Web Security Challenges

World Wide Web Conference 2006

Thomas Roessler, W3C
tlr@w3.org

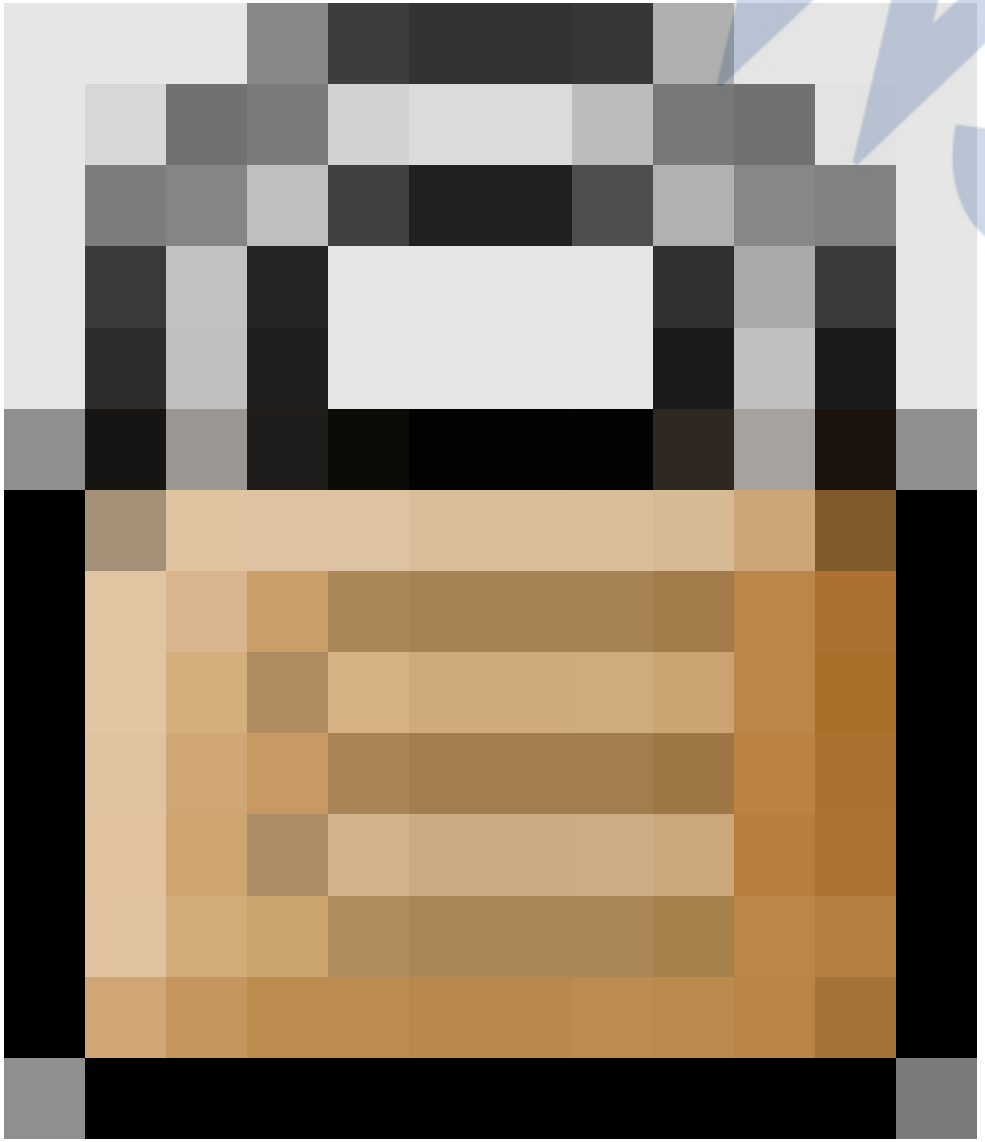
Overview

- Digression: XML Signature Authentication, Usability, and the Web
  Thomas Roessler, W3C
- Security Requirements for the Ubiquitous Web
  Dave Raggett, W3C
- Access Control, P.I.
  ~~*Charles McCathie Nevile, Opera*~~
  Thomas Roessler, W3C

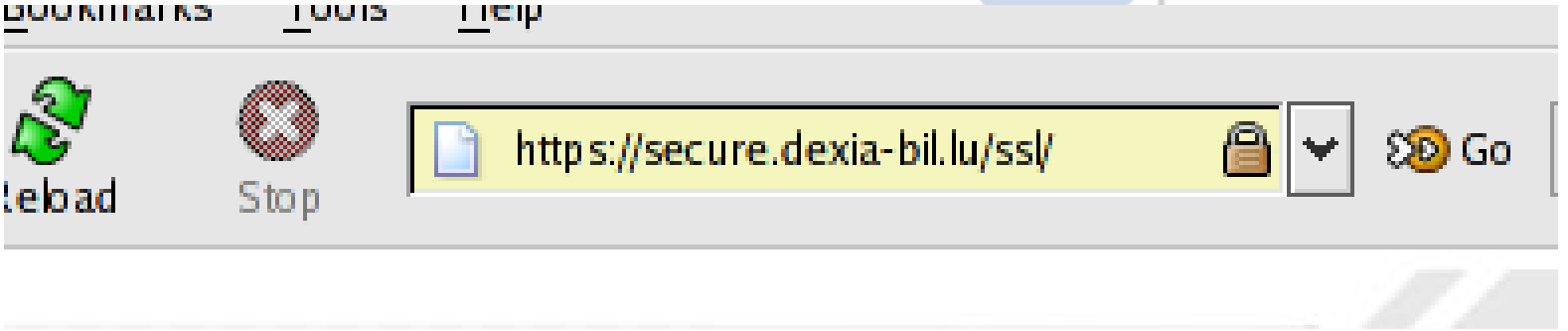
Digression: XML Signature

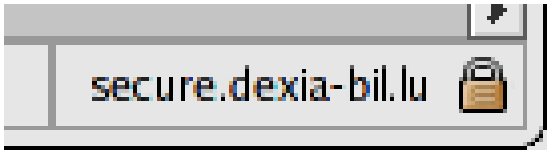
- XML Signature is coming of age.
- XML Canonicalization (C14N) has known issues.
  - xml:id – oops
  - xml:base – oops(2)
  - XML Core WG currently preparing C14N 1.1
- We're in listening mode about what the next steps should be for XML Signature.

