Electrosoft

Results That Drive Mission Success!

Digital Authentication – Mobile Platforms to the Rescue!

Dr. Sarbari Gupta, CISSP, CISA
CEO, Electrosoft

Identity Week USA 2024
Washington, DC
September 11, 2024

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

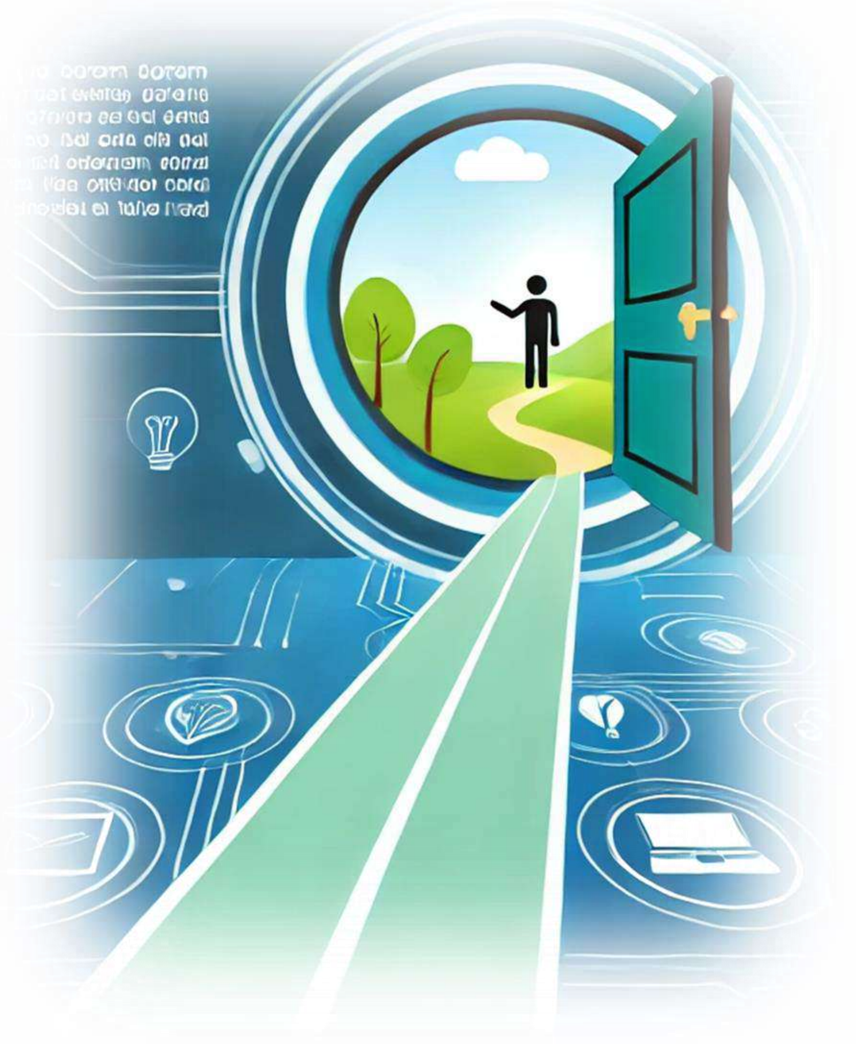
Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
Fax: (703) 437-9452

Agenda

- Introduction
- Capabilities of Mobile Devices
- Digital Authentication Support through Mobile Devices
- NIST SP 800-63-4 Connection
- Wrap-Up

Introduction

Basics



- What is Digital Authentication?
  - Verifying the identity of users attempting to access online services
- Traditional Authentication Factors
  - Something You Know (SYK)
    - Password, PIN, Passphrase
  - Something You Have (SYH)
    - Key Fob, Device, Smartcard
  - Something You Are (SYA)
    - Facial Image, Fingerprint, Voiceprint

