S. Blake-Wilson and Y.Wang
INTERNET-DRAFT
Expires: 12 May 2001
Certicom Corp.
13 November 2000

# ECDSA with XML-Signature Syntax
<draft-blake-wilson-xmldsig-ecdsa-00.txt>

## Status of this Memo



## Abstract

This document specifies how to use ECDSA (Elliptic Curve Digital Signature Algorithm) with the XML-digital signature syntax. The mechanism specified provides integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or included by reference.

## Table of Contents

## 1. Introduction

This document specifies how to use ECDSA (Elliptic Curve Digital Signature Algorithm) with the XML signature syntax.
The XML Digital Signature syntax, or XMLDSIG is specified in [RFC2807, XMLDSIG]. Currently there are only two digital signature methods defined for use within XMLDSIG: RSA signatures and DSA (DSS) signatures. This document introduces ECDSA signatures as a third method.

This specification uses both XML Schemas [XML-schema] and DTDs [XML].

## 2. ECDSA

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the DSA (also called DSS) signature method [FIPS186-2]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is defined in the ANSI X9.62 standard [ECDSA]; other compatible specifications include FIPS 186-2 [FIPS186-2], IEEE 1363 [IEEE1363], and SEC1 [SEC1]. [PKIX2] describes the means to carry ECDSA keys in X.509 certificates. Recommended elliptic curve domain parameters for use with ECDSA are given in [SEC2].

Like DSA, ECDSA incorporates the use of a hash function; currently, the only hash function defined for use with ECDSA is the SHA-1 message digest algorithm [FIPS-180-1].

ECDSA signatures are smaller than RSA signatures of similar cryptographic strength. ECDSA public keys (and certificates) are smaller than similar strength DSA keys, resulting in improved communications efficiency. Furthermore, on many platforms ECDSA operations can be computed faster than similar strength RSA or DSA operations (see [KEYS] for a security analysis of key sizes across public key algorithms). These advantages of signature size, bandwidth, and computational efficiency may make ECDSA an attractive choice for XMLDSIG implementations.

## 3. Specifying ECDSA within XMLDSIG

This section specifies the details of how to use ECDSA with the XML-signature syntax. It relies heavily on the syntax and namespace defined in [XMLDSIG].

### 3.1 Identifier

The XML namespace [XML-ns] URI that MUST be used by implementations of this (dated) specification is:

xmlns="http://www.certicom.com/2000/11/xmlecdsig#"

The identifier for the ECDSA signature algorithm is:

http://www.certicom.com/2000/11/xmlecdsig#ecdsa-sha1





### 3.2 Core Syntax

The syntax is defined via DTDs and [XML-Schema] with the following XML preamble, declaration, internal entity, and simpleType:

Schema Definition:

```
<?xml version='1.0'?>
<!DOCTYPE schema
   PUBLIC "-//W3C//DTD XMLSCHEMA 200010//EN" "http://www.w3.org/2000/10/XMLS
chema.dtd"
  [
   <!ATTLIST schema
     xmlns:ds CDATA #FIXED "http://www.w3.org/2000/09/xmldsig#">
   <!ATTLIST schema
     xmlns:ecds CDATA #FIXED "http://www.certicom.com/2000/11/xmlecdsig#">
   <!ENTITY ecdsig 'http://www.certicom.com/2000/11/xmlecdsig#'>
   <!ENTITY dsig 'http://www.w3.org/2000/09/xmldsig#'>
  ]>


<schema xmlns="http://www.w3.org/2000/10/XMLSchema"
      xmlns:ds="&dsig;"
      xmlns:ecds='&ecdsig;'
      targetNamespace="&ecdsig;"
      version="0.1"
      elementFormDefault="qualified">
```

DTD:

```
<!-- In order to include ECDSA in XML-signature syntax, the
```

```
        following definition of the entity Key.ANY SHOULD
        replace the one in [XMLDSIG]-->

   <!ENTITY % Key.ANY '(#PCDATA|KeyName|KeyValue|RetrievalMethod|
              X509Data|PGPData|MgmtData|DSAKeyValue|RSAKeyValue|
              ECDSAKeyValue)*'>
```

## 3.3 ECDSA Signatures

The output of the ECDSA algorithm consists of a pair of integers usually referred by the pair (r, s). The signature value consists of the base64 encoding of the concatenation of two octet-streams that respectively result from the octet-encoding of the values r and s. r and s are converted into octet strings of length [log_2 n/8], where n is the order of the elliptic curve base point, using the conversion routine specified in Section 4.3.1 of ANSI X9.62 [ECDSA].





## 3.4 ECDSA Key Values

The syntax used for ECDSA key values closely follows the ASN.1 syntax defined in ANSI X9.62 [ECDSA].