Web Authentication Today: A padlock means “secure.”



This is a padlock.

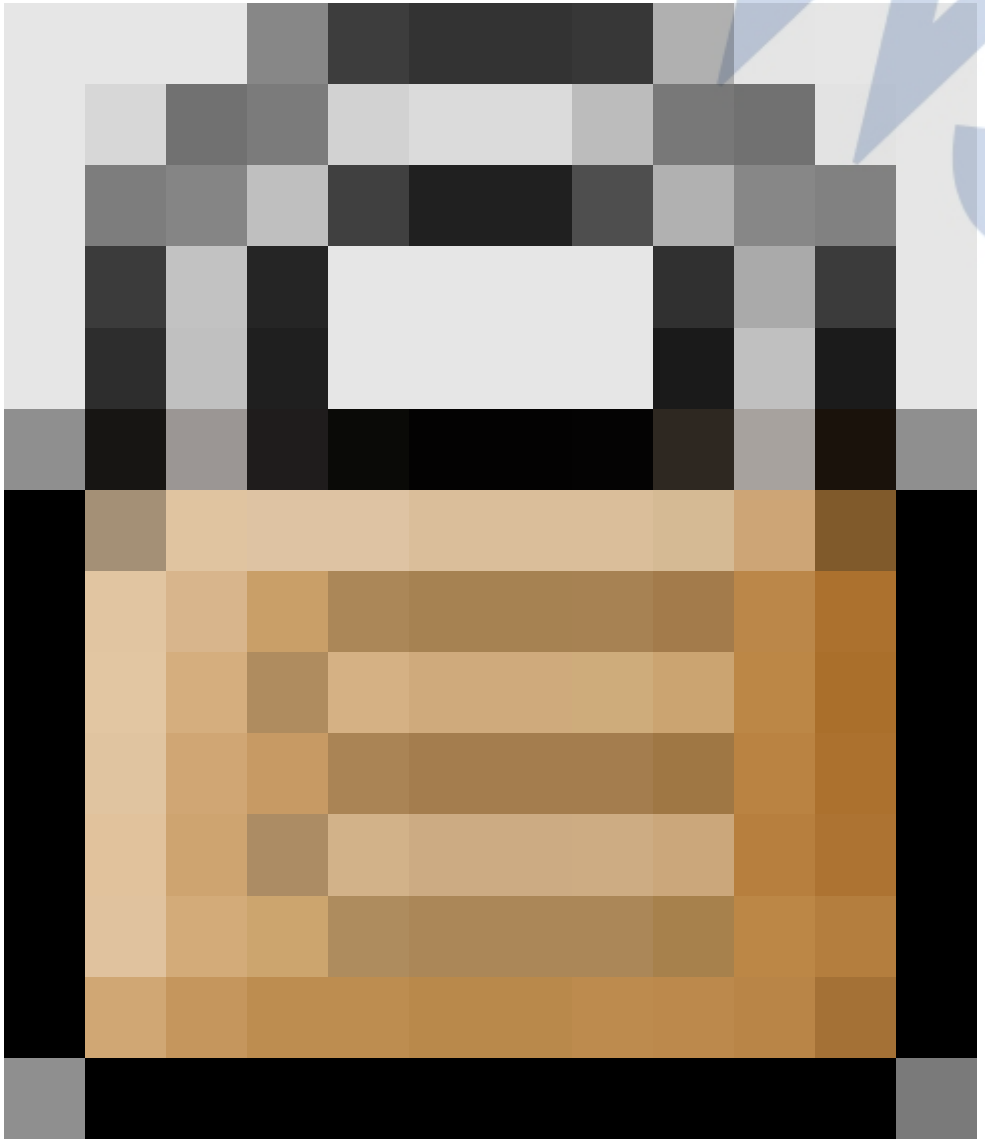




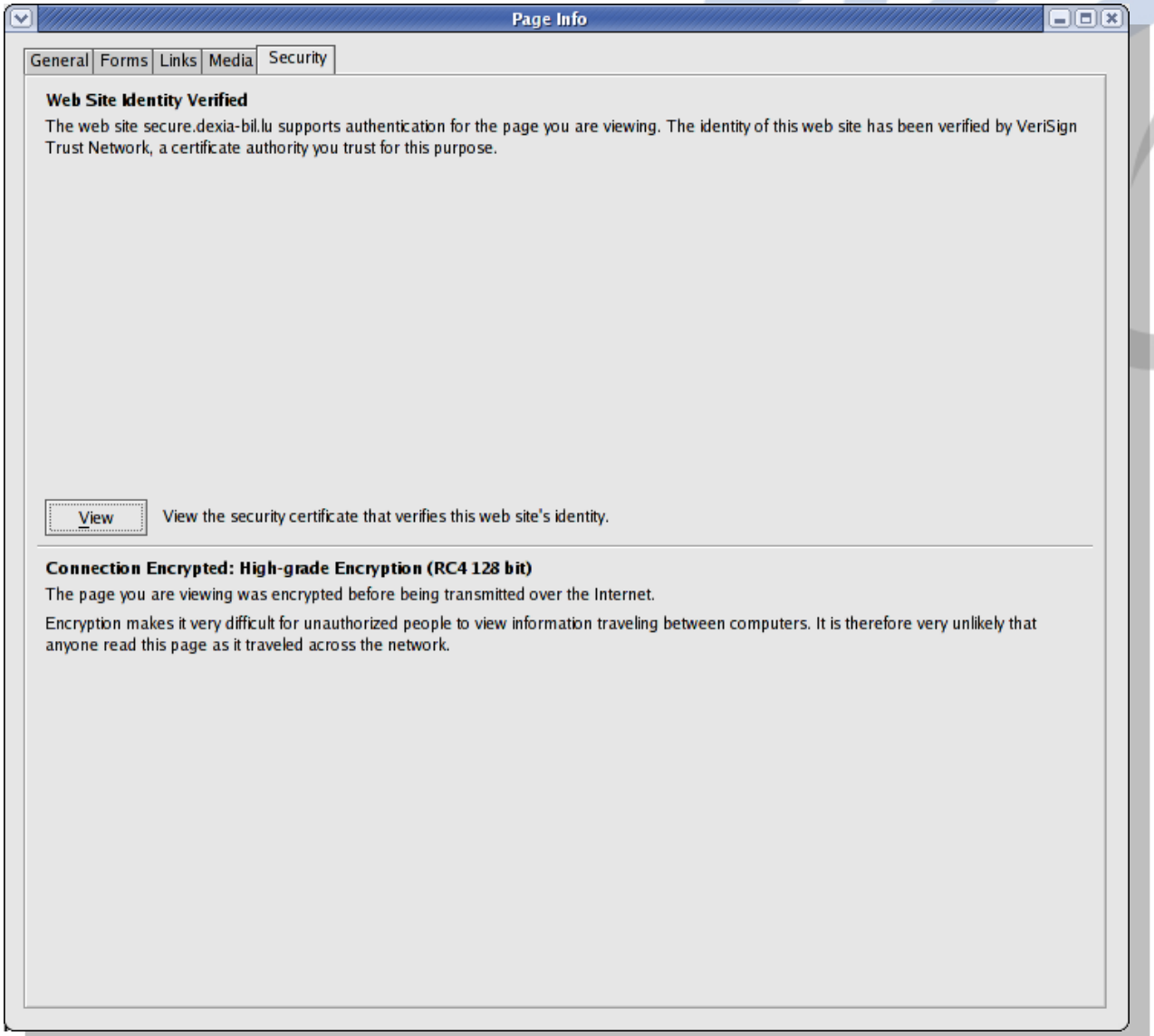
This is not a padlock.