Electrosoft

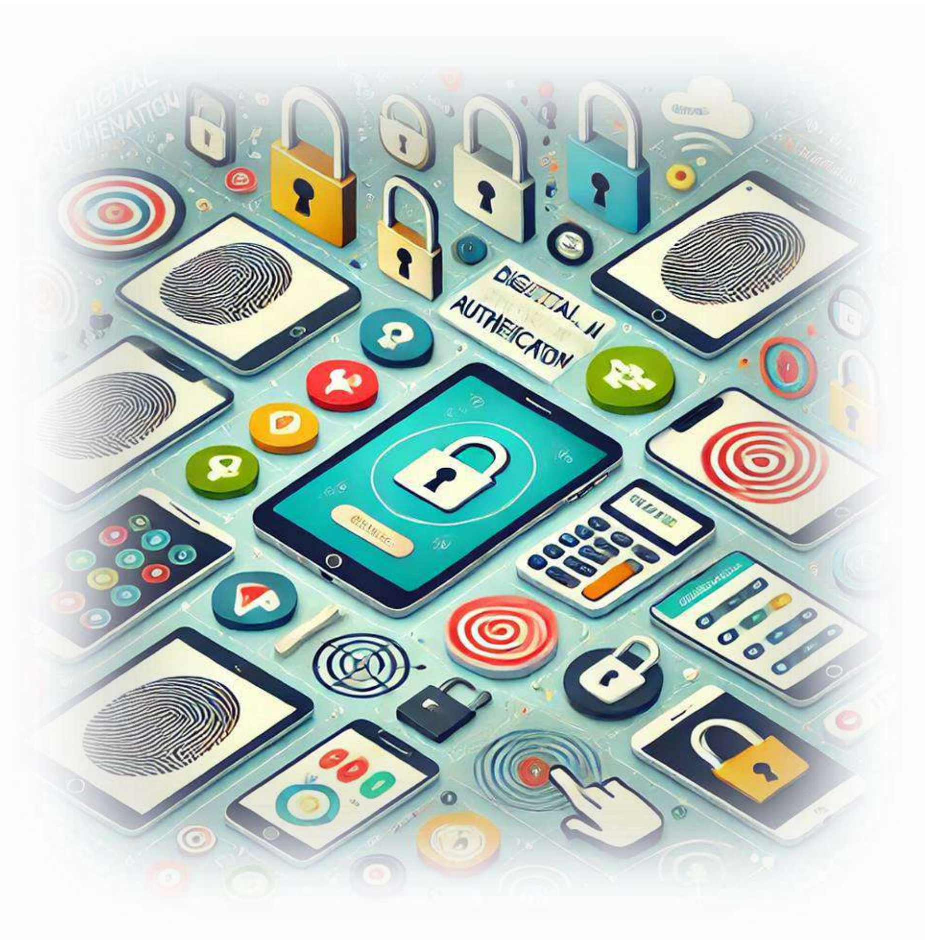
Current Challenges in Digital Authentication

- **Weak Passwords and Credential Reuse**
  - 80% of breaches involve compromised or weak credentials
- **Phishing and Social Engineering Attacks**
  - Users are often tricked into divulging credentials
- **Balancing Security and Usability:**
  - Need for robust security measures without impacting user experience

Electrosoft

Capabilities of Mobile Devices

Mobile Device as an Authentication Tool



- **Mobile Devices as Authentication Enablers**
  - Built-in Biometrics: Fingerprint sensors, facial recognition
  - Cryptographic Chips: Secure elements for storing secrets
  - Connectivity: Continuous access to the internet for real-time authentication
- **Advantages of Mobile Devices**
  - Ubiquitous
  - Personal and unique to each user
  - Always with the user, reducing dependency on external tokens
  - Offer built-in sensors and advanced hardware/software features

Capabilities - Smart Mobile Platforms (I)

- **Multiple Biometric Sensors**
  - Camera – Facial Image and Iris Scan
  - Fingerprint Scanner – Fingerprint
  - Voice – Voiceprint
- **Multiple Wireless Connectivity Mechanisms**
  - Cellular
  - Wi-Fi
  - Bluetooth
  - Near Field Communications (NFC)

Capabilities - Smart Mobile Platforms (II)

- **Multiple Contextual Sensors**
  - Accelerometer – senses axis-based motion, orientation, motion
  - Gyroscope – senses orientation and movement
  - Magnetometer – senses geographical direction (North, South, etc.)
  - GPS – determines location based on connection with GPS satellites
  - Barometer – measures air pressure
  - Proximity Sensor – determines distance from body

Capabilities - Smart Mobile Platforms (III)

- **Application Sandboxing**
  - Each App (or App Group) runs in its own sandbox
- **Reliable Network Time**
  - Important for secure transactions between parties
- **Cryptographic Capabilities**
  - Cryptographic key generation (symmetric / asymmetric)
  - Encryption / Decryption
  - Digital signature generation / verification
- **Secure Storage**
  - Cryptographic keys

