



PK-Enabling Mobile Devices with DoD PKI Credentials

DoD PKE
20-22 April 2016



Overarching Goals

- **Establish trust in device certificates used by the provisioning server to encrypt configuration data bound for a device**
- **Demonstrate possession and usage of existing smart card-based credentials**
- **Enable use of system APIs to exercise cryptographic keys without proliferation of certificates**
- **Decouple key management from device management**



Solution Fundamentals

- **Integrate into new DoD PKI enclave**
- **Source code available for review by the government**
- **Support centralized key generation**
- **Support distributed key generation**
- **Support use of recovered decryption keys**
- **Authenticate and authorize all parties involved in provisioning, i.e., devices, people, services**
- **Use NIST approved cryptographic algorithms and key sizes**
- **Support NIAP-validated or in-evaluation devices**



Solution Fundamentals (continued)

- **Demonstrate possession and control of CAC per NIST SP800-157**
- **Provision keys to work with system APIs**
- **Support system apps, e.g., mail, browser and VPN**
- **Support 3rd party and enterprise apps**
- **Avoid proliferation of certificates**
- **Facilitate automated revocation of software credentials for mobile devices when associated CAC is revoked, if necessary**



Solution Fundamentals (continued)

- **Provision keys independent of or in collaboration with MDM service**
- **Avoid manual side-loading of PKCS #12 files where possible**
- **Reduce touch labor**
 - **Avoid having user visit a provisioning facility**
- **Support modern certificate enrollment protocols (e.g., EST)**
- **Perform certificate validation per RFC 5280 using DoD trust anchors, revocation information providers, certificate policies, name constraints, etc.**
 - **RFC 5280 is the “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”**
 - **Defines certificate structure, CRL structure, certification path validation rules, etc.**



What is Purebred?

- **Key management server and set of apps for mobile devices**
- **Aims to facilitate separating key management from device management**
 - **Key management maintains affinity with PKI and is used across the enterprise**
 - **Device management can vary with operational scenario, e.g., service/agency**
- **Uses modified version of Apple's over-the-air profile delivery and configuration (OTA) protocol for all platforms**
 - **Modifications address device certificate vetting**



Purebred Status

- **Supports two phone platforms**
 - iOS and Android
- **Supports three table platforms**
 - iOS, Android and Microsoft Universal Windows Platform (UWP)
- **Supported versions**
 - iOS 8, iOS 9
 - Android 5 and Android 6
 - Windows 10 (on Surface Pro 3 and Surface Pro 4)
- **Common workflow across platforms**
 - Relatively minor differences in user experience per platform



Purebred Status (continued)

- **Supports system apps, enterprise apps and third-party apps**
 - **iOS**
 - System key chain receives keys shared via configuration profile
 - Enterprise apps (DISA signed) may use a common key chain access group allowing access to keys
 - Third-party apps may receive keys as PKCS #12 files via a document provider interface
 - **Android**
 - System key chain receives keys generated and imported during enrollment
 - **Microsoft**
 - Keys generated on TPM and associated with issued certificate in CAPI
 - Have not yet built for ARM (hence no support for Windows phones yet)
 - **Blackberry**
 - Works on PRIV now (Android-based)
 - Waiting on API mods to facilitate enrollment on BB10 devices

