

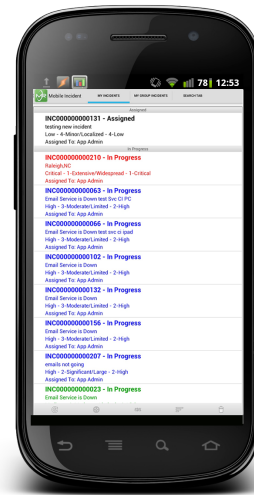
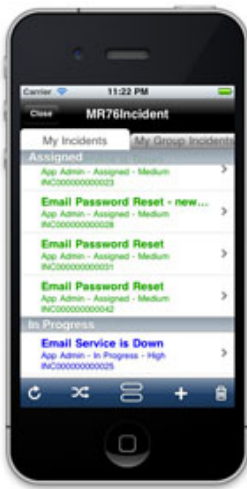


White Paper

## SPLITWARE MOBILITY PLATFORM: SECURE ENTERPRISE MOBILITY

Mobile Reach  
+1 919 336 2500

[www.mobilereach.com](http://www.mobilereach.com)



# Splitware Mobility Platform: Secure Enterprise Mobility

## Executive Summary

Enabling mobile access to enterprise applications and data provides a fantastic opportunity to optimize your mobile workforce and realize significant productivity gains. However, a necessary part of the cost of implementing a mobile enterprise application platform is ensuring that the solution is secure and can maintain data integrity, protection, and control of all information that flows between the corporate network and the mobile devices being used. As we move rapidly forward in the world of information technology, advancements in ways to crack even the most robust security systems continue to take advantage of outdated modalities in over-the-air data transfer.

This paper addresses four areas of security that must be considered when implementing a mobile enterprise application platform: Network Communication Security (securing data in transit between mobile devices and corporate systems), Device Security (securing the mobile device itself), Application Security (level of trust in the mobility software), and Data Protection (securing data when it resides on a mobile device or is being used on a mobile device).

Mobile Reach's Splitware Mobility Platform is currently in operation at a variety of Fortune 500 organizations, including many financial and health care institutions, as well as at many United States Military, Federal and Department of Defense Agencies, and state and local government organizations that have stringent standards and requirements for information security. These requirements are a very serious and important component of the Splitware Mobility Platform, which has been awarded the U.S. Army's Certificate of Networthiness, signifying successful compliance with rigid security testing.

This paper will discuss the software security measures that the Splitware Mobility Platform provides, above and beyond any existing network or device security measures. And, when additional protection is required, Mobile Reach will implement secure add-ons to meet the needs of your organization.

## Network Communication Security

Network Communication Security refers to the security of the network and communication protocols that are used to transmit data between devices. The Mobile Reach Splitware Mobility Platform can operate over any network that is required by the user and does not require any specific network components, except for a TCP stack.

The system architecture is intentionally flexible and modular so that it can operate over either fast or slow networks and seamlessly handles network interruption. Splitware minimizes the amount of data transferred between mobile client and backend application to only what is necessary and all data transferred is fully encrypted. In order to complete a secure loop, Splitware transmits data through a single TCP Port to reduce the requirements on firewall openings.


### **Encryption**

In order to protect critical data in all over-the-air transactions, the platform provides encryption options above and beyond the standard encryption provided by the network infrastructure and/or device being used in the system. The Splitware Mobility Platform provides four levels of encryption options with AES-256 being the highest, for those customers that require the highest level of protection.

Adopted by the U.S. Government, AES (Advanced Encryption Standard) is currently the most advanced, most extensively analyzed algorithms used in symmetric key cryptography. The AES comprises three block ciphers, AES-128, AES-192 and AES-256, with AES 256 being the most recent and advanced cipher. Splitware provides other encryption options, such as 3DES (Triple Data Encryption Standard), for environments that have slightly less stringent security requirements and may trade off for better network performance.

### **Offline Operation**

In some environments, wireless communication is simply not an option due to the inability to guarantee a secure enough wireless infrastructure. In these situations, Splitware applications can operate in a 100% offline environment. Critical enterprise infor-



mation is downloaded to the mobile device using a tethered USB cable connected to a secure PC. The user goes about their work in an offline mode, and then re-synchronizes data upon completion without ever needing to be connected to a wireless network.

