Abstract

The goal of the Universal Authentication Framework is to provide a unified and extensible authentication mechanism that supplants passwords while avoiding the shortcomings of current alternative authentication approaches.

This approach is designed to allow the relying party to choose the best available authentication mechanism for a particular end user or interaction, while preserving the option to leverage emerging device security capabilities in the future without requiring additional integration effort.

This document describes the FIDO architecture in detail, it defines the flow and content of all UAF protocol messages and presents the rationale behind the design choices.

Status of This Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current FIDO Alliance publications and the latest revision of this technical report can be found in the FIDO Alliance specifications index at

https://www.fidoalliance.org/specifications/

This document was published by the FIDO Alliance as a Implementation Draft. This document is intended to become a FIDO Alliance Proposed Standard. If you wish to make comments regarding this document, please Contact Us. All comments are welcome.

This Implementation Draft Specification has been prepared by FIDO Alliance, Inc. Permission is hereby granted to use the Specification solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this Specification for other uses must contact the FIDO Alliance to determine whether an appropriate license for such use is available.

Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The FIDO Alliance, Inc. and its Members and any other contributors to the Specification are not, and shall not be held, responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

THIS FIDO ALLIANCE SPECIFICATION IS PROVIDED “AS IS” AND WITHOUT ANY WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

1. Notation
   1.1 Key Words
2. Overview
   2.1 Scope
   2.2 Architecture
2.3 Protocol Conversation
   2.3.1 Registration
   2.3.2 Authentication
   2.3.3 Transaction Confirmation
   2.3.4 Deregistration
3. Protocol Details
   3.1 Shared Structures and Types
      3.1.1 Version Interface
      3.1.1.1 Attributes
3.1.2 Operation enumeration
3.1.3 OperationHeader dictionary
  3.1.3.1 Dictionary OperationHeader Members
3.1.4 Authenticator Attestation ID (AAID) typedef
3.1.5 KeyID typedef
3.1.6 ServerChallenge typedef
3.1.7 FinalChallengeParams dictionary
  3.1.7.1 Dictionary FinalChallengeParams Members
3.1.8 TLS ChannelBinding dictionary
  3.1.8.1 Dictionary ChannelBinding Members
3.1.9 JwkKey dictionary
  3.1.9.1 Dictionary JwkKey Members
3.1.10 Extension dictionary
  3.1.10.1 Dictionary Extension Members
3.1.11 MatchCriteria dictionary
  3.1.11.1 Dictionary MatchCriteria Members
3.1.12 Policy dictionary
  3.1.12.1 Dictionary Policy Members
3.2 Processing Rules for the Server Policy
  3.2.1 Examples
3.3 Version Negotiation
3.4 Registration Operation
  3.4.1 Registration Request Message
    3.4.2 RegistrationRequest dictionary
      3.4.2.1 Dictionary RegistrationRequest Members
3.4.3 AuthenticatorRegistrationAssertion dictionary
  3.4.3.1 Dictionary AuthenticatorRegistrationAssertion Members
3.4.4 Registration Response Message
3.4.5 RegistrationResponse dictionary
  3.4.5.1 Dictionary RegistrationResponse Members
3.4.6 Registration Processing Rules
  3.4.6.1 Registration Request Generation Rules for FIDO Server
  3.4.6.2 Registration Request Processing Rules for FIDO UAF Clients
  3.4.6.3 Registration Request Processing Rules for FIDO Authenticator
  3.4.6.4 Registration Response Generation Rules for FIDO UAF Client
  3.4.6.5 Registration Response Processing Rules for FIDO Server
3.5 Authentication Operation
  3.5.1 Transaction dictionary
    3.5.1.1 Dictionary Transaction Members
3.5.2 Authentication Request Message
3.5.3 AuthenticationRequest dictionary
  3.5.3.1 Dictionary AuthenticationRequest Members
3.5.4 AuthenticatorSignAssertion dictionary
  3.5.4.1 Dictionary AuthenticatorSignAssertion Members
3.5.5 AuthenticationResponse dictionary
  3.5.5.1 Dictionary AuthenticationResponse Members
3.5.6 Authentication Response Message
3.5.7 Authentication Processing Rules
  3.5.7.1 Authentication Request Generation Rules for FIDO Server
  3.5.7.2 Authentication Request Processing Rules for FIDO UAF Client
  3.5.7.3 Authentication Request Processing Rules for FIDO Authenticator
  3.5.7.4 Authentication Response Generation Rules for FIDO UAF Client
  3.5.7.5 Authentication Response Processing Rules for FIDO Server
3.6 Deregistration Operation
  3.6.1 Deregistration Request Message
3.6.2 DeregisterAuthenticator dictionary
  3.6.2.1 Dictionary DeregisterAuthenticator Members
3.6.3 DeregistrationRequest dictionary
  3.6.3.1 Dictionary DeregistrationRequest Members
3.6.4 Deregistration Processing Rules
  3.6.4.1 Deregistration Request Generation Rules for FIDO Server
  3.6.4.2 Deregistration Request Processing Rules for FIDO UAF Client
  3.6.4.3 Deregistration Request Processing Rules for FIDO Authenticator

4. Considerations
  4.1 Protocol Core Design Considerations
    4.1.1 Authenticator Metadata
      4.1.2 Authenticator Attestation
        4.1.2.1 Basic Attestation
          4.1.2.1.1 Full Basic Attestation
          4.1.2.1.2 Surrogate Basic Attestation
    4.1.3 Error Handling
1. Notation

Type names, attribute names and element names are written as `code`.

String literals are enclosed in `"`, e.g. "UAF-TLV".

In formulas we use `I` to denote byte wise concatenation operations.

The notation base64url refers to "Base 64 Encoding with URL and Filename Safe Alphabet" [RFC4648] without padding.

Following [WebIDL-ED], dictionary members are optional unless they are explicitly marked as `required`.

WebIDL dictionary members `must not` have a value of null.

Unless otherwise specified, if a WebIDL dictionary member is a `DOMString`, it `must not` be empty.

Unless otherwise specified, if a WebIDL dictionary member is a `List`, it `must not` be an empty list.

UAF specific terminology used in this document is defined in [FIDO glossary].

All diagrams, examples, notes in this specification are non-normative.

精彩的注释显示，某些字典成员需要在order to comply with FIDO requirements. Such members are marked in the WebIDL definitions found in this document, as `required`. The keyword `required` has been introduced by [WebIDL-ED], which is a work-in-progress. If you are using a WebIDL parser which implements [WebIDL], then you may remove the keyword `required` from your WebIDL and use other means to ensure those fields are present.

### 1.1 Key Words

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in [RFC2119].

2. Overview

This section is non-normative.

The goal of this Universal Authentication Framework is to provide a unified and extensible authentication mechanism that supplants passwords while avoiding the shortcomings of current alternative authentication approaches.

The design goal of the protocol is to enable Relying Parties to leverage the diverse and heterogeneous set of security capabilities available on end users' devices via a single, unified protocol.

This approach is designed to allow the FIDO Relying Parties to choose the best available authentication mechanism for a particular end user or interaction, while preserving the option for a relying party to leverage emerging device security capabilities in the future, without requiring additional integration effort.

2.1 Scope

This document describes FIDO architecture in detail and defines the UAF protocol as a network protocol. It defines the flow and content of all UAF messages and presents the rationale behind the design choices.
Particular application-level bindings are outside the scope of this document. This document is not intended to answer questions such as:

- What does an HTTP binding look like for UAF?
- How can a web application communicate to FIDO UAF Client?
- How can FIDO UAF Client communicate to FIDO enabled Authenticators?

The answers to these questions can be found in other UAF specifications, e.g. [UAFAppAPIAndTransport] [UAFASM] [UAFAuthnrCommands].

2.2 Architecture

The following diagram depicts the entities involved in UAF protocol.

![Diagram of UAF Architecture]

Of these entities, only these three directly create and/or process UAF protocol messages:

- FIDO Server, running on the relying party's infrastructure
- FIDO UAF Client, part of the user agent and running on the FIDO user device
- FIDO Authenticator, integrated into the FIDO user device

It is assumed in this document that a FIDO Server has access to the UAF Authenticator Metadata [UAFAuthnrMetadata] describing all the authenticators it will interact with.

2.3 Protocol Conversation

The core UAF protocol consists of four conceptual conversations between a FIDO UAF Client and FIDO Server.

- **Registration**: UAF allows the relying party to register a FIDO Authenticator with the user's account at the relying party. The relying party can specify a policy for supporting various FIDO Authenticator types. A FIDO UAF Client will only register existing authenticators in accordance with that policy.

- **Authentication**: UAF allows the relying party to prompt the end user to authenticate using a previously registered FIDO Authenticator. This authentication can be invoked any time, at the relying party's discretion.

- **Transaction Confirmation**: In addition to providing a general authentication prompt, UAF offers support for prompting the user to confirm a specific transaction.

  This prompt includes the ability to communicate additional information to the client for display to the end user, using the client's transaction confirmation display. The goal of this additional authentication operation is to enable relying parties to ensure that the user is confirming a specified set of the transaction details (instead of authenticating a session to the user agent).

- **Deregistration**: The relying party can trigger the deletion of the account-related authentication key material.

Although this document defines the FIDO Server as the initiator of requests, in a real world deployment the first UAF operation will always follow a user agent's (e.g. HTTP) request to a relying party.

The following sections give a brief overview of the protocol conversation for individual operations. More detailed descriptions can be found in the sections Registration Operation, Authentication Operation, and Deregistration Operation.

2.3.1 Registration

The following diagram shows the message flows for Registration.
2.3.2 Authentication

The following diagram depicts the message flows for the authentication operation.

![UAF Registration Message Flow Diagram](image)

**NOTE**

The client application should use the appropriate API to inform the FIDO UAF Client of the results of the operation (see section 2.3.1 in [UAFAppAPIAndTransport]) in order to allow the FIDO UAF Client to do some "housekeeping" tasks.

2.3.3 Transaction Confirmation

The following figure depicts the transaction confirmation message flow.

![Authentication Message Flow Diagram](image)

**NOTE**

The client application should use the appropriate API to inform the FIDO UAF Client of the results of the operation (see section 2.3.1 in [UAFAppAPIAndTransport]) in order to allow FIDO UAF Client to do some "housekeeping" tasks.
2.3.4 Deregistration

The following diagram depicts the deregistration message flow.

![Deregistration Message Flow Diagram](image)

**NOTE**

The client application should use the appropriate API to inform the FIDO UAF Client of the results of the operation (see section 2.3.1 in [UAFAppAPIAndTransport]) in order to allow the FIDO UAF Client to do some “housekeeping” tasks.

3. Protocol Details

*This section is normative.*

This section provides a detailed description of operations supported by the UAF Protocol.

Support of all protocol elements is mandatory for conforming software, unless stated otherwise.

All string literals in this specification are constructed from Unicode codepoints within the set U+0000..U+007F.

Unless otherwise specified, protocol messages are transferred with a UTF-8 content encoding.

**NOTE**

All data used in this protocol must be exchanged using a secure transport protocol (such as TLS/HTTPS) established between the FIDO UAF Client and the relying party in order to follow the assumptions made in [FIDOSecRef]; details are specified in section **4.1 TLS Protected Communication**.

The notation base64url(byte[8..64]) reads as 8-64 bytes of data encoded in base64url, “Base 64 Encoding with URL and Filename Safe Alphabet” [RFC4648] without padding.

The notation string[5] reads as five unicode characters, represented as a UTF-8 [RFC3629] encoded string of the type indicated in the declaration, typically a WebIDL [WebIDL-ED] DOMString.

As the UTF-8 representation has variable length, the *maximum* byte length of `string[5]` is `string[4+5]`.

All strings are case-sensitive unless stated otherwise.
This document uses WebIDL [WebIDL-ED] to define UAF protocol messages.
Implementations must serialize the UAF protocol messages for transmission using UTF-8 encoded JSON [RFC4627].

3.1 Shared Structures and Types

This section defines types and structures shared by various operations.

### 3.1.1 Version Interface

Represents a generic version with major and minor fields.

```webidl
interface Version {
  readonly attribute unsigned short major;
  readonly attribute unsigned short minor;
}
```

#### 3.1.1.1 Attributes

- **major** of type unsigned short, readonly:
  Major version, 1 for this specification.

- **minor** of type unsigned short, readonly:
  Minor version, 0 for this specification.

### 3.1.2 Operation enumeration

Describes the operation type of a UAF message or request for a message.

```webidl
enum Operation {
  "Reg",
  "Auth",
  "Dereg"
}
```

#### Enumeration description

- **Reg**: Registration
- **Auth**: Authentication or Transaction Confirmation
- **Dereg**: Deregistration

### 3.1.3 OperationHeader dictionary

Represents a UAF message Request and Response header.

```webidl
dictionary OperationHeader {
  required Version upv;
  required Operation op;
  DOMString appID;  // string[0..512]. The application identifier that the relying party would like to assert.
  DOMString serverData;  // string.
  Extension[] exts;
}
```

#### 3.1.3.1 Dictionary OperationHeader Members

- **upv** of type required Version:
  UAF protocol version. Major version must be 1 and minor version must be 0.