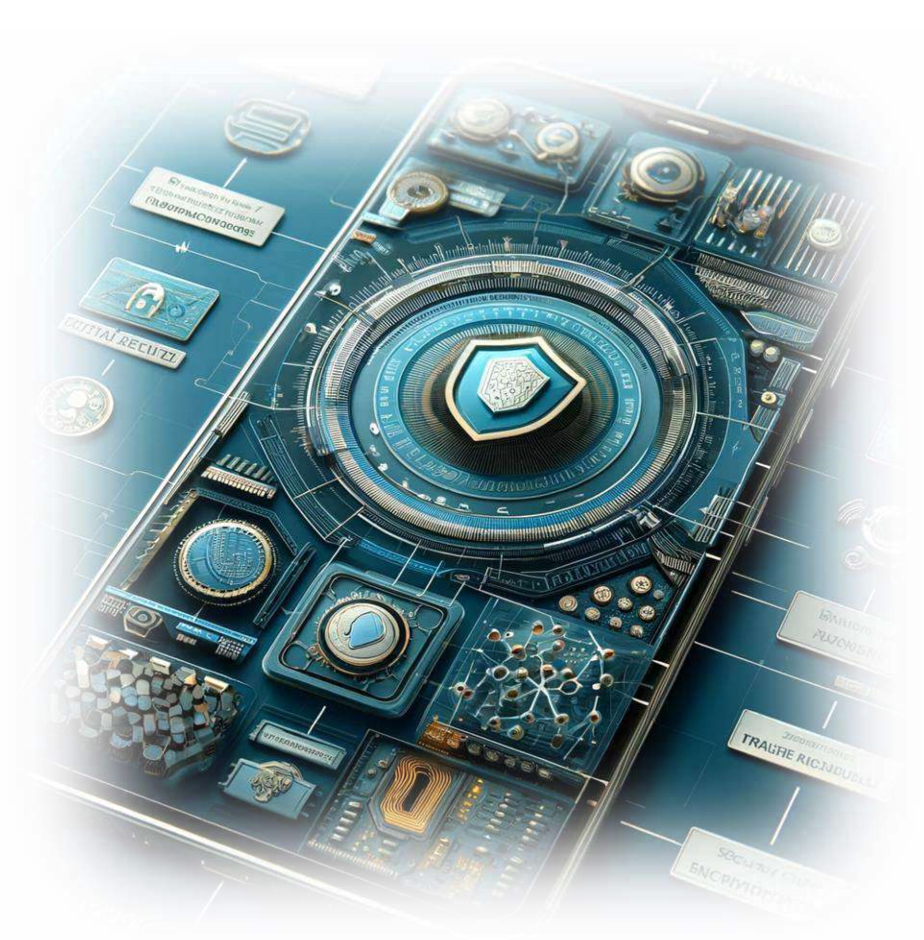
Digital Authentication Support through Mobile Devices

Authentication Apps on Mobile Devices

- **Password Managers**
  - Secure storage for complex passwords, autofill capabilities
  - Example: Integration with device biometrics (Face ID, Fingerprint)
- **OTP (One-Time Password) Generators**
  - TOTP (Time-based OTP) and HOTP (HMAC-based OTP) for 2FA
  - Examples: Google Authenticator, Microsoft Authenticator
  - Benefits: Offline operation, low cost, no reliance on SMS

Electrosoft

Leveraging Cryptographic Capabilities



- **Hardware Security Modules (HSMs)**
  - Secure Enclave (iOS) and TrustZone (Android) for key management
  - Protect cryptographic operations from the main OS
- **Public Key Infrastructure (PKI)**
  - Use of digital certificates for secure client authentication
  - Mobile apps using certificates for seamless, secure user access
- **Example Use Cases**
  - Banking apps using device-based certificates for transactions
  - Derived PIV Credentials

Biometric Authentication

- Mobile Biometric Sensors
  - Fingerprint, facial recognition, iris scanning
- Local Authentication
  - Unlocking devices or apps
- Using a Biometric as an Activation Factor
  - Enabling use of Multifactor Authentication (MFA) credentials

