2019 SECURITY CONGRESS

Me and My Mobile Device – A New Approach for Strong Multidimensional Authentication!

Dr. Sarbari Gupta, CISSP, CISA

President & CEO, Electrosoft

October 29, 2019

Old Fashioned Identity Authentication!

© Mike Baldwin / Cornered

BALDWIN
ATM
TO VERIFY YOU ARE WHO YOU SAY YOU ARE, STICK HEAD THROUGH HOLE

Agenda

- **Identity Authentication**
    - ***Fundamentals and Current State***
- **Smart Mobile Devices**
    - ***Capability/Feature Tour***
- **HyperAuth Model**
    - ***Leveraging the Smart Mobile Device***
    - ***Key Features and Benefits***

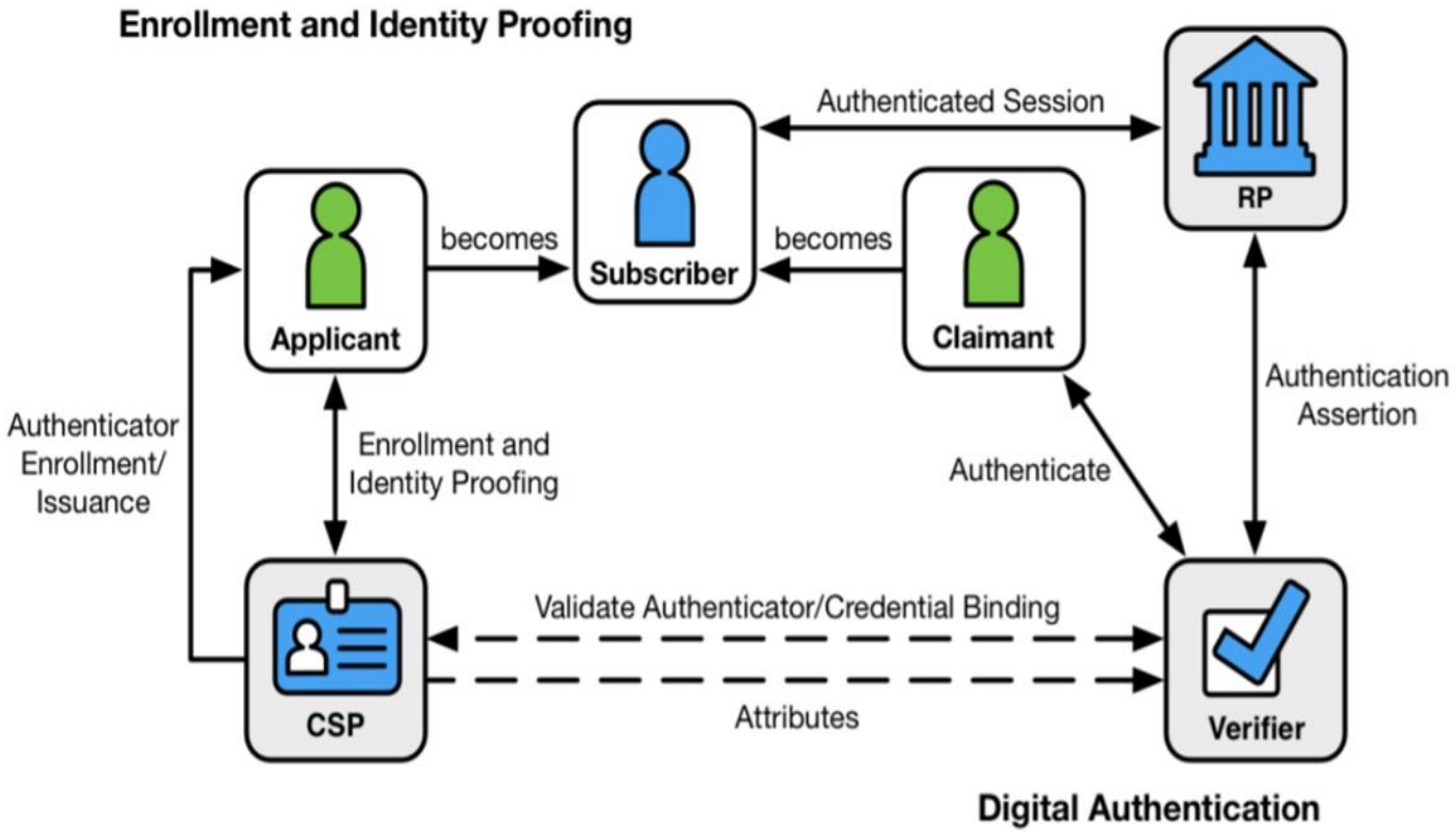
Identity Authentication

Fundamentals and Current State

Basic Definitions - [NIST SP 800-63-3]

