DIGITAL TRUST
from Silicon to Services

intercede

MyID

Trusted credentials for secure apps: MyID Mobile SDK

Add two-factor authentication to apps without needing to be a security expert; let the SDK handle the storage and use of credentials for you.

The MyID® Mobile SDK from Intercede® makes it easy for third party app developers to use credentials for strong authentication and data protection in their apps. It provides a simple goal-based API that allows developers to deliver cryptographic functions without needing to know how they work.

The MyID library performs all necessary secure element detection, user interaction (PIN entry) and key discovery. It handles finding the available credentials that can be used for authentication, so that developers don't have to worry about supporting multiple secure elements and credential structures, making it quick and easy to incorporate secure identity.

The MyID Mobile SDK handles the complexity associated with accessing credentials and making use of them, and can enforce policy. The solution works across multiple platforms such as iOS and Android.

The MyID Mobile SDK comes with API documentation, a pre-built library for each supported operating system and a test application, making it easy to build into apps. It is also compatible with external smart card readers attached to smartphones and tablets, allowing the use of credentials held on smart cards such as PIV cards.

Multiple mobile platforms

With your existing Cloud services

Using the latest mobile phone security features

How it works

Example use cases

Signing an outgoing email

The MyID Mobile SDK enables apps to present a plain-text email, which it signs using an appropriate key from the credential store. It then returns a signed S/MIME email with signature that is ready to send. If necessary, the MyID SDK will prompt the user for their PIN during the process. No further modification of the data should be needed by the app.

Decrypting an incoming email

To decrypt an email, the MyID Mobile SDK takes the encrypted email text presented by an app and decrypts it using the appropriate key in the device's credential store, returning a plain-text email. The user may be prompted to enter their PIN during the process in order to authenticate themselves, and this is handled by the SDK.

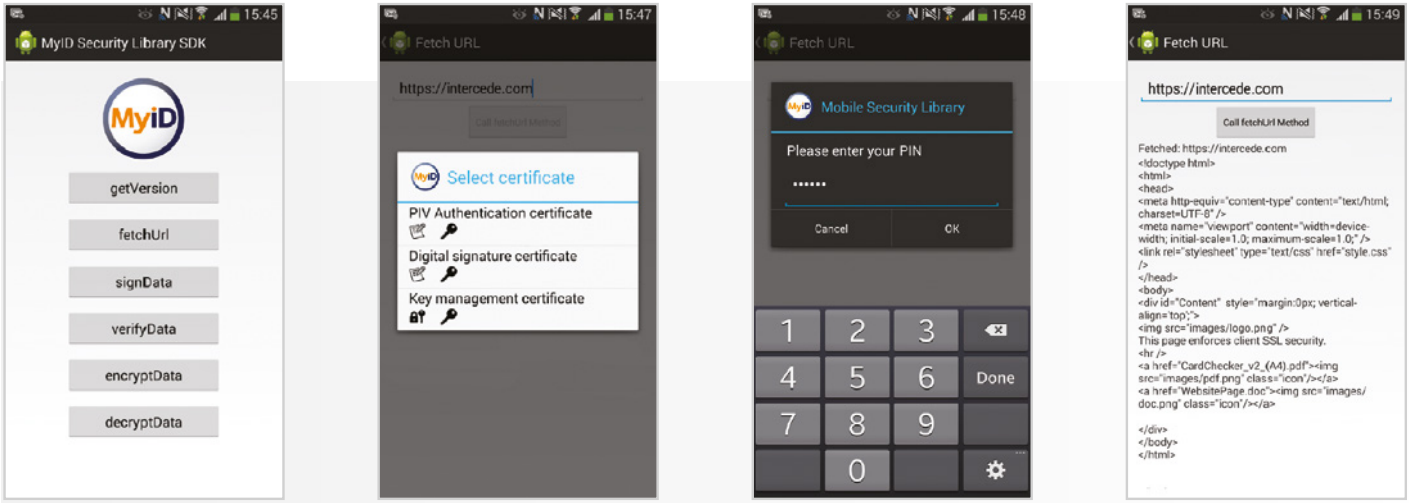
Creating a mutual SSL session

This function enables apps to present a URL string, which the MyID Mobile SDK connects to using a client authentication certificate from the credential store. Users may need to enter their PIN to authenticate during the process, after which the SDK can download the content for the app to display.

The MyID Mobile SDK comes with a sample app. This allows developers to see a demonstration of the process followed by the SDK when it needs to use credentials to perform a function.

Decrypting an incoming email

1. The developer chooses the function required from the available list, which includes getVersion, fetchUrl, signData, verifyData, encryptData and decryptData. In this example fetchUrl is used.
2. They enter the URL they would like to visit and click the 'Call fetchUrl Method' button.
3. Coordinating with the server request, the SDK looks for available credentials that can be used to authenticate the user and displays a list on screen. The developer then selects the appropriate certificate from the list.
4. The SDK presents the developer with a PIN popup, where they must enter their PIN and click OK.
5. If successful, the website page is returned. If the PIN entered is incorrect, a failure message will be displayed.



MyID Mobile SDK sample app Fetch URL process for Android

Features and benefits

Key features

- Add strong two-factor authentication to apps by accessing securely stored credentials
- Works across multiple platforms including iOS and Android
- Compatible with external card readers plugged into smartphones and tablets
- Supplied with API documentation, prebuilt libraries and a test application

@ info@intercede.com www.intercede.com intercedemyid
Suite 920, 1875 Explorer Street, Reston, VA 20190, USA +1 888 646 6943