## Device Security


Device security is a critical component to your mobile security strategy and pertains to the security of data by the mobile device itself. Because mobile devices are not stationary, they roam outside of the corporate network and are vulnerable to a much broader array of attacks. You will want to address the protection of sensitive data on mobile devices and what happens if a device gets lost or stolen.

Mobile Reach currently offers solutions on four well-secured platforms: iOS, Android, Windows Mobile and BlackBerry. On all platforms, Mobile Reach mobile applications require a User ID and Password, which is safely encrypted on the device and authenticated against the backend application.

## iOS Security

Apple designed the iOS platform with security at its core. iPhone, iPad, and iPod touch are designed with layers of security. Low-level hardware and firmware features protect against malware and viruses, while high-level OS features allow secure access to personal information and corporate data, prevent unauthorized use, and help thwart attacks. The tight integration of hardware and software on iOS devices allows for the validation of activities across all layers of the device. From initial boot-up to iOS software installation and through to third-party apps, each step is analyzed and vetted to ensure that each activity is trusted and uses resources properly.

The iOS security model protects information while still enabling mobile use, third-party apps, and syncing. Much of the system is based on industry-standard secure design principles—and in many cases, Apple has done additional design work to enhance security without compromising usability. The secure boot chain, code signing, and runtime process security all help to ensure that only trusted code and apps can run



on a device. iOS has additional security features to protect user data, even in cases where other parts of the security infrastructure have been compromised (for example, on a device with unauthorized modifications). Like the system architecture itself, these encryption and data protection capabilities use layers of integrated hardware and software technologies.

Every iOS device (iPhone, iPad, iPad Mini, iPod touch) has a dedicated AES 256 crypto engine built into the DMA path between the flash storage and main system memory, making file encryption highly efficient. Along with the AES engine, SHA-1 is implemented in hardware, further reducing cryptographic operation overhead.

The device's unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused into the application processor during manufacturing. No software or firmware can read them directly; they can see only the results of encryption or decryption operations performed using them. The UID is unique to each device and is not recorded by Apple or any of its suppliers. The GID is common to all processors in a class of devices (for example, all devices using the Apple A5 chip), and is used as an additional level of protection when delivering system software during installation and restore. Burning these keys into the silicon prevents them from being tampered with or bypassed, and guarantees that they can be accessed only by the AES engine.

In addition to the hardware encryption features built into iOS devices, Apple uses a technology called Data Protection to further protect data stored in flash memory on the device. This technology is designed with mobile devices in mind, taking into account the fact that they may always be turned on and connected to the Internet, and may receive phone calls, text, or emails at any time.

## **Android Security**

Android seeks to be the most secure and usable operating system for mobile platforms by re-purposing traditional operating system security controls to:

- Protect user data
- Protect system resources (including the network)

- Provide application isolation


To achieve these objectives, Android provides these key security features:

- Robust security at the OS level through the Linux kernel
- Mandatory application sandbox for all applications
- Secure interprocess communication
- Application signing
- Application-defined and user-granted permissions

At the operating system level, the Android platform provides the security of the Linux kernel, as well as a secure inter-process communication (IPC) facility to enable secure communication between applications running in different processes. These security features at the OS level ensure that even native code is constrained by the Application Sandbox. Whether that code is the result of included application behavior or a exploitation of an application vulnerability, the system would prevent the rogue application from harming other applications, the Android system, or the device itself.

The Android platform takes advantage of the Linux user-based protection as a means of identifying and isolating application resources. The Android system assigns a unique user ID (UID) to each Android application and runs it as that user in a separate process. This approach is different from other operating systems (including the traditional Linux configuration), where multiple applications run with the same user permissions.

This sets up a kernel-level Application Sandbox. The kernel enforces security between applications and the system at the process level through standard Linux facilities, such as user and group IDs that are assigned to applications. By default, applications cannot interact with each other and applications have limited access to the operating system. If application A tries to do something malicious like read application B's data or dial the phone without permission (which is a separate application), then the operating system protects against this because application A does not have the appropriate user



privileges. The sandbox is simple, auditable, and based on decades-old UNIX-style user separation of processes and file permissions.