- **Digital identity** is the unique representation of a subject engaged in an online transaction.
- **Digital authentication** is the process of determining the validity of one or more authenticators used to claim a digital identity.
- **Identity proofing** establishes that a subject is who they claim to be.
- **Successful authentication** provides reasonable risk-based assurances that the subject accessing the service today is the same as that which previously accessed the service.

Digital Identity Model - [NIST SP 800-63-3]



- RP – Relying Party (or Service Provider)
- CSP – Credential Service Provider

Traditional Factors of Authentication

- Something You Know
  - *Password, PIN, Passphrase*
- Something You Have
  - *Key Fob, Device, Smartcard*
- Something You Are
  - *Facial Image, Fingerprint, Voiceprint*

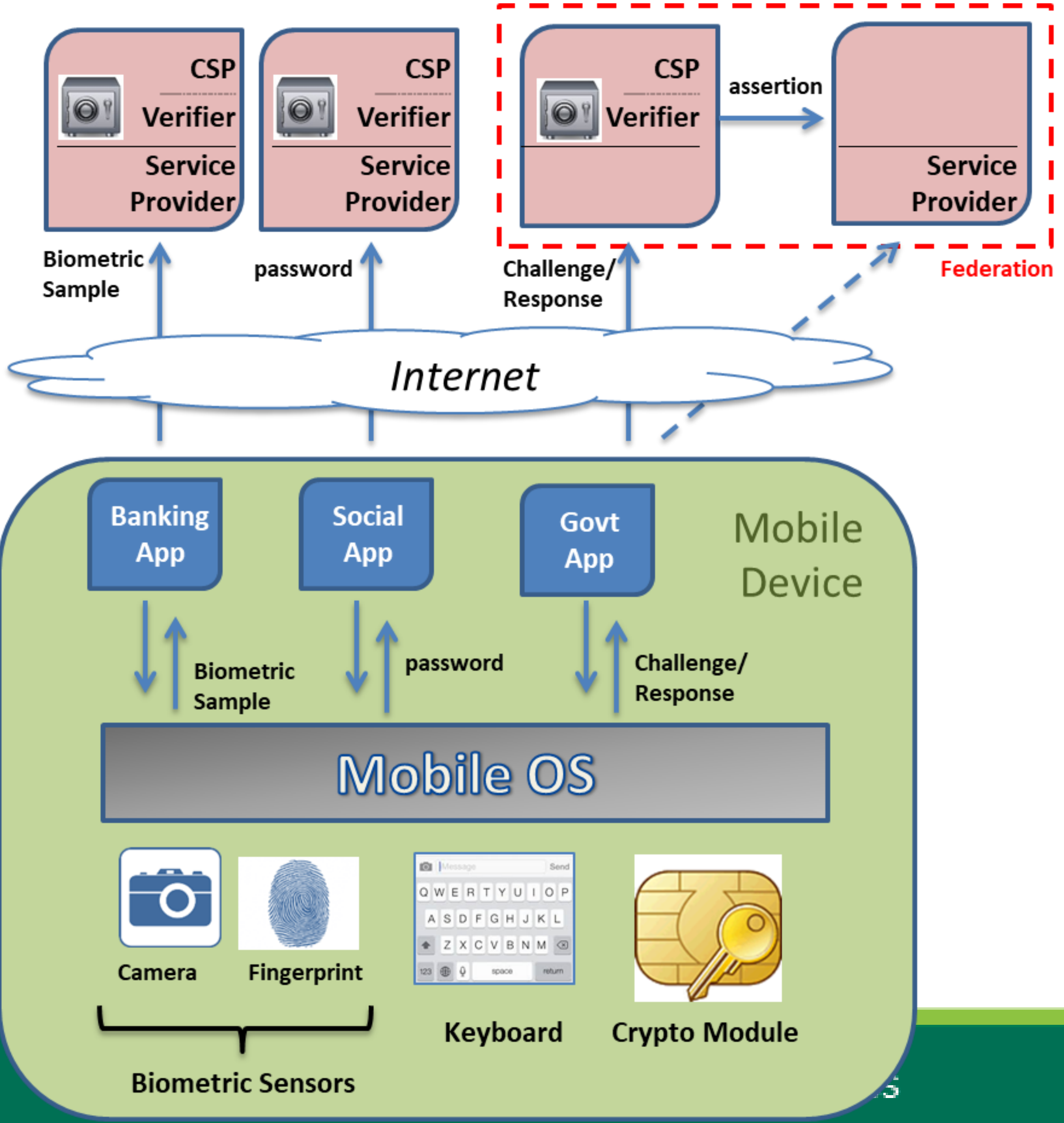
Traditional Authentication Models

- **Unique Identity Per Service: Service Provider (RP) also acts as its own CSP and Verifier**
  - ***User establishes unique token and credential for each Service Provider***
- **Federated Identity: Service Provider relies on Assertions from an external Verifier**
  - ***User may use single identity (token and credential) with multiple Service Providers***

- **Common Themes**
  - ***1, 2 or 3 factor authentication***
  - ***Verifier is remote to the User***

Traditional Authentication Scenarios

- Supports 1, 2 or 3 discrete factors
- Remote Verifiers maintain local copies of Authentication Reference Data
- Transmission of live authentication data over shared networks for verification
- Federation - Verifier sends assertion to Service Provider



KEY

- Authentication Reference Data Container

Smart Mobile Devices

Quick Capability/Feature Tour

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*
  - *Authentication Reference Data*

