Interagency Advisory Board

Meeting Agenda, Wednesday, August 22, 2012

1. **Opening Remarks**

2. **Use of PIV-I in Medical Disaster Response Demonstration** *(Dr. James, AMA and Craig Wilson, FEMA Contractor)*

3. **Considerations for the User Experience when PIV-Enabling Applications** *(Bill Erwin, DoD)*

4. **Update of the FICAM Trust Framework Provider Adoption Process** *(Anil John, GSA)*

5. **Initiatives and Products from Oracle Meeting FICAM Initiatives** *(Derrick Harcey, Oracle)*

6. **Closing Remarks**

Considerations for the User Experience when PIV-Enabling Applications
– OR –
How I Got Really Good At Selecting My PIV Auth Cert

Bill Erwin, DOD

PIV-Enablement Options

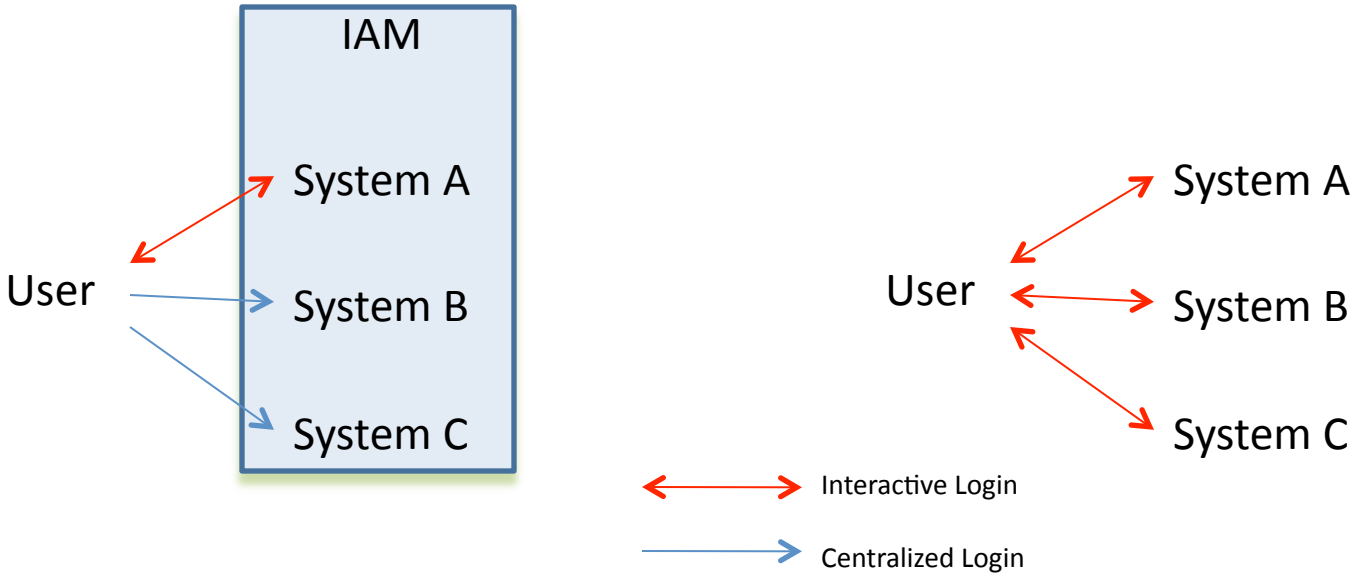
- FICAM Roadmap and Implementation Guidance identifies four solution architectures in Chapter 11 (Modernize LACS Infrastructure):
  1. Enterprise Authentication - Enterprise Authorization
     - Fully realized IAM suite
  2. Enterprise Authentication - Decentralized Authorization
     - Partial IAM suite / Single Sign-on *
  3. Decentralized Authentication – Enterprise Authorization
     - Partial IAM suite or roll-your-own application interfaces
  4. Decentralized Authentication – Decentralized Authorization
     - Chaos
- Option 1 is the preferred solution for a variety of reasons
- Option 4 seems to be the default in many agencies

