Controlled Vocabulary Enumeration Values for BASE-TDF

BASE-TDF-CVEnums

Version 2021-NOV

December 1, 2022

Distribution Notice:
    This document has been approved for Public Release and is available for use without restriction.

Table of Contents

List of Tables

Chapter 1 - CVEnumTDFAppliesToState for BASE-TDF

1.1 - Descriptive information

- Description: All valid data states that effect markings.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:tdf:state
- Created: 2012-06-27T11:19:00-04:00
- Source: IC-CIO
- Point of contact:
    - Office IC CIO
    - E-mail: ic-standards-support@odni.gov

1.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration:
CVEnumTDFAppliesToState.xml

Table 1 - CVEnumTDFAppliesToState Values

CVEnumTDFAppliesToState Values	
Value	**Documentation**
encrypted	Data that has been encrypted.
unencrypted	Data in plain text.

Chapter 2 - CVEnumTDFHashAlgorithm for BASE-TDF

2.1 - Descriptive information

- Description: All valid algorithms and patterns for hash algorithm for use with BindingValueType.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:tdf:hashalgorithm
- Created: 2012-06-27T11:19:00-04:00
- Source: IC-CIO
- Point of contact:
    - Office IC CIO
    - E-mail: ic-standards-support@odni.gov

2.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumTDFHashAlgorithm.xml

Table 2 - CVEnumTDFHashAlgorithm Values

CVEnumTDFHashAlgorithm Values	
Value	Documentation
SHA1	Secure Hash Algorithm (SHA) with a 160 bit message digest. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.
SHA256	Secure Hash Algorithm (SHA) with a 256 bit message digest.
SHA384	Secure Hash Algorithm (SHA) with a 384 bit message digest.
SHA512	Secure Hash Algorithm (SHA) with a 512 bit message digest.

Chapter 3 - CVEnumTDFSignatureAlgorithm for BASE-TDF

3.1 - Descriptive information

- Description: All valid signature algorithms and patterns for use with SignatureValueType.
- Multiplicity: Single-Valued
- URN: urn:us:gov:ic:cvenum:tdf:signaturealgorithm
- Created: 2012-06-27T11:19:00-04:00
- Source: IC-CIO
- Point of contact:
    - Office IC CIO
    - E-mail: ic-standards-support@odni.gov

3.2 - Permissible Values

The permissible values for this simple type are defined in the Controlled Value Enumeration: CVEnumTDFSignatureAlgorithm.xml

Table 3 - CVEnumTDFSignatureAlgorithm Regular Expressions

CVEnumTDFSignatureAlgorithm Values	
Regular Expression	**Documentation**
SHA(1|256|384|512)withRSA	Signature algorithm with a Secure Hash Algorithm (SHA-*) and the RSA encryption algorithm as defined in the OSI Interoperability Workshop, using the padding conventions described in http://www.rsasecurity.com/rsalabs/pkcs. The SHA digest length in bits is indicated by the integer immediately following SHA.
SHA(1|256|384|512)withRSAand[A-Z]+[0-9]*	Use of Secure Hash Algorithms with RSA and Mask Functions. For new signature schemes defined in PKCS1 v 2.0 for which the DigestwithEncryption form is insufficient, DigestwithEncryptionandMaskFunction can be used to form a name. Here, maskFucntion is a mask generation function such as MGF1. Example: SHA1withRSAandMGF1.
SHA(1|256|384|512)withECDSA	Signature algorithm with Secure Hash Algorithm (SHA-*) and ECDSA as defined in ANSI X9.62. Note: SHA1withECDSA is sometimes referred to simply as ECDSA, however this is an ambiguous and should not be used. The formal name SHA1withECDSA should be used.
SHA(1|256|384|512)withECDSAand[A-Z]+[0-9]*	Use of Secure Hash Algorithms with ECDSA and Mask Functions. For new signature schemes defined in PKCS1 v 2.0 for which the DigestwithEncryption form is insufficient, DigestwithEncryptionandMaskFunction can be used to form a name. Here, maskFucntion is a mask generation function such as MGF1. Example: SHA1withECDSAandMGF1.