Hyper Authentication (HyperAuth) Model

Leveraging the Smart Mobile Device

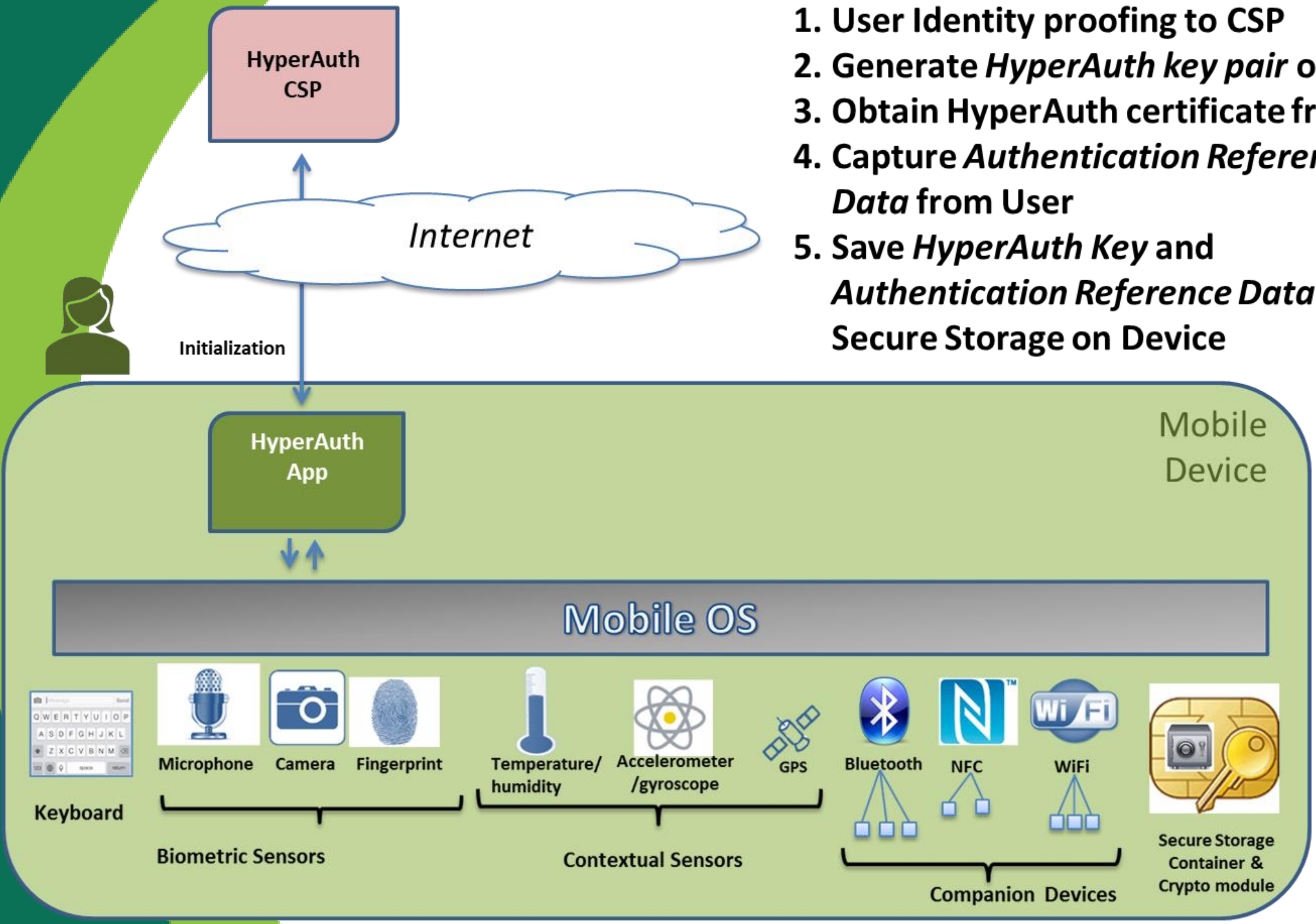
HyperAuth Model – Overview

- Leverages (biometric/contextual) sensors to:
  - *Allow User to enroll his/her Authentication Reference Data_(e.g., fingerprint, facial image, Wi-Fi SSIDs, companion devices)*
  - *Gather "live information" to authenticate User against reference data*
- Uses cryptographic capabilities to:
  - *Generate a HyperAuth key pair*
  - *Sign authentication results*
- Secure storage on device serves as trusted container for:
  - *HyperAuth private key*
  - *Authentication Reference Data for User*
- Supports multi-factor and context-aware "local authentication" of User
- Supports multiple and granular identity assurance levels

Mobile HyperAuth Model – Initialization

- User launches HyperAuth app on device and connects with HyperAuth CSP to:
  - *Perform remote identity proofing activities (e.g. answer knowledge-based questions)*
  - *Initialize the HyperAuth app with a unique asymmetric key-pair and signing certificate – the signing key is used to sign HyperAuth authentication tokens*
  - *Initialize local secure storage container with User's Authentocation Reference Data such as:*
    - biometric reference data
    - cryptographic keys
    - Selected contextual reference data(such as GPS location or identification of companion devices at their typical home or work locations)

Mobile HyperAuth Model – Initialization



Initialization

1. User Identity proofing to CSP
2. Generate *HyperAuth key pair* on device
3. Obtain HyperAuth certificate from CSP
4. Capture *Authentication Reference Data* from User
5. Save *HyperAuth Key* and *Authentication Reference Data* to Secure Storage on Device

