DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Mobile Derived Credentials

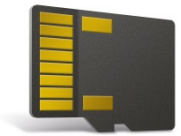
Purebred Information Brief

Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

Authentication on Mobile Devices
Before 2016

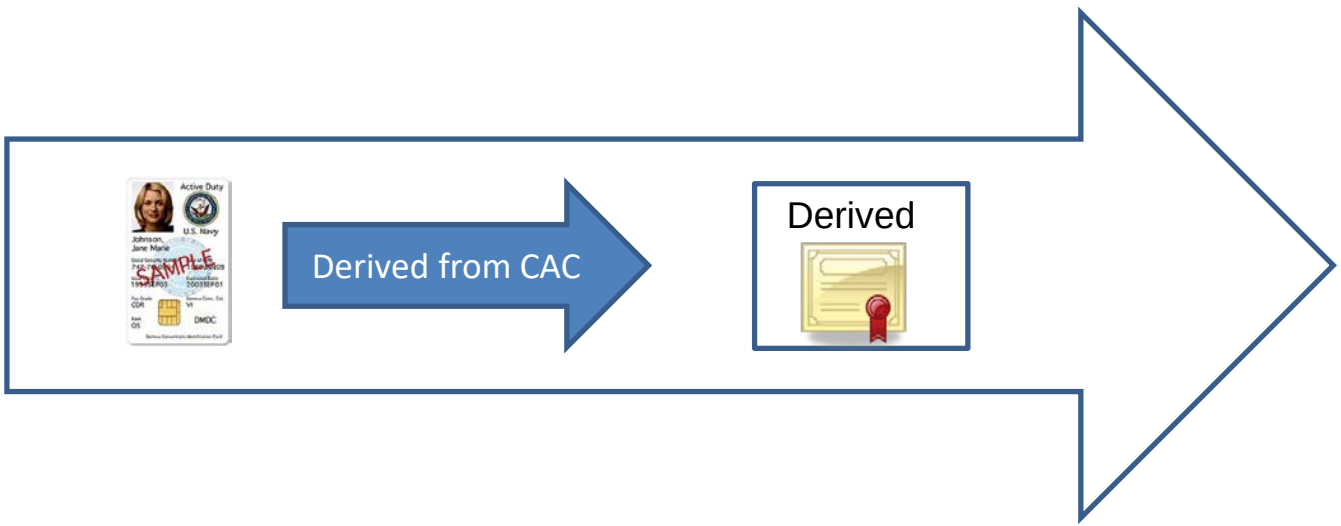
- **Same needs as on our office computers**
  - Sign, send, and encrypt email
  - Web authentication
- **Hardware challenge**
  - Connecting the smartphone to a smart card
- **Common Access Card (CAC) Sled issues**
  - Cost
  - Separate battery
  - User expectations
  - Restricts BYOD
- **microSD card HSM**
  - Limited use pilots
  - Requires specialized applications
  - Not all devices support SD cards



Source: Mark Norton, DoD CIO MILCOM 2014 Presentation

Authentication on Mobile Devices

2016+ Enter derived credentials issued to hardware-backed device native keystores



Authentication on Mobile Devices - DoD milestones

- **DoD CIO Mobile PKI Roadmap Memo – Sep 2014**
  - **Within 90 days, the DoD PKI PMO in conjunction with the DoD Public Key Enabling (PKE) and DoD PKI engineering teams shall design the approach for implementing an enterprise derived PKI credential issuance service for unclassified Commercial Mobile Devices (CMDs)**
- **NSA/DISA Industry Day – Oct 2015**
  - **Introduction of Purebred and its requirements to industry**
- **Purebred 1.0**
  - **Initial Production Capability - August 2016**
  - **Support for recovery of all user encryption keys – December 2016**

What is Purebred?

