Forging Digital Signatures

Albert Levi
Sabanci University
Istanbul, TURKEY
levi@sabanciuniv.edu

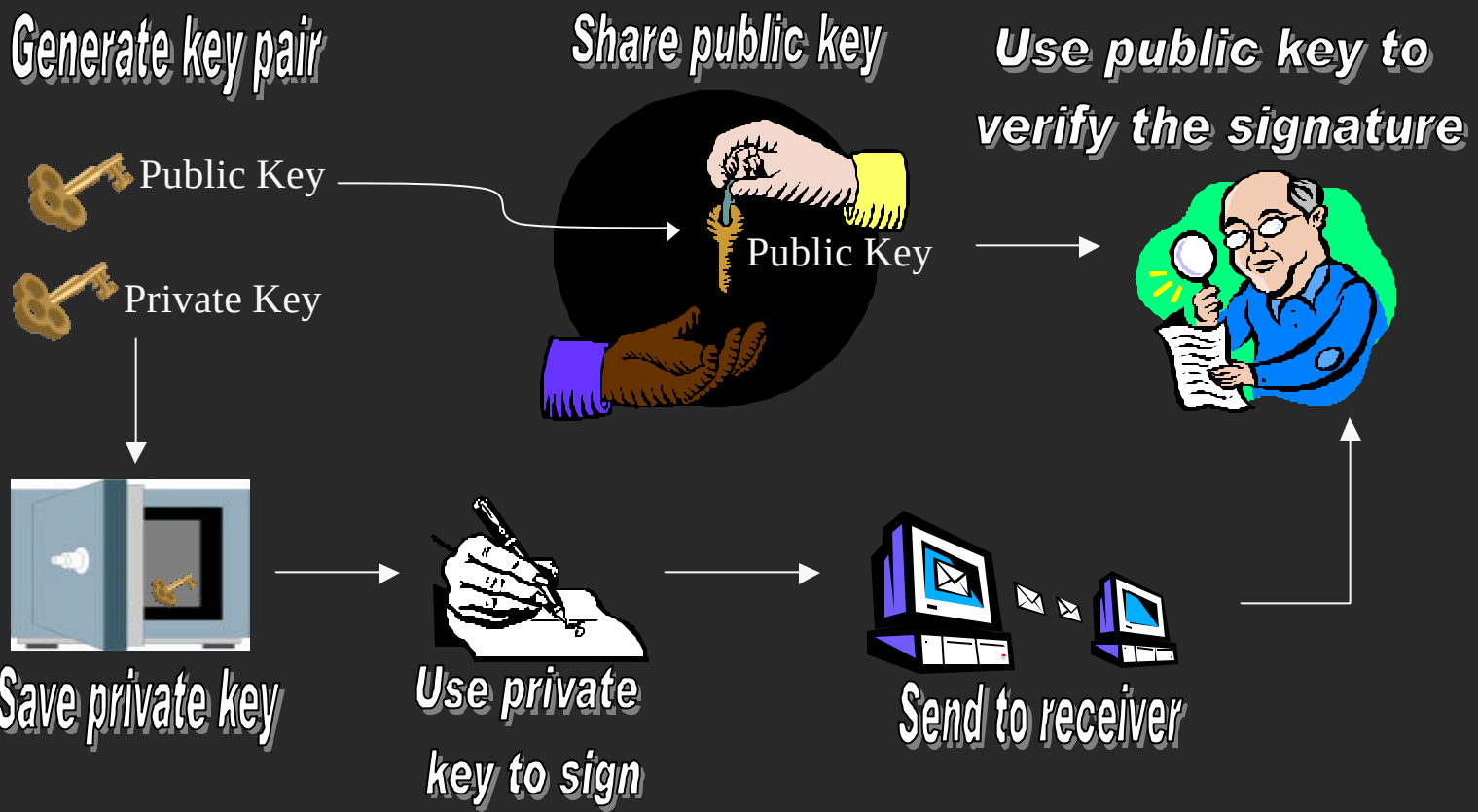
ACSAC 2002

Outline

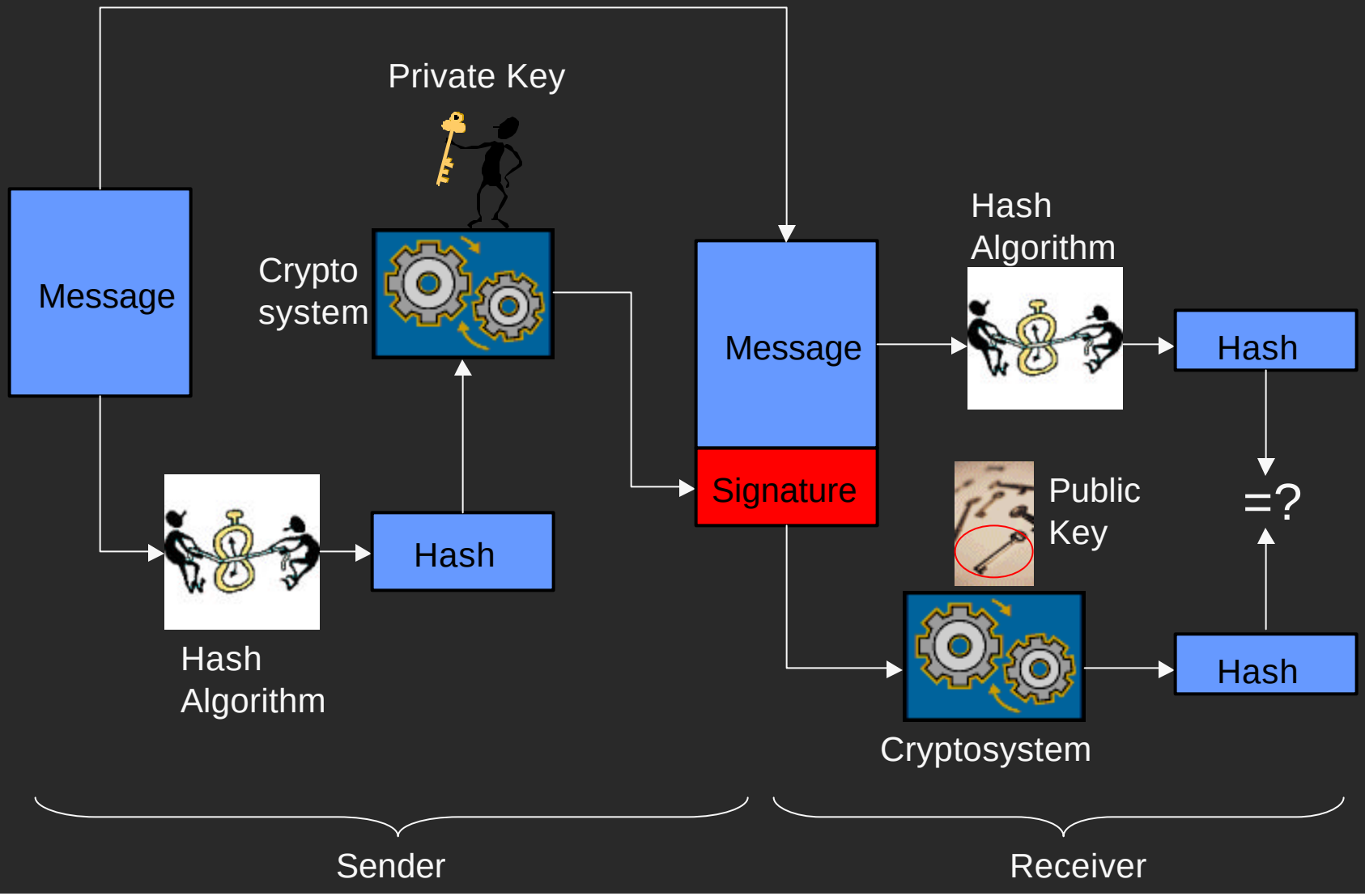
- What's a digital signature?
- How S/MIME handles digital signatures?
- How to obtain a certificate (a.k.a. digital ID)
- Tricks that you can do to get a bogus certificate
  - Sending a signed message using other's name
- Scope of a S/MIME signature and related problems
  - How to interpret a digital signature?

What is Digital Signature?

- Cryptographic processing over the message
- Uses public-key cryptography



In More Cryptographic Terms (e.g. RSA)



S/MIME

- Secure/Multipurpose Internet Mail Extensions
- A standard way for email encryption and signing
- IETF effort (RFCs 2632, 2633, 2634)
- Industry support
- Not a standalone software, a system that is to be supported by email clients
- Previous slide shows how S/MIME handles digital signatures
- Also provides encryption

Quick E-mail History

- SMTP and RFC 822
  - only ASCII messages
- MIME (Multipurpose Internet Mail Extensions)
  - content type
