



---

Managed by Fermi Research Alliance, LLC for the U.S. Department of Energy Office of Science

---

# MultiFactor Authentication

Al Lilianstrom

Group Leader, Authentication Services

November 10<sup>th</sup>, 2015

# Outline

---

- What is MultiFactor Authentication
- MultiFactor Levels
- Why use MultiFactor Authentication
- Factors
- Technology
- MultiFactor Authentication at Fermilab
- MultiFactor Futures

# What is MultiFactor Authentication

---

- MultiFactor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
- Multifactor authentication combines two or more independent credentials:
  - Something the user knows - knowledge
  - Something the user has – possession
  - And the user – inherence
  - Where the user is – location
  - The time

# MultiFactor Levels

---

- Level 1 – Username/Password. No Identity Proofing required
- Level 2 – CryptoCard. Identity proofing required
- Level 3 – At least two authentication factors are required as well as identity proofing
- Level 4 – Authentication is based on proof of possession of a key through a cryptographic protocol
  - In-person identity proofing is required.

More at <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

# Why use MultiFactor

---

- The goal of MFA is to create a layered defense

If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

# The Factors in MultiFactor

---

- The most common categories/credentials
  - Something you know (knowledge)
  - Something you have (possession)
  - Something you are (inherence)
- Knowledge - User names, passwords, PINs and the answers to secret questions
- Possession factors - Security token, key fob, an employee ID card or smart phone.
- Inherence - any biological traits that have been confirmed for the user
  - retina scans, iris scans, fingerprint scans, finger vein scans, etc

## Other Factors

---

- Location factors – smartphones with GPS
- Time factors - verification of employee IDs against work schedules

# Multifactor authentication technologies

---

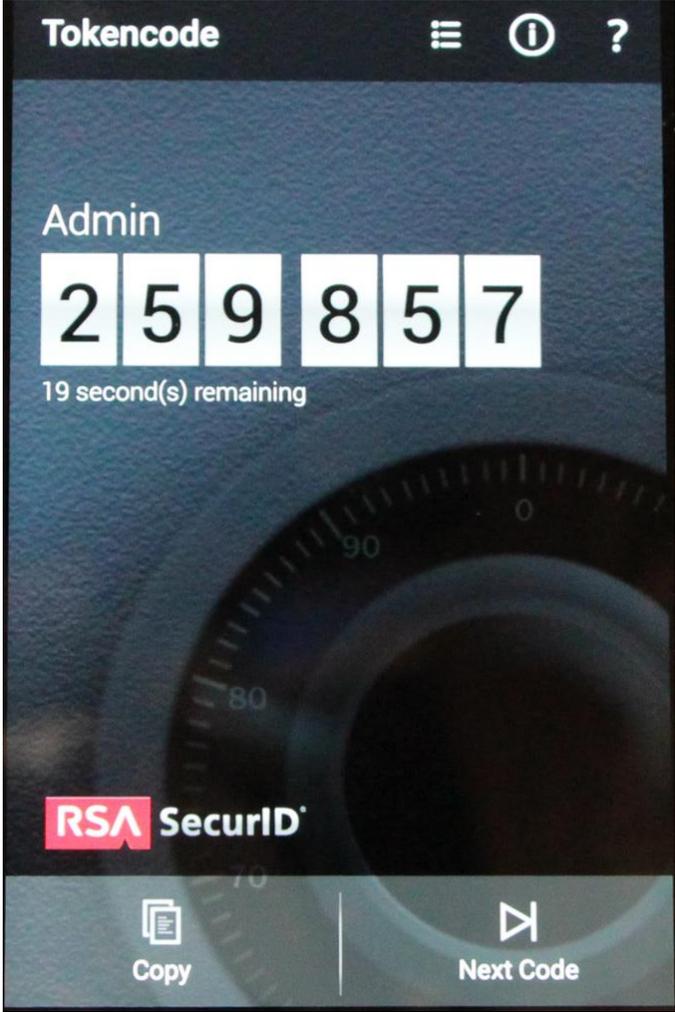
- Security tokens: Small hardware devices such as a key fob or USB drive
- Soft tokens: Software-based security token applications that generate a single-use login PIN
- Mobile authentication: SMS messages, phone calls, OTP apps, SIM cards and smartcards with stored authentication data
- Biometrics
- GPS in smartphones
- Employee ID and customer cards

# MultiFactor Authentication at Fermilab

---

- Fermilab implemented RSA SecurID
  - Commercial Application
  - Level 3
  - Requirements
    - Token
      - Something you have
      - Hardware or Software (smartphone app)
      - Provides a time sensitive passcode
    - PIN number
      - Something you know
        - Set when token is issued

# Tokens



# MultiFactor Authentication at Fermilab

---

- Usage
  - Windows
    - Select servers and desktops
    - Username and password used with token PIN/passcode
  - Linux
    - Select servers
    - Token PIN/passcode used instead of a Kerberos token
      - Requires kinit after login