- **op** of type required Operation:
  Name of FIDO operation this message relates to.

```webidl
NOTE
"Auth" is used for both authentication and transaction confirmation.
```

- **appID** of type DOMString:
  string[0..512]. The application identifier that the relying party would like to assert. There are three ways to set the appID [FIDOAppIDAndFacets]:

  1. If the element is missing or empty in the request, the FIDO UAF Client must set it to the FacetID of the caller.
  2. If the appID present in the message is identical to the FacetID of the caller, the FIDO UAF Client must accept it.
  3. If it is an URI with HTTPS protocol scheme, the FIDO UAF Client must use it to load the list of trusted facet identifiers from the specified URI. The FIDO UAF Client must only accept the request, if the facet identifier of the caller matches one of the trusted facet identifiers in the list returned from dereferencing this URI.

```webidl
NOTE
```
The new key pair that the authenticator generates will be associated with this application identifier.

**Security Relevance:** The application identifier is used by the FIDO UAF Client to verify the eligibility of an application to trigger the use of a specific `Auth.Key`. See [FIDOAppIDAndFacets](#).

---

**serverData** of type DOMString

```
string[1..1536].
```

A session identifier created by the relying party.

**NOTE**

The relying party can opaque store things like expiration times for the registration session, protocol version used and other useful information in `serverData`. This data is opaque to FIDO UAF Clients. FIDO Servers may reject a response that is lacking this data or is containing unauthorized modifications to it.

Servers that depend on the integrity of `serverData` should apply appropriate security measures, as described in Registration Request Generation Rules for FIDO Server and section ServerData and KeyHandle.

---

**exts** of type array of Extension

List of UAF Message Extensions.

### 3.1.4 Authenticator Attestation ID (AAID) typedef

```webidl
typedef DOMString AAID;
```

```
string[9]
```

Each authenticator must have an AAID to identify UAF enabled authenticator models globally. The AAID must uniquely identify a specific authenticator model within the range of all UAF-enabled authenticator models made by all authenticator vendors, where authenticators of a specific model must share identical security characteristics within the model (see Security Considerations).

The AAID is a string with format "V#M", where

- "#" is a separator
- "V" indicates the authenticator Vendor Code. This code consists of 4 hexadecimal digits.
- "M" indicates the authenticator Model Code. This code consists of 4 hexadecimal digits.

The Augmented BNF [ABNF] for the AAID is:

```
AAID = 4(HEXDIG) "#" 4(HEXDIG)
```

**NOTE**

HEXDIG is case insensitive, i.e. "03EF" and "03ef" are identical.

The FIDO Alliance is responsible for assigning authenticator vendor Codes.

Authenticator vendors are responsible for assigning authenticator model codes to their authenticators. Authenticator vendors must assign unique AAIDs to authenticators with different security characteristics.

AAIDs are unique and each of them must relate to a distinct authentication metadata file ([UAFAuthnrMetadata](#)).

**NOTE**

Adding new firmware/software features, or changing the underlying hardware protection mechanisms will typically change the security characteristics of an authenticator and hence would require a new AAID to be used. Refer to ([UAFAuthnrMetadata](#)) for more details.

### 3.1.5 KeyID typedef

```webidl
typedef DOMString KeyID;
```

```
base64url(byte[32...2048])
```

KeyID is a unique identifier (within the scope of an `Auth.Key`) used to refer to a specific `Auth.Key`. It is generated by the authenticator and registered with a FIDO Server.

The `(AAID, KeyID)` tuple must uniquely identify an authenticator's registration for a relying party. Whenever a FIDO Server wants to provide specific information to a particular authenticator it must use the `(AAID, KeyID)` tuple.

KeyID must be base64url encoded within the UAF message (see above).

During step-up authentication and deregistration operations, the FIDO Server should provide the KeyID back to the authenticator for the latter to locate the appropriate user authentication key, and perform the necessary operation with it.

Roaming authenticators which don't have internal storage for, and cannot rely on any ASM to store, generated key handles should provide the key handle as part of the `AuthenticatorRegistrationAssertion.asserion.KeyID` during the registration operation (see also section ServerData and KeyHandle) and get the key handle back from the FIDO Server during the step-up authentication (in the `MatchCriteria` dictionary which is part of the policy) or deregistration operations (see [UAFAuthnrCommands](#)) for more details.)
3.1.6 ServerChallenge typedef

```webidl
typedef DOMString ServerChallenge;
```

`ServerChallenge` is a server-provided random challenge. **Security Relevance:** The challenge is used by the FIDO Server to verify whether an incoming response is new, or has already been processed. See section [Replay Attack Protection](#) for more details.

The `ServerChallenge` should be mixed into the entropy pool of the authenticator. **Security Relevance:** The FIDO Server should provide a challenge containing strong cryptographic randomness whenever possible. See section [Server Challenge and Random Numbers](#).

3.1.7 FinalChallengeParams dictionary

```webidl
dictionary FinalChallengeParams {
  required DOMString appID;
  required ServerChallenge challenge;
  required DOMString facetID;
  required ChannelBinding channelBinding;
};
```

3.1.7.1 Dictionary `FinalChallengeParams` Members

- **appID** of type `required DOMString` `string[1..512]`
  - The value must be taken from the `appID` field of the `OperationHeader`.

- **challenge** of type `required ServerChallenge` `DOMString`
  - The value must be taken from the challenge field of the request (e.g. `RegistrationRequest.challenge`, `AuthenticationRequest.challenge`).

- **facetID** of type `required DOMString` `string[1..512]`
  - The value is determined by the FIDO UAF Client and it depends on the calling application. See [FIDOAppIDAndFacets](#) for more details. **Security Relevance:** The `facetID` is determined by the FIDO UAF Client and verified against the list of trusted facets retrieved by dereferencing the `appID` of the calling application.

- **channelBinding** of type `required ChannelBinding`
  - Contains the TLS information to be sent by the FIDO Client to the FIDO Server, binding the TLS channel to the FIDO operation.

3.1.8 TLS ChannelBinding dictionary

`ChannelBinding` contains channel binding information ([RFC5056](#)).

NOTE

- **Security Relevance:** The channel binding may be verified by the FIDO Server in order to detect and prevent MITM attacks.

At this time, the following channel binding methods are supported:

- `TLS ChannelID` ([id_pubkey](#)) `ChannelID`
- `serverEndPoint` ([RFC5929](#))
- `tlsServerCertificate` ([RFC5929](#))
- `tlsUnique` ([RFC5929](#))

Further requirements:
1. If data related to any of the channel binding methods, described here, is available to the FIDO UAF Client (i.e. included in this dictionary), it must be used according to the relevant specification.

2. All channel binding methods described here must be supported by the FIDO Server. The FIDO Server may reject operations if the channel binding cannot be verified successfully.

**NOTE**

- If channel binding data is accessible to the web browser or client application, it must be relayed to the FIDO UAF Client in order to follow the assumptions made in [FIDOSecRef].
- If channel binding data is accessible to the web server, it must be relayed to the FIDO Server in order to follow the assumptions made in [FIDOSecRef]. The FIDO Server relies on the web server to provide accurate channel binding information.

### WebIDL

```webidl
dictionary ChannelBinding {
    DOMString serverEndPoint;
    DOMString tlsServerCertificate;
    DOMString tlsUnique;
    DOMString cid_pubkey;
}
```

#### 3.1.8.1 Dictionary ChannelBinding Members

- **serverEndPoint** of type DOMString
  
  The field `serverEndPoint` must be set to the base64url-encoded hash of the TLS server certificate if this is available. The hash function must be selected as follows:
  
  1. if the certificate's `naturalAlgorithm` uses a single hash function and that hash function is either MD5 [RFC1321] or SHA-1 [RFC2634], then use SHA-256 [FIPS180-4];
  2. if the certificate's `naturalAlgorithm` uses a single hash function and that hash function is neither MD5 nor SHA-1, then use the hash function associated with the certificate's `naturalAlgorithm`;
  3. if the certificate's `naturalAlgorithm` uses no hash functions, or uses multiple hash functions, then this channel binding type's channel bindings are undefined at this time (updates to this channel binding type may occur to address this issue if it ever arises).

  This field **must** be absent if the TLS server certificate is not available to the processing entity (e.g., the FIDO UAF Client) or the hash function cannot be determined as described.

- **tlsServerCertificate** of type DOMString
  
  This field **must** be absent if the TLS server certificate is not available to the FIDO UAF Client.

  This field **must** be set to the base64url-encoded, DER-encoded TLS server certificate, if this data is available to the FIDO UAF Client.

- **tlsUnique** of type DOMString
  
  **must** be set to the base64url-encoded TLS channel `Finished` structure. It **must** be absent, if this data is not available to the FIDO UAF Client [RFC5929].

- **cid_pubkey** of type DOMString
  
  **must** be absent if the client TLS stack doesn't provide TLS ChannelID `[ChannelID]` information to the processing entity (e.g., the web browser or client application).

  **must** be set to "unused" if TLS ChannelID information is supported by the client-side TLS stack but has not been signaled by the TLS (web) server.

  Otherwise, it **must** be set to the base64url-encoded serialized [RFC4627] `JwkKey` structure using UTF-8 encoding.

### 3.1.9 JwkKey dictionary

**JwkKey** is a dictionary representing a JSON Web Key encoding of an elliptic curve public key [JWK].

This public key is the ChannelID public key minted by the client TLS stack for the particular relying party, `[ChannelID]` stipulates using only a particular elliptic curve, and the particular coordinate type.

```webidl
dictionary JwkKey {
    required DOMString kty = "EC";
    required DOMString crv = "P-256";
    required DOMString x;
    required DOMString y;
}
```

#### 3.1.9.1 Dictionary JwkKey Members

- **kty** of type required DOMString, defaulting to "EC".
  
  Denotes the key type used for Channel ID. At this time only elliptic curve is supported by [ChannelID], so it **must** be set to "EC" [JWA].

- **crv** of type required DOMString, defaulting to "P-256".
  
  Denotes the elliptic curve on which this public key is defined. At this time only the NIST curve `secp256r1` is supported by [ChannelID], so the `crv` parameter **must** be set to "P-256".

- **x** of type required DOMString
  
  Contains the base64url-encoding of the x coordinate of the public key (big-endian, 32-byte value).

- **y** of type required DOMString
  
  Contains the base64url-encoding of the y coordinate of the public key (big-endian, 32-byte value).
3.1.10 Extension dictionary

FIDO extensions can appear in several places, including the UAF protocol messages, authenticator commands, or in the assertion signed by the authenticator.

Each extension has an identifier, and the namespace for extension identifiers is FIDO UAF global (i.e. doesn’t depend on the message where the extension is present).

Extensions can be defined in a way such that a processing entity which doesn’t understand the meaning of a specific extension must abort processing, or they can be specified a way that unknown extension can (safely) be ignored.

Extension processing rules are defined in each section where extensions are allowed.

Generic extensions used in various operations.

```webidl
dictionary Extension {
  required DOMString id;
  required DOMString data;
  required boolean fail_if_unknown;
};
```

3.1.10.1 Dictionary Extension Members

**id** of type required DOMString

    string[1..32],

Identifies the extension.

**data** of type required DOMString

    Contains arbitrary data with a semantics agreed between server and client. The data is base64url-encoded.

This field may be empty.

**fail_if_unknown** of type required boolean

    Indicates whether unknown extensions must be ignored (false) or must lead to an error (true).

- A value of false indicates that unknown extensions must be ignored
- A value of true indicates that unknown extensions must result in an error.

NOTE

The FIDO UAF Client might (a) process an extension or (b) pass the extension through to the ASM. Unknown extensions must be passed through.

The ASM might (a) process an extension or (b) pass the extension through to the FIDO authenticator. Unknown extensions must be passed through.

The FIDO authenticator must handle the extension or ignore it (only if it doesn’t know how to handle it and fail_if_unknown is not set). If the FIDO authenticator doesn’t understand the meaning of the extension and fail_if_unknown is set, it must generate an error (see definition of fail_if_unknown above).

When passing through an extension to the next entity, the fail_if_unknown flag must be preserved (see [UAFASM] [UAFAuthnrCommands]).

If the FIDO protocol messages are not signed. If the security depends on an extension being known or processed, then such extension should be accompanied by a related (and signed) extension in the authenticator assertion (e.g. TAG_UAFV1_REG_ASSERTION, TAG_UAFV1_AUTH_ASSERTION).

If the security has been increased (e.g. the FIDO authenticator according to the description in the metadata statement accepts multiple fingers but in this specific case indicates that the finger used at registration was also used for authentication) there is no need to mark the extension as fail_if_unknown (i.e. tag 0x3E12 should be used [UAFAuthnrCommands]). If the security has been degraded (e.g. the FIDO authenticator according to the description in the metadata statement accepts only the finger used at registration for authentication but in this specific case indicates that a different finger was used for authentication) the extension must be marked as fail_if_unknown (i.e. tag 0x3E11 must be used [UAFAuthnrCommands]).

