# Transition to InCommon SSL Certificates Signed with SHA-2



## Summary


If you are using an InCommon SSL certificate that expires on or after 1/1/2016, you may need to obtain a new SSL certificate to avoid certificate warnings in at least one popular browser. This change is related to an industry-wide migration away from the SHA-1 signing algorithm in favor of SHA-2. Read on to learn more, or skip to Recommendations.


## SHA-1 Background

Most SSL certificates in use today are signed by a Certificate Authority (CA) using the SHA-1 algorithm. This includes all certificates issued by InCommon through the UW's Certificate Services prior to 10/01/2014. SHA-1 is considered to be cryptographically weak, but there are no practical attacks known at this time. The CA industry has been planning to deprecate SHA-1 and migrate to the stronger SHA-2 algorithm before an attack becomes practical.

## Browser Makers Force the Move to SHA-2

In November 2013, Microsoft announced that Windows would stop accepting SHA-1 certificates on 01/01/2017. More recently (August 2014) Google announced their timeline for deprecating SHA-1 certificates in Chrome. Google plans to successively phase in stricter warnings beginning in November 2014 and remove SHA-1 support completely at the same time as Microsoft. Good information on Mozilla's plans for Firefox and Apple's plans for Safari is not yet available.

Based on information from Google, it appears that Chrome will use icons in the address bar to visually indicate degraded security. The visual indicators are sensitive to the certificate expiration date, with certificates expiring in 2017 targeted first, then those expiring in 2016. Certificates expiring in 2014 and 2015 will not be impacted.

## Recommendations

Based on current information, we recommend you take the following actions depending on your situation.

| Your Situation | Recommended Action | Result |
|---|---|---|
| My certificate will expire in 2014 | Request a **new** certificate as your expiration date approaches | You will get a certificate signed with SHA-2 that will expire in 1, 2, or 3 years depending on the lifespan you requested |
| My certificate will expire in 2015 | Request a **new** certificate as your expiration date approaches | You will get a certificate signed with SHA-2 that will expire in 1, 2, or 3 years depending on the lifespan you requested |
| My certificate will expire in 2016 | Request a **new** certificate before January 2015 | You will get a certificate signed with SHA-2 that will expire in 1, 2, or 3 years depending on the lifespan you requested |
| My certificate will expire in 2017 | Request a **new** certificate before November 2014 | You will get a certificate signed with SHA-2 that will expire in 1, 2, or 3 years depending on the lifespan you requested |

## InCommon CA

The InCommon CA announced availability of SHA-2 SSL certificates on 9/22/2014. Offering SHA-2 certificates required deployment of new CA's, changes to the API used by UW Certificate Services, and updates to other InCommon administrative interfaces used by UW-IT staff in providing service.

## UW CA

The UW CA began offering SHA-2 certificates on 04/27/2016. SHA-1 certificates for legacy applications can be requested by sending email to help@uw.edu. SHA-1 Support will be reduced over the next few years–see UW CA SHA-1 Sunset for details.

## UW Certificate Services

UW Certificate Services began to support SHA-2 InCommon certificates with version 2.1.1 released on 10/01/2014. Version 2.1.1 also disabled certificate renewals since renewals would result in SHA-1 certificates with a 1 year lifespan and wouldn't help the migration to SHA-2. In Certificate Services version 2.2, released on 11/6/2014, we enabled renewals for SHA-2 certificates. Renewals for SHA-1 certificates will remain disabled. UW Certificate Services began to support SHA-2 UW CA certificates on 04/27/2016.

## FAQ

We will update this FAQ as needed.

**Q: How do I tell if my SSL certificate was signed with SHA-1 or SHA-2?**
A: All InCommon SSL certificates issued prior to 10/01/2014 via UW Certificate Services were signed with SHA-1. All UW CA certificates issued prior to 04/27/2016 via UW Certificate Services were signed with SHA-1. You can verify this by browsing to your web site and clicking the icon in your browser to view the SSL certificate. On the details screen for the certificate look for the "signature hash algorithm". You can also use tools like OpenSSL to view the details of a certificate.

**Q: How do I find out my certificates expiration date?**
A: You can view the expiration date by browsing to your web site and clicking the icon in your browser to view the SSL certificate. On the details screen for the certificate look for the "valid to" date. You can also find the expiration dates for your InCommon certificates by viewing them in UW Certificate Services at https://iam-tools.u.washington.edu/cs/.

