Identity Authentication using the PIV Token

Sarbari Gupta

sarbari@electrosoft-inc.com

October 6, 2004

Identity Authentication

- Definition
  - The process of establishing confidence in the identity of a User presenting a PIV Token
- Purpose
  - Allow an Agency to make access decision (to controlled Federal Resources) based on authenticated identity of the User and the Agency's own access control policy

Authentication Assurance Levels

- Resource Owner determines level of assurance required for authentication
- PIV Token Authentication Assurance Levels

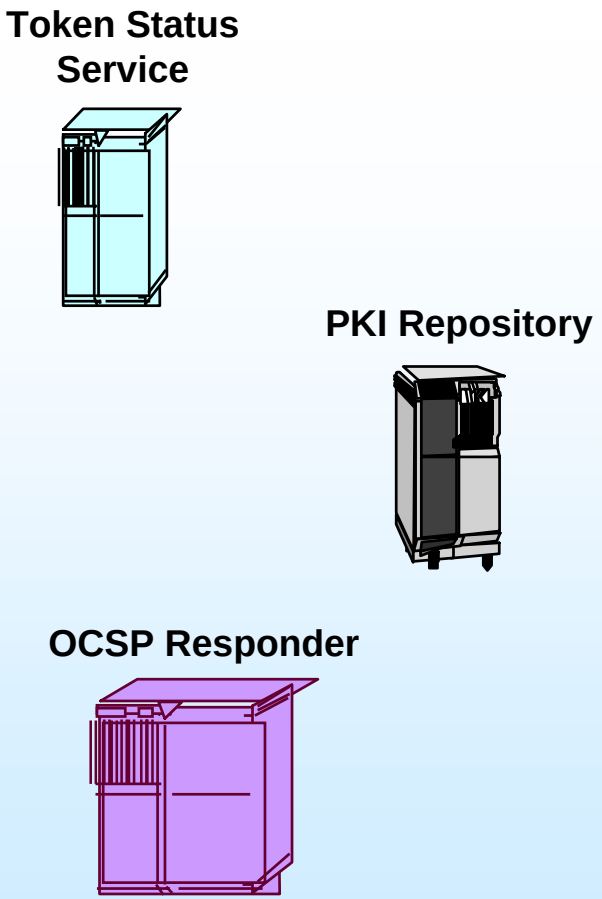
Authentication Assurance Level	Resistance to Threats
LOW	Forgery (limited), Illegitimate Use (limited)
MEDIUM	Forgery, Illegitimate Use (limited)
HIGH	Forgery, Illegitimate Use, Interposition

NOTE: Residual Access threat can be countered through use of backend systems and processes at any of the above levels

- PIV Token Use Threats
  - **Forgery**: Token cloning, tampering, bogus Token
  - **Illegitimate Use**: Use of valid Token by non-Owner
  - **Interposition**: Man-in-the-Middle Attacks on Protocol
  - **Residual Access**: Use of token beyond period of validity

Token Verification Infrastructure

- Token Status Service
  - LDAP Service
  - Provides status of PIV Token
- PKI Repository
  - LDAP Repository
  - Provides public key certificates and Certificate Revocation Lists (CRLs)
- OCSP Responder
  - OCSP Protocol
  - Provides Status of Certificate



PIV Token Authentication Environments

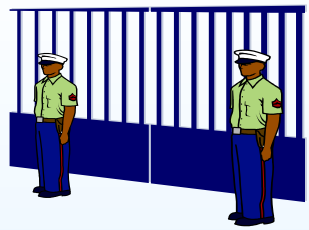
- Visual Authentication
  - No token reader
  - Human Intervention
- Contactless Authentication
  - Contactless Token Reader
  - No PIN Pad or Biometric Reader
- Contact-based Authentication
  - Contact Token Reader
  - PIN Pad
  - Biometric Reader

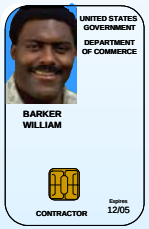
Authentication Environment	Suitable for Access Control to …
Visual	Physical Resources
Contactless	Physical Resources
Contact	Logical Resources, Physical Resources