    - Almost any of information can appear in an email message
- S/MIME: Secure MIME
    - new content types, like signature, encrypted data

Certificates

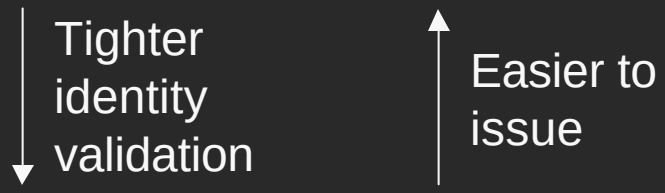
- Finding out correct public key of a user
  - Endorsed binding between the public key and the owner
  - Endorsed by a trusted Certification Authority (CA)
    - via CA's signature over the certificate
- How to determine user
  - by name?
  - by e-mail address?

Certificate Management in S/MIME

- CA-centered
- CA certificates come with the client software
- An ordinary user is not aware of the CAs that he/she trusts
- Certificates are sent along with the signed messages

Certificate Management in S/MIME

- One should get a certificate from a CA in order to send signed messages
- Certificates classes (common practice by most CAs)
  - Class 1
  - Class 2
  - Class 3



- CA certification policies (Certificate Practice Statement)
  - ID-control practices
    - Class 1: only email address
    - Class 2: against third party database
    - Class 3: apply in person and submit picture IDs and/or hard documentation

