Transit Fare Token PIV/CAC Application

Prepared by: Tim Baldridge
Date: 10.29.2014

Briefing Goals

- PIV Card Authentication Evolution
- OPACITY and PIV
- Transit Fare Token Requirement
- Transaction Optimization

PIV Card Authentication Evolution

- CAK Introduced in initial SP 800-73, April 2005
- UUID feature for NFI Cards in SP 800-73-3, Feb 2010
- Second Public Draft SP 800-73-4, May 2014
  - Asymmetric Card Authentication Key Mandatory
  - Card UUID Mandatory
  - Introduced Optional Secure Messaging (SM)

The "KEY" Point

- Proof of Possession – The "HAVE" Factor is established through the use of approved cryptographic algorithms and protocols to verify the possession and control of a "KEY" issued to a cardholder
- The association of a "KEY" to a cardholder is established by a trusted Issuer by binding the "KEY" to a cardholder identifier (UUID) in a certificate signed by the issuer
  - For CAK – x.509 Certificate
  - For SM – Card Verifiable Certificate (CVC)

SP 800-73-4 2nd Public Draft
B.1.3 Authentication Using Card Authentication Key

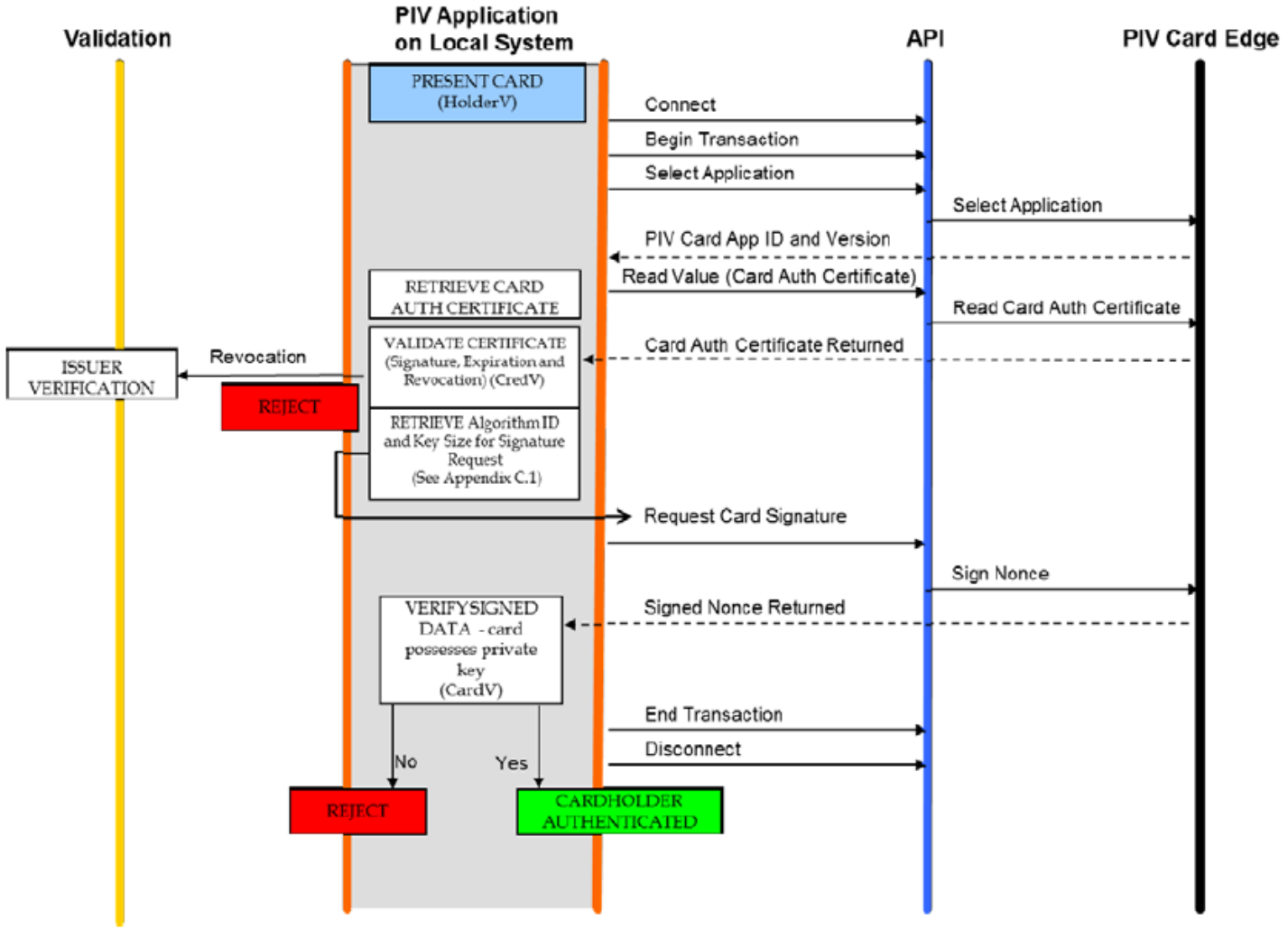
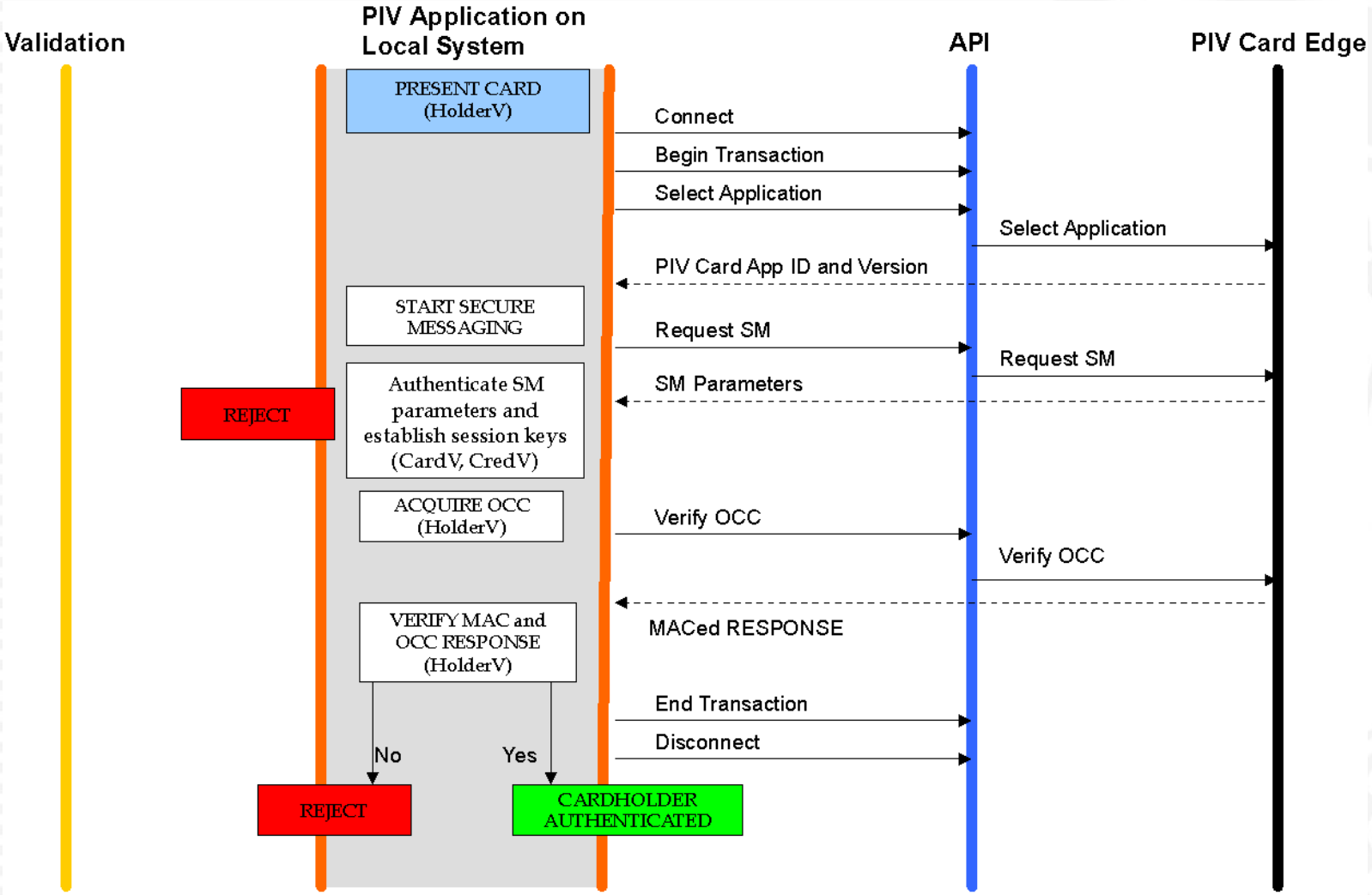


