WEB SECURITY

By Dr. V. DEEPIKA

Textbooks:

1. Web Security, Privacy and Commerce, Simson GArfinkel, Gene Spafford, O'Reilly.
2. Handbook on Database security applications and trends, Michael Gertz, Sushil Jajodia.

Unit - I

- The Web Security Problem
- Risk Analysis and Best Practices
- Cryptography and the Web
  - Cryptography and Web Security
  - Working Cryptographic Systems and Protocols
  - Legal Restrictions on Cryptography
- Digital Identification I: Passwords, Biometrics, and Digital Signatures
  - Physical Identification
  - Using Public Keys for Identification
  - Real-World Public Key Examples
- Digital Identification II: Digital Certificates, CAs, and PKI
  - Understanding Digital Certificates with PGP
  - Certification Authorities: Third-Party Registrars
  - Public Key Infrastructure
  - Open Policy Issues

WS Prerequisites

- Fundamental Computer Science Knowledge
- Networking & Internet Technologies
- Programming Skills
- Web Technologies
- Databases
- Operating System Security Basics
- Introductory Cryptography Concepts
- Basic Cybersecurity Principles

Fundamental Computer Science Knowledge

- Computer architecture and operating systems basics
- Memory, processes, CPU, file systems
- Basic networking concepts (DNS, IP, TCP/UDP, HTTP/HTTPS)

Networking & Internet Technologies

- OSI and TCP/IP models
- Basic routing and switching
- How web browsers and web servers communicate
- Client–server architecture
- HTTP methods (GET, POST, PUT, DELETE)

Programming Skills

- Python / Java / C / C++ / JavaScript
- Ability to write functions, handle input/output, use libraries
- Basic debugging and code testing skills

Web Technologies

- HTML, CSS, JavaScript
- Web application architecture
- Forms, cookies, sessions
- REST APIs (basics)

Databases

- Relational databases (MySQL, PostgreSQL, Oracle)
- SQL queries (SELECT, INSERT, UPDATE, DELETE)
- Joins, views, triggers, stored procedures
- Basic knowledge of NoSQL is beneficial (MongoDB)
- Understanding of indexing and query processing

Operating System Security Basics

- User accounts and permissions
- Filesystem permissions (read/write/execute)
- Process management
- Basic Linux/Windows administration

Introductory Cryptography Concepts

- Encryption vs. hashing
- Symmetric vs. asymmetric keys
- Digital signatures
- Certificates and PKI

Basic Cybersecurity Principles

- CIA triad (Confidentiality, Integrity, Availability)
- Threats, vulnerabilities, attack surface
- Malware types: viruses, worms, ransomware
- Security policies and best practices

Web security

Web Security (also called *Cybersecurity for the Web*) refers to the protections, techniques, and practices used to secure websites, web applications, and web services from threats, attacks, and unauthorized access.

It ensures:

- Confidentiality (data is protected)
- Integrity (data is not modified)
- Availability (services are accessible)
- Authentication & Authorization (only allowed users can access)

Why Web Security Is Needed

Because websites and web applications are frequently attacked by:

- Hackers
- Malware
- Bots
- Insider threats
- Network-level attacks

Examples of Web Security

1. **HTTPS / TLS Encryption:** Protects data transmitted between browser and server.

   Ex: When you see a lock icon in the browser, data is encrypted.

2. **Input Validation:** Prevents attackers from injecting harmful input.

   Ex: Rejecting a username like:

   admin' OR '1'='1

3. **Authentication & Authorization:** Ensures only legitimate users access resources.

   Ex: Multi-factor authentication (OTP login)

   Role-based access (Admin vs User)

4. **Web Application Firewall (WAF):** Filters and monitors HTTP traffic.

   Ex: Cloudflare WAF blocking SQL injection attempts.

5. **Secure Coding Practices:** Avoiding vulnerabilities while writing code.

   Ex: Using prepared statements in SQL

   Hashing passwords using bcrypt

Examples of Web Security

6. Protection Against Common Attacks:

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Clickjacking
- Denial of Service (DoS/DDoS)

7. Digital Certificates & PKI: Verifies authenticity of websites.

Ex: SSL certificate issued by DigiCert.

8. Regular Backups: Protects against data loss or ransomware.

Ex: Automatic daily backup of server files.

9. Server Hardening: Securing OS, software, and services.

Ex: Closing unused ports

Disabling default accounts

10. Monitoring & Logging: Tracks suspicious activities.

Ex: Failed login alerts

Intrusion detection systems (IDS)

Web security

"Web Security is the practice of protecting websites, servers, and users from cyber threats through encryption, authentication, secure coding, firewalls, and attack prevention mechanisms."

The Web Security Problem

A computer is *secure* when it behaves predictably and reliably.

Web security ensures that:

- Web servers
- Web browsers
- Web applications
- Internet infrastructure
- …all behave as expected, without unauthorized access or disruptions.

Three Primary Facets of Web Security

- Securing the Web Server
- Securing Information in Transit
- Securing the User's Computer

A. Securing the Web Server

You must ensure:

- Server keeps running (availability)
- Data on the server cannot be altered without permission (integrity)
- Only authorized users receive the data (confidentiality)

Tasks include:

- User authentication systems
- Secure scripts / applications
- Backup and recovery
- Logging, auditing, nonrepudiation
- Load balancing, redundancy, failover data centers
- Redundant Internet connections
- Securing DNS
- Protecting billing/records
- 24×7 monitoring (NOC)
- Physical security
- Staff training against emergencies + social engineering

B. Securing Information in Transit

Goal: Prevent others from reading, modifying, or destroying data exchanged between user and web server.

Protection methods:

- Physical network security (not practical)
- Hiding information (not reliable)
- Encryption (most practical → SSL/TLS)

SSL/TLS provides:

- Confidentiality
- Integrity
- Authentication

BUT SSL does not protect the endpoints (user device or server itself).

C. Securing the User's Computer

Users need:

- Virus-free, malware-free systems
- Secure browsers
- Privacy protections
- Safe handling of passwords/credentials

Threats:

- Viruses and worms (much more damaging than browser flaws)
- Automated attacks exploiting OS / application vulnerabilities
- Social engineering (e.g., worms)

Historically:

- Education was believed to be the solution
- Now: systems are too complex → rely more on technology (antivirus, sandboxes, automatic patching)

What Do Attackers Want?

Attackers try to make your system do things you don't want, such as:

- Steal confidential documents
- Corrupt or delete data
- Store illegal content on your machine
- Modify the OS to create new vulnerabilities
- Steal money (e.g., using banking apps)
- Block or deny access (DoS)
- Use your system to perform attacks on others
- Run unauthorized servers (IRC [Internet Relay Chat], botnet nodes)
- Gain publicity / recognition

Securing the Web Server

Layers to Secure:

- Underlying operating system (Unix, Windows, etc.)
- Web server software (Apache, IIS, Nginx)
- Scripts/Applications (CGI, PHP, ASP, Perl, etc.)

Common attack scenarios:

- Bad script lets attacker modify config and gain privilege
- Secure server but insecure database → attacker extracts user data

Securing the Web Server (cont..)

Hardening the server:

- Least privilege for users and processes
- Correct permissions for files and scripts
- Remove unnecessary services/features
- Separate services on different machines (mail, DB, web)
- Restrict admin access (SSH, secure tokens)
- Physical security
- Backup and disaster recovery

Policing Copyright

Goal: prevent illegal copying of web content.

Reality:

- Impossible to technically stop copying once data is displayed.
- Screenshots, recordings, photographs always possible.

Alternative:

- Digital watermarking

  Adds hidden marks in images/audio/video to track origin and ownership.

Securing Information in Transit – Details

Threats:

- Eavesdropping
- Modification of data
- Replay attacks
- Denial of Service (DoS)

Solution:

- SSL/TLS encryption

  Netscape's SSL enabled secure transmission of credit card numbers → boosted early e-commerce.

Limitations:

- SSL protects data *in transit* only, not at endpoints.
- DoS attacks can still disrupt service.

DoS events (example):
The Feb 2000 DoS attacks overwhelmed many major websites.

Securing the User's Computer – Details

Browser vulnerabilities existed but caused few real-world damages.

Actual major threats:

- Email-based worms (Email worms spread through infected email attachments or links.)
- Network service exploits (Exploiting vulnerabilities in network services like FTP, HTTP, DNS, SSH.)
- Malware infections (Infection by malicious software such as viruses, worms, ransomware, trojans.)

Reason:

Users often can't make correct security decisions due to complexity → need automated protection tools.

Risk Analysis and Best Practices

1. What is Risk Analysis?
2. Challenges of Risk Analysis in Computer Security
3. What are Best Practices?
4. Problems with Best Practices
5. Recommended Approach

By Dr. V. DEEPIKA

1. What is Risk Analysis?

Risk analysis is a process used to identify risks, estimate their likelihood, and evaluate the potential damage they can cause. Based on this, organizations create strategies to reduce or mitigate these risks.

Steps in Risk Analysis

1. Identify possible risks
2. Estimate the likelihood of each risk
3. Evaluate potential damage
4. Prioritize risks systematically

Example (Civil Engineering)

- Engineers calculate how much stress a bridge can handle.
- They estimate the chance of collapse and the potential damage.
- This helps to design safe, cost-effective structures.

2. Challenges of Risk Analysis in Computer Security

Risk analysis is less effective in computer security because:

- It is difficult to calculate the chances of attacks.
- New vulnerabilities appear constantly.
- We don't know whether risk increases or decreases over time.
- Damages from attacks are hard to estimate.
- Very few scientific studies exist.
- People often misjudge risk based on personal experience, not data.

3. What are Best Practices?

Best practices (also called due care) are a set of generally accepted guidelines, procedures, and policies believed to help organizations maintain a reasonable level of security.

- Best Practices = "Rules of thumb" for security.

Examples include:

- Keeping systems updated.
- Monitoring for new security threats.
- Applying security patches regularly.
- Using minimal software/services.
- Following standard security configurations.

4. Problems with Best Practices

- No single set of best practices fits all organizations.

  (e.g., a financial site vs. a community newsletter)
- Following best practices does not guarantee protection from all attacks.
- New, unpublished (zero-day) attacks can still succeed.
- Many organizations follow only the minimum standards, not the actual “best” practices.
- Best techniques may be too costly or unnecessary for some organizations.

5. Recommended Approach

It recommends combining risk analysis + best practices:

Balanced Approach

1. Start with known best practices
2. Perform risk analysis to adjust them
3. Apply only what is reasonable and suitable for your system
4. Use minimal required functionality on servers
5. Keep servers isolated
6. Stay updated with patches
7. Remain vigilant and prepared for unexpected issues

3. Cryptography and the Web Security

- Importance of Cryptography and Web Security
- Working Cryptographic Systems and Protocols
- Legal Restrictions on Cryptography

3.1. Importance of Cryptography in Web Security

- Cryptography protects data as it travels over the Internet.
- Used daily in web transactions, email, chat, VoIP, and conferencing.
- Without encryption, anyone with network access could read your data.
- Strong encryption makes intercepted data computationally impossible to decode.

Roles of Cryptography (Five Pillars)

a) Authentication

- Confirms identity of a user or sender.
- Digital signatures authenticate email/web transactions.
- Can complement passwords and biometrics.

b) Authorization

- Determines what an authenticated user is allowed to do.
- Cryptographic lists/keys help prevent falsification of access rights.

c) Confidentiality

- Encryption protects data from eavesdroppers.
- Ensures private communications over insecure networks.

Roles of Cryptography (cont..)

d) Integrity

- Ensures data has not been altered.
- Achieved using message digests & digital signatures.

e) Nonrepudiation

- Prevents denial of sending/performing a transaction.
- Digital receipts act as proof.
- True nonrepudiation is impossible—malware or forced action can invalidate claims.

3.2 Working Cryptographic Systems and Protocols

Cryptographic Systems vs. Protocols

- **Cryptographic System:** it's a collection of software/hardware that encrypts or decrypts data (browser + server).
- **Cryptographic Protocol:** rules governing how encrypted data is exchanged (e.g., SSL/TLS)

Types of Cryptographic Protocols

A. Offline Encryption (Email/File Protection)

Table 4-1. Cryptographic protocols for offline communications

Protocol	What does it do?	Widely deployed?	Programs and systems	URL
PGP/OpenPGP	Encryption and digital signatures for email and electronic documents	Yes	PGP (Network Associates)	*http://www.pgp.com/*
			Hushmail (Hush Communications)	*http://www.hushmail.com/*
			Veridis	*http://www.veridis.com/*
			Highware	*http://www.highware.com/*
			GNU Privacy Guard (GNU)	*http://www.gnupg.org/*
S/MIME	Encryption and digital signatures for email	No	Netscape Communicator (Netscape Communications)	*http://netscape.com/*
			Outlook (Microsoft)	
			Outlook Express (Microsoft)	*http://microsoft.com/*

Types of Cryptographic Protocols (cont..)

A. Offline Encryption (Email/File Protection)

Tools include:

- **PGP/OpenPGP**
  - First widespread public key system.
  - Provides confidentiality, integrity, nonrepudiation.
  - Uses key pairs; keys can be “certified” by others (web of trust).

- **S/MIME**
  - Encrypts email + attachments.
  - Relies on certificates from Certification Authorities (CAs).
  - More centralized but less widely adopted.

Types of Cryptographic Protocols (cont..)

A. Offline Encryption (Email/File Protection)

Tools include:

- **PGP/OpenPGP**

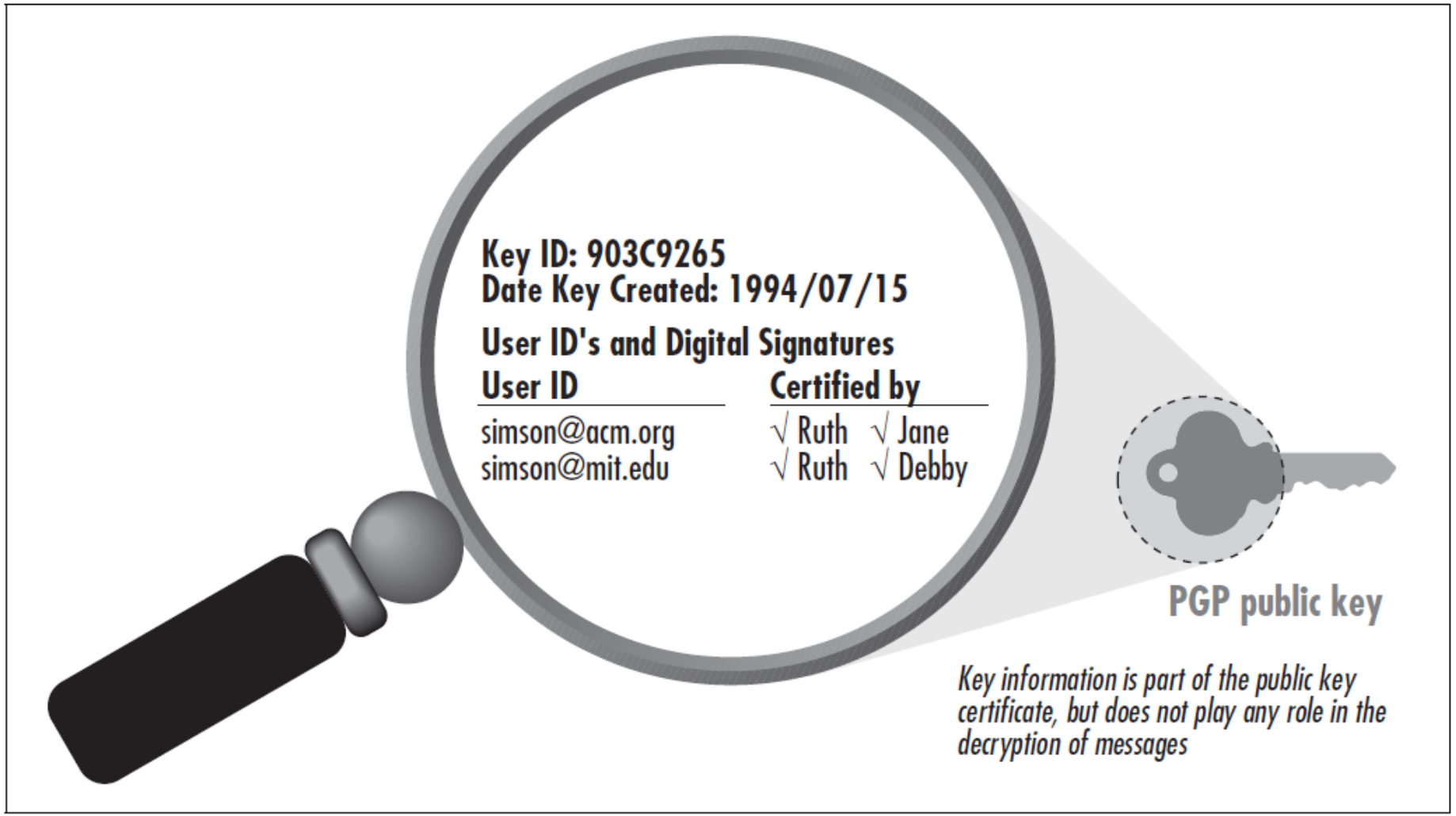

Figure 4-1. PGP keys consist of the actual public key that is used to encrypt or decrypt information, one or more email addresses, and one or more digital signatures attached to each email address.

Types of Cryptographic Protocols (cont..)

B. Online Cryptographic Protocols and Systems

- Used for web sessions, transactions, payments, DNS, etc.

Table 4-2. Cryptographic protocols for online communications

Protocol	What does it do?	Widely deployed?	Programs and systems	URL
DNSSEC (Secure DNS)	Provides secure hostname to IP address resolution	No	BIND, Version 9 (Internet Software Consortium)	*http://www.ietf.org/html.charters/dnsext-charter.html*
IPsec and IPv6	Secures IP traffic	No		*http://www.ietf.org/html.charters/ipsec-charter.html*
Kerberos	Provides secure authentication and cryptographic key exchange for higher-level protocols	Somewhat	Kerberos (MIT) Windows 2000 (Microsoft)[a]	*http://web.mit.edu/kerberos/www/*
PCT (Private Communications Technology)	Provides privacy for web transactions	No	Internet Explorer (Microsoft) Internet Information Server (Microsoft)	*http://www.graphcomp.com/info/specs/ms/pct.htm*

Types of Cryptographic Protocols (cont..)

B. Online Cryptographic Protocols and Systems

Table 4-2. Cryptographic protocols for online communications (continued)

Protocol	What does it do?	Widely deployed?	Programs and systems	URL
SET (Secure Electronic Transactions)	Provides privacy and nonrepudiation for credit card transactions; prevents merchants from getting credit card numbers	No	Capital One Wallet	*http://www.visa.com/set* *http://www.mastercard.com/set*
SSH (Secure Shell)	Provides secure remote access (telnet) protocol and additional provisions for encrypting other protocols such as email and X Windows	Yes	SSH Version 1.x, 2.x	*http://www.ssh.com*
			OpenSSH	*http://openssh.org*
			Putty	*http://www.chiark.greenend.org/uk/nsgtatham/putty/*
			SecureCRT (Vandyke Communications)	*htttp://www.vandyke.com/products/securecrt/*
SSL (Secure Sockets Layer)	Encrypts stream communications; mostly used for downloading web pages and email	Yes	Apache Web Server	*http://www.apache-ssl.org* *http://www.modssl.org/*
			Internet Information Server (Microsoft)	*http://www.microsoft.com/windows2000/technologies/web*
			Commerce Server (Netscape)	*http://home/netscape.com/eng/ssl3/*
			Most web browsers	

[a] The Microsoft version of Kerberos contains proprietary extensions not compatible with open standards.

B. Online Cryptographic Protocols and Systems (cont..)

- **SSL / TLS**
  - Most widely used protocol.
  - Provides confidentiality, integrity, authentication, nonrepudiation.
  - Replaced gradually by TLS.
- **PCT (Microsoft)**
  - SSL alternative; declining use.
- **SET (Secure Electronic Transaction)**
  - Designed for secure online credit card transactions.
  - Merchant cannot see card number.
  - Too complex → failed adoption.
- **DNSSEC**
  - Adds authentication & integrity to DNS.
  - Prevents DNS spoofing.
- **IPsec / IPv6**
  - Protects IP packets at network layer.
  - Used mainly for VPNs.

B. Online Cryptographic Protocols and Systems (cont..)

- **Kerberos**
  - Authentication system using symmetric keys.
  - Requires trusted central server.
  - Used mostly in academic & enterprise environments.
- **SSH**
  - Secure remote login, file transfer, tunneling.
  - Widely adopted as replacement for Telnet/FTP

3.3 Legal Restrictions on Cryptography

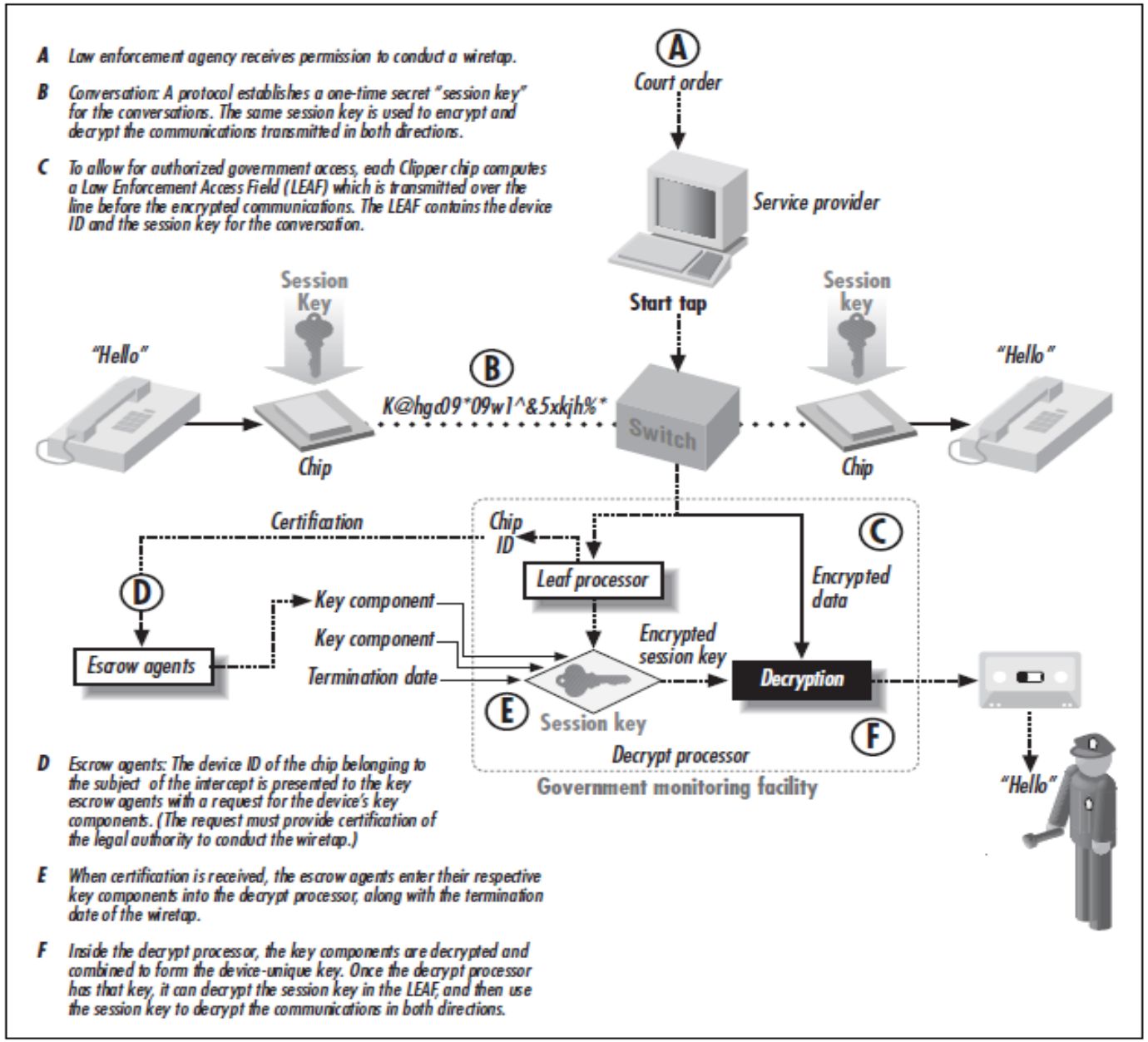

Figure 4-2. A copy of the key used to encrypt the message is included with the encrypted message in a block of data called the Law Enforcement Access Field (LEAF). Each LEAF is encrypted with a key that is unique to the particular Clipper chip. (Adapted with permission from a diagram prepared by SEARCH.)

