TECHNICAL BRIEF

SECURING SMARTPHONES IN THE MOBILE ENTERPRISE

MOTOROLA

THE CHALLENGE: MAINTAINING SECURITY IN THE SMARTPHONE AGE

Smartphones have found a home in the business world, where they help many enterprise workers communicate, collaborate and work smarter than ever before. But since most of the smartphone enterprise applications are native instead of web-based, computing is pushed back out to the edge (on the device) instead of on a centralized server inside the enterprise. As a result, security becomes an issue — IT needs to:

1. Secure data in transit as it travels between smartphone and enterprise server
2. Secure data stored on the device — a requirement for offline application access
3. Securely manage applications — from updating applications with new versions to removing application and associated data for users who leave the company or change jobs
4. Ensure enterprise level user authentication
5. Implement backend application authorization

This technical brief outlines how Motorola Solutions RhoMobile Suite addresses all five of these issues to enable the development of smartphone applications that not only increase worker productivity and their ability to better serve your customers, but also meet enterprise security requirements.

ISSUE 1: TRANSMISSION SECURITY

The majority of smartphone applications send information over the public Internet — and often this information is sensitive. As a result, smartphone applications need to secure the data that's in transit to and from the device.

Whether you are writing in Objective C, Android Java or RhoMobile Suite, best practices call for secure transactions using SSL via an HTTPS connection.

RhoMobile Suite keeps business data in transit between smartphone and enterprise server secure through support of SSL (https) as a transport — just the same as if you were writing in Objective C or Android Java. In fact, using SSL is easier with RhoMobile Suite. With the RhoMobile AsyncHttp.get call, you just need to list an https URL and the RhoMobile application will securely connect to the backend. By contrast, when writing to underlying software developer kits (SDKs), connecting to an https URL requires significantly different code — adding to the time and complexity of coding your application.

ISSUE 2: STORAGE SECURITY

With native smartphone apps (unlike mobile web applications), data must be available online and offline so workers can stay productive regardless of whether they have a wireless connection. This requires the storage of enterprise data on the smartphone.

To ensure the security of the stored data, sensitive information should be encrypted. As a best practice, when using RhoMobile Suite to create your native smartphone applications, you can easily encrypt data by enabling automatic data encryption using RhoElements. As a result, you can easily implement 256 bit AES encryption for all of your enterprise sensitive data. RhoMobile Suite will also be adding PKI (public/private key) encryption capabilities in upcoming releases of RhoElements.

ISSUE 3: MOBILE APP MANAGEMENT

Native smartphone apps introduce new management challenges. IT needs to be able to:

- Install new apps on user smartphones
- Install any app updates
- Remove apps and the associated data
- Remove the app management portal when appropriate

To further complicate app management challenges, many smartphones in use in the enterprise may be owned by users. While those users won't mind giving the enterprise control over the business applications on their personal device, they will likely resist giving the enterprise visibility into all the applications on their device.

RhoMobile Suite's RhoGallery provides the features required to address all of these issues. The first hosted mobile app management solution, RhoGallery allows you to easily manage your mobile apps (regardless of whether they were created with RhoMobile Suite). Simply group applications into "galleries" and invite users to join the appropriate gallery. Once a user joins, the appropriate applications are automatically downloaded to the smartphone. As new apps and updates to existing apps become available, they are also automatically downloaded to users' smartphones. And in the event a user changes jobs or leaves the companies, you can de-provision applications as well.

ISSUE 4: ENTERPRISE AUTHENTICATION

Native smartphone applications require data synchronization between the device and backend server. In order to ensure optimal security during synchronization, there must be "delegated authentication" to some form of enterprise directory — ideally, the company's well-maintained LDAP directory.

RhoMobile Suite's RhoConnect makes it easy to perform delegated authentication by simply providing an "authenticate" model that can call to any directory authority, typically requiring less than five lines of code.

ISSUE 5: BACKEND APP AUTHORIZATION

In addition to requiring the proper credentials to perform data synchronization, user credentials should also be required to login to the backend app to ensure only authorized users access your business data. A global "app ID" for all users does not provide sufficient security, putting your data at risk.

RhoMobile Suite's RhoConnect allows you to easily implement the best practice of backend app authentication — the sync source adapters themselves support the login authentication method, reducing coding and the effort required to secure business data.

CONCLUSION

As companies expand their mobile strategy and sensitive information is pushed farther and farther to the edge, mobile security takes center stage. Motorola Solutions understands the risks associated with enterprise mobility and provides the tools required to use best practices that have proven to keep company data secure. With RhoMobile Suite, you can:

- Send sensitive information via a secure SSL (https) connection
- Encrypt data stored on the device
- Easily manage only the corporate applications and data on devices, ensuring support for personal smartphones in use through enterprise BYOD initiatives
- Secure data synchronization operations by requiring delegated authentication to the enterprise directory
- Require login to the backend database to ensure that appropriate data is only released to authorized users

For information on how Motorola Solutions can help you create next-generation OS-agnostic mobile applications, please visit www.motorolasolutions.com/RhoMobileSuite

Part number: TB-SCRSMRTPHNES. Printed in USA 08/12.

MOTOROLA