tls
Internet-Draft
Intended status: Experimental
Expires: January 30, 2020

D. Benjamin
Google LLC

July 29, 2019

Legacy RSASSA-PKCS1-v1_5 codepoints for TLS 1.3
draft-davidben-tls13-pkcs1-00

Abstract

This document allocates code points for the use of RSASSA-PKCS1-v1_5 with client certificates in TLS 1.3.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 30, 2020.

Table of Contents

1. Introduction

TLS 1.3 [RFC8446] removed support for RSASSA-PKCS1-v1_5 [RFC8017] in CertificateVerify messages in favor of RSASSA-PSS. While RSASSA-PSS is a long-established signature algorithm, some legacy hardware cryptographic devices lack support for it. Due to performance requirements, such devices are uncommon in TLS servers, but are sometimes used by TLS clients for client certificates. Moreover, TLS negotiates the protocol version before client certificates, so this limitation can further impact adjacent connections that do not use affected keys.

This document allocates code points to use these legacy keys with client certificates in TLS 1.3.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. PKCS#1 v1.5 SignatureScheme Types

The following SignatureScheme values are defined for use with TLS 1.3.

```
enum {
    rsa_pkcs1_sha256_legacy(TBD1),
    rsa_pkcs1_sha384_legacy(TBD2),
    rsa_pkcs1_sha512_legacy(TBD3),
} SignatureScheme;
```

The above code points indicate a signature algorithm using RSASSA-PKCS1-v1_5 [RFC8017] with the corresponding hash algorithm as defined

in [SHS]. They are only defined for signatures in the client CertificateVerify message and are not defined for use in other contexts. In particular, servers intending to advertise support for RSASSA-PKCS1-v1_5 signatures in the certificates themselves should use the rsa_pkcs1_* constants defined in [RFC8446].

Clients MUST NOT advertise these values in the "signature_algorithms" extension of the ClientHello. They MUST NOT accept these values in the server CertificateVerify message.

Servers that wish to support clients authenticating with legacy RSASSA-PKCS1-v1_5-only keys MAY send these values in the "signature_algorithms" extension of the CertificateRequest message and accept them in the client CertificateVerify message. Clients with such legacy keys MAY negotiate the use of these signature algorithms if offered by the server. Clients SHOULD NOT negotiate them with keys that support RSASSA-PSS.

4. Security Considerations

Prior to this document, legacy RSA keys would prevent client certificate deployments from adopting TLS 1.3. The new code points allow such deployments to upgrade without replacing the keys. TLS 1.3 fixes a privacy flaw [PRIVACY] with client certificates, so upgrading is a particular benefit to these deployments.

Additionally, TLS negotiates protocol versions before client certificates. When sending a ClientHello, a TLS-1.3-capable client cannot determine if the server will request a legacy key. It may then offer TLS 1.3, to upgrade connections to other servers. A TLS-1.3-capable server that requests client certificates cannot then distinguish such a client from one with modern keys. It may then negotiate TLS 1.3 and send a CertificateRequest. The connection would then fail due to the legacy key, when it previously succeeded at TLS 1.2.

To recover from this failure, one side must globally disable TLS 1.3 or the client must implement an external fallback. Disabling TLS 1.3 impacts connections that would otherwise be unaffected by this issue, while external fallbacks break TLS's security analysis and may introduce vulnerabilities [POODLE]. The new code points reduce the pressure on implementations to select one of these mitigations.

However, the new code points also reduce the pressure on implementations to migrate to RSASSA-PSS. The above considerations do not apply to server keys, so these new code points are forbidden for use with server certificates. RSASSA-PSS continues to be required for TLS 1.3 servers using RSA keys.

Finally, when implemented incorrectly, RSASSA-PKCS1-v1_5 admits signature forgeries [MFSA201473]. Implementations producing or verifying signatures with these algorithms MUST implement RSASSA-PKCS1-v1_5 as specified in section 8.2 of [RFC8017]. In particular, clients MUST include the mandatory NULL parameter in the DigestInfo structure and produce a valid DER [X690] encoding. Servers MUST reject signatures which do not meet these requirements.

5. IANA Considerations

IANA is requested to create the following entries in the TLS SignatureScheme registry, defined in [RFC8446]. The "Recommended" column should be set to "N", and the "Reference" column should be set to this document.

Value	Description
TBD1	rsa_pkcs1_sha256_legacy
TBD2	rsa_pkcs1_sha384_legacy
TBD3	rsa_pkcs1_sha512_legacy

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/info/rfc8017>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[SHS] Dang, Q., "Secure Hash Standard", National Institute of Standards and Technology report, DOI 10.6028/nist.fips.180-4, July 2015.

[X690] ITU-T, "Information technology - ASN.1 encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ISO/IEC 8825-1:2002, 2002.

6.2. Informative References

[MFSA201473] Delignat-Lavaud, A., "RSA Signature Forgery in NSS", September 2014, <https://www.mozilla.org/en-US/security/advisories/mfsa2014-73/>.

[POODLE] Moeller, B., "This POODLE bites: exploiting the SSL 3.0 fallback", October 2014, <https://security.googleblog.com/2014/10/this-poodle-bites-exploiting-ssl-30.html>.

[PRIVACY] Wachs, M., Scheitle, Q., and G. Carle, "Push away your privacy: Precise user tracking based on TLS client certificate authentication", 2017 Network Traffic Measurement and Analysis Conference (TMA), DOI 10.23919/tma.2017.8002897, June 2017.

Author's Address

David Benjamin
Google LLC

Email: davidben@google.com