Legal Restrictions on Cryptography (cont..)

Figure 4-3. The "big brother inside" campaign attacked the Clinton Administration's Clipper chip proposal with a spoof on the successful "intel inside" marketing campaign.

Legal Restrictions on Cryptography (cont..)

Table 4-3. International agreements on cryptography

Agreement	Date	Impact
COCOM (Coordinating Committees for Multilateral Export Controls)	1991–1994	Eased restrictions on cryptography to allow export of mass-market and public-domain cryptographic software.
Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies	1996–present	Allows export of mass-market computer software and public-domain software. Other provisions allow export of all products that use encryption to protect intellectual property (such as copy protection systems).
Council of Europe	1995–present	Recommends that "measures should be considered to minimize the negative effects of the use of cryptography on investigations of criminal offenses, without affecting its legitimate use more than is strictly necessary."
European Union	2000–present	Export to other EU countries is largely unrestricted. Export to other countries may require a Community General Export Authorization (CGEA) or a General National License.

Legal Restrictions on Cryptography (cont..)

National regulations of cryptography throughout the world

Table 4-4 summarizes national restrictions on the import, export, and use of cryptography throughout the world as of March 2001.

Table 4-4. National restrictions on cryptography[a]

Country	Wassenaar signatory?	Import/export restrictions	Domestic use restrictions
Argentina	Yes	None.	None.
Australia	Yes	Export regulated in accordance with Wassenaar. Exemptions for public domain software and personal-use. Approval is also required for software that does not contain cryptography but includes a plug-in interface for adding cryptography.	None.
Austria	Yes	Follows EU regulations and Wassenaar Arrangement.	Laws forbid encrypting international radio transmissions of corporations and organizations.
Bangladesh		None apparent.	None apparent.
Belarus		Import and export requires license.	A license is required for design, production, sale, repair, and operation of cryptography.
Belgium	Yes	Requires license for exporting outside of the Benelux.	None currently, although regulations are under consideration.
Burma		None currently, but export and import may be regulated by the Myanmar Computer Science Development Council.	Use of cryptography may require license.
Brazil		None.	None.
Canada	Yes	Follows pre-December 1998 Wassenaar regulations. Public domain and mass-market software can be freely exported.	None.

Country	Wassenaar signatory?	Import/export restrictions	Domestic use restrictions
Chile		None.	None.
People's Republic of China		Requires license by State Encryption Management Commission for hardware or software where the encryption is a core function.	Use of products for which cryptography is a core function is restricted to specific products using preapproved algorithms and key lengths.
Columbia		None.	None.
Costa Rica		None.	None.
Czech Republic	Yes	Import allowed if the product is not to be used "for production, development, collection or use of nuclear, chemical or biological weapons." Export controls are not enforced.	None.
Denmark	Yes	Some export controls in accordance with Wassenaar.	None.
Egypt		Importers must be registered.	None.
Estonia		Export controlled in accordance with Wassenaar.	
Finland	Yes	Export requires license in accordance with EU Recommendation and Wassenaar, although a license is not required for mass-market goods.	None.
France	Yes	Some imports and exports may require a license depending on intended function and key length.	France liberalized its domestic regulations in March 1999, allowing the use of keys up to 128 bits. Work is underway on a new law that will eliminate domestic restrictions on cryptography.
Germany	Yes	Follows EU regulations and Wassenaar; companies can decide for themselves if a product falls within the mass-market category.	None.
Greece	Yes	Follows pre-December 1998 Wassenaar.	None.
Hong Kong Special Administrative Region		License required for import and export.	None, although encryption products connected to public telecommunication networks must comply with the relevant Telecommunications Authority's network connection specifications.
Hungary	Yes	Mirror regulations requiring an import license if an export license is needed from Hungary. Mass-market encryption software is exempted.	None.
Iceland		None.	None.
India		License required for import.	None.
Indonesia		Unclear.	Unclear.

Country	Wassenaar signatory?	Import/export restrictions	Domestic use restrictions
Ireland	Yes	No import controls. Export regulated under Wassenaar; no restrictions on the export of software with 64-bit key lengths.	Electronic Commerce Act 2000 gives judges the power to issue search warrants that require decryption.
Israel		Import and export require a license from the Director-General of the Ministry of Defense.	Use, manufacture, transport, and distribution of cryptography within Israel requires a license from the Director-General of the Ministry of Defense, although no prosecutions for using unlicensed cryptography are known and many Israeli users apparently do not have licenses.
Italy	Yes	Follows EU regulations.	Encrypted records must be accessible to the Treasury.
Japan		Export regulations mirror pre-December 1998 Wassenaar. Businesses must have approval for export of cryptography orders larger than 50,000 yen.	None.
Kazakhstan		Requires license.	License from the Committee of National Security required for research, development, manufacture, repair, and sale of cryptographic products.
Kyrgyzstan		None.	None.
Latvia		Mirrors EU regulations.	None.
Luxembourg	Yes	Follows pre-December 1998 Wassenaar.	None.
Malaysia		None.	None, although search warrants can be issued that require the decryption of encrypted messages.
Mexico		None.	None.
Moldova		Import and export requires a license from the Ministry of National Security.	Use requires a license from the Ministry of National Security.
The Netherlands	Yes	Follows Wassenaar. No license required for export to Belgium or Luxemburg.	Police can order the decryption of encrypted information, but not by the suspect.
New Zealand	Yes	Follows Wassenaar. Approval is also required for software that is designed for plug-in cryptography.	None.
Norway	Yes	Follows Wassenaar.	None.
Pakistan		None.	Sale and use of encryption requires prior approval.
Philippines		None.	Not clear.
Poland		Follows Wassenaar.	None.
Portugal	Yes	Follows pre-December 1998 Wassenaar.	None.

Country	Wassenaar signatory?	Import/export restrictions	Domestic use restrictions
Romania	Yes	No import controls. Exports according to Wassenaar.	None.
Russia		License required for import and export.	Licenses required for some uses.
Saudi Arabia		None.	"It is reported that Saudi Arabia prohibits use of encryption, but that this is widely ignored."
Singapore		No restrictions.	Hardware equipment connected directly to the telecommunications infrastructure requires approval. Police, with the consent of the Public Prosecutor, may compel decryption of encrypted materials.
Slovakia	Yes	In accordance with pre-December 1998 Wassenaar.	None.
Slovenia		None.	None.
South Africa		Import and export controls only apply to military cryptography.	No regulations for commercial use or private organizations. Use by government bodies requires prior approval.
South Korea	Yes	Import of encryption devices forbidden by government policy, not legislation. Import of encryption software is not controlled. Export in accordance with Wassenaar.	None.
Spain		Export in accordance with Wassenaar and EU regulations.	None apparent.
Sweden		Export follows Wassenaar. Export of 128-bit symmetric mass-market software allowed to a list of 61 countries.	Use of equipment to decode encrypted radio and television transmissions is regulated.
Switzerland		Import is not controlled. Export mirrors Wassenaar.	Some uses may be regulated.
Turkey		Follows pre-December 1998 Wassenaar controls.	No obvious restrictions.
United Kingdom		Follows EU and Wassenaar restrictions on export.	Regulation of Investigatory Powers Act 2000 gives the government the power to disclose the content of encrypted data.
United States of America	Yes	Few export restrictions.	None.
Uruguay		None.	None.
Venezuela		None.	None.
Vietnam		Import requires license.	None.

[a] Source material for this table can be found at *http://cwis.kub.nl/~frw/people/koops/cls2.htm*.

Legal Restrictions on Cryptography (cont..)

Cryptography is affected by:

- **Patent law** (early crypto patents restricted adoption)
- **Trade secret law** (proprietary algorithms often fail security review)
- **Export/import restrictions** (varies by country)
- **National security concerns** (military & law enforcement worry about losing surveillance ability)

Patents in Cryptography

- Early public key techniques were patented (Diffie–Hellman, RSA).
- All major public key patents have now expired.
- Patents slowed early adoption but no longer a major issue.

Trade Secret Issues

- Companies once used secret (proprietary) encryption algorithms.
- Secrecy does **not** improve security; public scrutiny makes algorithms stronger.
- Many “secret” algorithms (RC2, RC4, DVD-CSS) were leaked and broken.
- Conclusion: security through obscurity is ineffective.

Regulation of Cryptography

- Initially motivated by military secrecy (e.g., WWII Enigma lessons).
- Later adopted by law enforcement (fear of criminals using unbreakable encryption).
- Government concerns include:
  - Wiretap evasion
  - Encrypted devices blocking investigations
  - Encrypted communications (phones, apps, etc.)

Digital Identification

Digital Identification I: Passwords, Biometrics, and Digital Signatures

- Physical Identification
- Using Public Keys for Identification
- Real-World Public Key Examples

Digital Identification II: Digital Certificates, CAs, and PKI

- Understanding Digital Certificates with PGP
- Certification Authorities: Third-Party Registrars
- Public Key Infrastructure
- Open Policy Issues

4.Digital Identification I: Passwords, Biometrics, and Digital Signatures

- Identification enables trust, accountability, and access control
- Used in:
  - Financial transactions
  - Physical and digital access
  - Legal and governmental systems
- Goal:
  - Reduce impersonation risk
  - Quantify remaining (residual) risk

4.1. Physical Identification

- **Physical identification supports trust in daily activities**
- **Example:**
  - Renting a car using a driver’s license and credit card
- **Identification:**
  - Enables accountability
  - Works with legal systems
- **Absolute security is not required—acceptable risk is the goal**

Physical Identification (cont..)

- **Historically:**
  - Identity based on personal recognition within communities
- **Modern society:**
  - Relies on formal credentials
- **Identification is essential for:**
  - Credit
  - Contracts
  - Law enforcement
- **Online environments make identification more difficult**

Paper-Based Identification Techniques

- Most common physical identification method
- Issued by trusted authorities
- Examples:
  - Passports
  - Driver’s licenses
  - National ID cards
- Used when personal recognition fails

Verifying identity with physical documents

Step 1: Examine document authenticity

- Seals, laminations, materials

Step 2: Compare holder with photograph

Step 3: Secondary checks

- Signature comparison
- Personal questions

- Decisions often made with incomplete certainty

Verifying identity with physical documents (cont..)

- **Figure 6-1:**
  - Shows examples of credentials such as:
    - Passport
    - Driver's license
    - Gym membership card
- Demonstrates how physical documents act as identity credentials

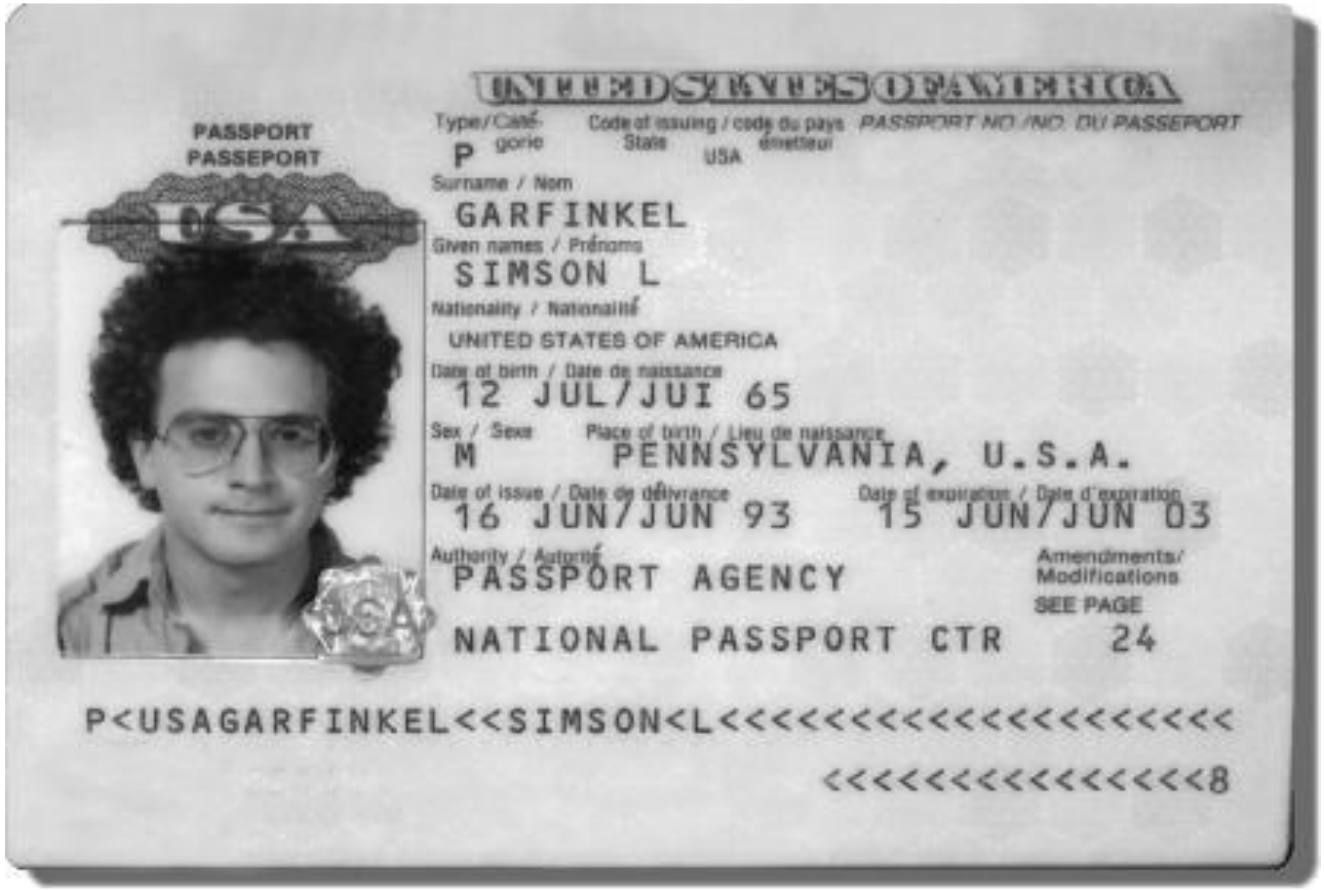

Figure 6-1. A driver's license, passport, or gym membership card is a credential that can be used to prove identification

Reputation of the issuing organization

- **Trust depends on the issuing authority**
- **Important factors:**
  - Verification standards
  - Protection of blank documents
  - Internal controls
  - Resistance to bribery
- **Government-issued IDs are more trusted than private cards**

Tamper-proofing the document

- Identification documents should be:
  - Tamper-resistant
  - Forgery-resistant
  - Tamper-evident
- Security techniques:
  - Special paper and ink
  - UV patterns
  - Laminates
  - Security holograms

Tamper-proofing the document (cont..)

- Examples:
  - Polaroid UV film and laminates
  - Security holograms on credit cards
- No system is perfect
- Goal: increase cost and difficulty of forgery

Computer-Based Identification Techniques

- **Used for over 50 years**
- **Originally for:**
  - Billing
  - Resource management
- **Key difference:**
  - Focus on **relative identification**, not absolute identity
- **System checks continuity of identity**

Computer-Based Identification Techniques (cont..)

- **Four authentication factors:**
  - Something that you know
  - Something that you have
  - Something that you are
  - Someplace where you are

Password-based systems: something that you know

- **User provides:**
  - Username
  - Password
- **System matches entered password with stored value**
- **Most widely used authentication method**

Password-based systems: something that you know (cont..)

- **Figure 6-2:**
  - Shows a basic password authentication process
  - User enters credentials
  - System verifies against stored data

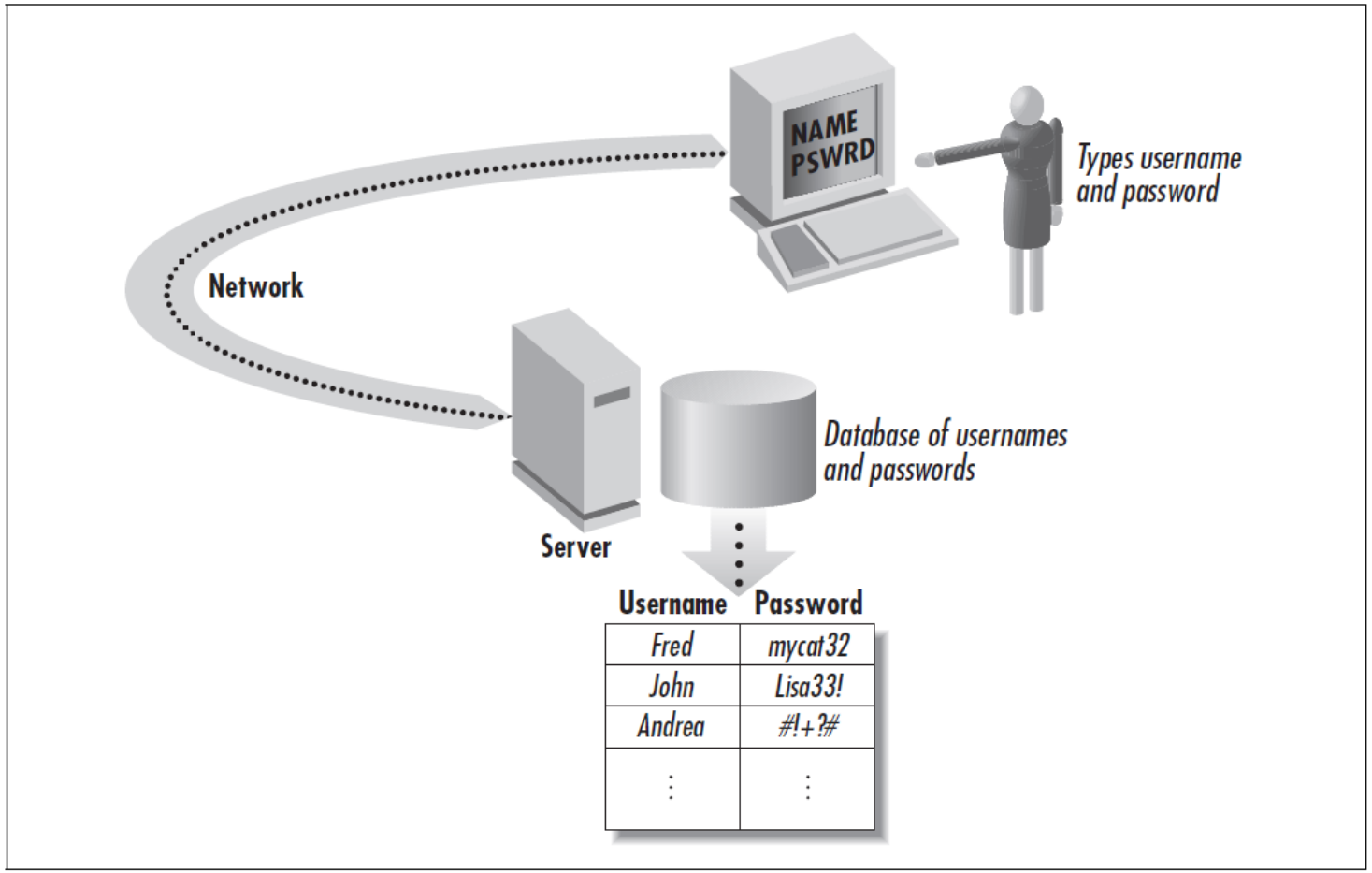

Figure 6-2. Using a username and a password to prove who you are

Password-based systems: something that you know (cont..)

Advantages

- Simple
- Low cost
- No special hardware

Problems

- Easy to forget
- Easy to share
- Vulnerable to attacks

Physical tokens: something that you have

- **Tokens authenticate by possession**
- **Examples:**
  - Keys
  - Magnetic cards
  - RFID cards
  - Smart cards

Physical tokens: something that you have (cont..)

- **Figure 6-3:**
  - Shows a hardware authentication token (e.g., Robocard)
- **Used to store or generate authentication information**

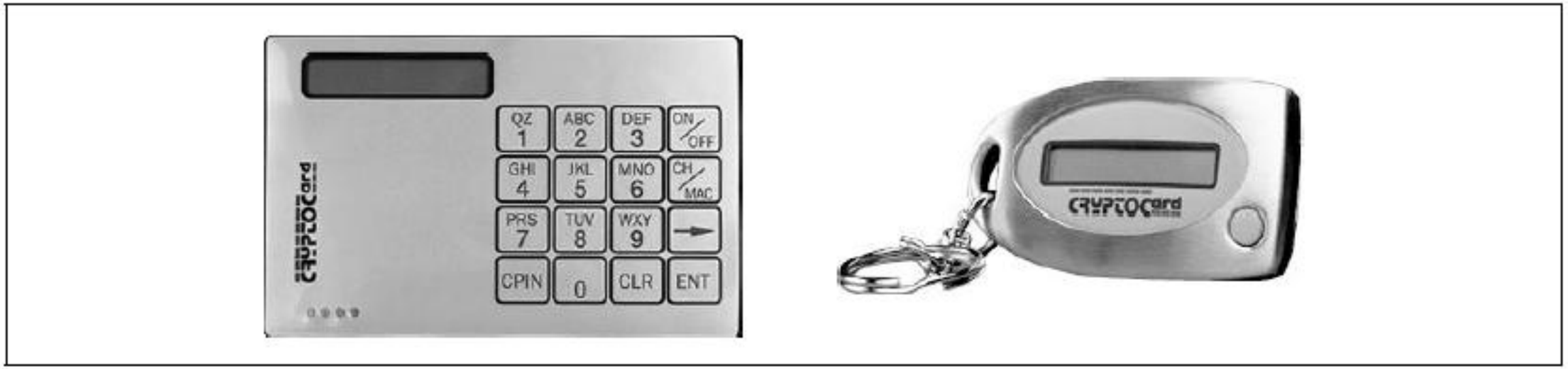

Figure 6-3. Using a token-based system to prove who you are (reprinted with permission)

Physical tokens: something that you have (cont..)