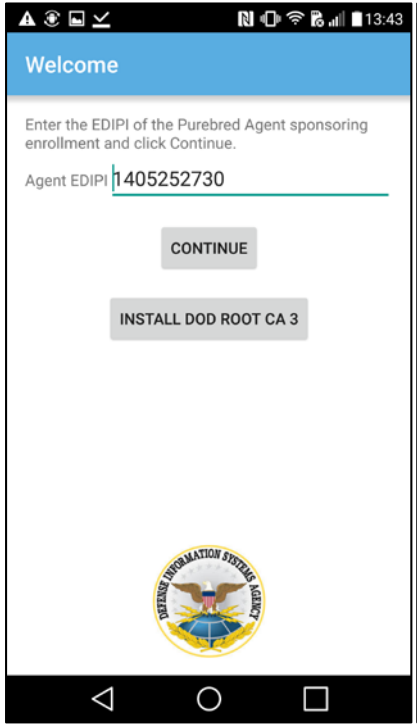
- **Purebred issued derived credentials enable users to utilize mobile signed and encrypted email and secure web browsing to CAC enabled websites without a reader or sled**
- **Purebred provides a secure over-the-air credentialing process through a series of one-time passwords and user demonstrated possession and usage of CAC**
- **Comprised of a key management server and set of apps for mobile devices**
  - **Certificate enrollment**
  - **Encryption key recovery capabilities**
- **Separates key management from device management**
  - **Key management maintains affinity with PKI and is used across the enterprise, i.e., there is one DoD PKI used by all**
  - **Device management can vary with operational scenario, i.e., different service/agency components can use different mobile device management (MDM) solutions**

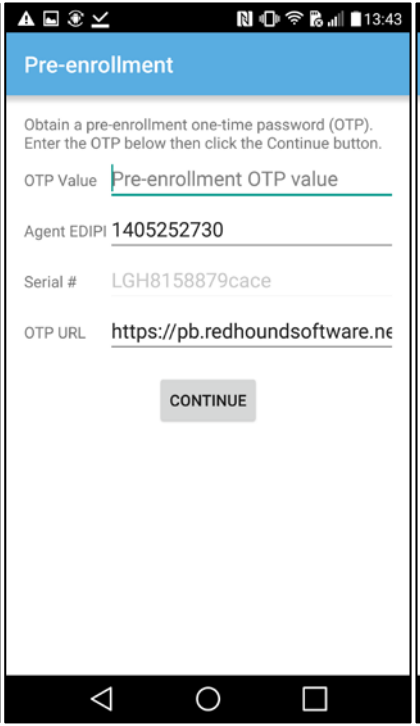
Purebred Supported Platforms

- **Supports four major mobile/tablet platforms & one USB platform**
  - **Apple iOS 8, iOS 9, iOS 10, iOS 11**
    - Managed and unmanaged
  - **Android 5, Android 6, Android 7**
    - Samsung Knox
    - Android for Work containers
    - Unmanaged
  - **Windows 10 and Windows 10 Anniversary Universal Windows Platform (UWP)***
    - Surface Pro 3 and Surface Pro 4
  - **Blackberry OS 10.3.3**
    - Work and personal
  - **Yubikey4**

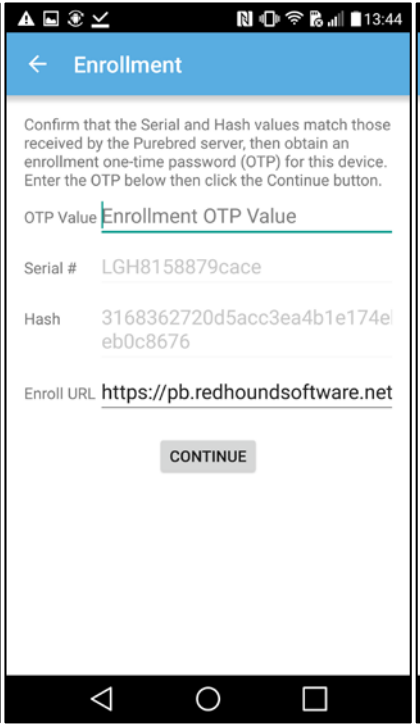
**Current ongoing DoD policy work with use of Virtual Smart Card and TPM technology*

