FIDO ECDAA Algorithm

FIDO Alliance Proposed Standard 23 May 2022

This version:

Previous version:

Editor:
Rolf Lindemann, Nok Nok Labs, Inc.

Contributors:
Jan Camenisch, IBM
Manu Drijvers, IBM
Alec Edgington, Trustonic
Anja Lehmann, IBM
Rainer Urian, Infineon

The English version of this specification is the only normative version. Non-normative translations may also be available.

Copyright © 2013-2022 FIDO Alliance All Rights Reserved.

Abstract

The FIDO Basic Attestation scheme uses attestation "group" keys shared across a set of authenticators with identical characteristics in order to preserve privacy by avoiding the introduction of global correlation handles. If such an attestation key is extracted from one single authenticator, it is possible to create a "fake" authenticator using the same key and hence indistinguishable from the original authenticators by the relying party. Removing trust for registering new authenticators with the related key would affect the entire set of authenticators sharing the same "group" key. Depending on the number of authenticators, this risk might be unacceptable high.

This is especially relevant when the attestation key is primarily protected against malware attacks as opposed to targeted physical attacks.

An alternative approach to "group" keys is the use of individual keys combined with a Privacy-CA [TPMv1-2-Part1]. Translated to FIDO, this approach would require one Privacy-CA interaction for each Uauth key. This means relatively high load and high availability requirements for the Privacy-CA. Additionally the Privacy-CA aggregates sensitive information (i.e. knowing the relying parties the user interacts with). This might make the Privacy-CA an interesting attack target.

Another alternative is the Direct Anonymous Attestation [BriCamChe2004-DAA]. Direct Anonymous Attestation is a cryptographic scheme combining privacy with security. It uses the authenticator specific secret once to communicate with a single DAA Issuer and uses the resulting DAA credential in the DAA-Sign protocol with each relying party. The DAA scheme has been adopted by the Trusted Computing Group for TPM v1.2 [TPMv1-2-Part1].

In this document, we specify the use of an improved DAA scheme based on [CamDriLeh16-DAA] [CCDLNU2017-DAA] that uses elliptic curves and bilinear pairings.

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://fidoalliance.org/specifications/.

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

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
1. Notation

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

String literals are enclosed in “”, e.g. “ED256”.

In formulas we use “||” to denote byte wise concatenation operations.

\( X = P^x \) denotes scalar multiplication (with scalar x) of a (elliptic) curve point P.

RAND(x) denotes generation of a random number between 0 and x-1.

RAND(G) denotes generation of a random number belonging to Group G.

Specific terminology used in this document is defined in [FIDO Glossary].

The type BigNumber denotes an arbitrary length integer value.

The type ECPoint denotes an elliptic curve point with its affine coordinates x and y.
The type ECPoint2 denotes a point on the sextic twist of a BN elliptic curve over \( F(q^2) \). The ECPoint2 has two affine coordinates each having two components of type BigNumber.

1.1 Conformance

As well as sections marked as non-normative, all authoring guidelines, diagrams, examples, and notes in this specification are non-normative. Everything else in this specification is normative.

The key words MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL in this specification are to be interpreted as described in [RFC2119].

2. Overview

This section is non-normative.

FIDO uses the concept of attestation to provide a cryptographic proof of the authenticator [FIDOGlossary] model to the relying party. When the authenticator is registered to the relying party (RP), it generates a new authentication key pair and includes the public key in the attestation message (also known as key registration data object, KRD). When using the ECDAA algorithm, the KRD object is signed using 3.5 ECDAA-Sign.

For privacy reasons, the authentication key pair is dedicated to one RP (to an application identifier AppID [FIDOGlossary] to be more specific). Consequently the attestation method needs to provide the same level of unlinkability. This is the reason why the FIDO ECDAA Algorithm doesn't use a basename (bsn) often found in other direct anonymous attestation algorithms, e.g. [BriCamChe2004-DAA] or [BFGSW-2011].

The authenticator encapsulates all user verification operations and cryptographic functions. An authenticator specific module (ASM) [FIDOGlossary] is used to provide a standardized communication interface for authenticators. The authenticator might be implemented in separate hardware or trusted execution environments. The ASM is assumed to run in the normal operating system (e.g. Android, Windows, ...).

2.1 Scope

This document describes the FIDO ECDAA attestation algorithm in detail.

2.2 Architecture Overview

ECDAA attestation defines global system parameters and ECDAA Issuer specific parameters. Both parameter sets need to be installed on the host, in the authenticator and in the FIDO Server. The ECDAA method consists of two steps:

- **ECDAA-Join** between the authenticator and the ECDAA Issuer to be performed before the first FIDO Registration. The ECDAA Issuer represents the authenticator vendor as it provides the credentials to attest the authenticator model.
  - \((n, B, sc, yc) = \text{GetNonceFromECDAAIssuer()}\)
  - \((D=Q, c1, s1) = \text{EcdaaJoin1}(X, Y, B, sc, yc, n)\)
  - \((A, B, C, D) = \text{EcdaaIssuerJoin}(Q, c1, s1)\)
  - \(\text{EcdaaJoin2}(A, C) \ // \text{store cre=(A, B, C, D)}\)

- and the pair of **ECDAA-Sign** performed by the authenticator and **ECDAA-Verify** performed by the FIDO Server of the relying party as part of the FIDO Registration.
  - Client: Attestation = (signature, KRD) = EcdaaSign(AppID)
  - Server: success=EcdaaVerify(signature, KRD, AppID)

The technical implementation details of the ECDAA-Join step are out-of-scope for FIDO. In this document we normatively specify the general algorithm to the extent required for interoperability and we outline examples of some possible implementations for this step.

The ECDAA-Sign and ECDAA-Verify steps and the encoding of the related ECDAA Signature are normatively specified in this document. The generation and encoding of the KRD object is defined in other FIDO specifications.

The algorithm and terminology are inspired by [BFGSW-2011]. The algorithm was modified in order to fix security weaknesses (e.g. as mentioned by [ANZ-2013] and [XYZF-2014]). Our algorithm proposes an improved task split for the sign operation while still being compatible to TPMv2 (without fixing the TPMv2 weaknesses in such case).