Figure B-4. Authentication using an asymmetric Card Authentication Key

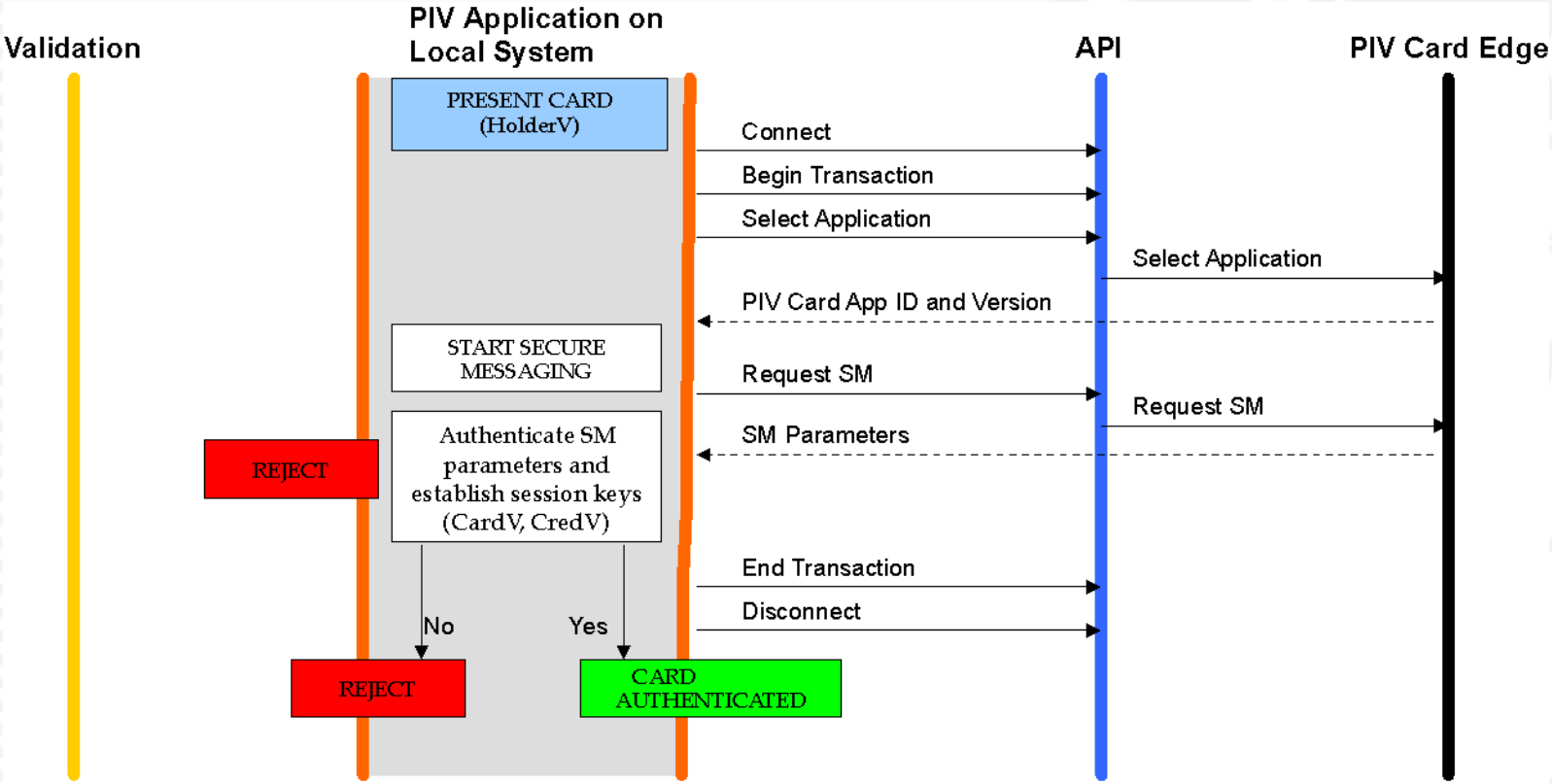
OPACITY and PIV

- For PIV, Secure Messaging (SM) a simplified profile of OPACITY with Zero Key Management - ZKM (ANSI 504-1) is described in SP 800-73-4 2nd Public Draft, Part 2, Section 4.1 Key Establishment Protocol
- SM is included for PIV for the purpose of protecting eavesdropping attacks on contactless PIV operations
- As a collateral benefit SM may be also be used for Card validation, like the Card Authentication Key (CAK)
- OPACITY is designed as an efficient and secure protocol based on Elliptic Curve Cryptography (ECC)

SP 800-73-4 2nd Public Draft
B.1.4 Authentication Using OCC (OCC-AUTH)



Authentication using SM (SM-Auth)



- Similar to OCC-Auth without Card Holder Validation
- One less transaction card-edge transaction than authentication with CAK

Transit Fare Token Requirement

- *Strongly resistant to tampering and counterfeiting*
- *Can be rapidly authenticated electronically*
  - *Fast Transaction time ~ 300mS (0.3 Seconds)*
- *Issued by providers whose reliability has been established*

- Fare collection system moves from stored value cards to a rider based back end account that is associated to a token presented at the fare gate

SM Transaction Basics

1. Host Resets Card and waits for Card to complete Power-On Self-Test and send Answer to Reset (ATR)
2. Host Selects PIV Application and Card Replies
3. Host generates an ephemeral key pair and initiates OPACITY ZKM protocol exchange with Card.
4. Card replies with AuthCryptogram and CVC.
5. Host validates both the AuthCryptogram and CVC, if valid then extracts the UUID from the CVC for access

Mandatory Security Checks

- Within the 300ms transaction, two critical cryptographic validations must always be performed
  - The “Host -> Card -> Host” crypto must validate
  - The signature on the CVC provided by the Card must validate before the host accepts the UUID for access