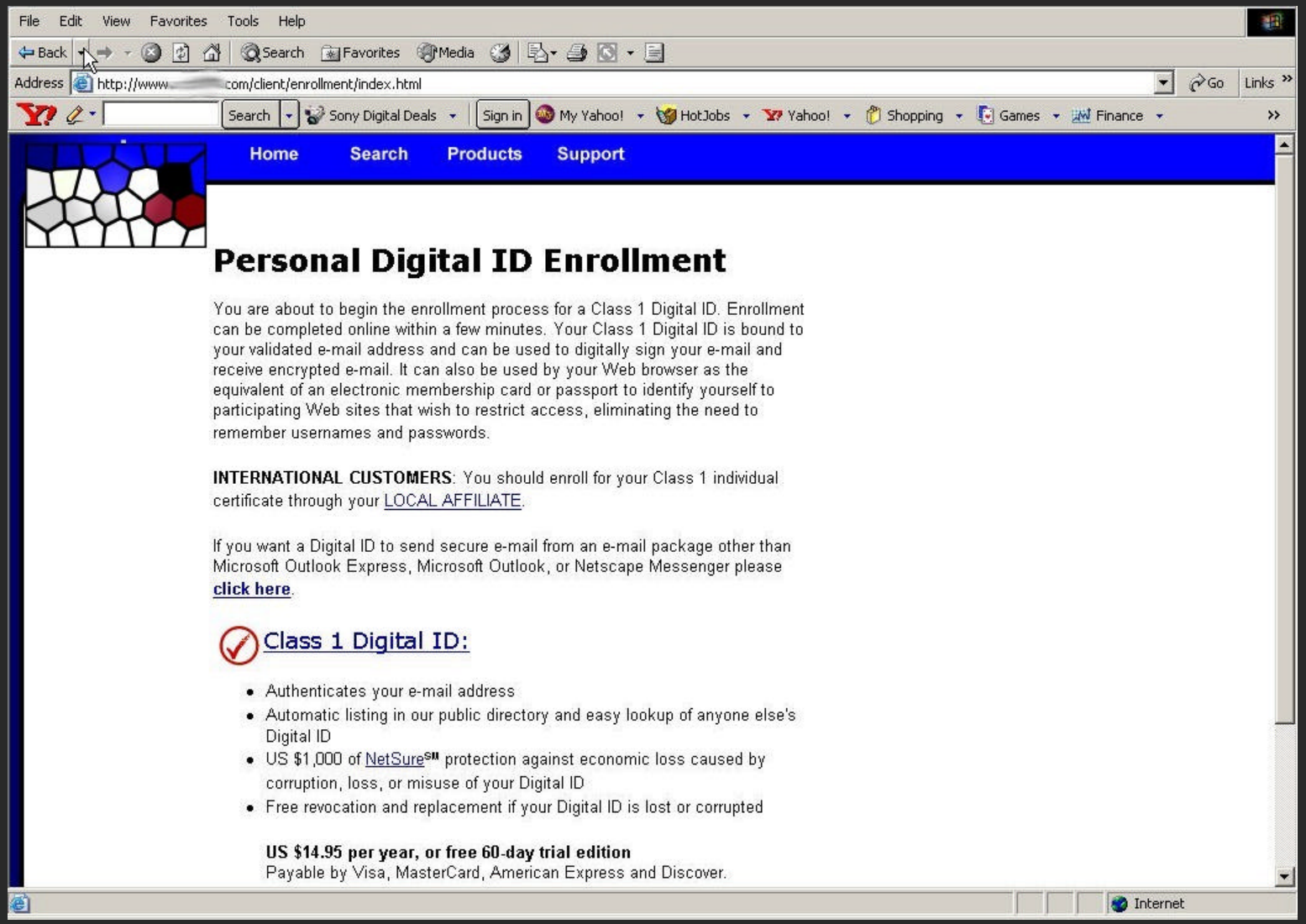
Attack 1: Class 1 Certificate Attack

- No identity check during registration
- Binding between public key and e-mail address
- It is possible to enroll under a different name
  - Name spoofing is possible in signed messages
- E-mail clients do not make this fact explicit to average users

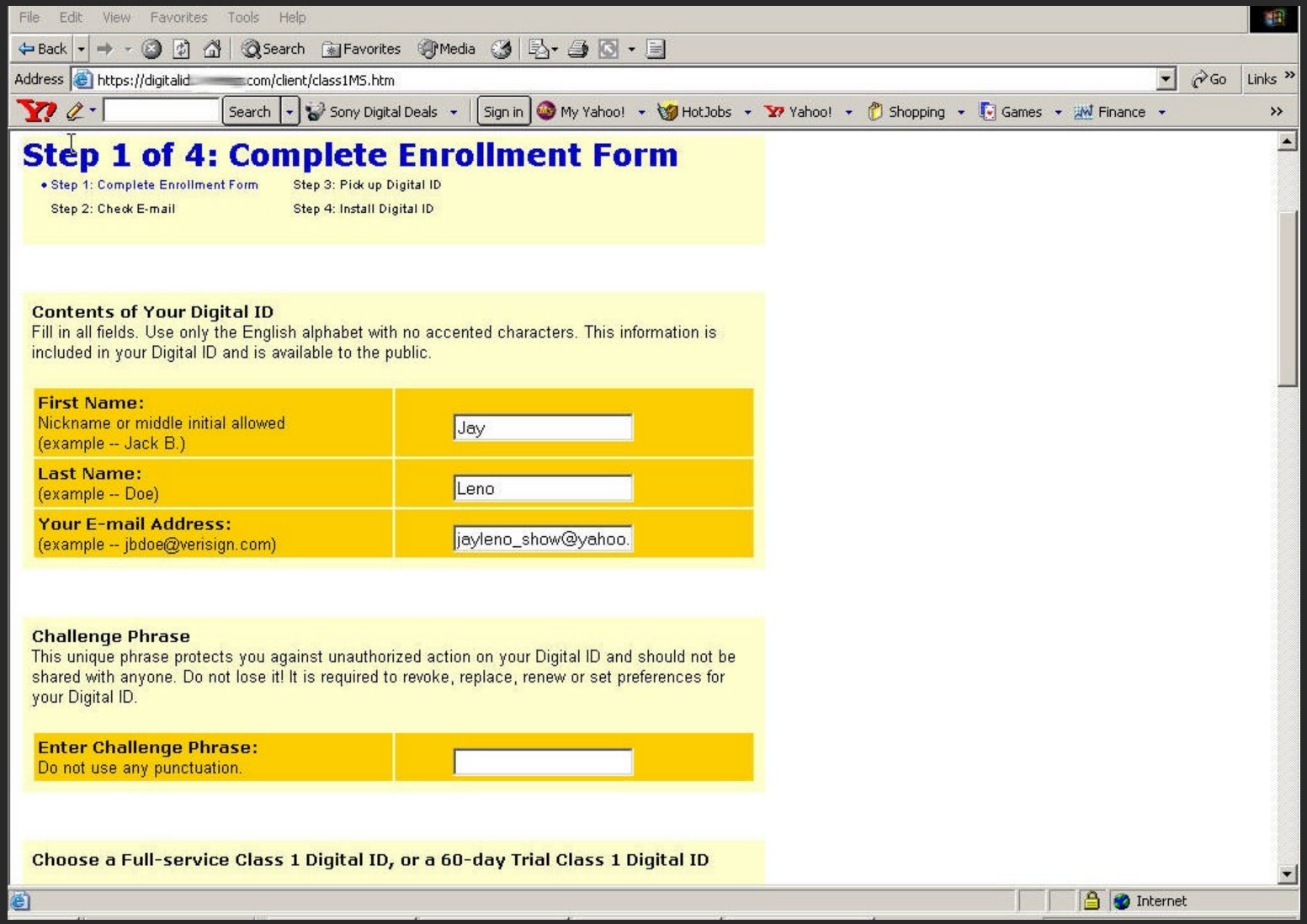
Attack 1: Class 1 Certificate Attack

- Step 1: Get an e-mail address that implies the person you want to imitate
- Step 2: Register for a certificate with that bogus name and e-mail address
- Step 3: Step up an outgoing e-mail account at your favorite e-mail client software with that bogus name
- Step 4: Send bogus signed messages