3. FIDO ECDAA Attestation

This section is normative.

3.1 Object Encodings

We need to convert BigNumber and ECPoint objects to byte strings using the following encoding functions:

3.1.1 Encoding BigNumber values as byte strings (BigNumberToB)

We use the I2OSP algorithm as defined in [RFC3447] for converting big numbers to byte arrays. The bytes from the big endian encoded (non-negative) number \( n \) will be copied right-aligned into the buffer area \( b \). The unused bytes will be set to 0. Negative values will not occur due to the construction of the algorithms.

**EXAMPLE 1:** Converting BigNumber \( n \) to byte string \( b \)

\[
\begin{bmatrix}
b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\
\end{bmatrix}
\]
The algorithm implemented in Java looks like this:

```java
ByteArray BigNumberToB(BigNumber inVal, // IN: number to convert
int size         // IN: size of the output.
) {
    ByteArray buffer = new ByteArray(size);
    int oversize = size - inVal.length;
    if (oversize < 0)
        return null;
    for (int i=oversize; i > 0; i--)
        buffer[i] = 0;
    ByteCopy( inVal.bytes, &buffer[oversize], inVal.length);
    return buffer;
}
```

3.1.2 Encoding `ECPoint` values as byte strings (ECPointToB)

We use the ANSI X9.62 Point-to-Octet-String [ECDSA-ANSI] conversion using the expanded format, i.e. the format where the compression byte (i.e. 0x04 for expanded) is followed by the encoding of the affine x coordinate, followed by the encoding of the affine y coordinate.

```java
{x, y} = ECPointGetAffineCoordinates(P)
len = G1.byteLength
byte string = 0x04 | BigIntegerToB(x,len) | BigIntegerToB(y,len)
```

3.1.3 Encoding `ECPoint2` values as byte strings (ECPoint2ToB)

The type `ECPoint2` denotes a point on the sextic twist of a BN elliptic curve over \( F_q \), see section 4.1 Supported Curves for ECDAA. Each `ECPoint2` is represented by a pair \((a, b)\) of elements of \( F_q \).

The group zero element is always encoded (using the encoding rules as described below) as an element having all components set to zero (i.e. \( cx.a=0 \), \( cx.b=0 \), \( cy.a=0 \), \( cy.b=0 \)).

We always assume normalized (non-zero) `ECPoint2` values (i.e. \( cz = 1 \)) before encoding them. Non-zero values are encoded using the expanded format (i.e. 0x04 for expanded) followed by the \( cx \) followed by the \( cy \) value. This leads to the concatenation of 0x04 followed by the first element \((cx.a)\) and second element \((cx.b)\) of the pair of \( cx \) followed by the first element \((cy.a)\) and second element \((cy.b)\) of the pair of \( cy \). All individual numbers are padded to the same length (i.e. the maximum byte length of all relevant 4 numbers).

```java
{cx, cy} = ECPointGetAffineCoordinates(P2)
len = G2.byteLength
byte string = 0x04 | BigIntegerToB(cx.a,len) | BigIntegerToB(cx.b,len)
| BigIntegerToB(cy.a,len) | BigIntegerToB(cy.b,len)
```

3.2 Global ECDAA System Parameters

1. Groups \( G_1, G_2 \) and \( G_T \), of sufficiently large prime order \( p \)
2. Two generators \( P_1 \) and \( P_2 \), such that \( G_1 = \langle P_1 \rangle \) and \( G_2 = \langle P_2 \rangle \)
3. A bilinear pairing \( e : G_1 \times G_2 \rightarrow G_T \). We propose the use of "ate" pairing (see [BarNae-2006]). For example source code on this topic, see BNPairings.
4. Hash function \( H \) with \( H : \{0,1\}^* \rightarrow \mathbb{Z}_p \)
5. \( (G_1, P_1, p, H) \) are installed in all authenticator(s) implementing FIDO ECDAA attestation.

**Definition of \( G_1, G_2, G_T, \) Pairings, hash function \( H() \)**

See section 4.1 Supported Curves for ECDAA.

3.3 Issuer Specific ECDAA Parameters

ECDAA Issuer Parameters parl consist of the following values:

1. Randomly generated ECDAA Issuer private key \( isk = (x, y) \) with \( [x, y = RAND(p)] \).
2. ECDAA Issuer public key \((X, Y)\), with \( X = P_1^x \) and \( Y = P_2^y \).
3. A proof that the ECDAA Issuer key was correctly computed
   1. `BigInteger \( r_x = RAND(p) \)`
   2. `BigInteger \( r_y = RAND(p) \)`
   3. `ECPoint2 \( U_s = P_2^x \)`
4. ECP\textsuperscript{2} \( U_2 = P^2 \)
5. BigInteger \( c = H(U_1 | U_1 | P_2 | X | Y) \)
6. BigInteger \( s_x = r_x + c \cdot x \pmod p \)
7. BigInteger \( s_y = r_y + c \cdot y \pmod p \)

4. ipk = \( X, Y, c, s_x, s_y \)

Whenever a party uses ipk for the first time, it must first verify that it was correctly generated:

\[
H(P^2_2 \cdot X^c | P^2_2 \cdot Y^c | P_2 | X | Y) \oplus c
\]

NOTE

\[
P_2^x \cdot X^c = P_2^x \cdot X^c = P_2^x = U_x
\]
\[
P_2^y \cdot Y^c = P_2^y \cdot Y^c = P_2^y = U_y
\]

The ECDAA Issuer public key \( c \) must be dedicated to a single authenticator model.

We use the element \( c \) of ipk as an identifier for the ECDAA Issuer public key (called ECDAA Issuer public key identifier).

3.4 ECDAA-Join

NOTE

One ECDAA-Join operation is required once in the lifetime of an authenticator prior to the first registration of a credential.

