Transportation
Security
Administration

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

TWIC® Technical Advisory TA-2022-TWIC002-V1.0

INFORMATIVE UPDATE REGARDING scQTL Vendor Test Cards

Introduction

This Technical Advisory informs a change in the configuration of vendor test cards supplied for the self-certification Qualified Technology List (scQTL) evaluation process.

Background and Definition

In anticipation of the soon to be issued Next Generation Transportation Worker Identification Credential (NEXGEN TWIC) card, test cards supplied for the scQTL have been modified to ensure modern day message digests can be processed by TWIC reader vendors.

Problem Statement

Migrating the message digests in scQTL vendor test cards from Secure Hashing Algorithm One (SHA1) to SHA2 (also known as SHA 256) to comply with the National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) current specifications (SP 800 -73 4 edition).

Description of New or Unique Process

Where applicable, the SHA1 message digests are now migrated to SHA2 (SHA256) for the scQTL vendor test cards. Note that existing issuance of production TWIC cards retain only the SHA1 message digest computation process.

Use of New or Unique Process

TWIC reader vendors are now required to support both SHA1 and SHA2 (SHA256) message digests as has been the case for PIV cards for many years.

Design Features of New or Unique Process

TWIC reader vendors shall ensure the declared message digest algorithm is either SHA1 or SHA2 (SHA256). One or both digest operations should be performed before failing a message verification operation based solely on SHA1.

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 available upon request. This companion document is based on the May 2012 clarified "TWIC Reader Hardware and Card Application" specification. 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 TWIC card application.

Keywords

Vendor Test Cards
NEXGEN TWIC
scQTL
SHA2
SHA256
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.

The companion document referred to in the Subject References section is available and is named:
"*TWIC Reader Revised Specification - V2 - 2021-12-09.pdf*" on which is based the test process for scQTL.

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