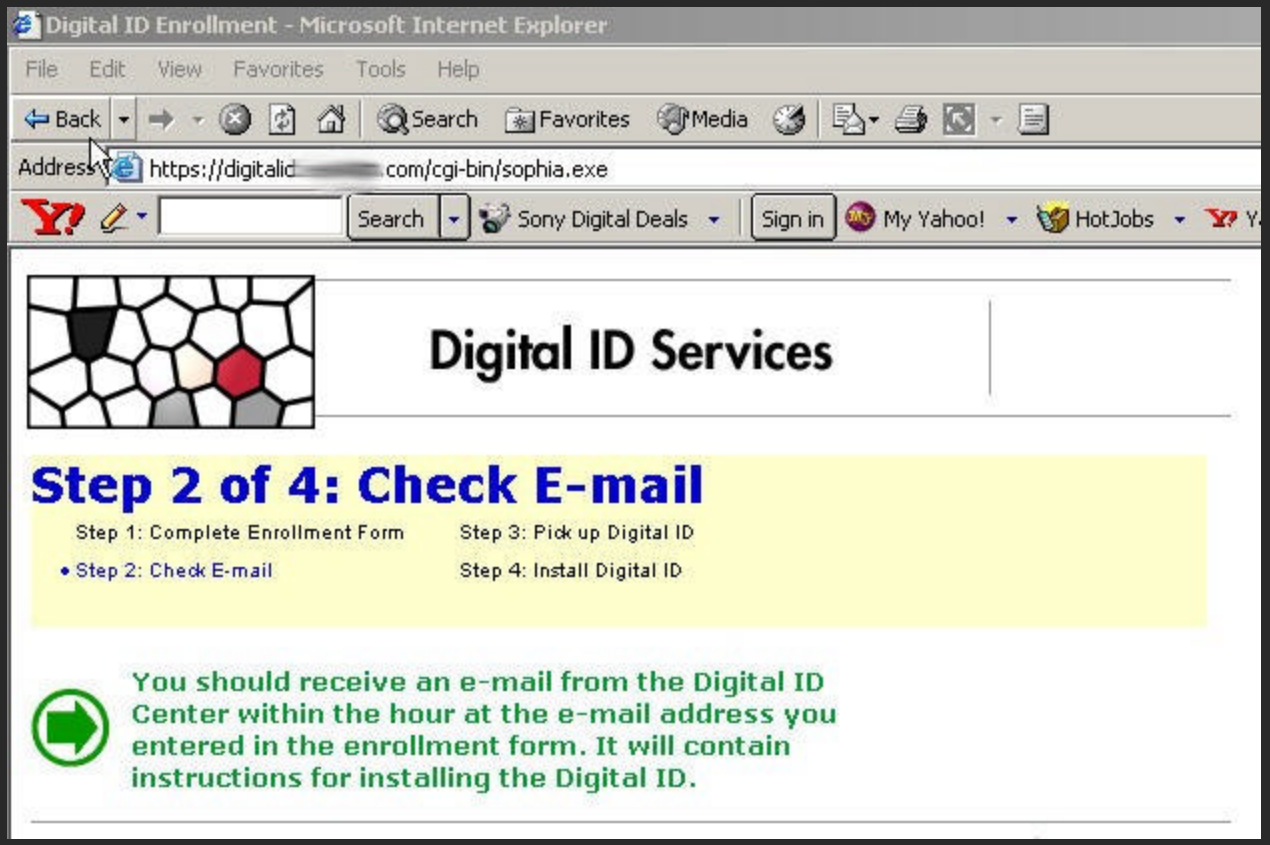
Step 2: Registration



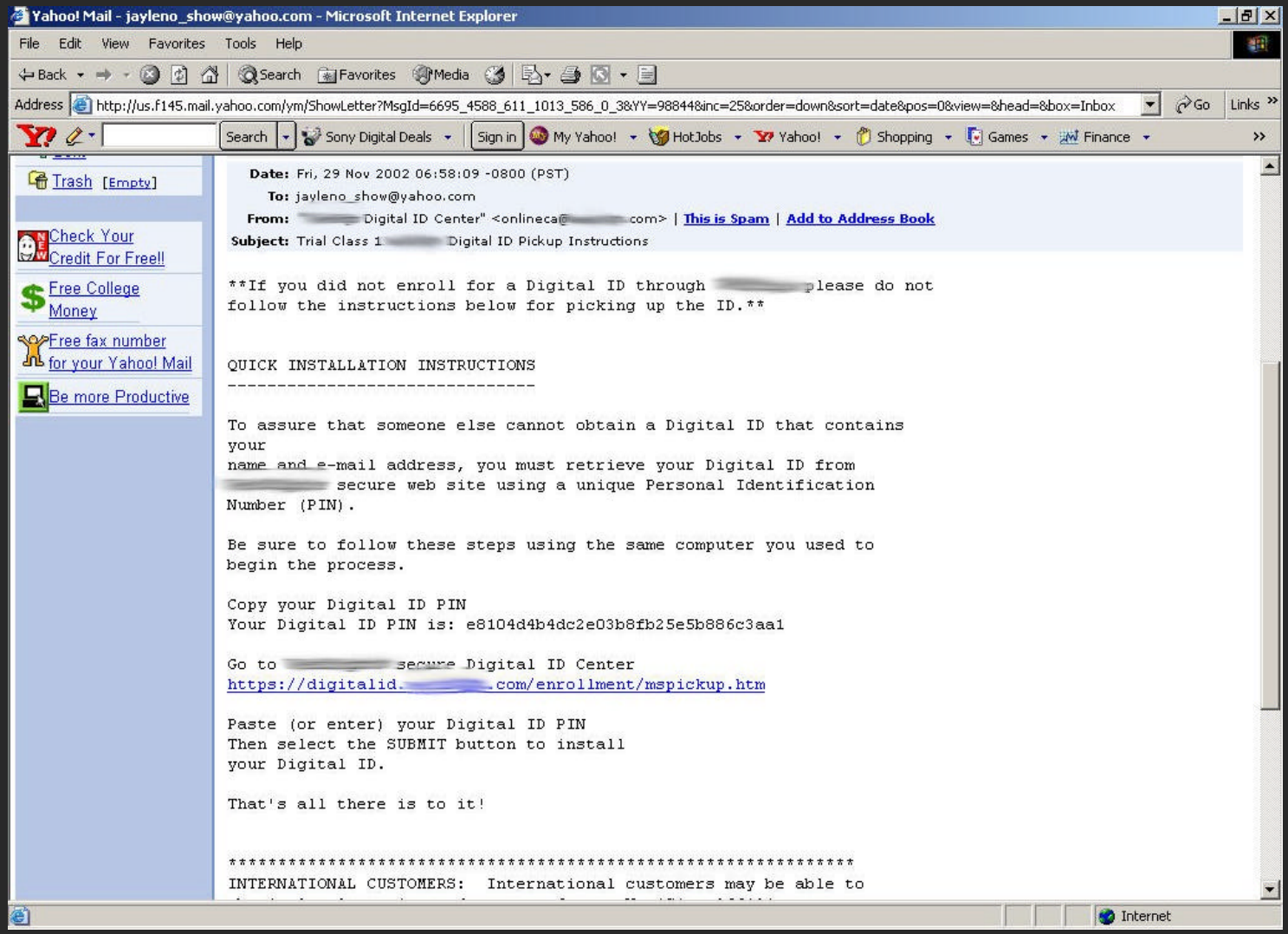
Step 2: Registration