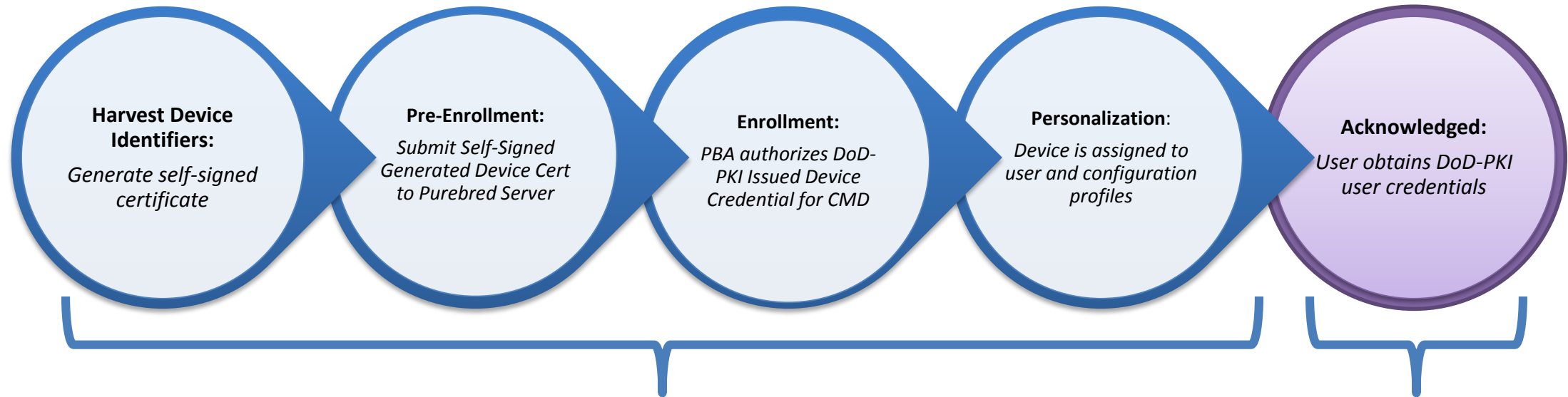


Workflow Characteristics

- **Purebred Agent provides EDIPI and two one-time password (OTP) values to enroll a device**
 - **First OTP associated the device with a fresh device-generated public key**
 - **Second OTP authorized device enrollment and provides attestation that the person performing the enrollment has visually vetted the device key**
- **Device provides one or two OTP values to provisions keys to a device**
 - **First OTP authorizes user enrollment (typically including one recovered key)**
 - **Second OTP authorizes recovery of additional decryption keys**
- **OTP values are obtained via mutually authenticated TLS sessions using PC-based browser and common access card (CAC)**
 - **OTP values generated per time-based OTP specification using an SP800-108 key derivation function (KDF) on a Thales hardware security module (HSM)**



Purebred Workflow



Stage 1: Obtaining a DoD-PKI Issued Device Credential

Role: Purebred Agent **OR** User or other PKI Sponsor* with remote Purebred Agent Support

