



SECURITY OF THE INTELLISYNC MOBILE SUITE PLATFORM

An Intellisync Corporation White Paper
October 2005



TABLE OF CONTENTS

- Intellisync Mobile Suite Platform Introduction 1
 - Reducing Risk 2
 - Safeguarding Mission-Critical Enterprise Data 2
- Part 1: Intellisync Mobile Suite Platform Architecture 3
 - Intellisync Mobile Suite Platform 3
 - Data Flow 3
 - Scalability 4
- Part 2: Enterprise Security 5
 - Intellisync Mobile Suite Platform Secure Gateway 5
 - Enterprise Reverse-Proxy 6
 - Deployment Strengths 7
 - Advanced Options for More Complex Networks 7
- Part 3: Data Security 8
 - How Information is Safely Transferred 8
 - Session-Based Key Exchange 8
 - Password Storage 8
 - Device Security 9
 - User Disablement 9
- Part 4: Key Authentication 10
 - Summary 10
- Appendix A: Information on Encryption Algorithms 11

SECURITY OF THE INTELLISYNC MOBILE SUITE PLATFORM FOR BEHIND THE FIREWALL APPLICATION

Introduction

With the rapid proliferation of both data-capable smartphones and high-speed wide area wireless networks, it has become increasingly critical that IT departments put into place security measures to protect corporate data that is finding its way outside their corporate firewall. There are a number of choices for insuring data security, and selection between these choices involves tradeoffs in usability, cost and administrative complexity.

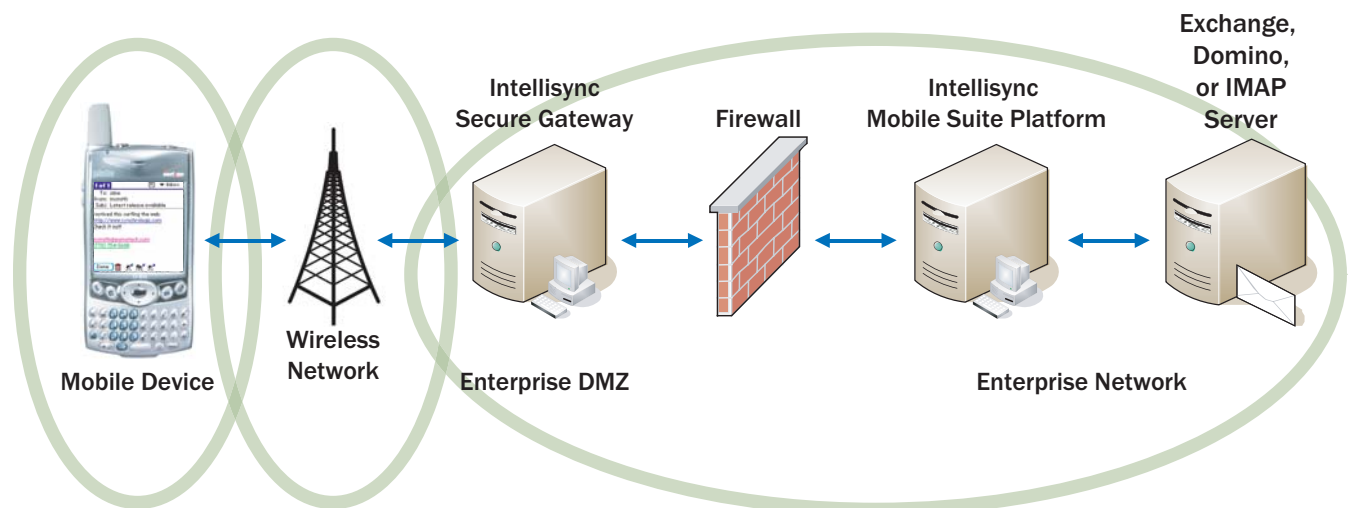
As enterprises move into providing wireless data applications for their mobile employees, data security becomes a key influencer in the decision process. So what is needed? What does an enterprise have to do to insure data is protected?

“What it really takes,” says Stewart S. Miller, author of *Wifi Security*, “is an end-to-end approach. Some solutions protect the data at the enterprise but offer no protection on the device. Others provide the end user with security tools, but ignore the IT manager. And many solutions ask the enterprise for the data but make the enterprise rely on their own firewalls to filter out the bad guys. It’s really very simple, you have to do it all – one hole is all it takes for a hacker to succeed.”

A simple way to plan for strong security is to track the data flow from end-to-end and create overlapping “rings” of security through which no unauthorized data or access can pass. To be effective, all the rings must be secure, including the corporate network, the carrier network and the mobile device. If these three environments are locked down, intruders will look elsewhere to easier targets.