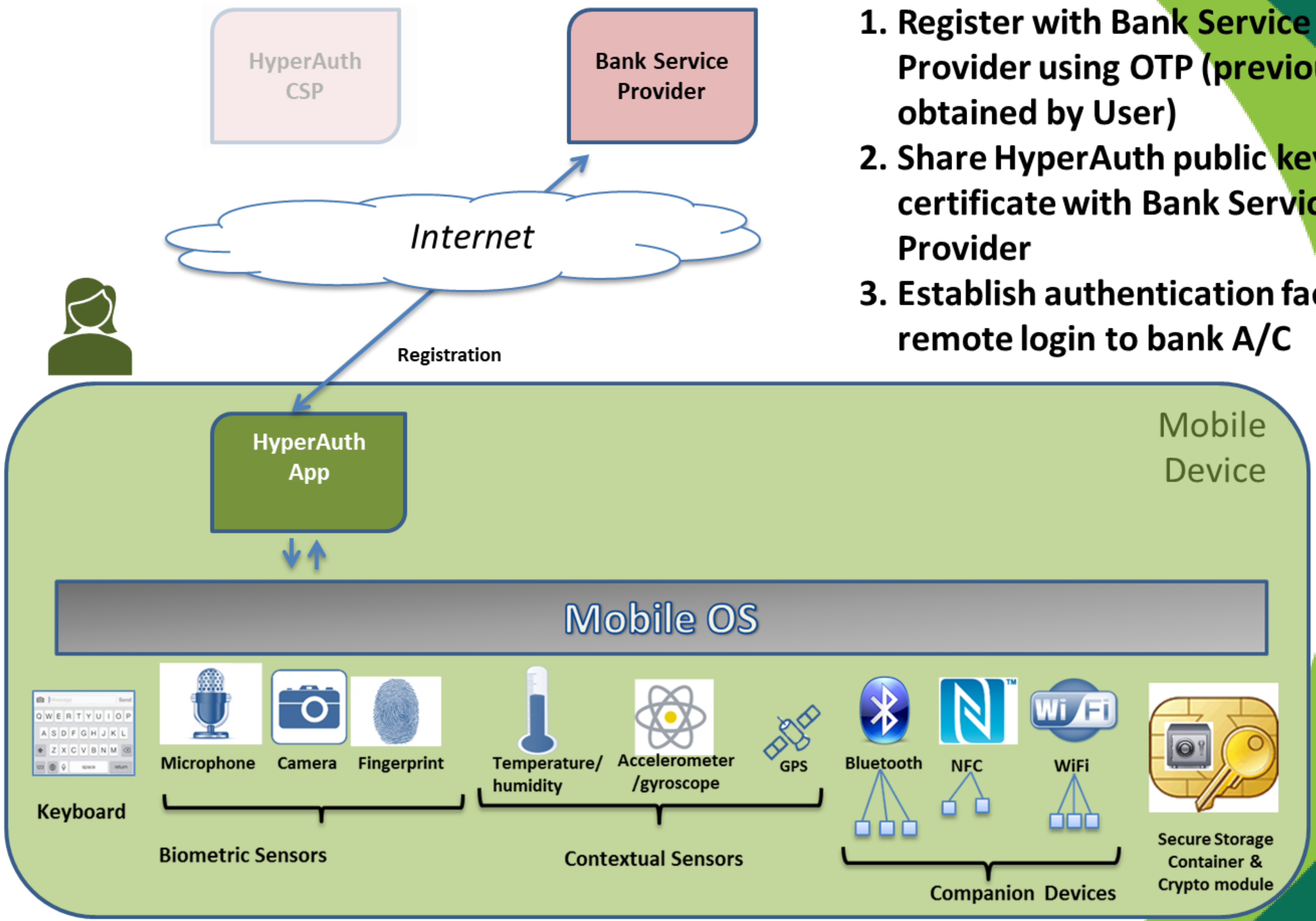
Mobile HyperAuth Model – Registration

- User goes to a Bank (or other service provider) and requests account access via mobile banking app
- Bank provides One Time Password (OTP) to pair User's account to mobile app
- User launches HyperAuth app and registers with Bank server using the OTP to connect to his/her account
- HyperAuth App shares HyperAuth public key and certificate with Bank server
- HyperAuth App interacts with User to establish a set of local authentication factors compatible with Bank server policy

