Authentication in the Cloud

Ramesh Rangachar
Creative Information Technology Inc.

Ground System Architectures Workshop

AEROSPACE
Assuring Space Mission Success

"Imagining the Future"

Renaissance Los Angeles Airport Hotel

Feb. 24–27, 2014

Agenda

- Definitions
- Approaches for Authentication
- Authentication in the Cloud
- Federated Identity
- Summary

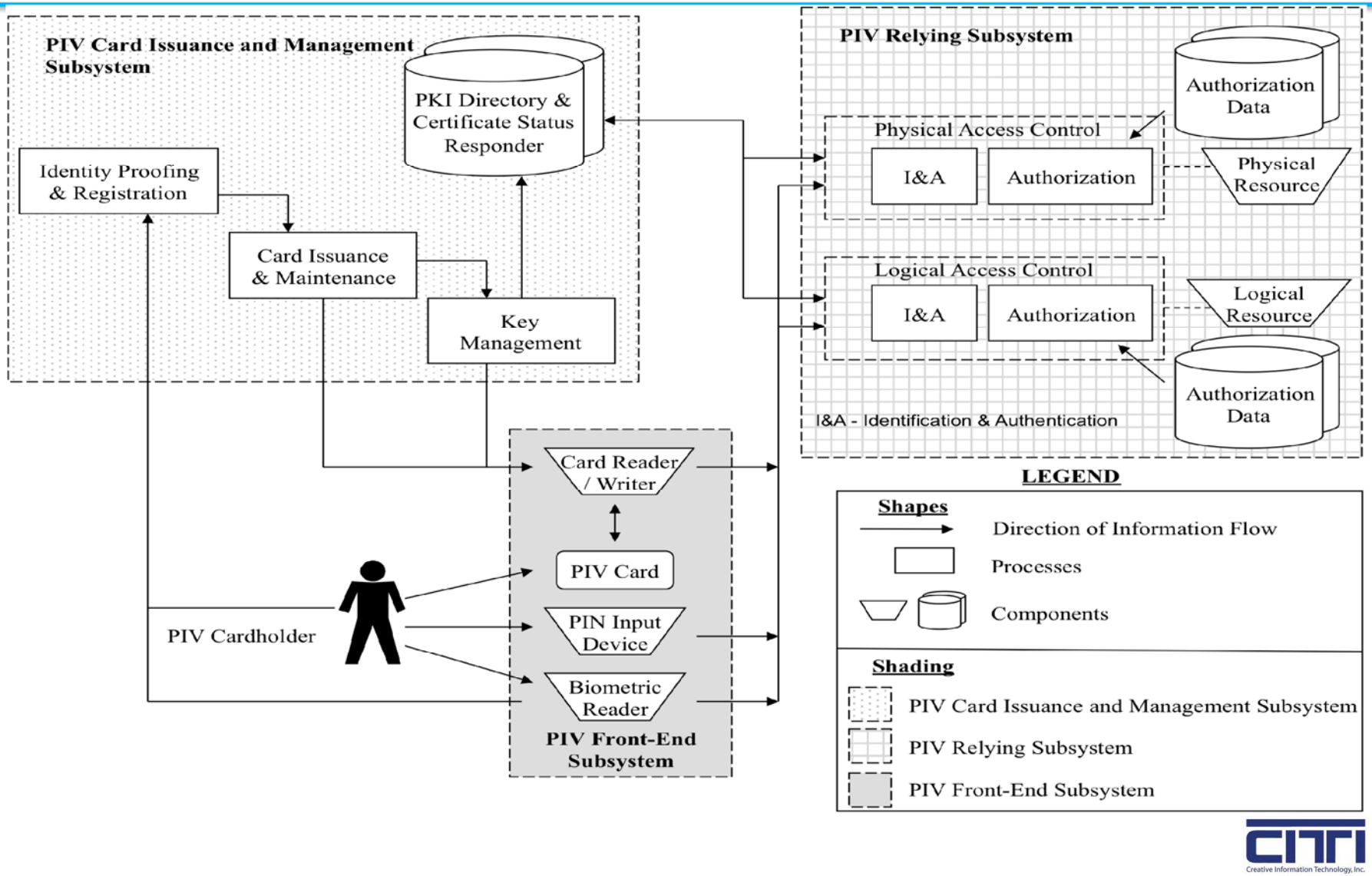
Definitions

- Authentication: Ensure that all individuals (or non-person entities) attempting access are properly validated
- Confidentiality: Ensure that all access to information is authorized
- Integrity: Protect information from unauthorized creation, modification, or deletion
- Nonrepudiation: Ensure the accountability of parties when gaining access and performing actions