Stage 2: Obtaining a DoD-PKI Issued User Credential

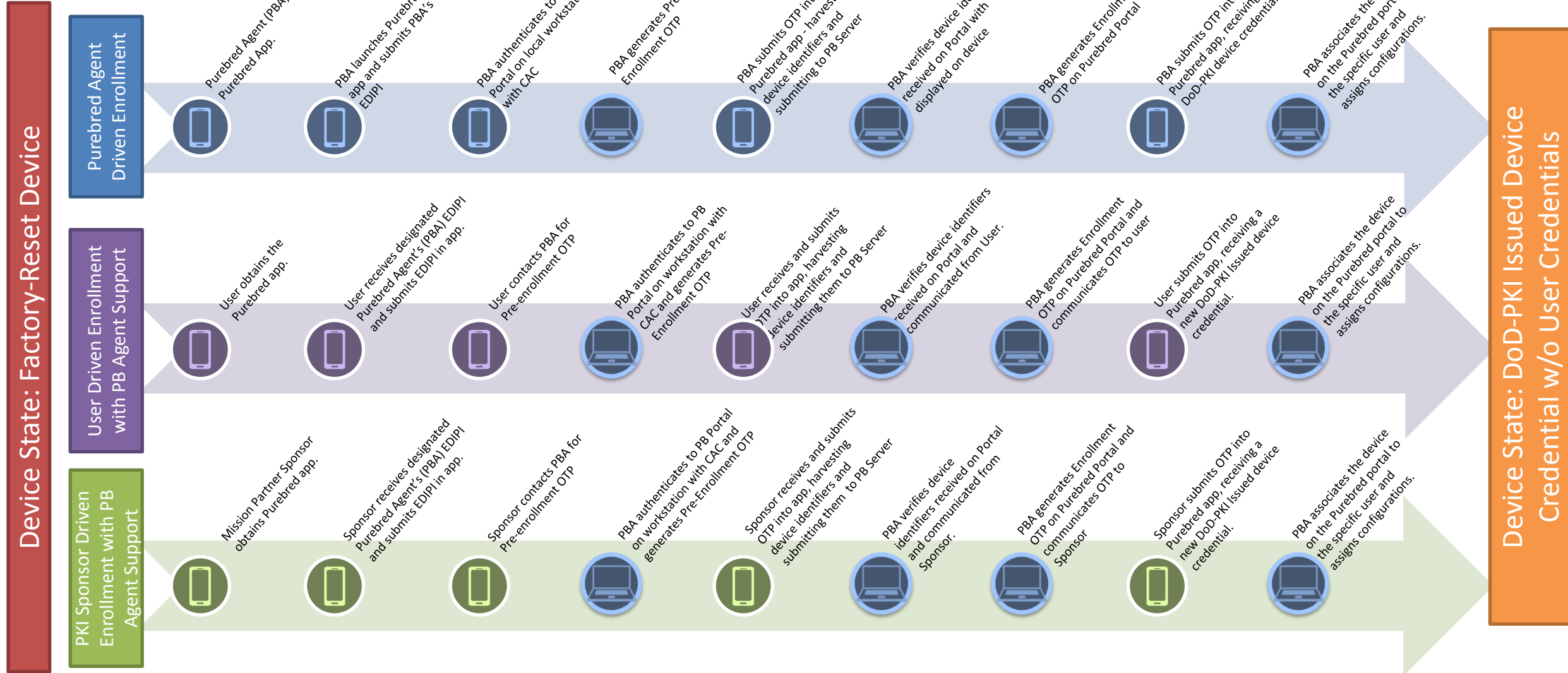
Role: User Only

* An example of another PKI Sponsor filling this role could be a Telephone Control Officer (TCO)