** Wait for it*

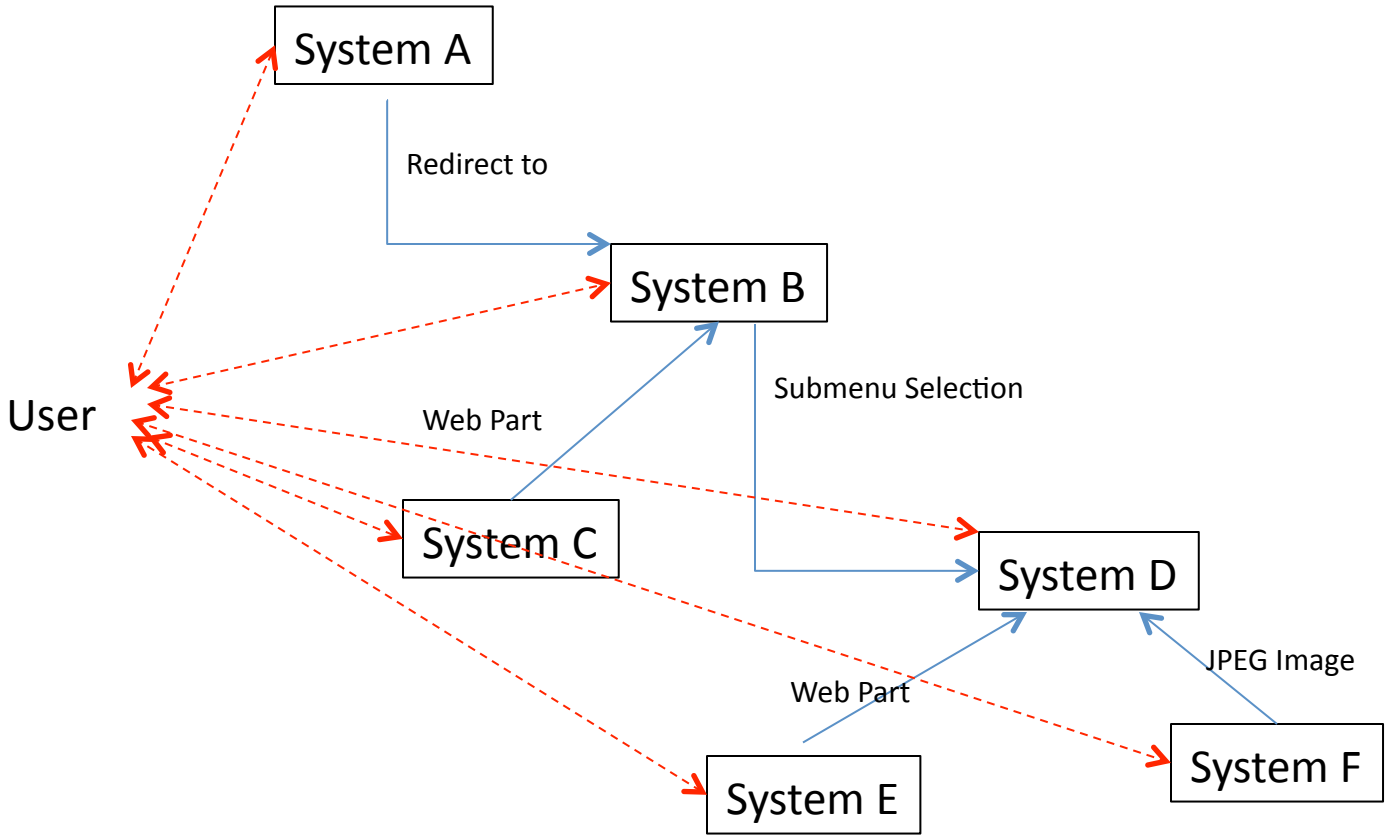
Enterprise vs. Decentralized Authentication

The first time the User hits a system protected by the IAM system, he is authenticated. Subsequent visits to other systems protected by the IAM system do not require re-authentication (unless desired)