ECDSA key values consist of two elements: ECDSAPublickey and ECCParameters. ECDSAPublicKey contains the ECDSA public key which is a point on the elliptic curve and is encoded as a base64 value of its octet-stream representation converted as specified in Section 4.3.1 of ANSI X9.62 [ECDSA]. The element ECCParameters specifies the associated elliptic curve domain parameters which are represented by the nicknames given to them in [SEC2].

Schema:

```
<element name='ECDSAKeyValue'>
  <complexType content='elementOnly'>
    <sequence minOccurs='1' maxOccurs='1'>
      <element name='ECDSAPublicKey' type='ecds:CryptoBinary'
             minOccurs='1' maxOccurs='1'/>
      <element name='ECCParameters' type='string'
             minOccurs='1' maxOccurs='1'/>
```

```
      </sequence>
    </complexType>
  </element>
```

DTD:

```
<!ELEMENT ECDSAKeyValue (ECDSAPublicKey, ECCParameters) >
<!ELEMENT ECDSAPublicKey (#PCDATA) >
<!ELEMENT ECCParameters (#PCDATA) >
```

## 4. Security Considerations

Implementers should ensure that appropriate security measures are in place when they deploy ECDSA within XMLDSIG. In particular, the security of ECDSA requires the careful selection of both key sizes and elliptic curve domain parameters. Selection guidelines for these parameters and some specific recommended curves that are considered safe are provided in [X9.62], [NIST-ECC], and [SEC2]. For further security discussion, see [XMLDSIG].

## 5. Intellectual Property Rights

The IETF has been notified of intellectual property rights claimed in regard to the specification contained in this document.
For more information, consult the online list of claimed rights (http://www.ietf.org/ipr.html).





The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

## 6. References

[ECDSA] American National Standards Institute. ANSI X9.62-1998, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm". January, 1999.

[FIPS-180-1] Federal Information Processing Standards Publication (FIPS PUB) 180-1, "Secure Hash Standard", April 17, 1995.

[FIPS-186-2] Federal Information Processing Standards Publication (FIPS PUB) 186-2, "Digital Signature Standard", January, 2000.

[IEEE1363] Institute for Electrical and Electronics Engineers (IEEE) Standard 1363-2000, "Standard Specifications for Public Key Cryptography", 2000.

[KEYS] Lenstra, A.K. and Verheul, E.R., "Selecting Cryptographic Key Sizes", October 1999. Presented at Public Key Cryptography Conference, Melbourne, Australia, January, 2000.
http://www.cryptosavvy.com/

[PKIX2] Bassham, L., Housley, R., and Polk, W., "Internet X.509 Public Key Infrastructure Representation of Public Keys and Digital Signatures in Internet X.509 Public Key Infrastructure Certificates", draft-ietf-pkix-ipki-pkalgs-00.txt. July, 2000.

[RFC2807] RFC 2807. XML Signature Requirements. J. Reagle, April 2000.
http://www.w3.org/TR/xmldsig-requirements





[SEC1] Standards for Efficient Cryptography Group, "SEC 1: Elliptic Curve Cryptography", Version 0.5, September, 1999.
http://www.secg.org

[SEC2] Standards for Efficient Cryptography Group, "SEC 2: Recommended Elliptic Curve Domain Parameters", Version 0.6, October, 1999. <http://www.secg.org>

[XML] Extensible Markup Language (XML) 1.0 Recommendation. T. Bray, J. Paoli, C. M. Sperberg-McQueen. February, 1998. http://www.w3.org/TR/1998/REC-xml-19980210

[XMLDSIG] XML-Signature Syntax and Processing. D. Eastlake, J. Reagle, D. Solo. July, 2000. Work in progess. http://www.w3.org/TR/2000/WD-xmldsig-core-20000711/

[XML-ns] Namespaces in XML Recommendation. T. Bray, D. Hollander, A. Layman. Janaury 1999. http://www.w3.org/TR/1999/REC-xml-names-19990114

[XML-schema] XML Schema Part 1: Structures Working Draft. D. Beech, M. Maloney, N. Mendelshohn. April 2000. http://www.w3.org/TR/2000/WD-xmlschema-1-20000407/ XML Schema Part 2: Datatypes Working Draft. P. Biron, A. Malhotra. April 2000. http://www.w3.org/TR/2000/WD-xmlschema-2-20000407/

## 7. Authors' Address

Simon Blake-Wilson
Yongge Wang
Certicom Corp.
5520 Explorer Dr.
Mississauga, ON, L4W 5L1

e-mail: {sblakewilson, ywang}@certicom.com

## 8. Full Copyright Statement