FIDO ECDAA Algorithm

FIDO Alliance Implementation Draft 20 February 2018

This version: https://fidoalliance.org/specs/fido-uaf-v1.2-id-20180220/fido-ecdaa-algorithm-v1.2-id-20180220.html
Editor: Rolf Lindemann, Nok Nok Labs, Inc.
Contributors:
  Jan Camenisch, IBM
  Manu Drvers, IBM
  Alec Edgington, Trustonic
  Ana Leonardino, IBM
  Rainer Urban, Infineon
Copyright © 2013-2018 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 [FIDO-DAA-Security-Proof] based on elliptic curves and bilinear pairings largely compatible with [CheLi2013-ECDAA] called ECDAA. This scheme provides significantly improved performance compared with the original DAA and basic building blocks for its implementation are part of the TPMv2 specification [TPMv2-Part1].

The improvements over [CheLi2013-ECDAA] mainly consist of security fixes (see [ANZ-2013] and [XYZF-2014]) when splitting the sign operation into two parts.

This specification includes the fixes of the issue regarding (1) the Diffie-Hellman oracle w.r.t. the secret key of the TPM and (2) regarding the potential privacy violations by fraudulent TPMs as proposed in [CCOLNU2017-DAA].

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 byFIDO 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, 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 Conformance
2. Overview
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 [FIDOglossary].

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 registration 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. [SrCamChe2004-DAA] or [BFGSW2011].

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.
  - \((n, B, sc, yc) = \text{GetNonceFromECDAAIssuer()}\)
  - \((D=Q, c1, s1) = \text{EcdaaJoin}(X, Y, B, sc, yc, n)\)
  - \((A, B, C, D) = \text{EcdaaIssuerJoin}(Q, c1, s1)\)
  - \(\text{EcdaaJoin}(A, C) // store c1=(A, B, C, D)\)

- 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 \(b\)

```
b0 b1 b2 b3 b4 b5 b6 b7 0 0 n0 n1 n2 n3 n4 n5
```

The algorithm implemented in Java looks like this:

**EXAMPLE 2:** Algorithm for converting BigNumber to byte strings

```
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.

**EXAMPLE 3:** Converting ECPoint \(P\) to byte string

```
(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 \(\mathbb{F}(t^2)\), see section 4.1 Supported Curves for ECDAA. Each **ECPoint2** is represented by a pair \((a, b)\) of elements of \(\mathbb{F}(t)\).

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).

