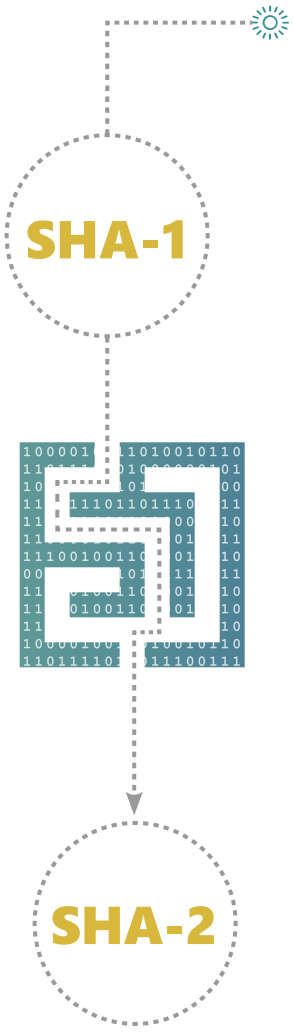
SHA-1 Deprecation Challenges and Solutions

WHITE PAPER I Published by CSS Research I Q2 2016

SHA-1 Deprecation Challenges and Solutions

WHITE PAPER | Published by CSS Research | Q2 2016



Overview

SHA-1 digital certificates are no longer being issued and are scheduled to reach their expiration before January 1, 2017. Continued use of SHA-1 certificates places your organization in a cryptographically insecure position against cyber adversaries. Research continues to confirm the theories of why the SHA-1 signing algorithm is weak and when it is likely to be broken by a hash collision. Projections of the computational and financial costs and time needed to crack SHA-1 have significantly lowered over the years. While hashing different messages should result in unique hashes, actual collisions can lead to the same hash value being produced for different messages, which can ultimately be exploited to create fake certificates.

Time is running out for you to identify and implement an SHA-1 deprecation plan to ensure that every certificate your organization uses is based on the secure SHA-2 algorithm. If you purchase digital certificates from a third-party Certificate Authority (CA), you may only need to contact your vendor to confirm their deprecation plan and timelines and ensure compatibility with your devices and systems. If you issue digital certificates from your own CA, your migration path will be different. Regardless of where your certificates originate from, planning and managing a successful transition will ensure a timely SHA-2 migration. The following information is intended to help you understand the reasons behind SHA-1 deprecation, deprecation timing, and SHA-2 migration challenges, as well as best practices and resources to complete the transition.

SHA-1 versus SHA-2

Hash values help ensure the integrity of a given piece of data because they are virtually guaranteed to be unique and unpredictable. Secure Hash Algorithm (SHA) is a type of cryptographic hash function created to ensure that data has not been modified.

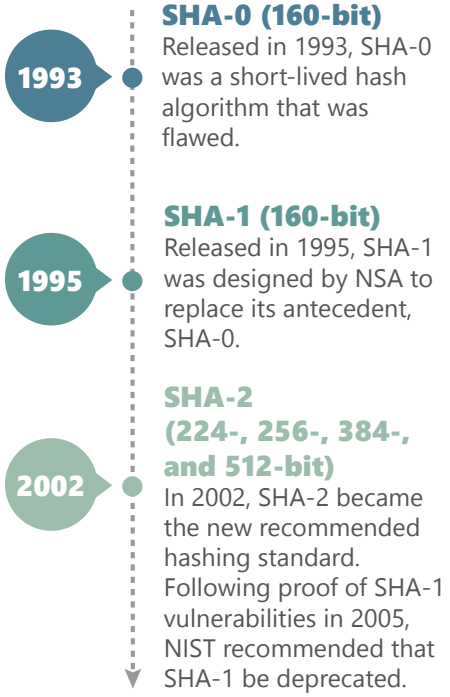
SHA accomplishes this by computing a cryptographic hash value for a given piece of data that is unique to that data. Different pieces of data yield unique hash values, and any change to a given piece of data will result in a different hash value. Differing hash values are the key to determining if data has been altered.

SHA-0 was a short-lived hash algorithm released in 1993. When it was discovered that the algorithm was flawed, the National Security Agency (NSA) designed a replacement, in 1995, called SHA-1. Both SHA-0 and SHA-1 are 160-bit hash functions. That means each and every possible piece of data will hash down to a 160-bit number. SHA-1 currently enjoys widespread adoption and is supported by most devices and systems that use cryptographic hash functions.

