[MS-WEBCRYPTO]:

Microsoft Edge Web Cryptography API Standards Support Document

---

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights**. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
- **Patents**. Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **License Programs**. To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.
- **Trademarks**. The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names**. The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Support. For questions and support, please contact dochelp@microsoft.com.

Revision Summary

Date	Revision History	Revision Class	Comments
4/25/2017	1.0	New	Released new document.
10/3/2017	1.0	None	No changes to the meaning, language, or formatting of the technical content.
2/22/2018	1.0	None	No changes to the meaning, language, or formatting of the technical content.
3/23/2018	1.0	None	No changes to the meaning, language, or formatting of the technical content.
8/28/2018	1.0	None	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction

This document describes the level of support provided by Microsoft Edge for the Web Cryptography API Recommendations [W3C-WEBCRYPTO], published 26 January 2017. The [W3C-WEBCRYPTO] specification describes a JavaScript API for performing basic cryptographic operations in web applications, such as hashing, signature generation and verification, and encryption and decryption.

1.1 Glossary

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as defined in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information.

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

[W3C-WEBCRYPTO] World Wide Web Consortium, "Web Cryptography API", W3C Recommendation 26 January 2017, https://www.w3.org/TR/2017/REC-WebCryptoAPI-20170126/

1.2.2 Informative References

None.

1.3 Microsoft Implementations

The following Microsoft web browsers implement some portion of the [W3C-WEBCRYPTO] specification:

- Microsoft Edge

Each browser version may implement multiple document rendering modes. The modes vary from one to another in support of the standard. The following table lists the document modes supported by each browser version.

Browser Version	Document Modes Supported
Microsoft Edge	EdgeHTML Mode

For each variation presented in this document there is a list of the document modes and browser versions that exhibit the behavior described by the variation. All combinations of modes and versions that are not listed conform to the specification. For example, the following list for a variation indicates that the variation exists in three document modes in all browser versions that support these modes:

Quirks Mode, IE7 Mode, and IE8 Mode (All Versions)

1.4 Standards Support Requirements

To conform to [W3C-WEBCRYPTO], a user agent must implement all required portions of the specification. Any optional portions that have been implemented must also be implemented as described by the specification. Normative language is usually used to define both required and optional portions. (For more information, see [RFC2119].)

The following table lists the sections of [W3C-WEBCRYPTO] and whether they are considered normative or informative.

Sections	Normative/Informative
1-7	Informative
8-18	Normative
19	Informative
Appendices A-C	Informative

1.5 Notation

The following notations are used in this document to differentiate between notes of clarification, variation from the specification, and points of extensibility.

Notation	Explanation
C####	This identifies a clarification of ambiguity in the target specification. This includes imprecise statements, omitted information, discrepancies, and errata. This does not include data formatting clarifications.
V####	This identifies an intended point of variability in the target specification such as the use of MAY, SHOULD, or RECOMMENDED. (See [RFC2119].) This does not include extensibility points.
E####	Because the use of extensibility points (such as optional implementation-specific data) can impair interoperability, this profile identifies such points in the target specification.

For document mode and browser version notation, see also section 1.3.

2 Standards Support Statements

This section contains all variations, clarifications, and extensions for the Microsoft implementation of [W3C-WEBCRYPTO].

- Section 2.1 describes normative variations from the MUST requirements of the specification.
- Section 2.2 describes clarifications of the MAY and SHOULD requirements.
- Section 2.3 describes extensions to the requirements.
- Section 2.4 considers error handling aspects of the implementation.
- Section 2.5 considers security aspects of the implementation.

2.1 Normative Variations

The following subsections describe normative variations from the MUST requirements of [W3C-WEBCRYPTO].

2.1.1 [MS-WEBCRYPTO] Section 10. Crypto interface

V0001: The crypto attribute is not exposed on WorkerGlobalScope

The specification states:

```
10. Crypto interface

    [NoInterfaceObject,Exposed=(Window,Worker)]
    interface GlobalCrypto {
        readonly attribute Crypto crypto;
    };
    ...
    WorkerGlobalScope implements GlobalCrypto;
```

EdgeHTML Mode

The `crypto` attribute is not exposed on `WorkerGlobalScope`.

2.1.2 [MS-WEBCRYPTO] Section 21. RSA-PSS

V0002: RSA-PSS is not supported

The specification states:

```
21. RSA-PSS
```

EdgeHTML Mode

RSA-PSS is not supported.

2.1.3 [MS-WEBCRYPTO] Section 23. ECDSA

V0003: ECDSA is not supported

The specification states:

```
23. ECDSA
```

EdgeHTML Mode

ECDSA is not supported.

2.1.4 [MS-WEBCRYPTO] Section 24. ECDH

V0004: ECDH is not suported

The specification states:

```
24. ECDH
```

EdgeHTML Mode

ECDH is not supported.

2.1.5 [MS-WEBCRYPTO] Section 25. AES-CTR

V0005: AES-CTR is not supported

The specification states:

```
25. AES-CTR
```

EdgeHTML Mode

AES-CTR is not supported.

2.1.6 [MS-WEBCRYPTO] Section 30. SHA

V0006: SHA-1 is not supported

The specification states:

```
30. SHA
```

EdgeHTML Mode

SHA-1 is not supported.

2.1.7 [MS-WEBCRYPTO] Section 31. HKDF

V0007: HKDF is not supported

The specification states:

```
31. HKDF
```

EdgeHTML Mode

HKDF is not supported.

2.1.8 [MS-WEBCRYPTO] Section 32. PBKDF2

V0008: PBKDF2 is not supported

The specification states:

```
32. PBKDF2
```

EdgeHTML Mode

PBKDF2 is not supported.

2.2 Clarifications

There are no clarifications of the MAY and SHOULD requirements of [W3C-WEBCRYPTO].

2.3 Extensions

There are no extensions to the requirements of [W3C-WEBCRYPTO].

2.4 Error Handling

There are no additional error handling considerations.

2.5 Security

There are no additional security considerations.

3 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

4 Index