3.1.11 MatchCriteria dictionary

Represents the matching criteria to be used in the server policy.

The `MatchCriteria` object is considered to match an authenticator, if all fields in the object are considered to match (as indicated the particular fields).

```webidl
dictionary MatchCriteria {
  AAID[] said;
  DOMString[] vendorID;
  KeyID[] keyID;
  unsigned long userVerification;
  unsigned short RAPIDFINGERPRINT;
  unsigned long slotIndex;
  unsigned short attestationTypes;
  DOMString[] attestationAttributes;
  unsigned short[] ATProofIntermediate;
  unsigned short[] authenticationAlgorithms;
  unsigned short[] attestationTypes;
  unsigned short authenticationVersion;
  Extension[] exts;
};
```

3.1.11.1 Dictionary MatchCriteria Members
**aaids** of type array of **AAID**

List of AAIDs, causing matching to be restricted to certain AAIDs.

The match succeeds if at least one AAID entry in this array matches `AuthenticatorInfo.aaid` [UAFASM].

**NOTE**

This field corresponds to `MetadataStatement.aaids` [UAFAuthnrMetadata].

**vendorIDs** of type array of **DOMString**

The vendorID causing matching to be restricted to authenticator models of the given vendor. The first 4 characters of the AAID are the vendorID (see `aaid`).

The match succeeds if at least one entry in this array matches the first 4 characters of `AuthenticatorInfo.aaid` [UAFASM].

**NOTE**

This field corresponds to the first 4 characters of `MetadataStatement.aaids` [UAFAuthnrMetadata].

**keyIDs** of type array of **KeyID**

A list of authenticator KeyIDs causing matching to be restricted to a given set of KeyID instances. (see [UAFRegistry]).

This match succeeds if at least one entry in this array matches.

**NOTE**

This field corresponds to `AppRegistration.keyIDs` [UAFASM].

**userVerification** of type **unsigned long**

A set of 32 bit flags which may be set if matching should be restricted by the user verification method (see [UAFRegistry]).

The match with `AuthenticatorInfo.userVerification` ([UAFASM]) succeeds, if the following condition holds (written in Java):

```java
if (/
    // They are equal
    (AuthenticatorInfo.userVerification == MatchCriteria.userVerification) ||
    // USER_VERIFY_ALL is not set in both of them and they have at least one common bit set
    ((AuthenticatorInfo.userVerification & USER_VERIFY_ALL) == 0) &&
    ((MatchCriteria.userVerification & USER_VERIFY_ALL) == 0) &&
    ((AuthenticatorInfo.userVerification & MatchCriteria.userVerification) != 0)
/
)
```

**NOTE**

This field value can be derived from `MetadataStatement.userVerificationDetails` as follows:

1. if `MetadataStatement.userVerificationDetails` contains multiple entries, then:
   1. if one or more entries `MetadataStatement.userVerificationDetails[i]` contain multiple entries, then: stop, direct derivation is not possible. Must generate `MatchCriteria` object by providing a list of matching AAIDs.
   2. if all entries `MetadataStatement.userVerificationDetails[i]` only contain a single entry, then: combine all entries `MetadataStatement.userVerificationDetails[0][0].userVerification` to `MetadataStatement.userVerificationDetails[N-1][0].userVerification` into a single value using a bitwise OR operation.

2. if `MetadataStatement.userVerificationDetails` contains a single entry, then: combine all entries `MetadataStatement.userVerificationDetails[0][0].userVerification` to `MetadataStatement.userVerificationDetails[N-1][0].userVerification` into a single value using a bitwise OR operation and additionally set the flag `USER_VERIFY_ALL`.

This method doesn’t allow matching authenticators implementing complex combinations of user verification methods, such as PIN AND (Fingerprint OR Speaker Recognition) (see above derivation rules). If such specific match rules are required, they need to be specified by providing the AAIDs of the matching authenticators.

**keyProtection** of type **unsigned short**

A set of 16 bit flags which may be set if matching should be restricted by the key protections used (see [UAFRegistry]).

This match succeeds, if at least one of the bit flags matches the value of `AuthenticatorInfo.keyProtection` [UAFASM].

**NOTE**

This field corresponds to `MetadataStatement.keyProtection` [UAFAuthnrMetadata].

**matcherProtection** of type **unsigned short**

A set of 16 bit flags which may be set if matching should be restricted by the matcher protection (see [UAFRegistry]).

The match succeeds if at least one of the bit flags matches the value of `AuthenticatorInfo.matcherProtection` [UAFASM].

**NOTE**

This field corresponds to the `MetadataStatement.matcherProtection` metadata statement. See [UAFAuthnrMetadata].
attachmentHint of type unsigned long
A set of 32 bit flags which may be set if matching should be restricted by the authenticator attachment mechanism (see [UAFRegistry]). This field is considered to match, if at least one bit flags matches the value of AuthenticatorInfo.attachmentHint [UAFASM].

NOTE
This field corresponds to the MetadataStatement.attachmentHint metadata statement.

tcDisplay of type unsigned short
A set of 16 bit flags which may be set if matching should be restricted by the transaction confirmation display availability and type. (see [UAFRegistry]). This match succeeds if at least one of the bit flags matches the value of AuthenticatorInfo.tcDisplay [UAFASM].

NOTE
This field corresponds to the MetadataStatement.tcDisplay metadata statement. See [UAFAuthnrMetadata].

authenticationAlgorithms of type array of unsigned short
An array containing values of supported authentication algorithm TAG values (see [UAFRegistry], prefix UAF_ALG_SIGN) if matching should be restricted by the supported authentication algorithms. This match succeeds if at least one entry in this array matches the AuthenticatorInfo.authenticationAlgorithm [UAFASM].

NOTE
This field corresponds to the MetadataStatement.authenticationAlgorithm metadata statement. See [UAFAuthnrMetadata].

assertionSchemes of type array of DOMString
A list of supported assertion schemes if matching should be restricted by the supported schemes. See section UAF Supported Assertion Schemes for details. This match succeeds if at least one entry in this array matches AuthenticatorInfo.assertionScheme [UAFASM].

NOTE
This field corresponds to the MetadataStatement.assertionScheme metadata statement. See [UAFAuthnrMetadata].

attestationTypes of type array of unsigned short
An array containing the preferred attestation TAG values (see [UAFRegistry], prefix TAG_ATTESTATION). The order of items must be preserved. The most-preferred attestation type comes first. This match succeeds if at least one entry in this array matches one entry in AuthenticatorInfo.attestationTypes [UAFASM].

NOTE
This field corresponds to the MetadataStatement.attestationTypes metadata statement. See [UAFAuthnrMetadata].

authenticatorVersion of type unsigned short
Contains an authenticator version number, if matching should be restricted by the authenticator version in use. This match succeeds if the value is lower or equal to the field AuthenticatorVersion included in TAG_UAFV1_REG_ASSERTION or TAG_UAFV1_AUTH_ASSERTION of a corresponding value in the case of a different assertion scheme.

NOTE
Since the semantic of the AuthenticatorVersion depends on the AAID, the field AuthenticatorVersion should always be combined with a single aaid in MatchCriteria. This field corresponds to the MetadataStatement.authenticatorVersion metadata statement. See [UAFAuthnrMetadata].

exts of type array of Extension
Extensions for matching policy.

3.1.12 Policy dictionary
Contains a specification of accepted Authenticators and a specification of disallowed Authenticators.

WebIDL
dictionary Policy {
  required MatchCriteria[[]] accepted;
  MatchCriteria[] disallowed;
};

3.1.12.1 Dictionary Policy Members

accepted of type array of array of required MatchCriteria
This field is a two-dimensional array describing the required authenticator characteristics for the server to accept either a FIDO registration, or authentication operation for a particular purpose.

This two-dimensional array can be seen as a list of sets. List elements (i.e. the sets) are alternatives (OR condition).

All elements within a set must be combined:

The first array index indicates OR conditions (i.e. the list). Any set of authenticator(s) satisfying these MatchCriteria in the first index is acceptable to the server for this operation.

Sub-arrays of MatchCriteria in the second index (i.e. the set) indicate that multiple authenticators (i.e. each set element) must be registered or authenticated to be accepted by the server.

The MatchCriteria array represents ordered preferences by the server. Servers must put their preferred authenticators first, and FIDO UAF Clients should respect those preferences, either by presenting authenticator options to the user in the same order, or by offering to perform the operation using only the highest-preference authenticator(s).

3.2 Processing Rules for the Server Policy

This section is normative.

The FIDO UAF Client must follow the following rules while parsing server policy:

1. During registration:
   1. **Policy.accepted** is a list of combinations. Each combination indicates a list of criteria for authenticators that the server wants the user to register.
   2. Follow the priority of items in **Policy.accepted[[]]**. The lists are ordered with highest priority first.
   3. Choose the combination whose criteria best match the features of the currently available authenticators
   4. Collect information about available authenticators
   5. Ignore authenticators which match the **Policy.disallowed** criteria
   6. Match collected information with the matching criteria imposed in the policy (see MatchCriteria dictionary for more details on matching)
   7. Guide the user to register the authenticators specified in the chosen combination

2. During authentication and transaction confirmation:

   **NOTE**

   Policy.accepted is a list of combinations. Each combination indicates a set of criteria which is enough to completely authenticate the current pending operation

   1. Follow the priority of items in **Policy.accepted[[]]**. The lists are ordered with highest priority first.
   2. Choose the combination whose criteria best match the features of the currently available authenticators
   3. Collect information about available authenticators
   4. Ignore authenticators which meet the **Policy.disallowed** criteria
   5. Match collected information with the matching criteria described in the policy
   6. Guide the user to authenticate with the authenticators specified in the chosen combination
   7. A pending operation will be approved by the server only after all criteria of a single combination are entirely met

3.2.1 Examples

This section is non-normative.

**EXAMPLE 1**: Policy matching either a FPS-, or Face Recognition-based Authenticator

```json

{  
  "accepted": [ 
    [ 
      [ 
        "userVerification": 2 ] 
    ], 
    [ 
      [ 
        "userVerification": 16 ] 
    ] 
  ]

```

**EXAMPLE 2**: Policy matching authenticators implementing FPS and Face Recognition as alternative combination of user verification methods

```json

{  
  "accepted": [ 
    [ 
      [ 
        "userVerification": 18 ] 
    ] 
  ]

```

Combining these two bit-flags and the flag USER_VERIFY_ALL (USER_VERIFY_ALL = 1024) into a single userVerification value would match authenticators implementing FPS and Face Recognition as a mandatory combination of user verification methods

```json

{  
  "accepted": [ [ 
    [ "userVerification": 1042 ] ] 
  ]

```

**EXAMPLE 4**: Policy matching the combination of a FPS based and a Face Recognition based authenticator

```json

{  
  "accepted": [ [ 
    [ "userVerification": 1042 ] ] 
  ]

```
Other criteria can be specified in addition to the `userVerification`:

**EXAMPLE 5:** Policy requiring the combination of a bound FPS based and a bound Face Recognition based authenticator

```json
{
  "accepted":
  [  
    {  "userVerification": 2},
    {  "userVerification": 16}
  ]
}
```

The policy for accepting authenticators of vendor with ID `1234` only is as follows:

**EXAMPLE 6:** Policy accepting all authenticators from vendor with ID `1234`

```json
{
  "accepted":
  [ { "vendorID": "1234"}]
}
```

### 3.3 Version Negotiation

The UAF protocol includes multiple versioned constructs: UAF protocol version, the version of Key Registration Data and Signed Data objects (identified by their respective tags, see [UAFRegistry]), and the ASM version, see [UAFASM].

**NOTE**

The Key Registration Data and Signed Data objects have to be parsed and verified by the FIDO Server. This verification is only possible if the FIDO Server understands their encoding and the content. Each UAF protocol version supports a set of Key Registration Data and SignedData object versions (called Assertion Schemes). Similarly, each of the ASM versions supports a set of Assertion Scheme versions.

As a consequence, the FIDO UAF Client must select the authenticators which will generate the appropriately versioned constructs.

For version negotiation the FIDO UAF Client must perform the following steps:

1. Create a set `FC_Version_Set` of version pairs, ASM version (`asm_version`) and UAF Protocol version (`upv`) and add all pairs supported by the FIDO UAF Client into `FC_Version_Set`.
   - e.g. `{(upv1, asm_version1), (upv2, asm_version1), ...}`

2. Intersect `FC_Version_Set` with the set of `upv` included in UAF Message (i.e. keep only those pairs where the `upv` value is also contained in the UAF Message).

3. Select authenticators which are allowed by the UAF Message Policy. For each authenticator:
   - Construct a set `Authnr_Version_Set` of version pairs including authenticator supported `asm_version` and the compatible `upv(s)`. 
     - e.g. `{(upv1, asm_version1), (upv2, asm_version1), ...}`
   - Intersect `Authnr_Version_Set` with `FC_Version_Set` and select highest version pair from it.
     - Take the pair where the `upv` is highest. In all these pairs leave only the one with highest `asm_version`.
   - Use the remaining version pair with this authenticator.