Mobile HyperAuth Model - Registration

Registration

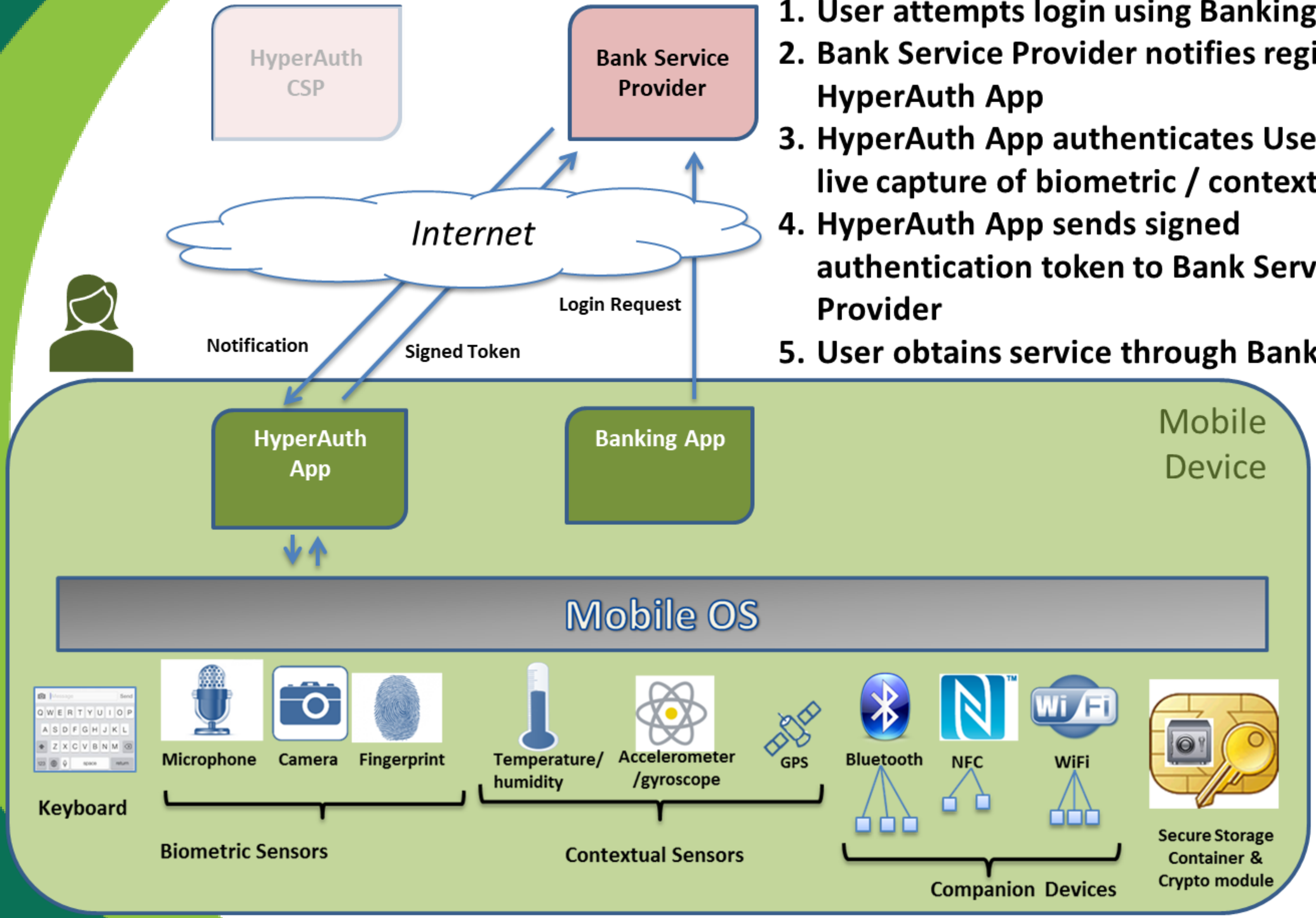
1. Register with Bank Service Provider using OTP (previously obtained by User)
2. Share HyperAuth public key and certificate with Bank Service Provider
3. Establish authentication factors for remote login to bank A/C



Mobile HyperAuth Model – Obtain Service

- User launches mobile banking app to login to Bank Server and obtain services
- Bank Server sends *mobile push notification* to User's registered HyperAuth app requesting authentication of User per Bank policy
- HyperAuth app launches as a result of the push notification and:
  - *Interacts with User to perform the required local authentication steps*
  - *Generates an Authentication Token indicating authentication result (success/failure)*
  - *Signs Authentication Token using HyperAuth private key and sends to Bank Server*
- Remote banking server:
  - *Validates signature on Authentication Token*
  - *Uses result as a basis for accepting the login from the mobile banking app*

Mobile HyperAuth Model – Obtain Service



Obtain Service

1. User attempts login using Banking App
2. Bank Service Provider notifies registered HyperAuth App
3. HyperAuth App authenticates User through live capture of biometric / contextual data