Advantages

- Easy to revoke if lost
- Supports access control

Problems

- Do not prove identity
- Can be stolen or copied

Physical tokens: something that you have (cont..)

Two-Factor Authentication

- Combines:
  - Token + password/PIN
- **Example**:
  - ATM card and PIN
- Improves security in high-risk systems

Biometrics: something that you are

- **Identification based on physical or behavioral traits**
- **Examples:**
  - Fingerprints
  - Iris scans
  - Facial recognition
  - Voice prints

Biometrics: something that you are (cont..)

- **Figure 6-4:**
  - Shows an iris recognition system
  - Used for biometric access control

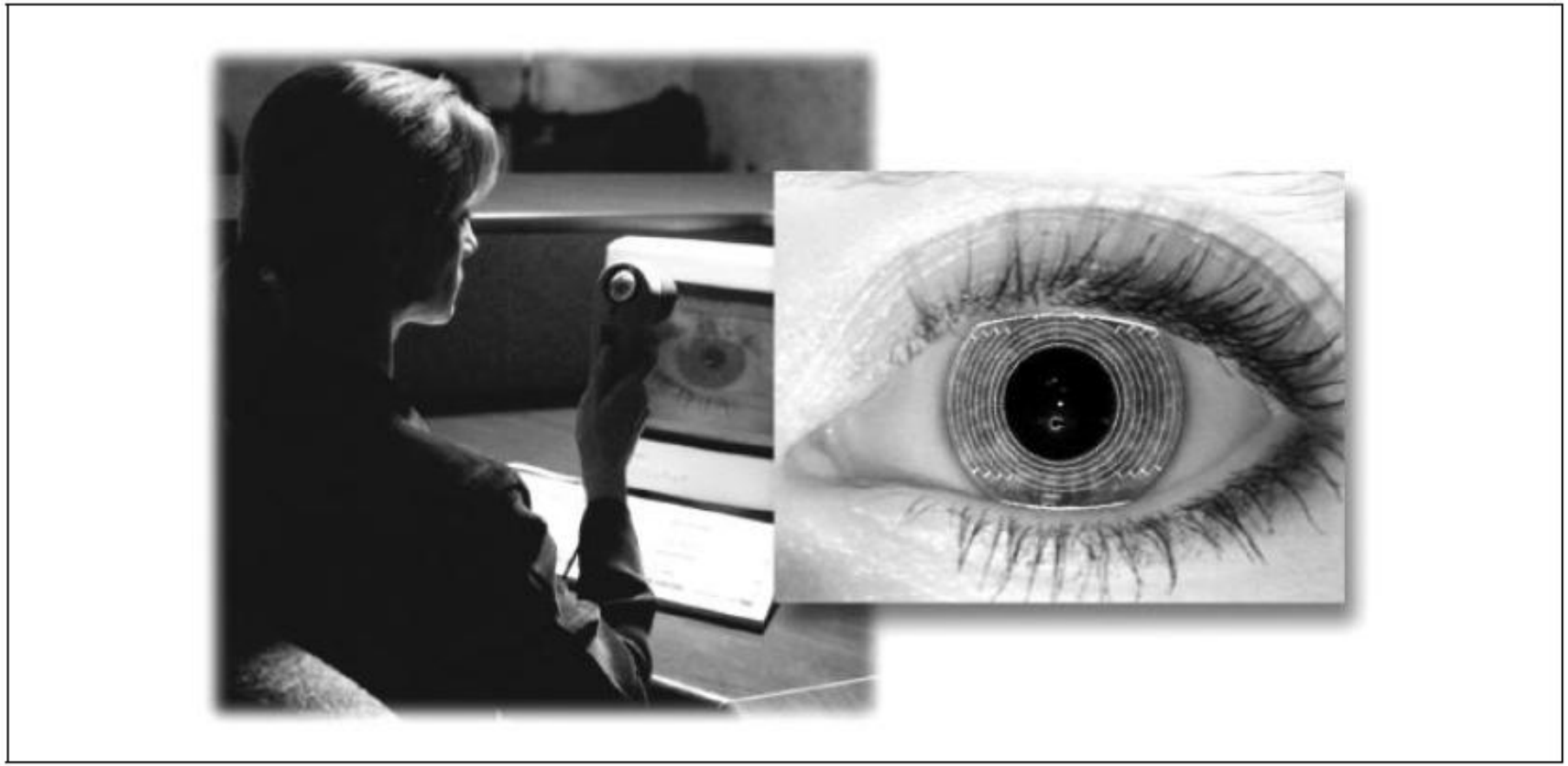

Figure 6-4. Using a biometric-based system to prove identity (reprinted with permission of Iridian)

Biometrics: something that you are (cont..)

Advantages

- Cannot be forgotten
- Hard to share or steal

Types

- Ongoing identification
- Absolute identification

Biometrics: something that you are (cont..)

Limitations:

- False positives
- False negatives
- Requires enrollment
- Database compromise is critical
- Sensors can be spoofed

Location: someplace where you are

- Authentication based on physical location
- **Examples:**
  - Region-restricted access
  - Authorized terminals only

Location: someplace where you are

Limitations:

- **GPS:**
  - Poor indoor performance
  - Difficult to secure data transmission
- **Rarely used alone**
- **Usually combined with other authentication methods**

4.2. Using Public Keys for Identification

- **Traditional identification techniques require:**
  - Physical presence of the individual
- **Remote identification (telephone, fax, Internet) increases:**
  - Risk of fraud
  - Risk of impersonation
- **Major weakness: replay attacks**

Replay Attacks

- **Replay attacks occur when:**
  - Authentication data is captured
  - The captured data is reused to impersonate a victim
- **Affect all digital identification systems:**
  - Passwords
  - Biometrics
  - Tokens
  - Position-based systems

Replay Attacks (cont..)

- **Biometric Example:**
  - Fingerprint scanner used for authentication
- **Problem arises when:**
  - One system captures the biometric
- **Another system verifies it over a network**

Replay Attacks (cont..)

- **Figure 6-5:**
  - Shows fingerprint data captured by one computer
  - Fingerprint is transmitted over a network
  - Attacker intercepts the digitized fingerprint
- **Attacker can later replay the fingerprint to impersonate the user**

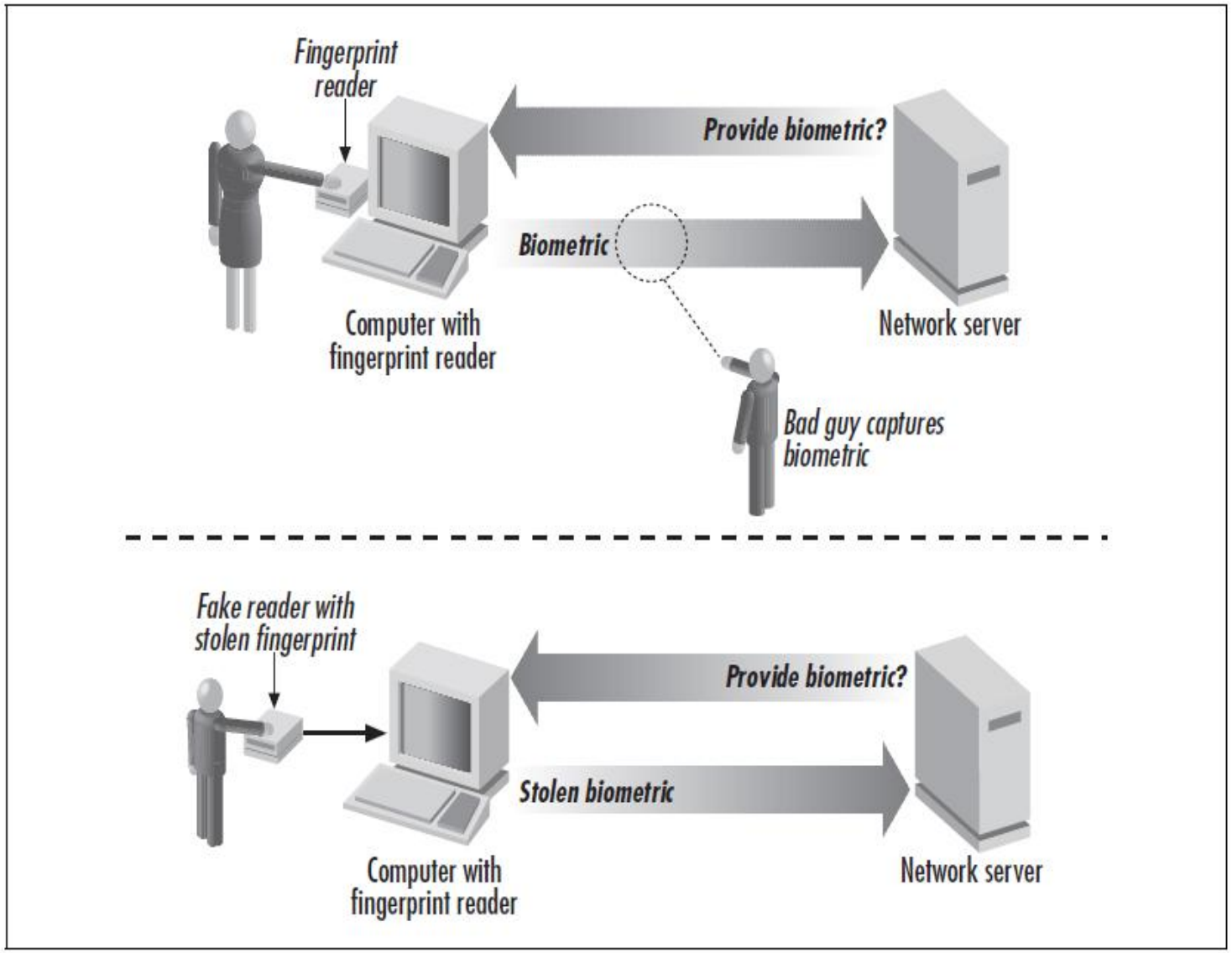

Figure 6-5. When a biometric verification is performed remotely over a computer network, the identification can be compromised by replay attacks (by tampering with the computer or software that measures the biometric).

Replay Attacks and Encryption

- **Simple encryption:**
  - Protects data during transmission
- **Limitation:**
  - If identification data is revealed once, it is permanently compromised
- **Example:**
  - Social Security numbers
  - Mother’s maiden name

Stopping Replay Attacks with Public Key Cryptography

- Public key cryptography eliminates replay attacks when properly implemented
- Uses two keys:
  - Public key (widely distributed)
  - Private key (kept secret)

Stopping Replay Attacks with Public Key Cryptography (cont..)

- **Private key:**
  - Used to create a digital signature
- **Public key:**
  - Used to verify the signature
- **Private key:**
  - Never sent over the network
- **Prevents attackers from capturing usable authentication data**

Offline authentication

- Used when authentication is verified at a later time

Steps:

1. User creates a message
2. User signs the message with private key
3. Message and signature sent to server
4. Server verifies signature using public key

Online authentication

- Used for real-time authentication
- More secure due to challenge-response protocol

Steps:

1. User connects to remote server
2. Server sends a random challenge
3. User signs challenge with private key
4. Signed challenge sent back
5. Server verifies signature using public key

PGP public keys

- **PGP (Pretty Good Privacy):**
  - Public key encryption system
  - Originally for email encryption and signatures
- **Now used for:**
  - Electronic documents
  - Key management

PGP public keys (Identity Card Concept)

- **PGP public key acts as:**
  - A digital identity card
- **Original PGP keys included:**
  - Person's name
  - RSA public key numbers
- **Newer versions allow:**
  - Photographs
  - Additional identity information