**NOTE**

Each version consists of major and minor fields. To order to compare two versions - compare the Major fields and if they are equal compare the Minor fields.

Each UAF message contains a version field. UAF Protocol version negotiation is always between FIDO UAF Client and FIDO Server.

### 3.4 Registration Operation

**NOTE**

The Registration operation allows the FIDO Server and the FIDO Authenticator to agree on an authentication key.
3.4.1 Registration Request Message

UAF Registration request message is represented as an array of dictionaries. Each dictionary contains a registration request for a specific protocol version. The array must not contain two dictionaries of the same protocol version. For version "1.0" the request is defined as RegistrationRequest dictionary.

EXAMPLE 7: UAF Registration Request

```json
{
  "header": {
    "upv": {
      "major": 1,
      "minor": 0
    },
    "op": "Reg",
    "appID": "https://uaf-test-1.noknoktest.com:8443/SampleApp/uaf/facets",
    "serverData": "IjycjPZYiWMaQ1tKLrJROiXQHmYG0tSSYGjP5mgjsDaM17RQgq0
dl3NNDDTx9d-aSR_6hGgclrU2F2Yj-12S67v5VmQHj4eWVseLulHdpk2v_hHtKSvv_DFqL4n
2IiUY6XZWVbOnvg"
  },
  "challenge": "H91W9yA9aAXF_1e1qoL_DhOKS14d8Tqy02cNoC6qKdpo",
  "username": "apa",
  "policy": {
    "accepted": [
      {
        "userVerification": 512,
```
"keyProtection": 1,
"tcDisplay": 1,
"authenticationAlgorithms": [
  1
],
"assertionSchemes": [
  "UAFV1TLV"
],
],
},
{"userVerification": 4,
"keyProtection": 1,
"tcDisplay": 1,
"authenticationAlgorithms": [
  1
],
"assertionSchemes": [
  "UAFV1TLV"
],
},
{"userVerification": 4,
"keyProtection": 1,
"tcDisplay": 1,
"authenticationAlgorithms": [
  2
]},
"userVerification": 4,
"keyProtection": 2,
"tcDisplay": 1,
"authenticationAlgorithms": [
  1,
  3
],
"assertionSchemes": [
  "UAFV1TLV"
],
"userVerification": 2,
"authenticationAlgorithms": [
  1,
  3
],
"assertionSchemes": [
  "UAFV1TLV"
],
"userVerification": 2,
"authenticationAlgorithms": [
  2
],
"assertionSchemes": [
  "UAFV1TLV"
],
"userVerification": 32,
"keyProtection": 2,
"assertionSchemes": [
  "UAFV1TLV"
],
"userVerification": 256,
"keyProtection": 16,
"assertionSchemes": [
  "UAFV1TLV"
],
"userVerification": 256,
"keyProtection": 16,
"assertionSchemes": [
  "UAFV1TLV"
]}
}
3.4.2 RegistrationRequest dictionary

RegistrationRequest contains a single, versioned, registration request.

```webidl
dictionary RegistrationRequest {
    required OperationHeader header;
    required DOMString username;
    required Policy policy;
    required ServerChallenge challenge;
    required DOMString username;
};
```

3.4.2.1 Dictionary RegistrationRequest Members

- **header** of type required OperationHeader
  
  Operation header. `Header.op` must be "Reg"

- **challenge** of type required ServerChallenge
  
  Server-provided challenge value

- **username** of type required DOMString
  
  String[1..128]

  A human-readable user name intended to allow the user to distinguish and select from among different accounts at the same relying party.

- **policy** of type required Policy
  
  Describes which types of authenticators are acceptable for this registration operation

3.4.3 AuthenticatorRegistrationAssertion dictionary

Contains the authenticator’s response to a RegistrationRequest message:

```webidl
dictionary AuthenticatorRegistrationAssertion {
    required DOMString assertionScheme;
    required DOMString assertion;
    DisplayPNGCharacteristicsDescriptor[] tcDisplayPNGCharacteristics;
    Extension[] exts;
};
```

3.4.3.1 Dictionary AuthenticatorRegistrationAssertion Members

- **assertionScheme** of type required DOMString
  
  The name of the Assertion Scheme used to encode the `assertion`. See [UAF Supported Assertion Schemes](#) for details.

  NOTE

  This assertionScheme is not part of a signed object and hence considered the suspected assertionScheme.

- **assertion** of type required DOMString
  
  base64url(byte[1..4096])

  Contains the `TAG_UAFV1_REG_ASSERTION` object containing the assertion scheme specific `ByrRegistrationData` (KRD) object which in turn contains the newly generated `UAuth.pub` and is signed by the Attestation Private Key.

  This assertion must be generated by the authenticator and it must be used only in this Registration operation. The format of this assertion can vary from one assertion scheme to another (e.g. for "UAFV1TLV" assertion scheme it must be `TAG_UAFV1_KRD`).

- **tcDisplayPNGCharacteristics** of type array of `DisplayPNGCharacteristicsDescriptor`
  
  Supported transaction PNG type [UAFAuthnrMetadata]. For the definition of the `DisplayPNGCharacteristicsDescriptor` structure See [UAFAuthnrMetadata](#).

- **exts** of type array of `Extension`
  
  Contains Extensions prepared by the authenticator

3.4.4 Registration Response Message

A UAF Registration response message is represented as an array of dictionaries. Each dictionary contains a registration response for a specific protocol version. The array must not contain two dictionaries of the same protocol version. For version “1.0” the response is defined as `RegistrationResponse` dictionary.

```json
{
    "assertions": [
        {
            "assertion": "AT7uAgM-sQALLgkAQUJDRCNBQkNEDi4HAAABAQEAAAEKLiAA9tBzZC64ecgVQBGSQb5QtEIPC8-Vav4HaHLZf1Laugj1Aczik9yWv1lpg-1C7B6414Adg6Z0u56XFPUCv5jEFgRgppAIAAAAAEAAAALAEAB3jvV0uVIR7wvYHl2fJMBkJH0-OCdW1UY
```

NOTE

This assertionScheme is not part of a signed object and hence considered the suspected assertionScheme.

EXAMPLE 8: Registration Response

```json
{
    "aaid": ["ABCD#ABCD"],
    "keyIDs": ["RfY_RDhsf4z5PCOhnZExMeVloZmK0hxaSi10tkY_c4"],
}
```
The FIDO Server must match the policy. But any of those (second dimension) of authenticators must be combined with (one or more of) the claim field provided with the authentication response.

NOTE
Line breaks in tcParams have been inserted for improving readability.

3.4.5 RegistrationResponse dictionary

Contains all fields related to the registration response.

```webidl
dictionary RegistrationResponse {
  required OperationHeader
  required DOMString
  required AuthenticatorRegistrationAssertion
}
```

3.4.5.1 Dictionary RegistrationResponse Members

- **header** of type required OperationHeader
  
  - **Operation** must be "Reg".

- **fcParams** of type required DOMString
  
  - The base64url-encoded serialized [RFC4627] `FinalChallengeParams` using UTF8 encoding (see `FinalChallengeParams` dictionary) which contains all parameters required for the server to verify the Final Challenge.

- **assertions** of type array of required AuthenticatorRegistrationAssertion
  
  - Response data for each Authenticator being registered.

3.6 Registration Processing Rules

3.6.1 Registration Request Generation Rules for FIDO Server

The policy contains a two-dimensional array of allowed `MatchCriteria` (see `Policy`). This array can be considered a list (first dimension) of sets of (second dimension) of authenticators (identified by `Authenticator`). All authenticators in a specific set `Authenticator` must be registered simultaneously in order to match the policy. But any of the entries in the list are valid, as the list elements are alternatives.

The FIDO Server must follow the following steps:

1. Construct appropriate authentication policy `p`
   
   - 1. For each set of authenticators `m`:
     
     1. Create an array of `MatchCriteria` objects, containing the set of authenticators to be registered simultaneously that need to be identified by the `n`th rule, create a `MatchCriteria` object `m`, where
       
       - `m.aaid` may be combined with (one or more of) `m.keyIDs`, `m.attachmentHint`, `m.authenticationVersion`, and `m.exts`, but `m.aaid` must not be combined with any other match criteria field.
       
       - If `m.aaid` is not provided - at least `m.authenticationAlgorithms` and `m.assertionsSchemes` must be provided

2. Add `m to v`, e.g. `v[j]=m`

3. Add `v to p.allowed`, e.g. `p.allowed[i]=v`

2. Create MatchCriteria objects `n` for all disallowed Authenticators.

   - 1. For each already registered AAID for the current user
      
      1. Create a `MatchCriteria` object `n` and add AAID and corresponding KeyIDs to `m.aaid` and `m.keyIDs`.

      The FIDO Server must include already registered AAIDs and KeyIDs into field `disallowed` to hint that the client should not register these again.

   2. Create a `MatchCriteria` object `n` and add the AAIDs of all disallowed Authenticators to `m.aaid`.

   The status (as provided in the metadata TOC (Table-of-Contents file) `DAFMetadataService`) of some authenticators might be
3.4.6.5 The FIDO UAF Client

1. FIDO Servers should not assume any implicit integrity protection of r.header.serverData.

2. FIDO Servers that depend on the integrity of r.header.serverData should apply and verify a cryptographically secure Message Authentication Code (MAC) to serverData and they should also cryptographically bind serverData to the related message, e.g. by re-including r.challenge, see also section ServerData and KeyHandle.

3. If needed - create MatchCriteria for other disallowed criteria (e.g. unsupported authenticationAlgs)
4. Add all m to p.disallowed.

2. Create a RegistrationRequest object r with appropriate r.header for each supported version, and

FIDO Servers should include already supported – reject the operation

3. In a UAF protocol version (see section Version Negotiation) and user agrees to register:

The FIDO UAF Client must follow the steps:

1. Add AppID, Username, FinalChallenge, AttestationType and all other required fields to the ASMRequest [UAFASM].

The FIDO UAF Client must follow the server policy and find the single preferred attestation type. A single attestation type must be provided to the ASM.

2. Send ASMRequest to the ASM

3.4.6.6 Registration Request Processing Rules for FIDO UAF Clients

The FIDO UAF Client must perform the following steps:

1. Choose the message m with major version 1 and minor version 0
2. Parse the message m
3. If a mandatory field in UAF message is not present or a field doesn't correspond to its type and value - reject the operation
4. Filter the available authenticators with the given policy and present the filtered authenticators to User. Make sure to not include already registered authenticators for this user specified in RegRequest.policy.disallowed, see also section "Register Command".
5. Obtain FacetID of the requesting Application. If the AppID is missing or empty, set the AppID to the FacetID.

Verify that the FacetID is authorized for the AppID according to the algorithms in [FIDOAppIDAndFacets].

- If the FacetID of the requesting Application is not authorized, reject the operation
6. Obtain TLS data if it is available
7. Create a FinalChallengeParams structure fcp and set fcp.appID, fcp.challenge, fcp.facetID, and fcp.channelBinding appropriately. Serialize [RFC4627] fcp using UTF8 encoding and base64url encode it.
   - FinalChallenge = base64url(serialize(utf8encode(fcp)))
8. For each authenticator that matches UAF protocol version (see section Version Negotiation) and user agrees to register:

   1. Add AppID, Username, FinalChallenge, AttestationType and all other required fields to the ASMRequest [UAFASM].

   The FIDO UAF Client must follow the server policy and find the single preferred attestation type. A single attestation type must be provided to the ASM.

   2. Send ASMRequest to the ASM

3.4.6.3 Registration Request Processing Rules for FIDO Authenticator

See [UAFAuthnrCommands], section "Register Command".

3.4.6.4 Registration Response Generation Rules for FIDO UAF Client

The FIDO UAF Client must follow the steps:

1. Create a RegistrationResponse message
2. Copy RegistrationRequest.header into RegistrationResponse.header
3. Set RegistrationResponse.fParams to FinalChallenge (base64url encoded serialized and utf8 encoded FinalChallengeParams)
4. Append the response from each Authenticator into RegistrationResponse.assertions
5. Send RegistrationResponse message to FIDO Server

3.4.6.5 Registration Response Processing Rules for FIDO Server

The following processing rules assume that Authenticator supports "UAFV1TLV" assertion scheme. Currently "UAFV1TLV" is the only defined and supported assertion scheme. When a new assertion scheme is added to UAF protocol - this section will be extended with corresponding processing rules.

The FIDO Server must follow the steps:

1. Parse the message
2. If protocol version (RegistrationResponse.header.upv) is not supported – reject the operation
3. If a mandatory field in UAF message is not present or a field doesn't correspond to its type and value - reject the operation
4. Verify that RegistrationResponse.header.serverData, if used, passes any implementation-specific checks against its validity. See also section ServerData and KeyHandle.
3. base64url decode RegistrationResponse.fcParams and convert it into an object (fcp)
4. Verify each field in fcp and make sure it is valid:
   1. Make sure fcp.appID corresponds to the one stored by the FIDO Server
   2. Make sure fcp.challenge has really been generated by the FIDO Server for this operation and it is not expired
   3. Make sure fcp.facetID is in the list of trusted FacetIDs [FIDOAppIDAndFacets]
   4. Make sure fcp.channelBinding is as expected (see section ChannelBinding dictionary)
5. For each assertion in RegistrationResponse.assertions
   1. Parse TLV data from a.assertion assuming it is encoded according to the suspected assertion scheme a.assertionscheme and make sure it contains all mandatory fields (indicated in Authenticator Metadata) it is supposed to have and has a valid syntax.
      - If it doesn't - continue with next assertion
   2. Retrieve the AAID from the assertion.
   
