GEOCENT

111 Veterans Blvd
Suite 1600
Metairie, LA 70005
800-218-9009
www.geocent.com

Leveraging the cloud and secure web-services as a platform for developing secure governmental mobile applications that support Bring Your Own Device (BYOD) initiatives

The U.S. government is currently struggling to find a solution to enabling a more mobile workforce as a means to reduce cost and increase employee satisfaction. The federal CIO, Steven VanRoekel, released the digital government strategy on May 23, 2012, which requires agencies to release more data for public consumption through Web APIs; extend government services to mobile devices; and make it easier for federal employees to acquire and use mobile devices on the job. To help implement this strategy, he has formed the Digital Services Innovation Center and created an advisory group to develop a bring-your-own-device (BYOD) policy for federal employees. While still under development, this group has identified three basic technical approaches to development of BYOD programs:

- **Virtualization**: Provide remote access to computing resources so that no data or corporate application processing is stored or conducted on the personal device
- **Walled garden**: Contain data or corporate application processing within a secure application on the personal device so that it is segregated from personal data
- **Limited separation**: Allow comingled corporate and personal data and/or application processing on the personal device with policies enacted to ensure minimum security controls are still satisfied

The choice of which technical approach to use depends on the intended audience, security requirements for the data, and specific needs of the organization.

Most of the current implementations tend to utilize either the virtualization approach or the walled garden approach, as these are the most secure and involve the least amount of risk for the government. Unfortunately, these approaches also tend to the most costly and least user-friendly options.

Virtualization approaches (currently being utilized by DHS) solve the mobile challenge by providing a sort of “virtual desktop” on the mobile device, and provide a user-interface only. All execution, control, and data are managed at the server. The trouble with this approach is that the flexibility afforded by mobile devices, specifically a rich user experience with minimal user-interface latency (the time it takes from button-press to actual result), is not realized. Apps tend to look and feel like a remote desktop, as that is in fact what they are.

The Walled Garden approach involves installing specialized software onto a device which creates a secure sandbox (walled off area) of the device in which government apps can run. While this solution allows application developers and users full access to all of the rich user interface capabilities of the device, it increases costs and has some negative impacts on user experience. Costs are increased as licenses to the sandbox environment must be purchased and managed, and it has a negative impact on the user experience in that users must switch modes to access government applications. This mode switching takes time, and requires extra steps by the user.

GEOCENT

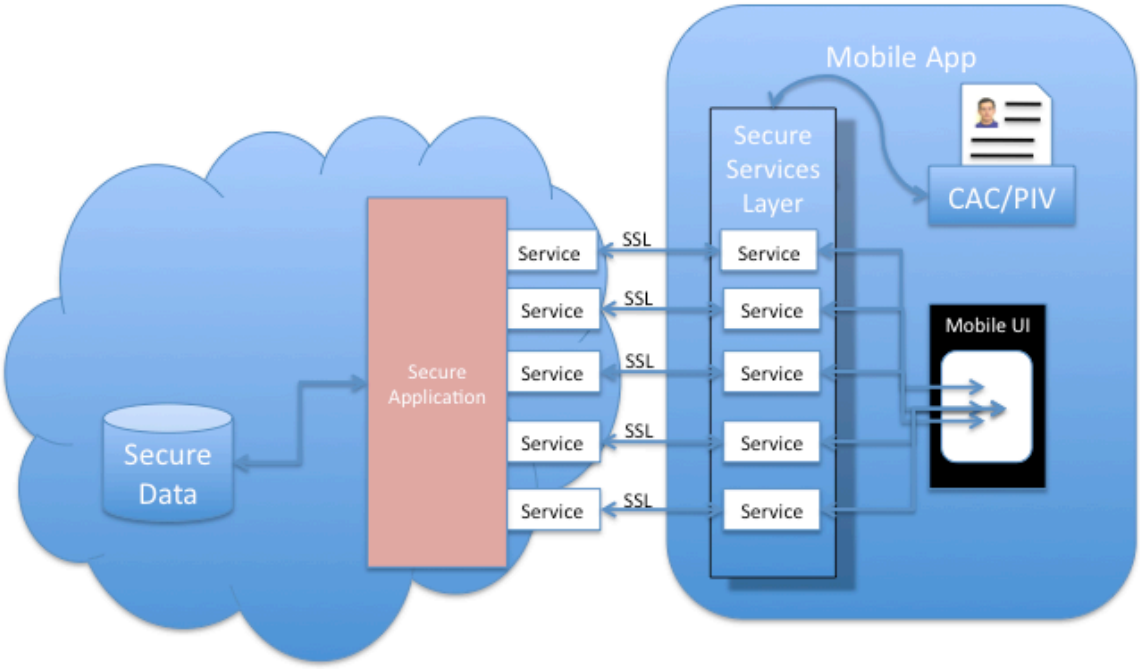
111 Veterans Blvd
Suite 1600
Metairie, LA 70005
800-218-9009
www.geocent.com