In order to use ECDAA, the authenticator must first receive ECDAA credentials from an ECDAA Issuer. This is done by the ECDAA-Join operation. This operation needs to be performed a single time (before the first credential registration can take place). After the ECDAA-Join, the authenticator will use the ECDAA-Sign operation as part of each FIDO Registration. The ECDAA Issuer is not involved in this step. ECDAA plays no role in FIDO Authentication / Transaction Confirmation operations.

In order to use ECDAA, (at least) one ECDAA Issuer is needed. The approach specified in this document easily scales to multiple ECDAA Issuer s, e.g. one per authenticator vendor. FIDO lets the authenticator vendor choose any ECDAA Issuer (similar to his current freedom for selecting any PKI infrastructure/service provider to issuing attestation certificates required for FIDO Basic Attestation).

- All ECDAA-Join operations (of the related authenticator s) are performed with one of the ECDAA Issuer entities.
- Each ECDAA Issuer has a set of public parameters, i.e. ECDAA public key material. The related Attestation Trust Anchor is contained in the metadata of each authenticator model identified by its AAGUID.

There are two different implementation options relevant for the authenticator vendors (the authenticator vendor can freely choose them):

1. In-Factory ECDAA-Join
2. Remote ECDAA-Join

In the first case, physical proximity is used to locally establish the trust between the ECDAA Issuer and the authenticator (e.g. using a key provisioning station in a production line). There is no requirement for the ECDAA Issuer to operate an online web service.

In the second case, some credential is required to remotely establish the trust between the ECDAA Issuer and the authenticator. As this operation is performed once and only with a single ECDAA Issuer, privacy is preserved and an authenticator specific credential can and should be used.

Not all ECDAA authenticator s might be able to add their authenticator model IDs (e.g. AAGUID) to the registration assertion (e.g. TPMs). In all cases, the ECDAA Issuer will be able to derive the exact authenticator model from either the credential or the physically proximate authenticator. So the ECDAA Issuer root key must be dedicated to a single authenticator model.

3.4.1 ECDAA-Join Algorithm

This section is normative.

NOTE

If this join is not in-factory, the value Q must be authenticated by the authenticator. Upon receiving this value, the ECDAA Issuer must verify that this authenticator did not join before.

1. The authenticator asks the ECDAA Issuer for the B value of the credential.
2. The ECDAA Issuer chooses a nonce BigInteger \( m = \text{RAND}(p) \) such that \( x = H(m) \) is on the curve and \( y_c = \sqrt{((x^2 + b) \pmod q)} \).
3. The ECDAA Issuer computes the B value of the credential as
4. The ECDAA Issuer sends m and yc to the authenticator.

5. The authenticator verifies that \( yc \geq H(m)^3 + b \), with b being the b-Value of the related curve.

6. The authenticator chooses and stores the ECDAA private key BigInteger \( sk = \text{RAND}(p) \)

7. The authenticator re-computes \( B = (H(m), yc) \)

8. The authenticator computes its ECDAA public key ECPoint \( Q = B^{sk} \)

9. The authenticator proves knowledge of \( sk \) as follows
   1. BigInteger \( r_1 = \text{RAND}(p) \)
   2. ECPoint \( U_1 = B^{r_1} \)
   3. BigInteger \( c_2 = H(U_1 \| B \| Q \| m) \)
   4. BigInteger \( n = \text{RAND}(p) \)
   5. BigInteger \( c_1 = H(n \| c_2) \)
   6. BigInteger \( s_1 = r_1 + c_1 \cdot sk \)

10. The authenticator sends \( Q, c_1, s_1, n \) via the ASM to the ECDAA Issuer.

11. The ECDAA Issuer verifies that the authenticator is "authentic" and that \( Q \) was indeed generated by the authenticator. In the case of an in-factory Join, this might be trivial; in the case of a remote Join this typically requires the use of other cryptographic methods. Since ECDAA-Join is a one-time operation, unlinkability is not a concern for that.

12. The ECDAA Issuer verifies that \( Q \in G_1 \) and verifies \( H(n \| H(B^{r_1} \cdot Q^{-c_1} \| B \| Q \| m)) \equiv c_1 \) (check proof-of-possession of private key).

### NOTE
\[
B^{r_1} \cdot Q^{-c_1} = B^{r_1 + c_1 \cdot sk} \cdot Q^{-c_1} = B^{r_1 + c_1 \cdot sk} \cdot B^{-c_1 \cdot sk} = B^{r_1} = U_1
\]

13. The ECDAA Issuer creates credential \((A, B, C, D)\) as follows
   1. ECPoint \( A = B^{l_1} \)
   2. ECPoint \( B \) as computed in the beginning.
   3. ECPoint \( C = (A \cdot Q)^{r_1} \)
   4. ECPoint \( D = Q \)

14. The ECDAA Issuer sends \( A, C \) to the authenticator. The authenticator still knows \( B \) and \( D \)

15. The authenticator checks that \( A, C \in G_1 \) and \( A \neq 1_{G_1} \)

16. The authenticator checks \( e(A, Y) \equiv e(B, P_2) \)

### NOTE
\[
e(A, Y) = e(B^{l_1}, P_2^x) = e(B, P_2^{l_1}) = e(B, P_2);
\]

17. and the authenticator checks \( e(C, P_2) \equiv e(A \cdot D, X) \)

### NOTE
\[
e(C, P_2) = e((A \cdot Q)^{r_1}, P_2); e(A \cdot D, X) = e(A \cdot Q, P_2^x) = e((A \cdot Q)^{r_1}, P_2)
\]

18. The authenticator stores credential \((A, B, C, D)\)

### 3.4.2 ECDAA-Join Split between Authenticator and ASM

This section is non-normative.

### NOTE
If this join is not in-factory, the value \( Q \) must be authenticated by the authenticator. Upon receiving this value, the authenticator did not join before.

1. The ASM asks the ECDAA Issuer for the B value of the credential.
2. The ECDAA Issuer chooses a nonce $m = \text{RAND}(p)$ such that $x = H(m)$ is on the curve and $yc = \sqrt{(x + b) \mod q}$.