   **NOTE**
   The AAID in TAG_UAFV1_KRD is contained in a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.TAG_AAID.

3. Verify that a.assertionscheme matches Metadata(AAID).assertionscheme
   - If it doesn't match - continue with next assertion
4. Verify that the AAID indeed matches the policy specified in the registration request.

   **NOTE**
   Depending on the policy (e.g. in the case of AND combinations), it might be required to evaluate other assertions included in this RegistrationResponse in order to determine whether this AAID matches the policy.

   - If it doesn't match the policy - continue with next assertion
5. Locate authenticator-specific authentication algorithms from Be authenticator metadata [UAFAuthnMetadata] using the AAID.
6. Hash RegistrationResponse.fcParams using hashing algorithm suitable for this authenticator type. Look up the hash algorithm in authenticator metadata, field AuthenticationAlgs. It is the hash algorithm associated with the first entry Blinked to a constant with prefix UAF_ALG_SIGN.
   - FCHash = hash (RegistrationResponse.fcParams)
7. If a.assertions contains an object of type TAG_UAFV1_REG_ASSERTION, then
   1. If a.assertion.TAG_UAFV1_REG_ASSERTION contains TAG_UAFV1_KRD as first element:
      1. Obtain Metadata(AAID).AttestationType for the AAID and make sure that a.assertion.TAG_UAFV1_REG_ASSERTION contains the most preferred attestation tag specified in field Criteria.attestationTypes in RegistrationRequest.policy (if this field is present).
         - If a.assertion.TAG_UAFV1_REG_ASSERTION doesn't contain the preferred attestation - it is recommended to skip this assertion and continue with next one
      2. Make sure that a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.FinalChallenge == FCHash
         - If comparison fails - continue with next assertion
   3. Obtain Metadata(AAID).AuthenticatorVersion for the AAID and make sure that it is lower or equal to a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.AuthenticatorVersion.
      - If Metadata(AAID).AuthenticatorVersion is higher (i.e. the authenticator firmware is outdated), B is recommended to assume increased risk. See sections "StatusReport dictionary" and "Metadata TOC object Processing Rules" in [UAFMetadataService] for more details on this.
4. Check whether a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.RegCounter is acceptable, i.e. it is either not supported (value is 0) or it is not exceedingly high
   - If a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.RegCounter is exceedingly high, this assertion might be skipped and processing will continue with next one
5. If a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD contains TAG_ATTESTATION_BASIC_FULL tag
   1. If entry AttestationRootCertificates for the AAID in the metadata [UAFAuthnMetadata] contains at least one element:
      1. Obtain contents of all TAG_ATTESTATION_CERT tags from a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_ATTESTATION_BASIC_FULL object. The occurrences are ordered (see [UAFAuthnCommands]) and represent the attestation certificate followed by the related Certificate chain.
      2. Obtain all entries of AttestationRootCertificates for the AAID in authenticator Metadata, field AttestationRootCertificates.
      3. Verify the attestation certificate and the entire certificate chain up to Be Attestation Root Certificate using Certificate Path Validation as specified in [RFC5280].
         - If verification fails - continue with next assertion
      4. Verify a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.TAG_ATTESTATION_BASIC_FULL.Signed using the attestation certificate (obtained before).
         - If verification fails - continue with next assertion
   2. If Metadata(AAID).AttestationRootCertificates for this AAID is empty - continue with next assertion
3. Mark assertion as positively verified
6. If a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD contains an object of type TAG_ATTESTATION_BASIC_SURROGATE
   1. There is no real attestation for the AAID, so we just assume the AAID is the real one.
   2. If entry AttestationRootCertificates for the AAID in the metadata is empty
      - Verify a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_ATTESTATION_BASIC_SURROGATE.Signed using a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.TAG_PUB_KEY
         - If verification fails - continue with next assertion
   3. If entry AttestationRootCertificates for the AAID in the metadata is not empty - continue with next assertion (as the AAID obviously is expecting a different attestation method).
3. Mark assertion as positively verified
7. If a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD contains another TAG_ATTESTATION tag - verify the attestation by
following appropriate processing rules applicable to that attestation. Currently this document only defines the processing rules for Basic Attestation.

2. If `a.assertion.TAG_UAFV1_REG_ASSERTION` contains a different object than `TAG_UAFV1_KRD` as first element, then follow the rules specific to that object.

3. Extract `a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.PublicKey` into `PublicKey`, `a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.KeyID` into `KeyID`, `a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.SignCounter` into `SignCounter`, `a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.TAG_ASSERTION_INFO.authenticatorVersion` into `AuthenticatorVersion`, `a.assertion.TAG_UAFV1_REG_ASSERTION.TAG_UAFV1_KRD.TAG_AAID` into `AAID`.

8. If `a.assertion` doesn’t contain an object of type `TAG_UAFV1_REG_ASSERTION`, then skip this assertion (as in this UAF v1 only `TAG_UAFV1_REG_ASSERTION` is defined).

6. For each positively verified assertion:
   + Store `PublicKey`, `KeyID`, `SignCounter`, `AuthenticatorVersion`, `AAID` and `a.tcDisplayPNGCharacteristics` into a record associated with the user’s identity. If an entry with the same pair of `AAID` and `KeyID` already exists then fail (should never occur).

3.5 Authentication Operation

<table>
<thead>
<tr>
<th>User</th>
<th>Authenticator</th>
<th>ASM</th>
<th>FIDO Client</th>
<th>User Agent</th>
<th>RP Web Server</th>
<th>RP Web App</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image.png" alt="Image of sequence diagram" /></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 8 UAF Authentication Sequence Diagram

During this operation, the FIDO Server asks the FIDO UAF Client to authenticate user with server-specified authenticators, and return an authentication response.

In order for this operation to succeed, the authenticator and the relying party must have a previously shared registration.

Fig. 9 UAF Authentication Cryptographic Data Flow

Diagram of cryptographic flow:

The FIDO Server sends the `AppID` (see [FIDOAppIDAndFacets](#)), the authenticator `policy` and the `ServerChallenge` to the FIDO UAF Client.

The FIDO UAF Client computes the hash of the `finalChallengeParams`, produced from the `ServerChallenge` and other values, as described in this document, and sends the `AppID` and hashed `finalChallengeParams` to the Authenticator.

The authenticator creates the `SignedData` object (see `TAG_UAFV1_SIGNED_DATA` in [UAFAuthnrCommands](#)) containing the hash of the `finalChallengeParams`, and some other values and signs it using the `UAuth.priv` key. This assertion is then cryptographically verified by the FIDO Server.
3.5.1 Transaction dictionary

Contains the Transaction Content provided by the FIDO Server:

```webidl
dictionary Transaction {
    required DOMString contentType;
    required DOMString content;
    DisplayPNGCharacteristicsDescriptor tcDisplayPNGCharacteristics;
}
```

3.5.1.1 Dictionary Transaction Members

**contentType** of type `required DOMString`

Contains the MIME Content-Type supported by the authenticator according to its metadata statement (see [UAFAuthnrMetadata]).

This version of the specification only supports the values `text/plain` or `image/png`.

**content** of type `required DOMString` base64url(byte[1...])

Contains the base64-url encoded transaction content according to the `contentType` to be shown to the user.

If `contentType` is "text/plain" then the content must be ASCII encoded text with a maximum of 200 characters.

**tcDisplayPNGCharacteristics** of type `DisplayPNGCharacteristicsDescriptor`

Transaction content PNG characteristics. For the definition of the `DisplayPNGCharacteristicsDescriptor` structure See [UAFAuthnrMetadata]. This field must be present if the `contentType` is "image/png".

3.5.2 Authentication Request Message

UAF Authentication request message is represented as an array of dictionaries. Each dictionary contains an authentication request for a specific protocol version. The array must not contain two dictionaries of the same protocol version. For version "1.0" the request is defined as a [UAFAuthenticationRequest] dictionary.

**EXAMPLE 9: UAF Authentication Request**

```json
[{
    "header": {
        "upv": {
            "major": 1,
            "minor": 0
        },
        "op": "Auth",
        "appID": "https://uaf-test-1.noknoktest.com:8443/SampleApp/uaf/facets",
        "serverData": "5s7n8-7_LDAtRIKKYqbAtTTOezVKCjl2mPorYzbpxRrZ-_3wWroMXsF_pLYjNhVl7bplAx4bkEwK6Ibl19EHGdfrDQ1q0tyEKhJFQqgjVwLloroxtTh1j8Is tpt7q",
        "challenge": "HQ1VkTUQC1NJDOo6OOWdxewrb9i5WhfJEIdhFxpeuU",
        "policy": {
            "accepted": [
            {
                "userVerification": 512,
                "keyProtection": 1,
                "tcDisplay": 1,
                "authenticationAlgorithms": [1]
            },
            {
                "assertionSchemes": ["UAFV1TLV"
            ]
            }
        }]
    },
    {
        "userVerification": 4,
        "keyProtection": 1,
        "tcDisplay": 1,
        "authenticationAlgorithms": [1]
    },
    {
        "assertionSchemes": ["UAFV1TLV"
    ]
    },
    {
        "userVerification": 4,
        "keyProtection": 1,
        "tcDisplay": 1,
        "authenticationAlgorithms": [2]
    },
    {
        "assertionSchemes": ["UAFV1TLV"
    ]
    },
    {
        "userVerification": 4,
        "keyProtection": 2,
        "tcDisplay": 1,
        "authenticationAlgorithms": [2]
    }]
```
3.5.3 AuthenticationRequest dictionary

Contains the UAF Authentication Request Message:

```webidl
dictionary AuthenticationRequest {
  required OperationHeader header;
  required ServerChallenge challenge;
  Transaction[] transaction;
  required Policy policy;
};
```

3.5.3.1 Dictionary AuthenticationRequest Members

- **header** of type **required** OperationHeader
  - `Header.op` must be “Auth”

- **challenge** of type **required** ServerChallenge
  - Server-provided challenge value

- **transaction** of type **array of** Transaction
  - Transaction data to be explicitly confirmed by the user.

  The list contains the same transaction content in various content types and various image sizes. Refer to [UAFAuthnrMetadata] for more information about Transaction Confirmation Display characteristics.

- **policy** of type **required** Policy
  - Server-provided policy defining what types of authenticators are acceptable for this authentication operation.

3.5.4 AuthenticatorSignAssertion dictionary
Represents a response generated by a specific Authenticator:

```webidl
dictionary AuthenticatorSignAssertion {
  required DOMString assertionScheme;
  required DOMString assertion;
  Extension[] exts;
};
```

### 3.5.4.1 Dictionary AuthenticatorSignAssertion Members

**assertionScheme** of type required DOMString

The name of the Assertion Scheme used to encode `assertion`. See [UAF Supported Assertion Schemes](#) for details.

**NOTE**

This assertionScheme is not part of a signed object and hence considered the *suspected* assertionScheme.

**assertion** of type required DOMString

`base64url(byte[1..4096])` Contains the assertion containing a signature generated by `UAuth.priv`, i.e. `TAG_UAFV1_AUTH_ASSERTION`.

**exts** of type array of Extension

Any extensions prepared by the Authenticator

### 3.5.5 AuthenticationResponse dictionary

Represents the response to a challenge, including the set of signed assertions from registered authenticators.

```webidl
dictionary AuthenticationResponse {
  required OperationHeader header;
  required DOMString fcParams;
  required AuthenticatorSignAssertion[] assertions;
};
```

### 3.5.5.1 Dictionary AuthenticationResponse Members

**header** of type required OperationHeader

`Header.op` must be “Auth”

**fcParams** of type required DOMString

The field `fcParams` is the base64url-encoded serialized [RFC4627](#) `FinalChallengeParams` in UTF8 encoding (see `FinalChallengeParams` dictionary) which contains all parameters required for the server to verify the Final Challenge.

**assertions** of type array of required AuthenticatorSignAssertion

The list of authenticator responses related to this operation.

### 3.5.6 Authentication Response Message

UAF Authentication response message is represented as an array of dictionaries. Each dictionary contains an authentication response for a specific protocol version. The array **must not** contain two dictionaries of the same protocol version. For version “1.0” the response is defined as `AuthenticationResponse` dictionary.

### 3.5.7 Authentication Processing Rules

**NOTE**

Line breaks in fcParams have been inserted for improving readability.

```json
EXAMPLE 10: UAF Authentication Response

```
3.5.7.1 Authentication Request Generation Rules for FIDO Server

The policy contains a 2-dimensional array of allowed MatchCriteria (see Policy). This array can be considered a list (first dimension) of sets (second dimension) of authenticators (identified by MatchCriteria). All authenticators in a specific set must be used for authentication simultaneously in order to match the policy. But any of those sets in the list are valid, i.e. the list elements are alternatives.

