Transportation Security Administration

NOTE: This Technical Advisory describes a matter which may impact your product.

TWIC Technical Advisory TA-2017-TWIC001-V1.0

New Content Signing Certificate for some TWIC cards

Introduction

This Technical Advisory details the change in the Content Signing Certificate as a result of the physical relocation of the Card Management System (CMS) for TWIC.

Background and Definition

The physical relocation of the TWIC CMS requires the associated Hardware Security Module (HSM) to use a new Content Signing Certificate and private key.

Problem Statement

The TWIC program will relocate in October 2017 the CMS producing TWIC cards. The Hardware Security Module (HSM) attached to this CMS will have new digital signing keys to sign data objects on each TWIC card issued.

Description of New or Unique Process

The process of signature verification on TWIC card data objects used by TWIC readers is not anticipated to be impacted as the new Content Signing Certificate will remain part of the Signed Cardholder Unique Identifier (CHUID). (See Technical Advisory 2014-TWIC001 for details of certificate structure).

Use of New or Unique Process

As stated in 2014, content signing certificates should not be cached as there are several signing certificates in use by TWIC. TWIC readers can obtain the content signing public key by fully reading the signed CHUID (TWIC or PIV).

Design Features of New or Unique Process

The relocation of the CMS and use of a new HSM should have no impact on TWIC readers validating data object signatures.

Comments

Questions on this Technical Advisory should be addressed to the TSA TWIC PMO TWIC Reader Hardware and Card Application Specification Project Editor, Gerald.Smith@associates.dhs.gov

.

Subject References

(Clarified) TWIC Reader Hardware and Card Application Specification, Version 1.1 Amendment 1, May 2012.

Keywords

TWIC
Content Signing Certificate

Standard Details

Refer to Section *A* in the Subject Reference document for using the Content Signing Certificate to validate data objects.

Specifications or Special Provision

- (Clarified) TWIC Reader Hardware and Card Application Specification, Version 1.1 Amendment 1, May 2012.

- Technical Advisory 2014-TWIC001 Change of Certificate Authority Service Provider which the details all the TWIC card certificates used by TWIC.

Supersedes Dates

There is no previous Technical Advisory issued that addresses this change.

This Technical Advisory shall be active until further notice. A revised notice may be sent after the new certificates are in effect.

Obtain more Information

More technical information on TWIC can be obtained by contacting the TWIC Program Office (PMO).

END

The format of the Content Signing Certificate is as follows:

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Signature Hash Algorithm	sha-1
Issuer Distinguished Name	cn=TWIC CA 1, ou= TSA Certification Authorities o = U.S. Government, c= US
Validity Period	Up to 8 years from date of issue in UTCT format
Subject Distinguished Name	cn = TWIC-Content-Signing-YYYY-nnn, ou = TWIC, o = TSA, c = US (where YYYY is a year and nnn is three numeric digits)
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	sha-1WithRSAEncryption
Extensions	
Authority key identifier	critical = no; keyID = Octet String (20 byte SHA-1 hash of the binary DER encoding of the Root CA's public key information)
Subject key identifier	critical = no; Octet String (20 byte SHA-1 hash of the binary DER encoding of the subject's public key information)
Key usage	critical = **yes**; Digital Signature (80)
Enhanced key usage Private key usage period	PIV content signing OID 2.16.840.1.101.3.6.7, TWIC content signing OID 1.3.6.1.4.1.29138.6.7. critical = no; 36 byte value of UTC time (not before / not after) DEPRECATED
Certificate policies	critical =no; Policy Identifier=2.16.840.1.101.3.6.7 (id-PIV-content-signing) , Policy Qualifier Info: [1] Policy Qualifier Id=CPS, Qualifier: 1.2.3.4.5 ; [2] Policy Qualifier Id=User Notice Qualifier: Information Not Available
Policy Mapping	
Subject Alternative Name	
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	
Name Constraints	
Policy Constraints	
Authority Information Access	critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: http://twicaia-twic.tsa.dhs.gov/AIA/CertsIssuedToTWICCA1.p7c critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: ldap://twicaia-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?cACertificate;binary
CRL Distribution Points	critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=http://twiccrl-twic.tsa.dhs.gov/CRLs/TIMCA1.crl critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://twiccrl-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?certificateRevocationList;binary
Properties	
Thumbprint Algorithm	sha-1
Thumbprint	20 byte Value