PIV Performance @ Door

Bob Dulude

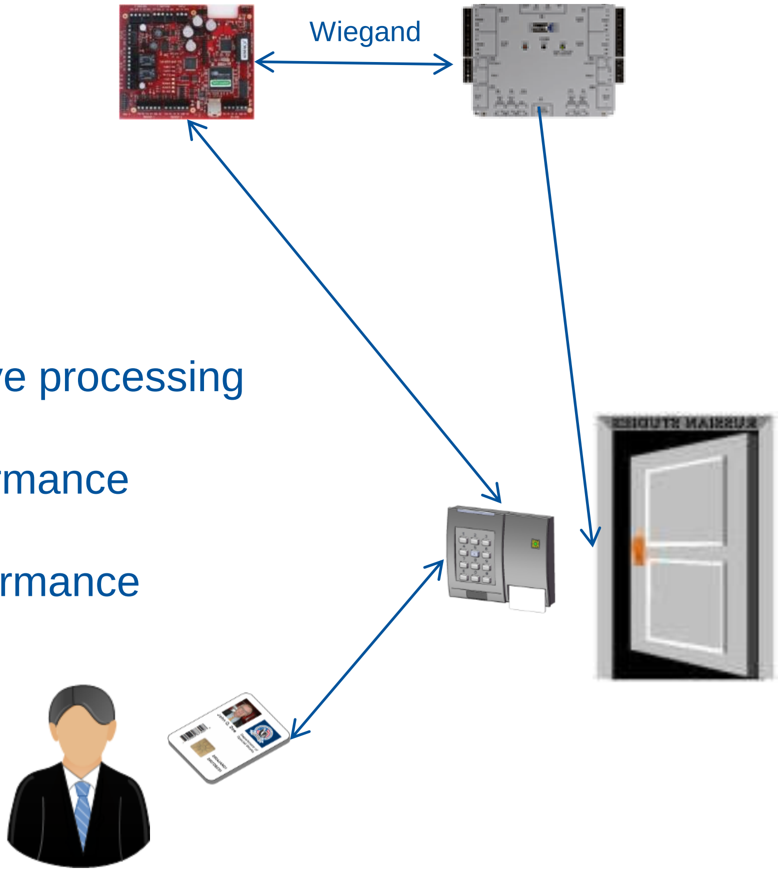
Director Federal Identity Initiatives

PROPRIETARY INFORMATION.
© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.

PKI Authentication Takes Time ~ 4 sec

Why does it take so long?

Multi-component System



1. Functionality spread over multiple devices
2. Data is transferred between devices
3. PIV authentication involves computer intensive processing
4. Not all PIV cards provide same level of performance
5. Not all controllers provide same level of performance
6. User impatience

PROPRIETARY INFORMATION.
© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.

Key Factors Affecting Performance

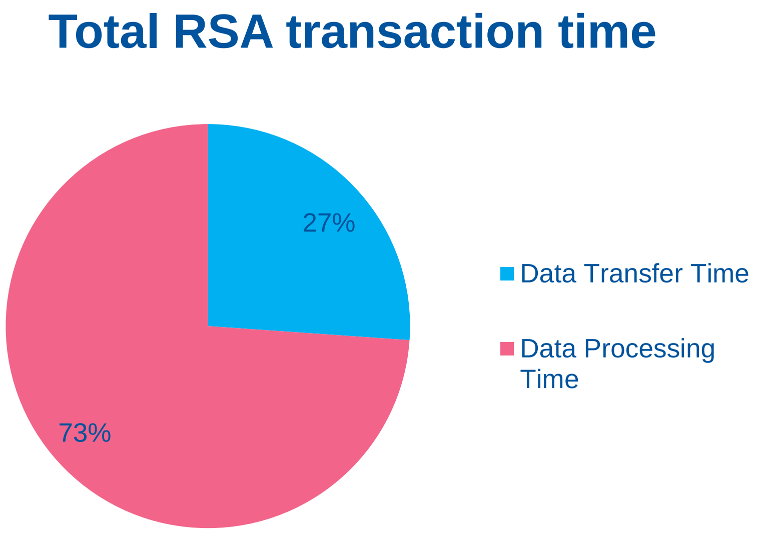
- Crypto processing times dependent upon
  - Key length
  - Cryptographic algorithm
  - Processor
- Data transfer times proportional to size of data elements & transfer speed
  - RSA Certificate ~ 2000 bytes (from 800-73-4)
  - Identifier length = 128, 200 bits
    - Wiegand transfer speed set by standard
- Card related factors
  - Crypto self-check ~ 400 ms
  - Age of card – older cards can be significantly slower
  - PIV Card performance varies significantly by manufacturer
- Hardware component performance
  - Controllers – performance varies by manufacturer
  - Readers – performance varies by manufacturer
- User impatience
  - Process restarts if cardholder removes card prior to completion

PROPRIETARY INFORMATION.
© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.