The FIDO Server must follow the steps:

1. Construct appropriate authentication policy \( p \)
   for each set of alternative authenticators do
   1. Create an 1-dimensional array of MatchCriteria objects \( v \) containing the set of authenticators to be used for authentication simultaneously that need to be identified by \( m \) MatchCriteria object.
      1. For each collection of authenticators \( m \) to be used for authentication simultaneously that can be identified by the same rule, create a MatchCriteria object \( m \), where
         - \( m.aaid \) may be combined with (one or more of) \( m.keyIDs, m.attachmentHint, m.authenticatorVersion, \) and \( m.exts \), but
         - \( m.aaid \) must not be combined with any other match criteria field.
         - If \( m.aaid \) is not provided - at least \( m.authenticationAlgorithms \) and \( m.authenticationScheme \) must be provided
      2. In case of step-up authentication (i.e. in the case where it is expected the user is already known due to a previous authentication step) every item in \( \text{policy.accepted} \) must include the AAID and KeyID of the authenticator registered for this account in order to avoid ambiguities when having multiple accounts at this relying party.
   2. Add \( m \) to \( v \), e.g. \( v[j+1]=m \)
   3. Create MatchCriteria objects \( m[j] \) for all disallowed authenticators.
      1. Create a MatchCriteria object \( m \) and add AAIDs of all disallowed authenticators to \( m.aaid \).
      2. If needed - create MatchCriteria \( m \) for other disallowed criteria (e.g. unsupported authenticationAlgs)
      3. Add all \( m \) to \( p \. disallowed \).
   4. Create an AuthenticationRequest object \( r \) with appropriate \( r.header \) for each supported version, and
      1. FIDO Servers should not assume any implicit integrity protection of \( r.header.serverData \). FIDO Servers that depend on the integrity of \( r.header.serverData \) should apply and verify a cryptographically secure Message Authentication Code (MAC) to serverData and they should also cryptographically bind serverData to the related message, e.g. by re-including \( r.challenge \), see also section ServerData and KeyHandle.

      \[ \text{NOTE} \]
      All other FIDO components (except the FIDO server) will treat \( r.header.serverData \) as an opaque value. As a consequence the FIDO server can implement any suitable cryptographic protection method.

   2. Generate a random challenge and assign it to \( r.challenge \)
   3. If this is a transaction confirmation operation - look up TransactionConfirmationDisplayContentTypes if TransactionConfirmationDisplayPNGCharacteristics from authenticator metadata of every Participating AAID, generate a list of corresponding transaction content and insert the list into \( r.transaction \).
      - If the authenticator reported (a dynamic) AuthenticatorRegistrationAssertion.toDisplayPNGCharacteristics during Registration it must be preferred over the (static) value specified in the authenticator Metadata.
   4. Set \( r.policy \) to our new policy object, created above, e.g. \( r.policy = p \).
   5. Add the authentication request message the array
   6. Send the array of authentication request messages to the FIDO UAF Client

3.5.7.2 Authentication Request Processing Rules for FIDO UAF Client

The FIDO UAF Client must follow the steps:

1. Choose the message with major version 1 and minor version 0
2. Parse the message
   - If a mandatory field in the UAF message is not present or a field doesn’t correspond to its type and value then reject the operation
3. Obtain FacetID Of the requesting Application. If the AppID is missing or empty, set the AppID to the FacetID.
   - If the FacetID is authorized for the AppID according to the algorithms in [FIDOAppIDAndFacets],
4. Filter available authenticators with the given policy and present the filtered list to User.
   - If AuthenticationRequest:policy:accepted list is empty then suggest any registered authenticator to the user for authentication
5. Let the user select the preferred Authenticator.
6. Obtain TLS data if it’s available.
7. Create a FinalChallengeParams structure \( fcp \) and set \( fcp.AppID, fcp.facetID, fcp.challenge, fcp.channelBinding \) and \( fcp.attachmentHint \) appropriately.
   - FinalChallenge = base64url(serialize(utf8encode(fcp)))
8. For each authenticator that supports an Authenticator Interface Version AIV compatible with message version AuthenticationRequest:header:upv (see Version Negotiation) and user agrees to authenticate with:
   1. Add AppID, FinalChallenge, Transactions (if present), and all other fields to the ASMRequest.
   2. Send the ASMRequest to the ASM.

3.5.7.3 Authentication Request Processing Rules for FIDO Authenticator

See [UAFAuthenticationCommands], section “Sign Command”. 

### 3.5.7.4 Authentication Response Generation Rules for FIDO UAF Client

The FIDO UAF Client must follow the steps:

1. Create an AuthenticationResponse message
2. Copy authenticationRequest.header into AuthenticationResponse.header
3. Fill out AuthenticationResponse.FinalChallengeParams with appropriate fields and then stringify it
4. Append the response from each authenticator into AuthenticationResponse.assertions
5. Send AuthenticationResponse message to the FIDO Server

### 3.5.7.5 Authentication Response Processing Rules for FIDO Server

#### NOTE

The following processing rules assume that authenticator supports "UAFV1TLV" assertion scheme. Currently "UAFV1TLV" is the only defined and supported assertion scheme. When a new assertion scheme is added to UAF protocol - this section will be extended with corresponding processing rules.

The FIDO Server must follow the steps:

1. Parse the message
   1. If protocol version (AuthenticationResponse.header.upv) is not supported – reject the operation
   2. If a mandatory field in UAF message is not present or a field doesn't correspond to its type and value - reject the operation
2. Verify that AuthenticationResponse.header.serverData, if used, passes any implementation-specific checks against its validity. See also section ServerData and KeyHandle.
3. base64url decode AuthenticationResponse.fcParams and convert into an object (fcp)
4. Verify each field in fcp and make sure it's valid
   1. Make sure AppID corresponds to the one stored by the FIDO Server
   2. Make sure FacetIds is in the list of trusted FacetIds [FIDOAppIdAndFacets]
   3. Make sure ChannelBinding is as expected (see section ChannelBinding dictionary)
5. Verify that the ServerChallenge submitted by the client has been generated by the FIDO server
6. Reject the response if any of the above checks fails
7. For each assertion, in AuthenticationResponse.assertions
   1. Parse TLV data from a.assertion assuming it is encoded according to the suspected assertion scheme a.assertionScheme and make sure it contains all mandatory fields (indicated in authenticator Metadata) it is supposed to have and has a valid syntax. If it doesn't - continue with next assertion
   2. Retrieve the AAID from the assertion.

#### NOTE

The AAID in TAG_UAFV1_SIGNED_DATA is contained in a.assertion.TAG_UAFV1_AUTH_ASSERTION.TAG_UAFV1_SIGNED_DATA.TAG_AAID.

3. Verify that a.assertionScheme matches Metadata(AAID).assertionScheme
   1. If it doesn't match – continue with next assertion
4. Make sure that the AAID indeed matches the policy of the Authentication Request
   1. If it doesn't meet the policy – continue with next assertion
5. If a.assertion contains an object of type TAG_UAFV1_AUTH_ASSERTION, then
   1. If a.assertion.TAG_UAFV1_AUTH_ASSERTION contains TAG_UAFV1_SIGNED_DATA as first element
      1. Obtain Metadata(AAID).AuthenticatorVersion for this AAID and make sure that it is lower or equal to a.assertion.TAG_UAFV1_AUTH_ASSERTION.TAG_UAFV1_SIGNED_DATA.TAGASSERTION_INFO.AuthenticatorVersion.
         1. If Metadata(AAID).AuthenticatorVersion is higher (i.e. the authenticator firmware is outdated), it is recommended to assume increased authentication risk. See "StatusReport dictionary" and "Metadata TOC object Processing Rules" in [UAFMetadataService] for more details on this.
   2. Retrieve a.assertion.TAG_UAFV1_AUTH_ASSERTION.TAG_UAFV1_SIGNED_DATA.TAG_KEYID as KeyID
   3. Locate UAuth.pub public key associated with (AAID, KeyID) in the user's record.
         1. If such record doesn't exist - continue with next assertion
   4. Verify the AAID against the AAID stored in the user's record at time of Registration.
         1. If comparison fails – continue with next assertion
   5. Locate authenticator specific authentication algorithms from Authenticator metadata (field AuthenticationAlgs)
   6. Check the Signature Counter a.assertion.TAG_UAFV1_AUTH_ASSERTION.TAG_UAFV1_SIGNED_DATA.SignCounter and make sure it is either not supported by the authenticator (i.e. the value provided and the value stored in the user's record are both 0) or it has been incremented (compared to the value stored in the user's record)
         1. If it is greater than 0, but didn't increment - continue with next assertion (as this is a cloned authenticator or a cloned authenticator has been used previously).
   7. Hash AuthenticationResponse.FinalChallengeParams using the hashing algorithm suitable for this authenticator type. Look up the hash algorithm in authenticator Metadata, field AuthenticationAlgs. It is the hash algorithm associated with the first entry related to a constant with prefix UAF_ALG_SIGN.
         1. FCHash = hash(AuthenticationResponse.FinalChallengeParams)
   8. Make sure that a.assertion.TAG_UAFV1_AUTH_ASSERTION.TAG_UAFV1_SIGNED_DATA.TAG_FINAL_CHALLENGE == FCHash
      1. If comparison fails – continue with next assertion
   9. If a.assertion.TAG_UAFV1_AUTH_ASSERTION.TAG_UAFV1_SIGNED_DATA.TAGASSERTION_INFO.authenticationMode == 2

#### NOTE

The transaction hash included in this AuthenticationResponse must match the transaction content specified in the
1. Make sure there is a transaction cached on Relying Party side.  
   - If not – continue with next assertion

2. Go over all cached forms of the transaction content (potentially multiple cached PNGs for the same transaction) and calculate their hashes using hashing algorithm suitable for this authenticator (same hash algorithm as used for FinalChallenge).  
   - For each cachedTransaction add hash(cachedTransaction) into cachedTransactionHashList

3. Make sure that a.TransactionHash is in cachedTransactionHashList  
   - If it's not in the list – continue with next assertion

10. Use UAuth.pub key and appropriate authentication algorithm to verify  
    a.assertion.TAG_UAFV1_AUTH_ASSERTION.TAG_SIGNATURE  
    - If signature verification fails – continue with next assertion

2. Update SignCounter in user's record with  
    a.assertion.TAG_UAFV1_AUTH_ASSERTION.TAG_UAFV1_SIGNED_DATA.SignCounter

6. if a.assertion.TAG_UAFV1_AUTH_ASSERTION contains a different object than TAG_UAFV1_SIGNED_DATA as first element, then follow the rules specific to that object.

7. Treat this assertion a as positively verified.

3.6 Deregistration Operation

This operation allows FIDO Server to ask the FIDO Authenticator to delete keys related to the particular relying party.

3.6.1 Deregistration Request Message

The FIDO UAF Deregistration request message is represented as an array of dictionaries. Each dictionary contains a deregistration request for a specific protocol version. The array must not contain two dictionaries of the same protocol version. For version “1.0” the request is defined as a DeregistrationRequest dictionary.

EXAMPLE 11: UAF Deregistration Request

```json
{
   "header": {
      "op": "Dereg",
      "upv": {
         "major": 1,
         "minor": 0
      },
      "appID": "https://uaf-test-1.noknoktest.com:8443/SampleApp/uaf/facets"
   },
   "authenticators": [
      {
         "aaid": "ABCD#ABCD",
         "keyID": "ZMCPn92yHv1Ip-iCiBb6i4ADq6ZOv569KpQvCVsJfKq"
      }
   ]
}
```

NOTE

There is no deregistration response object.

3.6.2 DeregisterAuthenticator dictionary

```webidl

dictionary DeregisterAuthenticator {
   required AAID aaid;
   required KeyID keyID;
};
```

3.6.2.1 Dictionary DeregisterAuthenticator Members

- **aaid** of type required AAID  
  AAID of the authenticator to deregister.

- **keyID** of type required KeyID  
  The unique KeyID related to UAuth.priv. KeyID is assumed to be be unique within the scope of an AAID only.

3.6.3 DeregistrationRequest dictionary

```webidl

dictionary DeregistrationRequest {  
   required OperationHeader header;
};
```
required DeregisterAuthenticator[] authenticators;

3.6.3.1 Dictionary DeregistrationRequest Members

header of type required OperationHeader
  Header.op must be "Dereg".

authenticators of type array of required DeregisterAuthenticator
  List of authenticators to be deregistered.