From a recent phishing attack. The attacker's site was, like the original, serving the form using plain HTTP.

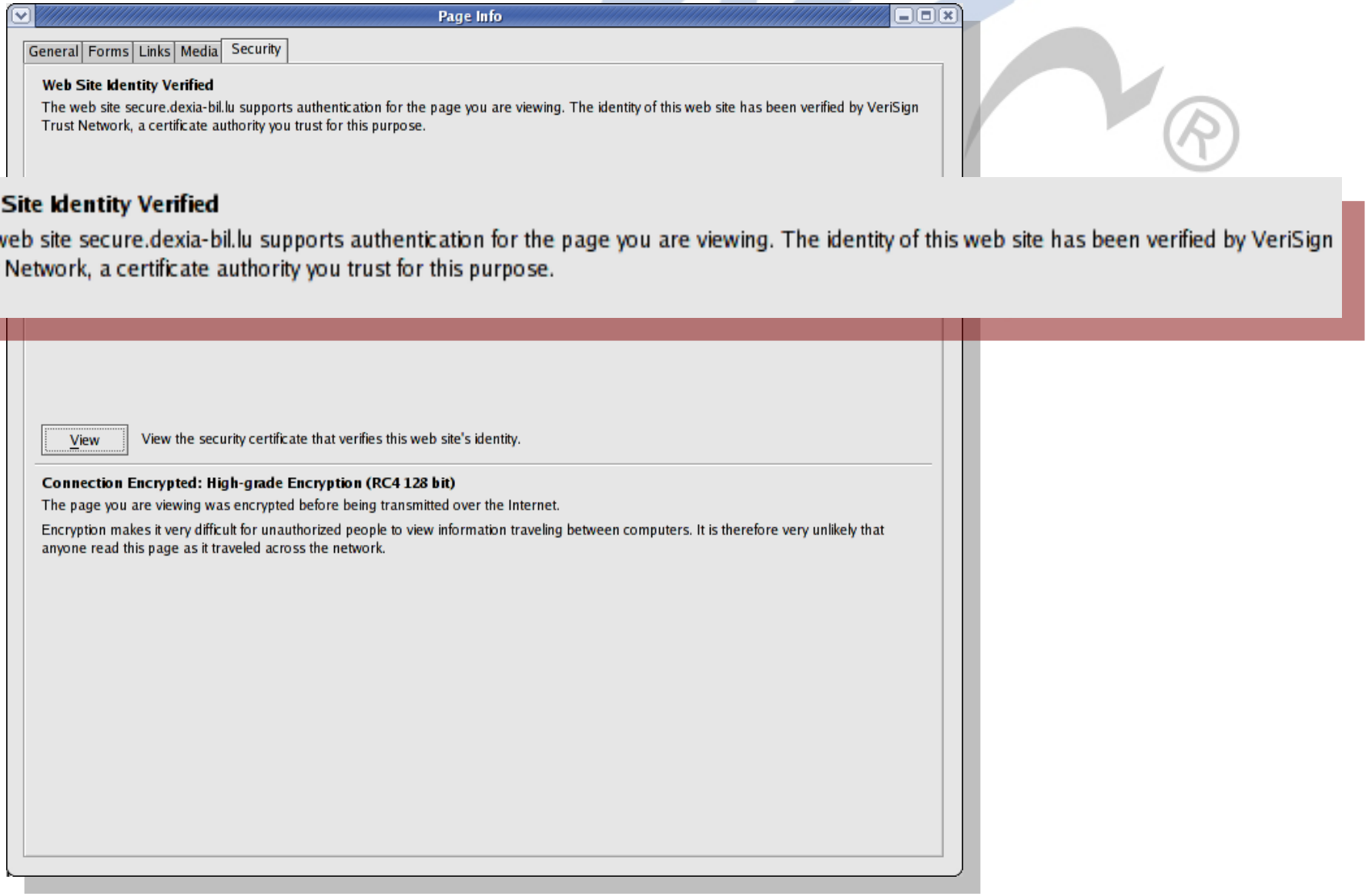
A padlock means “secure.” Not.



