Privacy Policy for the Purebred Registration app for Apple iOS

The Purebred Registration for iOS app is a component of the Purebred system developed by the Defense Information Systems Agency (DISA) to facilitate issuance of derived credentials to people who have been issued a Common Access Card (CAC). This document provides a privacy policy for use of the app in conjunction with the overall derived credential issuance system.

What User Data Collected

The Purebred Registration app directly collects very little personally identifiable information (PII) (see DOD 5400.11-r). The lone instance of PII solicited and stored by the app is the Electronic Data Interchange Personal Identifier (EDIPI) of a cooperating Purebred Agent. Additionally, the following information is collected by the app directly:

- Device serial number
- Operating system version
- Device type
- Device International Mobile Equipment Identifier (IMEI)
- Device Universal Unique Identifier (UUID)
- Device Unique Device Identifier (UDID)
- App version
- Time and time zone information
- One-time password (OTP) values

However, a variety of PII is sent to and through the Purebred Registration app as a consequence of user interactions with a Purebred Agent, the Purebred portal, a certification authority (CA) and the app. Personal data that transits the app and may be stored by the app includes:

- First name
- Last name
- Email address(es)
- Device user's EDIPI
- Recovered encryption certificates and corresponding private keys
- Freshly issued authentication and digital signature certificates and corresponding private keys

How User Data Is Collected

The Purebred Registration app writes diagnostic information to a log file. This logfile includes timestamps that can be used in concert with other information to determine the time zone configured on the device at the time an action was taken (note, the time zone configured on the device may have no relation to the user's actual location). Information may be logged at any point during app use, including upon launching the app or tapping any user interface elements within the app.

The Purebred Agent's EDIPI is obtained by the device user from the Purebred Agent. The value is entered into a text box on the first view of the app.

In some cases (configurable via managed app config values delivered by a Mobile Device Management system), various device information is collected via execution of the Over-the-air Profile Delivery and Configuration protocol. This information includes: device serial number, operating system version, device type, device IMEI, device UUID and device UDID. Operating system and device type information is also read via the UIDevice class.

A series of one-time password values are entered into the app during use. The first two of these are obtained from a Purebred Agent. The remaining OTP values are obtained from the portal by the device user.

Additional information is read from configuration profiles sent from the portal that provided the OTP values (the URL of the portal is visible in the Settings app). At present, the portal is only accessible from devices connected to the Department of Defense (DOD) Non-classified Internet Protocol Router Network (NIPRNet). OTP values are obtained via portal interfaces available only via NIPRNet. While any payload in the configuration profile reference may be delivered to the device (based on administrative choices), the primary payloads in use are: com.apple.security.scep, com.apple.security.pkcs12 and com.apple.eas.account.

How User Data Is Used

Diagnostic information collected by the app may be accessed in either of two ways: tapping anywhere in the app five times quickly, accessing the log file via iTunes File Share. When the tap mechanism is used, logs are displayed via Safari, which interacts with HTTP server embedded in the app.

The Purebred Agent's EDIPI is provided to the portal indicated in the Settings app during Pre-enrollment and Enrollment phases of use. This value is used by the portal to verify OTP values provided to the device user by the Purebred Agent. At present, the lifespan of the OTP values is limited to 180 seconds. The Enrollment OTP and User Key Management OTP values are context-specific, i.e., may only be redeemed relative to a given Purebred Agent/device or device user/device context.

Device information (including serial number, IMEI, UDID, UUID, operating system version and device type) are provided to the portal during pre-enrollment. Operating system version is also provided during user key management. The portal stores this information to inform policy decisions regarding whether to release payloads to a given device and to provide means of identifying the device in cooperating Mobile Device Management (MDM) systems. Where collected, the device serial number is encoded into a Simple Certificate Enrollment Protocol (SCEP) request and sent to a cooperating DOD Certification Authority (CA) to obtain a fresh certificate for the device. The issued certificate is provided to the portal during Pre-enrollment and subsequently used by the portal to encrypt confiration profiles during Enrollment and User Key Management phases of use. Where device serial number is not collected, a random value is generated by the app and used in place of the actual serial number. The certificate and corresponding private key are stored in the app's area of the system key chain. The certificate is additionally stored in the app's defaults database.