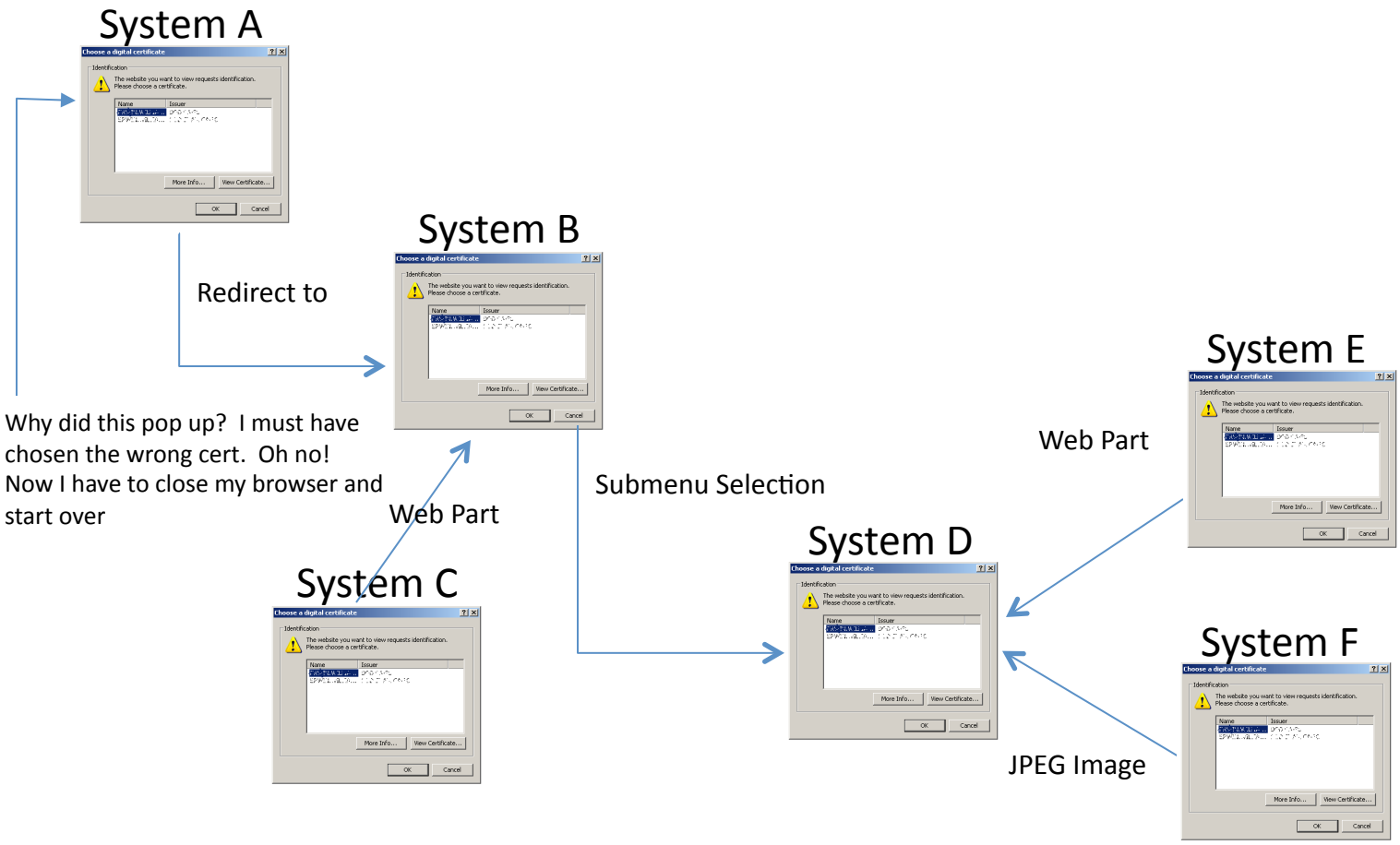
Every time the User hits a system, he is authenticated. The good news is that it is the PIV PIN that is entered, the bad news is that it requires selection of the appropriate certificate on the card – sometimes multiple times during a login attempt