A primary consideration for cryptographic hash designers is minimizing the probability that two different pieces of data yield the same hash value. When this happens, it's referred to as a "cryptographic hash collision." The problem is that while there are an infinite number of unique bits of data, there are limited numbers of computable hash values. Using SHA-1, there are 2^{160} possible cryptographic hash values. Mathematical theory tells us that the chances that any two messages computing to the same value should be about 1 in 2^{80}. In other words, in order to find two messages that computed the same value, you would have to try 2^{80} different messages before you would expect to find two whose hashes collide. While this very large number makes hash guessing improbable, crypto-mathematicians proved in 2005 that SHA-1 hash collisions could be calculated much quicker than simply trying 2^{80} different messages (2,000 times quicker, in fact). This is the reason that SHA-1 is being phased out of most governmental applications, and that National Institute of Standards and Technology (NIST) has recommended that SHA-1 not be used after 2010.

In 2002, SHA-2 became the new recommended hashing standard. SHA-2 is often called the SHA-2 family of hashes because it contains hashes of different sizes, including 224-, 256-, 384-, and 512-bit digests and is considered to be cryptographically strong. The encryption hash used in SHA-2 is significantly stronger and not subject to the same vulnerabilities as SHA-1.

Evolution of SHA-0 to SHA-2



 |

Ted Shorter, CTO
Certified Security Solutions

"While we have yet to see a SHA-1 certificate collision attack in the wild, it's clear that the SHA-1 algorithm is extremely vulnerable, and getting weaker all the time. Organizations should be done with, or in the midst of their migration to SHA-2. The risk to continued use of SHA-1 certificates is too great for any business to ignore." **— Ted Shorter, Certified Security Solutions (CSS) CTO**

The Rush to Deprecate SHA-1

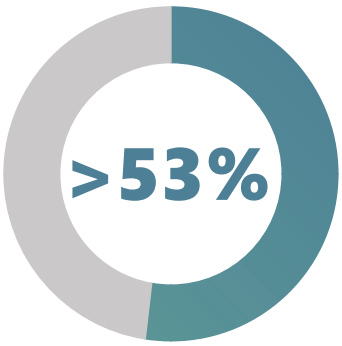
Research continues to offer undeniable proof of why the SHA-1 signing algorithm is weak and when it's likely to be cracked by a hash collision. Studies conducted by NIST, the NSA, and other research-based organizations have repeatedly concluded that SHA-1 can be broken and at the same time are projecting decreases in the financial costs and the amount of computational time needed to crack SHA-1.

Cryptographer and computer security and privacy specialist Bruce Schneier estimated to Ars Technica back in 2012 that performing a full-on collision attack on SHA-1 would cost $700,000 by 2015 and only $178,000 by 2018[1]. However, research conducted in September 2015 by an international team of security researchers estimates the time and money needed to produce a collision to be significantly less. Their conclusion is that freestart collision could now be successfully executed for the mere price of $75,000 to $120,000 – an amount that is well within the reach of cyber criminals.

"While we have yet to see a SHA-1 certificate collision attack in the wild, it's clear that the SHA-1 algorithm is extremely vulnerable, and getting weaker all the time. Organizations should be done with, or in the midst of their migration to SHA-2. The risk to continued use of SHA-1 certificates is too great for any business to ignore," said Ted Shorter, Certified Security Solutions (CSS) CTO. Malicious actors and criminal organizations could more easily and with less expense figure out the public and/or private keys used as the unique basis of identity and trust for certificates.

While research concludes that the shift to SHA-2 is needed, some organizations may not be moving as fast as needed to implement the warranted transition. In its weekly monitoring of public-facing certificates, CSS Research identified the percentage of certificates signed with SHA-1 at over 53% of the total certificates published to the Internet (March 21, 2016).[2]