**EXAMPLE 4:** Converting ECPoint2 \(P\) to byte string

```
(cx, cy) = ECPointGetAffineCoordinates(P)
len = G2.byteLength
byte string = 0x04 | BigIntegerToB(cx.a,len) | BigIntegerToB(cx.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 [BNPairs].
4. Hash function $H$ with $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$.
5. Hash function $H^G_1$ with $H : \{0, 1\}^* \rightarrow G_1$.
6. $(G^1, P, p, H, H^G_1)$ are installed in all authenticators implementing FIDO ECDAA attestation.

Definition of $G^1$, $G^2$, $G_T$, Pairings, hash function $H$ and $H^G_1$

See section 4.1 Supported Curves for ECDAA.

3.3 Issuer Specific ECDAA Parameters

ECDAA Issuer Parameters pari

1. Randomly generated ECDAA Issuer private key $i sk = (x, y)$ with $[x, y] = RAND(p)$.
2. ECDAA Issuer public key $(X, Y)$, with $X = P_2^x$ and $Y = P_2^y$.
3. A proof that the ECDAA Issuer key was correctly computed
   1. $\text{BigInteger} r_x = RAND(p)$
   2. $\text{BigInteger} r_y = RAND(p)$
   3. $\text{ECPoint2} U_x = P_{2^x}$
   4. $\text{ECPoint2} U_y = P_{2^y}$
   5. $\text{BigInteger} c = H(U_x|U_y|P_2^x|X|Y)$
   6. $\text{BigInteger} s^x = r_x + c \cdot x \pmod{p}$
   7. $\text{BigInteger} s_y = r_y + c \cdot y \pmod{p}$
4. $\text{ipk} = X, Y, c, s^x, s_y$

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

$$H(P_{2^x} \cdot X^{-c}|P_{2^y} \cdot Y^{-c}|P_2^x|X|Y) = c$$

NOTE

\[
\begin{align*}
P_{2^x} \cdot X^{-c} &= P_2^{x+cz} \cdot P_2^{-cz} = P_2^{x} = U_x \\
\frac{1}{P_{2^y}} \cdot Y^{-c} &= P_2^{y+cz} \cdot P_2^{-cy} = P_2^{y} = U_y
\end{align*}
\]

The ECDAA Issuer public key ipk must be dedicated to a single authenticator model.

We use the element $c$ of ipk as an identifier for theECDAA 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 Issuers, 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 authenticators) 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 and

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
This section is normative.

3.4.1 ECDAA Issuer

Not all ECDAA 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 authenticators 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 the 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

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 \( m = R A N D(p) \).
3. The ECDAA Issuer computes the B value of the credential as \( B = H^G(m) \) and sends \((s c, yc) = H G 1\_p r e(m)\) to the authenticator.
4. The authenticator chooses and stores the ECDAA private key BigInteger \( s k = R A N D(p) \)
5. The authenticator re-computes \( B = (h(s c), y c) \)
6. The authenticator computes its ECDAA public key ECP\( Q = B^{s k} \)
7. The authenticator proves knowledge of \( s k \) as follows
   1. BigInteger \( r^1 = R A N D(p) \)
   2. ECP\( U^1 = B^{r^1} \)
   3. BigInteger \( c^2 = H((U^1| P| Q|m) \)
   4. BigInteger \( n = R A N D(p) \)
   5. BigInteger \( c^1 = H(n|c^2) \)
   6. BigInteger \( s^1 = r^1 + c^1 \cdot s k \)
8. The authenticator sends \( Q, c^1, s^1, n \) via the ASM to the ECDAA Issuer
9. 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.
10. The ECDAA Issuer verifies that \( Q \in \mathbb{G}^1 \) and verifies \( H(n|H(B^{s^1} \cdot Q^{-c^1}| P| Q|m)) \equiv c^1 \) (check proof-of-possession of private key).

11. The ECDAA Issuer creates credential \((A, B, C, D)\) as follows
    1. ECP\( A = B^{1/y} \)
    2. ECP\( B \) as computed in the beginning.
    3. ECP\( C = (A \cdot Q)^y \)
    4. ECP\( D = Q \)
12. The ECDAA Issuer sends \( A, C \) to the authenticator. The authenticator still knows \( B \) and \( D \)
13. The authenticator checks that \( A, C \in \mathbb{G}^1 \) and \( A \neq 1^{\mathbb{G}^1} \)
14. The authenticator checks \( e(A, Y) \equiv e(B, P^y) \)

\[
\text{NOTE} \quad e(A, Y) = e(B^{1/y}, P^y) = e(B, P^y) = e(B, P^y); \]

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

\[
\text{NOTE} \quad e(C, P_2) = e((A \cdot Q)^y, P_2); e(A \cdot D, X) = e(A \cdot Q, P_2^y) = e((A \cdot Q)^y, P_2) \]

