Network Working Group S. Josefsson
Internet-Draft SJD AB
Intended status: Informational June 15, 2015
Expires: December 17, 2015

Using EdDSA in the Internet X.509 Public Key Infrastructure
draft-josefsson-pkix-eddsa-01

Abstract

This document specify algorithm identifiers and ASN.1 encoding formats for EdDSA digital signatures and subject public keys used in the Internet X.509 Public Key Infrastructure (PKIX) for Certificates and CRLs. Parameters for Ed25519 are defined.

Status of This Memo

Copyright Notice

1. Introduction

In [Ed25519], an elliptic curve signature system EdDSA was introduced, and a recommended choice of curve Ed25519 is chosen. EdDSA and Ed25519 was designed with performance and security in mind. Specification, test vectors and a sample implementation is available in [I-D.josefsson-eddsa-ed25519].

This RFC defines ASN.1 object identifiers for EdDSA for use in the Internet X.509 PKI [RFC5280], and parameters for Ed25519. This document serves a similar role as [RFC3279] does for RSA (and more), [RFC4055] for RSA-OAEP/PSS, and [RFC5758] for SHA2-based (EC)DSA.

2. Requirements Terminology

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].

3. EdDSA ASN.1 Object Identifier Tree

The root of the tree for the object identifiers defined in this specification is given by:

```
id-EdDSA OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.11591.4.12 }
```

[[TODO: Find a shorter OID. https://gitlab.com/jas/ietf-pkix-eddsa/issues/4]]

4. Subject Public Key Information Fields

In the X.509 certificate, the subjectPublicKeyInfo field has the SubjectPublicKeyInfo type, which has the following ASN.1 syntax:

```
 SubjectPublicKeyInfo  ::=  SEQUENCE  {
   algorithm         AlgorithmIdentifier,
   subjectPublicKey  BIT STRING
 }
```

The fields in SubjectPublicKeyInfo have the following meanings:

- algorithm is the algorithm identifier and parameters for the public key (see below).

- subjectPublicKey is the EdDSA public key.

The AlgorithmIdentifier type, which is included for convenience, is defined as follows:

```
AlgorithmIdentifier  ::=  SEQUENCE  {
  algorithm   OBJECT IDENTIFIER,
  parameters  ANY DEFINED BY algorithm OPTIONAL
}
```

The fields in AlgorithmIdentifier have the following meanings:

- algorithm identifies the cryptographic algorithm with an object identifier. This is the EdDSA OID defined below.

- parameters, which are optional, are the associated parameters for the algorithm identifier in the algorithm field.

5. EdDSA Public Keys

Certificates conforming to [RFC5280] may convey a public key for any public key algorithm. The certificate indicates the algorithm through an algorithm identifier. This algorithm identifier is an OID and optionally associated parameters.

This section identify the OID and parameters for the EdDSA algorithm. Conforming CAs MUST use the identified OIDs when issuing certificates containing EdDSA public keys. Conforming applications supporting EdDSA MUST, at a minimum, recognize the OID identified in this section.

The id-EdDSAPublicKey OID is used for identifying EdDSA public keys.

```
id-EdDSAPublicKey OBJECT IDENTIFIER ::= { id-EdDSA 1 }
```

The id-EdDSAPublicKey OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier.

EdDSA public keys use the parameter field to specify the particular instantiation of EdDSA parameters. The parameters field have the ASN.1 type EdDSAParameters as follows.

```
EdDSAParameters ::= ENUMERATED { ed25519 (1) }
```

The EdDSAParameters enumeration may be extended in the future.

The raw binary EdDSA public key is encoded directly in the subjectPublicKey BIT STRING object.

6. Key Usage Bits

The intended application for the key MAY be indicated in the keyUsage certificate extension.