Purebred Agent Views



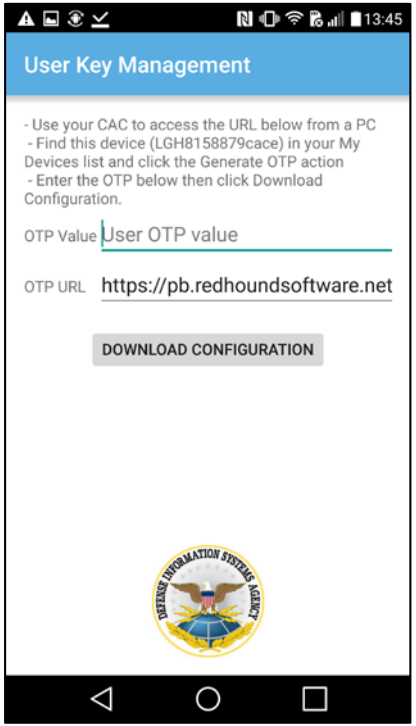


Info Collection/Phase 0/Vetting

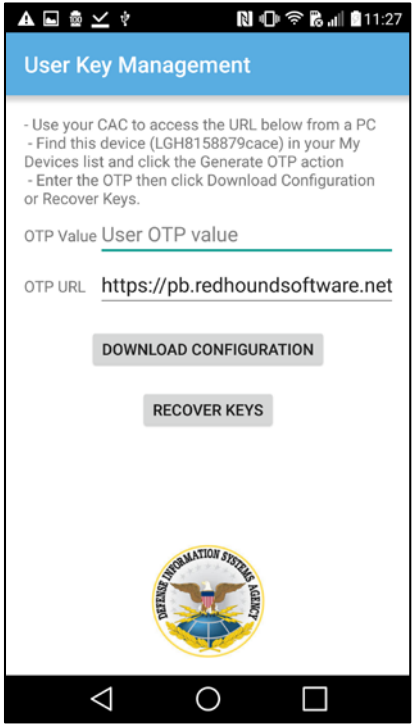


Phase 1/Phase 2/SCEP/Phase 3

Purebred User Views



User Key Management Update

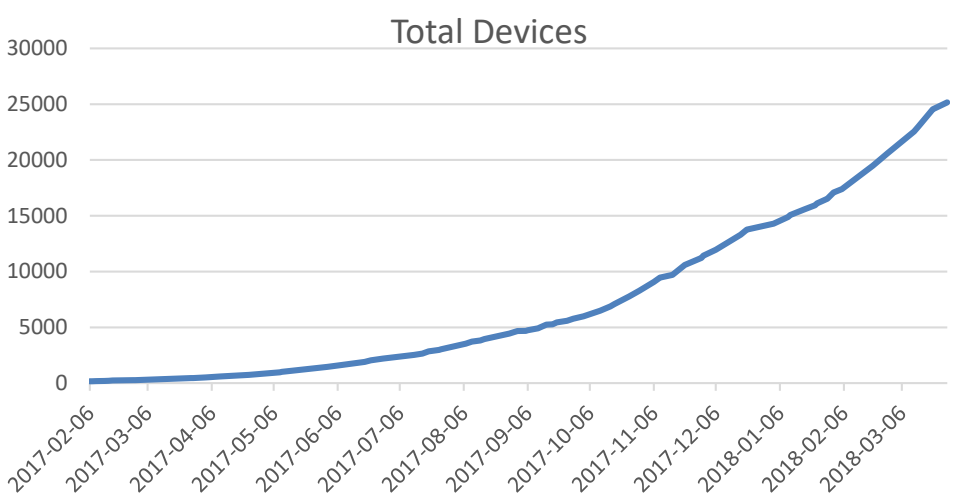


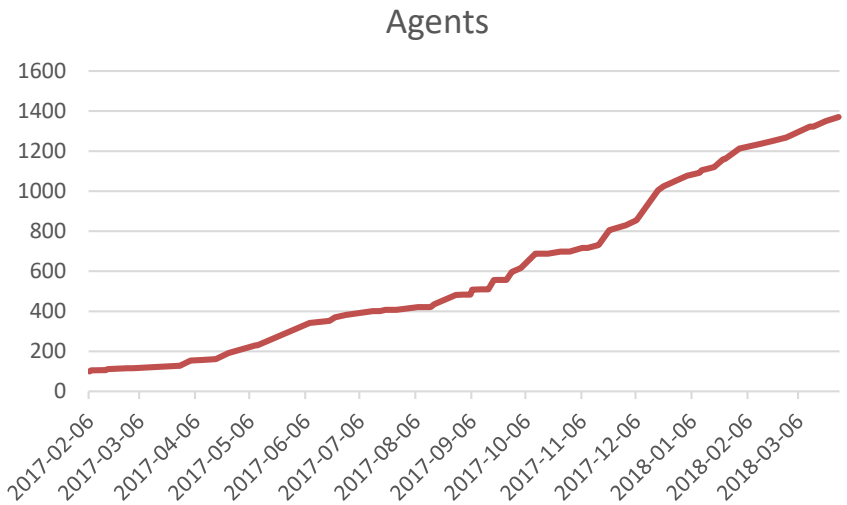
User Key Management Recovery

Purebred Status

- **Initial capability deployed Fall 2016**
- **Averaging 2000-3000 devices enrolling per month and 50-100 new agents trained and granted permission to enroll device to Purebred across all DoD mission partners**
- **Quarterly updates are deployed to provide new functionality and fixes**
- **Top Purebred server priorities:**
  - **1.4 - Attestation (hand off from Qualcomm contract, Samsung evaluation under way)**
  - **1.5 - Server/Certificate Authority high availability/service redundancy**
  - **2.0 – App and Server user interface improvement**
  - **Release independent major tasks:**
    - Purebred reachability from internet (whitelisting)
    - Agent nomination streamlining

Metrics (as of 28 Mar 2018)