4. HyperAuth App sends signed authentication token to Bank Service Provider
5. User obtains service through Banking App

HyperAuth – Key Features and Benefits

- Key Features
  - *Authentication assurance model based on:*
    - Multiple authentication factors (such as biometrics, PIN/password, cryptographic keys, companion devices)
    - Multiple contextual factors (such as GPS location, time, agitation level of device, time since last use, known companion devices paired through NFC/Bluetooth/Wi-Fi)
  - *Local identity authentication on mobile device*
    - Delivery of authentication results to relying parties
- Benefits
  - *Improved security*
  - *Enhanced user experience*
  - *Improved privacy protection*
  - *Ability to access wide variety of applications at different levels of sensitivity*

THANK YOU

Questions/Comments

Contact Information

- Contact Info: Dr. Sarbari Gupta – Electrosoft
  - *Email: sarbari@electrosoft-inc.com;*
  - *Phone: 703-437-9451 ext 12*
  - *LinkedIn: http://www.linkedin.com/profile/view?id=8759633*

- Electrosoft
  - *Web: http://www.electrosoft-inc.com*
  - *LinkedIn: https://www.linkedin.com/company/electrosoft/*
  - *Twitter: https://twitter.com/Electrosoft_Inc*
  - *HQ: 1893 Metro Center Drive, Suite 228*
    Reston VA 22066