```
Network Working Group                                          J. Hodges
Internet-Draft                                                    PayPal
Intended status: Informational                                 June 2016
Expires: December 3, 2016
```

Registries for Web Authentication (WebAuthn)
draft-hodges-webauthn-registries-00c

Abstract

This specification defines IANA registries for W3C Web Authentication [WebAuthn] attestation formats and extension identifiers.

Status of This Memo

Copyright Notice

Table of Contents

```
Network Working Group                                          J. Hodges
Internet-Draft                                                    PayPal
Intended status: Informational                                G. Mandyam
Expires: March 18, 2017                       Qualcomm Technologies Inc.
                                                      September 14, 2016
```

Registries for Web Authentication (WebAuthn)
draft-hodges-webauthn-registries-00c

Abstract

This specification defines IANA registries for W3C Web Authentication [WebAuthn] attestation formats and extension identifiers.

Status of This Memo

Copyright Notice

Table of Contents

/Users/jehodges/Documents/work/standards/W3C/webauthn/draft-hodges-webauthn-registries-00c.txt, Top line: 69

```
     4.2.  Initial WebAuthn Attestation Formats Registry Contents  .   5
     4.3.  Initial WebAuthn Extension Identifiers Registry Contents    5
   5.  Security Considerations . . . . . . . . . . . . . . . . . . .   7
   6.  Change Log  . . . . . . . . . . . . . . . . . . . . . . . . .   7
   7.  Acknowledgements  . . . . . . . . . . . . . . . . . . . . . .   7
   8.  Normative References  . . . . . . . . . . . . . . . . . . . .   7
   Author's Address  . . . . . . . . . . . . . . . . . . . . . . . .   7

1.  Introduction

   This specification defines IANA registries for W3C Web Authentication
   [WebAuthn] attestation formats and extension identifiers, and
   supplies initial entries within each registry.

2.  Registering WebAuthn Attestation Formats

   WebAuthn attestation format identifiers are strings whose semantic,
   syntactic, and string-matching criteria are specified in [WebAuthn],
   along with the concepts of attestation and attestation formats.

   WebAuthn attestation formats are registered on the advice of a
   Designated Expert (appointed by the IESG or their delegate), with a
   Specification Required (per [RFC5226]).

   The Expert(s) will establish procedures for requesting registrations,
   and make them available from the registry page.

   Registration requests consist of at least the following information:

   o  WebAuthn Attestation Format Identifier:
   o  Description: A relatively short description of the attestation
      format.
   o  Specification Document: Reference to the specification of the
      attestation format.
   o  Notes: [optional]

   The Expert(s) MAY define additional fields to be collected in the
   registry.  Each attestation format identifier added to this registry
   MUST be unique amongst the set of registered attestation format
   identifiers.


Hodges                  Expires December 3, 2016                [Page 2]

Internet-DraftRegistries for Web Authentication (WebAuthn)     June 2016




   See Section 4.2 for intial registrations, which may be used as
   examples for subsequent registrations.

   Registrations MUST reference a freely available specification, e.g.,
   as described in [RFC2026] Section 7.

   Note that WebAuthn attestation formats can be registered by third
   parties, if the Expert(s) determine that an unregistered attestation
   format is widely deployed and not likely to be registered in a timely
   manner.

   Decisions (or lack thereof) made by the Designated Expert can be
   first appealed to Application Area Directors (contactable using app-
   ads@tools.ietf.org email address or directly by looking up their
   email addresses on http://www.iesg.org/ website) and, if the
   appellant is not satisfied with the response, to the full IESG (using
   the iesg@iesg.org mailing list).
```