Electrosoft

Out-of-Band (OOB) Authentication

- **What is it?**
  - **Utilizing a separate communication channel (SMS, push notifications)**
- **Examples**
  - **Bank sends one time code via SMS for transactions**
  - **Mobile push notifications for approving logins**
- **Security Considerations**
  - **Risks: SIM swap attacks, malware interception**

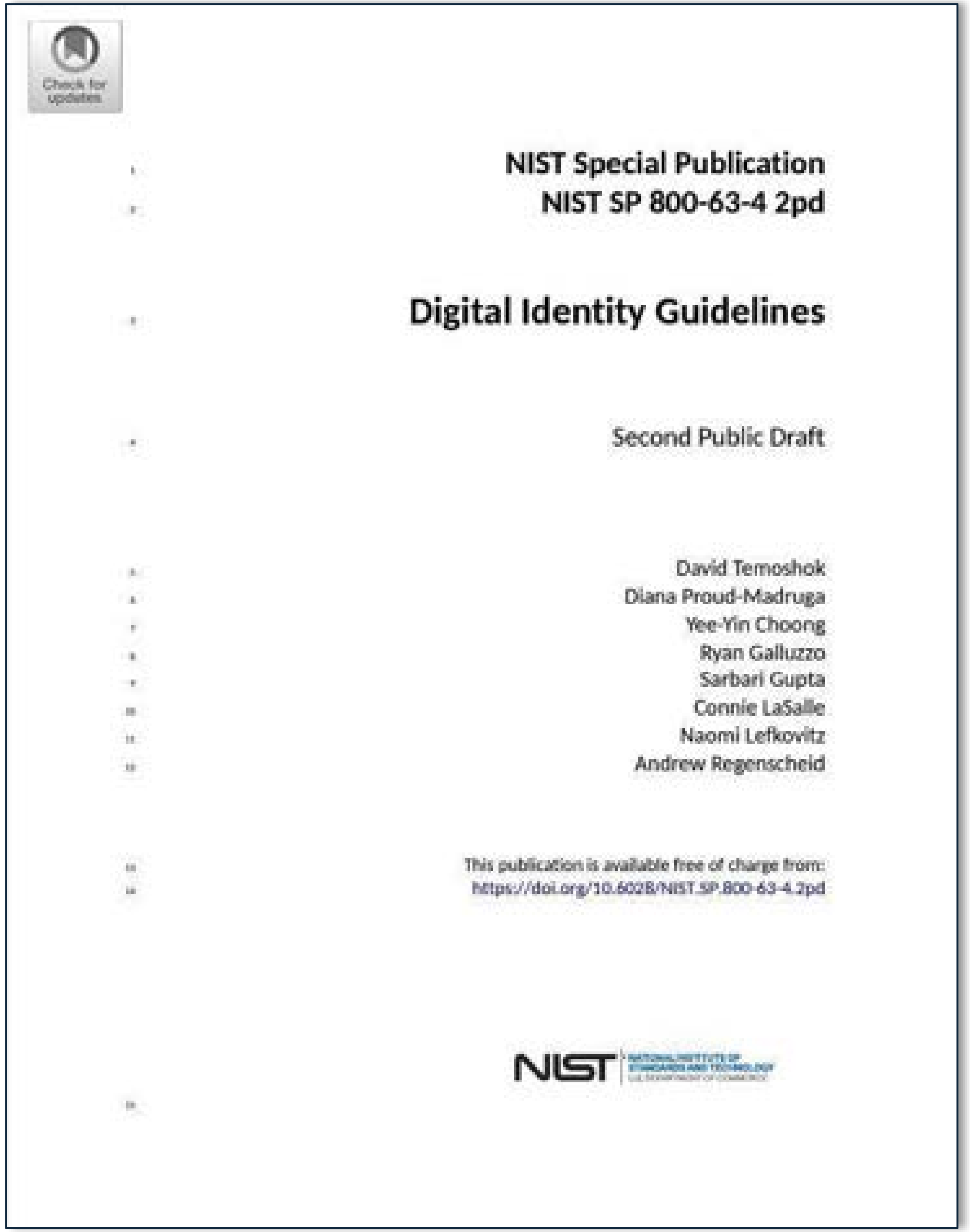
Emerging Trends and Future Capabilities

- FIDO2 and WebAuthn
  - Passwordless authentication using mobile devices
  - Use of mobile hardware for secure cryptographic credential storage (public/private keys)
  - Widely supported on mobile and traditional OS and Browser platforms
- Mobile Drivers License (mDL)
  - Digital version of traditional driver's license stored on mobile device (based on ISO 18013-5)
  - Can be used for identity verification both online and offline
  - Leverages Near Field Communication (NFC), QR codes
  - Incorporates data encryption and ability to control which information is shared
- Continuous and Adaptive Authentication
  - Continuous monitoring using mobile device sensors (location, behavior)
  - Adjust security dynamically based on detected risks

