

Introduction to Digital Certificates

WICS-Stanford University
July 29, 1998



Jim Cowing
Digital Resources Group

jim@drgsf.com
415.508.8959
www.drgsf.com

Agenda

- ❖ **Goals and Overview**
- ❖ **What is a Digital Certificate**
- ❖ **Purpose of a Digital Certificate**
- ❖ **Types of Certificates**
- ❖ **Industry Variation**
- ❖ **Certificate Usage Today**
- ❖ **Certificate Authorities**
- ❖ **Obtaining a Digital Certificate**



Goals and Overview

- ❖ What are Certificates?
- ❖ Why are they important to E-Commerce?
- ❖ Trust
- ❖ Practical issues: Browser location and Obtaining a certificates
- ❖ Types of certificates
- ❖ What is a Certificate Authority?
- ❖ Barriers to Certificates



Internet Commerce Today

News and Content (NY Times, WSJ, SJ Mercury News)

Shopping (Amazon.com; 800 Flowers, Autos by Tel)

**Travel and Entertainment (Airlines -United, Hotels- Hyatt-
Rental Cars-Hertz)**

Banking and Brokerage (Wells Fargo, Citibank & Schwab)

Governments (IRS, FTB, Treasury, federal agencies)

Health Care (Kaiser, HealthNet)

Information (MSNBC; CNN; Cnet; TechWire)



Keys to Internet Commerce ?

Willing Buyer and Seller

Product

Payment Mechanisms

Security

TRUST



Forms of Trust

Physical World

DMV Drivers License

Government Passport, or SSN Card

Bank ATM Card & PIN

Grocery Store Drivers License/ATM

Health Club Club Affiliation Card

Electronic World

Internet: Digital Certificates



What is a Certificate?

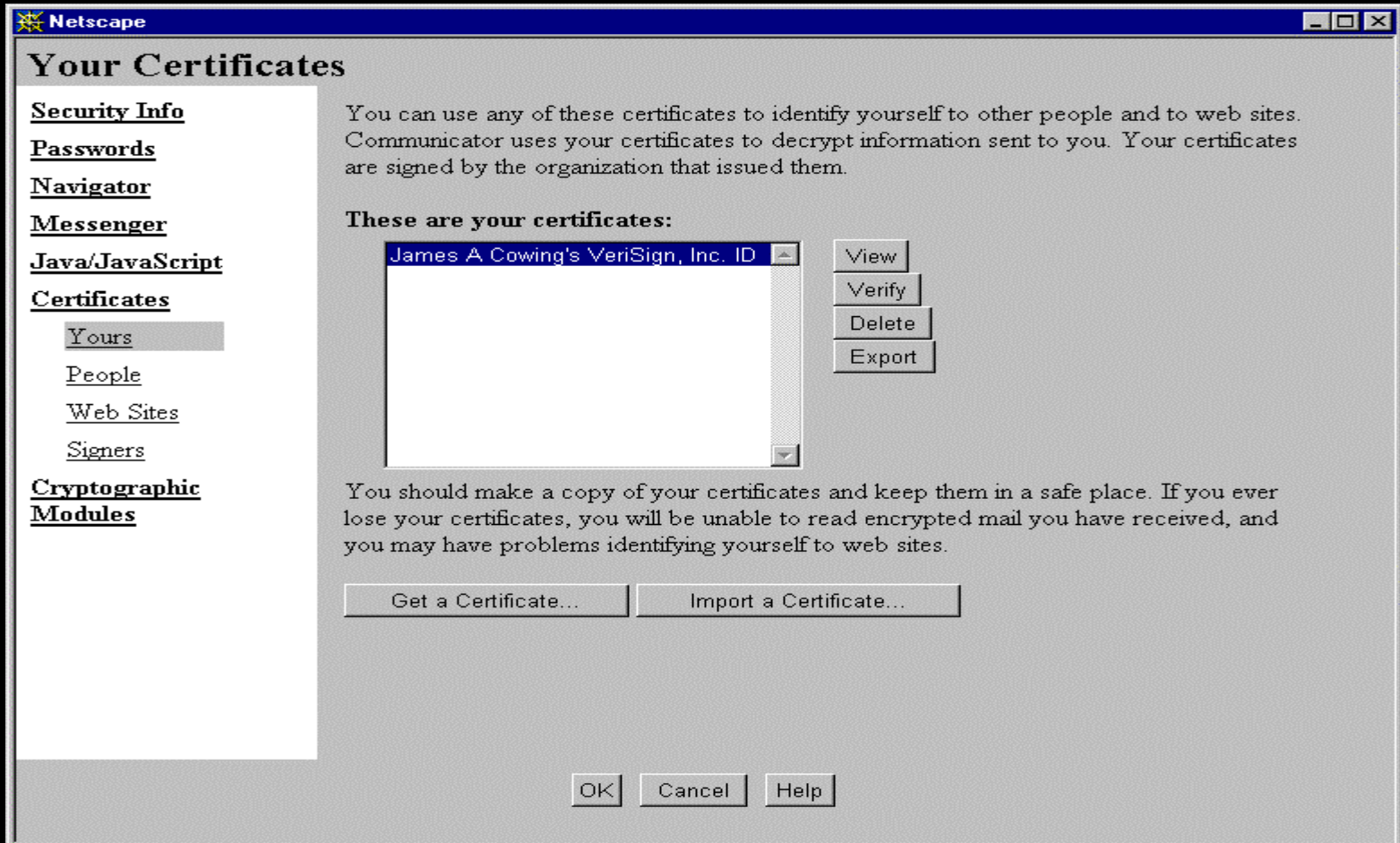
- ❖ Digital Document which attests to the binding of a public key of an individual or other entity.
- ❖ Verifies authenticity of the public key.
- ❖ Prevent impersonation by using a phony key.