Decentralized Authentications with Multiple Systems

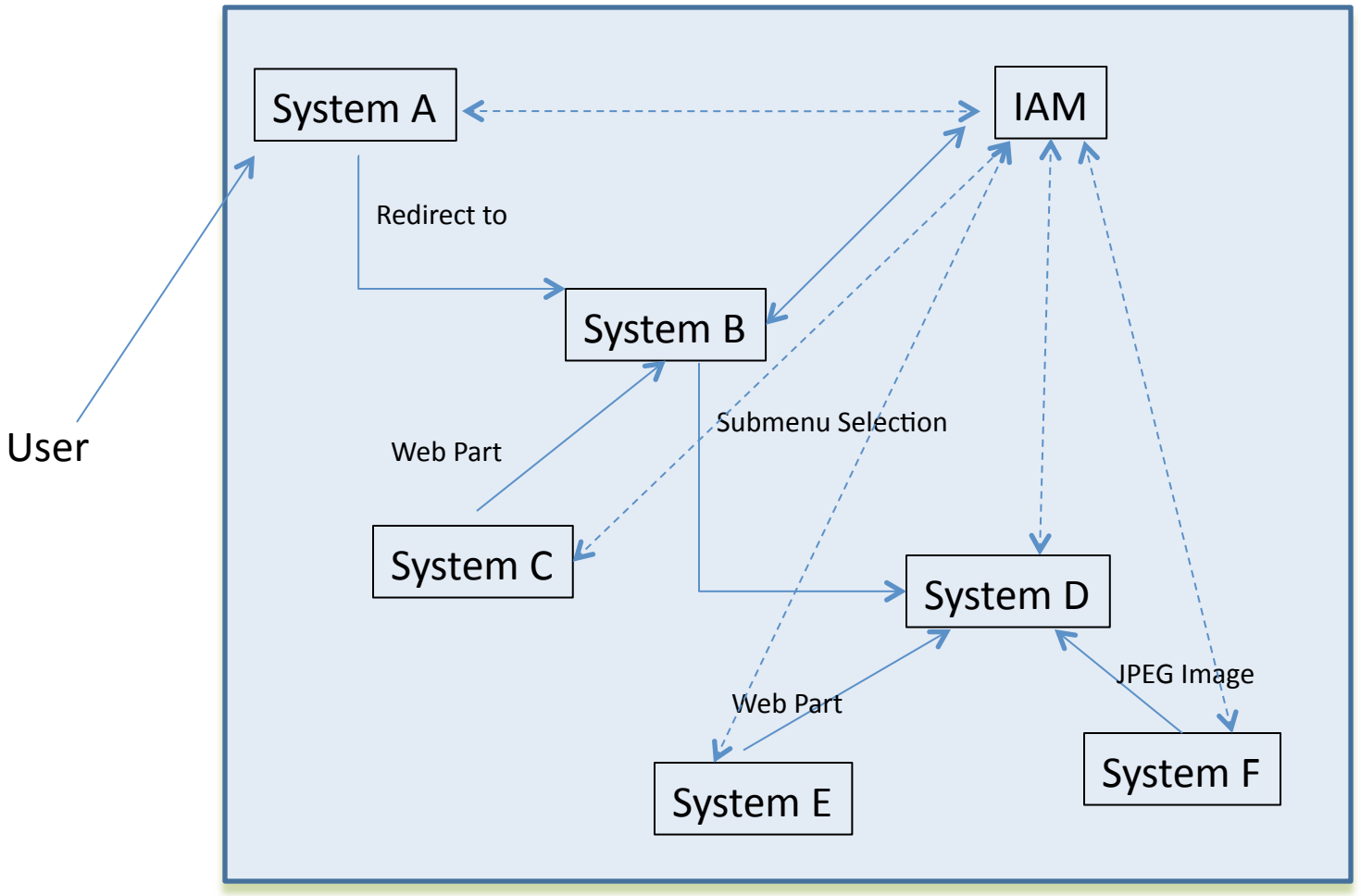


Decentralized Authentications From the User's Perspective



Assuming No Certificate Errors!!

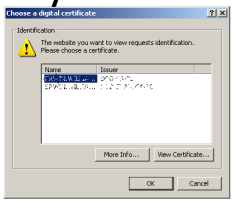
Enterprise Authentication with Multiple Systems



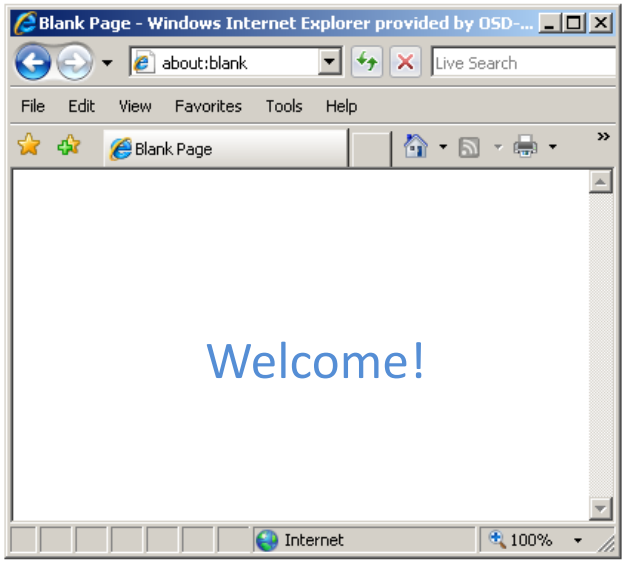
Enterprise Authentications From the User's Perspective

If this is the first login

System A



Otherwise…



An Important Point *

Single Sign-on ≠ PIV-enablement

Enterprise Authentication gives PIV-enablement along with appearance of Single Sign-on

** Here it is*

Another Important Point

ANY system URL that starts with https:// and is configured to accept or require client certificate authentication will prompt a login attempt – even malicious websites!

Questions?