3. The ECDAA Issuer computes the B value of the credential as $B = (H(m), yc)$.

4. The ECDAA Issuer sends $m$ and $yc$ to the ASM.

5. The ASM forwards $m$ and $yc$ to the authenticator.

6. The authenticator verifies that $yc^2 \equiv H(m)^3 + b$, with $b$ being the $b$-Value of the related curve.

7. The authenticator chooses and stores the private key $sk = \text{RAND}(p)$.

8. The authenticator re-computes $B = (H(m), yc)$.

9. The authenticator computes its ECDAA public key $ECPoint Q = B^{sk}$.

10. The authenticator proves knowledge of $sk$ as follows:

1. BigInteger $r_1 = \text{RAND}(p)$
2. ECPoint $U_1 = B^r$
3. BigInteger $c_2 = H(U_1|B|Q|m)$
4. BigInteger $n = \text{RAND}(p)$
5. BigInteger $c_1 = H(n|c_2)$
6. BigInteger $s_1 = r_1 + c_1 \cdot sk$

11. The authenticator sends $Q, c_1, s_1, n$ to the ASM, who forwards it to the ECDAA Issuer.

12. The ECDAA Issuer verifies that the authenticator is "authentic" and that $Q$ was indeed generated by the authenticator. In the case of an in-factory Join, this might be trivial; in the case of a remote Join this typically requires the use of other cryptographic methods. Since ECDAA-Join is a one-time operation, unlinkability is not a concern for that.

13. The ECDAA Issuer verifies that $Q \in G_1$ and verifies $H(n|H(B^{n_1}.Q^{c_1}|B|Q|m)) \equiv c_1$.

14. The ECDAA Issuer creates credential $(A, B, C, D)$ as follows:

1. ECPoint $A = B^{1/y}$
2. ECPoint $B$ as computed in the beginning.
3. ECPoint $C = (A \cdot Q)^x$
4. ECPoint $D = Q$

15. The ECDAA Issuer sends $A, C$ to the ASM. The ASM remembered $B$ and $D = Q$ from an earlier step.

16. The ASM checks that $A, B, C, D \in G_1$ and $A \neq 1_{G_1}$.

17. The ASM checks $e(A, Y) \equiv e(B, P_2)$.

18. and the ASM checks that $e(C, P_2) \equiv e(A \cdot D, X)$.


20. The authenticator stores $B, D$ and ignores further join requests.

NOTE
These values belong to the ECDAA secret key $sk$. They should persist even in the case of a factory reset.

### 3.4.3 ECDAA-Join Split between TPM and ASM

This section is non-normative.

NOTE
The Endorsement key credential (EK-C) and TPM2_ActivateCredentials are used for supporting the remote Join.

This description is based on the principles described in [TPMv2-Part1] section 24 and [Arthur-Challener-2015], page 109 ("Activating a Credential").

1. The ASM asks the ECDAA Issuer for the B value of the credential.
2. The ECDAA Issuer chooses a nonce $m = \text{RAND}(p)$ such that $x = H(m)$ is on the curve and $yc = \sqrt{((x + b) \mod q)}$.
3. The ECDAA Issuer computes the B value of the credential as $B = (H(m), yc)$.
4. The ECDAA Issuer sends $m$ and $yc$ to the ASM.
5. The ASM instructs the TPM to create a restricted key by calling TPM2_Create, giving the public key template TPMT_PUBLIC [TPMv2-Part2] (including the public key $P_1$ in field unique) to the ASM.
6. re-computes $B = (H(m), yc)$.
3. retrieves TPM Endorsement Key Certificate (EK-C) from the TPM

4. calls TPM2_Commit(keyhandle, P1) where keyhandle is the handle of the restricted key generated before (see above), P1 is set to (B.x,B.y), and s2 and y2 are set to B.x and B.y respectively. This call returns K, E, and ctr; where \(K = B^k = Q\), \(E = B^r\) is used as \(U\) value.

5. computes BigInteger \(c_2 = H(U || B || Q || m)\)

6. calls TPM2_Sign(\(c_2\), ctr), returning \(s, n\), where \(n = \text{RAND}(p)\), and \(s_1 = r_1 + c_1 \cdot sk\).

7. computes BigInteger \(c = H(n || c_2)\)

8. sends EK-C, \(\text{TPMT\_PUBLIC}\) (including \(Q\) in field \text{unique}), \(c, s, n\) to the ECDAA Issuer.

6. The ECDAA Issuer

1. verifies EK-C and its certificate chain. As a result the ECDAA Issuer knows the TPM model related to EK-C.

2. verifies that this EK-C was not used in a (successful) Join before

3. Verifies that the \text{objectAttributes} in \text{TPMT\_PUBLIC}[\text{TPMv2-Part2}] matches the following flags: \text{fixedTPM} = 1; \text{fixedParent} = 1; \text{sensitiveDataOrigin} = 1; \text{restricted} = 1; \text{encrypt} = 0; \text{sign} = 1.

4. examines the public key \(Q\), i.e. it verifies that \(Q \in G\)

5. checks \(H(n || H(B \cdot Q || B || Q || m)) = c_1\)

6. generates the ECDAA credential \((A, B, C, D)\) as follows
   1. ECPoint \(A = B^1\)
   2. ECPoint \(B\) as computed in the beginning.
   3. ECPoint \(C = (A \cdot Q)^x\)
   4. ECPoint \(D = Q\)

7. generates a secret (derived from a seed) and wraps the credential \(A, B, C, D\) using that secret.

8. encrypts the seed using the public key included in EK-C.

9. uses seed and name in KDFa (see [TPMv2-Part2] section 24.4) to derive HMAC and symmetric encryption key. Wrap the secret in symmetric encryption key and protect it with the HMAC key.

NOTE
The parameter name in KDFa is derived from \text{TPMT\_PUBLIC}, see [TPMv2-Part1], section 16.

10. sends the wrapped object including the credential from previous step to the ASM.

7. The ASM instructs the TPM (by calling TPM2_ActivateCredential) to

1. decrypt the seed using the TPM Endorsement key

2. compute the name (for the ECDAA attestation key)

3. use the seed in KDFa (with name) to derive the HMAC key and the symmetric encryption key.