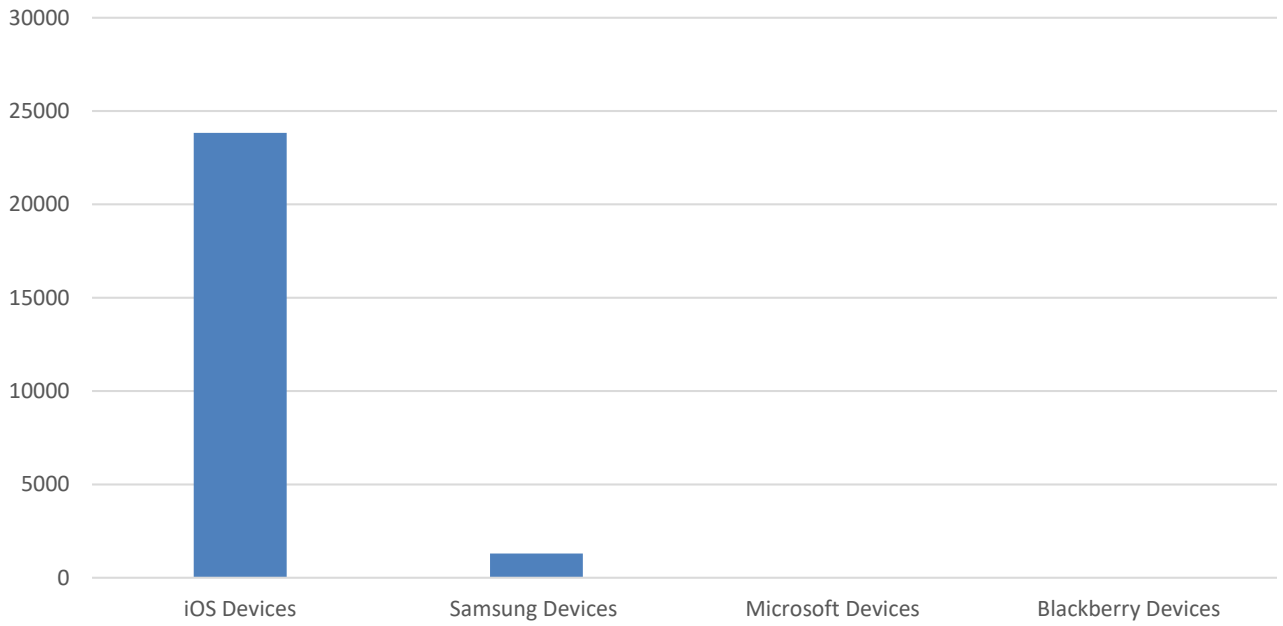




Devices: 25,160

Agents: 1,370

Devices by Type (as of 28 Mar 2018)



Purebred Mission Partner Cost

- **No direct cost – no additional fee for service**
  - **Purebred is a subcomponent of DoD Public Key Infrastructure (PKI)**
  - **Purebred credentialing is an optional free entitlement under DoD Mobility Unclassified Capability (DMUC) or can be offered by any other mobility/mobile device management (MDM) service**
- **In-direct costs to consider**
  - **Initial Integration Support**
    - Engineering and Test/Evaluation
    - Deploying PB registration app
    - Configuring MDM policies
    - Profile configuration management
    - General accreditation activities
  - **Purebred Agent Staffing (Sustainment)**
    - Agent nomination (what org/who will be agents?, is it in-scope if contractor?)
    - Enrollment support activities Training (free, provided by DISA)
    - User list management for migrations

Purebred Links

Information

- **Purebred Information - https://iase.disa.mil/pki-pke/Pages/purebred.aspx**
- **Purebred Agent Collaboration - https://www.milsuite.mil/book/groups/disa-purebred-agents-group**

rate us

take the 3-question survey
available on the AFCEA 365 app

visit us

DISA Booth # 443

follow us

Facebook/USDISA

Twitter/USDISA

www.disa.mil

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Assured Identity

Next Generation Authentication Information Brief

Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

Summary of Assured Identity Initiatives

- **Replace/augment the CAC for logical access**
- **Goals:**
  - Use a variety of factors/sensors to develop a patterns
  - Use pattern to create a continuously updated risk score
  - Securely compute locally on device

- **4 on-going initiatives:**
  - **Mobile Continuous Multifactor Authentication & Hardware Attestation Prototype**
    - Qualcomm Reference Devices with Snapdragon 845 Chipset
    - 3mo production pilot begins Oct 2018
  - **Behavior Based Privileged User Authentication Pilot**
    - Plurilock Biotracker measuring user's interaction with keyboard & mouse
    - 3mo production pilot on VDI started Jan 2018
  - **Rapid Innovation Fund CMFA Requirement for FY2018**
  - **Validating Identity with Wrist-worn Wearable pilot in April 2018**

Hardware-based Device Attestation and CMFA

- **Enhance Purebred issued credentials with hardware attestation**
- **Explore alternative mechanism to protecting credentials with CMFA versus single secret**
- **Exercise NIAP validated chipsets in commercially available phones**

System-on-Chip (SoC) Protection Profile Recommendations

- Identify requirements from MDFPP 3.0 and WLAN EP 1.0 that could be met by a SoC

So what?

- Demonstrate security functionality at integrated subsystem level to speed NIAP product evaluation of mobile device manufacturers handsets i.e. “Why does it take so long for the new Samsung phone to be available on DMUC?”