PII information is encoded into SCEP requests and sent to a cooperating DOD CA to obtain fresh derived credentials for the user. The issued certificate(s) and corresponding private key(s) are stored in the app's area of the system key chain. These certificates and private keys may be packaged and shared with the operating system via an HTTP server embedded in the app, subject to managed app config values passed to the device from an MDM system and subject to user acceptance of the resulting prompts. These certificates and private keys may be packaged and shared with third party apps via a document/provider interface, subject to Restrictions payloads applied by an MDM system and subject to user acceptance of the resulting prompts. The certificates and keys may be used for a variety of purposes, including mutually authenticated TLS, email signing, email encryption, email decryption, document signing, etc.

Though there is no sign-in required with the app, the provisioning of OTP value requires Purebred Agents and device users to access the portal using their CAC via mutually authenticated TLS.

Confirm Recipients of User Data are Compliant with Apple's Policies

To account for lack of a system-wide key chain in some iOS versions, the Purebred app features a document/provider interface to share certificates and private keys as Public Key Cryptographic Standard (PKCS) 12 files with third party apps that invoke the system's document/provider Application Programming Interfaces (APIs) using one or more of the uniform type identifiers listed at https://github.com/purebred. Use of the Purebred app is anticipated to be limited to apps managed by an MDM system. The MDM system should manage the installed apps to insure certificates and private keys are not shared with apps that are not compliant with Apple or DOD policy.

Beginning with the v2.x release of the Purebred app when used on iOS 14 and later, the app features a persistent token extension that allows apps that declare the com.apple.token key chain entitlement to exercise keys via an extension exposed by the Purebred app. As above, MDM restrictions are anticipated to limit apps that may exercise this feature.

Data Retention Policies

The Purebred app can be uninstalled subject to any MDM limitations. To clear any key chain items associated with the app, the user may browse to the Settings app and enable the Reset button on the User Key Management view. When clicked, this will delete items placed in the app's view of the system key chain by the user. Failure to reset the app state prior to uninstalling the app may leave keys in the system key chain, subject to operating system protections and key chain hygiene procedures.

Configuration profiles shared with the system can be deleted via the Settings app by navigating to the General->Profile & Device Management view then selecting and deleting any Purebred profile. Key chain hygiene will be managed by the operating system in these cases.

Deleting materials from third-party apps that received PKCS 12 files from the Purebred app is performed in accord with instructions accompanying the third-party app.

User or device information on the Purebred portal may only be deleted via cooperation of a Purebred Agent. Information generated and/or retained by the DOD PKI is managed in accord with the United States Department of Defense X.509 Certificate Policy.

Information pertaining to retention and recovery of the user's encryption credentials is covered in the DD-2842 subscriber agreement signed upon CAC issuance. Additional data retention information can be found in the Privacy Impact Assessment (PIA) for the DOD Public Key Infrastructure (PKI).

Privacy of Children

The Purebred Registration app is used to provision derived credentials for persons who possess and can use a Common Access Card (CAC), termed "subscribers" in the DOD Certificate Policy (CP) [DOD CP]. Furthermore, association of a device with a person is performed by a trained Purebred Agent. Persons under the age of 18 are not anticipated to have been issued a CAC nor have been associated with a device by a Purebred Agent. The Purebred app will not knowingly collect or use personal information from anyone under the age of 18.

Expectation of Privacy

When the Purebred app is launched the following language is displayed to the user. Similar language is displayed when accessing the portal and when accessing the network on which the portal is hosted.

```
You are accessing a U.S. Government information system. This information
system, including all related equipment, networks, and network devices, is
provided for U.S. Government-authorized use only. Unauthorized or improper
use of this system is prohibited, and may result in civil and criminal
penalties, or administrative disciplinary action. The communications and
data stored or transiting this system may be, for any lawful Government
purpose, monitored, recorded, and subject to audit or investigation. By
using this system, you understand and consent to such terms.
```

Bibliography

Reference	Title
CPR	Configuration Profile Reference
DD-2842	DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE OF ACCEPTANCE AND ACKNOWLEDGEMENT OF RESPONSIBILITIES - SUBSCRIBER
DOD 5400.11-r	DEPARTMENT OF DEFENSE PRIVACY PROGRAM
DOD CP	United States Department of Defense X.509 Certificate Policy
NIST SP 800-157	Guidelines for Derived Personal Identity Verification (PIV) Credentials
OTA	Over-the-air Profile Delivery and Configuration
PIA	Privacy Impact Assessment (PIA)