


# *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*

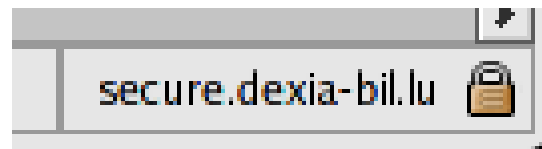
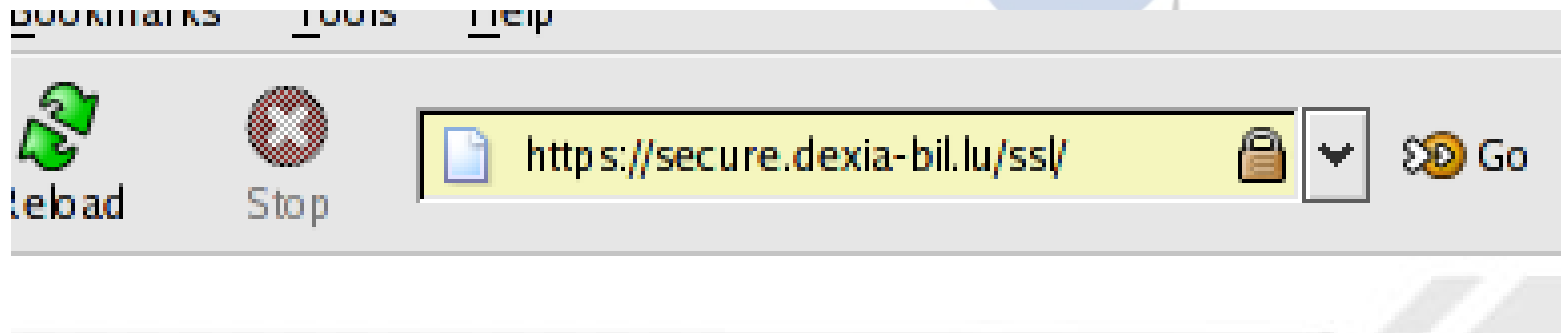
# Digression: XML Signature

- 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.



RegionsNet® Login ▲

Login ID: Password:

 Secure Login

RegionsNet Online Banking:

[Learn More](#) | [Demo](#) | [Enroll](#)  
[Agreement & Disclosure](#)

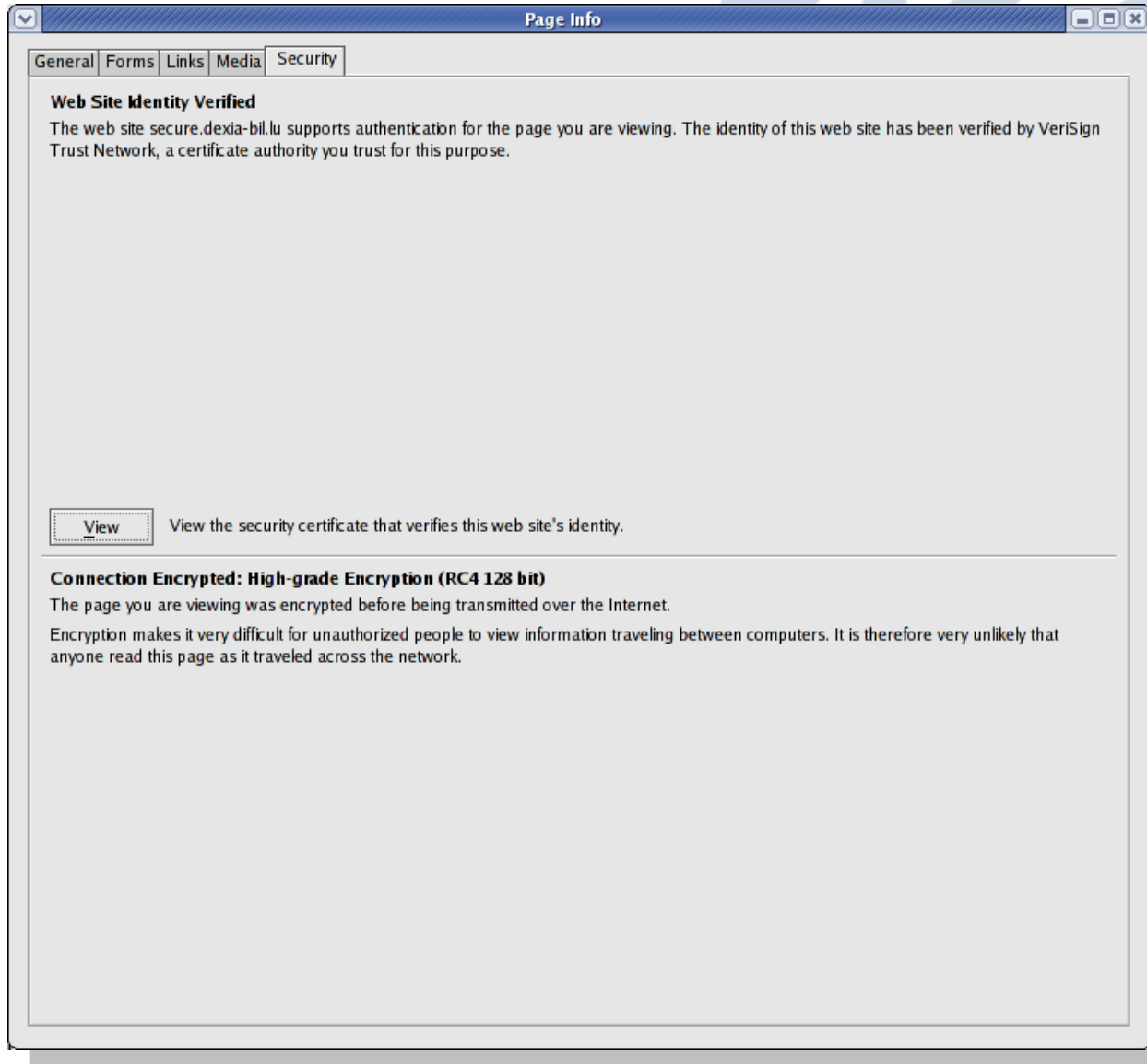
Other Online Services:

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

A padlock means “secure.” Not.

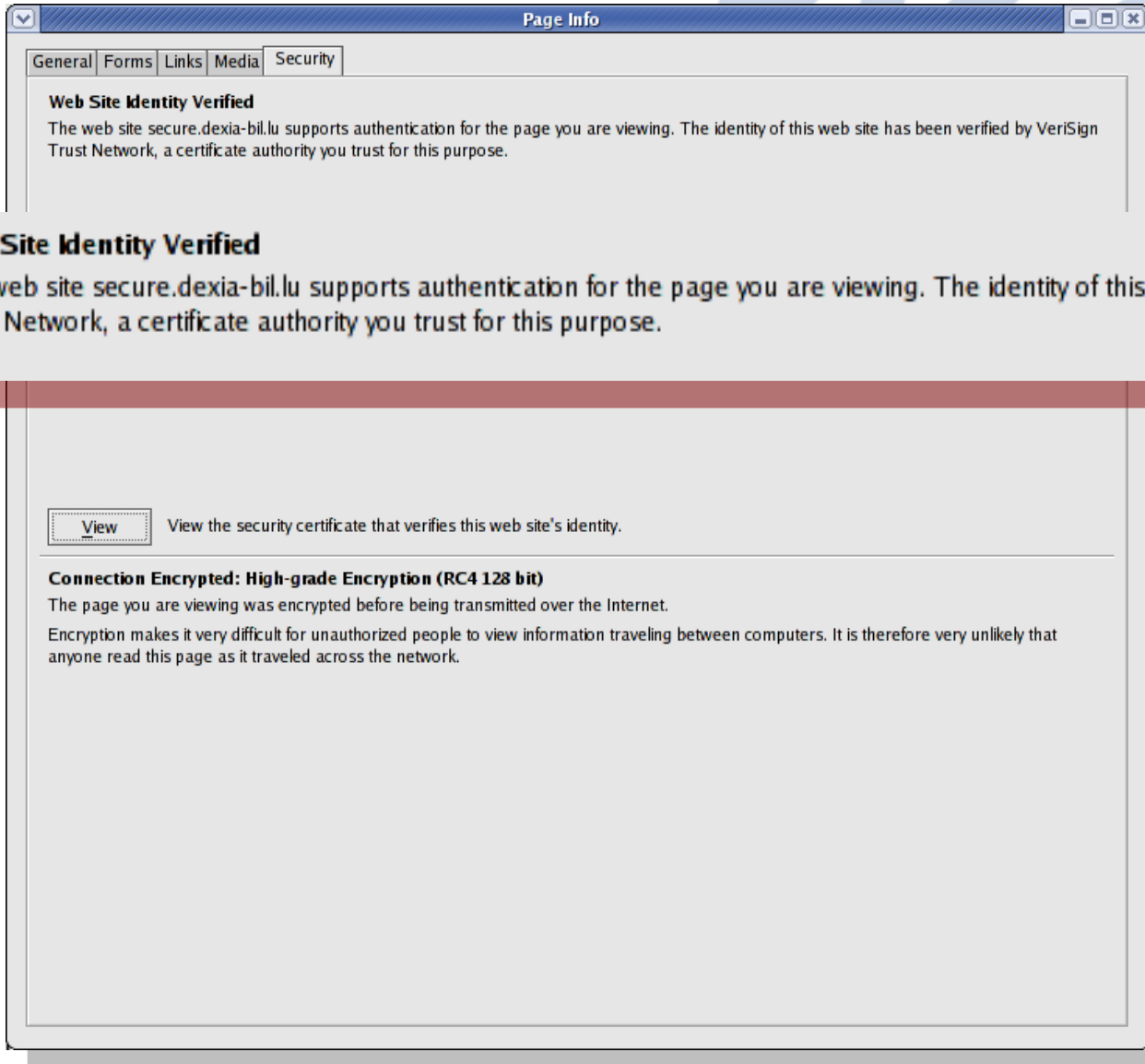


# Better don't click on the padlock, or else...





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



## Web Site Identity Verified

The web site secure.dexia-bil.lu