GSA PACS Analysis & Potential for Faster PACS Using Authenticating Readers

What We Found

- At GSA, the communications between the card and reader take approximately:
  - **4.0 to 4.8 seconds** for a card that it has not recently seen (where the Card Auth Cert must be read before doing the CAK challenge/response)
  - **3.5 to 4.4 seconds** for a card it has recently seen and has cached the Card Auth Cert (only read CHUID before doing the CAK challenge/response)

- Thoughts for improvement
  - Short term: eliminate wasted steps, optimize necessary steps
  - Medium term: faster crypto (ECC) and eliminate unneeded crypto self checks

What Happens at GSA Building

- Three basic steps:
  - Look for non-PIV applications (a waste of time, ~0.6 to 1.0 second)
  - Perform PIV Card Validation (~2.0 to 2.6 seconds, depending on if card data is cached)
  - Wait for PACS to issue an access decision (~0.9 seconds)

Overview of CAK Mode at GSA

Total Time: ~3.47 s

Non-PIV Related File Requests: **~611 ms**

Wait: ~47ms

PIV-Related Communication

Don't Read Card Authorization Certificate (Just CHUID)
~2.00 s

Wait: ~863ms

Deselect: ~4ms

Total Time: ~4.09 s

Non-PIV Related File Requests : **~615 ms**

Wait: ~48ms

PIV-Related Communication
+
Read Card Authorization Certificate (and CHUID)
~2.60 s

Wait: ~871ms

Deselect: ~4ms

What Happens - Takeaways

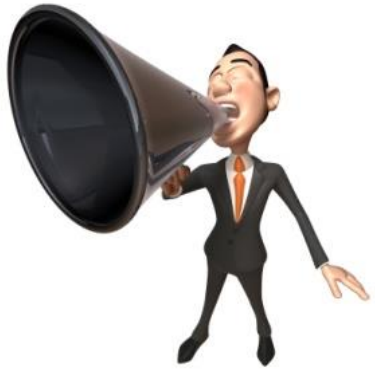
- Some communications at the beginning that take ~ 0.6 to 1.0 seconds are completely unnecessary
  - Asking for non-PIV Apps
  - Perform card crypto pre-checks
  - Deselecting card, then asking for PIV App and doing crypto pre-checks again
  - Could solve this by either not asking for non-PIV apps or not deselecting the card prior to asking for the PIV App
- Caching the Card Auth Cert may save ~0.6 sec
- Long poles in the tent are:
  - Performing the challenge/response (~1.2 sec)
  - Reading the Card Auth Cert (~0.6 sec)
  - Crypto Pre-checks (~0.6 to 1.0 sec)
  - PACS access decision (~0.9 sec)

Lessons Learned Background

- Lessons were indentified during interviews several federal agencies
- The interviews focused on their experience implementing and deploying PACS, as well as end user experience
- Findings were then consolidated into several overarching categories
- Recommendations are included to facilitate brainstorming

Communication

- Findings:
  - Communication and Expectations are important



- Recommendations:
  - Provide user training/education
  - Recommend users insert cards
  - Conduct outreach to senior management
  - Better communicate why it is important

Throughput

- Findings:
  - Throughput analysis is important

- Recommendations:
  - Perform a comprehensive throughput analysis including:
  - More turn styles may be needed
  - Lobbies may need to be rearranged

Develop, Install, and Deploy

- Findings:
  - A well executed PACS requires detailed planning

- Recommendations:
  - Develop Site Plan Analysis / Checklist
  - Use certified integrators
  - Provision users into PACS in advance of arrival/use
  - Ensure electricity quality