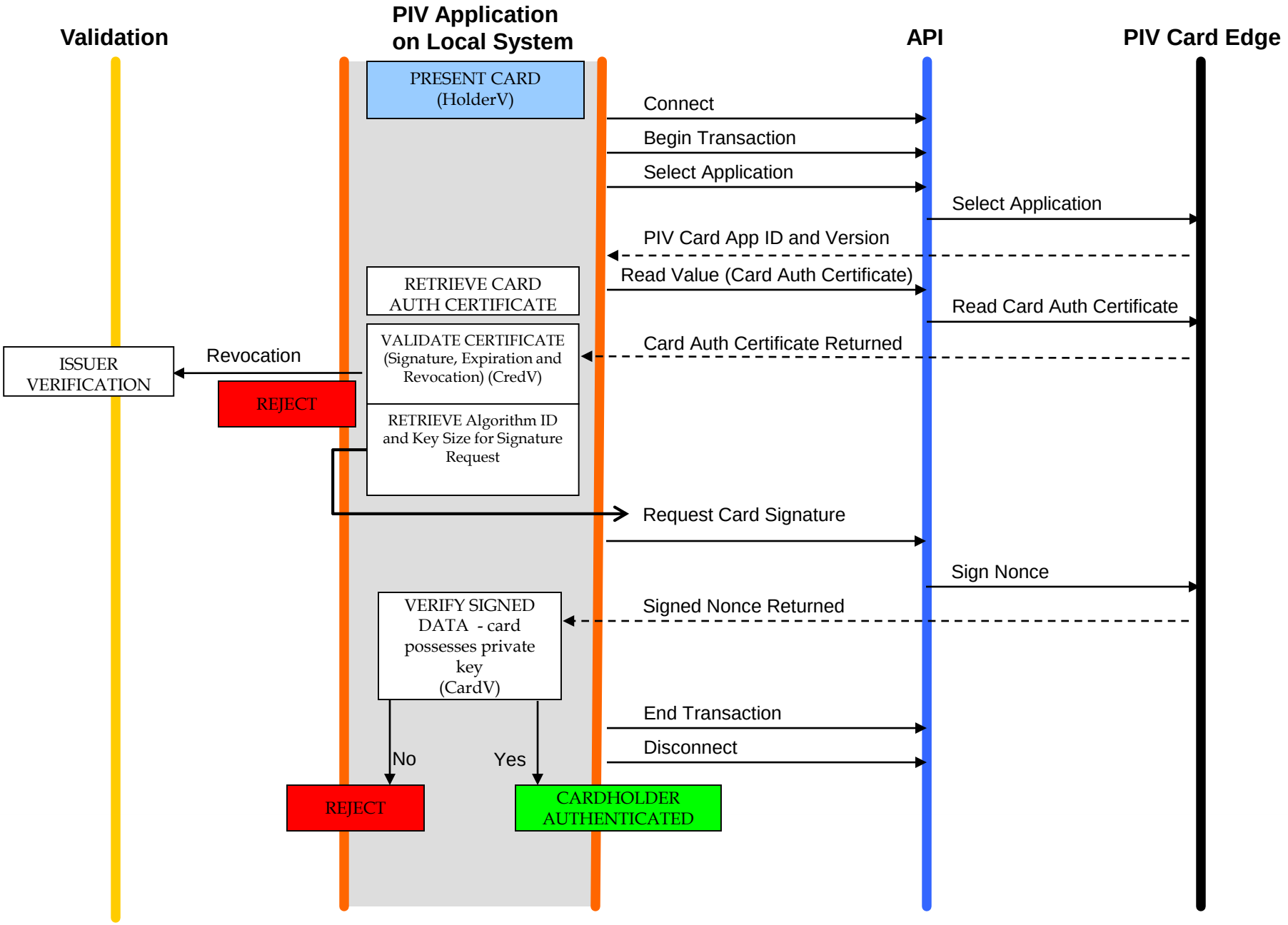
Overview on PKI-Enabled PACS Authentication (CAK AuthN)

Hildegard Ferraiolo

March 3, 2015

Authentication using Card Authentication Key



Caching Status Proxy

- PKI-CAK requires certificate validation
- Validation does not have to be performed at time card presented at door
  - Register certificate in a caching status proxy
  - Proxy validates certificate and periodically re-checks certificate status
  - Relying party simply queries proxy to determine whether certificate is valid

Power-up Self-tests

- PKI-CAK only involves a single cryptographic operation
- CAK is either 2048-bit RSA or ECC P-256
  - Card knows at time of power-up what type of cryptographic key is used for CAK

Thank you!

Questions?

Hildegard Ferraiolo
PIV Project Lead
NIST ITL Computer Security Division
hildegard.ferraiolo@nist.gov