



Transportation Security Administration

NOTE: This Technical Advisory describes an issue which may impact your product.

TWIC Technical Advisory TA-2008-TWIC001-V1.0

TWIC READER FUNCTIONALITY AUGMENTATION

Introduction

This Technical Advisory details a unique process that is necessary for reader manufacturers to support a specific technical change associated with a small percentage of cards issued under the Transportation Worker Identification Credential (TWIC) program.

Background and Definition

This Technical Advisory was precipitated by the need to have TWIC readers detect and uniquely process TWIC cards that were activated with a prematurely expired Issuer Object Signing certificate. This IOS certificate is located within the signed CHUID data object of both the TWIC and PIV card applications.

Problem Statement

The IOS certificate with serial number **"00 a0 09 c5 2a a9 0d 26 43 2c e8 76 81 73 35 a9 85"** was generated with an expiry "Not Valid After" date of 27 SEP 2007. A small number of TWIC cards were produced in 2008 and populated with this expired IOS certificate.

The audience for this Technical Advisory is TWIC reader manufacturers and other entities that perform IOS certificate validation as part of a data integrity and data security policy.

Description of New or Unique Process

If the IOS certificate is only used to verify signed objects, without further validation of the IOS certificate itself, then this interpretation process is not applicable.

For IOS certificate validation operations, the new process involves the possible interpretation of the NOT VALID AFTER field of the IOS certificate obtained by reading the signed CHUID field of the TWIC Card.

Specifically, if the IOS certificate serial number read from the signed CHUID matches the IOS certificate serial number stated in this Technical Advisory the NOT VALID AFTER date shall be interpreted as 27 SEP 2012 instead of the populated value of 27 SEP 2007 that exists in this field of the IOS certificate.

If there is no match of the IOS certificate serial number to the value stated in this Technical Advisory the NOT VALID AFTER date shall be used as it exists in the read IOS certificate.

Use of New or Unique Process

The unique process described in this Technical Advisory should either be implemented prior to any deployment of TWIC readers to the field OR implemented as a field upgrade to installed TWIC readers.

Design Features of New or Unique Process

What is unique about this process is the interpretation of the IOS certificate number to force a particular NOT VALID AFTER date. The process, as described, attempts to mimic the expected usage of a correctly formed IOS certificate in that the NOT VALID AFTER date of the expired IOS certificate is transformed to the same year as the current correctly formed IOS certificate.

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

TWIC Reader Hardware and Card Application Specification, Version 1.1 Amendment 1, 30 May 2008.

Keywords

TWIC
CHUID
Object Signing Certificate
NOT VALID AFTER DATE

Standard Details

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

Specifications or Special Provision

TWIC Reader Hardware and Card Application Specification, Version 1.1 Amendment 1, 30 May 2008.

Supersedes Dates

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

This Technical Advisory shall be active until October 1, 2012.

Obtain more Information

More technical information on TWIC can be obtained at:

http://www.tsa.gov/what_we_do/layers/twic/pilot_test.shtm

END