Approaches for Authentication

- Something you know (Password, PIN)
  - Most common form of authentication
  - Can be forgotten
- Something you have (smart card, token)
  - Carry something with you, use it every time you want to be authenticated
  - Can be lost or stolen
- Something you are (fingerprint, iris)
  - Biometric; based on some physical or behavioral trait
  - Much harder to lose
  - If stolen, cannot be “replaced”

Example: PIV Card



Other approaches

- Multiform Authentication (MFA)
  - More than one form of authentication is used to verify the legitimacy of a person or transaction
    - PIN/Password, Soft/Hard tokens, SMS, etc.
  - Makes it more difficult for an unauthorized person to access resources
  - Examples: Google, Windows Azure, AWS, PayPal, etc.
- Risk Based Authentication
  - Additional factors of authentication used based on “risk”
  - Example 1: Online banking from an unrecognized computer
  - Example 2: Periodically (once a week or month)

Authentication in the cloud

- Much bigger problem than authentication in local workstations or within a network domain
- Multiple clouds and multiple applications means multiple passwords
- Some services use multi-factor and risk-based authentication
- Solution: Federated identities

Federated Identity

- Federated identity: Linking a person's electronic identity and attributes stored across multiple distinct identity management systems
  - A service or application does not need to obtain and store users' credentials in order to authenticate users
  - It can use another "trusted identity management system" to authenticate the user
  - Examples: Use your Facebook, Google, or Paypal credentials elsewhere
- Benefits:
  - Authorization and authentication are decoupled
  - The Relying Party still controls the authorization
  - Users need to remember fewer passwords
  - Higher level of PII (Personally Identifiable Information) security and protection

Federated Identity Standards

- SAML (Security Assertion Markup Language):
  - Developed in 2002 by the OASIS Security Services Technical Committee (SAML 2.0 was ratified as an OASIS Standard in 2005)
  - An XML-based open standard for exchanging authentication and authorization
- OpenID:
  - An open standard released in 2006
  - Over one billion OpenID enabled user accounts and over 50,000 websites accepting OpenID for logins
  - Several large organizations either issue or accept OpenIDs, including Google, Facebook, Yahoo!, Microsoft, AOL, Sears, France Telecom, Novell, Sun, Telecom Italia, and many more
- OAuth:
  - Open standard available since 2006 (OAuth 2.0 in 2012)
  - Allows apps to share information via APIs with the right level of authorization

FCCX

- The Federal Cloud Credential Exchange (FCCX) allows agencies to securely interact with a single “broker” to authenticate consumers

- Centralized interface between agencies and credential providers reduces costs and complexity
- Enhanced consumer privacy and experience; user does not have to get a new credential for each agency application
- Decreased Federal government authentication costs

Summary

- Authentication: Ensure that all individuals (or non-person entities) attempting access are properly validated
- Approaches for Authentication
  - Something you know (Password, PIN)
  - Something you have (smart card, token)
  - Something you are (fingerprint, iris)
- Multiform Authentication and Risk Based Authentication further improve authentication, confidentiality, integrity, and non-repudiation
- Authentication in the Cloud is complicated by the number of passwords, tokens, etc. one needs to remember and manage
- Federated Identity significantly improves authentication in the cloud

References

- http://www.emc.com/security/rsa-securid/rsa-securid-hardware-authenticators.htm
- http://www.wired.com/threatlevel/2007/12/fbi-building-va/
- http://hawaiigreenit.com/cloudcomputing.html
- Douglas Glair, USPS. Federal Cloud Credential Exchange Briefing, October 16, 2013. http://ww*w.idecosystem.org/filedepot_download/1214/925*
- http://en.wikipedia.org/wiki/SAML_2.0
- http://openid.net/