Transportation
Security
Administration

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

TWIC® Technical Advisory TA-2019-TWIC002-V1.0

USE OF CONTENT SIGNING CERTIFICATE WITH TWIC®

Introduction

This Technical Advisory reaffirms the expected practice with respect to the use of the card resident Content Signing certificate located in the TWIC Signed CHUID data object.

Background and Definition

Since the inception of issuance in October of 2007, the practice for the use of the TWIC card content signing certificate is to only perform checks against the NOT VALID BEFORE date of the Content Signing certificate. In other words, the Content Signing certificate need only be valid at the date / time the objects were signed. This includes the date / time of the Certificate Authority (CA) signing certificate signing the Content Signing certificate (CA 1). The rationale for this is it permits the program to achieve the full life of the Content Signing certificate with respect to signed data. THIS PRACTICE IS LIMITED TO THE CONTENT SIGNING CERTIFICATE.

Problem Statement

The TWIC program will not refresh the Content Signing certificates when the new CA 1 SHA-256 certificate is issued for signing end-entity certificates. All signed data objects will continue to be signed using SHA-1.

Description of New or Unique Process

There will be no change to the Content Signing certificates. They will continue to be signed with the older CA 1 CA signing certificate (SHA-1) and ROOT (SHA-1).

Use of New or Unique Process

TWIC vendors are discouraged from caching the Content Signing certificate as the CA service provider shall populate for each TWIC card one of a limited set of Content Signing certificates.
The TWIC program recognizes that not all implementations will be able to decode the PKCS#7 certificate file to extract the DER binary encoded certificate(s). Therefore, TWIC will make available the DER Binary encoded form of the ROOT and intermediary CA certificates on request to TWIC-Technology@tsa.dhs.gov.

Design Features of New or Unique Process

No changes to the Content Signing certificate are being made at this time.

Comments

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

Subject References

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

Keywords

TWIC
Certificate Authority
Content Signing Certificate

Standard Details

Refer to Section 2 *References* in the Subject Reference document.

Specifications or Special Provision

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

Supersedes Dates

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

This Technical Advisory shall be active until further notice.

Obtain more Information

More technical information on TWIC can be obtained at the email address of:

TWIC-Technology@tsa.dhs.gov.

END