/Users/jehodges/Documents/work/standards/W3C/gmandyam/webauthn/draft-hodges-webauthn-registries-00c.txt, Top line: 69

```
     4.2.  Initial WebAuthn Attestation Formats Registry Contents  .   5
     4.3.  Initial WebAuthn Extension Identifiers Registry Contents    5
   5.  Security Considerations . . . . . . . . . . . . . . . . . . .   7
   6.  Change Log  . . . . . . . . . . . . . . . . . . . . . . . . .   7
   7.  Acknowledgements  . . . . . . . . . . . . . . . . . . . . . .   7
   8.  Normative References  . . . . . . . . . . . . . . . . . . . .   7
   Authors' Addresses  . . . . . . . . . . . . . . . . . . . . . . .   8

1.  Introduction

   This specification defines IANA registries for W3C Web Authentication
   [WebAuthn] attestation formats and extension identifiers, and
   supplies initial entries within each registry.

2.  Registering WebAuthn Attestation Formats

   WebAuthn attestation format identifiers are strings whose semantic,
   syntactic, and string-matching criteria are specified in [WebAuthn],
   along with the concepts of attestation and attestation formats.

   WebAuthn attestation formats are registered on the advice of a
   Designated Expert (appointed by the IESG or their delegate), with a
   Specification Required (per [RFC5226]).

   The Expert(s) will establish procedures for requesting registrations,
   and make them available from the registry page.

   Registration requests consist of at least the following information:

   o  WebAuthn Attestation Format Identifier:
   o  Description: A relatively short description of the attestation
      format.
   o  Specification Document: Reference to the specification of the
      attestation format.
   o  Notes: [optional]

   The Expert(s) MAY define additional fields to be collected in the
   registry.  Each attestation format identifier added to this registry
   MUST be unique amongst the set of registered attestation format
   identifiers.  The Experts(s) MAY also designate attestation formats


Hodges & Mandyam         Expires March 18, 2017                 [Page 2]

Internet-DraftRegistries for Web Authentication (WebAuthn)September 2016


   as proprietary if they lack complete specifications, and will assign
   a prefix indicating as such to the identifier.

   See Section 4.2 for intial registrations, which may be used as
   examples for subsequent registrations.

   Registrations MUST reference a freely available specification, e.g.,
   as described in [RFC2026] Section 7.

   Note that WebAuthn attestation formats can be registered by third
   parties, if the Expert(s) determine that an unregistered attestation
   format is widely deployed and not likely to be registered in a timely
   manner.

   Decisions (or lack thereof) made by the Designated Expert can be
   first appealed to Application Area Directors (contactable using app-
   ads@tools.ietf.org email address or directly by looking up their
   email addresses on http://www.iesg.org/ website) and, if the
   appellant is not satisfied with the response, to the full IESG (using
   the iesg@iesg.org mailing list).
```

3. Registering WebAuthn Extension Identifiers

WebAuthn extension identifiers are strings whose semantic, syntactic, and string-matching criteria are specified in [WebAuthn].

WebAuthn extension identifiers are registered on the advice of a Designated Expert (appointed by the IESG or their delegate), with a Specification Required (per [RFC5226]).

The Expert(s) will establish procedures for requesting registrations, and make them available from the registry page.

Registration requests consist of at least the following information:

- o WebAuthn Extension Identifier:
- o Description: A relatively short description of the extension.
- o Specification Document: Reference to the specification of the extension.
- o Notes: [optional]

The Expert(s) MAY define additional fields to be collected in the registry. Each extension identifier added to this registry MUST be unique amongst the set of registered extension identifiers.

See Section 4.3 for intial registrations, which may be used as examples for subsequent registrations.

Registrations MUST reference a freely available specification, e.g., as described in [RFC2026] Section 7.

Note that WebAuthn extensions can be registered by third parties, if the Expert(s) determine that an unregistered extension is widely deployed and not likely to be registered in a timely manner.

Decisions (or lack thereof) made by the Designated Expert can be first appealed to Application Area Directors (contactable using app-ads@tools.ietf.org email address or directly by looking up their email addresses on http://www.iesg.org/ website) and, if the appellant is not satisfied with the response, to the full IESG (using the iesg@iesg.org mailing list).

4. IANA Considerations

4.1. WebAuthn Attestation Formats and Extension Identifiers Registries

This specification establishes two registries:

- o the WebAuthn Attestation Formats registry; see Section 2. Initial registry contents are given in Section 4.2.
- o the WebAuthn Extension Identifiers registry; see Section 3. Initial registry contents are given in Section 4.3.

For both registries, the Expert(s) and IANA will interact as outlined below:

IANA will direct any incoming requests regarding the registry to the processes established by the Expert(s); typically, this will mean

3. Registering WebAuthn Extension Identifiers

WebAuthn extension identifiers are strings whose semantic, syntactic, and string-matching criteria are specified in [WebAuthn].

WebAuthn extension identifiers are registered on the advice of a Designated Expert (appointed by the IESG or their delegate), with a Specification Required (per [RFC5226]).

The Expert(s) will establish procedures for requesting registrations, and make them available from the registry page.