Hardware Attestation

- Use a mechanism to give device applications ability to provide cryptographically signed and encrypted data that describes the security state of the device
- Mechanism should include:

✓ HW, Firmware, TEE OS versions
✓ Android OS version and release
✓ Manufacturer and Device model
✓ Privacy-preserving Device ID
✓ Token signing at SoC HW Level
✓ Hash of secure boot verification key
✓ Trusted location

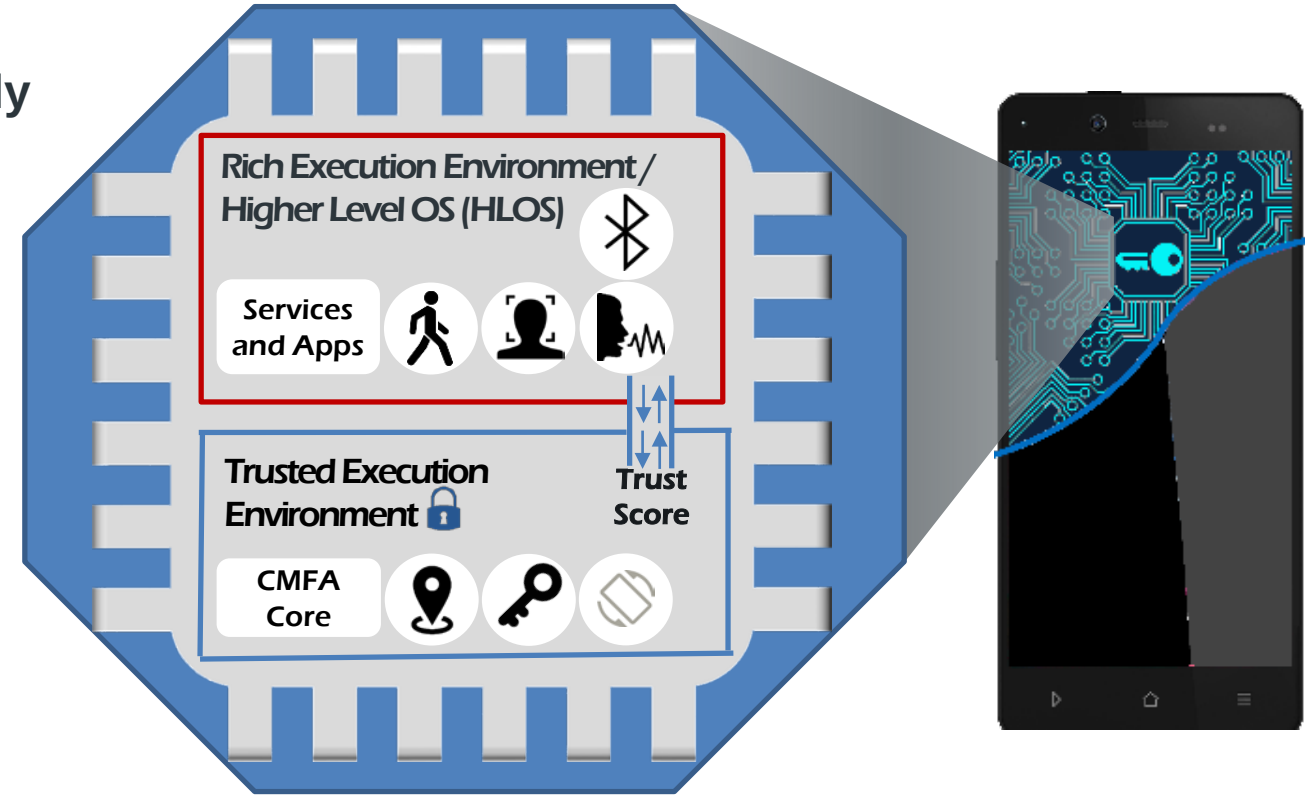
CMFA

- Design a system to maintain an authentication trust level at any given point in time to enable use to remain authenticated to their device so long as enough evidence
- Evidence should include gait, face and voice recognition
- System should factor power consumption of continuously polling from sensors