PGP public keys

- **Figure 6-6:**
  - Shows Simson Garfinkel's PGP public key in text form

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.5.8

mQGiBDPT4LYRBAD/sUgzCctn4KqHoK3ZoK/RKX4x5Lh88PaLdFUWNJiur/HWhNN/
F5yBppqgziFSB6DWZ/Wmrz+NcMjFroiXdtY96eEeRNVW/d4PiooJ+mx5EMoykbB+
YyEhNY7RmTPWDFSmfEZLjVCL17RzUsmXEqBx8LSYGyvS+UArzDsfamPHiQCg/xlE
NTw5r6+2hjpIokYoWFbc8ocEANtEoQOHGx9PG8XHXikpd1PNodkD68ubPz2D1WyO
RNqg6ZY1UtbsSLAhG+fidaJ+bm3+6JaN7F18nBBTnaLYqX8Vyc1NbWbFmr0Cx0Ed
ma4DDp8bxueqHuec1vdEoRqEbsA+2RXU3Qcr9CwhKHRTfg+IV/3M14ZOsF1BOZoc
SAFhA/43R2ziDS+sxrLmFY9jvRK1quLfT6kIPCZUKB+tA/VVLG3uHsruXuumRgUS
ZolbD05zvVOY5AP5/SZhT5GRiiNXpaWSDLBKPz/EJVsZ9Pg1QDq9KcrGzZX+ZDAh
ArMC8qIZniHE1mVwOjrTgszOx9khCBGvY0xO7CdEcdaidKPnpLQ1U21tc29uIEwu
IEdhcmZpbmt1bCA8c21tc29uZ0BhY20ub3JnPokATgQQEQIADgUCOodQ+wQLAwEC
AhkBAAoJEPKaG0LR8e7U+OsAoLgjooBAtrnYdVyjFIDED8vMvTPtAJ469yOR+kff
n/lSwV3Uu+xjaqha/rQwU21tc29uIEwuIEdhcmZpbmt1bCA8c2xnQHdhbGR1bi5j
YW1icmlkZ2UubWEudXM+iQBLBBARAgALBQI6KP+sBAsDAQIACgkQ8pobQtHx7tQp
zQCfauoGugUM6vcnaMUUC5dcATFiDWkAniBbMC32NBWYPh+dBpZiVnjiv3W8uQQN
BDPT4LgQEAD5GKB+WgZhekOQ1dwFbIeG7GHszUUfDtjgo3nGydx6C6zkP+NGlLYw
S1PXfAIWSIC1FeUpmamfB3TT/+OhxZYgTphluNgN7hBdq7YXHFHYUMoiV0MpvpXo
Vis4eFwL2/hMTdXjqkbM+84X6CqdFGHjhK1P0YOEqHm274+nQ0YIxswdd1ckOEri
xPDojhNn106SE2H22+s1Dhf99pj3yHx5sHIdOHX79sFzxIMRJitDYMPj6NYK/aEo
Jguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvMX86RA6dfSd7ZCLQI2wSbLaF6d
fJgJCo1+Le3kXXn11JJPmxiO/CqnS3wy9kJXtwh/CBdyorrWqULzBej5UxE5T7bx
br1LOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1WV/cd1JP
PT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq01uejaC1cjrU
GvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O9vPJI8BD8KVb
GI2Ou1WMuF040zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcKctaGxAMZyAcp
esqVDNmWn6vQC1CbAkbTCD1mpF1Bn5x8vY1LIhkmuquiXsNV6z3WFwACAhAAhjai
F3K0JVEIias6jAgLaVYmG4Omk61aI6cNdrgk/J6nqCwoGRJx0vpj6GOHkfHD+d64
b6Q5R6quhzHfRcs2OoCcSamGAK7kg9jtDDJ+zM/q+EH2N9/tLLX8nAG7qMuJN/IK
Jb7e438tnQjOjVaC4hW9Ju945vz1MWcJqeri9DffcnMIvLqC/aV7erJqy/A8aj5O
au29ud7Y9wQcF4XrEC3nRv5PTW4U2xmYRdqTajqjg8qtkTQCpp9SIGUGx4AVbnik
5qLM/awjiIKp+n0LN1VCp2IGsNJKAn0bFuheuQBNTRKfW7KwO6fRC76518rAalyv
/0HkFS/pBe6JcXTVRAGZ81RMqyrpvNjeBKHEsyU1ecq5Xra9KIN7cEDjWZyaTU4C
EE1nfFOTQtSbDzydT4dxmgLUG+HMRFE/g+Ax2I71QCLUYEDB/saSXgAkFU180VK9
niUANwdjRL60sZZTTrVQia+QStUIjVo/Ds691Iy0cZ4Zvjt9SFmRAvtPsZ0WfgOx
Df5TNI77nqWwoZHOEhLDMn+Wp+it4CDVJTzw98p7iE2IDXpoJE1suAl4VHdnCBsE
nmR9k7j5FnODBMKOvpp535az1PJwyV0fXQuO32snyrljb2nBV3dMkG2b4H85NT46
SUVZE/+UIwr6kKGe6rYTTrPUjQVkmq93TOoEmHKJAD8DBRgz0+C48pobQtHx7tQR
AvYTAJ9ATioJ1voy9+jLnQ8rrPDzxmAlnQCffTVnGNmzMxt8hO93MGXBwbf11bw=
=VW4i
-----END PGP PUBLIC KEY BLOCK-----
```

Figure 6-6. Simson Garfinkels's PGP public key, in text form

PGP public keys

- **Figure 6-7:**
  - Shows the same public key in graphical form using Windows PGPkeys
- **Anyone with the public key can verify signatures created using the matching private key**

Figure 6-7. Simson Garfinkel's PGP public key, as shown by the Windows PGPkeys program

Limits of Digital Signatures as Identity Proof

- **Digital signature proves:**
  - Possession of a private key
- **It does NOT prove:**
  - Real-world identity of the person
- **Anyone can create a key claiming to be:**
  - Famous people
  - Fictional characters

Creating and Storing the Private Key

For digital signatures to authenticate identity:

1. One key pair per person
2. Private key must remain secure
3. Trust mechanism must exist for verifying key ownership

Creating and Storing the Private Key (Security Challenges)

- **Poor key generation:**
  - Private key may be derived
- **Poor storage:**
  - Private key may be stolen
- **Evaluating public key systems:**

  - Often difficult in practice

Creating and Storing the Private Key (Most Secure Method)

- **Use a cryptographic coprocessor (smart card)**
- **Features:**
  - Microprocessor
  - Hardware random number generator
  - Secure key storage

Creating and Storing the Private Key (Smart Card)

- **Figure 6-8:**
  - Shows a smart card storing private keys and certificates
- **Private key:**
  - Never leaves the card
- **Data is sent into the card and signed internally**

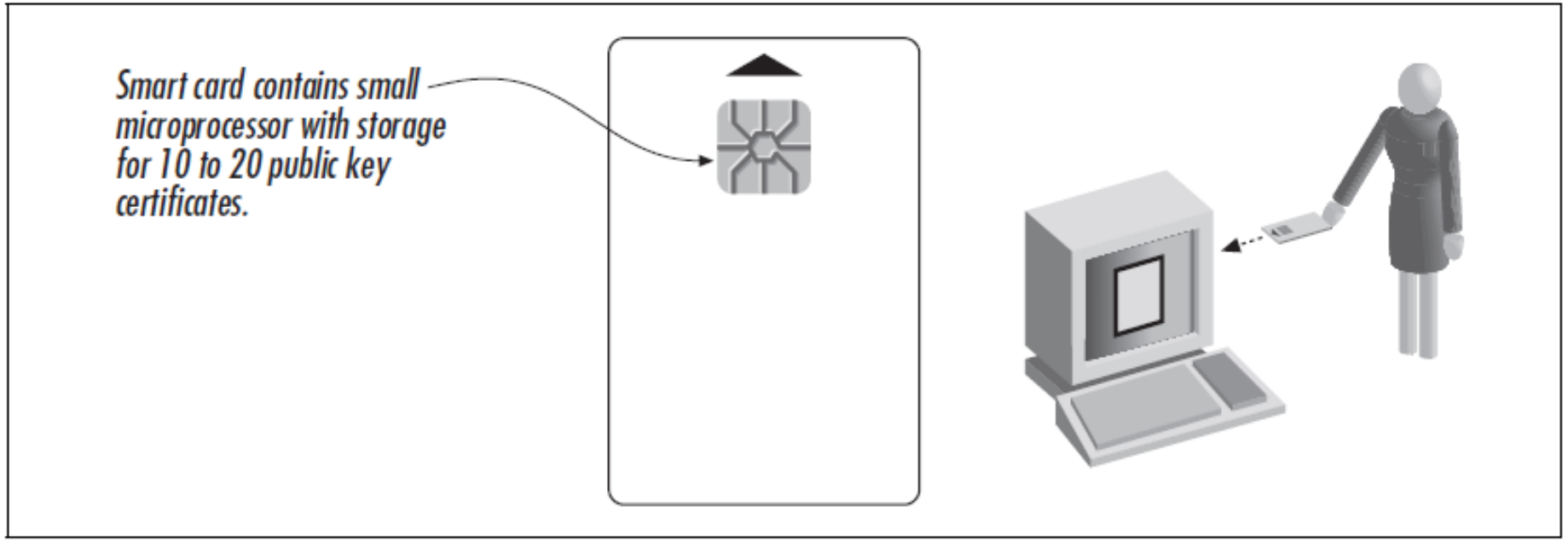

Figure 6-8. Using a smart card to store a private key/public key pair.

Creating and Storing the Private Key (Smart Card Enhancements)

- **Smart cards may require:**
  - PIN
  - Passphrase
- **Some include:**
  - Biometric fingerprint readers
- **Prevents misuse if card is stolen**

Creating and Storing the Private Key (Moderate Security Method)

- **Generate keys on desktop computer**
- **Store encrypted keys on:**
  - Floppy disk
  - Flash disk
- **Risk:**
  - Private key enters computer memory
  - Vulnerable to viruses and Trojan horses

Creating and Storing the Private Key (Least Secure Method)

- Third-party key generation