Registration requests consist of at least the following information:

o WebAuthn Extension Identifier:
o Description: A relatively short description of the extension.
o Specification Document: Reference to the specification of the extension.
o Notes: [optional]

The Expert(s) MAY define additional fields to be collected in the registry. Each extension identifier added to this registry MUST be unique amongst the set of registered extension identifiers.

See Section 4.3 for intial registrations, which may be used as examples for subsequent registrations.

Registrations MUST reference a freely available specification, e.g., as described in [RFC2026] Section 7.

Note that WebAuthn extensions can be registered by third parties, if the Expert(s) determine that an unregistered extension is widely deployed and not likely to be registered in a timely manner.

Decisions (or lack thereof) made by the Designated Expert can be first appealed to Application Area Directors (contactable using app-ads@tools.ietf.org email address or directly by looking up their email addresses on http://www.iesg.org/ website) and, if the appellant is not satisfied with the response, to the full IESG (using the iesg@iesg.org mailing list).

4. IANA Considerations

4.1. WebAuthn Attestation Formats and Extension Identifiers Registries

This specification establishes two registries:

o the WebAuthn Attestation Formats registry; see Section 2. Initial registry contents are given in Section 4.2.
o the WebAuthn Extension Identifiers registry; see Section 3. Initial registry contents are given in Section 4.3.

For both registries, the Expert(s) and IANA will interact as outlined below:

IANA will direct any incoming requests regarding the registry to the processes established by the Expert(s); typically, this will mean

```
   referring them to the registry HTML page.

   The Expert(s) will provide registry data to IANA in an agreed form
   (e.g. a specific XML format).  IANA will publish:

   o  The raw registry data
   o  The registry data, transformed into HTML
   o  The registry data in any alternative formats provided by the
      Expert(s)

   Each published document will be at a URL agreed to by IANA and the
   Expert(s), and IANA will set HTTP response headers on them as
   (reasonably) requested by the Expert(s).

   Additionally, the HTML generated by IANA will:

   o  Take directions from the Expert(s) as to the content of the HTML
      page's introductory text and markup
   o  Include a stable HTML fragment identifier for each registered
      attestation format or extension identifier



Hodges                  Expires December 3, 2016                [Page 4]

Internet-DraftRegistries for Web Authentication (WebAuthn)     June 2016




   All registry data documents MUST include Simplified BSD License text
   as described in Section 4.e of the Trust Legal Provisions
   (<http://trustee.ietf.org/license-info>).

4.2.  Initial WebAuthn Attestation Formats Registry Contents

   The WebAuthn Attestation Formats registry's initial contents are:

      WebAuthn Attestation Formats: packed
      Description: The "packed" attestation format is a WebAuthn-
      optimized format for attestation data.  It uses a very compact but
      still extensible encoding method.  This format is implementable by
      authenticators with limited resources (e.g., secure elements).
      Specification Document: [WebAuthn]


      WebAuthn Attestation Formats: tpm
      Description: The TPM attestation format returns an attestation
      statement in the same format as the packed attestation format,
      although the the rawData and signature fields are computed
      differently.
      Specification Document: [WebAuthn]


      WebAuthn Attestation Formats: android
      Description: Android-based, platform-provided authenticators may
      produce an attestation statement based on the Android SafetyNet
      API.
      Specification Document: [WebAuthn]


      WebAuthn Attestation Formats: android2
      Description: Platform-provided authenticators based on Android
      versions "N", and later, may provide a "hardware attestation"
      statement.
```

```
   referring them to the registry HTML page.

   The Expert(s) will provide registry data to IANA in an agreed form
   (e.g. a specific XML format).  IANA will publish:

   o  The raw registry data
   o  The registry data, transformed into HTML
   o  The registry data in any alternative formats provided by the
      Expert(s)

   Each published document will be at a URL agreed to by IANA and the
   Expert(s), and IANA will set HTTP response headers on them as
   (reasonably) requested by the Expert(s).

   Additionally, the HTML generated by IANA will:








Hodges & Mandyam          Expires March 18, 2017                [Page 4]

Internet-DraftRegistries for Web Authentication (WebAuthn)September 2016


   o  Take directions from the Expert(s) as to the content of the HTML
      page's introductory text and markup
   o  Include a stable HTML fragment identifier for each registered
      attestation format or extension identifier

   All registry data documents MUST include Simplified BSD License text
   as described in Section 4.e of the Trust Legal Provisions
   (<http://trustee.ietf.org/license-info>).

4.2.  Initial WebAuthn Attestation Formats Registry Contents

   The WebAuthn Attestation Formats registry's initial contents are:

      WebAuthn Attestation Formats: packed
      Description: The "packed" attestation format is a WebAuthn-
      optimized format for attestation data.  It uses a very compact but
      still extensible encoding method.  This format is implementable by
      authenticators with limited resources (e.g., secure elements).
      Specification Document: [WebAuthn]


      WebAuthn Attestation Formats: tpm
      Description: The TPM attestation format returns an attestation
      statement in the same format as the packed attestation format,
      although the the rawData and signature fields are computed
      differently.
      Specification Document: [WebAuthn]


      WebAuthn Attestation Formats: goog-android
      Description: Android-based, platform-provided authenticators may
      produce an attestation statement based on the Android SafetyNet
      API.
      Specification Document: [AndroidSafetyNet]


      WebAuthn Attestation Formats: goog-android2
      Description: Platform-provided authenticators based on Android
      versions "N", and later, may provide this proprietary "hardware
      attestation" statement.
```