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

3.4.2 ECDAA-Join Split between Authenticator and ASM
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 ASM asks the ECDAA Issuer for the B value of the credential.
2. The ECDAA Issuer chooses a nonce BigInteger \( m = RAN D(p) \)
3. The ECDAA Issuer computes the B value of the credential as \( B = H^{G_1}(m) \)
4. The ECDAA Issuer sends \((sc, yc) = HG_1.pre(m)\) to the ASM.
5. The ASM forwards \((sc, yc)\) to the authenticator
6. The authenticator chooses and stores the private key BigInteger \( sk = RAN D(p) \)
7. The authenticator re-computes \( B = (h(sc), yc) \)
8. The authenticator computes its ECDAA public key \( ECPoint \, Q = B^k \)
9. The authenticator proves knowledge of \( sk \) as follows
   1. BigInteger \( r_1 = RAN D(p) \)
   2. ECPoint \( U^1 = B^{r_1} \)
   3. BigInteger \( c^1 = H(U^1P^1|Q|m) \)
   4. BigInteger \( n = RAN D(p) \)
   5. BigInteger \( c^1 = H(n|c^2) \)
   6. BigInteger \( s^1 = r_1 + c^1 \cdot sk \)
10. The authenticator sends \( Q, c^1, s^1, n \) to the ASM, who forwards it 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 \( H(n|H(B^{G_1} \cdot Q^{-c^1}|P_1|Q|m)) \overset{\equiv}{=} c_1 \).
13. The ECDAA Issuer creates credential \( (A, B, C, D) \) as follows
   1. ECPoint \( A = B^{1/s} \)
   2. ECPoint \( B \) as computed in the beginning.
   3. ECPoint \( C = (A \cdot Q)^{c_1} \)
   4. ECPoint \( D = Q \)
14. The ECDAA Issuer sends \( A, C \) to the ASM. The ASM remembered \( B \) and \( D = Q \) from an earlier step.
15. The ASM checks that \( A, B, C, D \in G_1 \) and \( A \neq 1_{G_1} \)
16. The ASM checks \( e(A, Y) \overset{?}{=} e(B, P_3) \)
17. and the ASM checks that \( e(C, P_2) \overset{?}{=} e(A \cdot D, X) \)
18. The ASM stores \( A, B, C, D \) and sends \( A, C \) to the authenticator. The authenticator still knows \( B \) and \( D \).
19. 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 BigInteger \( m = RAN D(p) \).
3. The ECDAA Issuer computes the B value of the credential as \( B = H^{G_1}(m) \)
4. The ECDAA Issuer sends \((sc, yc) = HG_1.pre(m)\) to the ASM.
5. The ASM
   1. 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 \( P_3 \) in field \( unique \)) to the ASM.
   2. re-computes \( B = (h(sc), yc) \)
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 the objectAttributes in TPMv2-Part2 [TPMv2-Part2] matches the following flags: fixedTPM = 1; fixedParent = 1; sensitiveDataOrigin = 1; encryptedReplication = 0; restricted = 1; decrypt = 0; sign = 1.
3. examines the public key Q, i.e. it verifies that \( Q \in G^1 \).
4. checks \( H(n | H(B^{1/2} \cdot Q^{-1} | P | m)) \equiv c1 \).
5. generates the ECDAA credential \((A, B, C, D)\) as follows
   1. \( \text{ECPoint} \ A = B^{1/2} \)
   2. \( \text{ECPoint} \ B \) as computed in the beginning.
   3. \( \text{ECPoint} \ C = (A \cdot Q)^{2} \)
   4. \( \text{ECPoint} \ D = Q \)
6. generates a secret (derived from a seed) and wraps the credential \( A, B, C, D \) using that secret.
7. encrypts the seed using the public key included in EK-C.
8. 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 TPMv2_PUBLIC, see [TPMv2-Part1], section 16.

9. sends the wrapped object including the credential from previous step to the ASM.
10. The ASM instructs the TPM (by calling TPM2_ActivateCredential) to decrypt the seed using the TPM Endorsement key.
11. compute the name (for the ECDAA attestation key)
12. use the seed in KDFa (with name) to derive the HMAC key and the symmetric encryption key.
13. use the symmetric encryption key to unwrap the secret.

   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 ECDAA-Sign

3.5.1 ECDAA-Sign Algorithm

This section is normative.

\[ \text{signature, KRD} = \text{EcdaaSsign} \text{(String AppID)} \]

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. \( \text{KRD} = \text{BuildAndEncodeKRD}() \); // all traditional Registration tasks are here
2. \( \text{BigInteger} \ l = RAN \ D(p) \)