- Definition: Endorsement Key
  - The public key used by the host to validate the digital signature of a certificate.
  - For SM see 3.3.7 Secure Messaging Certificate Signer
  - For CAK it is the PK of the superior X.509 Certificate

Transaction Optimization

- The fundamental basis of a solution architecture for sub-second performance is a closed validation strategy at the access transaction.
  - All information to complete the cryptographic validations is available at the edge within allocated time
  - Credential revocation checks are not synchronous with access transaction - they may be performed periodically
  - The “Endorsement Key” is local to the access point and is retrieved by direct or indirect indexing based on the UUID

Transaction Optimization (cont)

- These optimizations infer a registration process that occurs before the access transaction which must include appropriate periodic revalidation
- Requirements for initial and periodic validation of an issuer asymmetric public Endorsement Key are based on the distribution method and Issuer practice, a single Endorsement key may be valid for millions of cards
- Requirements for initial and periodic validation individual cardholders are referenced to the UUID and based on associated information obtained at time of registration.

Additional Considerations

- There are two card performance metrics which are critical, 1) time for the FIPS 140 Power-Up Self-Test (POST), and 2) computational time for the AuthCryptogram OPACITY response ADPU
- ADPU transmission time and Host processing time must be efficient and complete within the remaining time. If Host processing is sufficiently long obtain the UUID before beginning SM for concurrent host processing
- ECC allows for smaller key objects with a marginal improvement in transmission times, and more importantly shorter computational times. SM requires ECC and for CAK ECC use is optional, however when used achieves a majority of the SM performance gain.

Questions?