supports authentication for the page you are viewing. The identity of this web site has been verified by VeriSign Trust Network, a certificate authority you trust for this purpose.

View

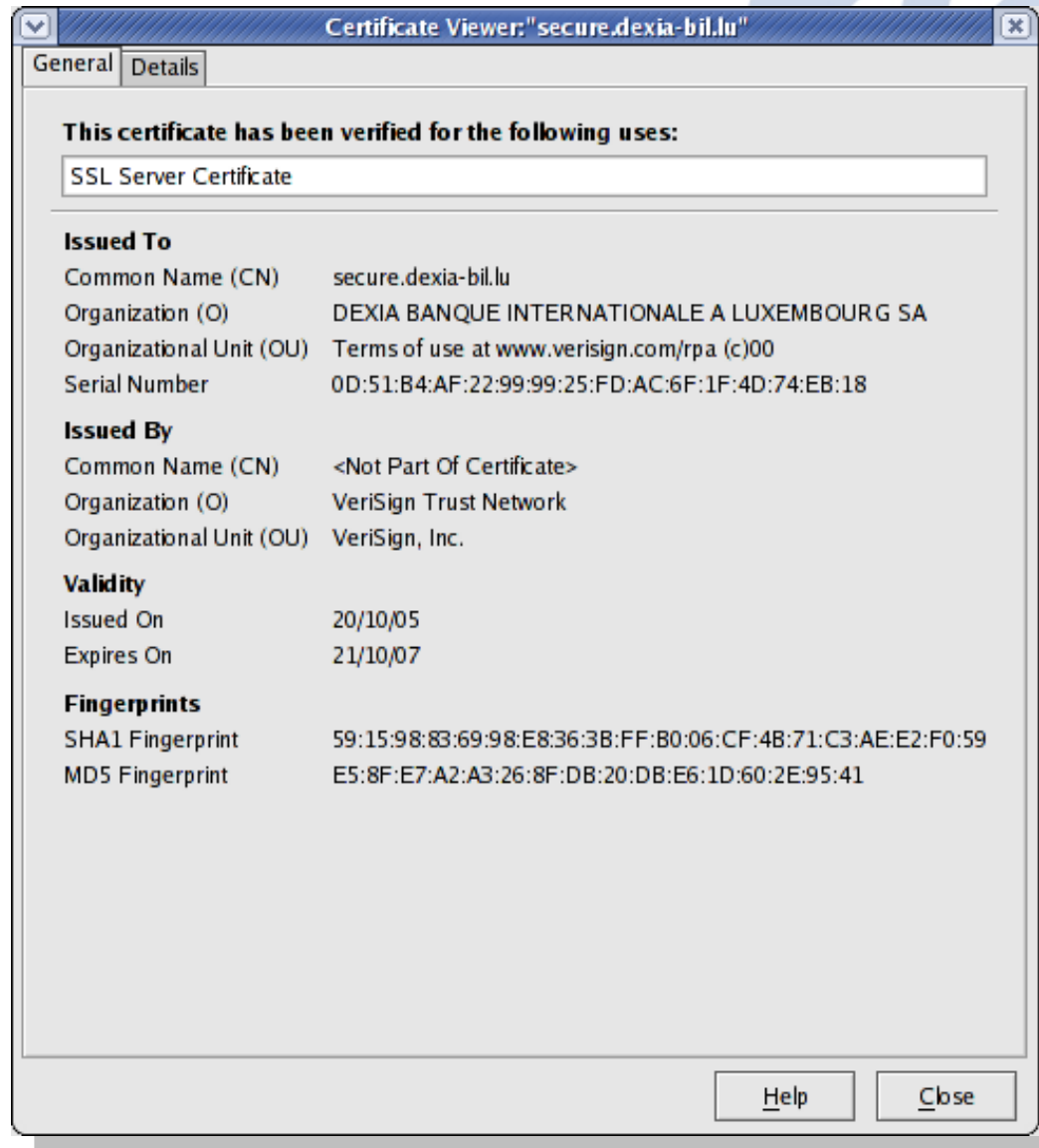
View the security certificate that verifies this web site's identity.