### **BlackBerry Security**

The BlackBerry product has been built from the ground up as a highly secure device and includes a BlackBerry Enterprise Server (BES), which provides robust device management as well as a variety of other services for BlackBerry devices. Mobile Data Services (MDS) provides a tunnel back into your intranet enabling secure connection through your firewall.

BlackBerry encrypts all data transmitted between the BES and the BlackBerry devices, and all data stored is also encrypted. Password authentication can be made mandatory, and, after ten incorrect attempts, the smartphone's memory is erased. All Splitware encryption and authentication is provided in addition to these standard BlackBerry services.

### **Windows Mobile Security**

Microsoft offers a Mobile Device Management server that provides similar functions to a BES. There are three options to consider for a secure connection back into the intranet. The most common option is a Virtual Private Network (VPN); Mobile Reach provides the ability to auto-dial the VPN connection so that the user does not need to ensure connectivity ahead of time. Another option is a Demilitarized Zone (DMZ) configuration of the Splitware Gateway. This means placing the Splitware Gateway in a DMZ so it is accessible via a TCP port to the WAN as well as having secure access into your intranet to connect to the enterprise server.

Finally, Access Point Name (APN) is a point of entry onto an IP network for a mobile device, the radio access equivalent of an ISP's dialup phone number. Each mobile device must be configured with appropriate settings to connect to the customer specific APN, which must be added to the carrier's home location register.

## Mobile Application Security

While many organizations put most of their security focus on network and systems infrastructure, 70% of all security vulnerabilities actually exist in the software application layer, according to Gartner Group. These security threats result from poorly written, easily “hackable” software code, a prevalent problem fueled by the fact that software engineering is not guided by the strict rules and regulations that govern other engineering disciplines.

You cannot “eyeball” a software application to even estimate its correctness. Software testing is a very involved, expensive, and imperfect process that directly correlates the time invested in the test process to the level of quality assurance associated with the product. Mobile application software adds another complication, which is the fact that it can be operating outside the physical confines of the organization, making it much more difficult to monitor and control.

Mobile Reach understands these concerns and employs many controls to ensure secure and correct operation of the entire Splitware Mobility Platform. The full product suite is self-contained, requiring no third-party applications or plug-ins. All of the software is internally designed, built, and tested, under a solid software development lifecycle that assures a high-quality product release and removes the risk of incorporating unknown application software into the equation.

Splitware’s client-server architecture does not use web browser or open source technologies that add another layer of security risk. In fact, the Splitware Mobility Platform has been built with a simple and modular architecture that was designed specifically to provide highly secure mobile extensions to an existing enterprise environment.

### **Security Features of Splitware**

- Splitware does not stage enterprise application data in a separate database, which would add another repository requiring protection.
- Splitware uses authentication controls that are managed by the enterprise application.



- Splitware incorporates user authentication, encryption, and validation on the mobile device.
- Splitware applications lock to prevent access by unauthorized users.
- Enterprise data is protected and only accessible inside the Splitware applications.
- Splitware can be configured to limit the data transferred between the enterprise data source and the mobile client, so that sensitive information can be removed from the data stream.

## Data Protection

Certainly one of the most basic requirements in a mobile environment is a secure wireless device. Loss or theft of a device occurs frequently, so applications that are left open or data that is not encrypted on the device is in jeopardy of being compromised.