The first ring starts at the enterprise, behind the firewall. Some customers will be comfortable with a hosted solution for wireless email, which typically involves a small server or application that is installed behind the firewall to talk to the company’s email servers. Hosted solutions are good for small to mid-sized companies because the security is built-in, but they lack administrative tools that IT professionals at larger companies desire.

A larger company needs a server that supports a full range of device management tools for controlling the mobile devices, and a gateway capability that filters incoming requests for information. Ideally, the server should initiate communications with a secure gateway located in the company’s DMZ, so that no unauthorized systems are allowed to send data into the system and the first ring is secure.



Once data goes from the server, through the gateway, and into the carrier's network, the second ring, the carrier network, has to insure that the data is safe and encrypted. Intellisync offers a range of encryption options from very basic up to full blown military-grade encryption. It gives the customer a choice and insures that they can make the data as secure as they want. Intellisync also make sure that both the data and the pipe carrying the data through the carrier network are encrypted, for added security.

The last ring encompasses the mobile device. On-device password protection is key, as is the ability to remotely suspend the device or delete data and applications. The goal is to eliminate the "nightmare scenarios" like a CEO losing their device at an industry convention full of competitors. By empowering both the user and the IT administrator with security options relating to the mobile device, the third ring is secure.

Intellisync understands the issues involved in providing data security and has implemented strong security in the Intellisync Mobile Suite Platform. This paper examines the specific security elements found if the Intellisync Mobile Suite Platform is implemented behind the corporate firewall.

The Intellisync Mobile Suite Platform offers the enterprise a flexible deployment architecture to meet stringent corporate security requirements. The Intellisync Mobile Suite Platform, secured behind the firewall, does not require inbound initiated connections to any segment of an enterprise network with the goal of maintaining a high state of security while syncing data no matter where the end user is located.

Reducing Risk

When the mobile device sends or receives information from the enterprise server it is sent within an envelope of encryption. Security conscious Enterprise IT administrators worry about data sent wirelessly. Adhering to the highest standards within a public key infrastructure makes it possible to safeguard mission-critical information without fear of interception by a hacker.

Hackers try to exploit vulnerabilities within a network. If there is an open service that leads into your enterprise server they will try to hijack it to gain access. Deploying an effective DMZ outside your enterprise network misdirects the hacker to a non-essential machine outside of the enterprise firewall.

Much like a car thief, hackers will try to exploit what is available and easy to access. If a network is too difficult to break into, often times the hacker will simply move on to his next target that is easier to penetrate.

Safeguarding Mission-Critical Enterprise Data

A mobile data synchronization solution must be designed with security in mind, with the platform and network working together. The platform should have embedded intelligence for filtering and discarding of any potentially threatening information that it receives. It should be configurable with concentric rings of security, with a front-end, secure mobile gateway that prevents inbound access to the core platform.

Applications must require authorization when starting a network session. Enterprise data should be encrypted with strong methods like AES or 3DES; otherwise the communication channel itself should be encrypted using SSL. Encryption options should be easily configured per the needs of the enterprise. All these must be accomplished by the platform while it maintains network efficiency and drives data at a fast, sustained rate.

PART 1: INTELLISYNC MOBILE SUITE ARCHITECTURE

The key elements of the Intellisync Mobile Suite Platform architecture are outlined in the diagram below. The architecture consists of the Intellisync Mobile Suite Platform, which resides behind the firewall and talks to the corporate messaging server, the carrier network that manages notifications to the device and the mobile device. These elements are described below.