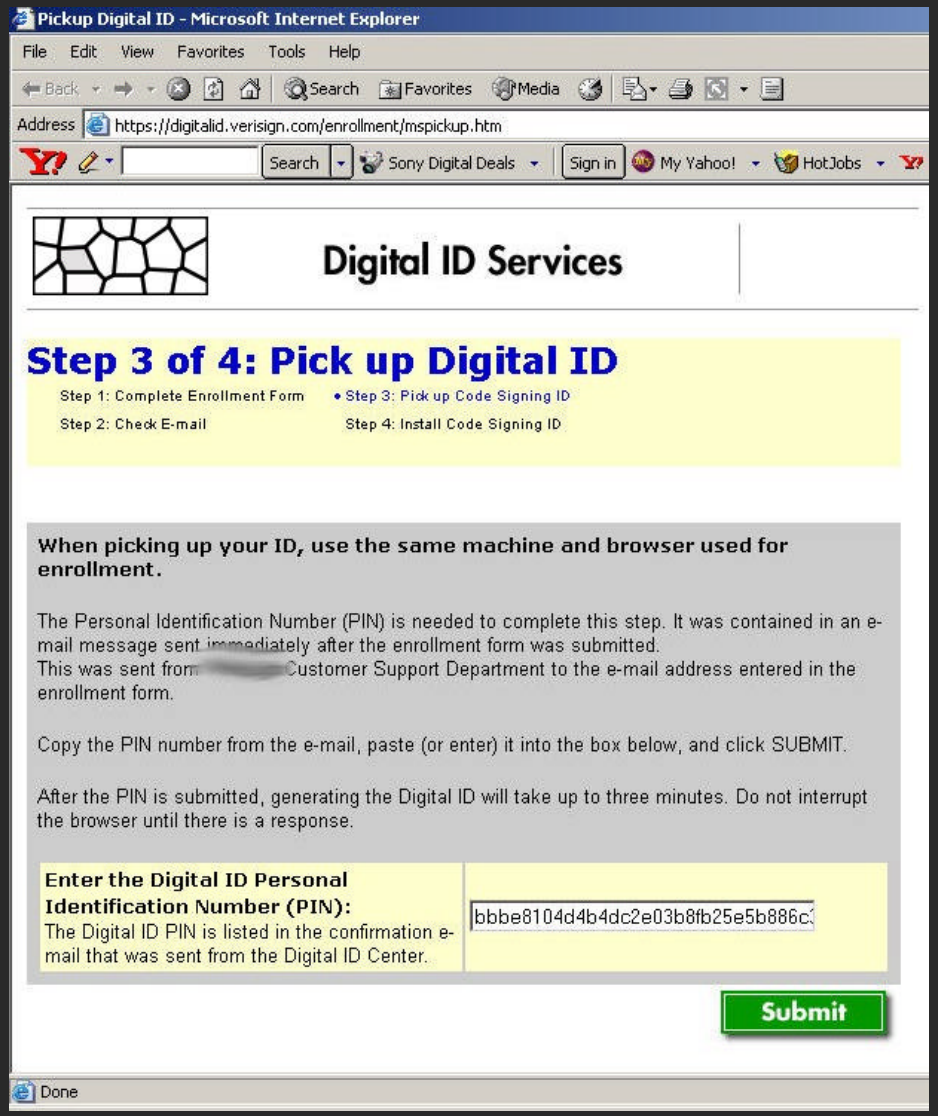
Step 2: Registration



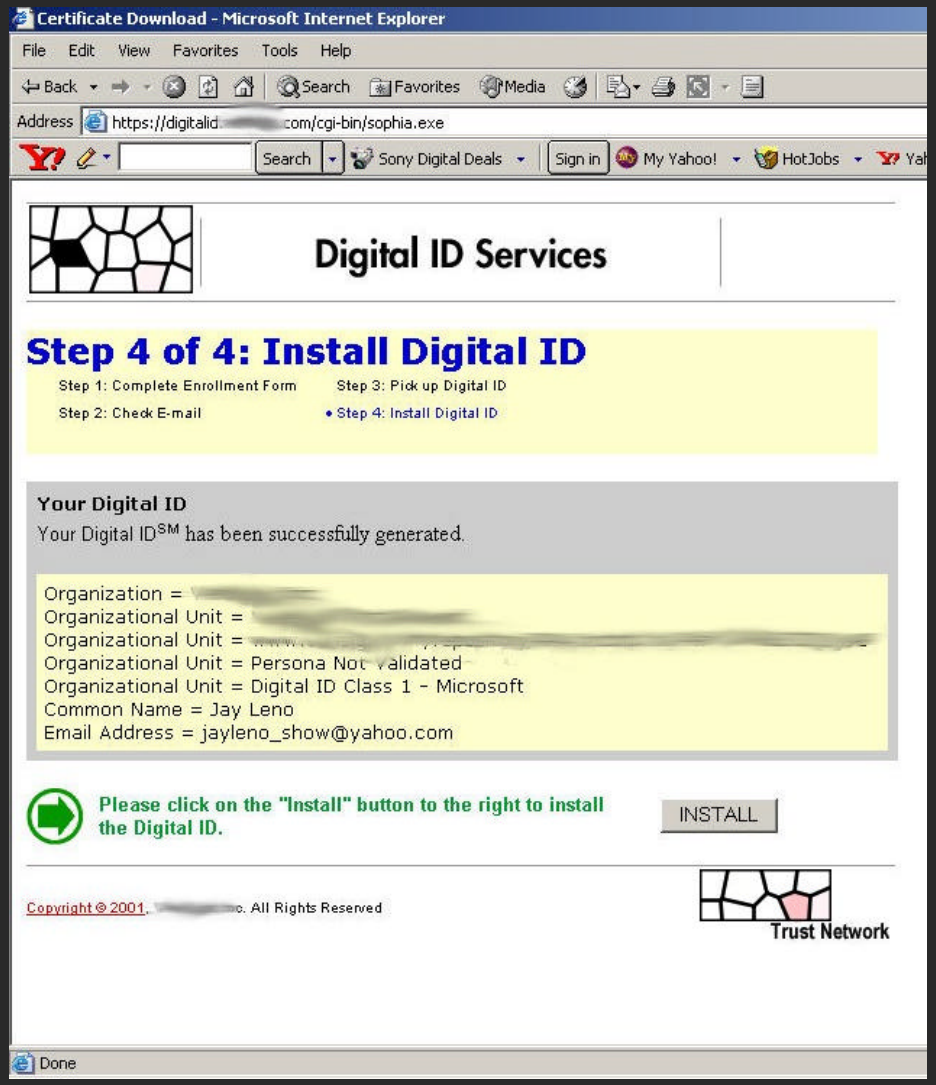
Step 2: Registration



Step 2: Registration