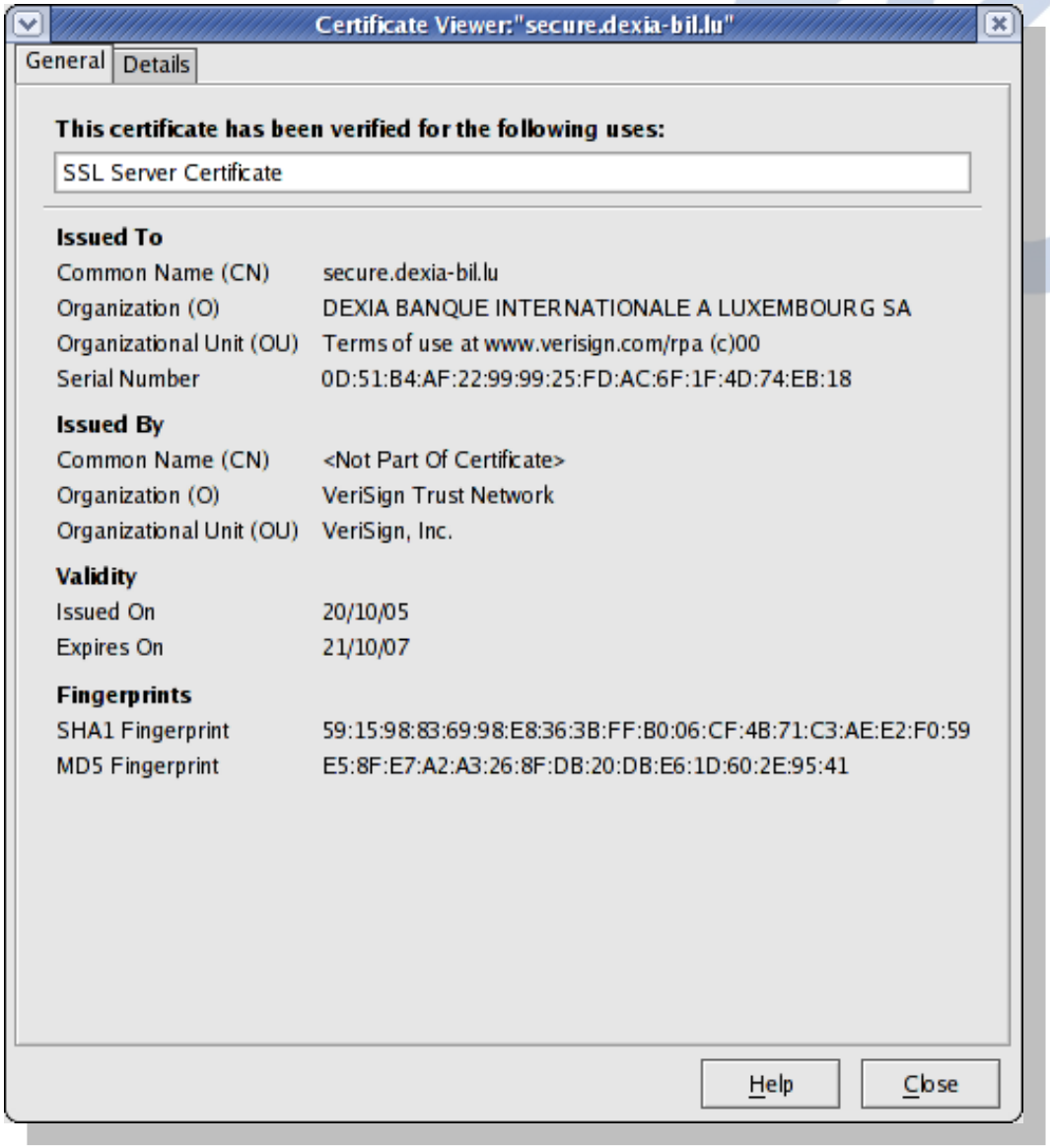
Better don't click on the padlock, or else...



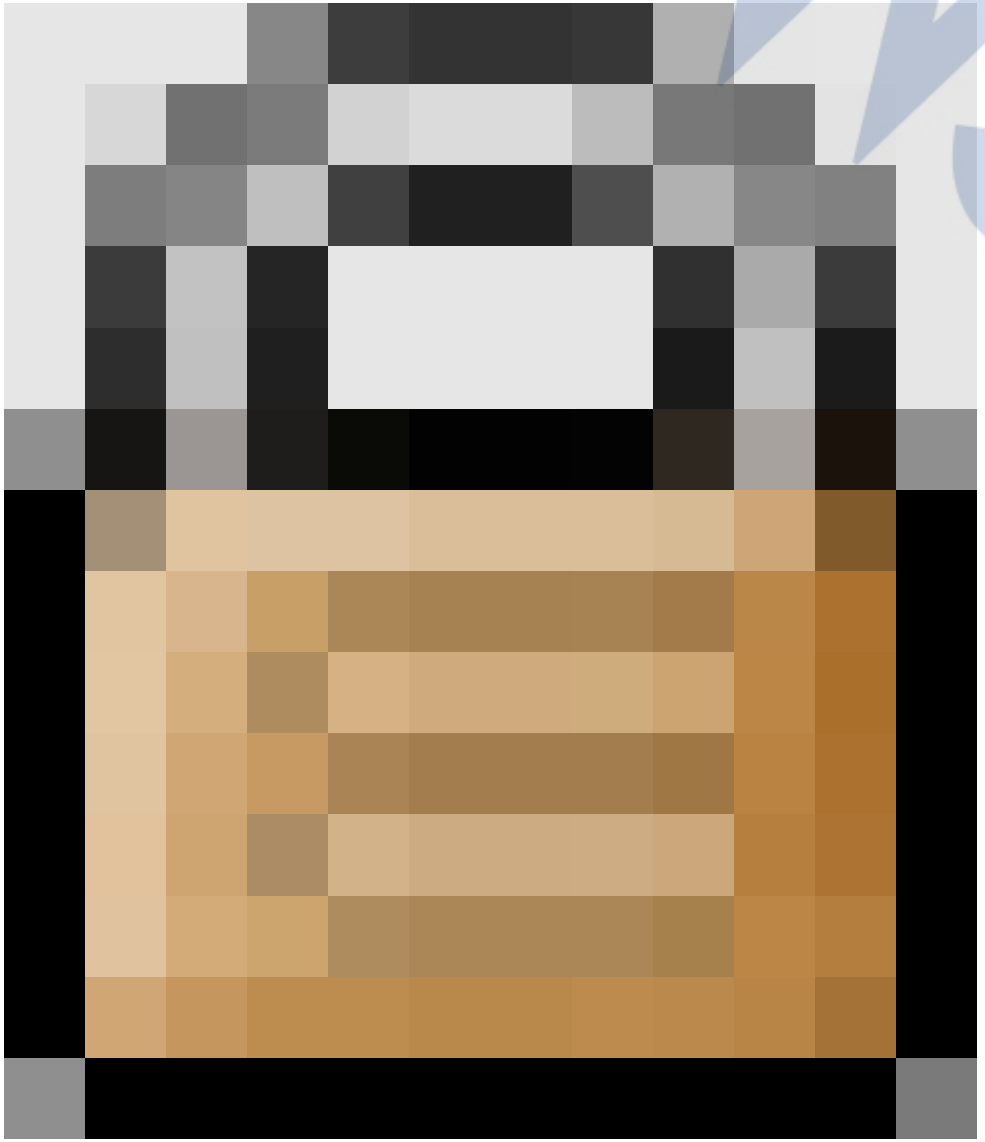
Better don't click on the padlock, or else...



