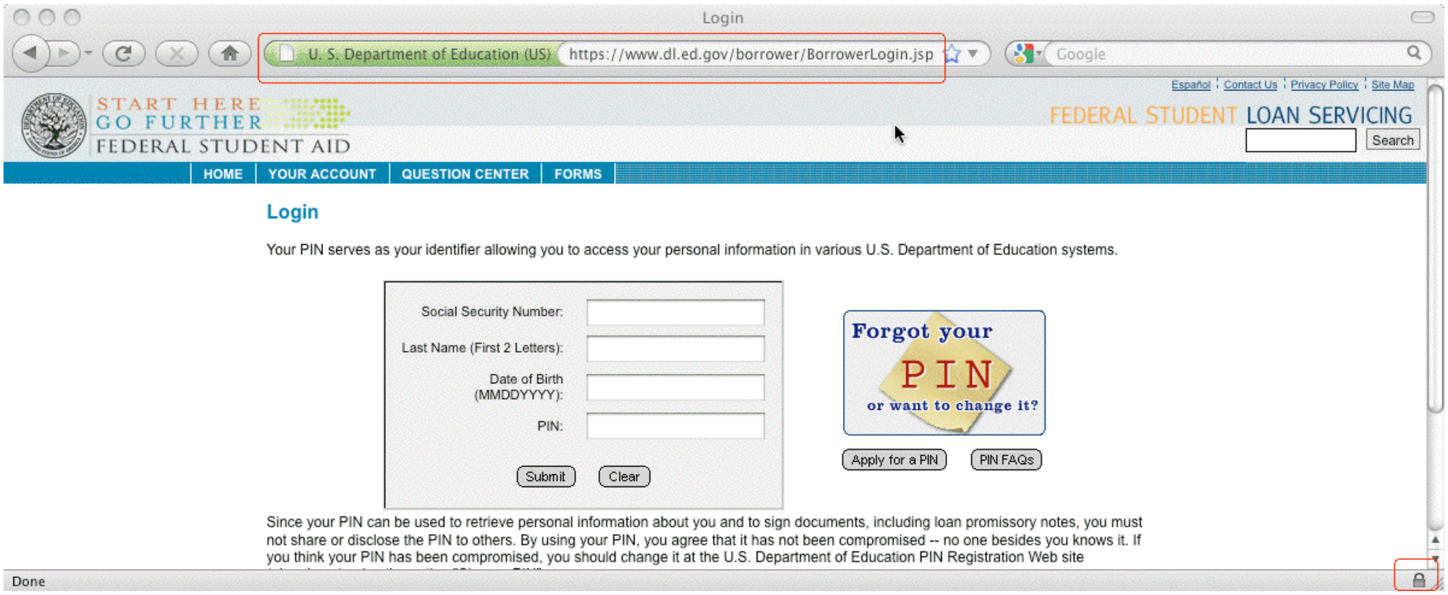
# SECURITY BEST PRACTICES FOR
# SECURE SOCKET LAYER (SSL) AND/OR TRANSPORT LAYER SECURITY (TLS)

When you order an item on the Internet and go to pay for your purchase, your credit card details will normally be collected via a secure web page that's protected with Secure Socket Layer (SSL) or Transport Layer Security (TLS).

Over time, you've probably come to recognize tangible signs that you're using a secure web page:

- Your browser will show a clickable padlock icon in the browser frame,
- The web site's address will be prefixed with https instead of just http, and
- If the site you're visiting uses a so-called "extended validation" or "EV" certificate, the identity of the site you're visiting will be shown in a clickable green-shaded background in most modern browsers.

For example:


Login
U. S. Department of Education (US)
https://www.dl.ed.gov/borrower/BorrowerLogin.jsp
Google
Español | Contact Us | Privacy Policy | Site Map
START HERE
GO FURTHER
FEDERAL STUDENT AID
FEDERAL STUDENT LOAN SERVICING
Search
HOME
YOUR ACCOUNT
QUESTION CENTER
FORMS
Forgot your PIN or want to change it?
Apply for a PIN
PIN FAQs
Submit
Clear
Done

Login

Your PIN serves as your identifier allowing you to access your personal information in various U.S. Department of Education systems.

Social Security Number:

Last Name (First 2 Letters):

Date of Birth (MMDDYYYY):

PIN:

Since your PIN can be used to retrieve personal information about you and to sign documents, including loan promissory notes, you must not share or disclose the PIN to others. By using your PIN, you agree that it has not been compromised -- no one besides you knows it. If you think your PIN has been compromised, you should change it at the U.S. Department of Education PIN Registration Web site

*Figure 1. Sample Department of Education secure web site protected with an extended validation certificate*

When we see those indicators when we visit a web site, we can have confidence that:

- We're interacting with the web site that we meant to connect to
- The information we send will be protected from eavesdropping during transmission, and
- What we sent will arrive intact and unchanged.