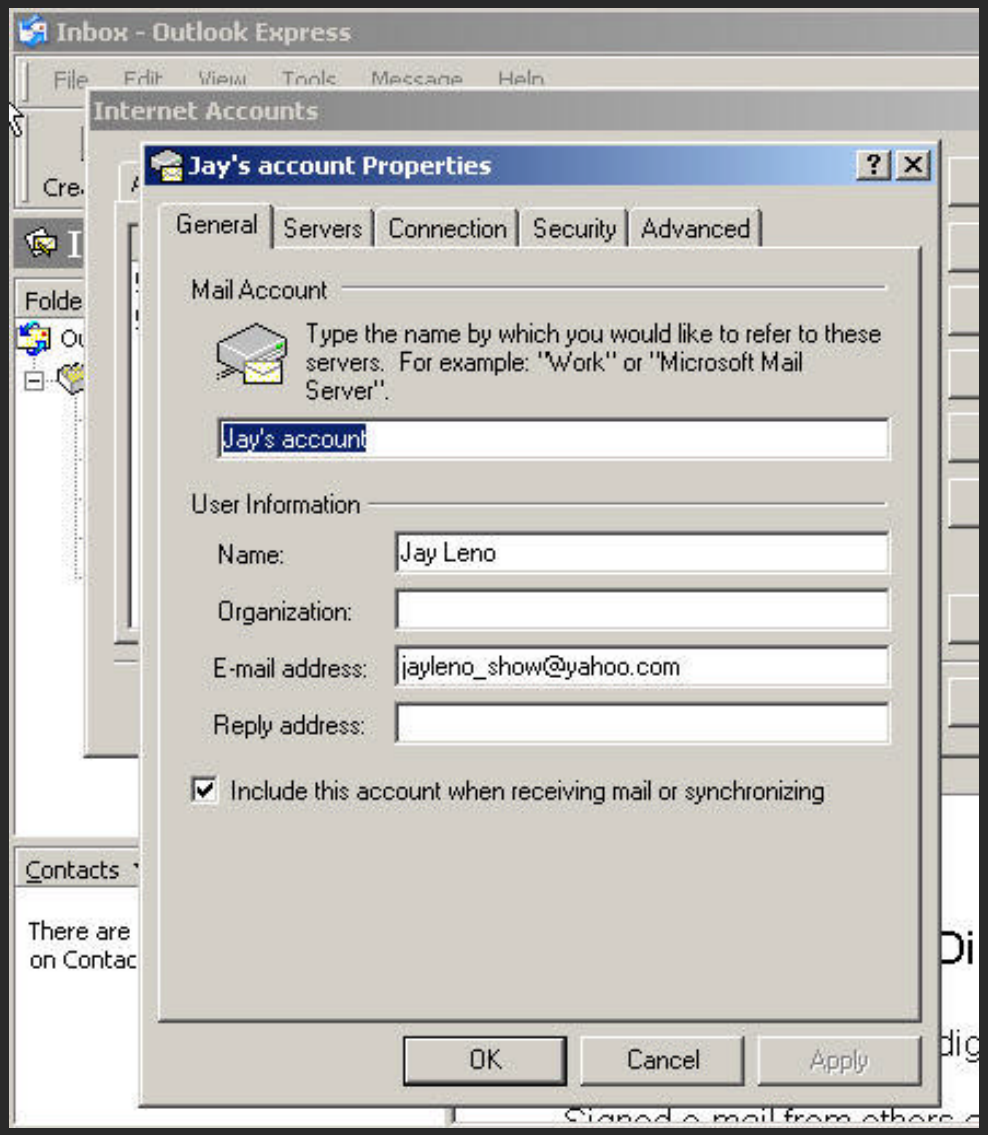


Step 2: Registration

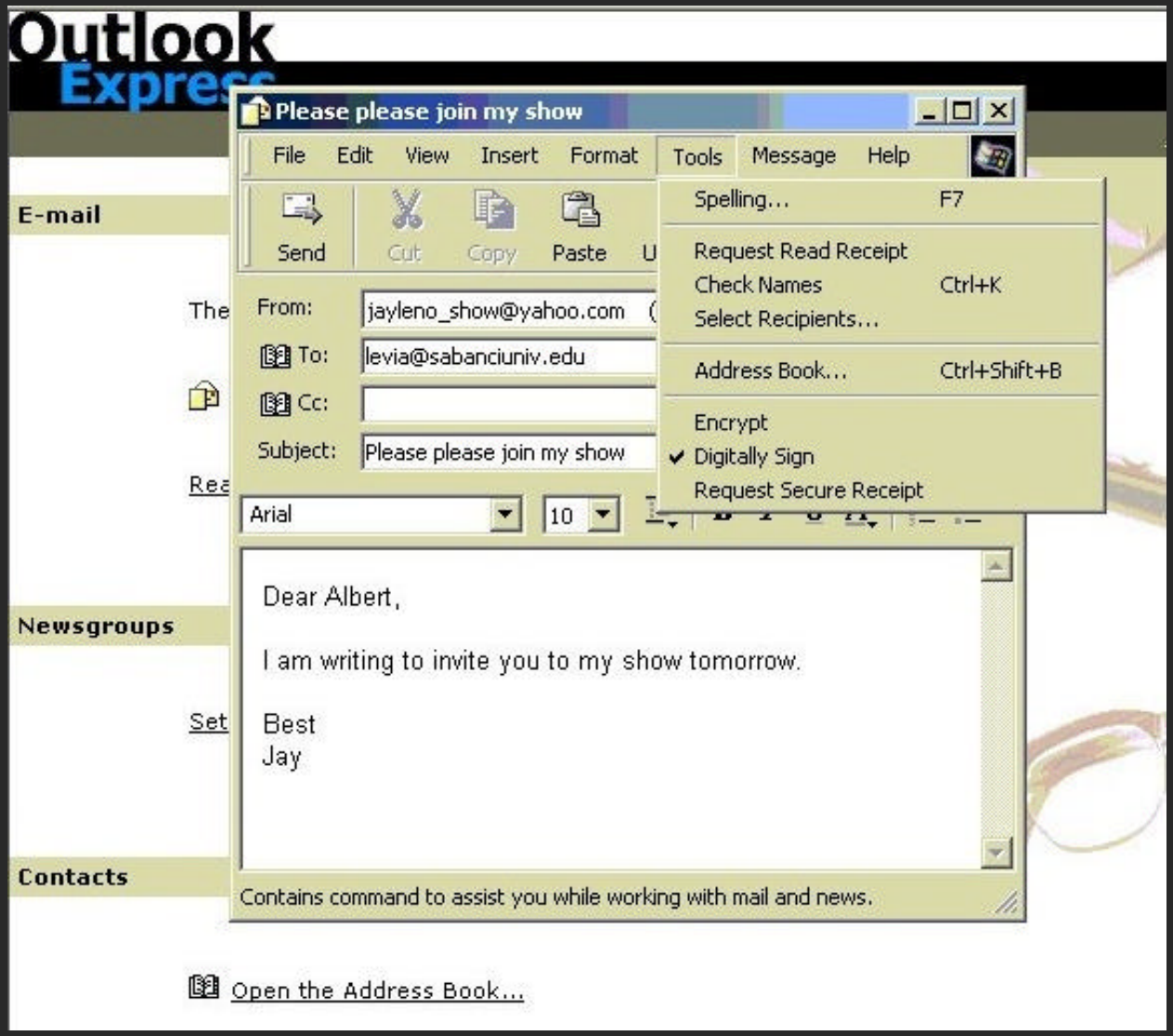


- Certificate is now installed