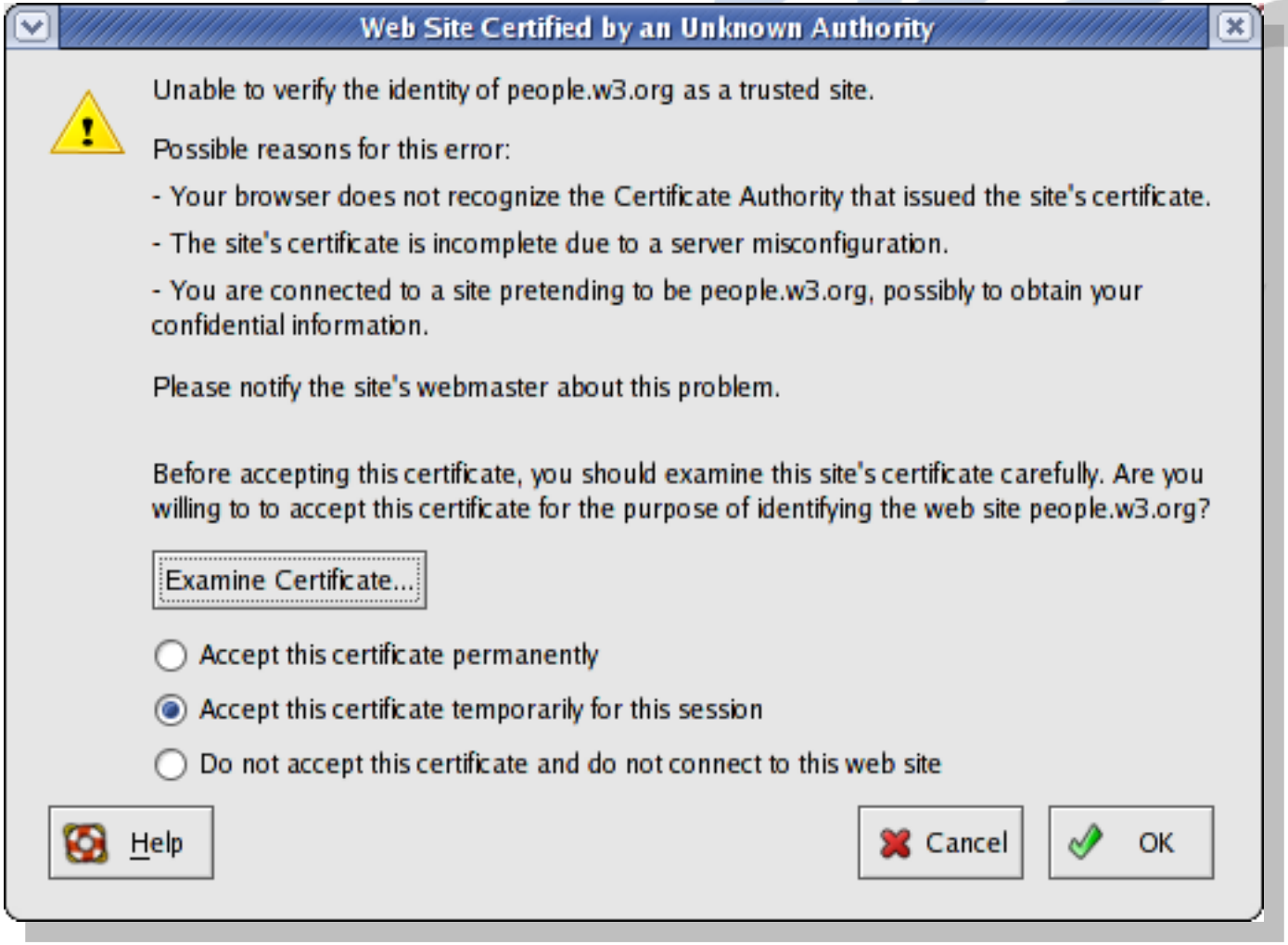
Better don't click on “View”, either



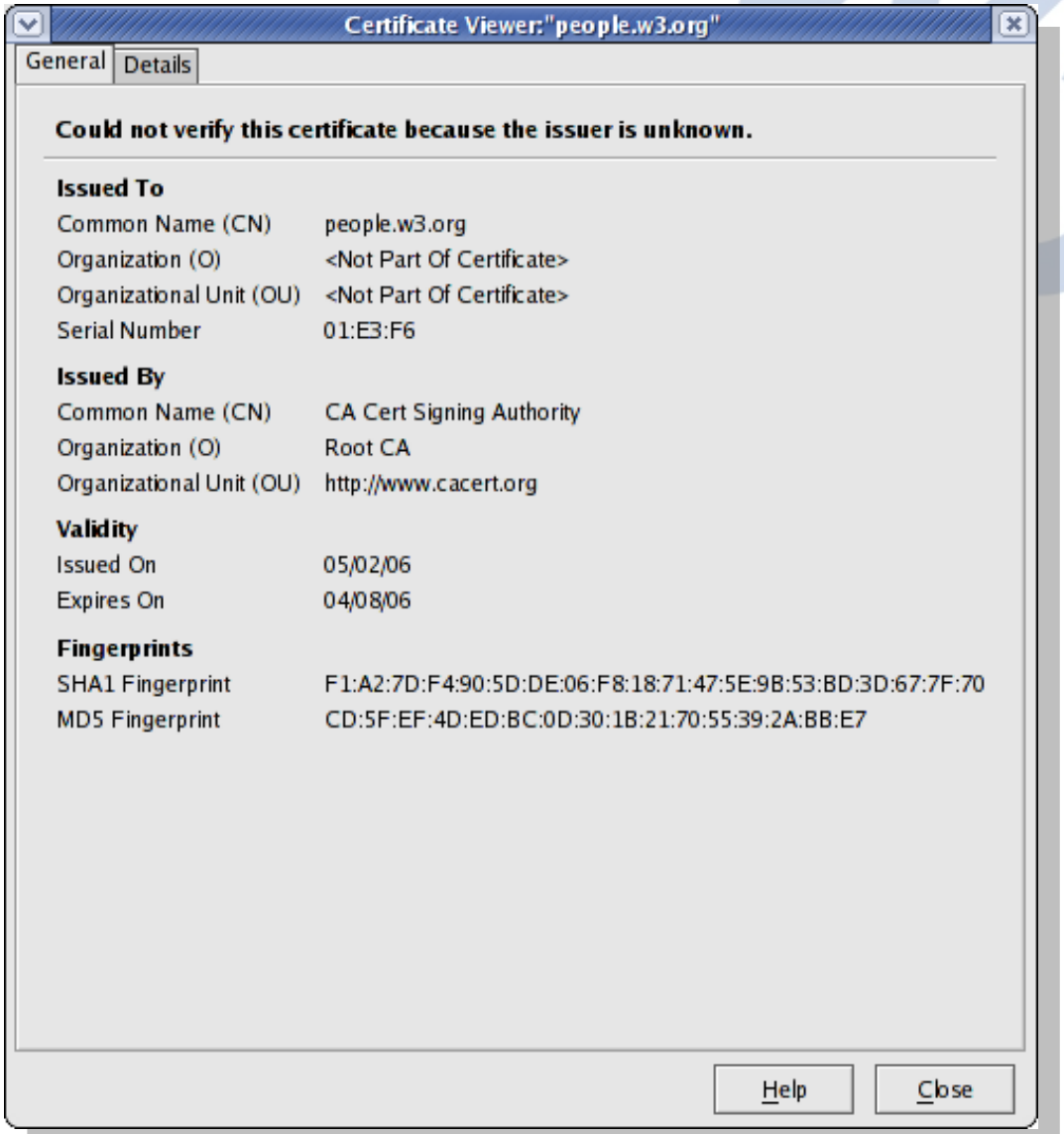