3. \( \text{ECPoint} \ R = A^l \)
4. \( \text{ECPoint} \ S = B^l \)
5. \( \text{ECPoint} \ T = C^l \)
6. \( \text{ECPoint} \ W = D^l \)
7. BigInteger $r = RAND(p)$
8. ECPoint $U = S'$
9. BigInteger $c_2 = H(U|S|W|AppID|H(KRD))$
10. BigInteger $n = RAND(p)$
11. $c = H(n | c_2)$
12. BigInteger $s = r + c \cdot sk \pmod{p}$
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.

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 $l = RAND(p)$
   2. ECPoint $R = A^l$
   3. ECPoint $S = B^l$
   4. ECPoint $T = C^l$
   5. ECPoint $W = D^l$
2. The ASM sends $l, AppID$ to the authenticator
3. The authenticator performs the following tasks
   1. $KRD = BuildAndEncodeKRD(l)$; // all traditional Registration tasks are here
   2. ECPoint $S' = B^l$
   3. ECPoint $W' = D^l$
   4. BigInteger $r = RAND(p)$
   5. ECPoint $U = S'$
   6. BigInteger $c_2 = H(U|S'|W'|AppID|H(KRD))$
   7. BigInteger $n = RAND(p)$
   8. $c = H(n | c_2)$
   9. BigInteger $s = r + c \cdot sk \pmod{p}$
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 algorithm is for the special case of a TPMv2 as authenticator. This case requires both the TPM and ASM to be honest for anonymity. Only the TPM must be trusted for unforgeability (see [CCDLNU2017-DAA]).

Algorithm outline
1. The ASM randomizes the credential
   1. BigNumber $l = RAND(p)$
   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 $K, L, E = S' = U$ 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 [UAAuthnCommands].
4. The ASM calls TPM2_Certify() on the newly created key with ctr from the TPM2_Commit and $E = U, S, W, AppID$ as qualifying data. The ASM receives signature value $s$ and related nonce $n$ and attestation block $KRD$ (i.e. TPMS_ATTEST structure in this case).
5. BigInteger $c_2 = H(E|S|W|AppID|H(KRD))$, using $KRD$ as returned by the previous step.
6. The ASM computes: $c = H(n | c_2)$
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)
- \( P \): System parameter generator of group \( G_1 \) (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 \( R, S, T, W \in G_1, R \neq 1^G, \) and \( S \neq 1^G \).
3. \( H(n|H(S^c \cdot W^{-c}|S|W|AppID)|H(KRD))) \cong c; \) fail if not equal

**NOTE**

\[ B = A^y = P^by \]
\[ D = Q^y = P^aksy = B^k \]
\( S = B^j \) and \( W = D^j \)
\( U = S^c \)
\[ S^a \cdot W^{-c} = S^{a+cs_k} \cdot W^{-c} = U \cdot S^{cs_k} \cdot W^{-c} \]
\[ = U \cdot B^{lcs_k} \cdot D^{dc} = U \cdot B^{lcs_k} \cdot B^{lcs_k} = U \]

4. \( e(R, Y) \cong e(S, P^a) \); fail if not equal

**NOTE**

\( e(R, Y) = e(A^1, P^by); e(S, P^a) = e(B^j, P^a) = e(A^by, P^a) \)

5. \( e(T, P^a) \cong e(R \cdot W, X) \); fail if not equal

**NOTE**

\( e(T, P^a) = e(C^1, P^a) = e(A^{sy} \cdot Q^{-y}, P^a); e(A^1 \cdot D^y, X) = e(A^1 \cdot Q^{-sy}, P^a) \)

6. for (all sk’ on RogueList) do if \( W \cong S^{sk'} \) fail;
7. // perform all other processing steps for new credential registration

**NOTE**

In the case of a TPMv2, i.e. KRD is a TPMS_ATTEST object. In this case the verifier must check whether the TPMS_ATTEST object starts with \( TPM_GENERATED \) magic number and whether its field \( objectAttributes \) contains the flag \( fixedTPM = 1 \) (indicating that the key was generated by the TPM).

8. return true;

4. FIDO ECDAA Object Formats and Algorithm Details

This section is normative.

4.1 Supported Curves for ECDAA

**Definition of G1**
BN curves have a Modulus defined in $\mathbb{F}_p$, where $\mathbb{F}_p$ is the finite field with $p$ elements. There is an element $a \in \mathbb{F}_p$ such that the ideal generated by the enclosed value.

**Definition of G2**

G2 is the p-torsion subgroup of $E'(F_p)$ where $E'$ is a sextic twist of $E$. With $E': y'^2 = x'^3 + b'$.

An element of $F'(q)$ 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.

**NOTE**

In the literature the pair $(a, b)$ is sometimes also written as a complex number $a + bi$.

**Definition of GT**

GT is an order-p subgroup of $F_q$.

