IEEE P802.11
Wireless LANs

|  |
| --- |
| NIST plan to transition away from SHA-1 |
| Date: 2023-03-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dorothy Stanley | Hewlett Packard Enterprise |  | +1 630-363-1389 | dorothy.stanley@hpe.com  |
|  |  |  |  |  |

Abstract

This document contains the information received 2023-01-25 from Lily Chen (NIST) regarding the NIST plan to transition away from SHA-1. The received document is embedded below and copied on the following pages.



Consideration of this information is delegated to TGme, see <https://www.ieee802.org/11/email/stds-802-11/msg06922.html> .

**NIST Transitioning Away from SHA-1 for All Applications**

NIST is introducing a plan to transition away from the current limited use of the Secure Hash Algorithm 1 (SHA-1) hash function. Other approved hash functions are already available. The transition will be completed by December 31, 2030, and NIST will engage with stakeholders throughout the transition process.

**Background**

SHA-1 was first specified in 1995 in Federal Information Processing Standard [(FIPS) 180-1](https://doi.org/10.6028/NIST.FIPS.180-1), *Secure Hash Standard (SHS)*. In 2005, a serious cryptanalytic attack was announced about SHA-1’s collision resistance – a necessary property for its use in digital signature applications. NIST responded in 2006 with an [announcement](https://csrc.nist.gov/news/2006/nist-comments-on-cryptanalytic-attacks-on-sha-1) encouraging a rapid transition to the use of the SHA-2 family of hash functions for digital signature applications, which were initially specified in [FIPS 180-2](https://csrc.nist.gov/publications/detail/fips/180/2/archive/2004-02-25). NIST began a competitive process to develop an additional hash function, which resulted in the SHA-3 family of hash functions published in 2015 as [FIPS 202](https://doi.org/10.6028/NIST.FIPS.202)***.* In 2011, NIST released** [SP 800-131A](https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final), which **announced the deprecation of SHA-1 when generating new digital signatures and restricted further use of SHA-1 to only where allowed in NIST protocol specific guidance.**

**Objective**

Cryptanalytic attacks on the SHA-1 hash function as used in other applications have become increasingly severe in recent years (["[SHA-1 is a Shambles](https://www.usenix.org/conference/usenixsecurity20/presentation/leurent)" by Leurent and Peyrin](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fia.cr%2F2020%2F014&data=04%7C01%7Cchristopher.celi%40nist.gov%7C66a968d83075400fab3508d9e1a6a091%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637788928054859623%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=y7ePECWBeW00PS1IzGMOHMTSz6nKQbtqzP9I27SKzpQ%3D&reserved=0), 2020). As a result, **NIST will transition away from the use of SHA-1 for applying cryptographic protection to all applications by December 31, 2030**.Note that after this termination date, it may be necessary to use SHA-1 for handling information protected prior to the termination date; the [SHA-1 specification](https://doi.org/10.6028/NIST.FIPS.180-1) will remain available for this purpose.

**Plan**

Before December 31, 2030, NIST plans to:

* Publish FIPS 180-5 (a revision of FIPS 180) to remove the SHA-1 specification,
* Revise [SP 800-131A](https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final) and other affected NIST publications to reflect the planned withdrawal of SHA-1, and
* Create and publish a transition strategy for the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP).

Throughout this process, NIST will actively engage with government agencies, validation testing laboratories, vendors, Standards Developing Organizations, sector/industry organizations, users, and other stakeholders to minimize potential impacts and facilitate a smooth transition.

**NIST encourages these entities to begin planning for this transition now**. By completing their transition before December 31, 2030, stakeholders – particularly cryptographic module vendors – can help minimize potential delays in the validation process.

**Contact**

Send questions about the transition in an email to sha-1-transition@nist.gov. Visit the [Policy on Hash Functions](https://csrc.nist.gov/Projects/hash-functions/NIST-Policy-on-Hash-Functions) page on CSRC to learn more.

**References:**