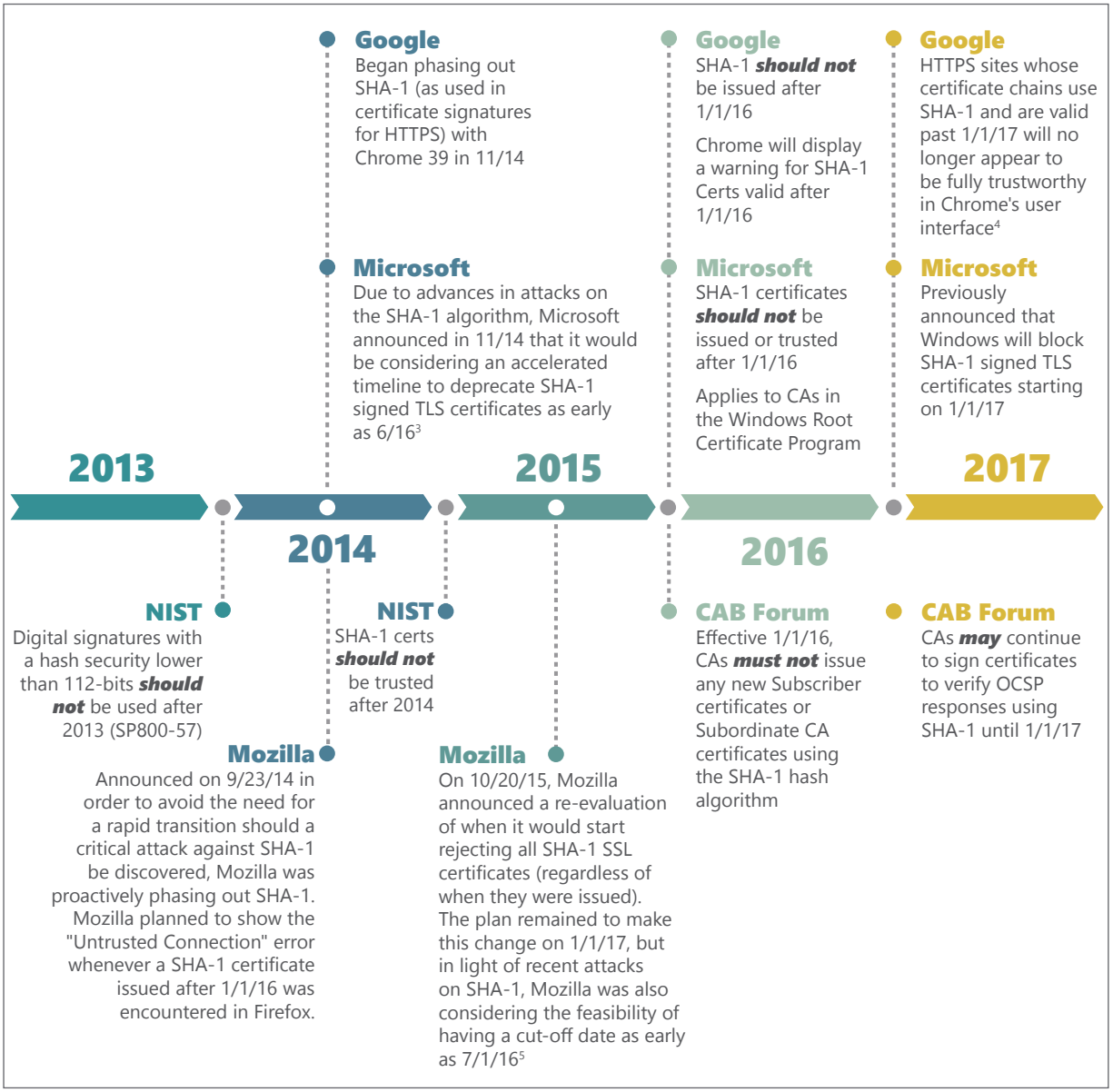
Public Certificates Signed with SHA-1 as of 03/21/16



Compounding Issues: Varying Deprecation Dates & SHA-2 Compatibility

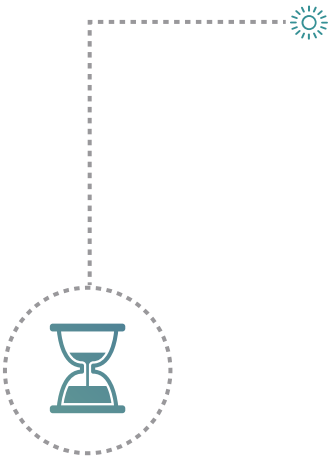
Compounding the issue of SHA-1 weakness is that industry-leading organizations, third-party CAs, and major browsers, including Microsoft, Google, and Mozilla, have announced differing SHA-1 deprecation plans. Certain browser deprecation dates are already impacting websites with SHA-1 certificates featuring expiration dates as early as December 31, 2015.

SHA-1 Deprecation Timeline



Another issue lies in the host of applications and devices that continue to rely on SHA-1. Many of them are not yet able to accept or understand SHA-2-based certificates. The widespread adoption of SHA-1 by systems requiring hashing functions might serve to illustrate the difficulty of SHA-2 adoption. The spectrum of possible crypto devices, applications, and systems demand a variety of management and upgrade paths. The most difficult issue is that not everything that uses SHA-1 is compatible with SHA-2.