Step 3: Set up local account



Step 4: Send signed but bogus messages



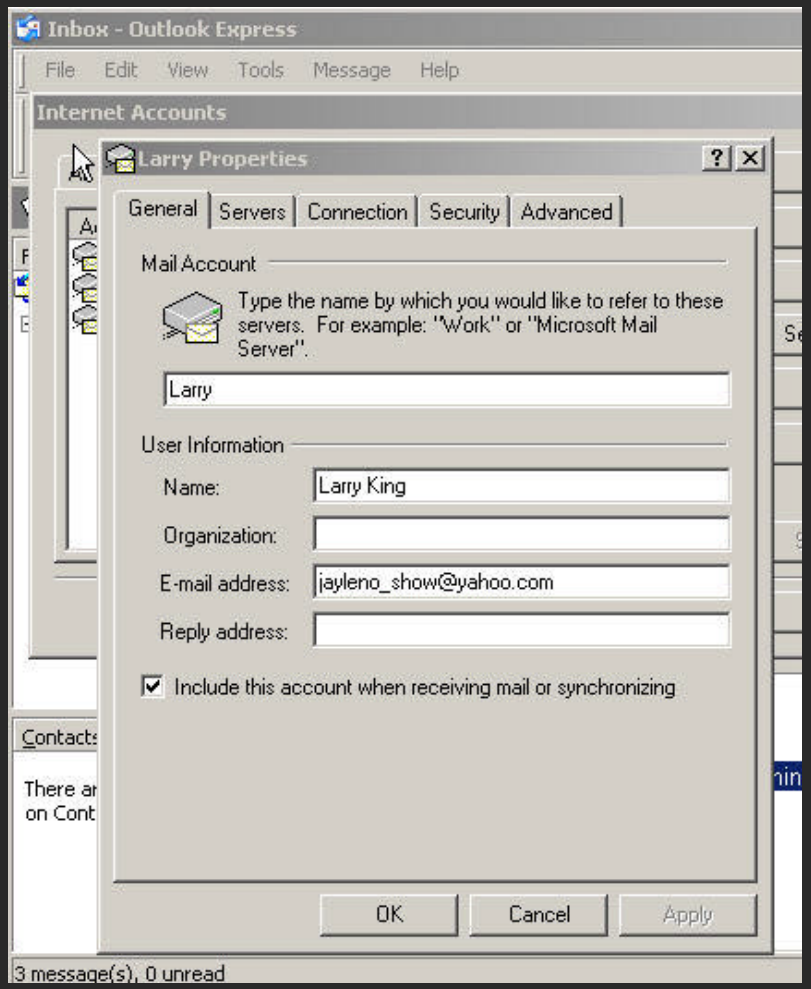
What's Wrong?