Purebred Workflow

Stage 1 - Device Enrollment

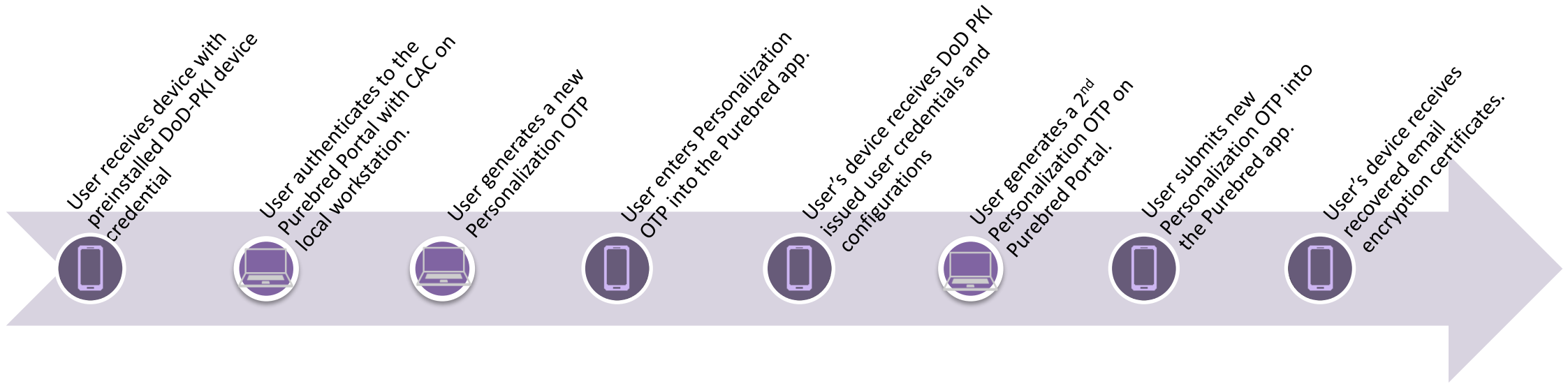




Purebred Workflow – User Enrollment

Stage 2 - Obtaining User Credentials

Device State: DoD-PKI Issued Device Credential w/o User Credentials



Device State: Device with DoD-PKI issued User Credentials



Using the Key Sharing Extension

- **Developers incorporate code similar to the following sample code into their application to allow users to view the Purebred Document Picker View to import keys:**

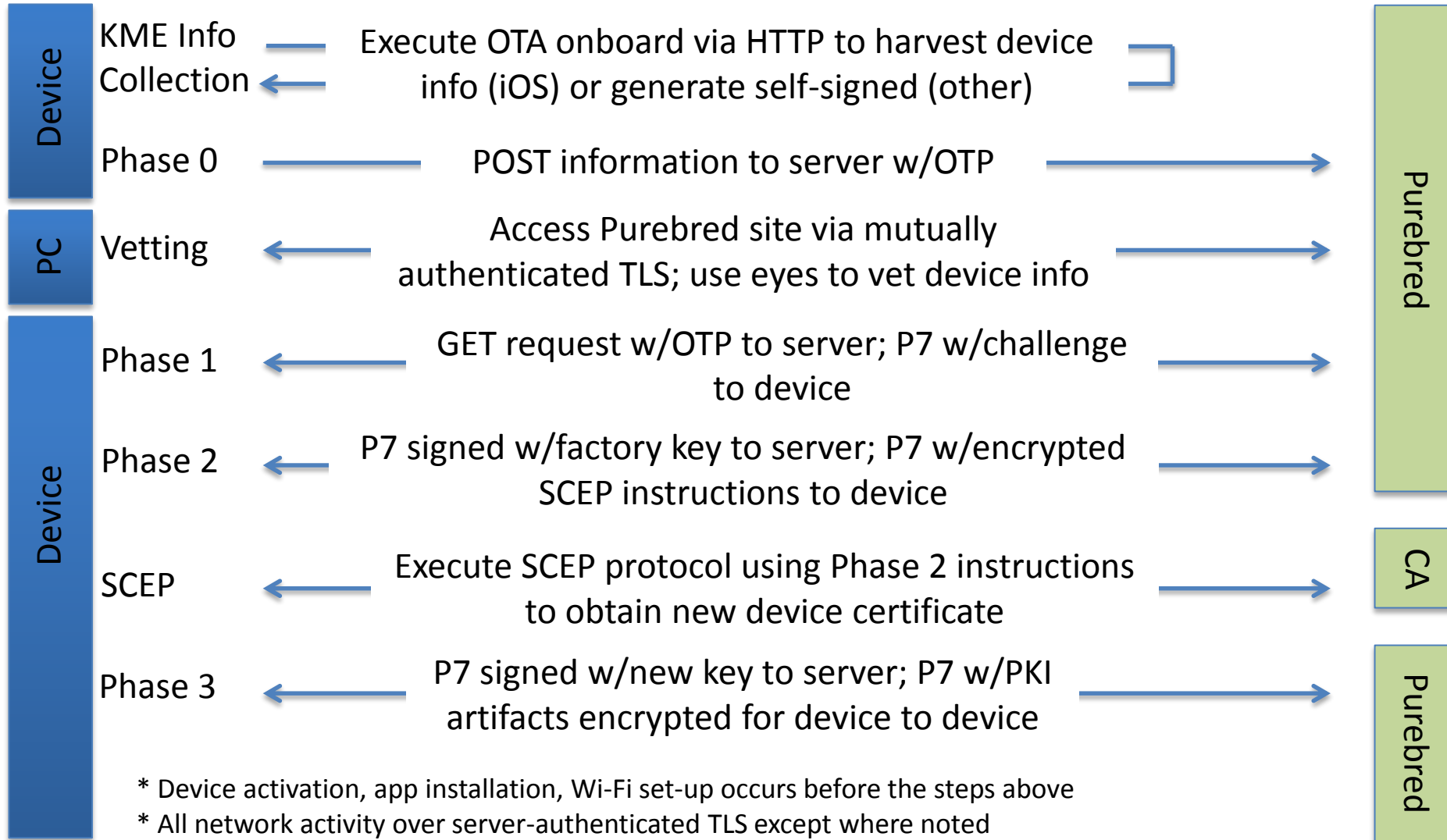
```
UIDocumentPickerViewController *documentPicker =  
    [[UIDocumentPickerViewController alloc]  
     initWithDocumentTypes:@[@"com.rsa.pkcs-12"]  
     inMode:UIDocumentPickerModeOpen];  
  
documentPicker.delegate = self;  
documentPicker.modalPresentationStyle = UIModalPresentationFormSheet;  
[self presentViewController:documentPicker  
    animated:YES completion:nil];
```