Specification Document: [AndroidHWAttstn]

4.3. Initial WebAuthn Extension Identifiers Registry Contents

The WebAuthn Extension Identifiers registry's initial contents are:

WebAuthn Extension Identifier: webauthn_txAuthSimple
Description: This signature extension allows for a simple form of transaction authorization. A WebAuthn Relying Party can specify a prompt string, intended for display on a trusted device on the authenticator
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_txAuthGeneric
Description: This generic txauth extension allows images to be used as prompts as well. This allows authenticators without a font rendering engine to be used and also supports a richer visual appearance than accomplished with the webauthn.txauth.simple extension.
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_authnSel
Description: This registration extension allows a WebAuthn Relying Party to guide the selection of the authenticator that will be leveraged when creating the credential. It is intended primarily for WebAuthn Relying Parties that wish to tightly control the experience around credential creation.
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_exts
Description: The Supported Extensions extension data is a list (CBOR array) of extension identifiers encoded as UTF-8 Strings. This extension is added automatically by the authenticator. This extension can be added to attestation statements.
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_uvi
Description: The user verification index (UVI) is a value uniquely identifying a user verification data record. The UVI data can be used by servers to understand whether an authentication was authorized by the exact same biometric data as the initial key generation. This allows the detection and prevention of "friendly fraud".
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_loc
Description: The location extension provides the client device's current location to the WebAuthn relying party, if supported by the client device and subject to user consent.

Specification Document: [AndroidHWAttstn]

4.3. Initial WebAuthn Extension Identifiers Registry Contents

The WebAuthn Extension Identifiers registry's initial contents are:

WebAuthn Extension Identifier: webauthn_txAuthSimple

Description: This signature extension allows for a simple form of transaction authorization. A WebAuthn Relying Party can specify a prompt string, intended for display on a trusted device on the authenticator
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_txAuthGeneric
Description: This generic txauth extension allows images to be used as prompts as well. This allows authenticators without a font rendering engine to be used and also supports a richer visual appearance than accomplished with the webauthn.txauth.simple extension.
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_authnSel
Description: This registration extension allows a WebAuthn Relying Party to guide the selection of the authenticator that will be leveraged when creating the credential. It is intended primarily for WebAuthn Relying Parties that wish to tightly control the experience around credential creation.
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_exts
Description: The Supported Extensions extension data is a list (CBOR array) of extension identifiers encoded as UTF-8 Strings. This extension is added automatically by the authenticator. This extension can be added to attestation statements.
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_uvi
Description: The user verification index (UVI) is a value uniquely identifying a user verification data record. The UVI data can be used by servers to understand whether an authentication was authorized by the exact same biometric data as the initial key generation. This allows the detection and prevention of "friendly fraud".
Specification Document: [WebAuthn]