4. use the symmetric encryption key to unwrap the secret.

8. The ASM

1. unwraps the credential \(A, B, C, D\) using the secret received from the TPM.

2. checks that \(A, B, C, D \in G_1\) and \(A \neq 1_{G_1}\)

3. checks \(e(A, Y) = e(B, P_2)\) and \(e(C, P_2) = e(A \cdot D, X)\)

4. stores \(A, B, C, D\)

3.5 ECDAA-Sign

NOTE
One ECDAA-Sign operation is required for the client-side environment whenever a new credential is being registered at a relying party.

3.5.1 ECDAA-Sign Algorithm

This section is normative.

\((\text{signature}, \text{KRD}) = \text{EcdaaSign(String AppID)}\)

Parameters

- \(p\): System parameter prime order of group G1 (global constant)
- \(\text{AppID}\): FIDO AppID (i.e. https-URL of TrustedFacets object)

Algorithm outline...
1. \( KRD = \text{BuildAndEncodeKRD}() \); // all traditional Registration tasks are here (e.g. key generation)
2. \( l = \text{RAND}(p) \); // use same random number algorithm as for key generation in step 1
3. ECPoint \( R = A^l \);
4. ECPoint \( S = B^l \);
5. ECPoint \( T = C^l \);
6. ECPoint \( W = D^l \);
7. BigInteger \( r = \text{RAND}(p) \); // use same random number algorithm as for key generation in step 1
8. ECPoint \( U = S^r \);
9. BigInteger \( c^2 = H(U||S||W||AppID||H(KRD)) \)
10. BigInteger \( n = \text{RAND}(p) \); // use same random number algorithm as for key generation in step 1
11. \( c = H(n \ | \ c^2) \)
12. BigInteger \( s = r + c \cdot sk \mod p \)
13. signature = \((c, s, R, S, T, W, n)\)
14. return (signature, \( KRD \))

### 3.5.2 ECDAA-Sign Split between Authenticator and ASM

This section is non-normative.

**Algorithm outline**

1. The ASM randomizes the credential
   1. \( l = \text{RAND}(p) \)

   **NOTE**
   
   All values \( l \) must be unguessable and unique, e.g. compute \( H(\text{RAND}(p), \text{AppID}, ++\text{seqCntr}) \) if in doubt about RAND quality, where seqCntr counts the ECDAA-Sign operations performed by this ASM.

2. ECPoint \( R = A^l \);
3. ECPoint \( S = B^l \);
4. ECPoint \( T = C^l \);
5. ECPoint \( W = D^l \);

2. The ASM sends \( l, \text{AppID} \) to the authenticator

3. The authenticator performs the following tasks
   1. \( KRD = \text{BuildAndEncodeKRD}() \); // all traditional Registration tasks are here (e.g. key generation)
   2. ECPoint \( S' = B^l \)
   3. ECPoint \( W' = D^l \)
   4. BigInteger \( r = \text{RAND}(p) \); // use same random number algorithm as for key generation in step 3.1
   5. ECPoint \( U' = S'^r \)
   6. BigInteger \( c^2 = H(U'||S'||W'||\text{AppID}||H(KRD)) \)
   7. BigInteger \( n = \text{RAND}(p) \); // use same random number algorithm as for key generation in step 3.1
   8. \( c = H(n \ | \ c^2) \)
   9. BigInteger \( s = r + c \cdot sk \mod p \)
   10. Send \( c, s, KRD, n \) to the ASM
4. The ASM sets signature = \((c, s, R, S, T, W, n)\) and outputs (signature, \( KRD \))

### 3.5.3 ECDAA-Sign Split between TPM and ASM

This section is non-normative.

**NOTE**

This split requires both the authenticator and ASM to be honest to achieve anonymity. Only the authenticator must be trusted for unforgeability. The communication between ASM and authenticator must be secure.
Algorithm outline

1. The ASM randomizes the credential
   1. BigNumber \( l = \text{RAND}(p) \)
   2. ECPoint \( R = A^l \)
   3. ECPoint \( S = B^l \)
   4. ECPoint \( T = C^l \)
   5. ECPoint \( W = D^l \)

2. The ASM calls TPM2_Commit() with \( P1 \) set to \( S \) and \( s2, y2 \) empty buffers. The ASM receives the result values \( K, L, E = S^r = U \) and ctr. \( K \) and \( L \) are empty since \( s2, y2 \) are empty buffers.

3. The ASM calls TPM2_Create to generate the new authentication key pair. The related private key might need to be protected with appropriate access control mechanisms, e.g. see section 8 of [UAFAuthnrCommands].

4. The ASM calls TPM2_Certify() on the newly created key with ctr from the TPM2_Commit and \( E = U, S, W, \text{AppID} \) as qualifying data. The ASM receives signature value \( s \) and related nonce \( n \) and attestation block \( \text{KRD} \) (i.e. TPMS_ATTEST structure in this case).

5. BigInteger \( c2 = H(E | S | W | \text{AppID} | H(\text{KRD})) \), using KRD as returned by the previous step.

6. The ASM computes: \( c = H(n | c2) \)

7. The ASM sets signature = \( (c, s, R, S, T, W, n) \) and outputs (signature, KRD)

3.6 ECDAA-Verify Operation

This section is normative.