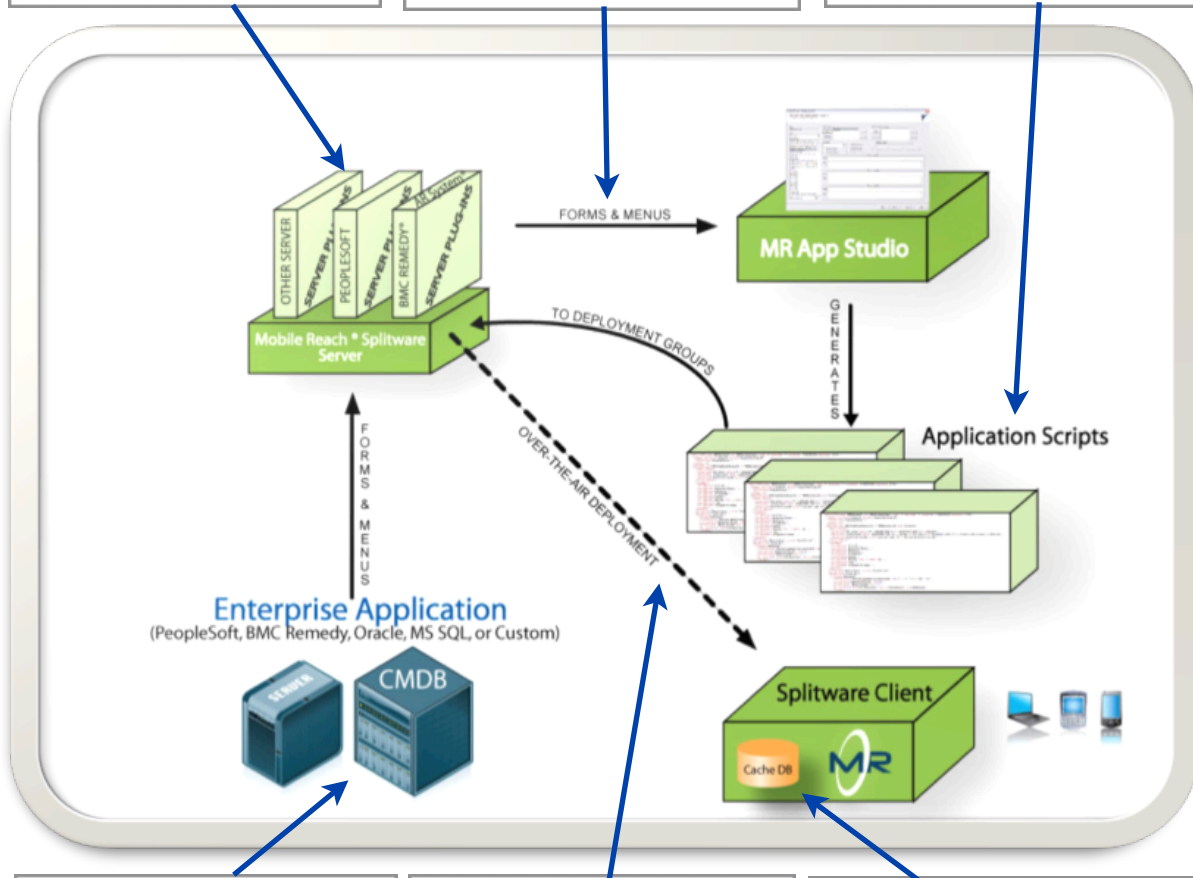
In order to prevent critical enterprise application data from being accessed by unauthorized users, Mobile Reach locks user applications automatically and can encrypt all application data stored on the device using the same encryption levels that are employed for over-the-air communication. Application data is only accessible through the Splitware application itself, which is protected with a User ID and Password. Passwords are also encrypted on the device to prevent unauthorized access. These passwords must be authenticated with the Enterprise backend application before use. So, in the case where a device does happen to end up in the wrong hands, the system administrator can reset the User's Enterprise password, preventing the device from being able to access the Enterprise application even if the rogue user is able to decrypt the password.

This encryption adds to any other security methods employed by the network (WiFi, cellular), device (iOS, Android, BlackBerry, Windows Mobile), VPN Client, or Device Management Software.

Splitware's plug-in architecture incorporates secure access to each enterprise application to ensure the most effective method.

When mobile applications are generated, data used can (and should be) minimized so that sensitive information is only transferred when required.

Secure application scripts are used to drive the client-side user interface. The mobile application scripts are encrypted.



Splitware extends existing enterprise application authentication to users on mobile devices. Mobile users must supply User ID and password to access.

Splitware encrypts all data transferred between the Splitware Gateway and the client on the mobile device.

Cache database is encrypted on the mobile device. Only the Splitware applications are able to access data in the encrypted database.

Another method for minimizing the risk of data exposure is to limit the data transmitted, used and stored in the mobile environment. Splitware provides the flexibility to operate with partial data records when an organization requires that sensitive data not flow outside of the protected corporate network. Certain fields can be eliminated from the Splitware mobile application.