- Loose control for Class 1 certificates for commercial reasons
  - visibility
  - market share
- The system becomes less secure for the name of security

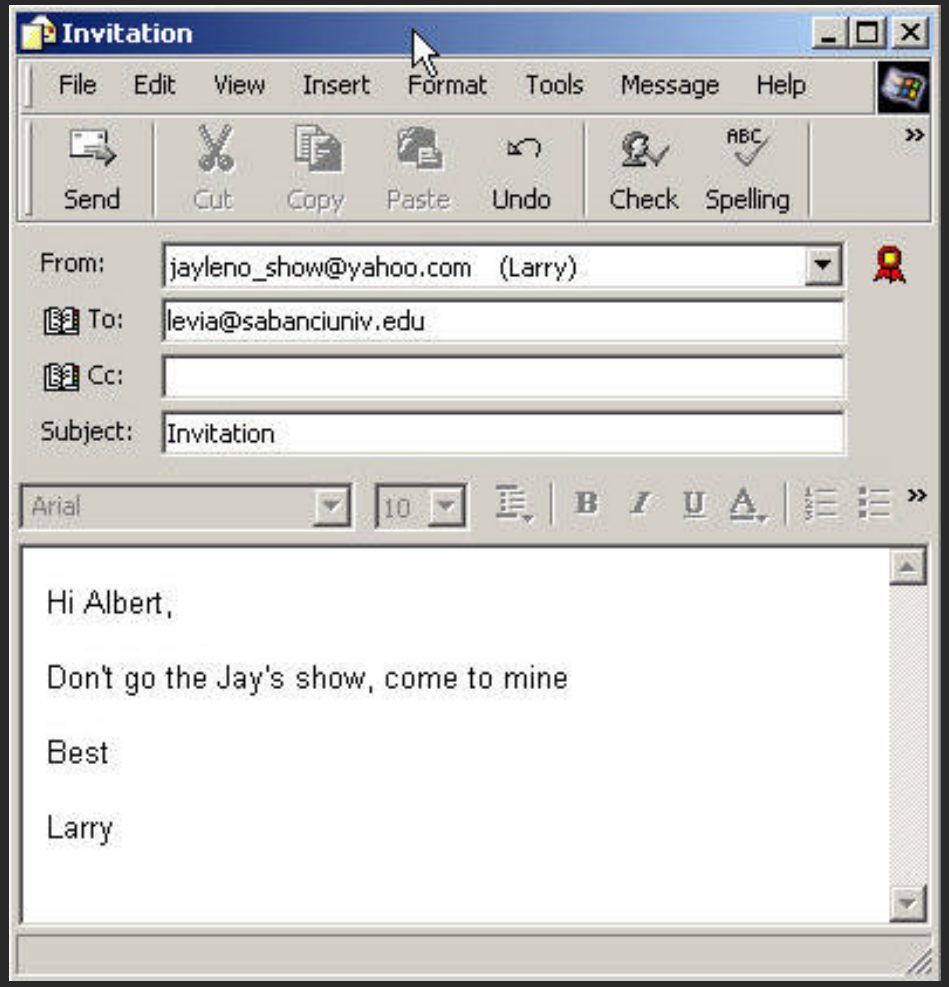
Attack 2: Use one's certificate to send e-mails under another name

- Step 1: Set up another e-mail account at local client
  - Same e-mail address
  - But a different name
- Step 2: Send bogus signed messages

Step 1: Set up another account



Step 2: Send bogus signed message



What's Wrong?

- During verification, e-mail client does not match the name in certificate with the name in e-mail
  - Only e-mail addresses are matched (as mentioned in RFC 2632 (S/MIME Certificate Handling)
- Verifier's manual check is needed
- Not a specific problem of class-1 certificates
  - Same attack is possible using class-2 and class-3 certificates
  - E-mail clients are not concerned with certificate classes

Attack 3: Forging the header

- The scope of a S/MIME signature does not include the e-mail header
  - from, to, cc, subject, date
- RFC 2633

  "S/MIME is used to secure MIME entities. A MIME entity may be a sub- part, sub-parts of a message, or the whole message with all its sub- parts. A MIME entity that is the whole message includes only the MIME headers and MIME body, and does not include the RFC-822 headers."
- Indeed, the mail header is modified without changing the verification status
- Problem of all classes of certificates

Attack 3: Forging the header

- RFC 822 headers resemble envelopes
  - Signature of the letter does not cover the envelope
  - so the signature over the email “message” does not cover the RFC-822 header
  - But we do not write *subject* over the envelopes

What should be done?

- Class 1 certificates should be discontinued
  - All certificate must be issued with a personal presence requirement or by the approval of trusted registration authorities
- E-mail clients must be aware of certificate classes and issue appropriate warnings to the verifiers

What should be done?

- It is up to you whether to believe a digital signature is valid or not
  - Use your reasoning, not your e-mail client's
- Try to identify people by their e-mail addresses
- Examine the details of certificate of the other party
- Do not trust Class 1 certificates
- Ask the sender to put all sensitive information within the message
  - Sender's identity
  - Subject
  - Date
- Don't let subject say all!