3.6.4 Deregistration Processing Rules

3.6.4.1 Deregistration Request Generation Rules for FIDO Server

The FIDO Server must follow the steps:

1. Create a deregistration request message m with major version of m.header.upv set to 1 and minor version set to 0
2. For each authenticator to be deregistered
   1. Create DeregisterAuthenticator object o for authenticator to be deregistered
   2. Set o.aaid and o.keyID appropriately
   3. Append o the m.authenticators
3. Send message to FIDO UAF Client

3.6.4.2 Deregistration Request Processing Rules for FIDO UAF Client

The FIDO UAF Client must follow the steps:

1. Choose the message with major version 1 and minor version 0
2. Parse the message
   * If a mandatory field in DeregistrationRequest message is not present or a field doesn't correspond to its type and value – reject operation
3. For each authenticator compatible with the message version DeregistrationRequest.header.upv and has an AAID equal to one of the provided AAIDs:
   1. Create appropriate ASMRequest for Deregister function and send it to the Authenticator

3.6.4.3 Deregistration Request Processing Rules for FIDO Authenticator

See [UAFASM] section "Deregister request".

4. Considerations

This section is non-normative.

4.1 Protocol Core Design Considerations

This section describes the important design elements used in the protocol.

4.1.1 Authenticator Metadata

It is assumed that FIDO Server has access to a list of all supported authenticators and their corresponding Metadata. authenticator metadata [UAFAuthnrMetadata] contains information such as:

- Supported Registration and Authentication Schemes
- Authentication Factor, Installation type, supported content-types and other supplementary information, etc.

In order to make a decision about which authenticators are appropriate for a specific transaction, FIDO Server looks up the list of authenticator metadata by AAID and retrieves the required information from it.

NORMATIVE

Each entry in the authenticator metadata repository must be identified with a unique authenticator Attestation ID (AAID).

4.1.2 Authenticator Attestation

Authenticator Attestation is the process of validating authenticator model identity during registration. It allows Relying Parties to cryptographically verify that the authenticator reported by FIDO UAF Client is really what it claims to be.

Using authenticator Attestation, a relying party "example-rp.com" will be able to verify that the authenticator model of the "example-Authenticator", reported with AAID "1234#5678", is not malware running on the FIDO User Device but is really a authenticator of model "1234#5678".

NORMATIVE

FIDO Authenticators should support "Basic Attestation" described below. New Attestation mechanisms may be added to the protocol over time.

NORMATIVE

FIDO Authenticators not providing sufficient protection for Attestation keys (non-attested authenticators) must use the UAuth.priv key in order to formally generate the same KeyRegistrationData object as attested authenticators. This behavior must be properly declared in the Authenticator Metadata.
4.1.2.1 Basic Attestation

**NORMATIVE**

There are two different flavors of Basic Attestation:

**Full Basic Attestation**
Based on an attestation private key shared among a class of authenticators (e.g. same model).

**Surrogate Basic Attestation**
Just syntactically a Basic Attestation. The attestation object self-signed, i.e. it is signed using the UAuth.priv key, i.e. the key corresponding to the UAuth.pub key included in the attestation object. As a consequence it **does not** provide a cryptographic proof of the security characteristics. But it is the best thing we can do if the authenticator is not able to have an attestation private key.

4.1.2.1.1 Full Basic Attestation

**NOTE**
FIDO Servers must have access to a trust anchor for verifying attestation public keys (i.e. Attestation Certificate trust store) in order to follow the assumptions made in [FIDOSecRef]. Authenticators must provide its attestation signature during the registration process for the same reason. The attestation trust anchor is shared with FIDO Servers out of band (as part of the Metadata). This sharing process should be done according to [UAFMetadataService].

**NOTE**
The protection measures of the Authenticator's attestation private key depend on the specific authenticator model's implementation.

**NOTE**
The FIDO Server must load the appropriate Authenticator Attestation Root Certificate from its trust store based on the AAID provided in KeyRegistrationData object.

**NOTE**
In this Full Basic Attestation model, a large number of authenticators must share the same Attestation certificate and Attestation Private Key in order to provide non-linkability (see Protocol Core Design Considerations). Authenticators can only be identified on a production batch level or an AAID level by their Attestation Certificate, and not individually. A large number of authenticators sharing the same Attestation Certificate provides better privacy, but also makes the related private key a more attractive attack target.

**NOTE**
A given set of authenticators sharing the same manufacturer and essential characteristics must not be issued a new Attestation Key before at least 100,000 devices are issued the previous shared key.

![Attestation Certificate Chain](image)

4.1.2.1.2 Surrogate Basic Attestation

**NORMATIVE**
In this attestation method, the UAuth.priv key **must** be used to sign the Registration Data object. This behavior **must** be properly declared in the Authenticator Metadata.

**NOTE**
FIDO Authenticators not providing sufficient protection for Attestation keys (non-attested authenticators) must use this attestation method.

4.1.3 Error Handling
FIDO UAF is designed to be compatible with a variety of existing authenticators (TPMs, Fingerprint Sensors, Secure Elements, etc.) and also future authenticators designed for FIDO. Therefore extensibility is a core capability designed into the protocol.

It is considered that there are two particular aspects that need careful extensibility. These are:

- Cryptographic key provisioning (KeyRegistrationData)
- Cryptographic authentication and signature (SignedData)

The combination of KeyRegistrationData and SignedData schemes is called an Assertion Scheme.

The UAF protocol allows plugging in new Assertion Schemes. See also UAF Supported Assertion Schemes.

The Registration Assertion defines how and in which format a cryptographic key is exchanged between the authenticator and the FIDO Server.

The Authentication Assertion defines how and in which format the authenticator generates a cryptographic signature.

The generally-supported Assertion Schemes are defined in [UAFRegistry].

4.1.5 Username in Authenticator

FIDO UAF supports authenticators acting as first authentication factor (i.e. replacing username and password). In this case the authenticator stores the username (uniquely identifying an account at the specific relying party) internally. See [UAFAuthnrCommands], section "Sign Command" for details.

4.1.6 TLS Protected Communication

In order to protect the data communication between FIDO UAF Client and FIDO Server a protected TLS channel must be used by FIDO UAF Client (or User Agent) and the Relying Party for all protocol elements.

1. The server endpoint of the TLS connection must be at the Relying Party
2. The client endpoint of the TLS connection must be either the FIDO UAF Client or the User Agent / App
3. TLS Client and Server should use TLS v1.2 or newer and should only use TLS v1.1 if TLS v1.2 or higher are not available. The "anon" and "null" TLS crypto suites are not allowed and must be rejected; insecure crypto-algorithms in TLS (e.g. MD5, RC4, SHA1) should be avoided [ISP 800-131A].

We recommend, that the

1. TLS Client verifies and validates the server Certificate chain according to [RFC5280], section 6 "Certificate Path Validation". The certificate revocation status should be checked (e.g. using OCSP [RFC2560] or CRL based validation [RFC5280]) and the TLS server identity should be checked as well [RFC8125].
2. TLS Client's trusted certificate root store is properly maintained and at least requires the CAs included in the root store to annually pass Web Trust or ETSI (ETSI TS 101 456, or ETSI TS 102 042) audits for SSL CAs.

See [TR-03116-4] and [SHEFFER-TLS] for more recommendations on how to use TLS.

4.2 Implementation Considerations

4.2.1 Server Challenge and Random Numbers

A ServerChallenge needs appropriate random sources in order to be effective (see [RFC4086] for more details). The (pseudo-)random numbers used for generating the Server Challenge should successfully pass the randomness test specified in [Doros99] and they should follow the guideline given in [SP800-90b].

4.3 Security Considerations

There is no "one size fits all" authentication method. The FIDO goal is to decouple the user verification method from the authentication protocol and the authentication server, and to support a broad range of user verification methods and a broad range of assurance levels. FIDO authenticators should be able to leverage capabilities of existing computing hardware, e.g. mobile devices or smart cards.

The overall assurance level of electronic user authentications highly depends (a) on the security and integrity of the user's equipment involved and (b) on the authentication method being used to authenticate the user.

When using FIDO, users should have the freedom to use any available equipment and a variety of authentication methods. The relying party needs reliable information about the security relevant parts of the equipment and the authentication method itself in order to determine whether the overall risk of an electronic authentication is acceptable in a particular business context. The FIDO Metadata[UAPMetadataService] is intended to provide such information.

It is important for the UAF protocol to provide this kind of reliable information about the security relevant parts of the equipment and the authentication method itself to the FIDO server.
The overall security is determined by the weakest link. In order to support scalable security in FIDO, the underlying UAF protocol needs to provide a very high conceptual security level, so that the protocol isn't the weakest link.

**Relying Parties define Acceptable Assurance Levels.** The FIDO Alliance envisions a broad range of FIDO UAF Clients, FIDO Authenticators, and FIDO Servers to be offered by various vendors. Relying parties should be able to select a FIDO Server providing the appropriate level of security. They should also be in a position to accept FIDO Authenticators meeting the security needs of the given business context, to compensate assurance level deficits by adding appropriate implicit authentication measures, and to reject authenticators not meeting their requirements. FIDO does not mandate a very high assurance level for FIDO Authenticators, instead it provides the basis for authenticator and user verification method competition.

**Authentication vs. Transaction Confirmation.** Existing Cloud services are typically based on authentication. The user launches an application (i.e. User Agent) assumed to be trusted and authenticates to the Cloud service in order to establish an authenticated communication channel between the application and the Cloud service. After this authentication, the application can perform any actions to the Cloud service using the authenticated channel. The service provider will attribute all those actions to the user. Essentially the user authenticates all actions performed by the application in advance until the service connection or authentication times out. This is a very convenient way as the user doesn't get distracted by manual actions required for the authentication. It is suitable for actions with low risk consequences.

However, in some situations it is important for the relying party to know that a user really has seen and accepted a particular content before he authenticates it. This method is typically being used when non-repudiation is required. The resulting requirement for this scenario is called What You See Is What You Sign (WYSIWYS).

UAF supports both methods; they are called "Authentication" and "Transaction Confirmation". The technical difference is, that a 8th Authentication user confirms a random challenge, where the case of Transaction Confirmation the user also confirms human readable content, i.e. the contract. From a security point, in the case of authentication the application needs to be trusted as it performs any action once the authenticated communication channel has been established. In the case of Transaction Confirmation only the transaction confirmation display component implementing WYSIWYS needs to be trusted, not the entire application.

**Distinct Attestable Security Components.** For the relying party in order to determine the risk associated with an authentication, it is important to know details about some components of the user's environment. Web Browsers typically send a "User Agent" string to the web server. Unfortunately any application could send any string as "User Agent" to the relying party. So this method doesn't provide strong security. FIDO UAF is based on a concept of cryptographic attestation. With this concept, the component to be attested owns a cryptographic secret and authenticates its identity with this cryptographic secret. In FIDO UAF the cryptographic secret is called "Authenticator Attestation Key". The relying party gets access to reference data required for verifying the attestation.

In order to enable the relying party to appropriately determine the risk associated with an authentication, all components performing significant security functions need to be attestable.

In FIDO UAF significant security functions are implemented in the FIDO Authenticators. Security functions are:

1. Protecting the attestation key.
2. Generating and protecting the Authentication key(s), typically one per relying party and user account on relying party.
3. Verifying the user.
4. Providing the WYSIWYS capability ("Transaction Confirmation Display" component).

Some FIDO Authenticators might implement these functions in software running on the FIDO User Device, others might implement these functions in "hardware", i.e. software running on a hardware segregated from the FIDO User Device. Some FIDO Authenticators might even be formally evaluated and accredited to some national or international scheme. Each FIDO Authenticator model has an attestation ID (AAID), uniquely identifying the related security characteristics. Relying parties get access to these security properties of the FIDO Authenticators and the reference data required for verifying the attestation.

**Resilience to leaks from other verifiers.** One of the important issues with existing authentication solutions is a weak server side implementation, affecting the security of authentication of typical users to other relying parties. It is the goal of the FIDO UAF protocol to decouple the security of different relying parties.

**Decoupling User Verification Method from Authentication Protocol.** In order to decouple the user verification method from the authentication protocol, FIDO UAF is based on an extensible set of cryptographic authentication algorithms. The cryptographic secret will be unlocked after user verification by the Authenticator. This secret is then used for the authenticator-to-relying party authentication. The set of cryptographic algorithms is chosen according to the capabilities of existing cryptographic hardware and computing devices. It can be extended in order to support new cryptographic hardware.

**Privacy Protection.** Different regions in the world have different privacy regulations. The FIDO UAF protocol should be acceptable in all regions and hence must support the highest level of data protection. As a consequence, FIDO UAF doesn't require transmission of biometric data to the relying party nor does it require the storage of biometric reference data (ISOBiometrics) at the relying party. Additionally, cryptographic secrets used for different relying parties shall not allow the parties to link actions to the same user entity. UAF supports this concept, known as non-linkability. Consequently, the UAF protocol doesn't require a trusted third party to be involved in every transaction.

Relying parties can interactively discover the AAIDs of all enabled FIDO Authenticators on the FIDO User Device using the Discovery interface [UAFAuthnCommands]. The combination of AAIDs adds to the entropy provided by the client to relying parties. Based on such information, relying parties can fingerprint clients on the internet (see Browser Uniqueness at 4 and https://wiki.mozilla.org/Fingerprinting). In order to minimize the entropy added by FIDO, the user can enable/disable individual authenticators – even when they are embedded in the device (see [UAFAuthnCommands], section "privacy considerations").

### 4.3.1 FIDO Authenticator Security

See [UAFAuthnCommands].