From an end-user's point of view, these web security protections are critical to our online confidence.

If we couldn't trust online websites with sensitive information, we wouldn't be able to accomplish basic everyday higher education tasks such as logging in to read our email, working in our teaching and learning system, accessing high performance research clusters, cutting purchase orders, or any of the myriad other sensitive instructional, research, or administrative tasks we all do every day.

***But what about the secure web sites that higher education itself runs? What are the best common practices that we should be following in deploying our own secure web sites?***

Version 1.0, June 30th, 2011, http://pages.uoregon.edu/joe/one-pager-tls/
Feedback? Contact Joe St Sauver, Ph.D., joe@uoregon.edu or joe@internet2.edu
Disclaimer: All opinions expressed in this document are those of the author and do not necessarily represent the opinion of any other entity.

**Some Best Common Practices for Higher Education Secure Web Sites**

**1. If a university web site collects sensitive information, do so only over a secure web server.** Sensitive information includes passwords as well as personally identifiable information such as SSNs, credit card numbers, grades, driver's license and passport-related information, medical information, etc.

**2. Make sure your web server's software, including a) the server's operating system, b) Apache (or whatever web server software you're running), c) OpenSSL, and d) mod_ssl are up-to-date!**

**3. Use only strong cryptography.** SSL/TLS relies on cryptography for security. One factor that affects the security of your secure session is the SSL protocol you use. DON'T use SSL 2. DO use SSL 3 or TLS 1.0. If your implementation supports it, TLS 1.1 or TLS 1.2 is better still. Make sure your server also only uses "medium" or "strong" ciphers. Do NOT use 40 or 56 bit ciphers, null ciphers, or anonymous ciphers. Check your SSL/TLS deployment by visiting the site evaluator that's at **https://www.ssllabs.com/ssldb/**

**4. Standardize on extended validation certificates.** While you can get and use so-called "domain validation" certificates, and those certificates will be adequate when it comes to protecting your traffic from eavesdropping or modification on the network, only minimal technical means[1] are used to make sure that those certificates are issued to an authorized requestor. As a result, we recommend that you routinely/only use extended validation ("green bar") certificates on all secure servers.[2] When extended validation certificates are issued, much more attention is devoted to ensuring that your identity has been validated, and that you are authorized to use the domain name associated with that EV certificate.

**5. Use host-specific certificates, don't use wild card certificates.** Wild card certificates allow a single certificate to be used for multiple servers. For example, a wildcard certificate covering *.example.edu would be able to be used for www.example.edu, but also for departmental web sites such as alumni.example.edu, chemistry.example.edu, english.example.edu, financial-aid.example.edu, german.example.edu, etc. While that flexibility is convenient, each of those sites will be less rigorously identified, and arguably less well controlled, than if protected with individual host-specific certificates.

**6. Do NOT use SGC (Server Gated Cryptography) certificates.** SGC support is no longer needed.

**7. Encourage use of browsers that support OCSP.** From time to time, parties may want to revoke a certificate that has been compromised, mis-issued or otherwise no-longer-to-be-relied-upon. This change in status is typically signaled via Certificate Revocation Lists ("CRLs", RFC5280) and/or the Online Certificate Status Protocol ("OCSP", RFC2560). While most modern browsers, such as current versions of Firefox, support CRL and OCSP, some other browsers may not. If your users rely on browsers that fail to check certificate relevant revocation protocols, they run the risk of relying on untrustworthy certificates. You may also want to encourage your users to run "Certificate Patrol," a popular Firefox extension.

**8. Recognize that SSL/TLS can secure <u>more</u> than <u>just</u> web servers.** You can also use SSL/TLS to secure POP and IMAP connections, authenticated SMTP connections, and other network services. Anytime a password crosses the network, think, "I should be protecting that information with SSL/TLS."

[1] Typically, before issuing a domain validation certificate, a certificate authority will send a confirmation email to the whois point of contact associated with the certificate's domain name, or perhaps require temporary creation of an arbitrary specified CNAME under the domain as "proof" that you effectively control that domain.

[2] While extended validation certificates can cost up to $1500 per certificate (in quantity one) if purchased "retail" from some vendors, if purchased through the InCommon Certificate Service ( http://www.incommon.org/cert/ ), EV certificates are currently available at no additional charge. InCommon participants should effectively be able to use EV certificates everywhere.