# MultiFactor – Windows



# MultiFactor – Linux

```
lilstrom@mypi: ~  
lilstrom@mypi ~  
This is  
Fermilab  
States Go  
rized or  
of privac  
Any or  
be inter  
and disc  
enforceme  
agencies,  
user cons  
ing, aud  
authorize  
Unauthori  
istrative  
By contin  
and cons  
DIATELY i  
warning.  
Fermilab  
use, may  
Enter PASSCODE:   
enforcement personnel, as well as authorized officials of other  
agencies, both domestic and foreign. By using this system, the  
user consents to such interception, monitoring, recording, copy-  
ing, auditing, inspection, and disclosure at the discretion of  
authorized site or Department of Energy personnel.  
Unauthorized or improper use of this system may result in admin-  
istrative disciplinary action and civil and criminal penalties.  
By continuing to use this system you indicate your awareness of  
and consent to these terms and conditions of use. LOG OFF IMME-  
DIATELY if you do not agree to the conditions stated in this  
warning.  
Fermilab policy and rules for computing, including appropriate  
use, may be found at http://www.fnal.gov/cd/main/cpolicy.html  
Direct questions regarding this system to the FNAL ServiceDesk  
(x2345 or servicedesk.fnal.gov)  
#####  
Standard maintenance downtime for all fnalu nodes is Wednesdays at 7:30am.  
If maintenance is required a posting will appear below this message.  
#####  
Terminal type is xterm  
There are no available articles.  
/bin/touch: cannot touch `/afs/fnal.gov/files/home/room3/lilstrom/.Info': Permis  
sion denied  
-bash-3.2$
```

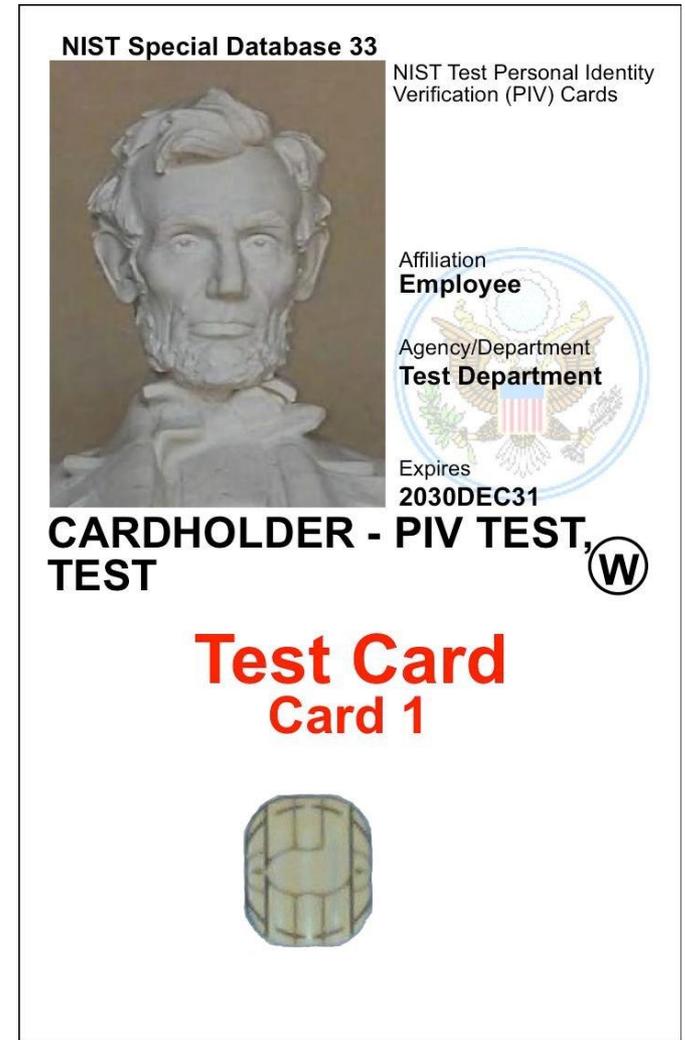
# MultiFactor in 2016

---

- Level 4 MultiFactor may be required for “elevated access”
  - Elevated access is not yet completely defined
    - Required by DOE – due September 30<sup>th</sup>, 2016
  - Reminder – In Level 4 Authentication is based on proof of possession of a key through a cryptographic protocol
- HSPD-12 aka PIV
  - Developed by the U.S. government to comply with Homeland Security Presidential Directive 12 (HSPD-12), Personal Identity Verification (PIV) credentials provide government users with physical and logical access to U.S. federal buildings and networks via a PKI-enabled smartcard.
  - PIV card has a chip – much like new credit cards
    - Chip contains a certificate (or certificates) that identify the user

# MultiFactor in 2016

- If required - Fermilab plans to implement PIV-I not HSPD-12
  - What is PIV-I?
    - Trusted basic identity and credential
    - Personal Identity Verification Interoperability for Non-Federal Issuers FICAM PIV-I FAQ
    - Motivation - Interoperable credential for organizations doing business with the government
- Level 4 differs from Level 3 in that the card must be inserted into the device that is being logged into



# Links

---

- [How to Install RSA SecurID Token on iOS or Android](#)
- [Making a Linux system accessible without Kerberos using RSA SecurID](#)
- [Using RSA SecurID Token](#)
- [How to reset your PIN for a key fob](#)
- [Logging In from Off-Site](#)
- [PIV vs PIV-I](#)

# Questions

---

Al Lilianstrom

lilstrom@fnal.gov