Intellisync Mobile Suite Platform

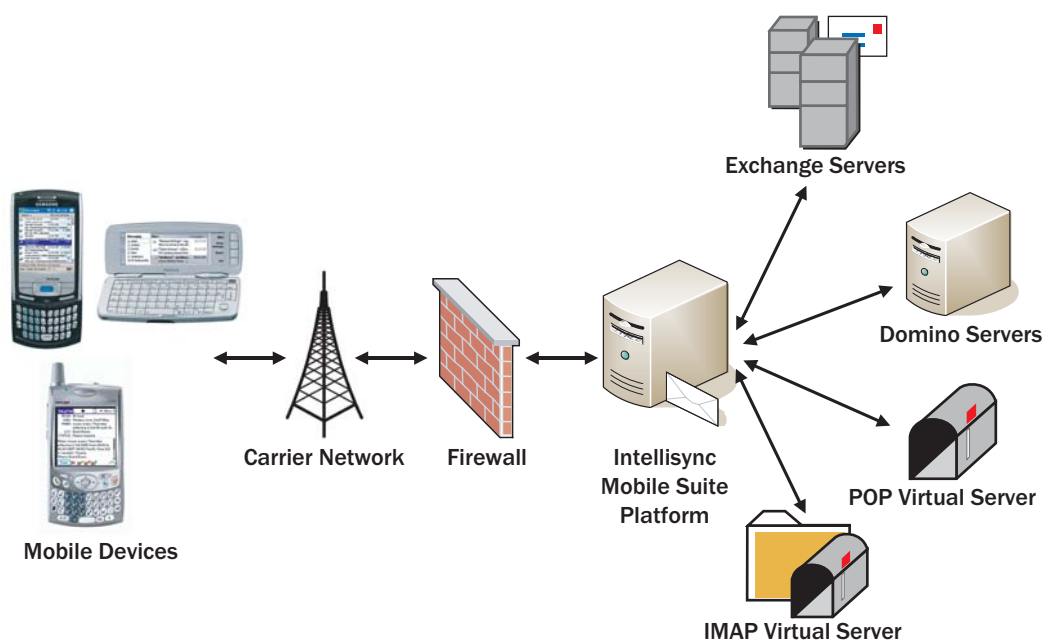
The Intellisync Mobile Suite Platform resides behind the corporate firewall. When a message arrives at the corporate email server, the Intellisync Mobile Suite Platform synchronizes a copy of the message (encrypted and compressed) to the appropriate mobile device. The Intellisync Mobile Suite Platform offers enhanced security, direct control of all server configurations and device management capabilities. The solution requires dedicated server hardware that connects with a corporate groupware server.

While there are several security options to consider and configure when implementing the Intellisync Mobile Suite Platform, the benefits of achieving greater control and configurability make this solution extremely secure for synchronizing mission-critical data.

Data Flow

Inside your enterprise network is your corporate messaging server, capable of providing email and PIM (calendar, contacts, tasks, notes) services. The Intellisync Mobile Suite Platform sits close to the corporate messaging server on the network and is connected to the mail server at all times when push is enabled. Synchronization can be initiated manually, or automatically using either scheduled intervals, or network push. Full email and PIM synchronization are supported for Microsoft Exchange and IBM Lotus Domino servers. Email support is also provided for corporate IMAP servers.

To ensure a secure architecture, the Intellisync Mobile Suite Platform establishes an outbound TCP/IP connection to the carrier network. The carrier network delivers push notifications and data to the mobile device. When the Intellisync Mobile Suite Platform detects new information on the user's groupware server, it sends a push notification to the device via the established connections. The device then establishes an encrypted session with the Intellisync Mobile Suite Platform to allow synchronization of the data.



Scalability

Mobile devices connect and register with the Intellisync Mobile Suite Platform on dedicated port. The Intellisync Mobile Suite Platform leverages this established socket to send notifications out to the mobile device. TCP traffic allowed on this TCP port is very limited and specific in purpose. This traffic contains a notification that there is new data (needing to be synchronized) on the server and it tells the device what action must be performed.

PART 2: ENTERPRISE SECURITY

In addition to the overall architecture of the Intellisync Mobile Suite Platform outlined above, there is an additional capability that enterprises can configure for their particular implementation that adds to the already strong security picture. These involve implementing a Secure Gateway in the enterprise DMZ. This section will outline these options and compare and contrast them.

Intellisync Mobile Suite Platform Secure Gateway

Some enterprise environments have strict rules regarding opening dedicated ports in the firewall to enterprise applications. The Intellisync Mobile Suite Platform Secure Gateway helps meet this requirement and will act as the “middle man”, handling synchronization traffic between the mobile device and the enterprise. The Secure Gateway is a software that provides enterprises with additional security by restricting access to the Intellisync Mobile Suite Platform that resides behind the firewall.