WebAuthn Extension Identifier: webauthn_loc
Description: The location extension provides the client device's current location to the WebAuthn relying party, if supported by the client device and subject to user consent.

```
      Specification Document: [WebAuthn]




      WebAuthn Extension Identifier: webauthn_uvm
      Description: The user verification mode (UVM) extension returns to
      the Webauthn relying party which user verification methods
      (factors) were used for the WebAuthn operation.
      Specification Document: [WebAuthn]



Hodges                   Expires December 3, 2016                [Page 6]

Internet-DraftRegistries for Web Authentication (WebAuthn)      June 2016


5.  Security Considerations

   See [WebAuthn] for relevant security considerations.

6.  Change Log

   Note to RFC Editor: Please remove this section before publication.

   This is the initial -00 rev of this spec, hence no changes to log
   here at this time.

7.  Acknowledgements

   Thanks to Mark Nottingham for valuable comments and suggestions.

8.  Normative References

   [AndroidHWAttstn]
              Google, "Android Hardware Attestation", Andorid Developers
              Reference   , 2016,
              <https://developer.android.com/reference/android/
              security/>.




   [RFC2026]  Bradner, S., "The Internet Standards Process -- Revision
              3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996,
              <http://www.rfc-editor.org/info/rfc2026>.

   [RFC5226]  Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              DOI 10.17487/RFC5226, May 2008,
              <http://www.rfc-editor.org/info/rfc5226>.

   [WebAuthn]
              Bharadwaj, V., Le Van Gong, H., Balfanz, D., Czeskis, A.,
              Birgisson, A., Hodges, J., Jones, M., and R. Lindemann,
              "Web Authentication: An API for accessing Scoped
              Credentials", World Wide Web Consortium (W3C)
              Recommendation-track, May 2016, <https://www.w3.org/TR/
              webauthn/>.

Author's Address
```

```
      Specification Document: [WebAuthn]
```

```
Hodges & Mandyam         Expires March 18, 2017                  [Page 6]

Internet-DraftRegistries for Web Authentication (WebAuthn)September 2016
```

```
      WebAuthn Extension Identifier: webauthn_uvm
      Description: The user verification mode (UVM) extension returns to
      the Webauthn relying party which user verification methods
      (factors) were used for the WebAuthn operation.
      Specification Document: [WebAuthn]

5.  Security Considerations

   See [WebAuthn] for relevant security considerations.

6.  Change Log

   Note to RFC Editor: Please remove this section before publication.

   This is the initial -00 rev of this spec, hence no changes to log
   here at this time.

7.  Acknowledgements

   Thanks to Mark Nottingham for valuable comments and suggestions.

8.  Normative References

   [AndroidHWAttstn]
              Google, "Android Hardware Attestation", Andorid Developers
              Reference   , 2016,
              <https://developer.android.com/reference/android/
              security/>.
```

```
   [AndroidSafetyNet]
              Google, "Android SafetyNet Attestation", 2016,
              <https://developer.android.com/training/safetynet/
              index.html>.
```

```
   [RFC2026]  Bradner, S., "The Internet Standards Process -- Revision
              3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996,
              <http://www.rfc-editor.org/info/rfc2026>.

   [RFC5226]  Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              DOI 10.17487/RFC5226, May 2008,
              <http://www.rfc-editor.org/info/rfc5226>.
```

```
Hodges                    Expires December 3, 2016                [Page 7]

Internet-DraftRegistries for Web Authentication (WebAuthn)     June 2016


   Jeff Hodges
   PayPal
   2211 North First Street
   San Jose, California  95131
   US

   Email: Jeff.Hodges@PayPal.com
```

```
Hodges & Mandyam         Expires March 18, 2017                 [Page 7]

Internet-DraftRegistries for Web Authentication (WebAuthn)September 2016


   [WebAuthn]
              Bharadwaj, V., Le Van Gong, H., Balfanz, D., Czeskis, A.,
              Birgisson, A., Hodges, J., Jones, M., and R. Lindemann,
              "Web Authentication: An API for accessing Scoped
              Credentials", World Wide Web Consortium (W3C)
              Recommendation-track, May 2016, <https://www.w3.org/TR/
              webauthn/>.

Authors' Addresses

   Jeff Hodges
   PayPal
   2211 North First Street
   San Jose, California  95131
   US

   Email: Jeff.Hodges@PayPal.com


   Giridhar Mandyam
   Qualcomm Technologies Inc.
   5775 Morehouse Drive
   San Diego, California  92121
   USA

   Phone: +1 858 651 7200
   Email: mandyam@qti.qualcomm.com.com
```

```
Hodges & Mandyam         Expires March 18, 2017                 [Page 8]
Hodges                    Expires December 3, 2016                [Page 8]
```