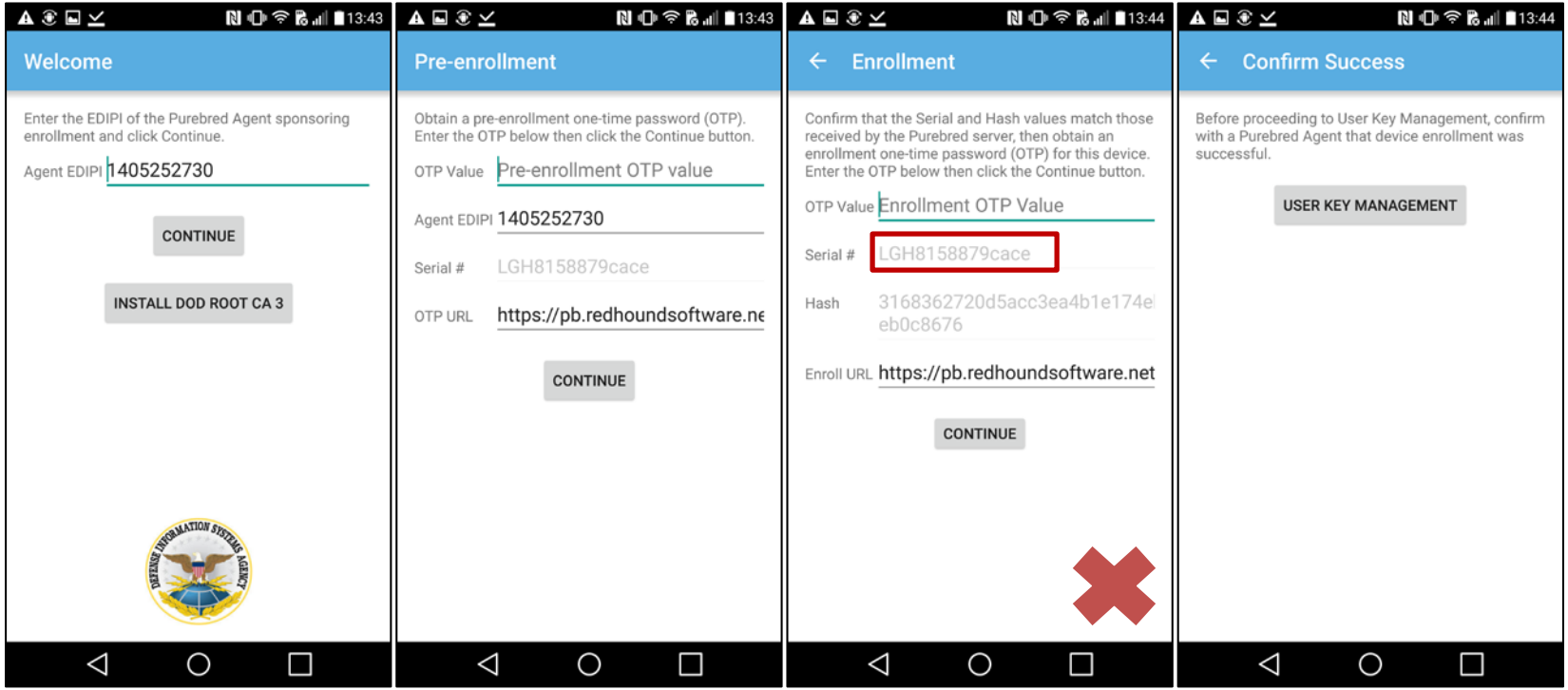
Utilizing the ARM TrustZone Architecture: TEE and REE

Increased Trust

Leverage commercially designed and manufactured cryptographic objects for signing sensor data