Visual Authentication

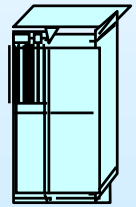
Physical Facility
Entry Point

Access Authorized





Token Status Service

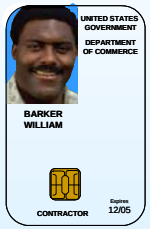


Visual comparison of Token holder and picture on Token followed by online status check of Token ID

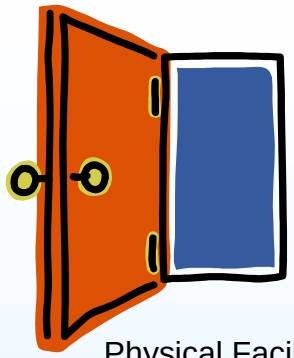
Visual Authentication Assurance Levels

- Low
  - Guard inspects PIV Token for
    - Physical Integrity
    - Match of picture to Token Holder
- Medium
  - Guard inspects PIV Token for
    - Physical Integrity
    - Match of picture to Token Holder
  - Guard inspects Second Picture ID
    - Match name and picture on both PIV Token and Second ID

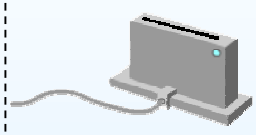
Contactless Authentication



Access Authorized



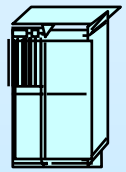
Physical Facility
Entry Point



Contactless Token
Reader

Control Panel

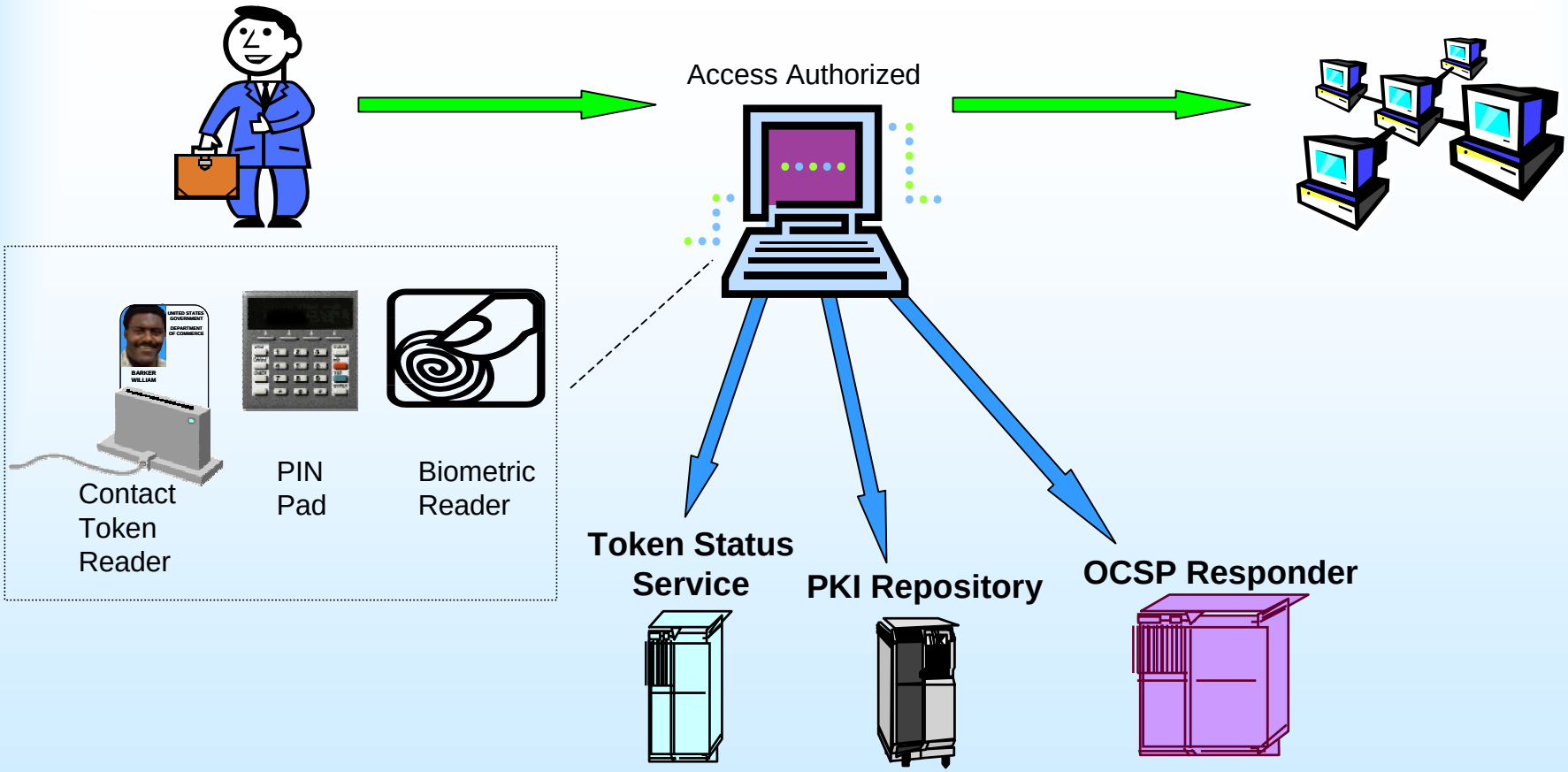
Token Status Service



Contactless Authentication Assurance Levels

- Low
  - PACS LOW Scheme
    - Open read of FASC-N (Electronic Token Holder ID)
    - Match of FASC-N to “Authorized FASC-N List”
- Medium
  - PACS Medium Scheme
    - Open read of FASC-N and Token Unique ID
    - Computation of Unique Authorization String
    - Compare to list of “Authorized Strings”

Contact Reader Authentication



Contact Token Authentication Assurance Levels

- Low (I)
  - PACS LOW Scheme
    - Open read of FASC-N
    - Match of Token ID to “Authorized List”
- Low (2)
  - Biometric Match-off-Card
    - Open read of Biometric Template from Token
    - No signature check on biometric template
    - Compare Token Holder’s biometric to template from Token

Contact Token Authentication Assurance Levels (contd.)

- Medium
  - PACS Medium Scheme
    - Open read of FASC-N and Token Unique ID
    - Compute Unique Authorization String
