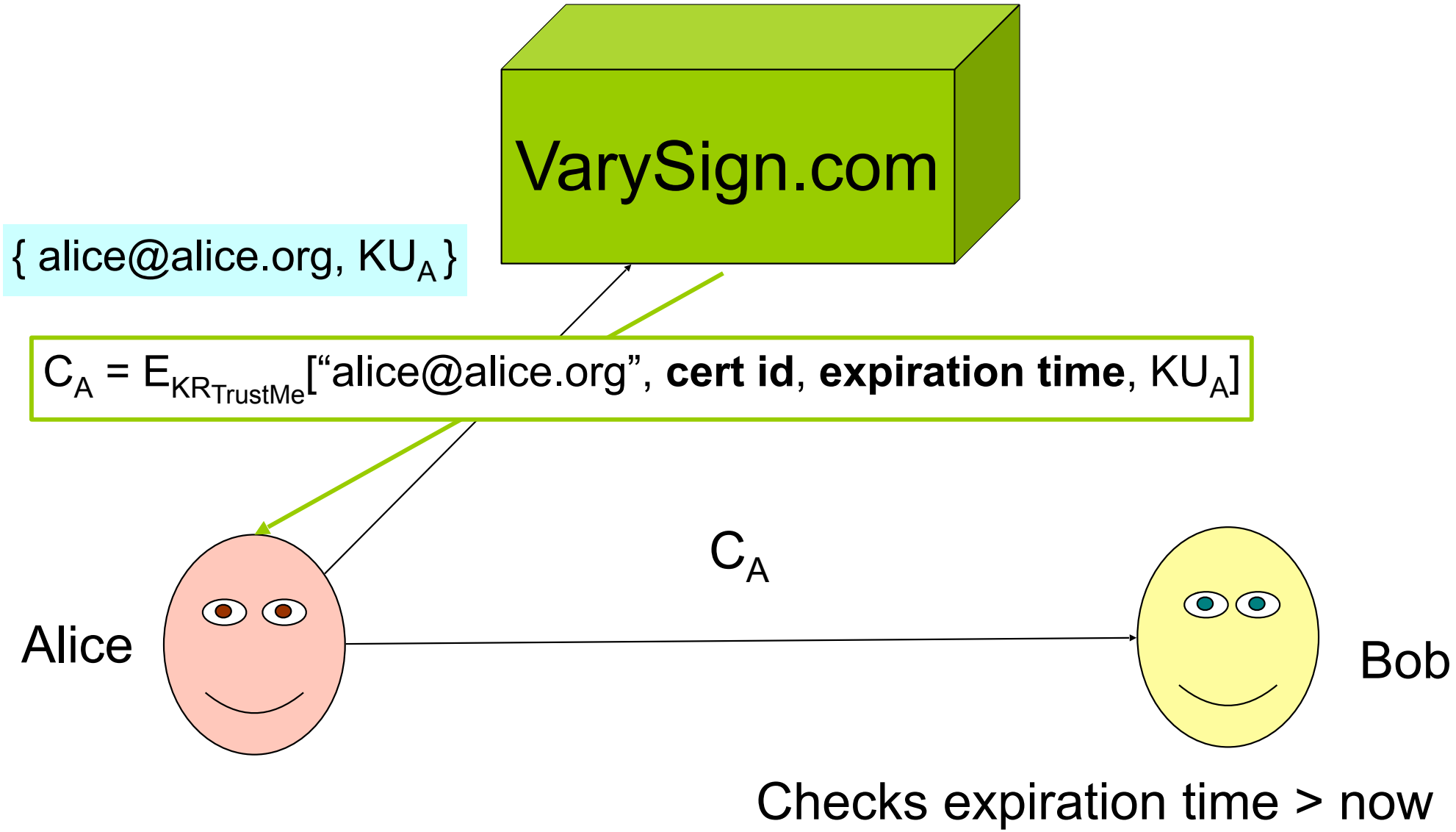
  Verisign’s marketing claim could be:

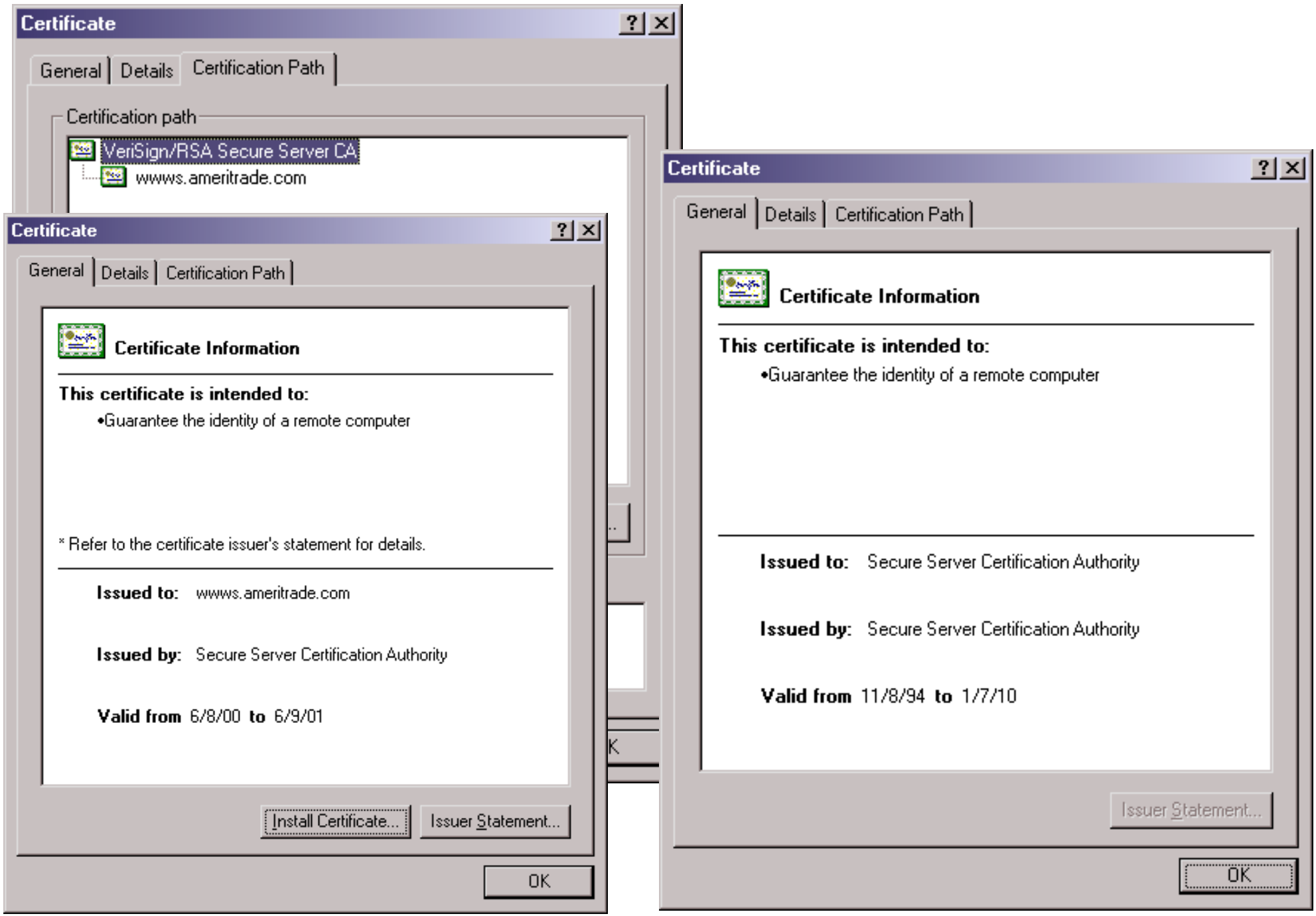
  “trillion times a trillion times a trillion times a trillion times a trillion times a trillion times a trillion times a trillion times ten thousand (in Britain it is a trillions time a trillion times a trillion times a trillion times a billion times a thousand) times stronger”

  (but that would sound even sillier!)
- Businesses authentication: “out-of-band” communication, records