If the keyUsage extension is present in an end-entity certificate that conveys an EdDSA public key with the id-EdDSAPublicKey object identifier, then the keyUsage extension MUST contain one or both of the following values:

```
nonRepudiation; and
digitalSignature.
```

If the keyUsage extension is present in a certification authority certificate that conveys an EdDSA public key with the id-EdDSAPublicKey object identifier, then the keyUsage extension MUST contain one or more of the following values:

```
nonRepudiation;
digitalSignature;
keyCertSign; and
cRLSign.
```

7. EdDSA Signatures

Certificates and CRLs conforming to [RFC5280] may be signed with any public key signature algorithm. The certificate or CRL indicates the algorithm through an algorithm identifier which appears in the signatureAlgorithm field within the Certificate or CertificateList. This algorithm identifier is an OID and has optionally associated parameters. For illustration the Certificate structure is reproduced here:

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }
```

Recall the definition of the AlgorithmIdentifier type:

```
AlgorithmIdentifier  ::=  SEQUENCE  {
  algorithm   OBJECT IDENTIFIER,
  parameters  ANY DEFINED BY algorithm OPTIONAL
}
```

This document identify an AlgorithmIdentifier OID for EdDSA signatures. No parameters are defined. The EdDSA parameters follow from the public-key parameters.

The data to be signed is prepared for EdDSA. Then, a private key operation is performed to generate the signature value. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate or CertificateList in the signatureValue field.

The id-EdDSASignature OID is used for identifying EdDSA signatures.

```
       id-EdDSASignature OBJECT IDENTIFIER ::= { id-EdDSA 2 }
```

The id-EdDSASignature OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier. The parameters field MUST be absent. To further clarify how to encode the parameters field, due to historical misunderstandings in this area, it MUST NOT have an ASN.1 type NULL.

8. Examples

An example of a X.509v1 certificate using EdDSA would be:

```
-----BEGIN CERTIFICATE-----
MIHpMIGTAgIAgDAOBgorBgEEAdpHBAwCBQAwEjEQMA4GA1UEAxMHRXhhbXBsZTAeFw0xNTA2MDgx
NDEzMTNaFw0xNTA5MDgxNDEzMTNaMBIxEDAOBgNVBAMTB0V4YW1wbGUwNTAOBgorBgEEAdpHBAwB
BQADIwAEIOWj2mfLDCaC9FMMddwIg9WxktAcusgNUUUSVaa2pNlAMA4GCisGAQQB2kcEDAIFAANB
AAZCIvRcw03Utgmf8Xmgx0lQbp5XBzDG3xNquT2urGD+GMfbJSAGmx/dDoDre1ZctxG2XLZ249ly
fGTaTn5Fiw8=
-----END CERTIFICATE-----
```

An example of a raw Ed25519 public key certificate:

```
MDUwDgYKKwYBBAHaRwQMAQUAAyMABCAu4FI+ME5I7qtL2Kh0nJryEqLjrM0kh4yJwU1QUYEdQg==
```

9. Acknowledgements

Text and/or inspiration were drawn from [RFC5280], [RFC3279], [RFC4055], [RFC5480], and [RFC5639].

Thanks to Klaus Hartke and Ilari Liusvaara for fixes, ideas and discussion.

10. IANA Considerations

None.

11. Security Considerations

The security considerations of [RFC5280] and [I-D.josefsson-eddsa-ed25519] apply accordingly.

12. References

12.1. Normative References

[I-D.josefsson-eddsa-ed25519]
Josefsson, S. and N. Moller, "EdDSA and Ed25519", draft-josefsson-eddsa-ed25519-02 (work in progress), February 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

12.2. Informative References

[RFC3279] Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, April 2002.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, June 2005.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, March 2009.

[RFC5639] Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, March 2010.

[RFC5758] Dang, Q., Santesson, S., Moriarty, K., Brown, D., and T. Polk, "Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA", RFC 5758, January 2010.

[Ed25519] Bernstein, J., Duif, , Lange, , Schwabe, , and Yang, "Ed25519: High-speed high-security signatures", WWW http://ed25519.cr.yp.to/ed25519-20110926.pdf, September 2011.

Author's Address

Simon Josefsson
SJD AB

Email: simon@josefsson.org