- **Once imported and installed into the developer keychain, developers can build applications to enable use of these keys.**

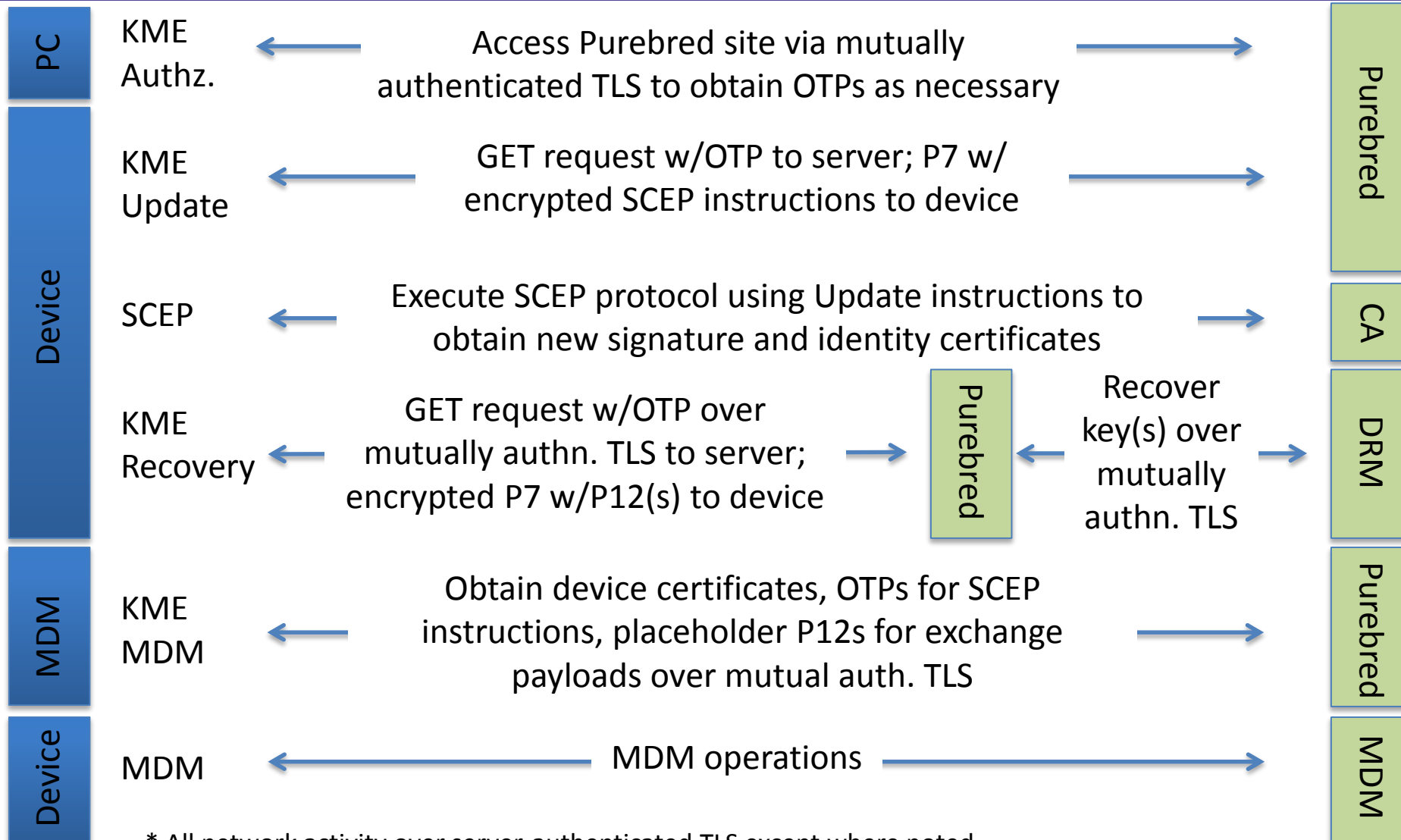


OTA KME

- **Over-the-air Profile Delivery and Configuration Protocol w/ Key Management Extensions (OTA KME)**
 - **Collection of provisioning practices, device-facing web interfaces and MDM-facing web interfaces**
- **OTA KME aims to use the OTA protocol while establishing trust in device certificates and avoiding having users visit a provisioning facility**
 - **Purebred is the first implementation of OTA KME**



* Device activation, app installation, Wi-Fi set-up occurs before the steps above
 * All network activity over server-authenticated TLS except where noted
 * OTP generation not shown (mutual authn. TLS from PC to Purebred)



* All network activity over server-authenticated TLS except where noted




Purebred Agent Views

Begin Enrollment

Enter the EDIPI of the Purebred Agent sponsoring enrollment and click Continue.

Agent EDIPI EDIPI of Purebred Agent

CONTINUE



Pre-enroll Device

Obtain a pre-enrollment one-time password (OTP). Enter the OTP below then click the Continue button.

OTP URL https://purebred.example.com

UUID b7d2c494-6503-4f4f-8686-19bct

Serial # LGH8158879cace

IMEI 359872060393815

OTP Value Pre-enrollment OTP value

CONTINUE

Enroll Device

Confirm that the Serial and Hash values match those received by the Purebred server, then obtain an enrollment one-time password (OTP) for this device. Enter the OTP below then click the Continue button.