The limited separation approach has the ability to provide an answer to both of these problems, however government agencies are wary of this approach except for the most publicly accessible of data. This is due to the potential security risks involved with this approach, including potential breach of data. This risk is especially high when any data is stored on the device, as devices can easily be lost or stolen. Because of this, the limited separation approach will likely have few use cases.

This paper proposes an approach that provides the best of both worlds, security and integrity coupled with rich user-experience capabilities afforded by the mobile device. This approach falls somewhere between the virtualization and the limited separation approach.

The approach proposed here will provide complete separation of data and processing without requiring a walled garden. We accomplish this by developing a full-blown mobile application that leverages cloud-computing hosted web-services.

The following diagram shows the basic technical approach:



The approach utilizes the mobile device for the purpose it is best suited, to provide a rich user experience. The mobile app is developed as rich mobile app, with full access to all mobile features (touch-sensors, GPS, camera, audio, etc.), however, the app provides no real processing of data, and minimal (if any) storage of data. All data storage, application processing, and business logic are executed on a secure application server. By using this approach, there is no risk of data being retrieved from the device if lost or stolen, as by design the app should store little or no data.

GEOCENT

111 Veterans Blvd
Suite 1600
Metairie, LA 70005
800-218-9009
www.geocent.com

The Secure Services Layer and CAC/PIV integration are the keys to making this a secure solution. The Secure Services Layer integrates with the CAC or PIV card, utilizes the keys within the card to establish a two-way Secure Socket Layer (SSL) connection with the secure application. In addition to securing the connection, the CAC signature credentials are utilized to authenticate the user to the application.

Because this approach utilizes Web Services secured via CAC/PIV authentication and encryption, support for the server-side already exists. All existing FIPS and DoD compliance mandates can be utilized to secure the server-side application components of the system. Current IA policies can be fully and properly enforced.

The approach presented here is similar in many respects to the way most mobile application development is currently performed; especially for complex applications that require significant storage or computation. Cloud computing for storage as well as processing is a common use-case for app development, and thus the design patterns are familiar to most mobile developers.

Implementation

Geocent utilized this approach to develop the Mobile C4ISuite for SPAWAR Systems Center Pacific. Our application provides a rich mobile app for interfacing with the Commander Navy Installations Command (CNIC) C4ISuite system. The C4ISuite provides operations centers the ability to share their status information and the output of their C4I systems to provide more complete situational awareness (SA) to all operators in support of emergency operations.

The mobile application provides rapid access to several key areas of the system including urgent notices, ATFP reports, operational status, and C4I Chat. Urgent notices can be viewed as well as created by the mobile app, and also provides the ability to take pictures associate them with urgent notices as well as display them on the C4ISuite One Common Picture. ATFP reports can be viewed as well as created by the app. The chat feature allows two-way communication with field users.

The Geocent team had to develop 5 custom components to enable the prototype capability to transition to interface with the production application:

1. Bluetooth Connection to the Android Application: Leveraging the same PC/SC middleware used for desktop CAC readers, Geocent had to develop custom Java and C code to interface with the Java Native Interface on the Android device.
2. Secure Bluetooth Connection: Geocent developed custom code to manage and help to establish the interface between the BAI Bluetooth reader and the Android application.
3. Two-factor Authentication to application: Geocent developed middleware for the Mobile application. If at any time the CAC is removed from the BAI 3000MP, the user is immediately logged out of the application and must re-establish user authentication to the C4I suite using two factor authentication. The user must have their CAC inserted into the reader and provide their PIN number for authorization to the application.

GEOCENT

111 Veterans Blvd
Suite 1600
Metairie, LA 70005
800-218-9009
www.geocent.com

4. Android Application connection over SSL to the application: Once authenticated to the application, an encrypted, secure tunnel is created to allow the mobile device user to send and view data without compromising security.
5. Encrypt all application related data: The displayed data is all driven by the application services and is not retained on the device. Draft reports, audio recordings, and photos generated from within the app are encrypted and are only accessible to the CAC authenticated user

All of these components were developed as reusable modules that can be embedded within any mobile app to provide similar functionality.

It is interesting to note that the development of this mobile application require no changes to the server code, as secure web services were already available for use by the application.