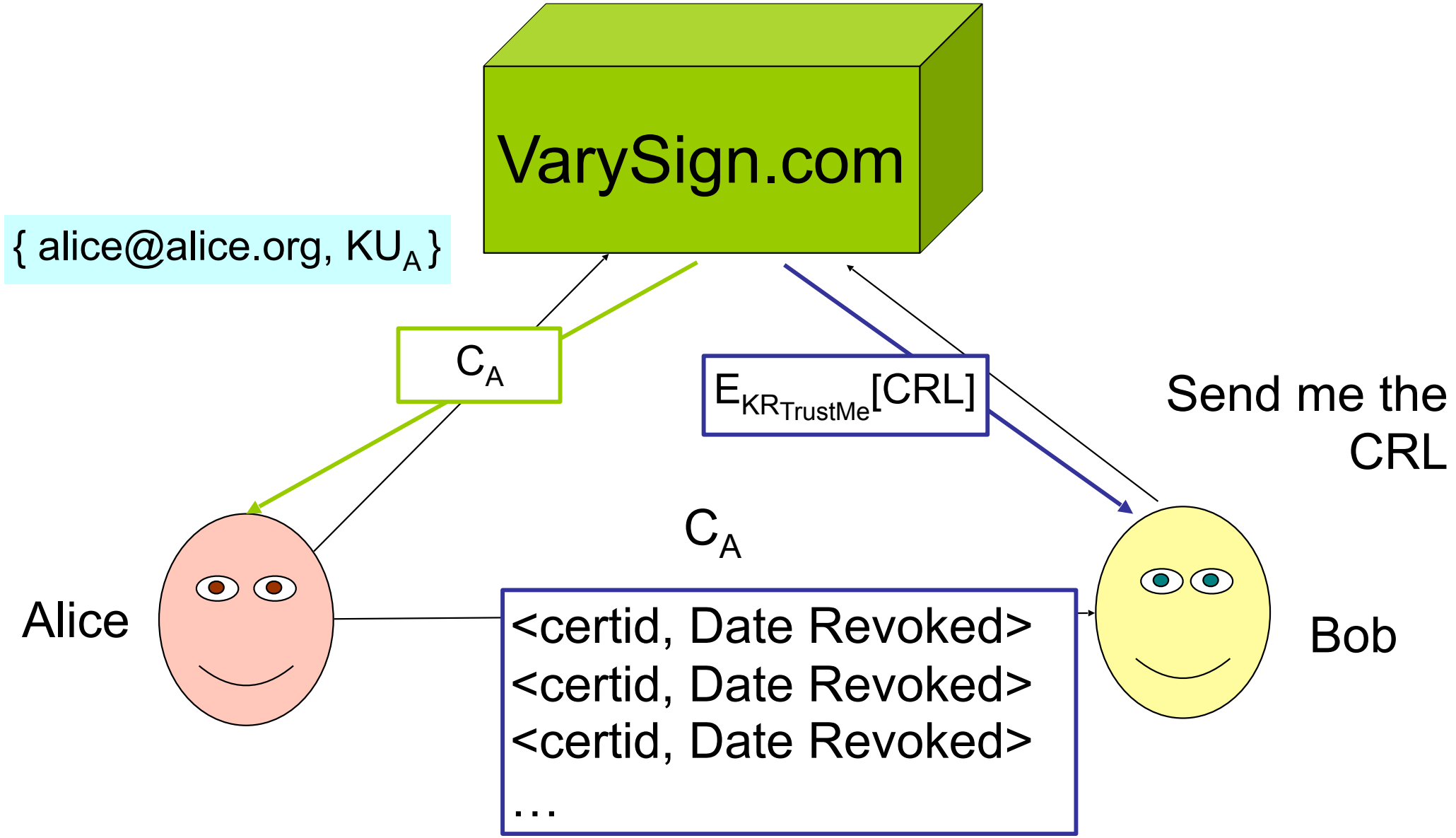

VeriSign Inc. - www.verisign.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.verisign.com/developer/notice/authenticode/
Go Links
VeriSign
HOME | PRODUCTS | CONSULTING | TRAINING | SUPPORT | CORPORATE
SEARCH:
All VeriSign GO
CORPORATE
Hot Jobs
Investor Relations
News Center
Contact Us
RESOURCES
Repository
Site Map
VERISIGN
International GO
Home > Security Notice
VeriSign Security Alert Fraud Detected in Authenticode Code Signing Certificates March 22, 2001
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. In this scenario, it is possible that the fraudulent party could create a destructive program or ActiveX control, then sign it using either certificate and host it on a Web site or distribute it to other Web sites.
Local intranet

Limiting The Damage




Certificate
General
Details
Certification Path
Certification path
VeriSign/RSA Secure Server CA
wwws.ameritrade.com
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended to:
•Guarantee the identity of a remote computer
* Refer to the certificate issuer's statement for details.
Issued to: wwws.ameritrade.com
Issued by: Secure Server Certification Authority
Valid from 6/8/00 to 6/9/01
Install Certificate...
Issuer Statement...
OK
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended to:
•Guarantee the identity of a remote computer
Issued to: Secure Server Certification Authority
Issued by: Secure Server Certification Authority
Valid from 11/8/94 to 1/7/10
Issuer Statement...
OK