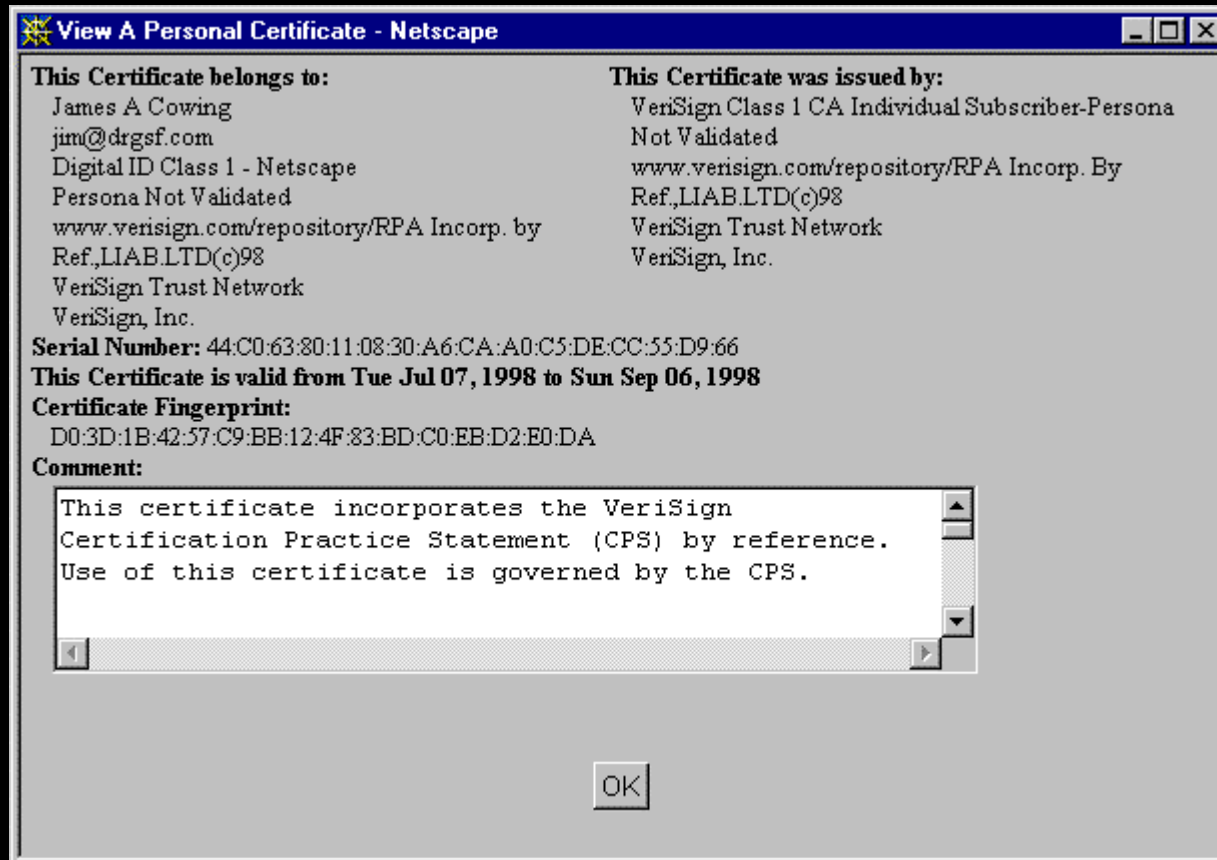
Digital Certificates contain:

- ❖ Name of Entity being Certified
- ❖ Public Key
- ❖ Name of Certificate Authority
- ❖ Serial Number
- ❖ Expiry Date
- ❖ Other information (optional)

Storing Your Digital Certificate



Viewing a Digital Certificate Netscape



Viewing a Digital Certificate Microsoft IE

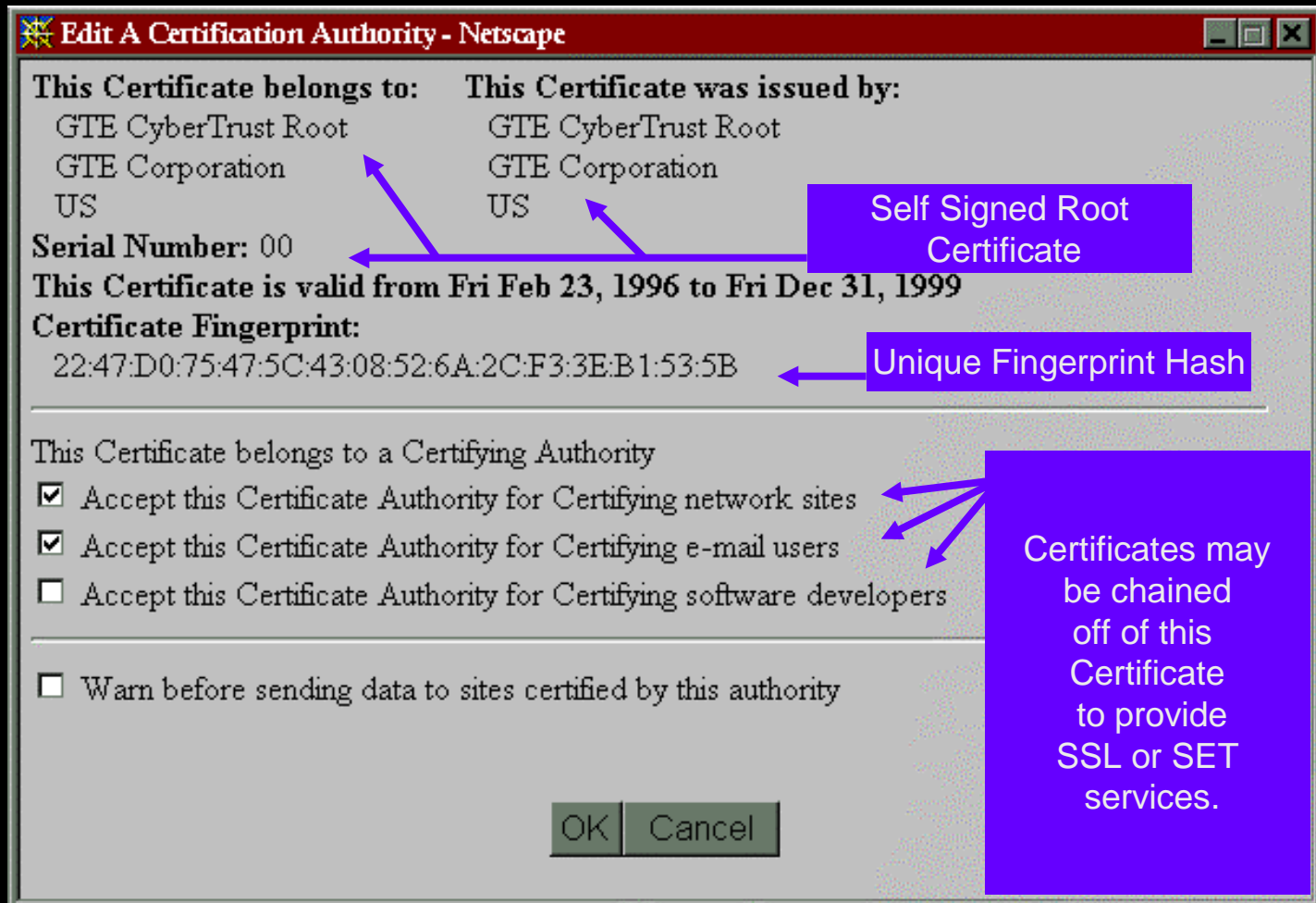





Levels of Digital Certificates

- ❖ Individual Certificates
- ❖ Subordinate RA Certificates
- ❖ Root Certificates
- ❖ Hierarchical Chaining of Certificates

