What does OnGuard read from PIV and TWIC cards?

Question

What does OnGuard read from PIV and TWIC cards?

Answer

This question is best answered by first explaining what data (or applications) is on these cards.

The PIV card application includes the following containers (some, as labeled, are optional).
• Card Capabilities Container (CCC) - supports lookup on data model and application info.
• Cardholder Unique Identifier (CHUID) - contains primarily physical access control info:
    o FASCN - Federal Agency Smart Credential Number.
    o GUID - issuer IPv6 address or all zeros; for future migration aware from FASCN (all 0's for us).
    o DUNS - number for non-federal FASCN issuer.
    o Authentication Key Map - optional based on card authentication certificate key.
    o Expiration Date - card expiration date.
• Card Holder Fingerprints - primary and secondary fingerprints.
• Card Holder Facial Image (Optional) - card holder facial image.
• Printed Information (Optional) - contains the information that is required to be printed on PIV cards (this printed information does not have to be encoded on the card, making this optional):
    o Name
    o Employee Affiliation
    o Organizational Affiliation
    o Card Expiration Date
    o Agency Card Serial Number
    o Issuer Identification
• X.509 Certificate for PIV Authentication - certificate used to authenticate the card and cardholder using PIN
• X.509 Certificate for Digital Signature (Optional) - certificate used for signing data.
• X.509 Certificate for Key Management (Optional) - certificate used for encrypting data.
• X.509 Certificate for Card Authentication (Optional) - certificate used for device to device authentication purposes.
• Security Object - for data protection.
A TWIC card has the PIV application listed above, plus a TWIC application containing:
• Unsigned Cardholder Unique Identifier – An unsigned version of the CHUID. Included to allow faster reading speeds than that of the signed CHUID.
• TWIC Privacy Key (TPK) – used to encipher/decipher the reference biometric template stored in the TWIC card application.
• Cardholder Unique Identifier – Signed CHUID.
• Cardholder Fingerprints – The enciphered biometric reference template.

• Security Object – for data protection.

OnGuard imports the following from PIV cards:

• CHUID - only the FASCN, GUID, DUNS, and card expiration date are imported. The DUNS is an optional element for the CHUID and it is used for non-federal issuers. For government issued cards that contain the PIV application, this will not be encoded on the cards, and therefore will not be imported.

• Fingerprints* - two ANSI 378 templates for the primary and secondary template are imported. These templates are stored in one 378 template on the card but are split up when storing them in the OnGuard database.

• Facial image* - the facial image is imported into OnGuard as a JPEG compressed photo. Typically the photo on the card is compressed using JPEG-2000; OnGuard performs this conversion to JPEG automatically.

• Printed Information* - the name (parsed into first name, last name, middle initial, or full name as printed), employee affiliation, organizational affiliation, agency card serial number, and issuer Identification are all imported. The card expiration date, as printed on the card, is NOT imported into OnGuard since this is already imported from the CHUID, which is always encoded on all PIV cards.

*Important: The fingerprints, facial image, and printed information data is ONLY imported if the cardholder enters their PIN during import. If the "forgot PIN" option is being used then only the CHUID will be imported. The reason for this is due to the access rules for the various data containers.

OnGuard imports the following from TWIC cards:

• PIV Application Data - All of the information that is imported for PIV cards (listed above).

• FASCN – The FASCN portion of the CHUID is imported into the BADGE_TWIC_PRIVACY_KEY table. This table references the BADGE table. This field is not accessible from the user interface.

• TWIC Privacy Key (TPK) – This is imported into the BADGE_TWIC_PRIVACY_KEY table. This table references the BADGE table. This field is not accessible from the user interface.

Applies To

OnGuard (All versions)

Additional Information