Revoking Certificates



Certificate Questions

- How do participants acquire the authority's public key?
- If authority's private key is compromised, everything is vulnerable!
  - Keep the key locked up well

Problems with Certificates

- Depends on a certificate authority
  - Needs to be a big, trusted entity
  - Needs to make money (or be publicly funded)
- Need to acquire a certificate
  - Makes anonymity difficult
  - Requires handshaking

PGP (Pretty Good Privacy)

- Keyring: list of public keys, signed by owner's private key

  Alice's keyring:

  $E_{KR_{Alice}}$ (<"bob@bob.com", KU_{Bob}>,

  <"cathy@sharky.com", KU_{Cathy}>)

- Exchanging Keyrings (Web of Trust)
  - Complete Trust: I trust Alice's keyring (add the public key pairings to my own keyring)
  - Partial Trust: I sort of trust Alice, but require confirmation from someone else too (I need to get $E_{KR_{Cathy}}$ (<"bob@bob.com", KU_{Bob}>) before trusting KU_{Bob}

Charge

- Look at the certificate chains when you browse the web
  - Find a certificate with a trust chain more than two levels deep
- Update your browser CRLs: when were they last updated?

Avoiding Certificates

- What if your identity (e.g., your email address) is your public key?

- Is it possible to do this with RSA?

  Do you want your email address to be a 200-digit “random” number?

Identity Based Encryption

- [Shamir 1984], [Boneh & Franklin 2003]

  public-key = identity

  private-key = F(master-key, identity)

The owner of the master-key is the new authority. Must be careful who it gives private keys to.

Key-Generating Service

- Holds master-key
- Participants request private keys from KGS
  - Sends s to KGS, requests corresponding private key
  - KGS authenticates requestor
  - If valid, computes F(master-key, s) and sends over secure channel
- How does the trust given to the KGS compare to that given to CA in SSL?

KGS can decrypt all messages! With certificates, certificate owner still has her own private key.

But, CA can impersonate anyone by generating a certificate with a choosen public-key.

Shamir's IBE Signature Scheme

- Setup: done by KGS
  - Select p, q large primes
  - $N = pq$
  - Choose e relatively prime to $\varphi(N) = (p\text{-}1)(q\text{-}1)$
  - Choose d satisfying $ed \equiv 1 \bmod \varphi(N)$
  - Choose h a cryptographic hash function
- Publish N, e and h to all participants
- Keep d secret master-key

Shamir's Signatures

- Generating a private key

  privatekey(ID) = $ID^d \bmod N$

  – Can only be done by KGS (d is master secret)

- Signing a message M with identity ID

  – Obtain g = privatekey(ID) from KGS

  – Choose random r less than N

  – Compute signature (s, t):

$$t = r^e \bmod N$$

$$s = g\, r^{h(t \| M)} \bmod N$$

Warning: book typesetting is off and wrong range for h!

Verifying a Signature

- KGS produced $g = ID^d \bmod N$
- Recipient knows ID and M, system parameters e and N

$$t = r^e \; mod \; N$$

$$s = g \; r^{h(t \,\|\, M)} \bmod N$$

- Verify (ID, s, t, M)

$$s^e = ID \; t^{h(t \,||\, M)} \bmod N$$

$$(ID^d \; r^{h(t \,\|\, M)})^{e} \bmod N$$
$$\equiv ID^{de} \, r^{h(t \,\|\, M)e} \bmod N$$
$$\equiv ID \; r^{eh(t \,\|\, M)} \bmod N$$
$$\equiv ID \; t^{h(t \,\|\, M)} \bmod N$$

What does non-forgibility of a Shamir IBE signature rely on?

Identity-Based Encryption

- Shamir's scheme – signatures only, not encryption
- Boneh & Franklin, 2001
  - First practical, provably secure IBE scheme
  - Builds on elliptic curves

Issues in IBE

- Complete trust in KGS
  - With Boneh & Franklin's system can use secret sharing techniques to divide this trust among multiple entities
  - Could you do this with Shamir's IBE signatures?
- Revocation
  - Can include expiration times in identities
  - But no way to revoke granted private keys