Digital Certificate -- Root CA Certificate



Edit A Certification Authority - Netscape

This Certificate belongs to:
GTE CyberTrust Root
GTE Corporation
US

This Certificate was issued by:
GTE CyberTrust Root
GTE Corporation
US

Serial Number: 00

This Certificate is valid from Fri Feb 23, 1996 **to** Fri Dec 31, 1999

Certificate Fingerprint:
22:47:D0:75:47:5C:43:08:52:6A:2C:F3:3E:B1:53:5B

This Certificate belongs to a Certifying Authority

- Accept this Certificate Authority for Certifying network sites
- Accept this Certificate Authority for Certifying e-mail users
- Accept this Certificate Authority for Certifying software developers

Warn before sending data to sites certified by this authority

OK Cancel

Self Signed Root Certificate

Unique Fingerprint Hash

Certificates may be chained off of this Certificate to provide SSL or SET services.



What is a Certificate Authority

- ❖ Trusted authority that issues a certificate that vouches for the identity of those to whom it issues certificates with a given public key.
- ❖ CA's public key must be trustworthy.



Certificate Issuance Process

- ❖ Generate public/private key pair
- ❖ Sends public key to CA
- ❖ Proves identity to CA - verify
- ❖ CA signs and issues certificate
- ❖ CA e-mails certificate or Requestor retrieves certificate from secure website.
- ❖ Requestor uses certificate to demonstrate legitimacy of their public key.