NOTE

One ECDAA-Verify operation is required for the FIDO Server as part of each FIDO Registration.

boolean EcdaaVerify(signature, AppID, KRD, ModelName)

Parameters

- \( p \): System parameter prime order of group \( G_1 \) (global constant)
- \( P_2 \): System parameter generator of group \( G_2 \) (global constant)
- signature: \( (c, s, R, S, T, W, n) \)
- AppID: FIDO AppID
- KRD: Attestation Data object as defined in other specifications.
- ModelName: the claimed FIDO authenticator model (i.e. either AAID or AAGUID)

Algorithm outline

1. Based on the claimed ModelName, look up \( X, Y \) from trusted source
2. Check that \( R, S, T, W \in G_1, R \neq 1_{G_1}, \text{and } S \neq 1_{G_1} \).
3. \( H(nH(S^r \cdot W^{-c} | S | W | \text{AppID} | H(\text{KRD}))) \overset{?}{=} c \); fail if not equal

   \[
   \begin{align*}
   B &= A^y = P_1^y \\
   D &= Q = B^k \\
   S &= B^l \; \text{and} \; W = D^l \\
   U &= S^r \\
   S^s \cdot W^{-c} &= S^{s+ck} \cdot W^{-c} = U \cdot S^{ck} \cdot W^{-c} \\
   &= U \cdot B^{ck} \cdot D^{ck} = U \cdot B^{ck} \cdot B^{-ck} = U
   \end{align*}
   \]
4. \( e(R, Y) = e(S, P_2); \) fail if not equal

\[
e(R, Y) = e(A^l, P_2^x); e(S, P_2) = e(B^l, P_2) = e(A^{l_y}, P_2)
\]

5. \( e(T, P_2) = e(R \cdot W, X); \) fail if not equal

\[
e(T, P_2) = e(C^l, P_2) = e(A^{l \cdot Q^{l_y}}, P_2); e(A^l \cdot D^l, X) = e(A^l \cdot Q^{l_y}, P_2^x)
\]

6. for (all sk’ on RogueList) do if \( W \neq S^k \) fail;

7. // perform all other processing steps for new credential registration

8. return true;

4. **FIDO ECDAA Object Formats and Algorithm Details**

   *This section is normative.*

4.1 **Supported Curves for ECDAA**

**Definition of G1**

G1 is an elliptic curve group \( E : y^2 = x^3 + ax + b \) over \( F(q) \) with \( a = 0 \).

**Definition of G2**

G2 is the p-torsion subgroup of \( E'(F_{q^2}) \) where \( E' \) is a sextic twist of \( E \). With \( E' : y'^2 = x^3 + b' \).

An element of \( F(q^2) \) is represented by a pair \((a, b)\) where \( a + bX \) is an element of \( F(q)[X]/<X^2 + 1> \). We use angle brackets \(<Y>\) to signify the ideal generated by the enclosed value.

**Definition of GT**

GT is an order-p subgroup of \( F_{q^2} \).

**Pairs**

We propose the use of Ate pairings as they are efficient (more efficient than Tate pairings) on Barreto-Naehrig curves [DevScoDah2007].

**Supported BN curves**

We use pairing-friendly Barreto-Naehrig [BarNae-2006] [ISO15946-5] elliptic curves. The curves TPM_ECC_BN_P256 and TPM_ECC_BN_P638 curves are defined in [TPMv2-Part4].

BN curves have a Modulus \( q = 36 \cdot u^4 + 36 \cdot u^3 + 24 \cdot u^2 + 6 \cdot u + 1 \) [ISO15946-5] and a related order of the group \( p = 36 \cdot u^4 + 36 \cdot u^3 + 18 \cdot u^2 + 6 \cdot u + 1 \) [ISO15946-5].

- **TPM_ECC_BN_P256** is a curve of form \( E(F(q)) \), where \( q \) is the field modulus [TPMv2-Part4] [BarNae-2006]. This curve is identical to the P256 curve defined in [ISO15946-5] section C.3.5.

**NOTE**

According to cryptographic research, this curve provides approx. 96 bits of security (see Crypto and CHES 2016_) and hence should NOT be used any longer.
- The values have been generated using \( u = -753085173716300289 \).
- Modulus \( q = 11579208923731493687268865612444717420583578757556761201951981049002892769644518163 \)
- Group order \( p = 11579208923731493687268865612444717420583578757556761201951981049002892769644518163 \)
- \( p \) and \( q \) have length of 256 bit each.
- \( b = 3 \)
- \( P_{1,256} = (x=1, y=2) \)
- \( b' = (a=3, b=3) \)
- \( P_{2,256} = (x, y) \), with
  - \( P_{2,256}.x = (a=114909019869825495805094438766505779201460871441403458685386522624680861435, b=35574367275806345419306346468619132090758060623913174762536247107606148811) \)
  - \( P_{2,256}.y = (a=650760217911503023887857970107222586124471742058357897372641249576517861439865105660388351777247 \)

- **TPM_ECC_BN_P638 [TPMv2-Part4]** uses
  - The values have been generated using \( u = -3657354809924433626299827442042423208620483 \)
  - Modulus \( q = 641593209463000232827928286881680117116729879043238547681370616895915585449723794945051781991794253 \)
  - The related order of the group is \( p = 641593209463000232827928286881680117116729879043238547681370616895915585449723794945051781991794253 \)
  - \( p \) and \( q \) have length of 638 bit each.
- \( b = 257 \)
- \( P_{1,638} = (x=64159320946300023282849222586168801116729879043238547681370616895915585449723794945051781991794253 \)
  - \( P_{1,638}.x = (a=641981315470262367403199689624663165015260219273187383871010005014237978377771652517297172225 \)
  - \( P_{1,638}.y = (a=62269649573552082775130678147180522602607282568626687887202660204709926200680026261220052024314419522215791182512425301878002011 \)

- **ECC_BN_DSD_P256 [DevScuDah2007]** section 3 uses
  - The values have been generated using \( u = 691752902764108938 \)
  - Modulus \( q = 82434016654036077912173535319003883657178181138622892211673224128190294893183 \)
  - The related order of the group is \( p = 82434016654036077912173535319003883657178181138622892211673224128190294893183 \)
  - \( p \) and \( q \) have length of 256 bit each.
- \( b = 3 \)
- \( P_{1,DSD_P256} = (1, 2) \)
- \( b' = (a=3, b=3) \)
- \( P_{2,DSD_P256} = (x, y) \), with
  - \( P_{2,DSD_P256}.x = (a=7348134655530501180719409052734799052621421628200018757361137491036750387705920446973214 \)
  - \( P_{2,DSD_P256}.y = (a=632491054685712356185595904840355591759258295778771983534530246540633843286379521908061170557257501883 \)