A padlock means “secure.” Not.



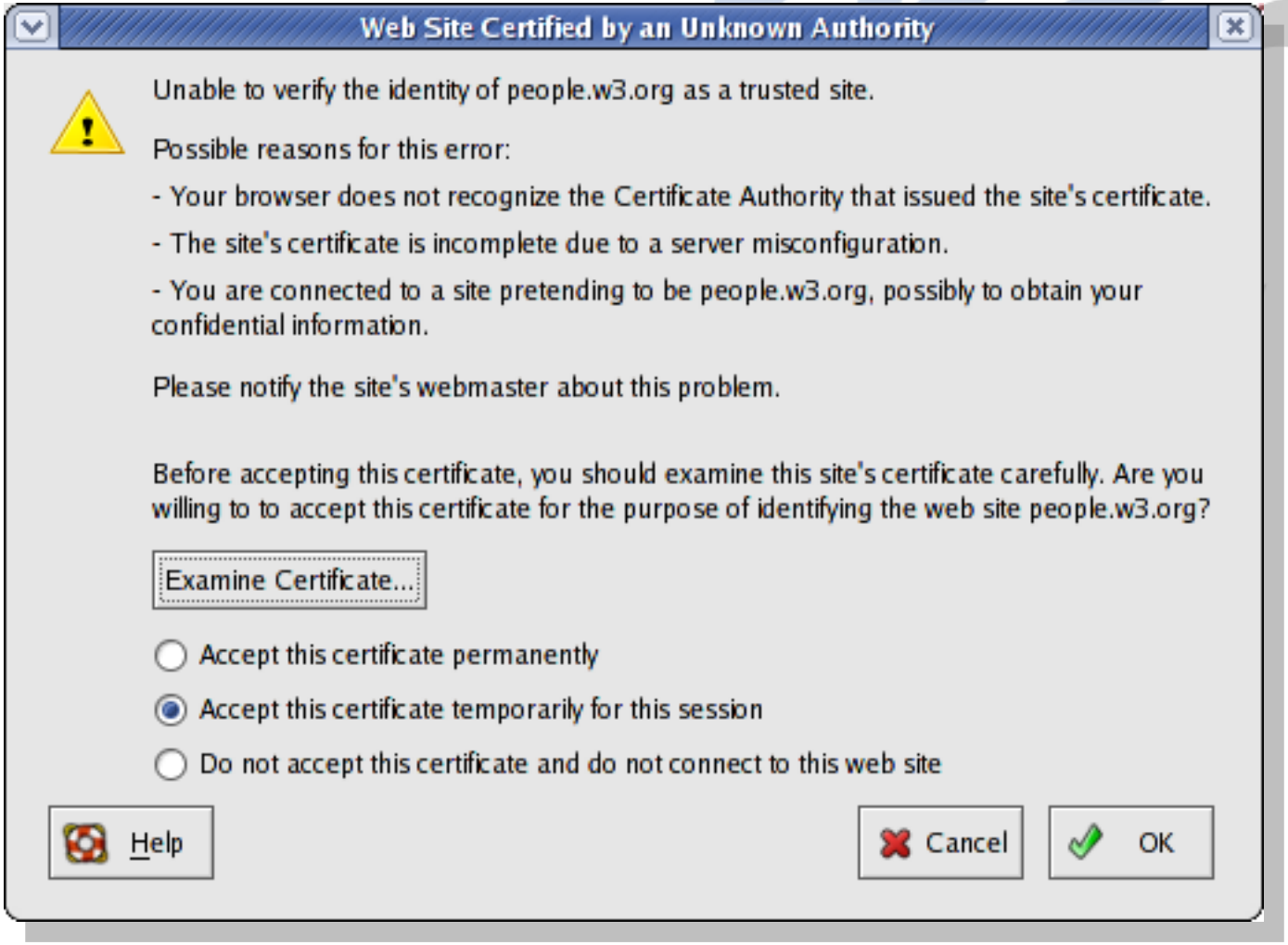
But it gets worse...