NIST Special Publication 800-63-4 Connection

NIST SP 800-63-4 2pd

- **Second Public Draft**
  - Released Aug 21, 2024
- **Public Comment Period**
  - 8/21/24 to 10/7/24
- **Four (4) Volumes**
  - SP 800-63-4: Digital Identity Risk Management and Model
  - SP 800-63A-4: Identity Proofing and Enrollment
  - SP 800-63B-4: Authentication and Authenticator Management
  - SP 800-63C-4: Federation and Assertions



Check for updates

NIST Special Publication
NIST SP 800-63-4 2pd

Digital Identity Guidelines

Second Public Draft

David Temoshok
Diana Proud-Madruga
Yee-Yin Choong
Ryan Galluzzo
Sarbari Gupta
Connie LaSalle
Naomi Lefkovitz
Andrew Regenscheid

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-4.2pd

NIST

NIST SP 800-63B-4 2pd Authenticator Types

- Password (SYK)
  - Secret value chosen by and either memorized or recorded by the subscriber
- Look-Up Secret (SYH)
  - Physical or electronic record that stores a set of shared secrets
- Single-factor OOB Device (SYH)
  - Physical device that is uniquely addressable
  - Can communicate securely over distinct communications channel
- Multi-factor OOB Device (SYH)
  - Out-of-Band Device that can be used only after successful input of an activation factor
- Single Factor OTP (SYH)
  - Hardware or Software-based tool with an embedded secret used for generating one-time passwords
- Multi-factor OTP (SYH and (SYK or SYA))
  - An OTP generator that can be used only after successful input of an activation factor
- Single-Factor Cryptographic Authenticator (STH)
  - Hardware or Software-based cryptographic module used to prove possession of encapsulated cryptographic keys via an authentication protocol
- Multi-factor Cryptographic Authenticator (SYH and (SYK or SYA))
  - Cryptographic authenticator that can be used only after successful input of an activation factor

Support for SP 800-63B-4 Authenticators

SP 800-63B-4 Authenticator Type	Support on Mobile Devices
Password	Password Managers
Look-up-Secret	List of Pre-Generated Secrets stored on Mobile Device
Single-factor Out-of-Band Device	One time use code sent via SMS
Multi-factor Out-of-Band Device	Same as above but enabled by Face/PIN/Fingerprint
Single-Factor OTP	Authenticator Apps that generate OTPs
Multi-factor OTP	Same as above but enabled by Face/PIN/Fingerprint
Single-Factor Cryptographic Authenticator	Single-factor FIDO2
Multi-Factor Cryptographic Authenticator	Multi-factor FID02, mDL

Wrap-Up

Electrosoft

Security Considerations and Best Practices

- **Risks of Mobile-Based Authentication**
  - Device theft or loss, malware, phishing
- **Mitigation Strategies**
  - Regular software updates
  - Using encrypted storage
  - Strong PINs/passwords
  - Enabling remote wipe
  - App-based MFA
- **User Education**
  - Training users to recognize threats like phishing and social engineering

Conclusion

- **Key Points**
  - Mobile devices offer multiple layers of authentication apps, biometrics, cryptographic capabilities
  - They provide robust security while enhancing usability
- **Recommendations**
  - Encourage adoption of mobile-based authentication strategies
  - Continuous improvement and adaptation to emerging threats
- **Final Thoughts**
  - Mobile devices are not just a convenience but a key enabler of secure, user-friendly digital authentication

Discussion and Contact Information

- **Dr. Sarbari Gupta**
  - **LinkedIn: https://www.linkedin.com/in/sarbari-gupta/**
- **Electrosoft**
  - **Web: http://www.electrosoft-inc.com**
  - **LinkedIn: https://www.linkedin.com/company/electrosoft/**
  - **HQ: 1893 Metro Center Drive, Suite 228**
    Reston VA 20190