Some Performance Metrics

Derived from Task Time Measurements

RSA 2048	
Data Transfer Times	***ms***
Card - Reader	200
Reader - PAM	397
PAM - Controller	414
Controller - Door	0
Sub Total	**1011**
Data Processing Times	***ms***
Processing on Card	1367
Processing on PAM	1200
Processing on Controller	100
Sub Total	**2667**
Total RSA transaction time	**3678**


Total RSA transaction time

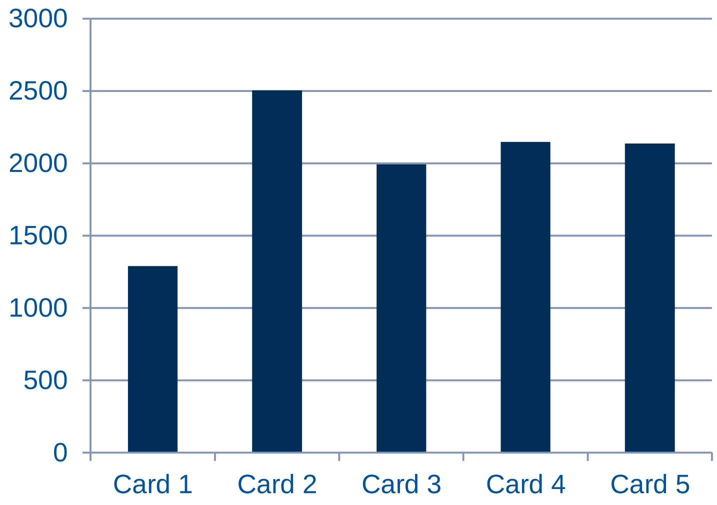
Plus crypto self check =~ 4 sec

ASSA ABLOY
An ASSA ABLOY Group brand
PROPRIETARY INFORMATION.
© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.

Measured Card Performance Variance

- Sum of measured RSA times over contact interface of following ***operations:***
  - Connection to reader
  - Selection of PIV applet
  - Read CHUID (2339 bytes)
  - Verify PIN
  - Signing process (2048 bits)

Card Contact Interface Processing Times (milliseconds)			Variance	
Card 1	1291			
Card 2	2504		1213	94%
Card 3	1993		702	54%
Card 4	2148		857	66%
Card 5	2137		846	66%



CAK Processing Times
Card Contact Interface (milliseconds)

ASSA ABLOY
An ASSA ABLOY Group brand
PROPRIETARY INFORMATION.
© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.

Options for Improved Performance

1. Algorithm, shorter key size
   - Replace RSA with ECC algorithms and keys
     - Key size decreases from 2048 to 256 bits
     - Signature smaller, processing faster
   - Focus on CAK certificate for ECC;
     - Minimizes infrastructure impact as primary use is PACS
2. Policy changes
   - Optimize card’s crypto self-check, or
   - Develop crypto module that doesn’t require self-check
3. Card performance
   - Newer cards are in general faster
   - Test/publish card performance to drive processing optimization
4. Move the authentication functionality into the controller
   - Save 400 ms by eliminating the Wiegand transfer process

PROPRIETARY INFORMATION.
© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.

Measured CAK Transaction Using ECDSA

- Test setup and process
  - Used PAM logging functionality to record times
  - Test Card 1: NIST RSA 2048 CAK
  - Test Card 2: NIST ECC P-256 CAK
  - Series of 10 measurements per card
  - *Start time* = ‘card detected’ msg received from reader
    - Card power-up not included; crypto check ?
  - *Stop time* = ‘Wiegand transfer complete’; PAM to controller
    - Controller processing not included
  - Timing limited to 100 ms granularity
- Measured RSA 2048 bit processing time = 3.25 +/- .05
- Measured ECC P-256 bit processing time = 2.17 +/- .07
- Processing time saved moving to ECDSA ~ 1.1 seconds
  - Assumes unmeasured times (e.g., card power up) same for both cases
- Expected ECDSA total transaction time ~ 2.9 seconds
  - Need additional savings to meet proposed target

© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.

Potential Performance Improvements

- Current observed transaction times =~ 4 sec
- Transaction time target <= 1.5 sec
- Required improvement to meet target >= ~ 2.5 sec
- Measured performance improvements
  - ECDSA transaction time savings = ~ 1.1 sec
  - Move authentication functionality to controller† = ~ .4 sec
- Required additional time savings = ~ 1 sec
- Potential areas for additional performance improvements
  - Optimized card self-crypto check
  - Improved card processing performance over NIST Test Cards
  - Improved reader processing performance
  - Improved authentication processing (controller) performance

† Requires hardware change for existing systems

PROPRIETARY INFORMATION.
© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.

Bob Dulude Ph.D.
Director HID Federal Identity Initiative

Mobile: +1 781 710-0436
Office: +1 781 591-0913
Email: bdulude@hidglobal.com

PROPRIETARY INFORMATION.
© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Contents are confidential and proprietary and not intended for external distribution.