- **ECC_BN_130P512 [ISO15946-5]** section C.3.7 uses
  - The values have been generated using \( u = 1389196945704700980403314812820401523727 \)
  - Modulus \( q = 134078097929942597099574024998025805437245134385751115804945274271459609988107555044539653245714590501512644436683325 \)
  - The related order of the group is \( p = 134078097929942597099574024998025805437245134385751115804945274271459609988107555044539653245714590501512644436683325 \)
  - \( p \) and \( q \) have length of 512 bit each.
- \( b = 3 \)
- \( P_{1,ISO_P512} = (x=1, y=2) \)
- \( b' = (a=3, b=3) \)
- \( P_{2,ISO_P512} = (x, y) \), with
\( P_{2.\text{ISO}_P512.x} = (a=3 094 648 157 539 090 131 026 477 120 117 259 896 222 920 557 994 037 039 545 437 079 729 804 516 315 481 514 566 156 984 454 73 190 248 967 907 724 153 072 490 467 902 779 495 072 074 560 452 474 412 673 836 012 873 126 926 524 076 966 265 127 900 471 529) \)


**NOTE**
Spaces are used inside numbers to improve readability.

### Hash Algorithm \( H \)

Depending on the curve, we use \( H(x) = \text{SHA256}(x) \mod p \) or \( H(x) = \text{SHA512}(x) \mod p \) as hash algorithm \( H: \{0, 1\}^* \rightarrow \mathbb{Z}_p \).

The argument of the hash function must always be converted to a byte string using the appropriate encoding function specific in section 3.1 Object Encodings, e.g. according to section 3.1.3 Encoding ECPoint2 values as byte strings (ECPoint2ToB) in the case of ECPoint2 points.

**NOTE**
We don't use IEEE P1363.3, section 6.1.1 IHF1-SHA with security parameter \( t \) (e.g. \( t=128 \) or \( 256 \)) as it is more complex and not supported by TPMv2.

### 4.2 ECDAA Algorithm Names

We define the following JWS-style algorithm names (see [RFC7515]):

- **ED256**
  - TPM_ECC_BN_P256 curve, using SHA256 as hash algorithm \( H \).

- **ED256-2**
  - ECC_BN_DSD_P256 curve, using SHA256 as hash algorithm \( H \).

- **ED512**
  - ECC_BN_ISO512 curve, using SHA512 as hash algorithm \( H \).

- **ED638**
  - TPM_ECC_BN_P638 curve, using SHA512 as hash algorithm \( H \).

### 4.3 ecdaaSignature object

The fields \( c \) and \( s \) both have length \( N \). The fields \( R, S, T, W \) have equal length (\( 2\times N+1 \) each).

In the case of BN_P256 curve (with key length \( N=32 \) bytes), the fields \( R, S, T, W \) have length \( 2\times 32+1=65 \) bytes. The fields \( c \) and \( s \) have length \( N=32 \) each.

The ecdaaSignature object is a binary object generated as the concatenation of the binary fields in the order described below (total length of 356 bytes for 256bit curves):

<table>
<thead>
<tr>
<th>Value</th>
<th>Length (in Bytes)</th>
<th>Description</th>
</tr>
</thead>
</table>
| UINT8[] ECDAA_Signature_c | N | The c value, \( c = H(n | c2) \) as returned by EcdaaSign encoded as byte string according to BigNumberToB. Where  
- \( c2 = H(U | S | W | KRD | AppID) \)  
- \( U = S' \), with \( r = \text{RAND}(p) \) computed by the signer.  
- \( KRD \) is the the entire to-be-signed object (e.g. TAG_UAFV1_KRD in the case of FIDO UAF).  
- \( S = B', \) with \( l = \text{RAND}(p) \) computed by the signer and \( B = A^l \) computed in the ECDAA-Join |
| UINT8[] ECDAA_Signature_s | N | The s value, \( s = r + c \times sk \mod p \), as returned by EcdaaSign encoded as byte string according to BigNumberToB. Where  
- \( r = \text{RAND}(p) \), computed by the signer at FIDO registration (see Authenticator and ASM)  
- \( p \) is the group order of \( G1 \)  
- \( sk \): is the authenticator’s attestation secret key, see above |
<table>
<thead>
<tr>
<th>ECDAA_Signature_n</th>
<th>N</th>
<th>The Nonce value n, as returned by EcdaaSign encoded as byte string according to BigNumberToB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UINT8[] ECDAA_Signature_R</td>
<td>2*N+1</td>
<td>$R = A^l$; computed by the ASM or the authenticator at FIDO registration; encoded as byte string according to ECPointToB. Where</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- $l = \text{RAND}(p)$, i.e. random number $0 \leq l \leq p$. Computed by the ASM or the authenticator at FIDO registration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- And where $R = A^l$ denotes the scalar multiplication (of scalar l) of a curve point A.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Where A has been provided by the ECDAA Issuer as part of ECDAA-Join: $A = B^{1/y}$, see 3.4.1 ECDAA-Join Algorithm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Where p is a system value, injected into the authenticator and $y$ is part of the ECDAA Issuer private key $\text{isk}=(x,y)$.</td>
</tr>
<tr>
<td>UINT8[] ECDAA_Signature_S</td>
<td>2*N+1</td>
<td>$S = B^l$; computed by the ASM or the authenticator at FIDO registration encoded as byte string according to ECPointToB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Where B has been provided by the ECDAA Issuer on Join: $B = (H(m), yc)$, see 3.4.1 ECDAA-Join Algorithm.</td>
</tr>
<tr>
<td>UINT8[] ECDAA_Signature_T</td>
<td>2*N+1</td>
<td>$T = C^l$; computed by the ASM or the authenticator at FIDO registration encoded as byte string according to ECPointToB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- $C = (A \cdot Q)^x$, provided by the ECDAA Issuer on Join</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- $x$ is a components of the ECDAA Issuer private key, $\text{isk}=(x,y)$.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- $Q$ is the authenticator public key.</td>
</tr>
<tr>
<td>UINT8[] ECDAA_Signature_W</td>
<td>2*N+1</td>
<td>$W = D^l$; computed by the ASM or the authenticator at FIDO registration encoded as byte string according to ECPointToB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Where $D = Q$ is computed by the ECDAA Issuer at Join (see 3.4.1 ECDAA-Join Algorithm).</td>
</tr>
</tbody>
</table>

5. Considerations

This section is non-normative.

