Transportation Security Administration

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

TWIC® Technical Advisory TA-2023-TWIC001-V1.0

UPDATE ON SHA 256 CONTENT SIGNING CERTIFICATE

Introduction

This Technical Advisory informs a change in the configuration of production cards to use a Content Signing certificate and Content Signing digital signatures based on SHA 256.

Background and Definition

In anticipation of the new Credential Management System (CMS) soon to be put into production, the Content Signing certificate and related Content Signing digital signature on many objects will transition from SHA1 to SHA 256.

Problem Statement

Migrating the message digests of each Content Signing digital signature in TWIC cards from Secure Hashing Algorithm One (SHA1) to SHA2 (also known as SHA 256) is to comply with the National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) current specifications (refer to SP 800 -73-4 edition).

Description of New or Unique Process

Where applicable, the SHA1 message digests are now migrated to SHA2 (SHA 256) for TWIC cards. Note that prior issuance of production TWIC cards retain only the SHA1 message digest computation process. Relying parties will need to support both SHA1 and SHA 256 Content Signing digital signatures for up to 5 years after this change takes effect.

Use of New or Unique Process

TWIC reader vendors and other relying parties are now required to support both SHA1 and SHA2 (SHA 256) message digests for the Content Signing digital signature.

Design Features of New or Unique Process

TWIC reader vendors shall ensure the declared message digest algorithm is either SHA1 or SHA2 (SHA 256). Alternatively, one or both Content Signing digital signature operations may be performed.

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

A companion TWIC reader specification, crafted specifically for scQTL TWIC reader evaluations, is now available upon request. This companion document is based on the May 2012 clarified "TWIC Reader Hardware and Card Application" specification which remains in effect. This recently crafted companion document's purpose is focused on what a TWIC reader should do and hence removes most of the language formally defining the broader TWIC card application.

Keywords

Vendor Test Cards
NEXGEN TWIC
scQTL
SHA1
SHA2
SHA 256
Reader Evaluation
Companion Reader Specification

Standard Details

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

Specifications or Special Provision

A TWIC Reader specification (for existing "legacy" card issuance) companion document is available upon request.

Forward looking, a NEXGEN TWIC specification, in four (4) parts, is available upon request to TSA.

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