    - Compare to list of “Authorized Strings”

Contact Token Authentication Assurance Levels (contd.)

- High (1)
  - PACS High Scheme with PIN
    - Open read of FASC-N and Token Unique ID
    - Collect Token Holder PIN
    - Conduct Challenge-Response between Token Reader and Token
    - Compare Token Response to expected value (computed with collected and local info)
- High (2)
  - Biometric Match-off-Card with Signature Check
    - Open read of Signed Biometric Template from Token
    - Signature check on biometric template
    - Compare Token Holder's biometric to template from Token

Contact Token Authentication Assurance Levels (contd.)

- High (3)
  - Invoke Challenge-Response using Token Private Key
    - Issue Asymmetric Key Challenge to Token
    - Collect Token Holder PIN/Biometric and pass to Token
    - Receive Response to Challenge from Token
    - Verify digital signature on Response
    - Verify Token Holder's Certificate chain

PIV Token Authentication Summary

Authentication Mechanism	Assurance Level	Resource Suitability	Shorthand
Visual	Low	Physical	VIS
Visual+2nd Picture ID	Medium	Physical	VIS-ID
Biometric Match	Low	Physical	BIO
Biometric Match+Dig Sig Verification	High	Physical, Logical	BIO-S
PACS Low	Low	Physical	PACS-L
PACS Medium	Medium	Physical	PACS-M
PACS High	High	Physical, Logical	PACS-H
PKI Challenge Response	High	Physical, Logical	PKI

Network Connectivity	User Processing Volume	No Card Reader	Contactless Environment	Contact-Based Environ
No Connectivity	High User Volume	VIS	PACS-L	PACS-H
			PACS-M	
	Low User Volume	VIS-ID	PACS-L	
			PACS-M	
Network Connectivity	High User Volume	VIS/SC	PACS-L/SC	PACS-H/SC
			PACS-M/SC	
	Low User Volume	VIS-ID/SC	PACS-L/SC	PKI/SC
			PACS-M/SC	

NOTE: **SC** implies the use of online status check for PIV token or its resident credentials

Questions??