- **Problem**:
  - Private key already compromised
- Used by some organizations for:
  - Email monitoring
  - Key escrow

Creating a public key/private key pair with PGP

- PGP provides a **key generation wizard**
- Accessed via:
  - “New Key” option in PGPkeys

Creating a public key/private key pair with PGP (cont..)

- **Figure 6-9:**
  - Shows “New Key” option in PGPkeys

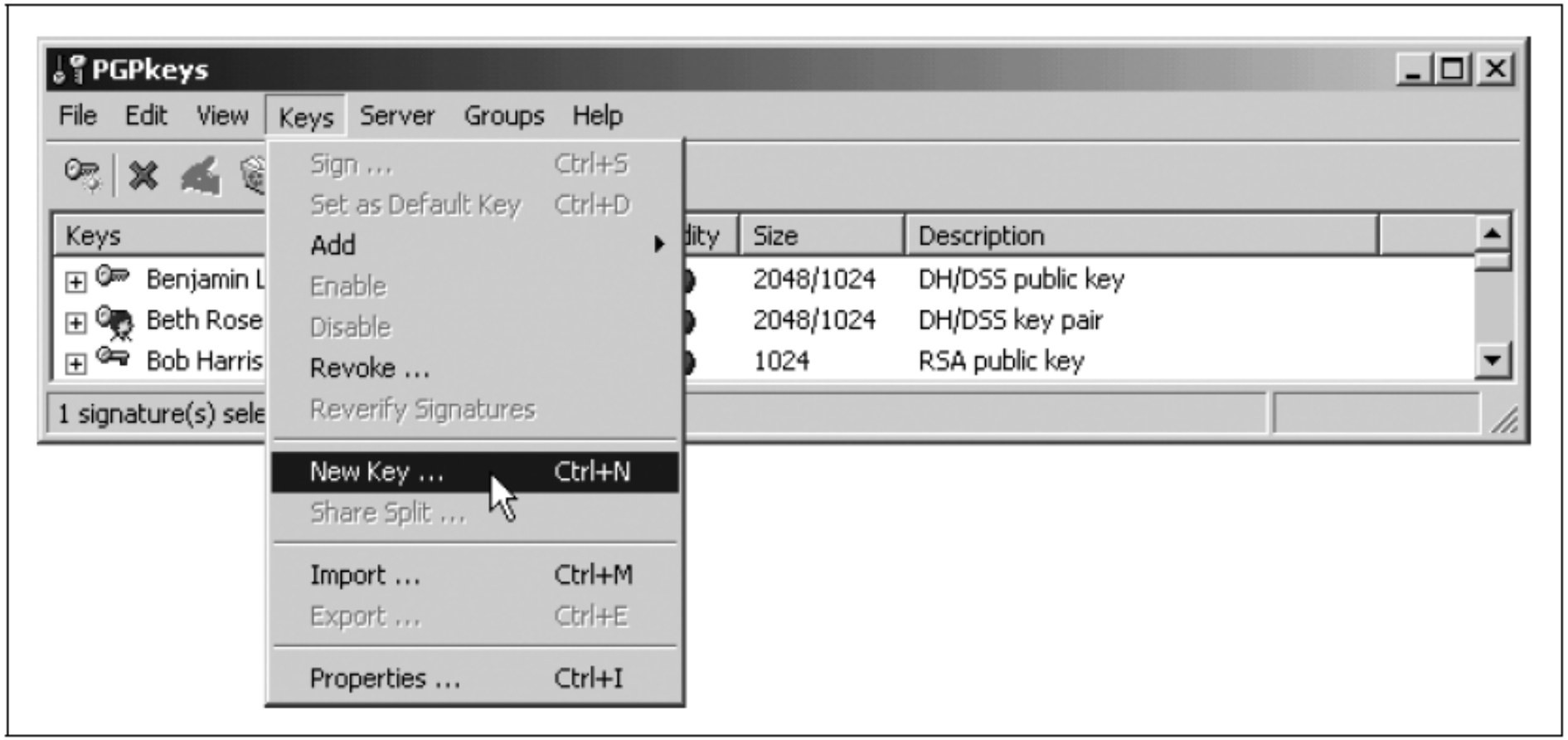

Figure 6-9. To create a new PGP key, select the “New Key...” option from the “Keys” menu of the PGPkeys application program

Creating a public key/private key pair with PGP (cont..)

- **Figure 6-10:**
  - Shows PGP Generation Wizard
- **User enters:**
  - Name
  - Email address

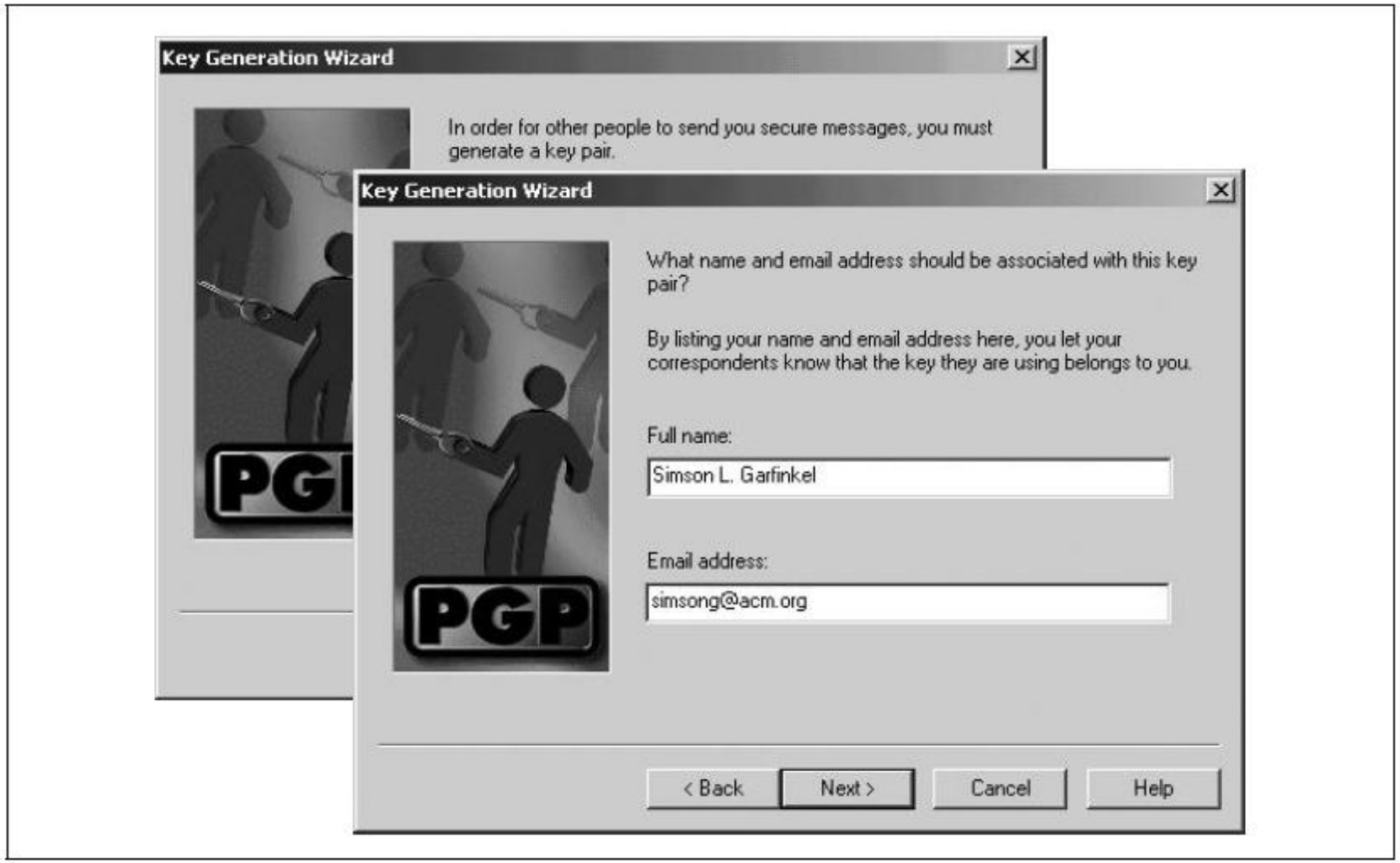

Figure 6-10. When you run the PGP Key Generation Wizard, you will be prompted to enter your full name and email address. This information is recorded on the key. You can change the full name or email address at a later time, but if you do, you will need to have your key reassigned.

Creating a public key/private key pair with PGP (Algorithm Selection)

- PGP supports:
  - RSA
  - DSA
- User selects:
  - Algorithm
  - Key size

Creating a public key/private key pair with PGP

- **Figure 6-11:**
  - Shows key type and key size selection
- Larger key size:
  - More secure
  - Slower performance

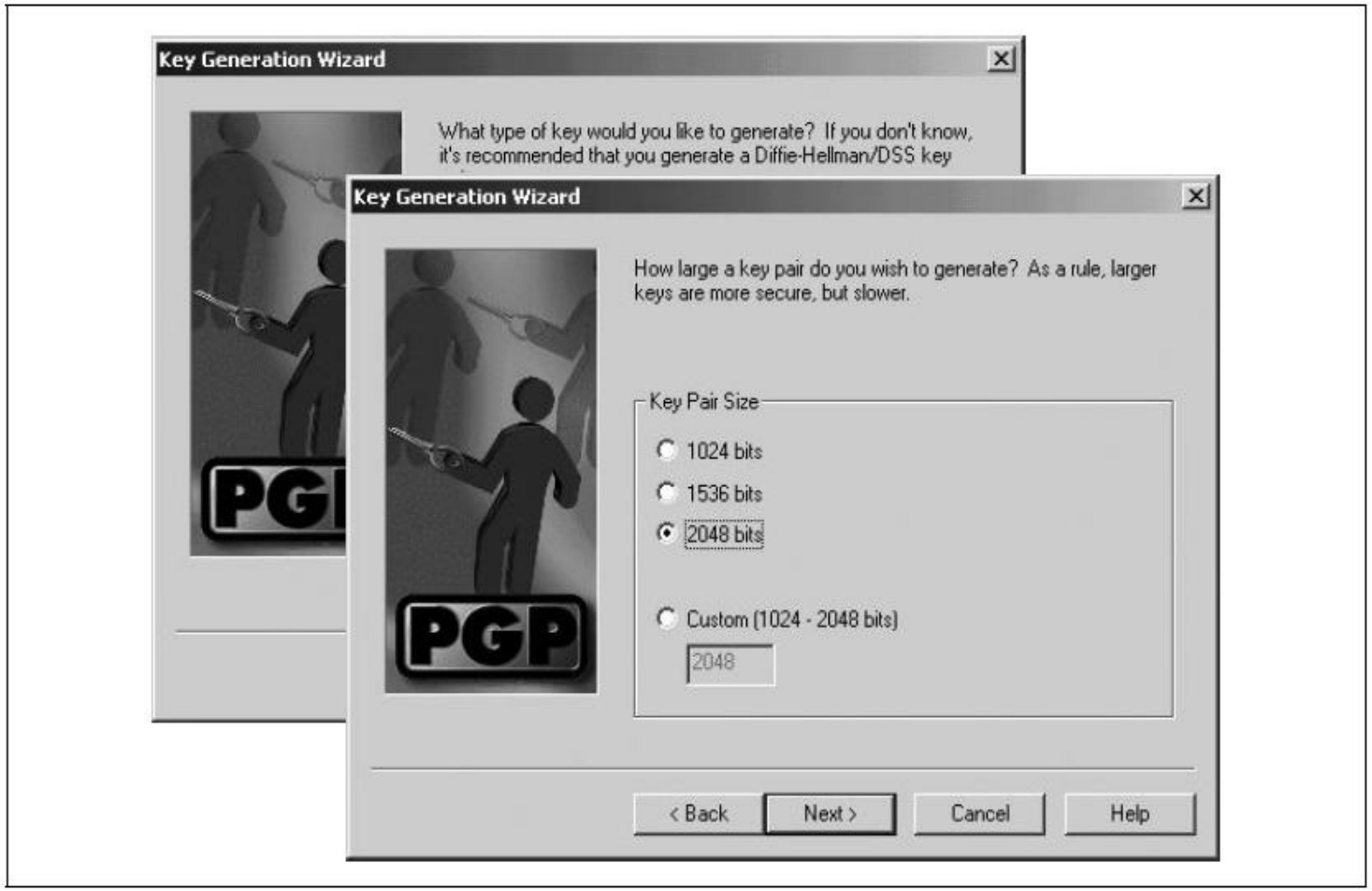

Figure 6-11. After you have given the PGP Key Generation Wizard your name, you will be asked to choose whether you are creating a Diffie-Helman/DSS key or an RSA key. Although PGP recommends that you use a Diffie-Helman key, such keys are not compatible with older versions of PGP. After you choose which algorithm the key will use, you can choose the key's size.

Creating a public key/private key pair with PGP (Passphrase)

- Passphrase encrypts private key
- Only protection for private key
- PGP evaluates:
  - Passphrase quality

Creating a public key/private key pair with PGP

- Figure 6-12:
  - Shows passphrase quality meter
- Good passphrases:
  - Long
  - Letters, numbers, spaces

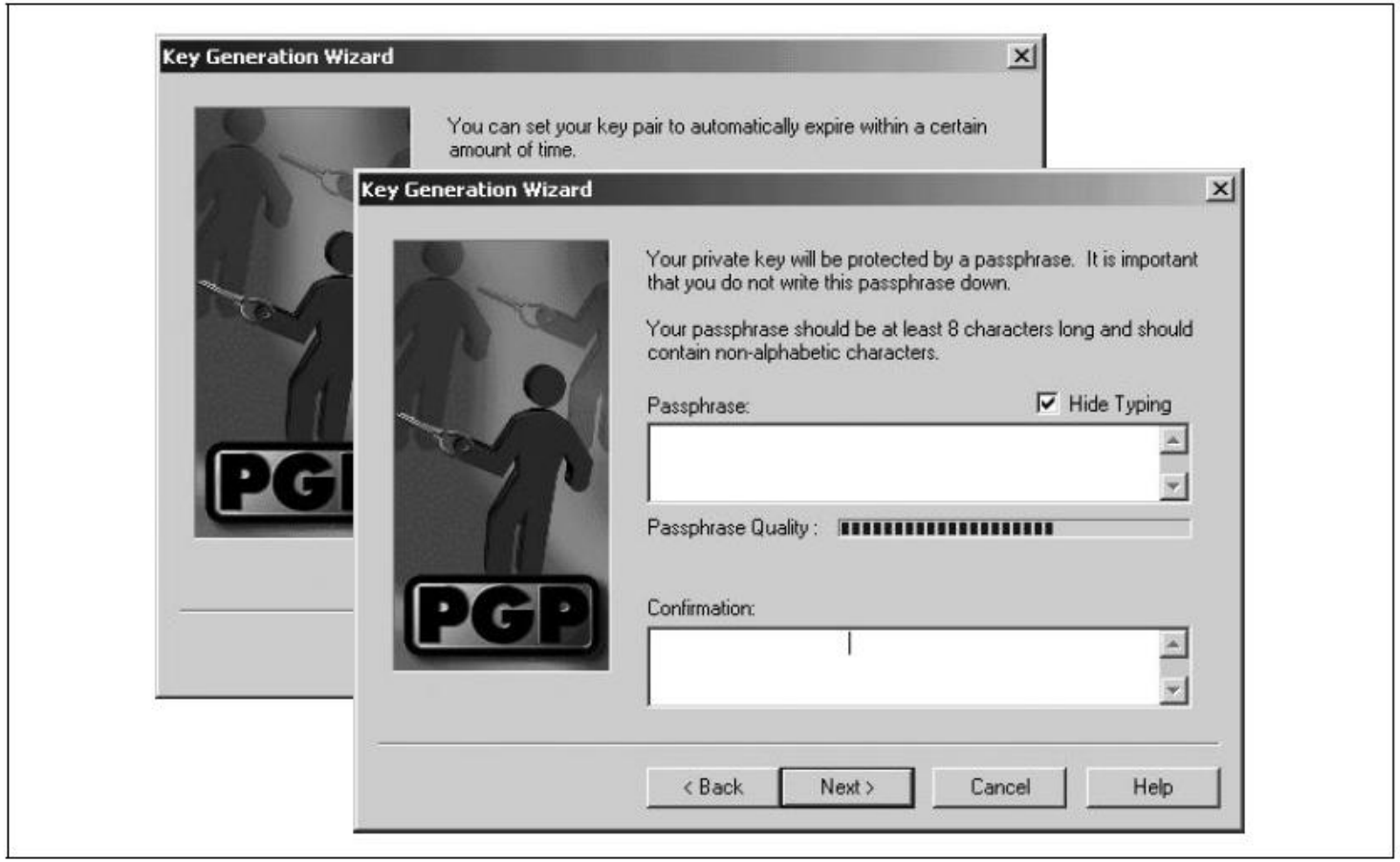

Figure 6-12. The PGP Key Generation Wizard allows you to specify when your key automatically expires. Although this is useful in high-security applications, most users won't use this feature. After you choose an expiration time, you are prompted for a passphrase. PGP shows a passphrase rating.

Creating a public key/private key pair with PGP

- Figure 6-13:
  - Shows final key creation

Figure 6-13. Once all of the parameters of the key have been entered, the PGP Key Generation Wizard creates a key pair.

Smart cards

- Smart cards improve private key protection
- **Advantages**:
  - Remove key access when card removed
  - PIN or biometric protection
  - Automatic key erasure after failed attempts

Smart cards (Limitations)

- If card is lost or damaged:
  - Keys are lost
- Long-term encryption:
  - May require key escrow or duplication
- Signing keys:
  - Can be replaced without data loss

Smart cards (Security Concerns)

- Smart cards are not fully tamper-proof
- Vulnerabilities:
  - Operating system flaws
  - Physical attacks
- Historical attacks:
  - Anderson and Kuhn (1996) smart card attack

Smart cards (Advanced Attacks)

- **Timing attacks:**
  - Analyze operation time differences
- Differential Power Analysis (DPA):
  - Analyze power consumption patterns
- These attacks can reveal private keys

4.3 Real-World Public Key Examples

- Public key cryptography used for **real-world authentication**
- Two major systems discussed:
  - **PGP** – offline authentication
  - **SSH** – online authentication
- Focus on **identity verification, authorship, and secure access**

Document Author Identification Using PGP

- Email lacks built-in authorship verification
- “From:” field can be easily forged
- Messages pass through multiple systems → risk of modification
- Peter Steiner’s 1993 New Yorker cartoon:
  - “On the Internet, nobody knows you’re a dog”
- PGP enables authentication of document authorship

Uses of PGP Digital Signatures

- Originally designed for confidentiality
- Now widely used for:
  - Digitally signing security advisories
  - Signing security-related source code
- Provides:
  - Integrity
  - Authentication
  - Non-repudiation

CERT/CC's PGP signatures

- Originally
- CERT/CC sends security advisories via email
- Advisories often recommend critical actions
- Risk: attackers could issue phony advisories
- CERT/CC uses PGP digital signatures to prevent abuse
- Signed messages begin with:
  - ----BEGIN PGP SIGNED MESSAGE---

Nature of PGP Signatures

- PGP signatures appear complex and official
- Cannot be verified visually
- Must be verified using PGP software
- Verification confirms:
  - Message integrity
- Possession of the private key