Organizations and major browsers are designating different dates for official SHA-1 deprecation, and these projected dates are changing all the time. Upgrading a PKI from SHA-1 to SHA-2 will not only require policy and procedure updates and the installation of new CAs that are capable of issuing SHA-2 certificates, but also ensuring that all subscribers, relying parties, applications, and devices can actually use the resulting SHA-2-based certificates.

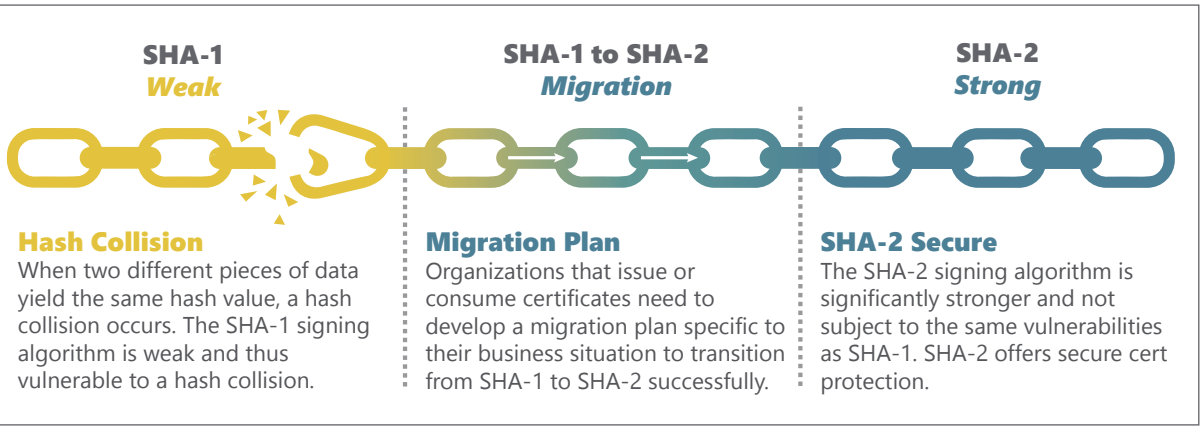


Time is Running Out. What Should You Do?

Simply put, SHA-1 is weak. Critical devices and systems continue to rely on SHA-1, time is running out, and action must be taken. Without adopting SHA-2, not only do organizations and users run the risk of not being able to trust that data is authentic, but in the case of public-facing browsers, users will be notified of "untrusted connections" or even experience lack of access – all because of a vulnerable SHA-1 certificate. Given the lower cost and increasing advancements in computing power and cryptanalysis, it's not a matter of if an SHA-1 collision will occur, it's a matter of when.

Organizations that issue or consume certificates need a transition plan. Industry-leading CAs and browsers are taking this seriously. So, too, should organizations that manage their own PKI infrastructure, CA, and digital certificates. Both large and small organizations are vulnerable today, and reacting after an outage or breach can prove to be ugly, often costing millions of dollars.

Migration from SHA-1 to SHA-2 for Secure Cert Protection



Best Practices for SHA-2 Migration Planning

Ultimately, there is no single information security authority requiring organizations to phase out SHA-1 and migrate to SHA-2. There are also no formal deadlines, other than those imposed by major browsers and industry leaders. This means that you'll need to assess your unique situation based on how your business manages (or does not manage) PKI to determine your course of action. There is no telling when SHA-1 will be broken, but the risk increases on a daily basis, and the time to react is now.

Best Practices for SHA-2 Migration Planning

01 Recommendation

If your organization issues certificates from an internal CA

- Assess your internal PKI/CA needs for your SHA-2 transition, including hardware, software, people, policies, and procedures related to the creation, management, distribution, storage and revocation of digital certificates.
- Review your entire certificate inventory, hashing algorithms used, and expiration timing.
- Confirm hardware and software interoperability with SHA-2.
- Identity PKI changes, including a new CA.
- Create and implement your transition plan.

02 Recommendation

If your organization issues certificates from a third-party CA

- Contact your third-party certificate provider for formal deprecation dates and determine your involvement in the process.
- Review your entire certificate inventory, hashing algorithms used, and expiration timing.
- Confirm hardware and software interoperability with SHA-2.
- Create and implement your transition plan in coordination with your vendor.