**Pairings**

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 [BarNaen2006] [ISO15946-5] elliptic curves. The curves $\text{TPM}\_\text{ECC}\_\text{BN}\_\text{P256}$ and $\text{TPM}\_\text{ECC}\_\text{BN}\_\text{P638}$ 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].

- $\text{TPM}\_\text{ECC}\_\text{BN}\_\text{P256}$ is a curve of form $E/F(q)$, where $q$ is the field modulus [TPMv2-Part4] [BarNaen2006]. This curve is identical to the P256 curve defined in [ISO15946-5] section C.3.5.

The values have been generated using $u = -75308517327166300289$.

- Modulus $q = 11579208923731493687268856124477427056878355761205198700495226226966415163$.
- Group order $p = 115792089237314936872688561244774270568783559598884002685844877599942533073617037$.
- $p$ and $q$ have length of 256 bit each.

- $b = 3$.
- $P_{256} = (x=1, y=2)$.

- $b' = (a=3, b=3)$.
- $P_{256} = (x, y)$, with

- $\mathbb{P}_{256} = (x=11490901896250495805094437865057792001460737844034078286685522624680861435, b=3557436372780634193638648681931297075806056239132972167076711648811)$.

- $P_{256} = (x=11579208923731493687268856124477427056878355761205198700495226226966415163, b=113380538078397236146298017450764176886349848360105630536665545426459479368)$.

- $\text{TPM}\_\text{ECC}\_\text{BN}\_\text{P638}$ [TPMv2-Part4] uses

The values have been generated using $u=3653750408992443632629897444204508242302626089433$.

- Modulus $q = 6415939204630002382849232226891688011762978990343356367167988515542974793951749253196909681481516071$.
- Group order $p = 641593920463000238284923222689168801176297899034335636716798851554972394940517819911794525325919690619779570557792001460737844034078286685522624680861435, b=3557436372780634193638648681931297075806056239132972167076711648811$.
- $P_{638} = (x=11490901896250495805094437865057792001460737844034078286685522624680861435, b=113380538078397236146298017450764176886349848360105630536665545426459479368)$.
- \( P_{DSD\_P256} = (1, 2) \)
- \( b' = (a=3, b=8) \)
- \( P_{DSD\_P256} = (x, y) \), with
  - \( P_{DSD\_P256}.x = (a=73\, 481\, 346\, 555\, 305\, 118\, 071\, 940\, 904\, 527\, 347\, 990\, 526\, 214\, 212\, 698\, 180\, 576\, 973\, 201\, 374\, 397\, 013\, 567\, 073\, 039\), \( b = 28\, 955\, 468\, 426\, 222\, 256\, 383\, 171\, 634\, 927\, 293\, 329\, 392\, 145\, 263\, 879\, 318\, 611\, 908\, 127\, 165\, 887\, 947\, 997\, 417\, 463 \)
  - \( P_{DSD\_P256}.y = (a=3\, 632\, 491\, 054\, 685\, 712\, 358\, 616\, 318\, 558\, 909\, 408\, 435\, 559\, 591\, 759\, 282\, 597\, 787\, 781\, 393\, 534\, 962\, 445\, 630\, 353\), \( b = 60\, 960\, 585\, 579\, 607\, 838\, 639\, 544\, 584\, 959\, 654\, 864\, 947\, 372\, 740\, 800\, 177\, 666\, 763 \)

**ECC\_BN\_ISO\_P512**

[ISO15946-5] section C.3.7 uses

The values have been generated using \( u = 138\, 919\, 694\, 570\, 470\, 098\, 040\, 331\, 481\, 282\, 401\, 523\, 727 \)

Modulus \( q = 13\, 407\, 807\, 929\, 942\, 597\, 099\, 574\, 024\, 998\, 205\, 830\, 437\, 246\, 153\, 344\, 875\, 111\, 580\, 494\, 527 \)

The related order of the group is \( p = 13\, 407\, 807\, 929\, 942\, 597\, 099\, 574\, 024\, 998\, 205\, 830\, 437\, 246\, 153\, 344\, 875\, 111\, 580\, 494\, 527 \)

\( p \) and \( q \) have length of 512 bit each.

- \( b = 3 \)

- \( P_{ISO\_P512} = (x=1, y=2) \)
- \( b' = (a=3, b=3) \)
- \( P_{ISO\_P512} = (x, y) \), with
  - \( P_{ISO\_P512}.x = (a=3\, 094\, 648\, 157\, 539\, 090\, 131\, 026\, 477\, 120\, 117\, 259\, 896\, 222\, 920\, 557\, 994\, 037\, 039\, 545\, 437\, 079\, 729\, 804\, 516\, 315\, 481\, 514\, 666\, 156\, 984\, 245\, 473\, 190\, 248\, 967\, 907\, 724\, 152\, 072\, 490\, 467\, 902\, 779\, 495\, 072\, 074\, 156\, 718\, 085\, 785\, 269\)
  - \( b = 3\, 776\, 690\, 234\, 788\, 102\, 103\, 015\, 760\, 376\, 468\, 067\, 863\, 580\, 475\, 949\, 014\, 286\, 075\, 850\, 384\, 033\, 870\, 546\, 339\, 773\, 119\, 295\, 555\, 161\, 718\, 985\, 244\, 561\, 452\, 474\, 412\, 673\, 836\, 012\, 873\, 126\, 926\, 524\, 076\, 966\, 265\, 127\, 900\, 471\, 529 \)