Obtaining CERT/CC's PGP key – Overview

- GP requires signer's public key to verify signature
- If key is missing → PGP reports verification failure
- Two methods:
  1. Download from CERT/CC website
  2. Download from a PGP key server

Downloading Key from CERT/CC Website

- Key downloaded directly from CERT/CC web server
- Higher assurance of authenticity
- **Figure 6-14:**
  - Browser prompt to open or save the key file

Figure 6-14. When you download the file, Internet Explorer allows you to open the file directly or save it to your disk. Choose "Open" to view the file with the PGPkeys application.

Downloading Key from CERT/CC Website

- **Figure 6-15:**
  - PGP displaying key details and import option

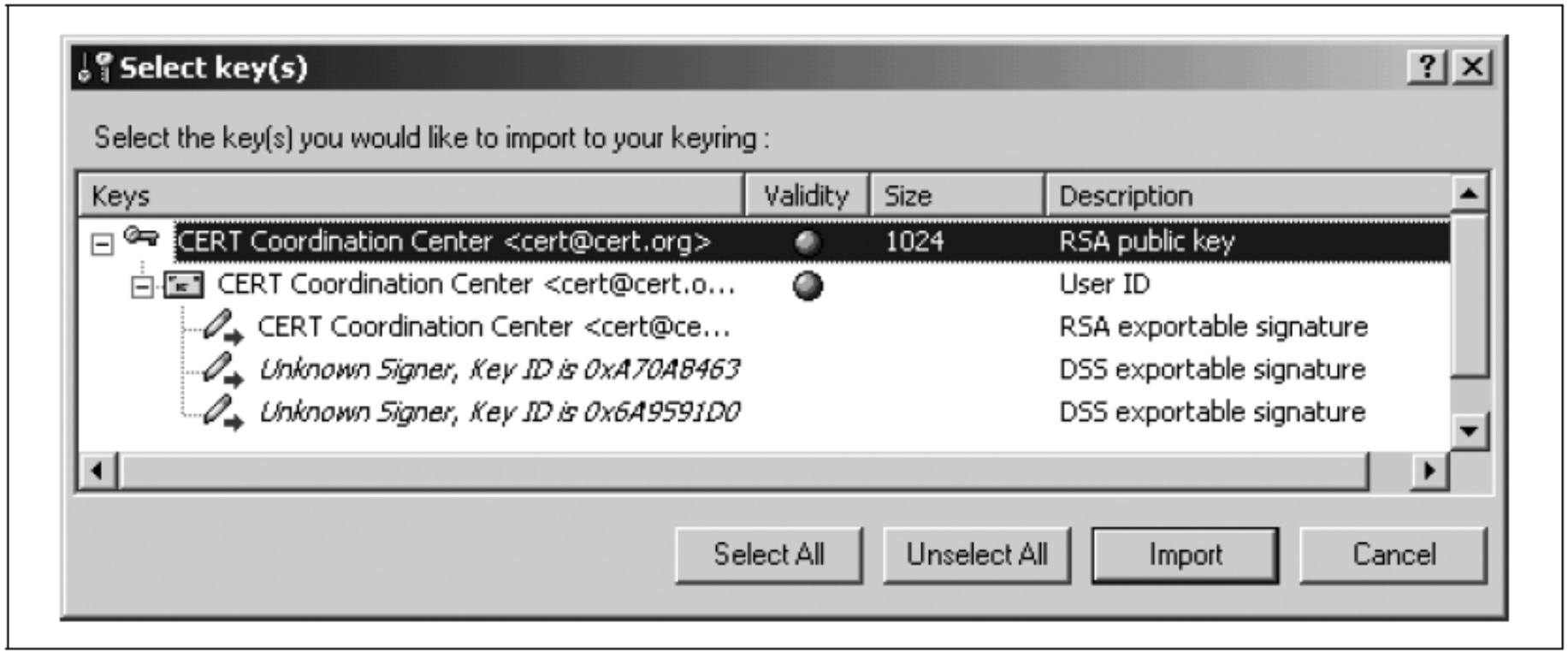

Figure 6-15. The PGPkeys application allows you to view the contents of any key on your hard disk. Once you view the key, you can decide whether or not to "import" the key—that is, to add it to your key chain.

Downloading Key from PGP Key Server

- Use PGP's Server → Search option
- **Figure 6-16:**
  - Key server search interface

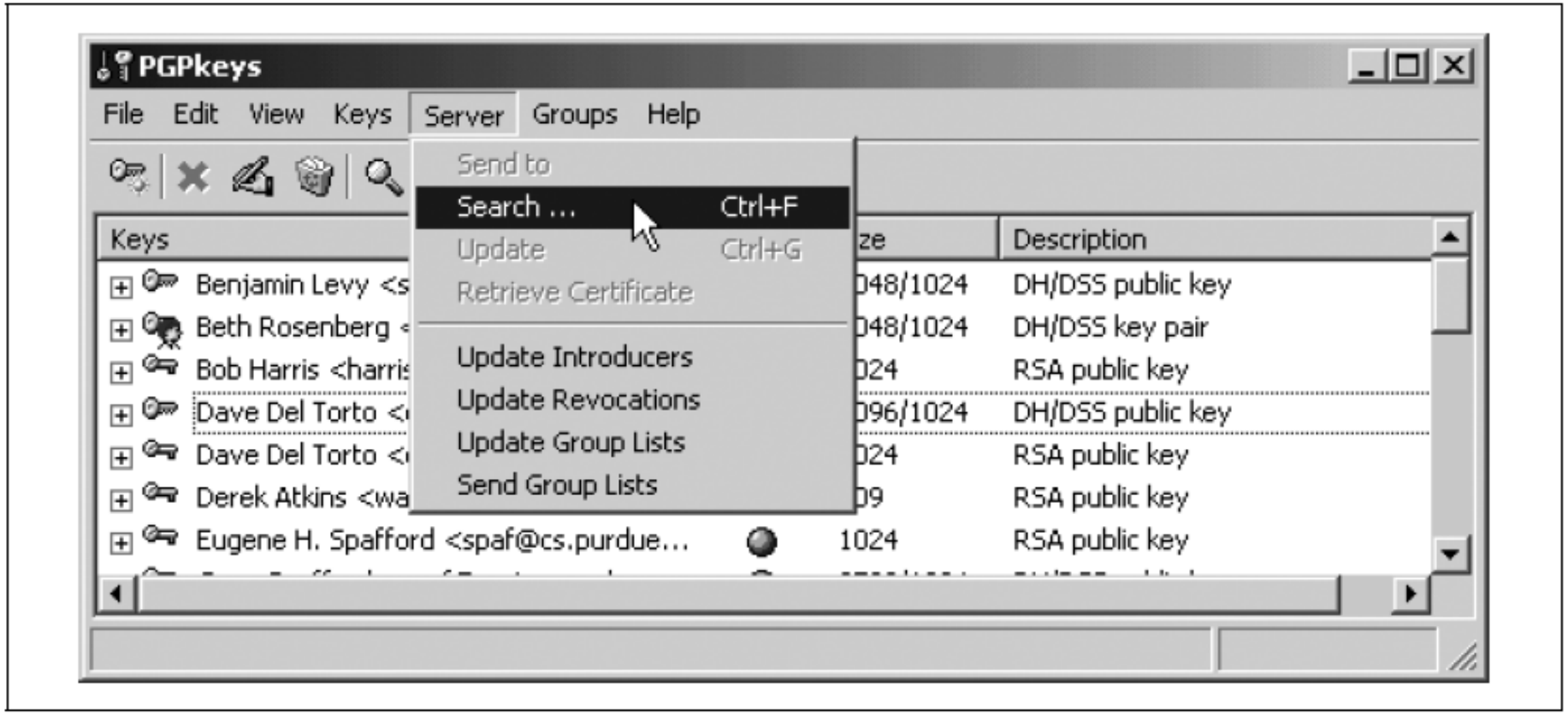

Figure 6-16. To search for a key on the PGP public key server, choose "Search..." from the "Server" menu

Downloading Key from PGP Key Server

- **Figure 6-17:**
  - Searching by KeyID

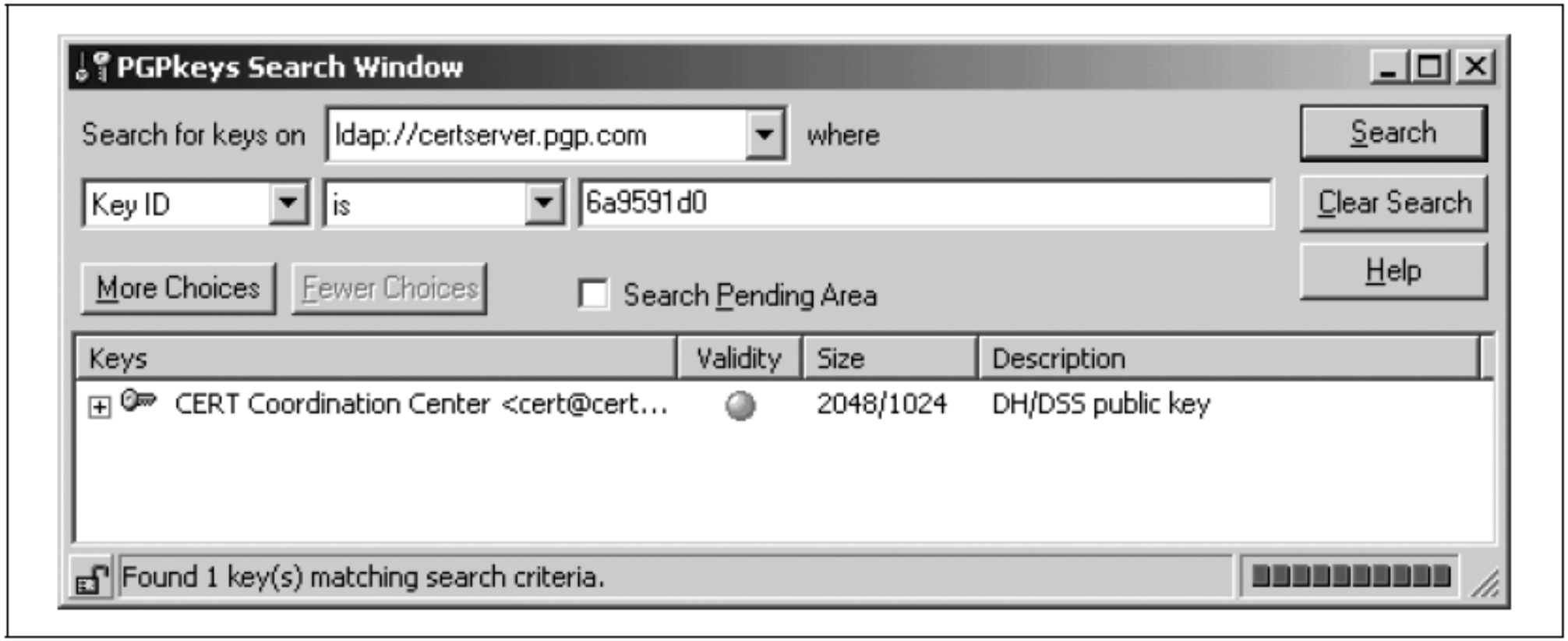

Figure 6-17. Searching for Key0x6A9591D0 on the PGP public key server finds the PGP key for the CERT Coordination Center

Downloading Key from PGP Key Server

- **Figure 6-18:**
  - Importing key into local key ring

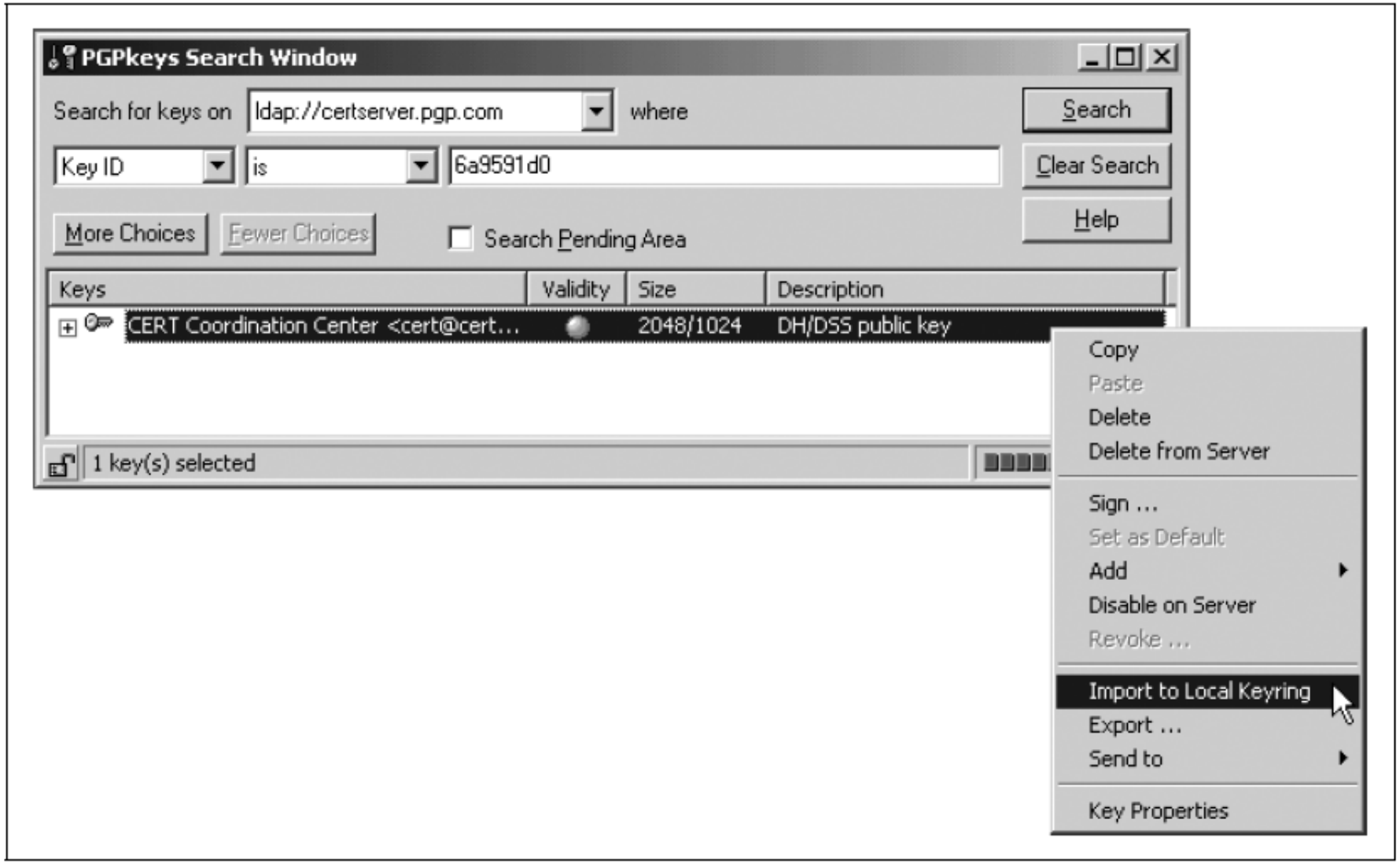

Figure 6-18. After you find a key on the public key server, you can import it by right-clicking on the key and choosing "Import to Local Keyring."

Verifying the PGP-signed File

- Verification possible via:
  - Command-line PGP
  - Graphical PGP interface
- Output indicates:
  - “Good signature”
  - Signer identity
  - Timestamp

Graphical Verification with PGP

- **Figure 6-19:**
  - Right-click file → Verify signature

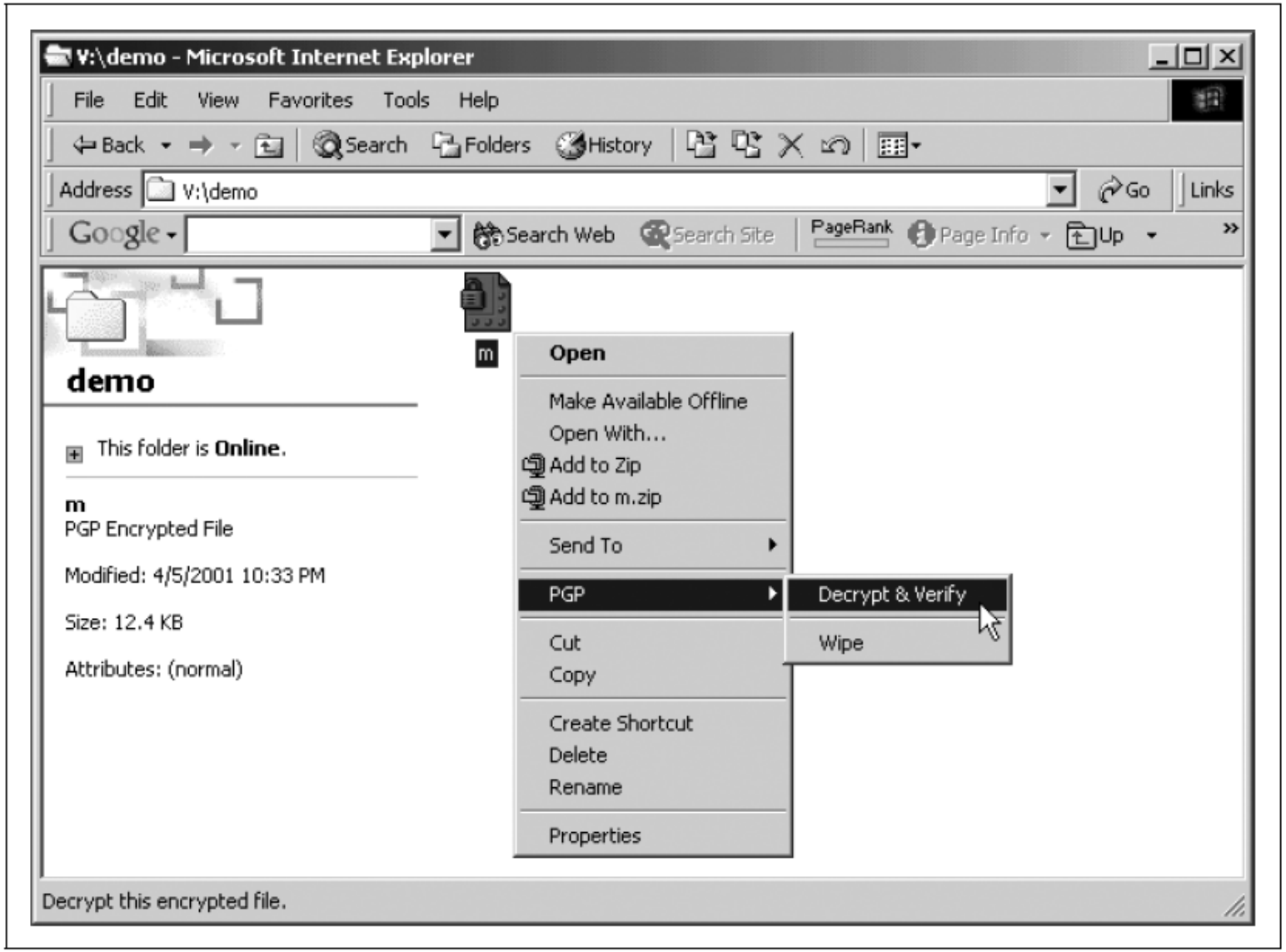

Figure 6-19. You can decrypt a PGP-encrypted file directly from Explorer by right-clicking on the file and choosing "Decrypt & Verify" from the PGP menu.

Graphical Verification with PGP

- **Figure 6-20:**
  - PGP processing the verification

Figure 6-20. PGP displays the "Decrypting File(s)..." pop-up while it is decrypting a file. You can cancel this operation by clicking on the Cancel button.

Graphical Verification with PGP

- **Figure 6-21:**
  - Result window showing signature validity

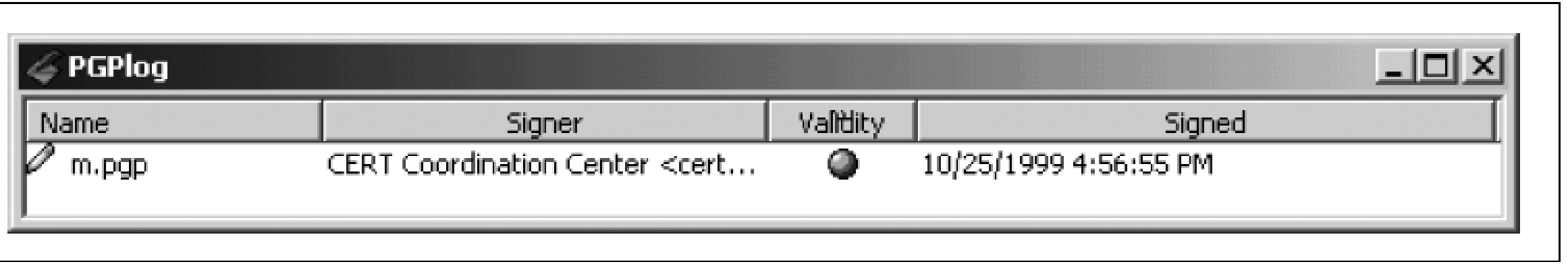

Figure 6-21. The PGPlog window will tell you whether a signature on a file is valid. In this case, the dot under "Validity" is green, and the signature is valid.

PGP Certification – Limitation

- PGP proves possession of private key
- Does NOT automatically prove real-world identity
- Anyone can create keys with fake names
- CERT/CC avoids this by publishing keys on its website

Public Key Authentication Using SSH

- **SSH (Secure Shell):**
  - Secure remote login protocol
  - Encrypts all communication
- Commonly used as a secure alternative to Telnet
- Supports:
  - Password authentication
  - Public key authentication (RSA)

RSA Authentication in SSH

- User registers RSA public key with SSH server
- Matching private key allows password-less login
- Key pair generated using **ssh-keygen**
- Files created:
  - identity.pub – public key
  - identity – private key

SSH Public Key Installation

- Public key copied to:
  - .ssh/authorized_keys on remote system
- Authorized keys file:
  - Lists keys allowed to log in without password
- After installation:
  - User logs in directly using private key

SSH Authentication Process

- Uses challenge-response protocol
- Server sends a random number (nonce)
- Client signs nonce with private key
- Server verifies signature using public key

SSH Authentication Process

- **Figure 6-22:**
  - Schematic of SSH public key authentication

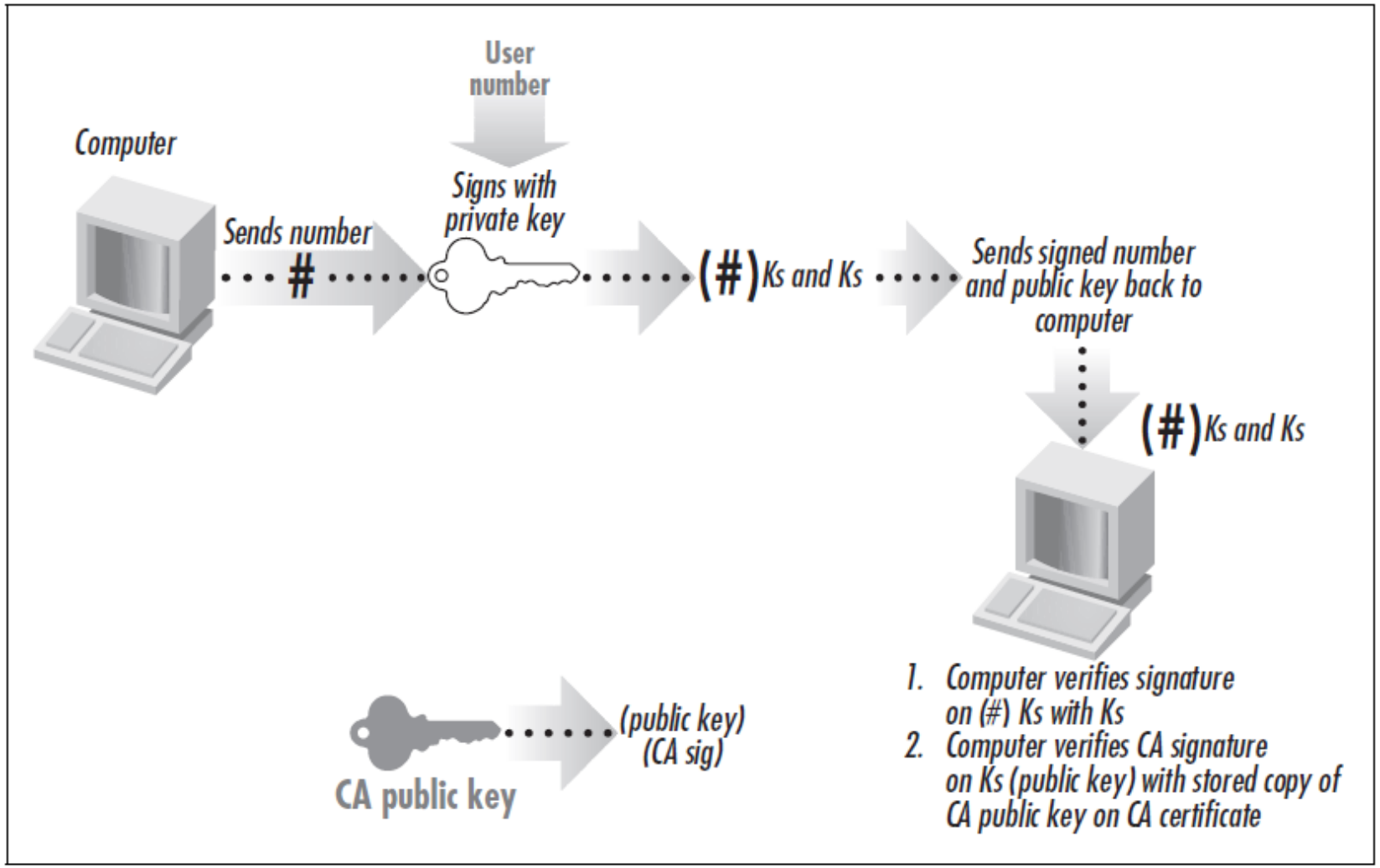

Figure 6-22. In a public key challenge-response process, a computer can provide a person with a number (the challenge) which must be signed. If the person can sign the number and return it to the computer, and if the digital signature can then be verified by the computer using the public key on file for the individual, the person must possess the private key that matches the given public key.

Security Properties of SSH Authentication

- Prevents replay attacks
- Private key never transmitted
- Eavesdropper cannot forge signatures
- Vulnerable if:
  - Private key is stolen
  - Key is not encrypted with passphrase

5. Digital Identification II: Digital Certificates, CAs, and PKI

- Digital certificates enable large-scale identity systems
- Bind:
  - Public key