03 Recommendation

If your organization issues certificates from multiple sources

- Create and manage multiple transition plans.

** If you need professional services from an external PKI expert, get on their radar now. Many PKI consulting organizations are currently filling their schedules with SHA-2 transition projects.*

Getting Started: Certified Security Solutions (CSS) Can Help

If you have questions about the SHA-2 migration or are seeking PKI expertise to assist with the transition, don't hesitate to contact the CSS PKI professionals. As a cyber security market leader for enterprise and IoT digital identity security for data, devices, and applications, CSS PKI experts are actively working with clients to help them address their unique situation through PKI Health Checks and PKI Professional Service engagements.

About Certified Security Solutions (CSS)

As the market leader in enterprise and IoT digital identity security for data, devices, and applications, CSS is a cyber security company that builds and supports platforms to enable secure commerce for global businesses connected to the Internet. Headquartered in Cleveland, Ohio, with operations throughout North America, CSS is at the forefront of delivering innovative software products and SaaS solutions that are secure, scalable, economical, and easy to integrate into any business. Visit www.css-security.com for more information.

About CSS Research

CSS Research is a specialized division of CSS launched to monitor threat intelligence for more than 3.7 Billion IP addresses, offering continuous oversight and threat intelligence insights on the digital certificates used to secure SSL/TLS connections across the Internet. Other key departmental features include threat intelligence thought leadership, driving and executing initiatives focused on improving early detection of certificate vulnerabilities, identifying compromises and forgeries and supporting key customer accounts with deep knowledge and expertise.

Contact Us

css-security.com

877.715.5448

In preparation for participating in the Google-sponsored Certificate Transparency project, CSS Research monitors and publishes weekly public SSL/TLS data on more than 3.7 billion IPv4 addresses, including:

- Total certificates identified (SSL/TLS, ECC, device certificates, etc.)
- Certificate issuer market share
- Self-signed certificates versus those issued by a CA
- Certificate issuance and expiration statistics
- Signature algorithm breakdown (SHA-1 / SHA-2, etc.)

Weekly statistics, additional initiative information, and the option for organizations to request their own custom Public SSL Report can be found on the CSS Research web page.

Additional Resources

2016 Public Key Infrastructure (PKI) and Internet of Things (IoT) Security Predictions: CSS believes that in 2016, the need for trusted digital identities will become paramount to overall security within the global Internet. As businesses continue to brace against cyber adversaries and look to secure the Internet of Things (IoT), Public Key Infrastructure (PKI) is making a resurgence as an economical, reliable, and proven technology that delivers a secure and high-performance solution. Read the CSS blog reviewing the predictions of CSS security experts for 2016, and how they'll impact decision makers.

Freestart Collision for SHA-1: Researchers Marc Stevens, Pierre Karpman, and Thomas Peyrin released a new hash attack called "Freestart Collisions". Read the CSS blog about the new attack on SHA-1 and how it has dramatically reduced the time it takes to calculate SHA-1 collisions.

PKI Professionals LinkedIn Group: The group's mission focuses on uniting security professionals to share insights on PKI technologies and digital identity security trends. Click here to register for the group.

CSS Who We Are & What We Do: Certified Security Solutions (CSS) is a cyber security company that builds and supports platforms to enable secure commerce for businesses connected to the Internet. This data sheet provides an overview of who CSS is and how we can assist your organization with an effective security strategy. Click here for the CSS datasheet.

References

1. Goodin, D. (2015, October 08). SHA1 algorithm securing e-commerce and software could break by year's end. Retrieved March 08, 2016, from http://arstechnica.com/security/2015/10/sha1-crypto-algorithm-securing-internet-could-break-by-years-end/

2. CSS Research (2016, March 16). SSL Certificate Report as of 3-21-16. Retrieved March 22, 2016, from https://www.css-security.com/research/

3. Pflug, K. (2015, November 04). SHA-1 Deprecation Update. Retrieved March 09, 2016, from https://blogs.windows.com/msedgedev/2015/11/04/sha-1-deprecation-update/

4. Palmer, C., & Sleevi, R. (2014, September 05). Gradually sunsetting SHA-1. Retrieved March 08, 2016, from https://security.googleblog.com/2014/09/gradually-sunsetting-sha-1.html

5. Barnes, R. (2015, October 20). Continuing to Phase Out SHA-1 Certificates. Retrieved March 09, 2016, from https://blog.mozilla.org/security/2015/10/20/continuing-to-phase-out-sha-1-certificates/