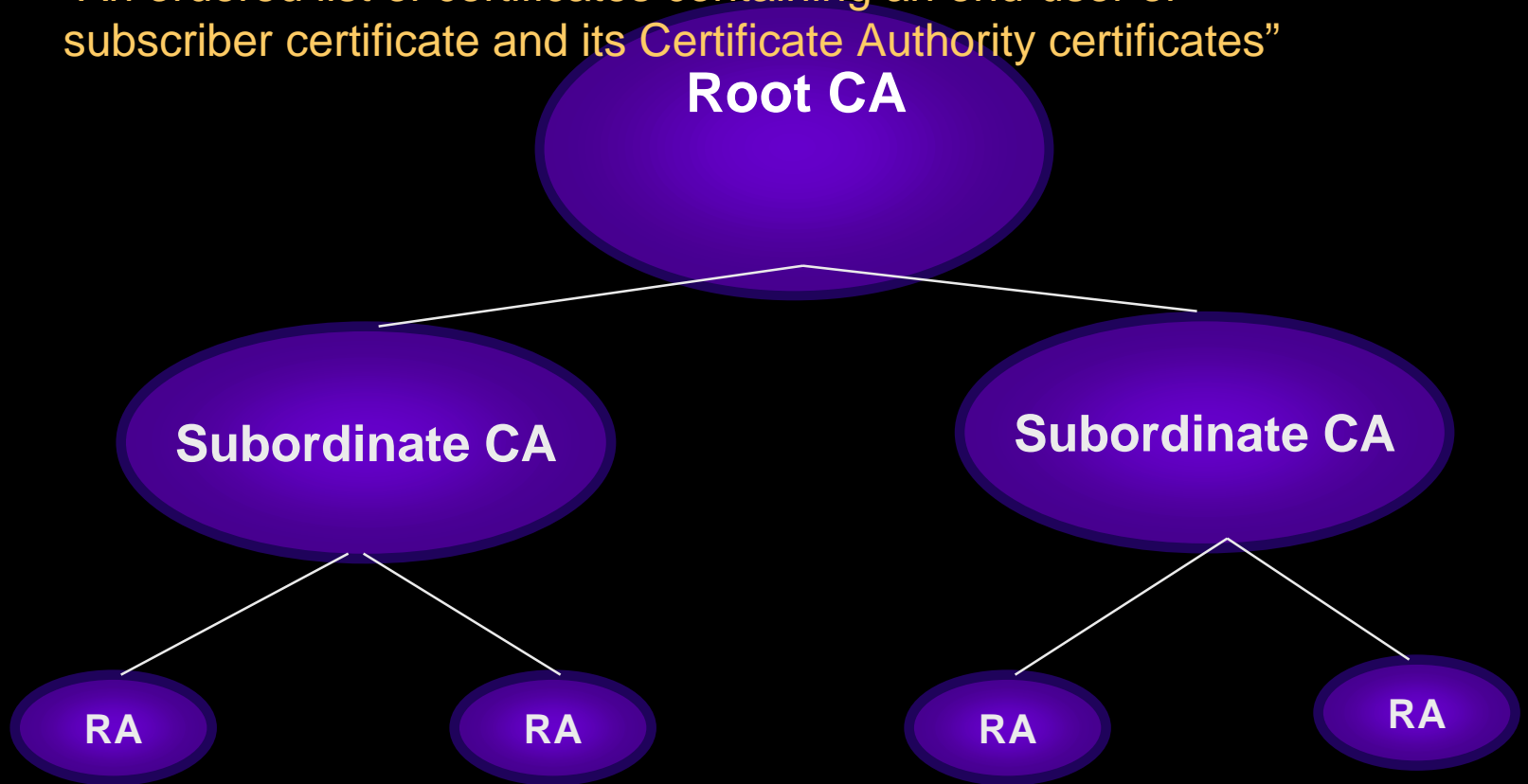


Certificate Hierarchies

- ❖ Trusted Chain or Hierarchies
- ❖ Root Certificate
- ❖ Subordinate CA Certificates
- ❖ Registration Authority Certificates
- ❖ End-User Certificates
- ❖ Multiple Roots in a trusted Chain

Certificate Chains

“An ordered list of certificates containing an end-user or subscriber certificate and its Certificate Authority certificates”



*Hierarchical
Chain of Trust*



CA versus RA

- ❖ Delegation of Authority or Segregation of Roles - Issuance and authentication
- ❖ Issuance: Physical process of signing the certificate
- ❖ Authentication: Determining the identity and relationship of public key and signer
- ❖ **CERTIFICATION AUTHORITY (CA)**: Person or entity with authority to issue certificates.
- ❖ **REGISTRATION AUTHORITY (RA)**: Entity trusted to register other entities or to authenticate those who are being issued a certificate.



Who are the Certificate Authorities

VeriSign

GTE CyberTrust

Entrust

IBM

CertCo

USPS / Cylink



Types of Certificates

- ❖ E-Mail Certificates
- ❖ Browser Certificates
- ❖ Server (SSL) Certificates
- ❖ Software Signing Certificates
- ❖ Corporate Empowerment Certificates
- ❖ SET Certificates
- ❖ EDI Certificates

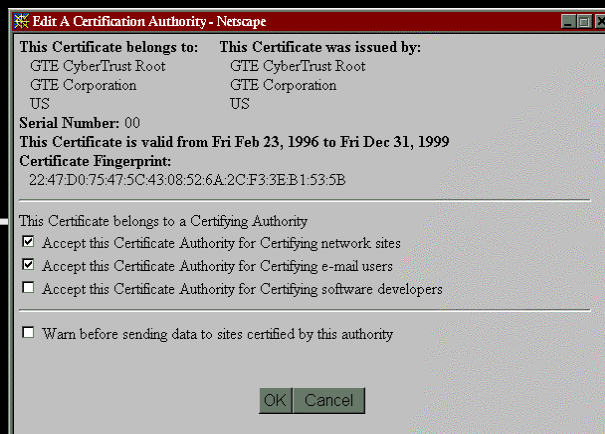
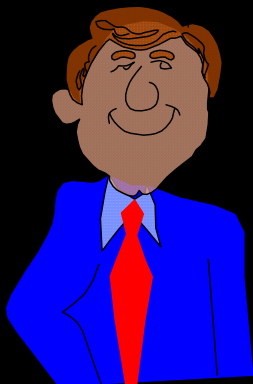


Roles of Certificates

- ❖ Identity (Validation)
- ❖ Brand (Relationship)
- ❖ Server (SSL)
- ❖ Security and Authentication (SET)

Uses of Digital Certificates in the Corporate World

Employee



Remote Access

Intranet

Email

HR Records

Internet

Mainframes

Potential cost savings.



Users of Digital Certificates

- ❖ Internet Banking
- ❖ Internet Brokerage
- ❖ Internet Content Publishers
- ❖ Software Publishers
- ❖ Health Care
- ❖ Secure Electronic Transactions (SET)



Barriers to Certificates

- ❖ Portability
- ❖ Liability
- ❖ Interoperability
- ❖ Revocation
- ❖ Market Acceptance
- ❖ Password-based reliance



Other Challenges to Certificates

- ❖ Authentication process
- ❖ Secure request methods - email / web-based
- ❖ Distribution channels - email / web
- ❖ Revocation/renewal process
- ❖ Support infrastructure
- ❖ Preparedness for compromise

More Digital Certificate Information

National Institute for Standards and
Technology (NIST)
www.nist.gov

RSA www.rsa.com

IBM World Registry
www.ibm.com/security

VeriSign FAQ

http://digitalid.verisign.com/client/help/id_intro.htm

http://digitalid.verisign.com/client/help/crp_intr.htm

Microsoft

www.microsoft.com/security

VeriFone

www.verifone.com

GlobeSet

www.globeset.com

DRG Digital Resources Group



Secure Electronic Commerce Consulting