  - Identity information
- Signed by trusted authorities

5.1. Understanding Digital Certificates with PGP

- **Digital certificate:**
  - Signed block of data
  - Contains public key + identity info

Understanding Digital Certificates with PGP

- **Figure 7-1:**
  - Conceptual digital certificate
- PGP public keys are full digital certificates

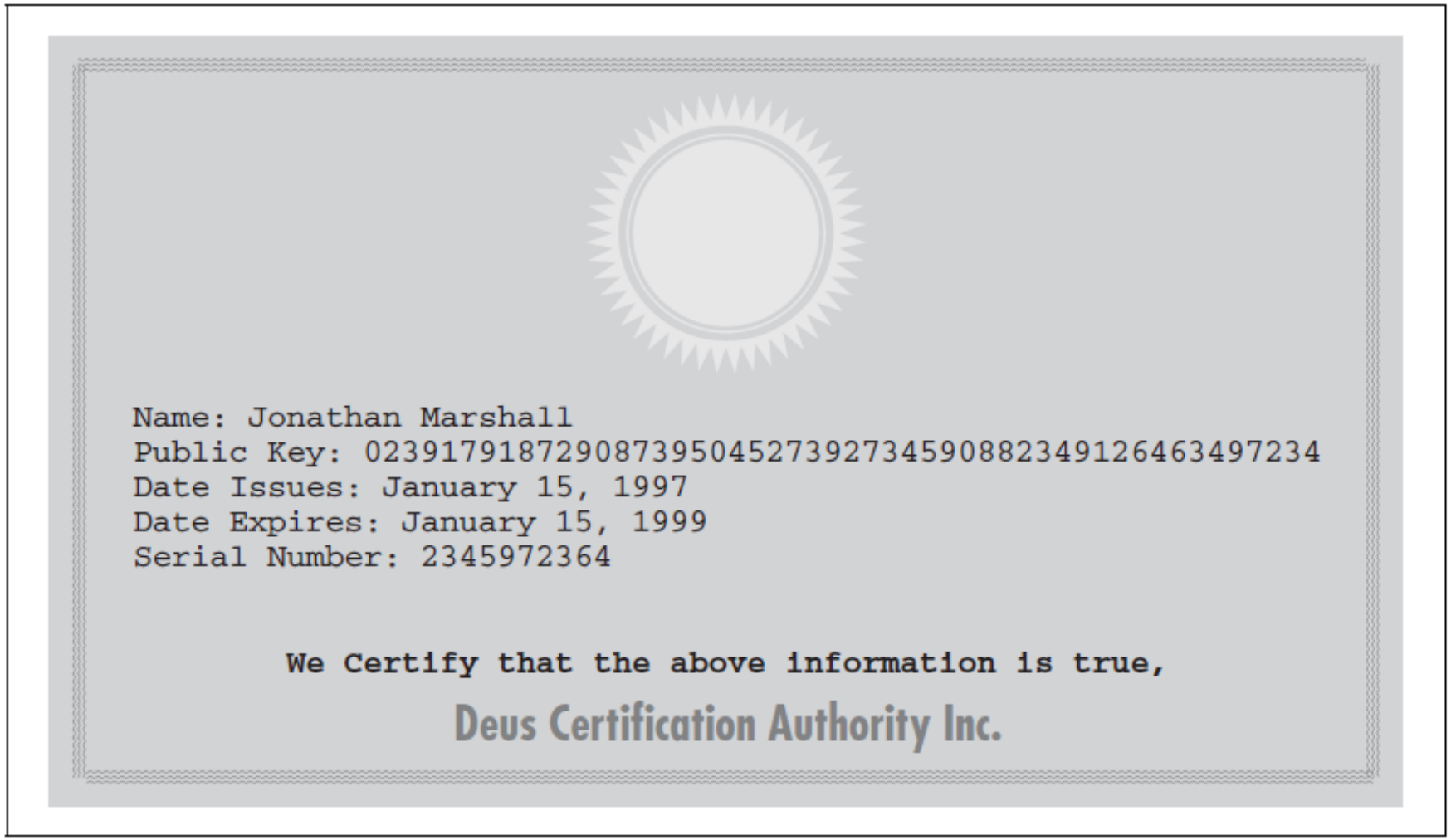

Figure 7-1. A digital certificate consists of a public key, additional information such as a person's name or affiliation, and a digital signature from a certification authority (CA).

Certifying Your Own Key

- PGP allows users to:
  - Create and self-certify keys
  - Certify their own identity information

- This freedom led to widespread adoption but also resulted in many **fraudulent keys.**

Certifying Your Own Key

- **Figure 7-2:**
  - Fake celebrity keys

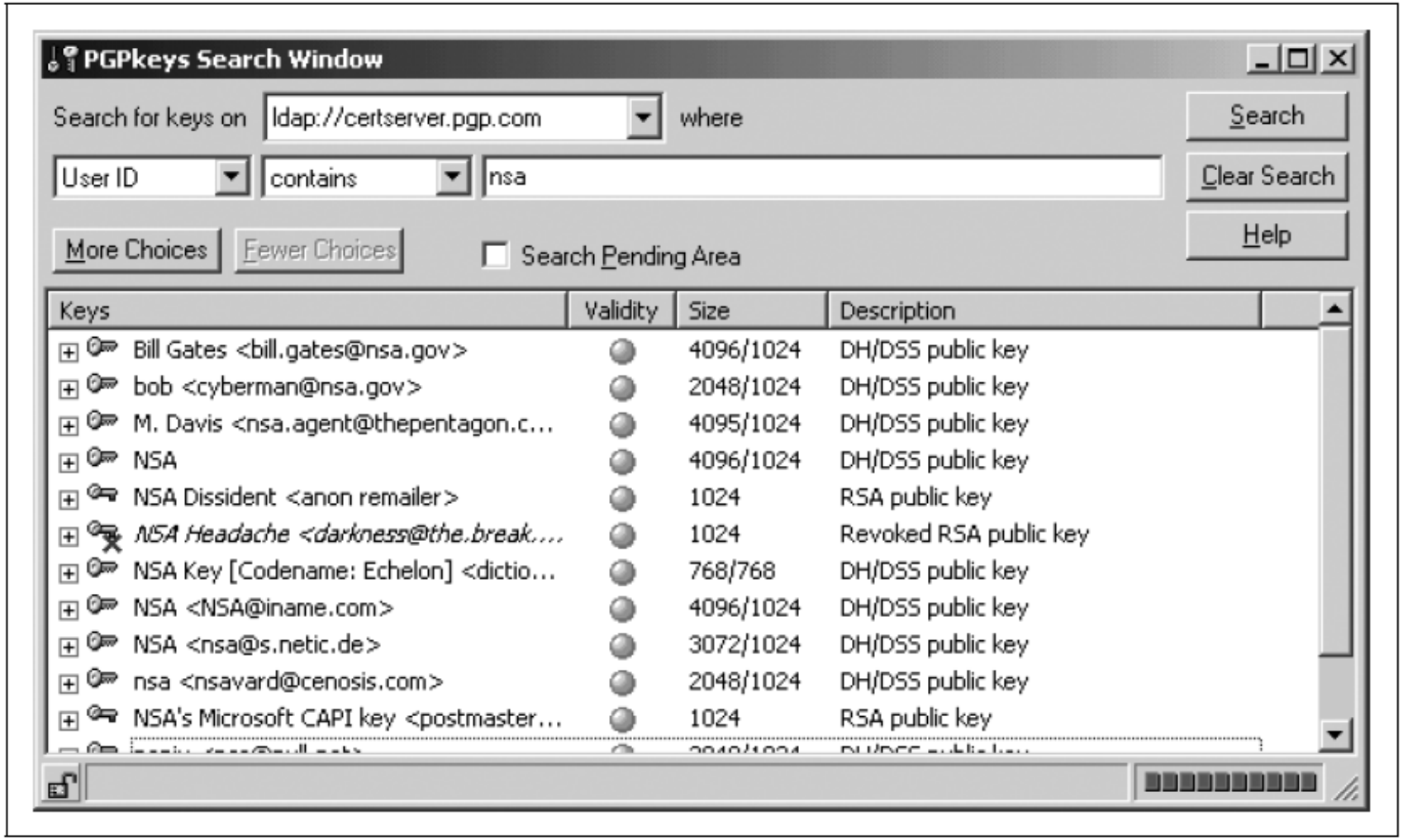

Figure 7-2. Many keys put on the PGP key server don't really belong to the person whose name is listed on them

Certifying Your Own Key

- **Figure 7-3:**
  - CERT/CC warning about fraudulent key

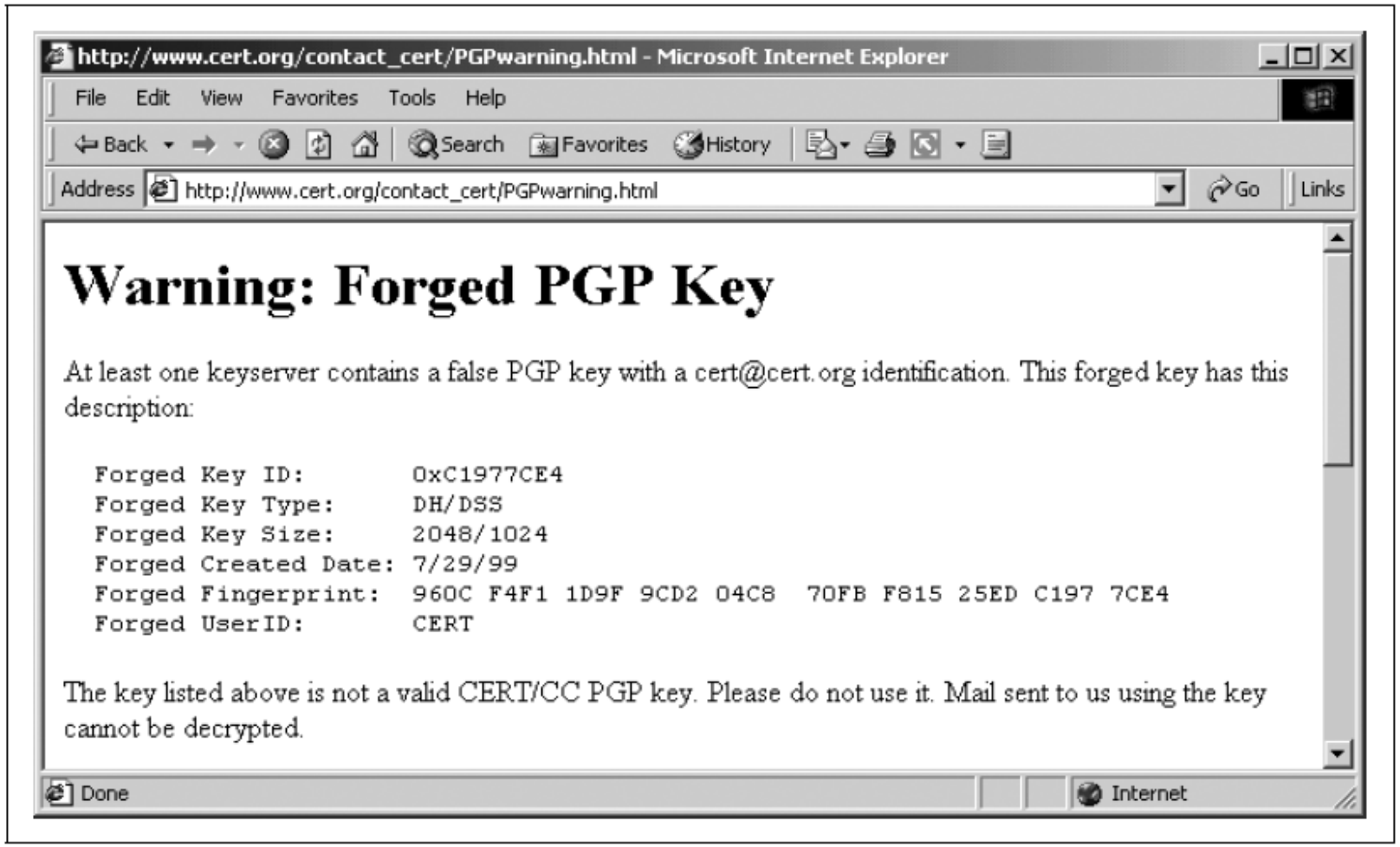

Figure 7-3. CERT/CC issued a warning about a fraudulent PGP key with CERT/CC's name that was put on the PGP key server.

Certifying Other People's Keys: PGP's "Web of Trust"

- PGP models trust socially, similar to how people trust others through acquaintances.
- Users can sign other users' keys, asserting that the key belongs to that person.

Trust and Validity

PGP distinguishes between:

- **Validity**: Whether the key truly belongs to the claimed identity.
- **Trust**: How much confidence you have in the key holder to certify others.

Figure 7-4 shows a PGP key ring displaying varying levels of trust and validity.

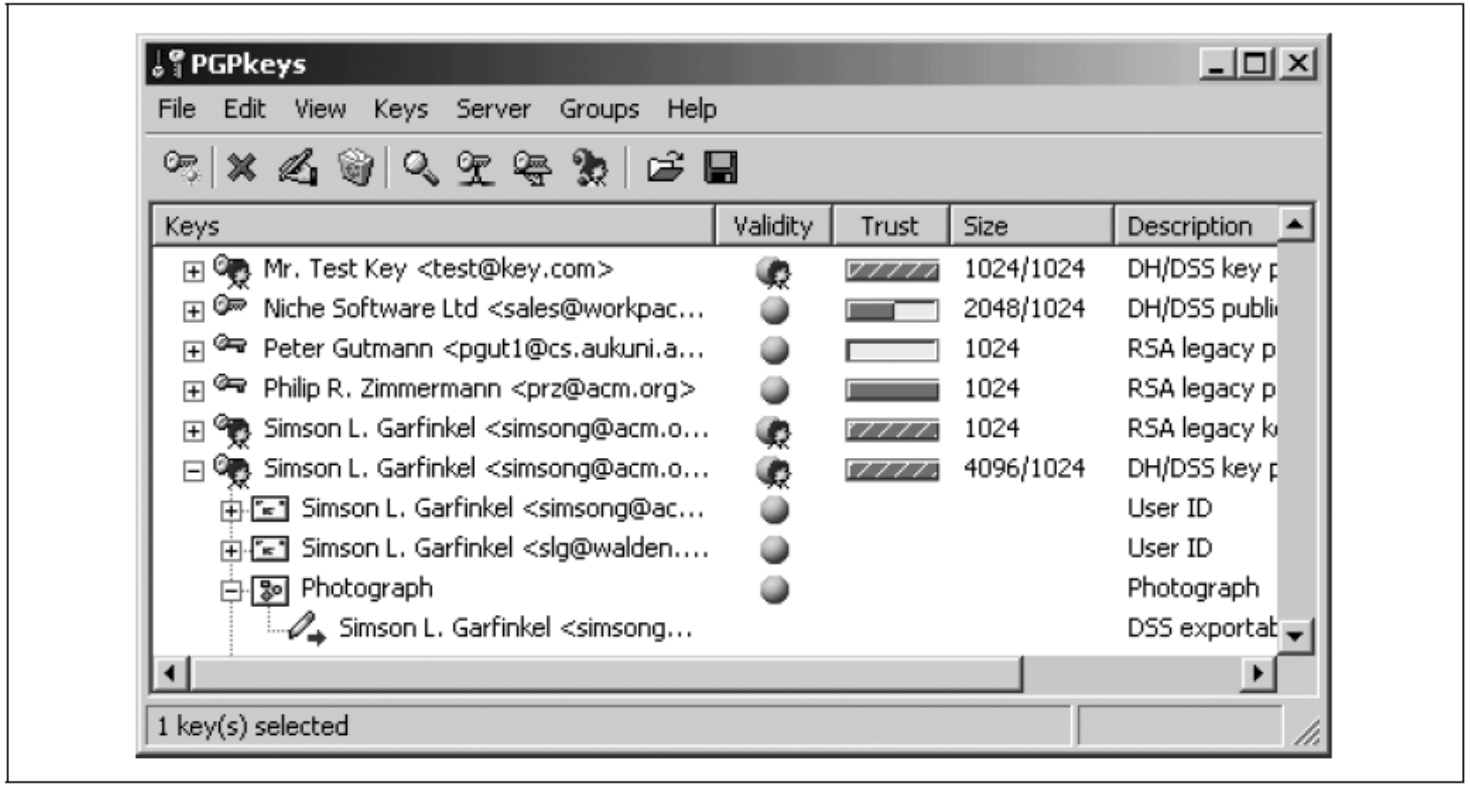

Figure 7-4. The PGPkeys application

Trust and Validity

- Phil Zimmermann envisioned a decentralized Web of Trust, shown in Figure 7-5.

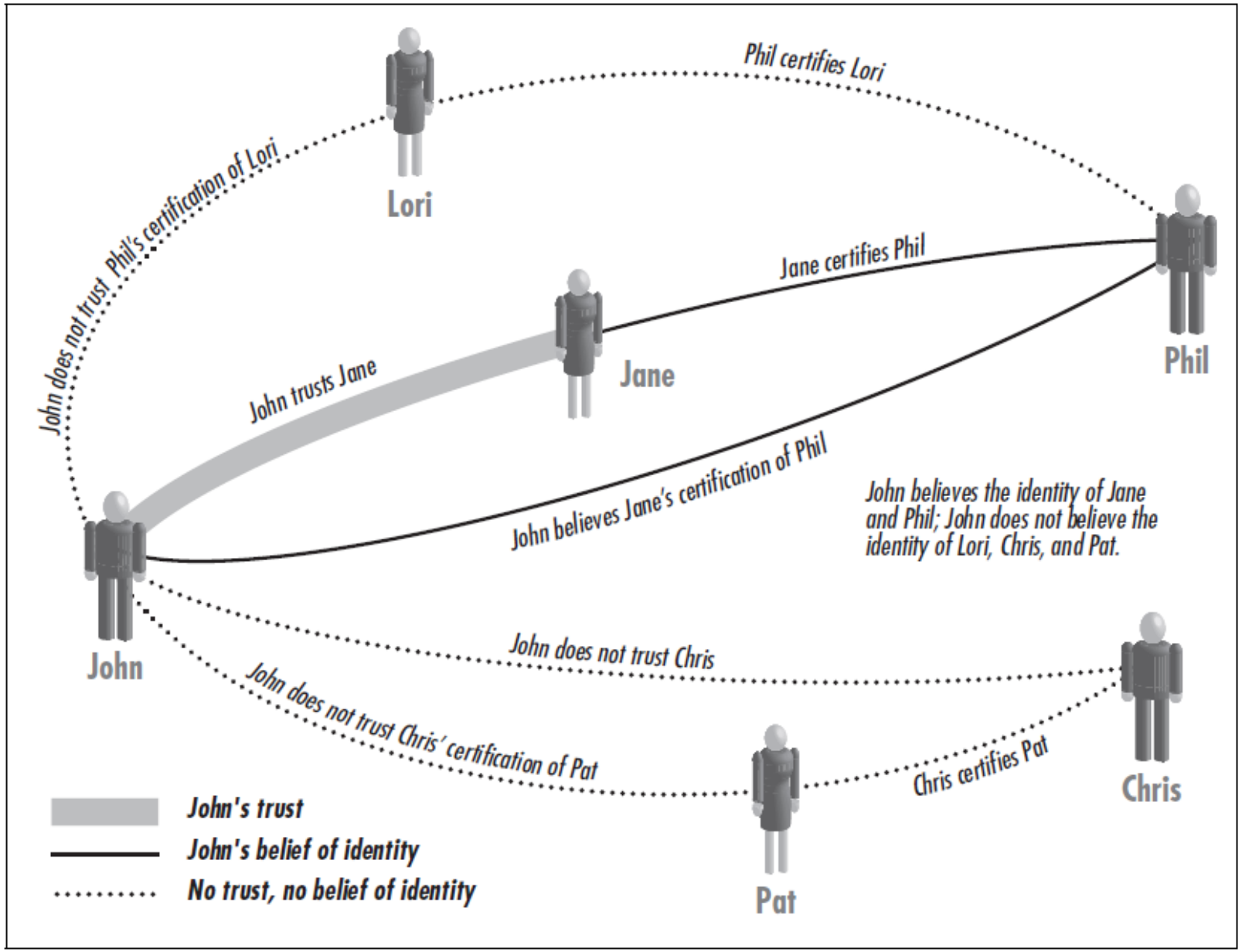

Figure 7-5. The PGP Web of Trust

The Web of Trust and Key Servers

- Figure 7-6 shows multiple signatures on a public key retrieved from a PGP key server.
- Trusted signatures help distinguish real keys from fraudulent ones.

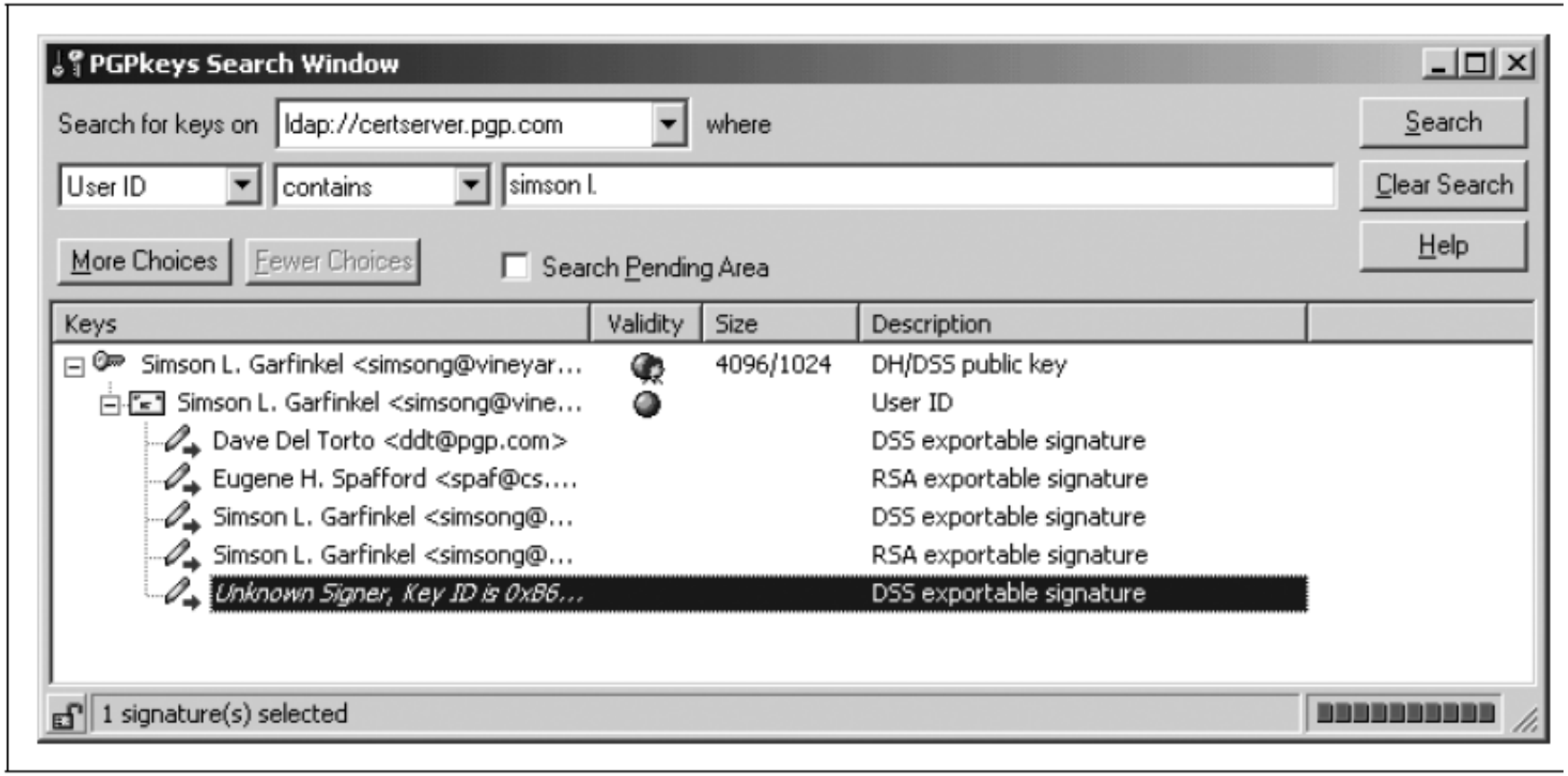

Figure 7-6. Simson's key on the PGP key server has five signatures on it.

Key Signing Parties

Key signing parties allow users to:

- Exchange keys
- Verify identity using official documents
- Sign each other's keys

While socially effective, they are impractical for large-scale systems and raise privacy concerns.

5.2. Certification Authorities: Third-Party Registrars

A Certification Authority (CA) issues digital certificates by signing public keys.

Examples include:

- Internal organizational CAs
- Outsourced CAs
- Trusted third-party CAs (e.g., VeriSign)
- **Figure 7-7:**
  - CA-issued certificate structure

Figure 7-7. A schematic certification authority certificate.

Certification Practices Statement (CPS)

- Legal document published by CA

A CPS describes:

- How certificates are issued
- How identity is verified
- Liability policies

- **Answers**:
  - “What does this certification mean?”

The X.509 v3 Certificate

Most CAs issue X.509 v3 certificates.

Each certificate **contains**:

- Version
- Serial number
- Subject identity
- Public key
- CA signature

Figure 7-8 - structure of an X.509 v3 certificate

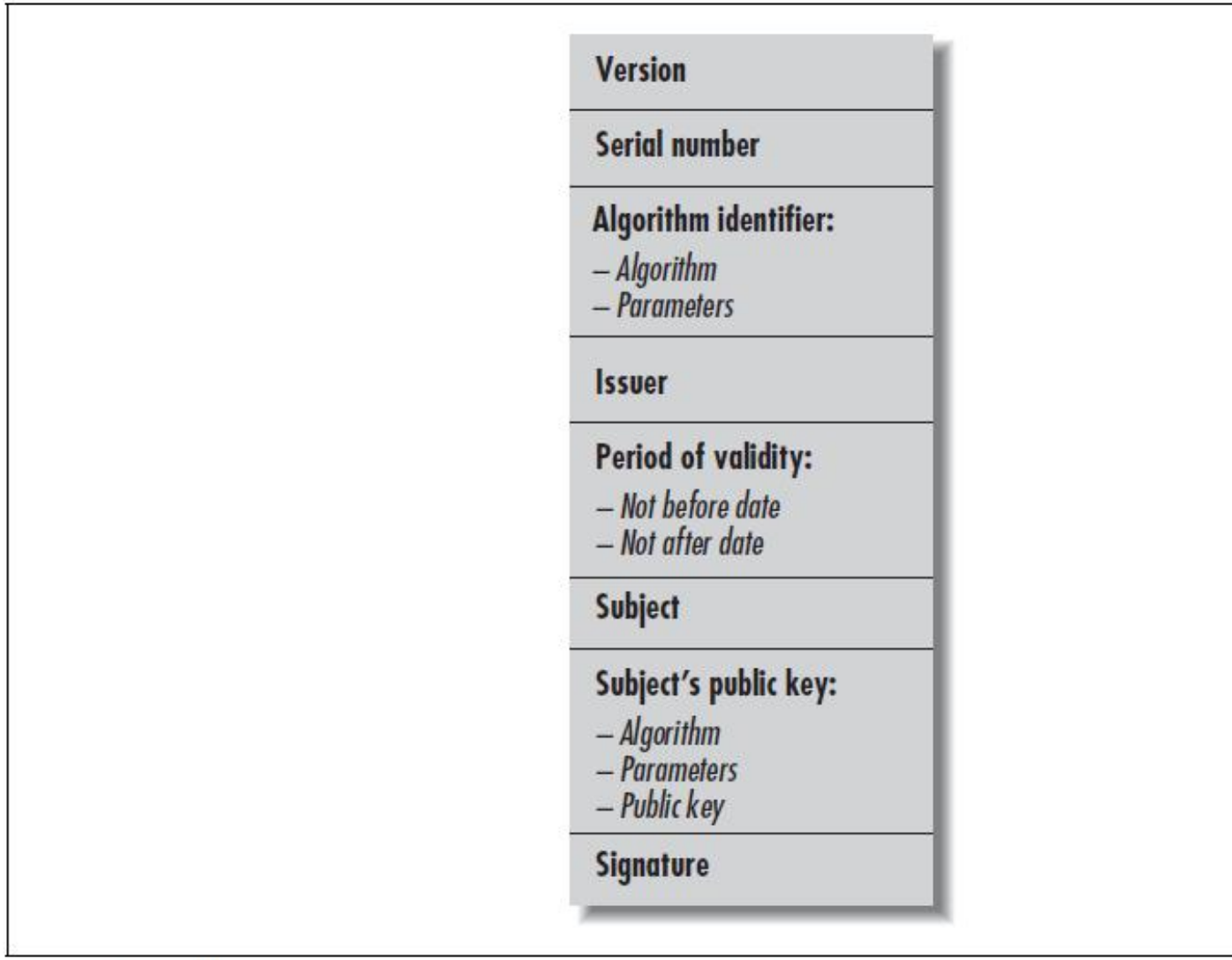

Figure 7-8. The schematic structure of a typical X.509 certificate

Exploring X.509 v3 Certificates

- Viewed using Internet Explorer
- **Figure 7-9:**
  - General certificate properties view

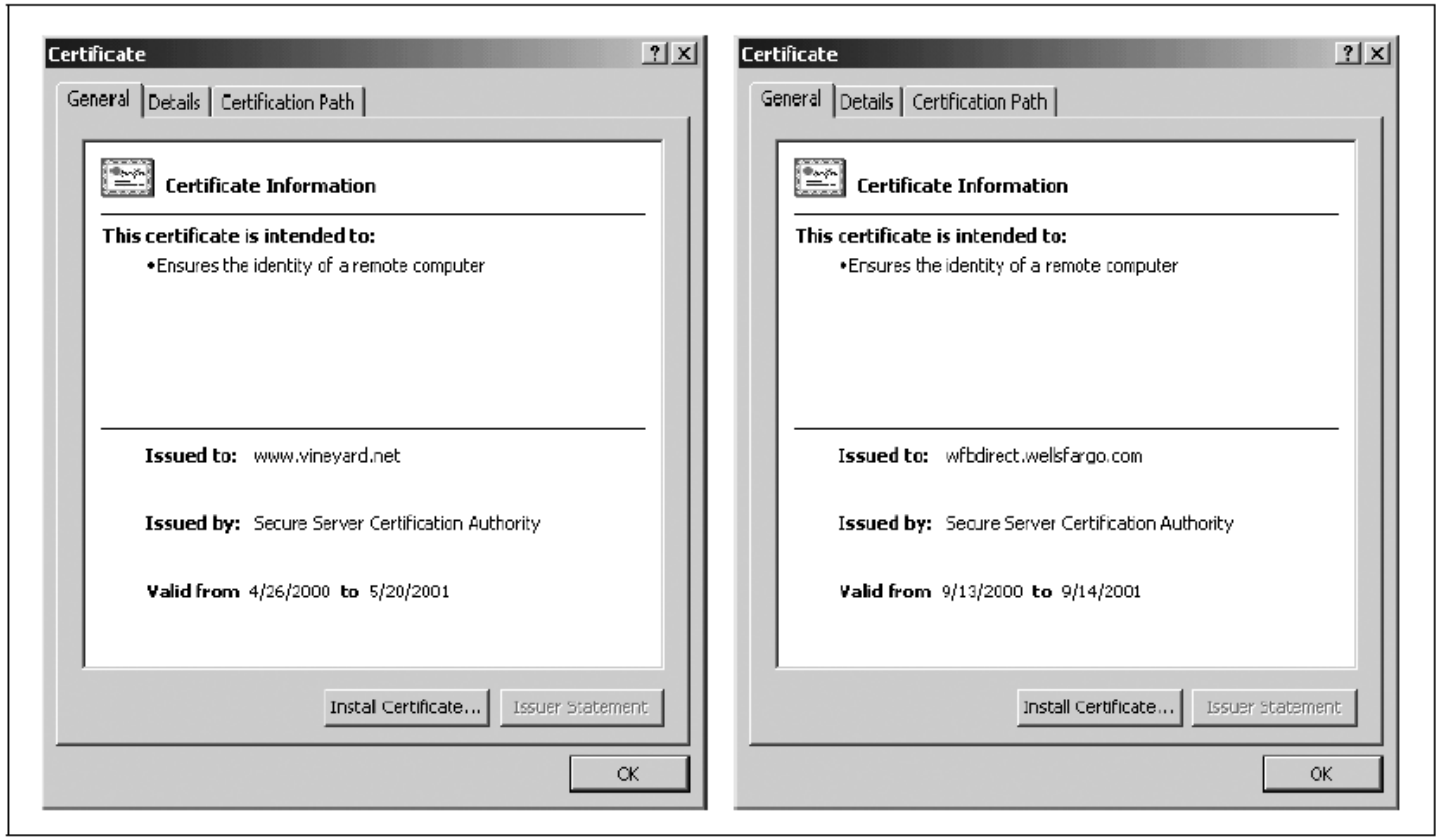

Figure 7-9. The "General" certificate properties, as viewed by Internet Explorer, for certificates downloaded from Vineyard.NET and Wells Fargo.

Exploring X.509 v3 Certificates

- **Figure 7-10:**
  - Detailed fields (Subject, Thumbprint, and validity period.)

Field Code	Meaning
CN	Common Name (for SSL certificates, the Common Name should be the DNS address of the server)
OU	Organizational Unit
O	Organization
L	Location
S	State
C	Country

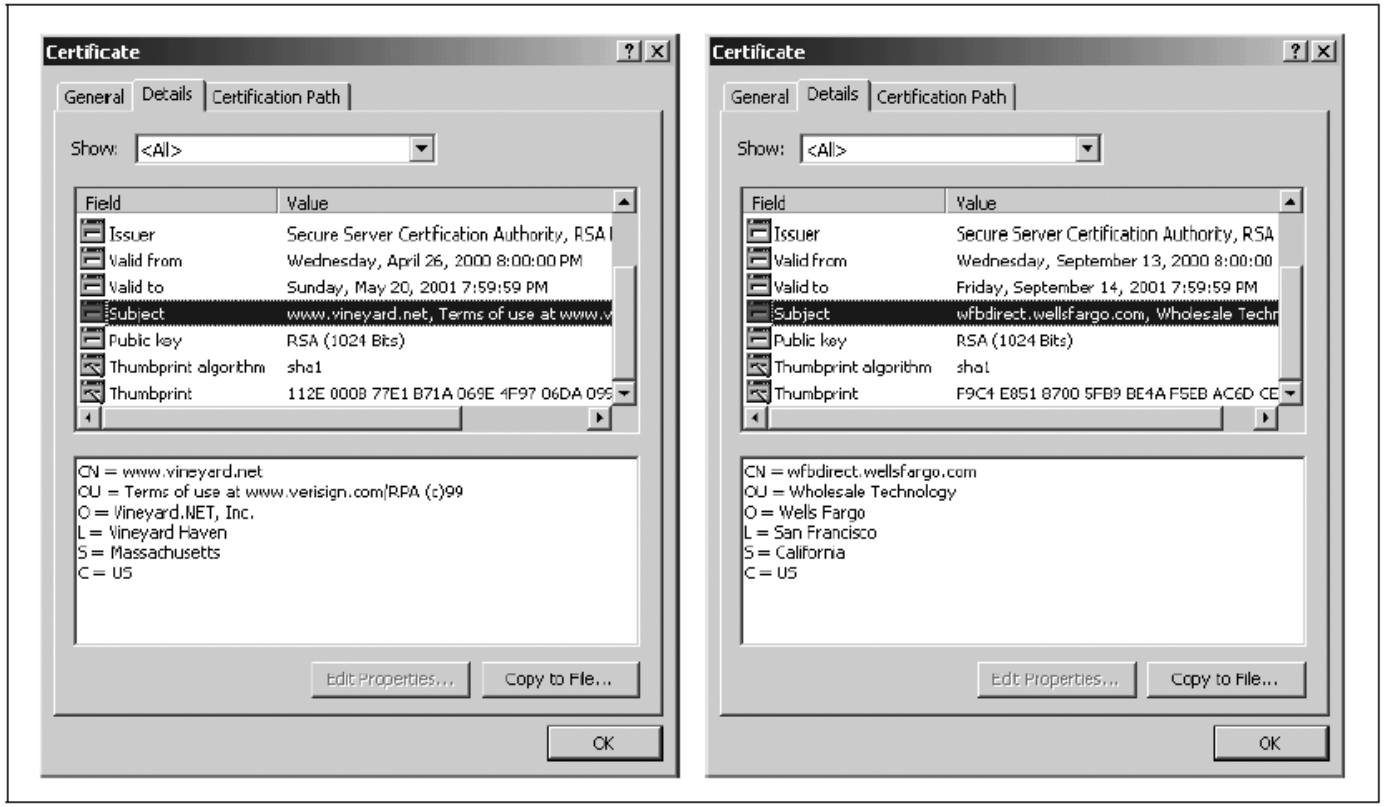

Figure 7-10. Some of the additional fields in the X.509 v3 certificates belonging to Vineyard.NET and Wells Fargo, as displayed by Microsoft Internet Explorer.

Exploring X.509 v3 Certificates

- **Figure 7-11:**
  - Certificate Path (certificate chain)

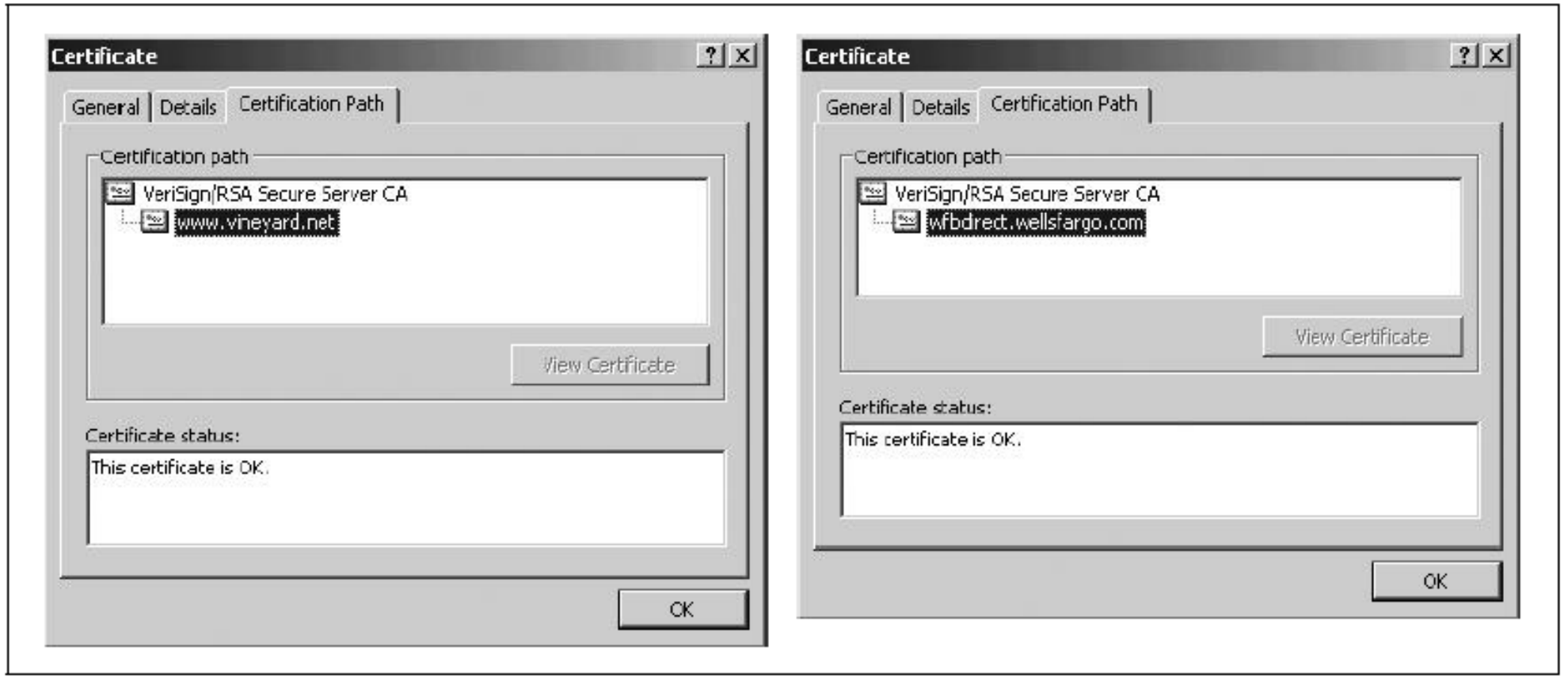

Figure 7-11. The Certificate Path panel for the certificates belonging to Vineyard.NET and Wells Fargo, as displayed by Microsoft Internet Explorer.

Self-Signed Certificates

- Signed by their own private key
- **Figure 7-12:**
  - Early self-signed CA certificate
- Trust comes from:

  - Software vendors bundling CA keys

  - Social trust in the software ecosystem