Improving Purebred Enrollment Process



Info Collection/Phase 0/Vetting

Phase 1/Phase 2/SCEP/Phase 3

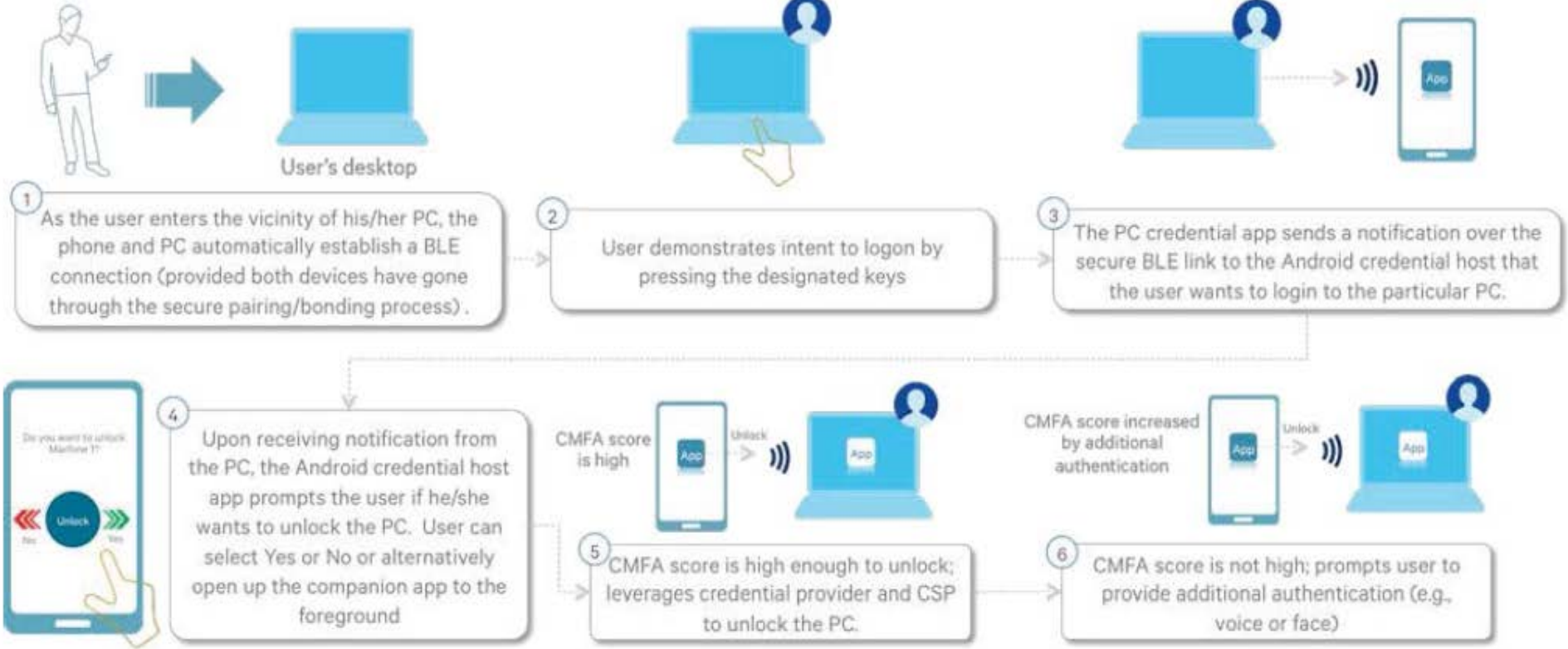
CMFA Verifiers

Verifier	Modality	Sensors
Face Recognition	Face	Camera
Voiceprint Identification	Voice	Microphone
Gait Recognition	User's pattern of walking	Accelerometer, Gyroscope

Contextual Information

Position	Person Location	GPS
WiFi	Person Location	WiFi
Bluetooth	Paired Device(s)	Bluetooth
Cell Tower ID	Person Location	Modem

Mobile cMFA Production Pilot



Conclusion

- Assured Identity is comprised of 4 on-going initiatives
- Aim to replace or augment the CAC for logical access and authentication
- Enhancing Purebred capability with issuing hardware policy OIDs and signed assertions of genuine device identifiers
- Align to a mobile-centric vision
- Sufficient authentication and assurance to facilitate single platform for multi-networks

rate us

take the 3-question survey
available on the AFCEA 365 app

visit us

DISA Booth # 443

follow us

Facebook/USDISA

Twitter/USDISA

www.disa.mil

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**