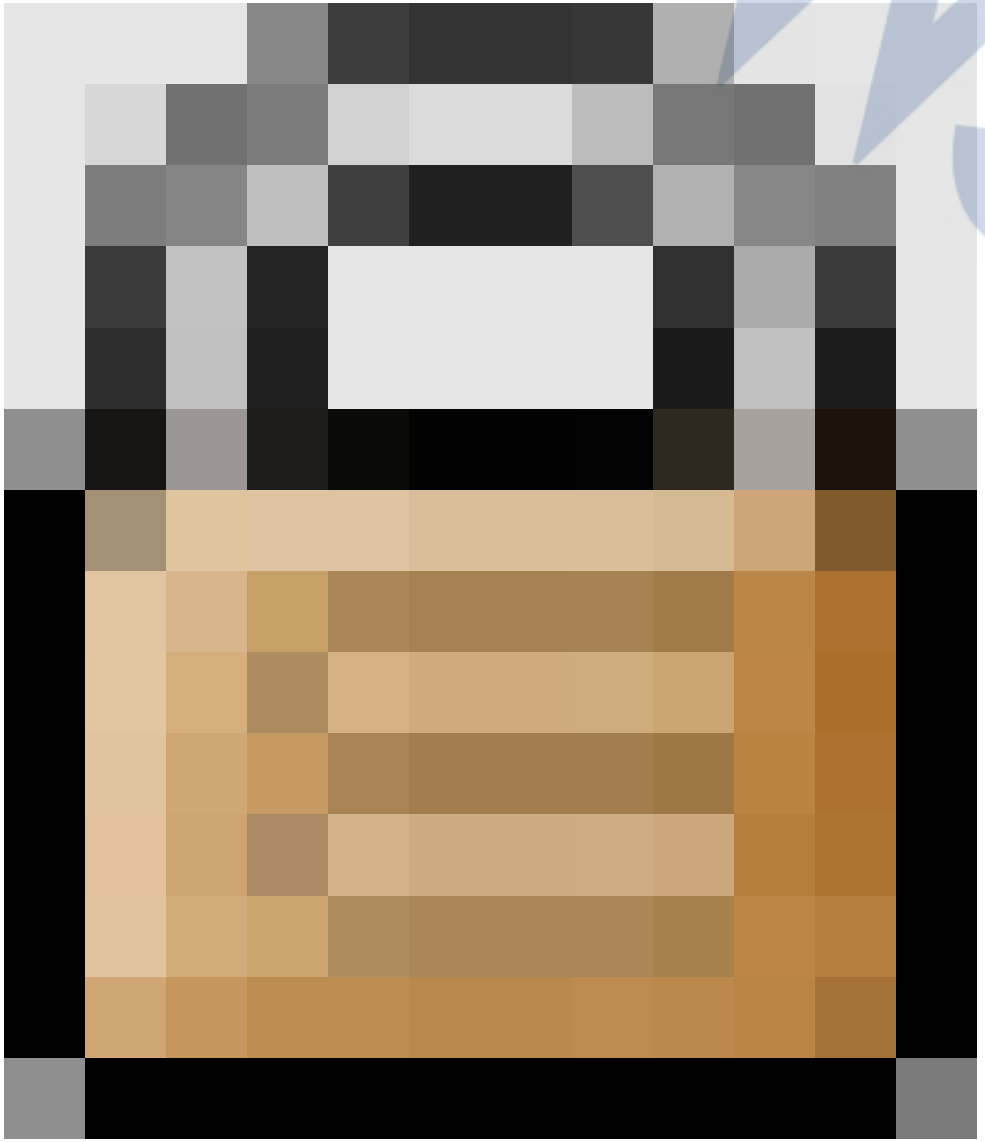
“Examine”


Certificate Viewer:"people.w3.org"
General
Details
Could not verify this certificate because the issuer is unknown.
Issued To
Common Name (CN) people.w3.org
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 01:E3:F6
Issued By
Common Name (CN) CA Cert Signing Authority
Organization (O) Root CA
Organizational Unit (OU) http://www.cacert.org
Validity
Issued On 05/02/06
Expires On 04/08/06
Fingerprints
SHA1 Fingerprint F1:A2:7D:F4:90:5D:DE:06:F8:18:71:47:5E:9B:53:BD:3D:67:7F:70
MD5 Fingerprint CD:5F:EF:4D:ED:BC:0D:30:1B:21:70:55:39:2A:BB:E7
Help
Close

Or the user could go with the default...



A padlock means “secure.” Not.