```
Data:
        Version: 0 (0x0)
        Serial Number:
            02:41:00:00:01
        Signature Algorithm: MD2 digest with RSA Encryption
        Issuer: C=US, O=RSA Data Security, Inc.,
                OU=Secure Server Certification Authority
        Validity:
            Not Before: Wed Nov  9 15:54:17 1994
            Not After: Fri Dec 31 15:54:17 1999
        Subject: C=US, O=RSA Data Security, Inc.,
                 OU=Secure Server Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: RSA Encryption
            Public Key:
                Modulus:
                    00:92:ce:7a:c1:ae:83:3e:5a:aa:89:83:57:ac:25:
                    01:76:0c:ad:ae:8e:2c:37:ce:eb:35:78:64:54:03:
                    e5:84:40:51:c9:bf:8f:08:e2:8a:82:08:d2:16:86:
                    37:55:e9:b1:21:02:ad:76:68:81:9a:05:a2:4b:c9:
                    4b:25:66:22:56:6c:88:07:8f:f7:81:59:6d:84:07:
                    65:70:13:71:76:3e:9b:77:4c:e3:50:89:56:98:48:
                    b9:1d:a7:29:1a:13:2e:4a:11:59:9c:1e:15:d5:49:
                    54:2c:73:3a:69:82:b1:97:39:9c:6d:70:67:48:e5:
                    dd:2d:d6:c8:1e:7b
                Exponent: 65537 (0x10001)
    Signature Algorithm: MD2 digest with RSA Encryption
    Signature:
        88:d1:d1:79:21:ce:e2:8b:e8:f8:c1:7d:34:53:3f:61:83:d9:
        b6:0b:38:17:b6:e8:be:21:8d:8f:00:b8:8b:53:7e:44:67:1e:
        22:bd:97:27:e0:9c:85:cc:4a:f6:85:3b:b2:e2:be:92:d3:e5:
        0d:e9:af:5c:0e:0c:46:95:ff:a1:1c:5e:3e:e8:36:58:7a:73:
        a6:0a:f8:22:11:6b:c3:09:38:7e:26:bb:73:ef:00:bd:02:a4:
        f3:14:0d:30:3f:61:70:7b:20:fe:32:a3:9f:b3:f4:67:52:dc:
        b4:ee:84:8c:96:36:20:de:81:08:83:71:21:8a:0f:9e:a9
```

Figure 7-12. The original RSA Secure Server Certification Authority certificate

Types of Certificates

Four major types are used:

1. Certification authority certificates
2. Server certificates
3. Personal certificates
4. Software publisher certificates

Each supports different authentication needs

Figure 7-13. Digital signatures and software publisher certificates are used to verify the integrity and authorship of software that is downloaded over the Internet.

How May I Certify Thee?

The Windows operating system allows you to specify for what purposes a certificate can be used. Allowable uses include:

- Server Authentication
- Client Authentication
- Code Signing
- Secure Email
- Time Stamping
- Microsoft Trust List Signing
- Microsoft Time Stamping
- IP security end system
- IP security tunnel termination
- IP security user
- Encrypting File System
- Windows Hardware Driver Verification
- Windows System Component Verification
- OEM Windows System Component Verification
- Embedded Windows System Component Verification
- Key Pack Licenses
- License Server Verification
- Smart Card Logon
- Digital Rights
- File Recovery

Additional purposes can be added on a certificate-by-certificate basis using the "Edit Properties..." button in the Certificate/Details panel (see Figure 7-10).

Netscape Navigator 6.0 also allows you to specify the so-called *trust settings* of what a certificate can be used for (see Figure 7-14). Perhaps because Navigator is not integrated with the operating system, Netscape allows only three uses for each certificate:

- "This certificate can identify web sites."
- "This certificate can identify mail users."
- "This certificate can identify software makers."

Figure 7-14. Netscape Navigator 6.0's Security Manager allows you to specify for what purpose a certificate will be used.

Minimal Disclosure Certificates

- Digital certificates can threaten privacy by revealing excessive information.
- **Minimal disclosure certificates** allow selective proof of facts without revealing identity.
- They were invented by **Stefan Brands** and licensed to **Zero Knowledge Systems.**

Revocation

- Certificates must be revoked when:
  - Keys are compromised
  - Issued incorrectly
  - Authorization changes
- **VeriSign–Microsoft incident** (2001) illustrates the importance of revocation.

Certificate Revocation Lists (CRLs)

A **CRL** lists revoked certificates.

Problems include:

- Large size
- Delays
- Poor implementation

Real-Time Certificate Validation

- Uses online CA checks
- **Alternatives include:**
  - XML Key Management Specification
  - SAML
- **Issues**:
  - Scalability
  - Denial of Service attacks

Short-Lived Certificates

- Very short expiration times
- Reduce revocation complexity
- Require frequent re-issuance
- Effective alternative to CRLs

5.3. Public Key Infrastructure

- Public key infrastructure (PKI) is a collection of
  - Digital certificates
  - Certification authorities (CAs)
  - S/w Tools, systems, and hardware
- It is used to deploy and manage public key cryptography.
- It enables secure communication,
  - authentication,
  - data integrity, and
  - nonrepudiation in distributed systems.

Meaning of “Public” in PKI

- Early vision:
  - Single, government-operated PKI
  - State-certified certificates for all citizens
- Certificates expected to function as:
  - Electronic equivalents of driver’s licenses
- Used for:
  - digitally signing tax returns and
  - conducting official online transactions.

Why the Public PKI Vision Did Not Happen

- No single government-run PKI emerged
- Private companies (e.g., VeriSign) issued millions of certificates
- Trust hierarchies used by hundreds of millions of users
- Operated by **private businesses**, not governments
- “Public” refers to **public keys**, not public ownership

Certification Authorities: Some History

- 1995: Netscape Communications entered the market
- WWW usage expanding rapidly
- Mosaic was dominant browser
- Netscape aimed to enable **Internet commerce**
- two major objections are raised by banks and security experts

1. Lack of protection for credit card numbers
2. No reliable way to verify the identity of online merchants

- To address these issues, Netscape developed the Secure Sockets Layer (SSL) protocol, which provided:
- Encrypted communication channels
- Server authentication using digital certificates
- SSL ensures that certificate signed by a trusted certification authority.

Netscape's SSL Trust Model

Netscape introduced a **broken key / whole key** icon in its browser:

- Whole key → SSL enabled and secure
- Broken key → No SSL, insecure

Consumers were advised not to enter credit card information on sites without SSL.

Netscape's model achieved:

1. Revenue generation by requiring SSL-enabled servers (Netscape Commerce Server)
2. Mandatory purchase of CA-signed certificates

Instead of operating its own CA, Netscape partnered with RSA Data Security, which already ran RSA Certification Services.

Rise of Competition and VeriSign

- Microsoft broke Netscape's dominance by releasing Internet Information Server (IIS). Open-source implementations like SSLeay further expanded SSL availability.
- Despite this, competition among CAs failed to flourish, largely due to RSA's aggressive enforcement of its patents. In 1995, RSA spun off its CA services into VeriSign, which quickly became dominant.

Browser Support for Multiple Certification Authorities

Netscape Navigator **Versions**

- Version 1.0: One CA (RSA Secure Server CA)
- Version 2.0: User-added CAs allowed
- Version 3.0: 16 CAs at 11 organizations

  (AT&T, BBN, Canada Post, VeriSign, Thawte, etc.)

Figure reference:

- The certificate manager figure shows viewing, deleting, and adding CA certificates.

Internet Explorer 3.0

- Shipped with a subset of Navigator's CA certificates.
- Despite technical readiness for competition, **VeriSign became the dominant CA**, absorbing competitors such as Thawte.

Internet Explorer Preinstalled Certificates

Internet Explorer ships with **preinstalled certificates**, which users can view via:

1. Internet Options
2. Content tab
3. Certificates button

Figure 7-15 reference:

- The Certificates panel figure displays certificate categories

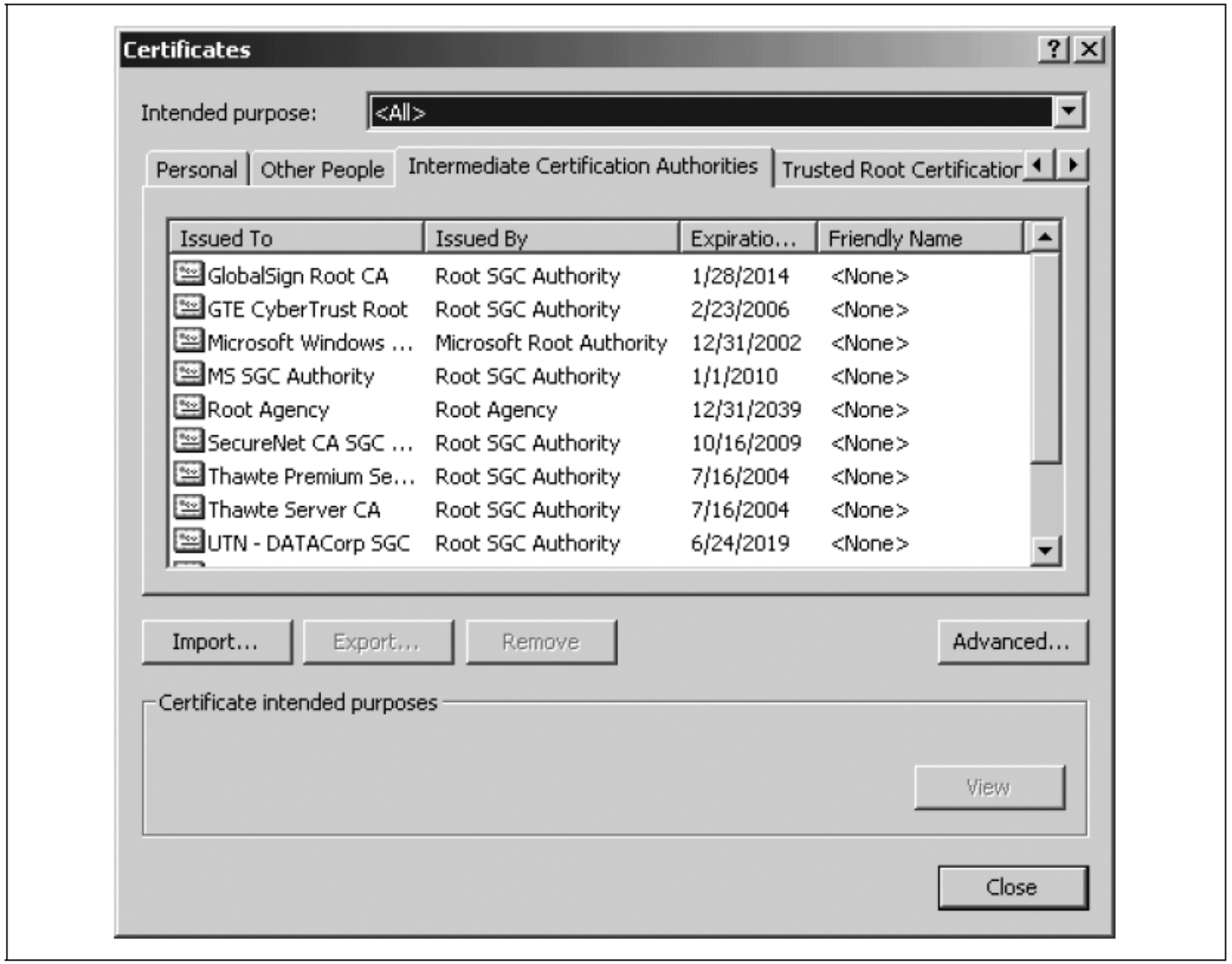

Figure 7-15. Internet Explorer comes with a set of built-in CA certificates.

Certificate Types

Personal

- Certificates issued to the user for identification and email encryption.

  (No default certificates)

Other People

- Certificates for verifying others' email signatures.

  (No default certificates)

Intermediate Certification Authorities

- CA certificates bundled but not fully trusted.

Trusted Root Certification Authorities

- Self-signed root certificates forming the roots of trust hierarchies.

Certificate Types

- **Table 7-1 reference:**

  The table lists trusted root CAs bundled with Internet Explorer.

- IE distributes **107 certificates**, all given equal trust—raising concerns about **unequal real-world reliability**.

Table 7-1. Certification authority keys bundled with Internet Explorer 5.0

Certification authority	Country	# of certificates
ABA.ECOM, Inc.	U.S.	1
Autoridad Certificadora de la Asociacion Nacional del Notariado Mexicano	Mexico	1
Autoridad Certificadora del Colegio Nacional de Corre-duria Publica Mexicana	Mexico	1
Baltimore EZ (Digital Signature Trust)	U.S.	1

Certificate Types

Table 7-1. Certification authority keys bundled with Internet Explorer 5.0 (continued)

Certification authority	Country	# of certificates
Belgacom E-Trust	Belgium	1
C&W HKT SecureNet	Hong Kong	4
CA 1 (ViaCode)	Great Britain	1
Certiposte	France	2
Certisign Certificadora Digital Ltda.	Brazil	4
Certplus	France	4
Deutsche Telekom	Germany	2
Digital Signature Trust	U.S.	6
Entrust.net	U.S.	1
Equifax Secure Certification Authority	U.S.	4
EUnet International	N/A	1
FESTE	Spain	2
First Data Digital Certificates	U.S.	1
FNMT	Spain	1
GlobalSign	Belgium	1
GTE CyberTrust	U.S.	3
IPS Seguridad	Spain	1
Microsoft	U.S.	3
National Retail Federation (Digital Signature Trust)	U.S.	1
NetLock Tanusitvanykiado	Hungary	3
PTT Post	Netherlands	1
Saunalahden Serveri Oy	Finland	2
Secure Server Certification Authority, RSA Data Security	U.S.	1
SecureNet	Australia	4
SecureSign, Japan Certification Services, Inc.	Japan	3
Servicios de Certificacion, Servicios Electronicos, Administracion Nacional de Correos	Uruguay	1
SIA S.p.A.	Italy	2
Swisskey AG	Switzerland	1
TC TrustCenter for Security in Data Networks GmbH	Germany	5
Thawte Consulting	South Africa	6
United Parcel Service (Digital Secure Trust)	U.S.	1
UserTrust	U.S.	5
ValiCert Validation Authority	U.S.	3

Certificate Types

Table 7-1. Certification authority keys bundled with Internet Explorer 5.0 (continued)

Certification authority	Country	# of certificates
VeriSign	U.S.	21
Xcert EZ (Digital Secure Trust)	U.S.	1

Netscape Navigator Preinstalled Certificates

- Netscape Navigator also includes many CA certificates.

Figure 7-14 reference:

- The Netscape Personal Security Manager figure shows certificate management.

Figure 7-14. Netscape Navigator 6.0's Security Manager allows you to specify for what purpose a certificate will be used.

Netscape Navigator Pre

Table 7-2 reference:

- The table lists CA keys bundled with Netscape Navigator 6.0.

Certification authority	Country	# of certificates
ABA.ECOM, Inc	U.S.	1
AddTrust	Sweden	4
American Express	U.S.	2
Baltimore CyberTrust	U.S.	3
BankEngine	Canada	1
BelSign Object Publishing CA (Since renamed GlobalSign)	Brussels,	4
beTRUSTed	"WW"[a]	1
CertEngine	Canada	1
Deutsche Telekom	Germany	1
Digital Signature Trust	U.S.	4
E-Certify	Canada	2
Entrust.net	U.S.	3
Equifax Secure Certification Authority	U.S.	5
FortEngine	Canada	1
GlobalSign	Belgium	5
GTE CyberTrust	U.S.	5
MailEngine	Canada	1
TC TrustCenter	Germany	5
Thawte Consulting	South Africa	6
TraderEngine	Canada	1
United States Postal Service	U.S.	1
UserTrust	U.S.	5
ValiCert Validation Authority	U.S.	4
VeriSign (and RSA)	U.S.	18
Visa International	U.S.	5
Xcert (Digital Secure Trust)	U.S.	5

[a] This is what the key says; it does not correspond to any particular country code.

Multiple Certificates for a Single CA

- Some CAs issue **multiple certificates** to indicate different trust levels.

  VeriSign has over **21 certificates**.
- **Table 7-3 and Table 7-4 references:**

  These tables show the evolution of VeriSign certificates (1996 vs 2001).
- VeriSign introduced **NetSure Protection**, an extended warranty program with **per-certificate liability limits**, not per-transaction limits.

Multiple Certificates for a Single CA

Table 7-3. VeriSign certificates in 1996

Certificate name	Certificate type	Certification practice	Cost	Liability protection
Class 1	Client[a]	VeriSign assures that the user can receive email at the given address and that no other certificate for the email address has been issued.	Free (nominally $9.95/year)	$100
Class 2	Client	VeriSign assures the identity of a digital ID holder through online identity verification against a consumer database.	$19.95/year	$5,000
Class 3	Client	VeriSign validates the entity applying for the certificate using background checks and investigative services.	$290/first year; $75/renewal	$100K
Secure Server	Server	VeriSign validates the entity applying for the certificate using background checks and investigative services.	$290/first year; $75/renewal	$100K

Multiple Certificates for a Single CA

Table 7-4. VeriSign certificates in 2001

Certificate name	Certificate type	Strength[a]	Certification practice	Cost	NetSure protection
Class 1 Digital ID	Client[b]	N/A	VeriSign assures that the user can receive email at the given address.	$14.95 per year	$1000
Secure Site	Server	40-bit	VeriSign validates the entity applying for the certificate by verifying the organization's address using Dunn & Bradstreet.	$349 per year	$100K
Secure Site Pro	Server	128-bit	VeriSign validates the entity applying for the certificate by verifying the organization's address using Dunn & Bradstreet.	$895	$250K
Commerce Site	Server	40-bit	VeriSign validates the entity applying for the certificate by verifying the organization's address using Dunn & Bradstreet. Price includes a performance audit of the web site from two cities.	$995	$100K
Commerce Site Pro	Server	128-bit	VeriSign validates the entity applying for the certificate by verifying the organization's address using Dunn & Bradstreet. Price includes a performance audit of the web site from ten cities.	$1495	$250K
OnSite for ServerIDs	Intermediate CA	40-bit or 128-bit	After validating an organization and negotiating a fee, VeriSign issues a certificate that allows the organization to issue its own certificates for SSL servers throughout its own enterprise.	Negotiated	

Shortcomings of Today's CAs

- **Lack of permanence for Certificate Policies field**
- Certificates contain URLs pointing to **Certification Practice Statements (CPS)**.
- **Figure 7-16 and Figure 7-17 references:**

  Figures show CPS URLs that are no longer accessible, even though certificates remain valid.
- CAs must maintain CPS URLs **for the lifetime of certificates**, possibly **20+ years**, but many fail to do so.

Shortcomings of Today's CAs

Figure 7-16. The General panel of Internet Explorer's Certificate window shows general information abut a certificate

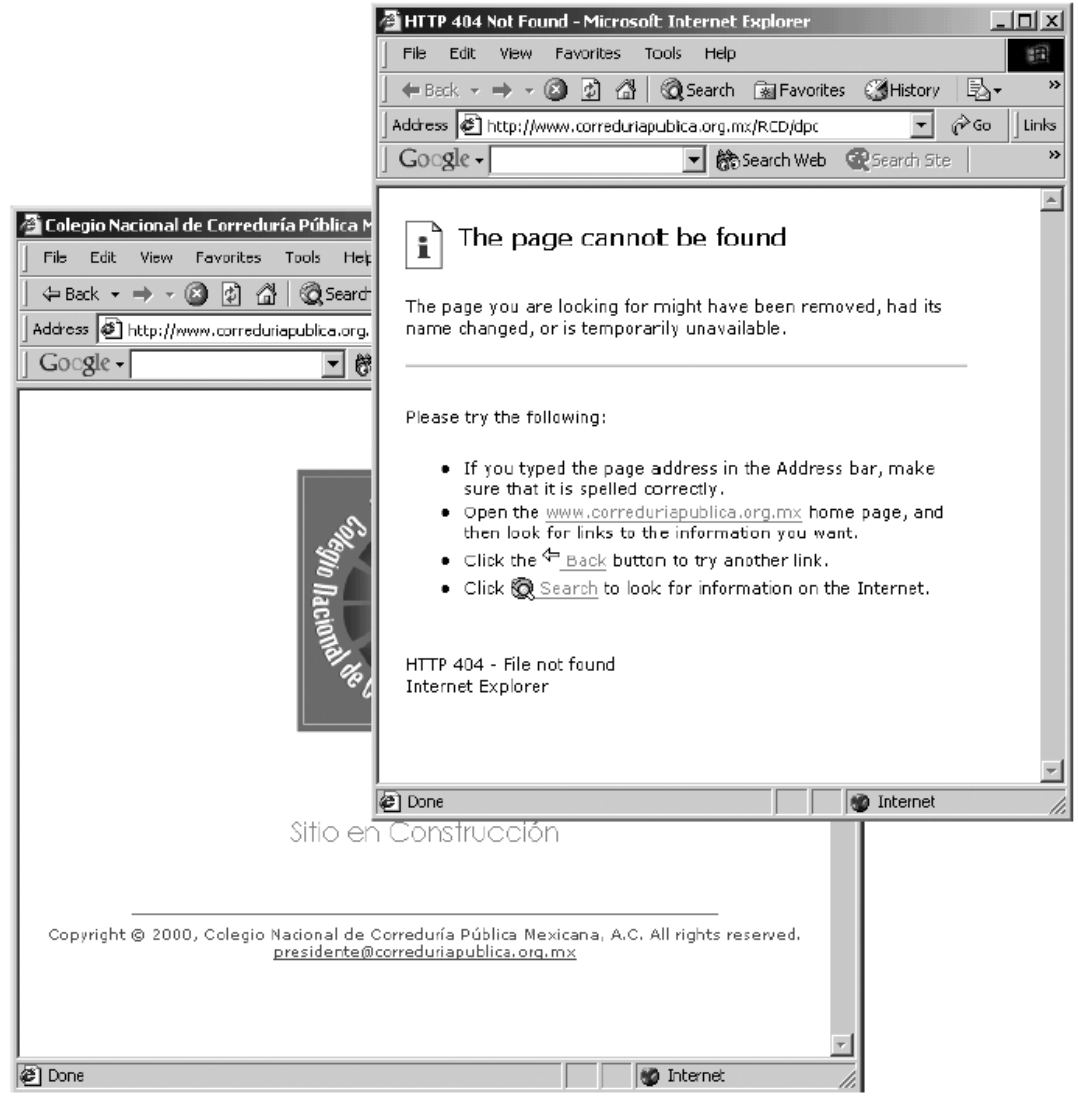

Figure 7-17. All CAs are not created equal. The home page of the web server for the Colegio Nacional de Correduria Publica Mexicana, A.C. reveals that the site is "en construcción"—and has been, apparently, for more than a year. The URL for the CA's certification practies statement does not exist. Yet this CA's key is fully trusted by Internet Explorer.

Inconsistencies for “Subject” and “Issuer” fields

- Different CAs use **inconsistent Distinguished Name (DN) formats**, making automated verification difficult.

Examples include:

- ValiCert
- VeriSign
- PTT Post
- SecureNet

Consistency is critical for **programmatic certificate validation.**

Unrealistic expiration dates

- Early certificates expired too soon (1999). Later certificates swung too far in the opposite direction, with expiration dates extending to **2028**.
- **Figure 7-18 reference:**
  The figure shows long-lived certificates with potentially weak cryptographic strength.

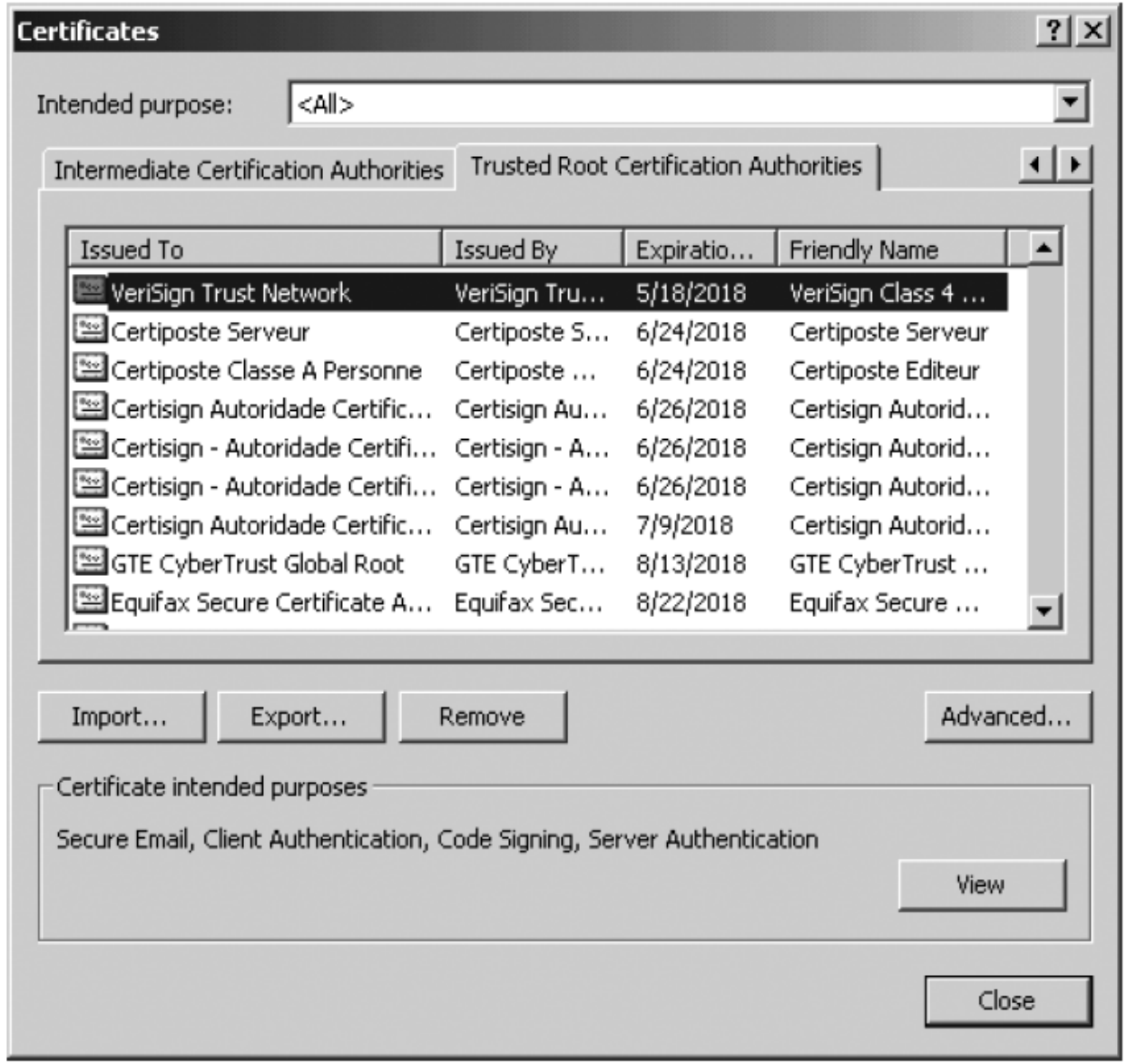

Figure 7-18. VeriSign distributes many keys with Internet Explorer 5.5 that have unrealistically late expiration dates

5.4. Open Policy Issues

- Despite growing fraud and digital signature legislation, **widespread PKI adoption remains elusive**. Managing millions of certificates across many CAs remains largely untested at scale.

Private Keys Are Not People

- Digital signatures prove **access to a private key,** not identity.
- End-user systems are often insecure:
  - Malware
  - Viruses
  - Trojan horses
  - Weak random number generators
- Even encrypted private keys must be decrypted for use, making them vulnerable.
- Smart cards may help, but **cannot guarantee absolute security**

Distinguished Names Are Not People

- Possession of a certificate does not guarantee that the **Distinguished Name** is accurate.

Key issues:

- Trustworthiness of CAs
- Audits and accreditation
- Policy enforcement
- Accidental or fraudulent issuance

There Are Too Many Robert Smiths

- **Names** alone are insufficient identifiers in large populations.
- **Certificates** must include additional unique identifying information.

Today’s Digital Certificates Don’t Tell Enough

Modern certificates lack:

- Age
- Gender
- Photograph
- Biometrics

Adding such data raises **serious privacy concerns**, highlighting the tension between **identity and anonymity**.

X.509 v3 Does Not Allow Selective Disclosure

- X.509 certificates do not support selective disclosure.
- **Alternative approaches:**
  - Multiple certificates
  - SPKI project
- Selective disclosure allows proving **specific attributes** without revealing full identity.

Digital Certificates Allow for Easy Data Aggregation

- Digital certificates may become **powerful aggregation tools**, enabling large-scale profiling more effectively than Social Security numbers.

How Many CAs Does Society Need?

Key questions:

- One CA vs many CAs
- Centralized power vs fragmentation
- Risk of exclusion from cyberspace

Carl Ellison questions whether identity certification always requires CAs.

How Do You Loan a Key?

Key-sharing scenarios raise unresolved questions:

- Delegation
- Role-based keys
- Legal responsibility
- Revocation

Why Do These Questions Matter?

- Digital signatures are **brittle**:
  - Minor changes invalidate signatures
  - Fail to show where changes occurred
- Paper documents still offer advantages in **tamper visibility**

Brad Biddle on Digital Signatures and E-SIGN

- This section outlines the legal evolution of electronic signatures:
- Utah Digital Signature Act
- Criticism of PKI-centric laws
- Shift to technology-neutral approaches

E-SIGN and UETA

- Recognize electronic signatures
- Are technology-neutral
- Replace Utah-style PKI mandates

Electronic Contracting

Electronic contracts follow traditional contract principles:

- Offer
- Acceptance
- Consideration

Digital signatures improve proof, not validity

“Signed Writing” Requirements

- Most contracts do not require signed writings.
- E-SIGN and UETA simplify compliance for electronic records.

Proof

Proof of:

- Contract formation
- Contract terms
- Party identity

Digital signatures reduce disputes but are not always cost-effective.