  - \( P_{ISO\_P512}.y = (a=7\, 593\, 872\, 605\, 334\, 070\, 150\, 001\, 723\, 245\, 210\, 278\, 735\, 800\, 573\, 263\, 881\, 411\, 015\, 285\, 406\, 372\, 548\, 542\, 328\, 752\, 430\, 917\, 597\, 485\, 450\, 360\, 707\, 892\, 769\, 159\, 214\, 115\, 916\, 255\, 816\, 324\, 924\, 295\, 339\, 525\, 688\, 777\, 569\, 132\, 644\, 242\, b=9\, 131\, 995\, 053\, 349\, 122\, 285\, 871\, 305\, 684\, 665\, 648\, 028\, 094\, 505\, 015\, 281\, 268\, 488\, 257\, 987\, 110\, 193\, 875\, 868\, 586\, 868\, 792\, 041\, 571\, 666\, 587\, 093\, 146\, 239\, 570\, 057\, 834\, 816\, 183\, 220\, 952\, 460\, 187\, 617\, 700\, 670\, 514\, 736\, 173\, 834\, 408\)
yc to the authenticator. The authenticator computes HG1(m) = (H(sc), yc).

Given the value sc, the original message m can be recomputed by skipping the first 4 bytes.

### 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 P256 curve, using SHA256 as hash algorithm H.

**ED512**
ECC BN ISOP512 curve, using SHA512 as hash algorithm H.

**ED638**
TPM ECC BN P638 curve, using SHA512 as hash algorithm H.

### 4.3 edcdaSignature object

The fields c and s both have length N. The fields R, S, T, W have equal length (2*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*32+1=65 bytes. The fields c and s have length N=32 each.

The edcdaSignature 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>
<tbody>
<tr>
<td>UINT8[]</td>
<td>ECDAA Signature_c</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UINT8[]</td>
<td>ECDAA Signature_s</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UINT8[]</td>
<td>ECDAA Signature_n</td>
<td>N</td>
</tr>
<tr>
<td>UINT8[]</td>
<td>ECDAA Signature_R</td>
<td>2*N+1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UINT8[]</td>
<td>ECDAA Signature_S</td>
<td>2*N+1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UINT8[]</td>
<td>ECDAA Signature_T</td>
<td>2*N+1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UINT8[]</td>
<td>ECDAA Signature_W</td>
<td>2*N+1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 5. Considerations

This section is non-normative.

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

### 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 authenticators (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 Issuers public key \((ipk=(X,Y,c,sx, sy))\) 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 \(sk\) 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 \(sk\).

### 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 \(\text{Sig}2=(R,S,T,W)\) 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 Concatenation

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>Description</th>
<th>Usage Location(s)</th>
<th>JOSE Implementation Requirements</th>
<th>Change Controller</th>
<th>Specification Documents</th>
<th>Algorithm Analysis Document(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;ED256&quot;</td>
<td>FIDO ECDAA algorithm based on TPM_ECC_BN_P256 [TPMv2-Part4] curve using SHA256 hash algorithm.</td>
<td>&quot;alg&quot;, i.e. used with JWS.</td>
<td>Optional</td>
<td>FIDO Alliance, Contact Us</td>
<td>Sections 3, FIDO ECDAA Attestation and 4, FIDO ECDAA Object Formats and Algorithm Details of [FIDO-EccdaaAlgorithm].</td>
<td>[FIDO-DAA-Security-Proof]</td>
</tr>
<tr>
<td>&quot;ED512&quot;</td>
<td>ECDAA algorithm based on ECC_BN_ISOP512 [ISO15946-5] curve using SHA512 algorithm.</td>
<td>&quot;alg&quot;, i.e. used with JWS.</td>
<td>Optional</td>
<td>FIDO Alliance, Contact Us</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algorithm Name</th>
<th>Description</th>
<th>Usage Location(s)</th>
<th>JOSE Implementation Requirements</th>
<th>Change Controller</th>
<th>Specification Documents</th>
<th>Algorithm Analysis Document(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;ED638&quot;</td>
<td>FIDO ECDAA algorithm based on ECC_BN_ISOP512 [ISO15946-5] curve using SHA512 algorithm.</td>
<td>&quot;alg&quot;, i.e. used with JWS.</td>
<td>Optional</td>
<td>FIDO Alliance, Contact Us</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>