A detailed security analysis of this algorithm can be found in [CamDriLeh16-DAA].

5.1 Algorithms and Key Sizes

The proposed algorithms and key sizes are chosen such that compatibility to TPMv2 is possible.

5.2 Indicating the Authenticator Model

Some authenticator_s (e.g. TPMv2) do not have the ability to include their model (i.e. vendor ID and model name) in attested messages (i.e. the to-be-signed part of the registration assertion). The TPM's endorsement key certificate typically contains that information directly or at least it allows the model to be derived from the endorsement key certificate.

In FIDO, the relying party expects the ability to cryptographically verify the authenticator model.

We require the ECDAA Issuer_s public key ($\text{ipk}=(X,Y,c, sx,sy)$) to be dedicated to one single authenticator model (e.g. as identified by AAID or AAGUID).

5.3 Revocation

If the private ECDAA attestation key $\text{sk}$ of an authenticator has been leaked, it can be revoked by adding its value to a RogueList.

The ECDAA-Verifier (i.e. FIDO Server) check for such revocations. See section 3.6 ECDAA-Verify Operation.

The ECDAA Issuer is expected to check revocation by other means:

1. if ECDAA-Join is done in-factory, it is assumed that produced devices are known to be uncompromised (at time of production).
2. if a remote ECDAA-Join is performed, the (remote) ECDAA Issuer already must use a different method to remotely authenticate the authenticator (e.g. using some endorsement key). We expect the ECDAA Issuer to perform a revocation check based on that information. This is even more flexible as it does not require access to the authenticator ECDAA private key $\text{sk}$.

5.4 Pairing Algorithm

The pairing algorithm $e$ needs to be used by the ASM as part of the Join process and by the verifier (i.e. FIDO relying party) as part of the verification (i.e. FIDO registration) process.
The result of such a pairing operation is only compared to the result of another pairing operation computed by the same entity. As a consequence, it doesn't matter whether the ASM and the verifier use the exact same pairings or not (as long as they both use valid pairings).

5.5 Performance

For performance reasons the calculation of \( \text{Sig2} = (R, S, T, W) \) may be performed by the ASM running on the FIDO user device (as opposed to inside the authenticator). See section 3.5.2 ECDAA-Sign Split between Authenticator and ASM.

The cryptographic computations to be performed inside the authenticator are limited to G1. The ECDAA Issuer has to perform two G2 point multiplications for computing the public key. The Verifier (i.e. FIDO relying party) has to perform G1 operations and two pairing operations.

5.6 Binary Concatentation

We use a simple byte-wise concatenation function for the different parameters, i.e. \( H(a,b) = H(a|b) \).

This approach is as secure as the underlying hash algorithm since the authenticator controls the length of the (fixed-length) values (e.g. U, S, W). The AppID is provided externally and has unverified structure and length. However, it is only followed by a fixed length entry - the (system defined) hash of KRD. As a consequence, no parts of the AppID would ever be confused with the fixed length value.

5.7 IANA Considerations

This specification registers the algorithm names "ED256", "ED512", and "ED638" defined in section 4. FIDO ECDAA Object Formats and Algorithm Details with the IANA JSON Web Algorithms registry as defined in section "Cryptographic Algorithms for Digital Signatures and MACs" in [RFC7518].

<table>
<thead>
<tr>
<th>Algorithm Name</th>
<th>&quot;ED256&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm Description</td>
<td>FIDO ECDAA algorithm based on TPM_ECC_BN_P256 [TPMv2-Part4] curve using SHA256 hash algorithm.</td>
</tr>
<tr>
<td>Algorithm Usage Location(s)</td>
<td>&quot;alg&quot;, i.e. used with JWS.</td>
</tr>
<tr>
<td>JOSE Implementation Requirements</td>
<td>Optional</td>
</tr>
<tr>
<td>Change Controller</td>
<td>FIDO Alliance, Contact Us</td>
</tr>
<tr>
<td>Specification Documents</td>
<td>Sections 3. FIDO ECDAA Attestation and 4. FIDO ECDAA Object Formats and Algorithm Details of [FIDOEcdaaAlgorithm].</td>
</tr>
<tr>
<td>Algorithm Analysis Document(s)</td>
<td>[CamDriLeh16-DAA]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algorithm Name</th>
<th>&quot;ED512&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm Usage Location(s)</td>
<td>&quot;alg&quot;, i.e. used with JWS.</td>
</tr>
<tr>
<td>JOSE Implementation Requirements</td>
<td>Optional</td>
</tr>
<tr>
<td>Change Controller</td>
<td>FIDO Alliance, Contact Us</td>
</tr>
<tr>
<td>Specification Documents</td>
<td>Sections 3. FIDO ECDAA Attestation and 4. FIDO ECDAA Object Formats and Algorithm Details of [FIDOEcdaaAlgorithm].</td>
</tr>
<tr>
<td>Algorithm Analysis Document(s)</td>
<td>[CamDriLeh16-DAA]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algorithm Name</th>
<th>&quot;ED638&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm Usage Location(s)</td>
<td>&quot;alg&quot;, i.e. used with JWS.</td>
</tr>
<tr>
<td>JOSE Implementation Requirements</td>
<td>Optional</td>
</tr>
<tr>
<td>Change Controller</td>
<td>FIDO Alliance, Contact Us</td>
</tr>
<tr>
<td>Specification Documents</td>
<td>Sections 3. FIDO ECDAA Attestation and 4. FIDO ECDAA Object Formats and Algorithm Details of [FIDOEcdaaAlgorithm].</td>
</tr>
<tr>
<td>Algorithm Analysis Document(s)</td>
<td>[CamDriLeh16-DAA]</td>
</tr>
</tbody>
</table>

A. References

A.1 Normative references