Enroll URL https://purebred.example.com

Serial # LGH8158879cace

Hash f32447e27a68c06554966b34871fdd53512

OTP Value Enrollment OTP Value

CONTINUE

Confirm Success

Before proceeding to User Key Management, confirm with a Purebred Agent that device enrollment was successful.

USER KEY MANAGEMENT



Purebred User Views

The image displays two side-by-side screenshots of a mobile application interface titled "User Key Management". Both screens show the same instructions and input fields, but differ in the available actions.

Left Screenshot (Time: 16:07):

- Title:** User Key Management
- Instructions:**
 - Use your common access card (CAC) to access the URL below from a PC
 - Find this device (LGH8158879cace) in your My Devices list and click the Generate OTP action
 - Enter the OTP below then click Download Configuration.
- OTP URL:**
- OTP Value:**
- Action:** A grey button labeled "DOWNLOAD CONFIGURATION".

Right Screenshot (Time: 16:09):

- Title:** User Key Management
- Instructions:**
 - Use your common access card (CAC) to access the URL below from a PC
 - Find this device (LGH8158879cace) in your My Devices list and click the Generate OTP action
 - Enter the OTP below then click Download Configuration or Recover Keys.
- OTP URL:**
- OTP Value:**
- Action:** A grey button labeled "RECOVER KEYS".

Both screenshots feature the Department of Defense Information Systems Agency (DISA) logo at the bottom center and standard Android navigation icons at the very bottom.



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION