

# Digital Signing Specification

---

**Product:** EVM-CR  
**Feature:** Digital File Signatures

**Support to:** Defense Cost and Resource Center  
**Contract No:** W91WAW-08-D-0031/0008  
Tecolote Research, Inc.

**Date:** 07/08/2013  
**Document Version:** 1.1

**Prepared by:** John McGahan  
Eric Guerber  
Burt LeClercq  
Will Parke

Software Products/Services Group  
Tecolote Research, Inc.

# 1. Digital Signature of Files

## 1.1 Purpose

This feature shall implement the tools and procedures necessary to apply a digital signature to files intended for upload to the EVM Central Repository (EVM-CR), and the subsequent verification thereof. The system shall ensure that both the person who signs a document, and anyone who subsequently downloads it, can verify that its contents are identical to when it was signed, and that the certification credentials of the signer were valid at the time the file was uploaded to the EVM-CR.

The net effect of this feature provides two desirable outcomes. 1) A signed file cannot be repudiated at a later date by the signing party. 2) The EVM-CR can provide credible assurance that signed files' content has not changed since the time it was signed, and that the encryption certificate used to sign a file was checked for authenticity/validity at the time it was uploaded.

This specification was created with due consideration of current Federal Information Processing Standards and United States Department of Defense External Certification Authority X.509 Certificate Policy. The initial version of the specification requires use of the SHA-1 cryptographic hash algorithm because it is widely supported across existing information technology infrastructure. Support for the SHA-2 algorithms is anticipated in a future version of the specification. In the future, use of SHA-1 may be deprecated and use of SHA-2 may be required.

## 1.2 Business Process

- 1.2.1 The file author will require a digital signature tool to apply the signature to the files. A tool will be provided by the DCARC that meets the attached specifications. Any tool that meets the specifications will be acceptable for the digital signing process. The file author will also require a DoD (Department of Defense) approved ECA (External Certificate Authority) digital certificate with which to sign the files.
- 1.2.2 After acquiring the digital signing tool and certificate the file author will use the tool to sign each file to be submitted individually.
- 1.2.3 Once the files are prepared they will be uploaded and submitted to the EVM-CR in the normal manner.
- 1.2.4 When the EVM-CR receives a signed file the system will extract the file and the signature portions of the package. The EVM-CR will then verify the signature and file content. The system will save the signature information and whether or not the signature and file were valid.
- 1.2.5 The system will then provide a user interface that will allow EVM-CR users to view the signature information and verification messages. The system will allow users to download either the extracted file (without the signature attached) or the signed file package, as desired.

## 2. FIPS-140 Compliance

All tools used in the DCARC file signing process should use cryptographic modules that have been certified as compliant with the Federal Information Processing Standard 140-2. FIPS 140-2: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

## 3. DCARC Signed File Specification (v. 1.0.0.0)

### 3.1 Signed File Format

3.1.1 A DCARC Signed File consists of a single target file and a digital signature created for that file using a DoD approved ECA certificate. The target file and the digital signature are stored as distinct files in an archive file. The digital certificate is included as part of the digital signature.

3.1.2 The creation and representation of the digital signature for a DCARC Signed File conforms to a subset of the procedures and syntax defined by the XML Signature standard. The archive file format used is the ZIP file format. The digital certificate used in the signing process must be a DoD approved ECA X.509 certificate.

### 3.2 Signed File Contents

3.2.1 The signed file will be authenticated only if it meets the syntactic and procedural requirements defined below.

2.2.1.1 The file must be a valid ZIP file containing four file entries. These file entries must have the exact names listed below.

version  
content  
signature  
filename

The file names must not be qualified with directory names. All other file names, with or without qualifying directory names, are reserved for use in future versions of this specification. The file entries may or may not be compressed; if compressed, the file entries must use the Deflate compression method. The file entries must not be encrypted. The extension of the Signed File should be “.dcarcsf”.

2.2.1.2 The ‘version’ file must be a valid text file starting with the following two lines of text in the order given:

type: dcarc\_signed\_file/xml  
version: 1.0.0.0

Any additional text is reserved for use in future versions of this specification. Requirements for the encoding of the text file are specified below.

2.2.1.3 The ‘content’ file must reproduce the exact byte sequence of the target file being signed.

2.2.1.4 The ‘signature’ file must be a valid XML document representing a digital signature as defined in the XML Signature standard. Additional requirements for the purposes of a DCARC Signed File include the following:

The XML document must have the following element hierarchy and sequence:

- Signature
  - SignedInfo
    - CanonicalizationMethod
    - SignatureMethod
    - Reference
      - DigestMethod
      - DigestValue
  - SignatureValue
  - KeyInfo
    - X509Data
      - X509IssuerSerial
        - X509IssuerName
        - X509SerialNumber
      - X509Certificate

Each element must appear exactly once except for X509Certificate which may appear one or more times.

Requirements for the attributes and values of the elements include the following:

- The algorithm for the canonicalization method must be:
  - Canonical XML: <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>
- The algorithm for the signature method must be the following:
  - RSAwithSHA1: <http://www.w3.org/2000/09/xmldsig#rsa-sha1>
- The Reference element must include a URI attribute with the following value:
  - “content” (minus the quotes)
- The algorithm for the digest method must be the following:
  - SHA1: <http://www.w3.org/2000/09/xmldsig#sha1>
- The issuer name and serial number specified must match the signing certificate
- The signing certificate must be included in the list of certificates
- Additional certificates in the chain of trust of the signing certificate may be included in the list of certificates

The Reference element must not include any Transform elements.

Requirements for the encoding of the XML document are specified below.

2.2.1.5 The ‘filename’ file must be a valid text file containing the original file name of the target file. The file name must be valid according the requirements of the NTFS file system. The file name must not be qualified with a directory name. The file name may be followed by a newline delimiter which will not be interpreted as part of the file name. Requirements for the encoding of the text file are specified below.

2.2.1.6 The text files defined above, including the ‘signature’ XML document, must be encoded as UTF-8, with an optional byte-order mark. Lines of text in text files, excluding insignificant whitespace in XML documents, must be delimited by one of the following sequences of characters:

[carriage return][line feed]  
[carriage return]  
[line feed]

These requirements do not apply to the ‘content’ file, in case it is a text file.

#### 2.2.1.7 Requirements for the authentication of a DCARC Signed File, beyond those defined in XML Signature, include the following:

- Only explicitly approved algorithms may be used during the signing process.
- The digital signature must be created using a private key corresponding to a public key that is part of a DoD approved ECA X.509 certificate, and this certificate must be included with the signature data.
- During the signing process, the message digest algorithm must be applied directly to the exact byte sequence of the target file, with no intermediate processing of any kind, including canonicalization or transformation.

#### 2.2.1.8 References:

FIPS 140-2: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

FIPS Publications: <http://csrc.nist.gov/publications/PubsFIPS.html>

XML Signature - XML Signature Syntax and Processing, Second Edition. 2008:  
<http://www.w3.org/TR/xmlsig-core/>

Zip File Format - .ZIP File Format Specification, Version 6.3.2. 2007.

X.509 - ITU-T Recommendation X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. 2008.

NTFS - Inside the Windows NT File System. 1994.

UTF-8 - “UTF-8 encoding scheme,” The Unicode Standard, Version 6.0, §3.9 D92, §3.10 D95. 2011.