### 4.3.2 Cryptographic Algorithms

In order to keep key sizes small and to make private key operations fast enough for small devices, it is suggested that implementers prefer ECDSA (ECDSA-ANSI) in combination with SHA-256 / SHA-512 hash algorithms. However, the RSA algorithm is also supported. See [UAFRegistry] "Authentication Algorithms and Key Formats" for a list of generally supported cryptographic algorithms.

One characteristic of ECDSA is that it needs to produce, for each signature generation, a fresh random value. For effective security, this value must be chosen randomly and uniformly from a set of modular integers, using a cryptographically secure process. Even slight biases in that process may be turned into attacks on the signature schemes.

**NOTE**

If such random values cannot be provided under all possible environmental conditions, then a deterministic version of ECDSA should be used (see [RFC6979]).

### 4.3.3 Application Isolation
There are two concepts implemented in FIDO UAF to prevent malicious applications from misusing AppID specific keys registered with FIDO Authenticators. First concept is called “FacetID Assertion” and second is based on the "KHAccessToken". For information on the FacetID concept see [FIDOAppIDAndFacets].

4.3.3.1 Isolation using KHAccessToken

Authenticators might be implemented in dedicated hardware and hence might not be able to verify the calling software entity (i.e. the ASM).

The KHAccessToken allows restricting access to the keys generated by the FIDO Authenticator to the intended ASM. It is based on a Trust On First Use (TOFU) concept.

FIDO Authenticators are capable of binding UAuth.Key with a key provided by the caller (i.e. the ASM). This key is called KHAccessToken.

This technique allows making sure that registered keys are only accessible by the caller that originally registered them. A malicious App on a mobile platform won’t be able to access keys by bypassing the related ASM (assuming that this ASM originally registered these keys).

The KHAccessToken is typically specific to the AppID, PersonaID, ASMToken and the CallerID. See [UAFASM] for more details.

NOTE

On some platforms, the ASM additionally might need special permissions in order to communicate with the FIDO Authenticator. Some platforms do not provide means to reliably enforce access control among applications.

4.3.4 TLS Binding

Various channel binding methods have been proposed (e.g. [RFC5929] and [ChannelID]).

UAF relies on TLS server authentication for binding authentication keys to AppIDs. There are threats:

1. Attackers might fraudulently get a TLS server certificate for the same AppID as the relying party and they might be able to manipulate the DNS system.
2. Attackers might be able to steal the relying party’s TLS server private key and certificate and they might be able to manipulate the DNS system.

And there are functionality requirements:

1. UAF transactions might span across multiple TLS sessions. As a consequence, “tls-unique” defined in [RFC5929] might be difficult to implement.
2. Data centers might use SSL concentrators.
3. Data centers might implement load-balancing for TLS endpoints using different TLS certificates. As a consequence, "tls-server-end-point" defined in [RFC5929], i.e. the hash of the TLS server certificate might be inappropriate.
4. Unfortunately, hashing of the TLS server certificate (as in "tls-server-end-point") also limits the usefulness of the channel binding in a particular, but quite common circumstance. If the client is operated behind a trusted (to that client) proxy that acts as a TLS man-in-the-middle, your client will see a different certificate than the one the server is using. This is actually quite common on corporate or military networks with a high security posture that want to inspect all incoming and outgoing traffic. If the FIDO Server just gets a hash value, there’s no way to distinguish this from an attack. If sending the entire certificate is acceptable from a performance perspective, the server can examine it and determine if it is a certificate for a valid name from a non-standard issuer (likely administratively trusted) or a certificate for a different name (which almost certainly indicates a forwarding attack).
FIDO Server will detect such changes if the modified value is unacceptable.

### 4.3.5 Session Management

FIDO does not define any specific session management methods. However, several FIDO functions rely on a robust session management being implemented by the relying party’s web application:

**FIDO Registration**

A web application might trigger FIDO Registration after authenticating an existing user via legacy credentials. So the session is used to maintain the authentication state until the FIDO Registration is completed.

**FIDO Authentication**

After success FIDO Authentication, the session is used to maintain the authentication state during the operations performed by the user agent or mobile app.

Best practices should be followed to implement robust session management (e.g. [OWASP2013]).

### 4.3.6 Personas

FIDO supports unlinkability [AnonTerminology] of accounts at different relying parties by using relying party specific keys. Sometimes users have multiple accounts at a particular relying party and even want to maintain unlinkability between these accounts. Today, this is difficult and requires certain measures to be strictly applied.

FIDO does not want to add more complexity to maintaining unlinkability between accounts at a relying party. In the case of roaming authenticators, it is recommended to use different authenticators for the various personas (e.g. "business", "personal"). This is possible as roaming authenticators typically are small and not excessively expensive.

In the case of bound authenticators, this is different. FIDO recommends the "Persona" concept for this situation. All relevant data in an authenticator are related to one Persona (e.g. "business" or "personal"). Some administrative interface (not standardized by FIDO) of the authenticator may allow maintaining and switching Personas.

<table>
<thead>
<tr>
<th>NORMATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The authenticator must only &quot;know&quot; / &quot;recognize&quot; data (e.g. authentication keys, usernames, KeyIDs, ...) related to the Persona being active at that time.</td>
</tr>
</tbody>
</table>

With this concept, the User can switch to the "Personal" Persona and register new accounts. After switching back to "Business" Persona, these accounts will not be recognized by the authenticator (until the User switches back to "Personal" Persona again).

In order to support the persona feature, the FIDO Authenticator-specific Module API [UAFASM] supports the use of a PersonasID to identify the persona in use by the authenticator. How Personas are managed or communicated with the user is out of scope for FIDO.

### 4.3.7 ServerData and KeyHandle

Data contained in the field serverData (see Operation Header dictionary) of UAF requests is sent to the FIDO UAF Client and will be echoed back to the FIDO Server as part of the related UAF response message.

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The FIDO Server should not assume any kind of implicit integrity protection of such data nor any implicit session binding. The FIDO Server must explicitly bind the serverData to an active session.</td>
</tr>
</tbody>
</table>

In some situations, it is desirable to protect sensitive data such that it can be stored in arbitrary places (e.g. in serverData or in the KeyHandle). In such situations, the confidentiality and integrity of such sensitive data must be protected. This can be achieved by using a suitable encryption algorithm, e.g. AES with a suitable cipher mode, e.g. CBC or CTR [CTRMode]. This cipher mode needs to be used correctly. For CBC, for example, a fresh random IV for each encryption is required. The data might have to be padded first in order to obtain an integral number of blocks in length. The integrity protection can be achieved by adding a MAC or a digital signature on the ciphertext, using a different key than for the encryption, e.g. using HMAC [FIPS198-1]. Alternatively, an authenticated encryption scheme such as AES-GCM [SP800-38D] or AES-CCM [SP800-38C] could be used. Such a scheme provides both integrity and confidentiality in a single algorithm and using a single key.

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>When protecting serverData, the MAC or digital signature computation should include some data that binds the data to its associated message, for example by re-including the challenge value in the authenticated serverData.</td>
</tr>
</tbody>
</table>

### 4.3.8 Authenticator Information retrieved through UAF Application API vs. Metadata

Several authenticator properties (e.g. UserVerificationMethods, KeyProtection, TransactionConfirmationDisplay, ...) are available in the Metadata [UAAuthnrMetadata] and through the FIDO UAF Application API. The properties included in the metadata are authoritative and are provided by a trusted source. When in doubt, decisions should be based on the properties retrieved from the Metadata as opposed to the data retrieved through the FIDO UAF Application API.

However, the properties retrieved through the FIDO UAF Application API provide a good "hint" what to expect from the Authenticator. Such "hints" are well suited to drive and optimize the user experience.

### 4.3.9 Policy Verification

FIDO UAF Response messages do not include all parameters received in the related FIDO UAF request message into the to-be-signed object. As a consequence, any MITM could modify such entries.

FIDO Server will detect such changes if the modified value is unacceptable.
For example, a MITM could replace a generic policy by a policy specifying only the weakest possible FIDO Authenticator. Such a change will be detected by FIDO Server if the weakest possible FIDO Authenticator does not match the initial policy (see Registration Response Processing Rules and Authentication Response Processing Rules).

4.3.10 Replay Attack Protection

The FIDO UAF protocol specifies two different methods for replay-attack protection:

1. Secure transport protocol (TLS)
2. Server Challenge.

The TLS protocol by itself protects against replay-attacks when implemented correctly [TLS].

Additionally, each protocol message contains some random bytes in the ServerChallenge field. The FIDO server should only accept incoming FIDO UAF messages which contain a valid ServerChallenge value. This is done by verifying that the ServerChallenge value, sent by the client, was previously generated by the FIDO server. See FinalChallengeParams.

It should also be noted that under some (albeit unlikely) circumstances, random numbers generated by the FIDO server may not be unique, and in such cases, the same ServerChallenge may be presented more than once, making a replay attack harder to detect.

4.3.11 Protection against Cloned Authenticators

FIDO UAF relies on the UAuth.Key to be protected and managed by an authenticator with the security characteristics specified for the model (identified by the AAID). The security is better when only a single authenticator with that specific UAuth.Key instance exists. Consequently FIDO UAF specifies some protection measures against cloning of authenticators.

Firstly, if the UAuth private keys are protected by appropriate measures then cloning should be hard as such keys cannot be extracted easily. Secondly, FIDO specifies a Signature Counter (see Authentication Response Processing Rules and [UAFAuthnrCommands]). This counter is increased by every signature operation. If a cloned authenticator is used, then the subsequent use of the original authenticator would include a signature counter lower to or equal to the previous (malicious) operation. Such an incident can be detected by the FIDO Server.

4.3.12 Anti-Fraud Signals

There is the potential that some attacker misuses a FIDO Authenticator for committing fraud, more specifically they would

1. Register the authenticator to some relying party for one account
2. Commit fraud
3. Deregister the Authenticator
4. Register the authenticator to some relying party for another account
5. Commit fraud
6. Deregister the Authenticator
7. and so on...

NOTE

Authenticators might support a Registration Counter (RegCounter). The RegCounter will be incremented on each registration and hence might become exceedingly high in such fraud scenarios. See [UAFAuthnrCommands] for more details.

4.4 Interoperability Considerations

FIDO supports Web Applications, Mobile Applications and Native PC Applications. Such applications are referred to as FIDO enabled applications.

Web applications typically consist of the web application server and the related Web App. The Web App code (e.g. HTML and JavaScript) is rendered and executed on the client side by the User Agent. The Web App code talks to the User Agent via a set of JavaScript APIs, e.g. HTML DOM. The FIDO DOM API is defined in [UAFAppAPIAndTransport]. The protocol between the Web App and the Relying Party Web Application Server is typically proprietary.
Mobile Apps play the role of the User Agent and the Web App (Client). The protocol between the Mobile App and the Relying Party Web Application Server is typically proprietary.

Native PC Applications play the role of the User Agent, the Web App (Client). Those applications are typically expected to be independent from any particular Relying Party Web Application Server.

It is recommended for FIDO enabled applications to use the FIDO messages according to the format specified in this document.

It is recommended for FIDO enabled application to use the UAF HTTP Binding defined in [UAFAppAPIAndTransport].

5. UAF Supported Assertion Schemes

This section is normative.

5.1 Assertion Scheme "UAFV1TLV"

This Assertion Scheme allows the authenticator and the FIDO Server to exchange an asymmetric authentication key generated by the Authenticator.

This assertion scheme is using Tag Length Value (TLV) compact encoding to encode registration and authentication assertions generated by authenticators. This is the default assertion scheme for UAF protocol.

TAGs and Algorithms are defined in [UAFRegistry].

The authenticator must use a dedicated key pair (UAuth.pub/UAuth.priv) suitable for the authentication algorithm specified in the Metadata statement [UAFAuthnMetadata] for each relying party. This key pair should be generated as part of the registration operation.

Conforming FIDO Servers must support all authentication algorithms and key formats listed in document [UAFRegistry].

Conforming authenticators must support at least one Authentication Algorithm and one Key Format listed in [UAFRegistry].

5.1.1 KeyRegistrationData

See [UAFAuthnCommands], section "TAG_UAFV1_KRD".

5.1.2 SignedData

See [UAFAuthnCommands], section "TAG_UAFV1_SIGNED_DATA".

6. Definitions

See [FIDOGlossary].

7. Table of Figures

   Fig. 1 The UAF Architecture
   Fig. 2 UAF Registration Message Flow
   Fig. 3 Authentication Message Flow
   Fig. 4 Transaction Confirmation Message Flow
   Fig. 5 Deregistration Message Flow
   Fig. 6 UAF Registration Sequence Diagram
   Fig. 7 UAF Registration Cryptographic Data Flow
   Fig. 8 UAF Authentication Sequence Diagram
   Fig. 9 UAF Authentication Cryptographic Data Flow
   Fig. 10 Attestation Certificate Chain
   Fig. 11 FIDO Entity Verification Overview
   Fig. 12 FIDO Interoperability Overview

A. References

A.1 Normative references


[FIDOGlossary]