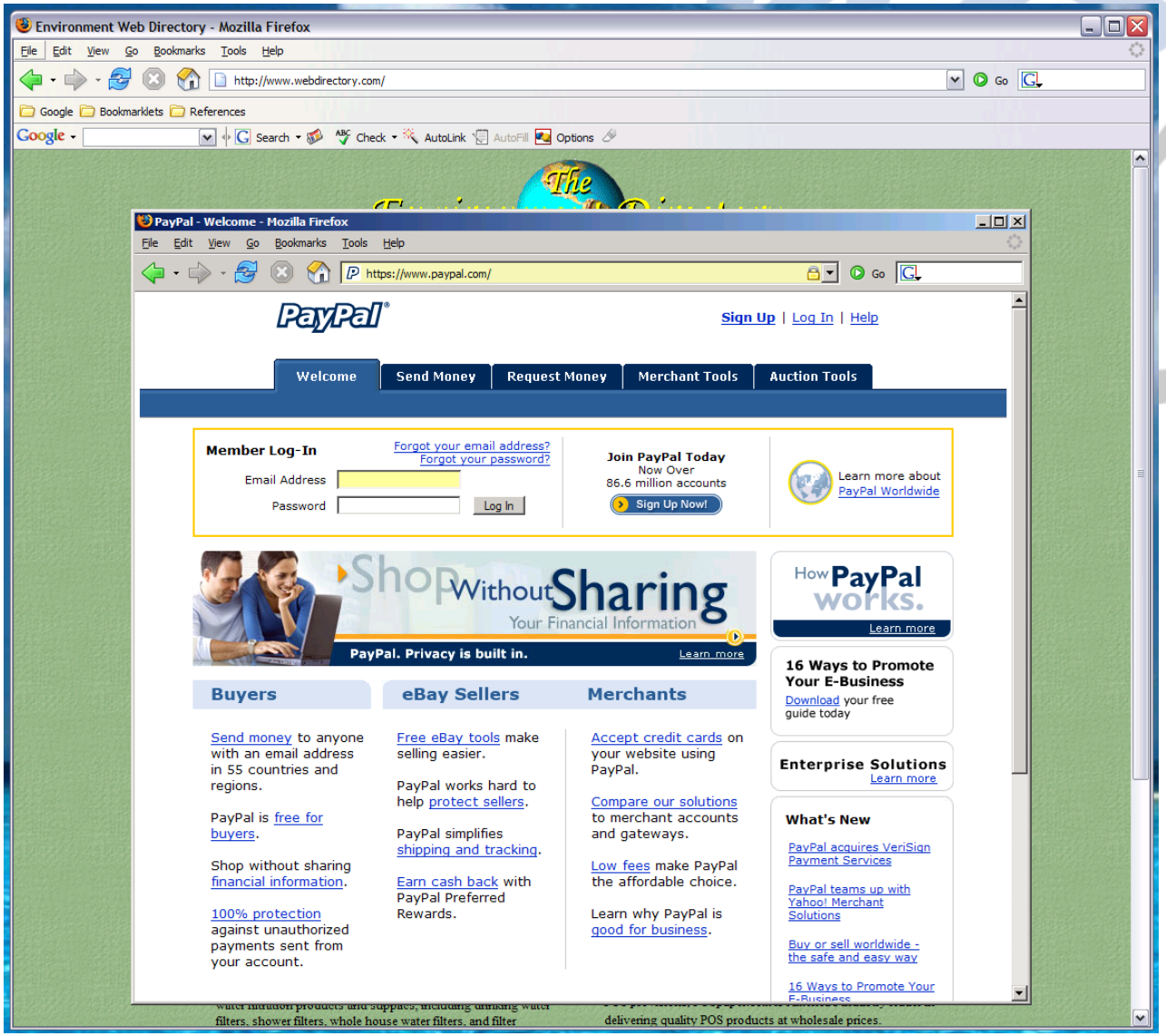
Can we do better than this?

- The padlock doesn't make sense.
- X.509 certificates are technical gibberish.
- Current implementation doesn't even help suspicious users.
- Can we make Web authentication more usable?
- 15/16 March: Workshop in NYC
  - 41 position papers, 60 participants, 23 presentations
  - banks, browser & security vendors, academics, content providers

Workshop Results
Secure Chrome & Secure Metadata

- Show different stuff to users
  - logos?
  - “this is a bank site”? “verified by ***”?
- Show it safely
  - The part of the user interface that displays metadata must be protected from faking through mark-up and scripting.
  - Restrict browsers' abilities.
  - Specific security mode?

Which one is the browser?



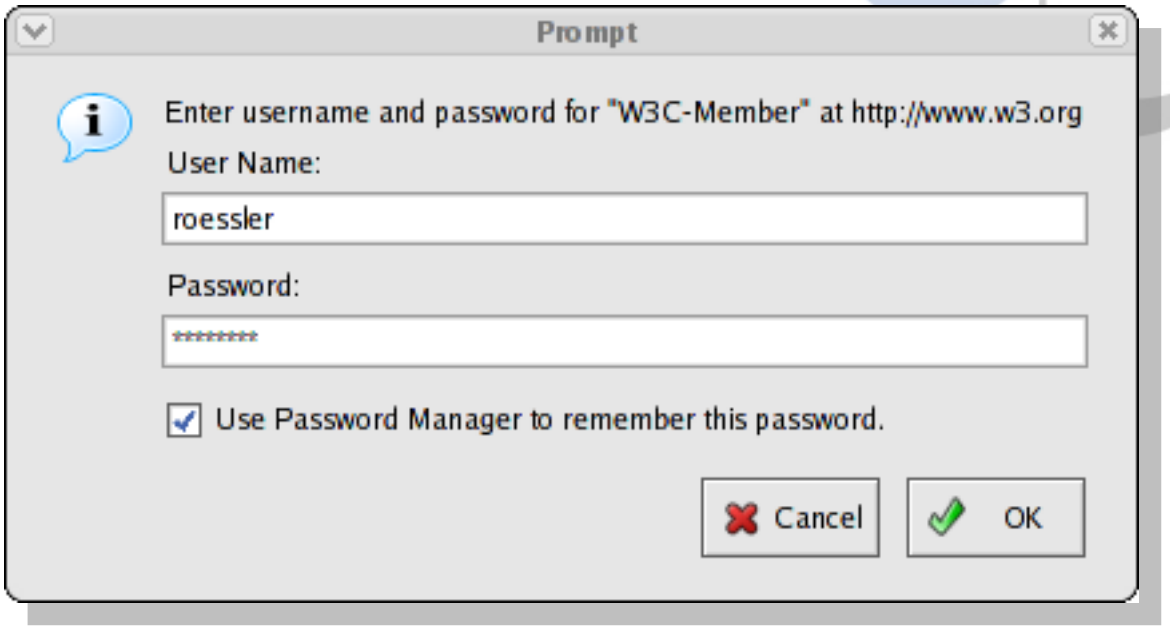
From: http://www.w3.org/2005/Security/usability-ws/presentations/37-google

What can W3C do here?

- Enable browser vendors to restrict functionality in a concerted way.
- Enable content providers to connect security features to their brands.
- Specify data to be displayed.
  - could be “please use the logoType extension”
  - could be more complex than that – think content labels

Forms and authentication

- HTTP authentication isn't used widely



Forms and authentication

- HTML forms, POST and Cookies are the state of the art

HTML Forms and HTTP Authentication

- If user agents could recognize that an HTML form is used for credentials....
  - user agents could manage credentials, reliably
  - user agents could give the current user interfaces and combine them with HTTP-level authentication
  - user agents could trigger intelligent user interface behaviour – this could be a hook for login rituals
- New tags v. microformats / annotations?

Where do we go from here?

- Next step: charter draft(s).
- Please join the discussion:
  http://lists.w3.org/Archives/Public/public-usable-authentication/
- Nearby:
  - IETF is discussing possible future developments on HTTP authentication
  - Online Identity (dix, Infocard, OpenID, ...)