

Upgrading Weak Keys in Metadata

 **Deprecated**

Note that this page has been deprecated. The information it contains is no longer current.

In January 2010, InCommon Operations announced that all [certificates in metadata](#) must have at least 2048-bit keys by the end of December 2012. In anticipation of this deadline, InCommon Operations began a comprehensive communications campaign in June 2012. The goal of the campaign was to inform Site Administrators of the security risks associated with weak keys in metadata, and to educate them how to mitigate the risk, that is, how to [migrate a certificate with a strong key into metadata](#). To make a long story short, the last remaining weak key was removed from InCommon metadata on March 28, 2013. This wiki page and its child page ([Report on Weak Keys in Metadata](#)) are the historical record of this effort.

 **Weak Key Final Report**

The last weak key (i.e., 1024-bit key) was removed from InCommon metadata on March 28, 2013. Since all *new* certificates are now required (by the software) to have at least 2048-bit keys, InCommon metadata will remain free of weak keys indefinitely.

The report data in the following frame is **LIVE DATA** (view a copy of the [most current data](#) in its own browser window)

We have compiled a [complete list of certificates in metadata](#) for your convenience. This file is updated daily.

Historical Summary of Weak Keys in Metadata

	2012-08-17	2012-09-20	2012-10-10	2012-10-22	2012-11-12	2012-12-17	2012-12-27	2013-01-30	2013-03-28
IdPs:	26	19	15	15	15	11	11	7	0
SPs:	65	53	48	40	35	25	18	12	0
			InCCollaborate: report	InCCollaborate: report	InCCollaborate: report	InCCollaborate: report	InCCollaborate: report	InCCollaborate: report	

A [Report on Weak Keys in Metadata](#) records the history of weak keys in metadata.

 **Optimal Key Size**

The InCommon Technical Advisory Committee recommends that all certificates in metadata contain 2048-bit keys. Keys larger than 2048 bits are allowed but not recommended since such keys are computationally expensive (for all parties, both IdPs and SPs) but yield little increase in security.

Be aware that certificate migration may take weeks depending on how often your federation partners refresh metadata. Related to this, a new document on [Certificate Migration](#) describes how to systematically replace an old certificate with a new certificate in metadata without affecting interoperability.

 **Certificate Migration**

Do not simply replace one certificate with another in metadata! Consult the [Certificate Migration](#) topic for recommended practices that insure continued interoperability throughout the migration process.

In the InCommon Federation, the use of long-lived, self-signed [X.509 certificates in metadata](#) is strongly recommended. A self-signed certificate containing a 2048-bit key is easily created with the OpenSSL command-line tool. Before doing so, develop a strategy for [securely handling the private key](#), since the security of your deployment (and that of your partners) depends on the security of the private key used to sign and/or decrypt messages.

File	Modified
PDF File ReportOnWeakKeysinMetadata-2012-10-10.pdf	Oct 20, 2012 by trscavo@internet2.edu
PDF File ReportOnWeakKeysinMetadata-2012-10-22.pdf	Oct 20, 2012 by trscavo@internet2.edu
PDF File ReportOnWeakKeysinMetadata-2012-11-12.pdf	Nov 12, 2012 by trscavo@internet2.edu
PDF File ReportOnWeakKeysinMetadata-2012-12-17.pdf	Dec 17, 2012 by trscavo@internet2.edu
PDF File ReportOnWeakKeysinMetadata-2012-12-27.pdf	Dec 27, 2012 by trscavo@internet2.edu
PDF File ReportOnWeakKeysinMetadata-2013-01-30.pdf	Jan 30, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-01-04.txt	Mar 28, 2013 by trscavo@internet2.edu

Text File cert-raw-data-2012-12-27.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2012-11-12.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2012-12-13.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2012-12-14.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-01-23.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-01-18.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-01-09.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-01-11.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-01-15.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-02-19.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-02-18.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-01-30.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-02-01.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-02-11.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-02-28.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-02-20.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-02-22.txt	Mar 28, 2013 by trscavo@internet2.edu
Text File cert-raw-data-2013-02-26.txt	Mar 28, 2013 by trscavo@internet2.edu

[Download All](#)