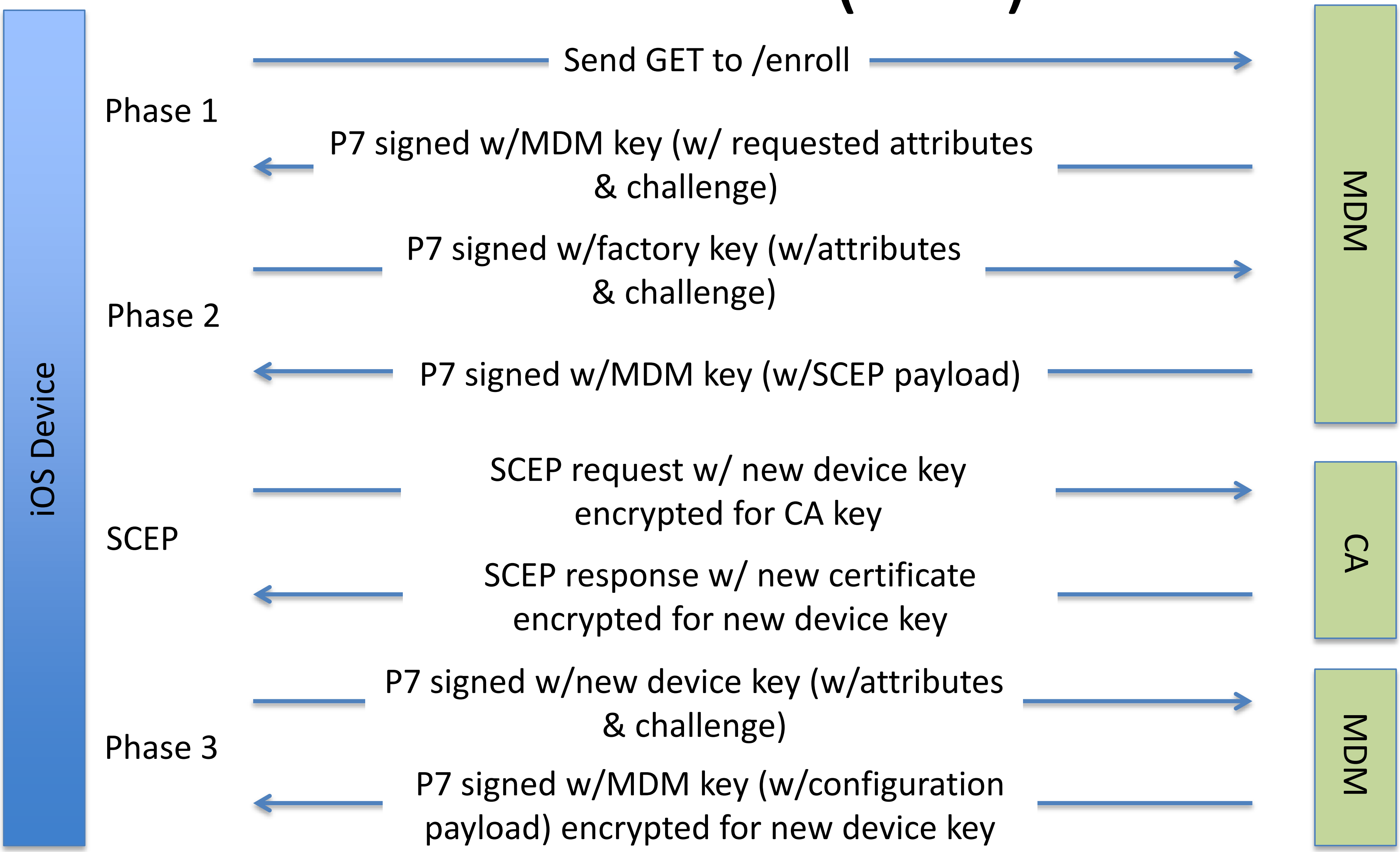
Purebred Overview

Background

- Mobile devices are presently enrolled using manual techniques
  - Keys are generated on a PC and are manually installed
- A more automated approach is desired for scalability and security
  - Purebred aims to address this desire
  - Initially focused on iOS devices only

Basic over-the-air (OTA) Flow



iOS Device

MDM

CA

MDM

Phase 1

Send GET to /enroll

P7 signed w/MDM key (w/ requested attributes & challenge)

Phase 2

P7 signed w/factory key (w/attributes & challenge)

P7 signed w/MDM key (w/SCEP payload)

SCEP

SCEP request w/ new device key encrypted for CA key

SCEP response w/ new certificate encrypted for new device key

Phase 3

P7 signed w/new device key (w/attributes & challenge)

P7 signed w/MDM key (w/configuration payload) encrypted for new device key

Some problems with automated iOS provisioning

- OTA protocol relies on server-authenticated TLS validated using native trust anchor (TA) store (inviting man-in-the-middle attacks)
- Device certificates do not contain any identifiers typically associated with or observable on a device (i.e., no serial number or IMEI)
- Devices use 1024-bit RSA keys for authentication during enrollment
- Device keys and certificates may change during iOS updates
  - No details are available regarding how issuance of these certificates is secured (despite a request for such details from Apple)

Some problems with automated iOS provisioning (continued)

- Keys generated on mobile devices are of unknown quality
- The over-the-air (OTA) protocol uses SCEP to provision newly generated keys
  - Red Hat CA SCEP interface is incomplete and not scalable
- PKCS #12 passwords are relatively broadly shared when using a mobile device management (MDM) system
  - Decryption private key typically conveyed where certificate would suffice
- Poor TA management practices

Primary aims of Purebred effort

- Demonstrate device registration, personalization and enrollment with DoD PKI using more automated techniques
- Demonstrate key management independent of and in collaboration with an MDM system
- Demonstrate centralized and distributed key generation
- Demonstrate improved one-time password practices in a Red Hat CA SCEP implementation

Terminology

- Pre-entry: device information is entered into the Purebred or MDM system prior to beginning device registration or enrollment
- Pre-enrollment: device information (including vendor-issued device certificate) is entered into Purebred
- Enrollment: Phase 1 and 2 of the OTA protocol are performed to install a DoD-issued credential for authentication and encryption purposes during Phase 3

Terminology (continued)

- Personalization: an association between the device user’s EDIPI and one or more device identifiers is established
- Registration: phase 3 of the OTA protocol is performed (possibly for a second time) to install one or more credentials issued to the device user

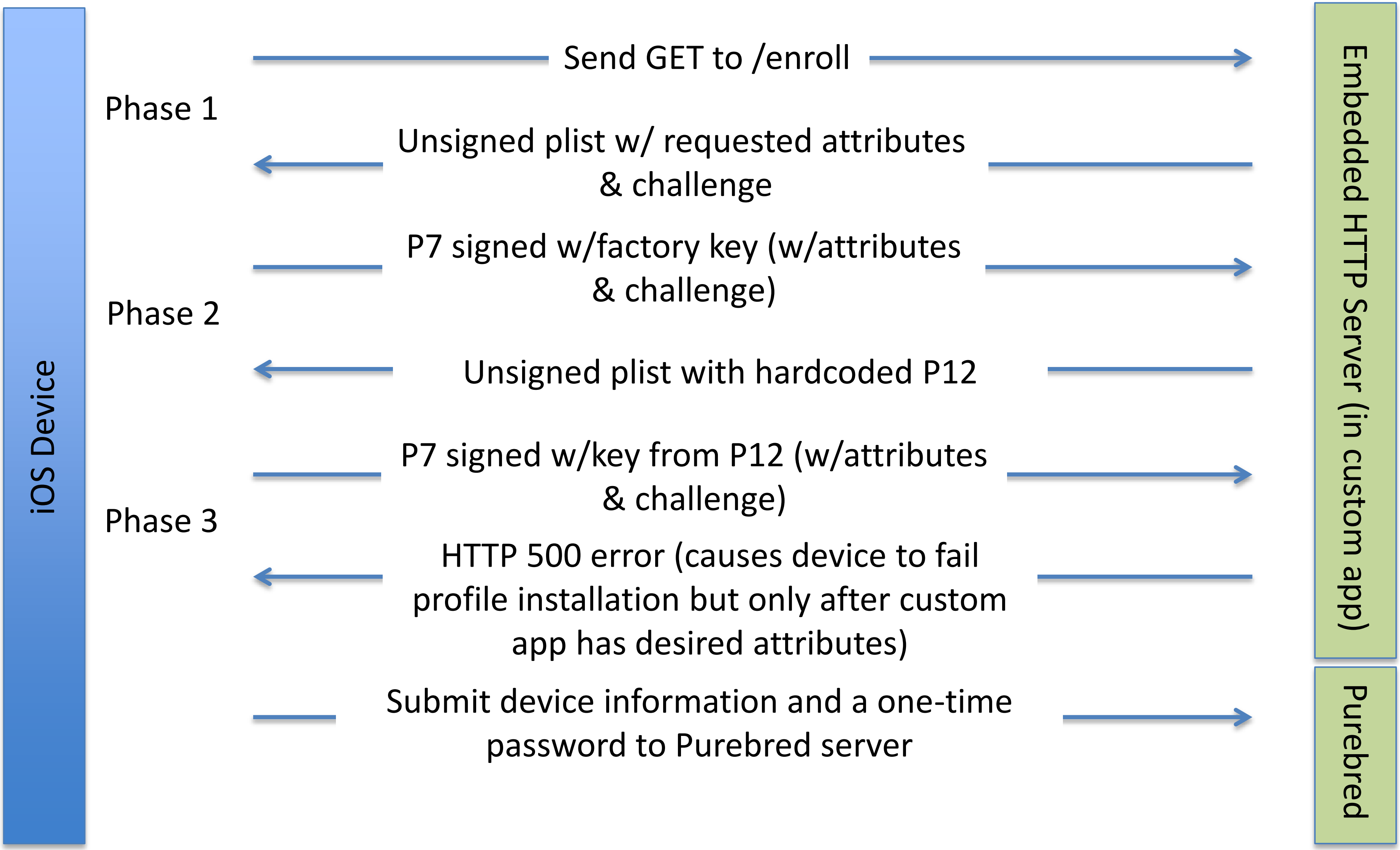
Primary Purebred Components

- Custom iOS application
  - Used to harvest information not readily visible on the device (like device certificate)
- Purebred server
  - Used to manage devices to which keys will be provisioned
- SCEP servlet and OTP plug-in for Red Hat CA
  - More complete SCEP implementation with support for improved one-time password (OTP) utilization

Phase 0

- The OTA protocol defines three phases that transition a device from having an Apple-issued device certificate to having a enterprise-issued device certificate and a set of configuration payloads
- Unfortunately, the OTA protocol and the Apple-issued device certificate do not provide sufficient authentication of devices for enrollment with the DoD PKI to proceed without performing some additional steps
  - These additional steps are called “Phase 0” in Purebred, to indicate the steps are performed before the three phases of the OTA protocol
  - Two flavors are considered
    - Factory-to-enterprise-to-user
    - Factory-to-user

Phase 0 Flow



iOS Device

Embedded HTTP Server (in custom app)

Purebred

Phase 1

Send GET to /enroll

Unsigned plist w/ requested attributes & challenge

Phase 2

P7 signed w/factory key (w/attributes & challenge)

Unsigned plist with hardcoded P12

Phase 3

P7 signed w/key from P12 (w/attributes & challenge)

HTTP 500 error (causes device to fail profile installation but only after custom app has desired attributes)

Submit device information and a one-time password to Purebred server

Factory-to-enterprise-to-user

- Device information is entered into the site
  - Possibly by administrator configuring the device, possibly during some pre-entry activity
- Custom application is installed on device
- Administrator visits Purebred site via mutually authenticated TLS session to obtain a one-time password (OTP)
- OTP is entered into the custom application
- Custom application is used to harvest device information
  - Does so by running incomplete OTA cycle against embedded HTTP server (Phase 0)
- Device information and OTP is submitted to the Purebred server via server-authenticated HTTPS

Factory-to-enterprise-to-user (cont.)

- Administrator returns to the Purebred web interface to confirm the device information
- Custom application is used to start the OTA protocol
  - A DoD-issued device certificate is installed along with placeholder/expired configuration profile
- Device is placed in storage
- Later, the administrator assigns the device to a user in the Purebred web interface and gives the device to the user
- User clicks Update Profile on the device to obtain personalized settings (including DoD-issued keys)

Factory-to-user

- Similar steps with user interacting with the Purebred web site via mutually authenticated TLS session to confirm device information
  - Two different one-time passwords are used (one generated using EDIPI of the user and one generated using the UUID harvested by the custom application)
  - No need for placeholder configuration profile

Phases 1-3

- As defined in OTA protocol specification
- Will support use of SCEP for device-based key generation or P12 for centralized key generation
- Will be capable of providing configuration profiles (Exchange and VPN) that use PKI credentials
  - Other configuration profiles types will be delegated to MDM server, at least initially
- Not integrated with MDM, but will provide complimentary services to enable preparation of configuration profiles using some Purebred-generated artifacts
  - OTP values for SCEP and “bogus” P12 files to bootstrap SMIME encryption capabilities with pre-placed key

Questions?

Pure Breed Applicability Note

The Pure Breed approach is the first look at developing an OTA PKI provisioning capability. The Simple Certificate Enrollment Protocol (SCEP) approach utilized was in response to the capability of iOS at this time since that was the mobile device utilized in the DISA soft cert pilot. Each OS approach will require an analysis in determining the hardware and protocols that are available for use as well as the security and processes required to implement an OTA PKI provisioning capability for that particular OS. But the overall approach contained within Pure Breed document is the core of the concept in developing an OTA PKI provisioning capability.

The goal is to eventually get to a common protocol across the various mobile OS such as the NSA preferred Enrollment over Secure Transport (EST) or a hardened SCEP approach are two such examples. But in the near term a different interface process may be required for each mobile OS, but the core provisioning system and the general approach remains the same for each mobile OS. It will just be the outward facing interface process may end up being unique for each mobile OS for now until a common protocol is supported between the various mobile OS by the multiple mobile device OEMs .

For vendors, academia, etc.

This is being distributed for your information at this time based on the list of vendors who expressed interest in understanding our approach to OTA PKI Provisioning. This is not a solicitation nor is it a request for white papers on this topic but strictly for information purposes only. These documents were presented at the recent DISA PKI provisioning TIM and they may be forwarded. Comments are accepted on these documents, but DISA will not entertain or reply to any questions submitted with any comments that may be provided in response to this information. This is due to the fact that the current workload involved in this effort does not provide the luxury to respond now or in the near future. Also in fairness, it will not be feasible to distribute answers to all that have received this email or will be forwarded this information in the future. At some point, an RFI may be required and if so, then the FAR rules of acquisition will apply and will be executed appropriately.

For Federal Agencies and DoD Components.

Questions may be submitted, but no guarantee is provided on the timeliness of reply as noted above due to workload and priorities. But an effort will be made to get back to you to provide a reasonable response short of requiring a full up briefing on our efforts. As noted above, this is mainly for informational purposes to make your Agency or DoD Component aware of current DISA efforts.

Greg Youst
DISA Chief Mobility Engineer
301-225-9501
Gregory.f.youst.civ@mail.mil