**Q: If I have a SHA-1 certificate that is expiring, can I just renew it to get a SHA-2 certificate?**
A: No. InCommon's policy for SHA-1 certificate renewals requested before 01/01/2016 is to issue a SHA-1 certificate that will expire in 1 year. Beginning on 01/01/2016 they will not allow renewal of any SHA-1 certificates. After consideration of InCommon's policy, UW Certificate Services disabled the renewal feature in version 2.1.1 released on 10/01/2014. Expired SHA-1 certificates from the UW CA can be renewed.

**Q: Requesting a new certificate instead of a renewal requires I submit a Certificate Signing Request (CSR). Is that extra work really necessary?**
A: Yes. Unfortunately, that is the only way to get a SHA-2 certificate. If you still have the CSR you used to create your SHA-1 certificate, it's possible to use it again to get a SHA-2 certificate. Otherwise, you'll need to create a new CSR.

**Q: If I request a new InCommon SSL certificate, do I have to do anything special with my Certificate Signing Request (CSR) to ensure the certificate will be signed with SHA-2?**
A: No. UW Certificate Services will handle that for you.

**Q: My web server has the InCommon intermediate certificate (InCommon Server CA) installed. It appears to be signed with SHA-1. Do I need to get a new intermediate certificate too?**
A: Yes. SHA-2 SSL certificates depend on a new set of CAs, each with their own SHA-2 certificates. In the past there was only one intermediate certificate, but for SHA-2 there are two. You will need to have both of these intermediate certificates installed on your web server in order for browsers to follow the chain to a trusted root certificate.

> **10/6/2014 Update**
>
> One of InCommon's two new intermediate certificates was signed with SHA-512. (SHA-2 is a family of algorithms that includes SHA-256, SHA-384, and SHA-512.) The SHA-512 intermediate has been found to have some interoperability issues so, as of today, that intermediate CA is using a new certificate signed with SHA-384. The original SHA-512 certificate is still valid for any InCommon SSL certificates issued from 10/01/2014 through 10/05/2014 that include the SHA-512 certificate in their chain of trust.

**Q: What is an intermediate certificate?**
A: Intermediate certificates provide a way for the browser to link your SSL certificate (which it doesn't trust by default) up to a root certificate that it does trust. CAs often delegate some functions to a sub-CA, which can in turn further delegate to another sub-CA. Each CA in the chain must have it's own certificate issued by its parent. The information in each certificate allows the browser to build a chain of trust.

**Q: What are the InCommon intermediate certificates and where can I get them?**
A: Certificates issued from 10/01/2014 through 10/05/2014 use a different certificate chain than those issued 10/6/2014 and later:

- **10/1/2014 through 10/5/2014:** AddTrustExternal CA Root > UserTrust RSA Certification Authority > InCommon RSA Server CA (SHA-512) > your SSL certificate
- **On or after 10/6/2014:** AddTrustExternal CA Root > UserTrust RSA Certification Authority > InCommon RSA Server CA (SHA-384) > your SSL certificate

If you download your certificate in the PKCS7 format, the correct intermediate certificates will automatically be included. If you download the PEM format you will only receive your SSL cert but instructions and a link to obtain the intermediate certificates is provided. See InCommon SSL Intermediate Certificates.

**Q: What will happen if I don't migrate to an SSL certificate signed with SHA-2?**
A: That depends on the browser, the expiration date for the certificate, and the current date. Initially the user may see warnings or changes in the security icons used in the address bar. By 1/1/2017 all major browsers will reject certificates signed with SHA-1.

**Q: Will my UWCA SSL certificates be affected?**
A: We've recommended against using UWCA certificates for SSL on https web sites for a few years now. If you are still using a UWCA SSL certificate for this purpose we recommend you replace it with an InCommon SSL certificate. See the Certificate Services wiki for more information: https://wiki.cac.washington.edu/x/KDaoAQ.

**Q: What about UWCA certificates my application uses to authenticate to UW web services and directory services?**
A: Many UW web services and directory services require application clients to use UWCA certificates to authenticate. These certificates are signed with SHA-2 if they were issued on or after 04/27/2016. SHA-1 certificates for legacy applications can be requested by sending email to help@uw.edu. Application developers are encouraged to remove support for SHA-1 certificates from their applications.

## Getting Assistance

If you have questions concerning your InCommon SSL certificates or UW CA certificates and the migration to SHA-2, contact us at iam-support@uw.edu.

## More Reading

- SHA1 Deprecation Policy (Microsoft)
- Microsoft Retiring SHA-1 in 2016 (Bruce Schneier)
- Intent to Deprecate: SHA-1 certificates (Google)
- Gradually sunsetting SHA-1 (Google)
- Google acceleration of SHA-1 deprecation draws resistance (SC Magazine)