Privacy Policy for the Sample Key Provider and Key Share Consumer apps

The Sample Key Provider (SKP) and Key Share Consumer (KSC) apps are test apps made available to vendors developing apps that integrate with the Purebred Registration for iOS app. The Purebred Registration 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 test apps. Source code for the test apps is available at https://github.com/purebred.

What User Data Collected

SKP and KSC are test apps and are not intended to handle "real" data. As such, there is no expectation that either will process personally identifiable information (PII). Users are advised to refrain from using either app in conjuection with any information of value. The remain of this section describes data that is collected.

SKP supports importing PKCS12 files provided by the user via the iTunes File Share interface. The nature of these files is controlled by the user. SKP features a set of test PKCS12 files that may be used without using iTunes File Share as an import mechanism.

KSC supports importing PKCS12 files via its document/provider interface. The source for the PKCS12 files is selected by the user.

If the user elects to use real data with the SKP and KSC test apps, a variety of PII may be stored by the app including:

- First name(s)
- Last name(s)
- Email address(es)
- EDIPI(s)
- Device serial number(s)
- Authentication, digital signature, encryption or device certificates and corresponding private keys

How User Data Is Collected

SKP may, at the user's election, import keys shared with the app via the iTunes File Share interface. The user must take steps to share PKCS12 files via iTunes, then click the button in the app to import the files then enter the correct password to decrypt the PKCS12 file.

The primary purpose of KSC is demonstrate how to integrate with the "key sharing" interface of the Purebred Registration for iOS app. Accordingly, the app may be used to import certificates and private keys from apps that broadcast support for one or more of the uniform type identifiers (UTIs) sought by KSC. The list of UTIs is set via the Settings app. PKCS12 file information is shared via this mechanism (either as a single PKCS12 file or as a zip file containing multiple PKCS12 files) and the password is shared via the system pasteboard.

How User Data Is Used

SKP provides a key sharing interface that may be exercised by any app that supports the target set of UTIs. The 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 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.

KSC imports PKCS 12 files via a document/provider interface and stores the keys in its view of the system key chain. Details of the keys may be viewed via the app.

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

In lieu of a system-wide key chain, the SKP app uses a document/provider interface to share certificates and private keys as PKCS 12 files with third party apps that invoke the system's document/provider APIs using one or more of the uniform type identifiers listed at https://github.com/purebred. Use of the SKP app is anticipated to be limited to test scenarios and possibly subject to Restrictions imposed by an MDM system.

Data Retention Policies

The SKP and KSC apps can be uninstalled subject to any MDM limitations. Each app provides means to clear any key chain items associated with the app. Failure to clear the key chain prior to uninstalling the app may leave keys in the system key chain, subject to operating system protections and key chain hygiene procedures.

Deleting materials from third-party apps that received PKCS12 files from the SKP app is performed in accord with instructions accompanying the third-party app.