### Connection Encrypted: High-grade Encryption (RC4 128 bit)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

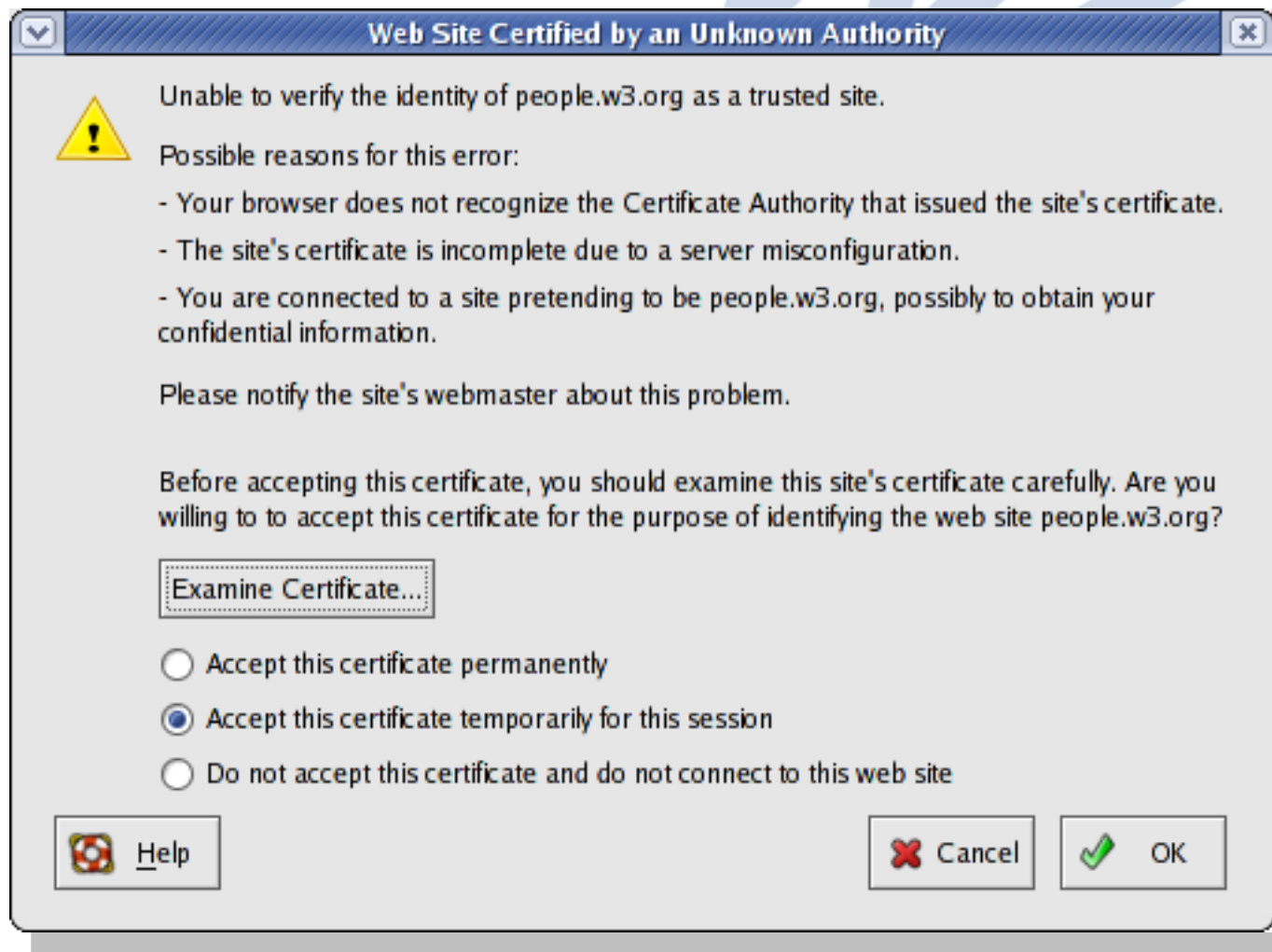
# Better don't click on “View”, either



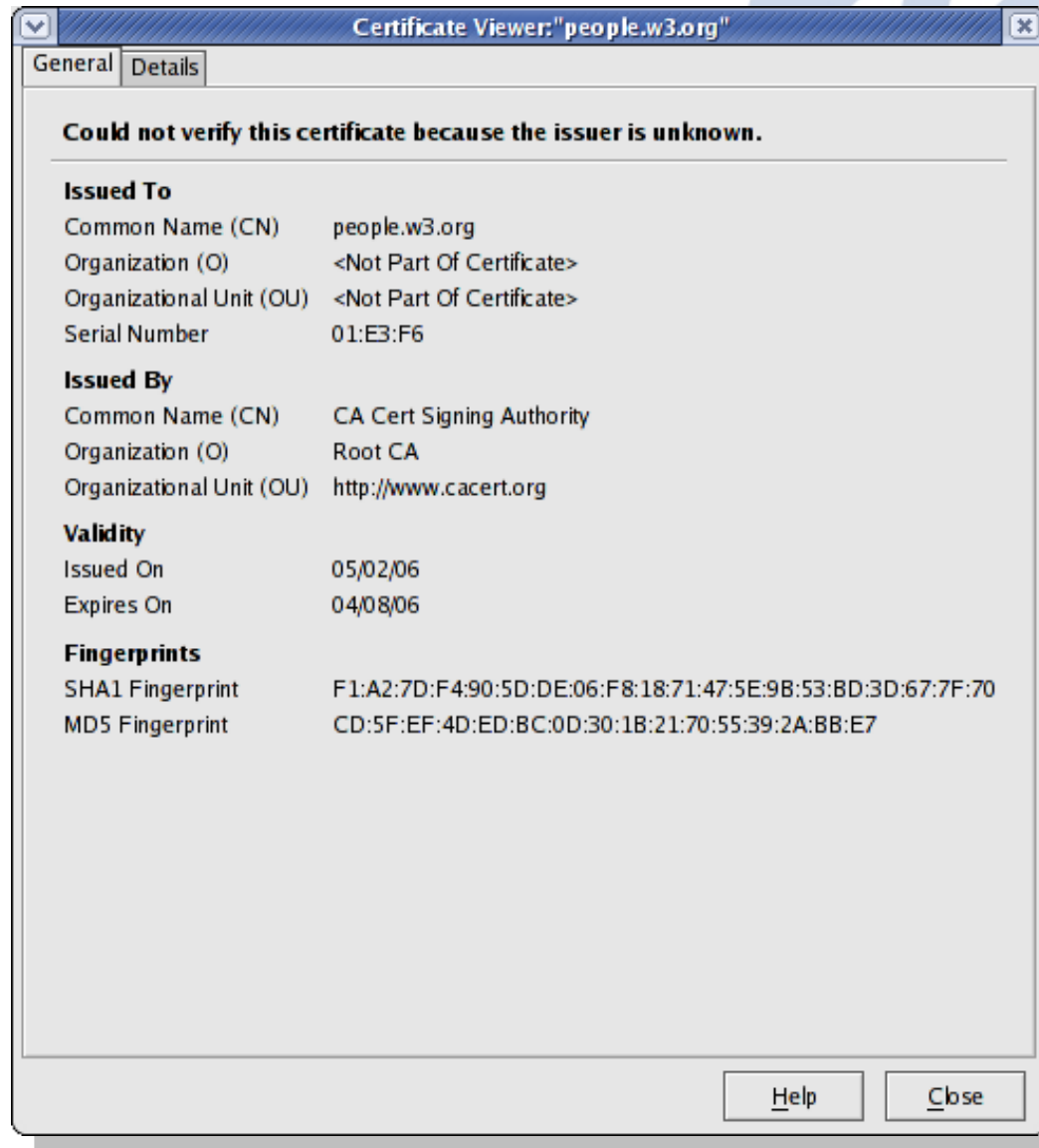
A padlock means “secure.” Not.



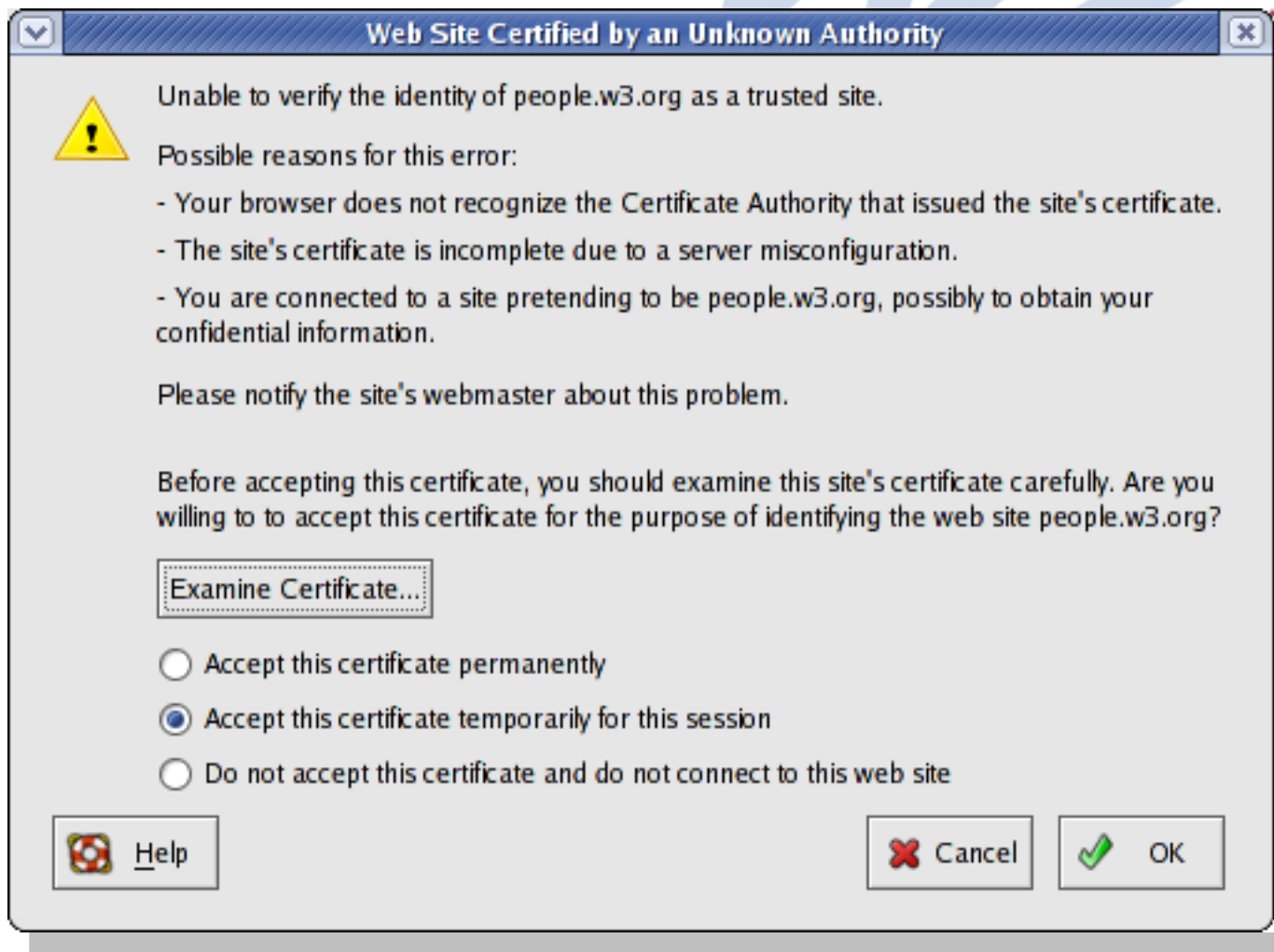
# But it gets worse...



# “Examine”



# 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?



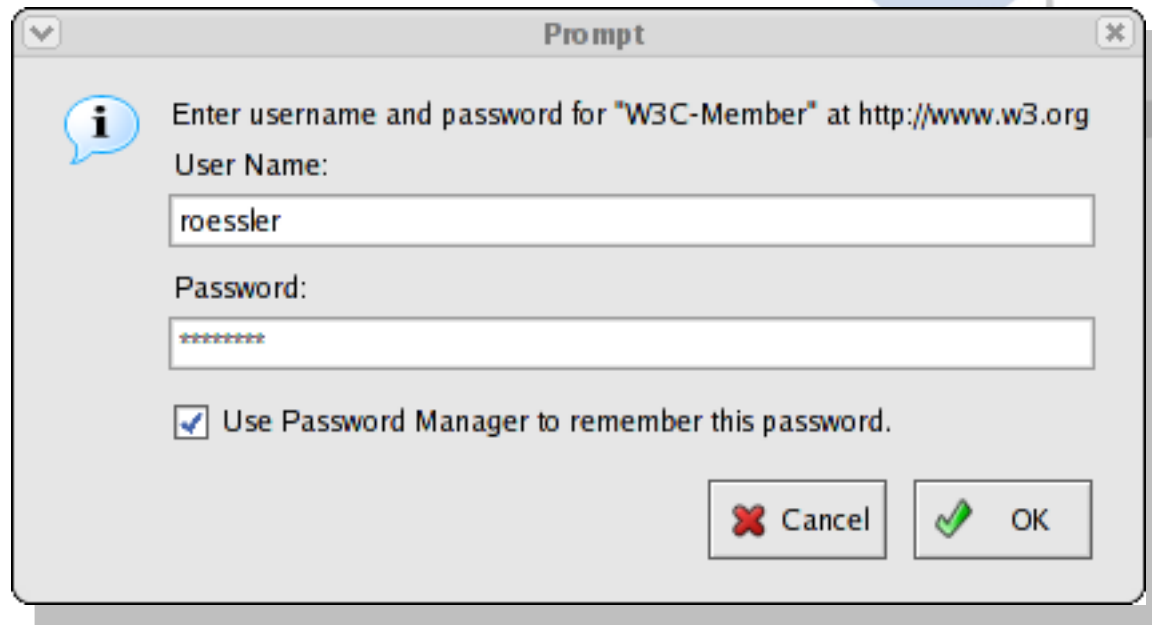
From: <http://www.w3.org/2005/Security/usability-ws/presentations/37-google>

# 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



A screenshot of a 'Prompt' dialog box. The title bar reads 'Prompt'. The main text says 'Enter username and password for "W3C-Member" at <http://www.w3.org>'. Below this, there are two input fields: 'User Name:' with the text 'roessler' and 'Password:' with a masked password '\*\*\*\*\*'. At the bottom, there is a checked checkbox labeled 'Use Password Manager to remember this password.' and two buttons: 'Cancel' (with a red X icon) and 'OK' (with a green checkmark icon).

# Forms and authentication

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



The image shows a login form for RegionsNet. It has a gold background and a dark brown header with the text "RegionsNet® Login" and a small upward-pointing triangle icon. Below the header, there are two input fields: "Login ID:" and "Password:". Below these fields is a red button with a white padlock icon and the text "Secure Login". Below the button, there is a section for "RegionsNet Online Banking:" with three links: "[Learn More](#)", "[Demo](#)", and "[Enroll Agreement & Disclosure](#)". Below this section, there is a section for "Other Online Services:" with a dropdown menu that currently displays "-Select a Service-".

# 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, ...)