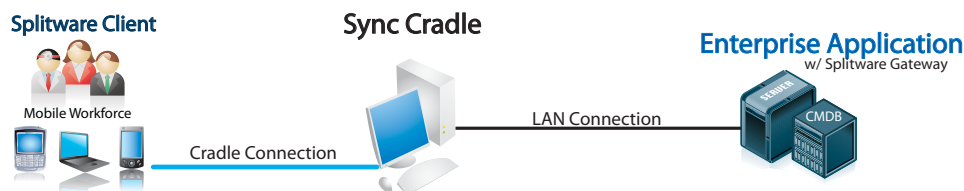
### Data Security Compliance

In recognition of its secure network architecture, the Splitware Mobility Platform has been awarded a Certificate of Networkiness by the United States Army. This certificate signifies successful completion of stringent security testing and identifies the product as trustworthy. Mobile Reach also meets HIPAA Compliance regulations and has passed all customer security testing.

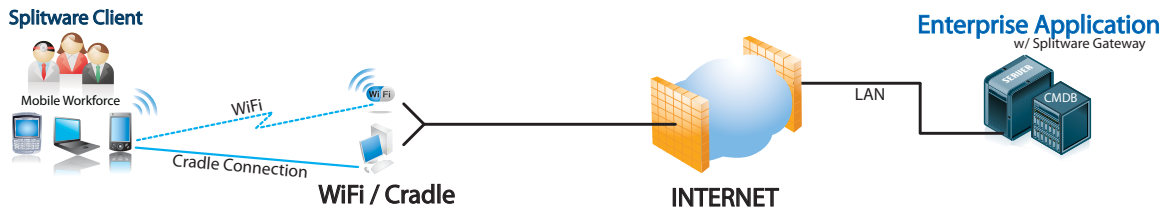
### Secure Splitware Communication

The Splitware Mobility Platform can be configured to connect your mobile workforce with your backend applications in a number of different ways, depending on your environment. All configurations incorporate the security features described above.

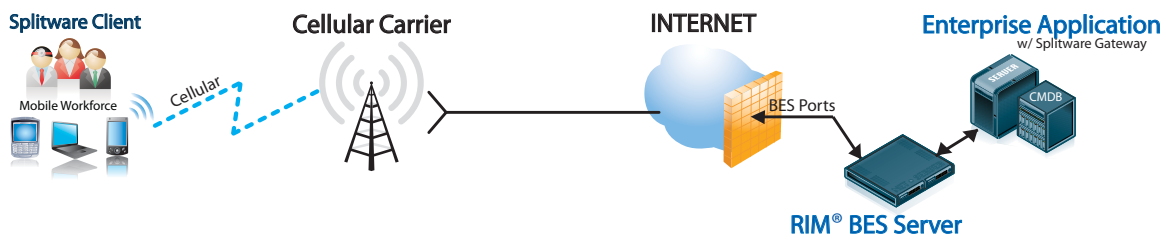
When wireless connectivity is not available or not desired, the mobile workforce is connected via Sync Cradle directly to network. Data is synchronized by Splitware.



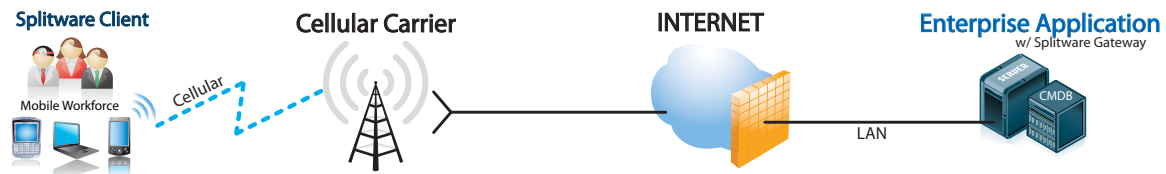
When mobile workers are outside of the enterprise environment and must connect over the Internet, the Splitware client opens up a communication path only when necessary, and securely transmits data.



When Splitware applications are provided on BlackBerry devices, RIM’s BES Server provides a secure transport, while Mobile Reach still encrypts all data sent through the network.



When Splitware runs on smartphones, a secure cellular connection is used to transport data across the network to the Splitware Gateway and then on to the enterprise application.



When Splitware runs on RFID devices and readers, a secure WiFi connection is used to transport data across the network to the Splitware Gateway and then on to the enterprise application.