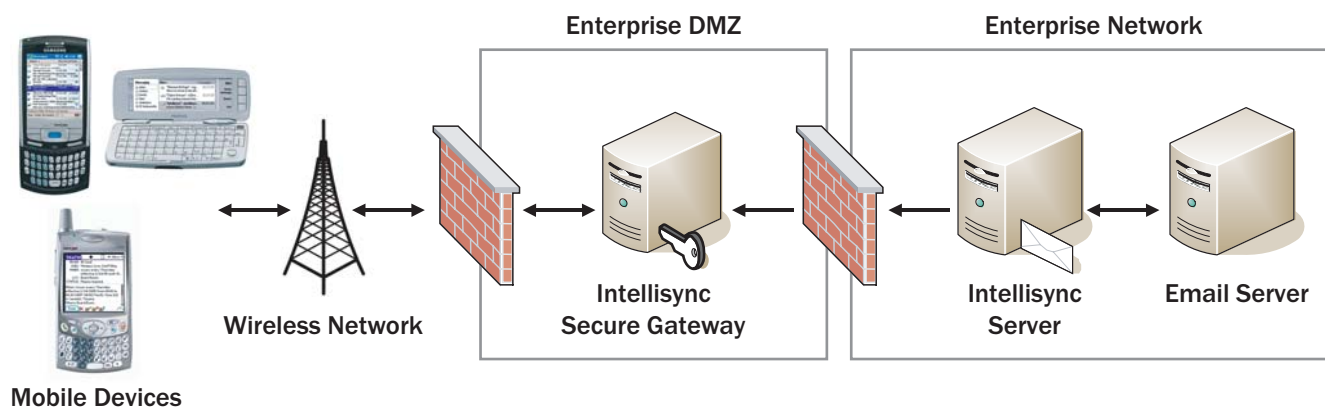
The Secure Gateway provides the ability to have only outbound-initiated connections from the enterprise for sync traffic. The Secure Gateway is 100% Java code and Microsoft IIS is not required to make it function within

your enterprise. The Secure Gateway runs on a separate locked down Windows Server residing in the enterprise DMZ.

Customers are provided with step-by-step instructions on how to deploy the Secure Gateway. When the Intellisync Mobile Suite Platform is first initiated, it sends an outbound session initiation request to the Secure Gateway and establishes a secure connection.

Whenever the Secure Gateway needs to communicate a synchronization transaction to the Intellisync Mobile Suite Platform, it does not initiate a connection through the firewall to contact the server by itself – it leverages the connection already established from the Intellisync Mobile Suite Platform to the Secure Gateway. Direct mobile device access through the firewall to the corporate network is not provided in this model.

Without the risk of any unsolicited incoming connections through open ports, Intellisync Mobile Suite Platform can effectively protect the internal network against any potential intrusions. When the Secure Gateway is the only responsible server with the capability to retrieve information beyond the internal corporate firewall, you gain a very important level of



control over the synchronization of your data. From a security standpoint, information only comes into the enterprise from a source that is trusted.

As outlined above in Part 1, when there is new information on your groupware server, the Intellisync Mobile Suite Platform will send a push notification to the device using the carrier network. This notification will let a device know it needs to sync with the enterprise server to acquire data from a specific application or set of applications (email, calendar, contacts, etc).

The mobile device does not create a connection directly to the enterprise. Instead, it establishes a connection to the Secure Gateway. Information is encrypted at your mobile device, and then transmitted to the Secure Gateway. The Secure Gateway examines the AES encrypted data and does a port and protocol change all in the DMZ. The data is not decrypted, however, until it is safely inside the corporate firewall at the Intellisync Mobile Suite Platform.

Before forwarding the data to the Intellisync Mobile Suite Platform, the Secure Gateway exercises “packet filtering” on your incoming transmission. This is done to determine that your incoming traffic is sent in a form that the Intellisync Mobile Suite Platform expects. If, for any reason, a data transmission comes into the Secure Gateway in a format not consistent with what it expects, the data stream is terminated. In order to ensure that nobody is able to spoof an authentic data transmission, the Secure Gateway has its own level of intelligence to know when data is sent in the correct format (and when it is not). Information is instantly routed through the Intellisync Mobile Suite Platform Secure Gateway to the Intellisync Mobile Suite Platform.

With the Secure Gateway in place, customers can enable access to a variety of services including GAL lookup, email access from a Web Interface, the corporate intranet, and application access for web-based applications. The Secure Gateway can offer access to any certified information allowed by the server behind the firewall. The client would use the embedded secure login procedures and encrypted key technology to communicate with the Secure Gateway when requesting information.

In summary, the Secure Gateway is a smart security server that resides in the DMZ. Its entire function is to protect data transmitted from the mobile device to the enterprise. Since there is never a direct connection from the mobile device to the enterprise, it is not possible for an attacker to exploit any connection to the enterprise used for the synchronization of mobile devices.

Enterprise Reverse-Proxy

What if your enterprise has already installed its own type of DMZ security server that monitors and filters all traffic between the Internet and the Enterprise? If this is you, then you are most likely running something like Microsoft ISA Server, Netegrity Siteminder, or Apache server inside the DMZ acting as a buffer between the outside world and your enterprise. This is another option for configuring the path used for sync traffic to get to the Intellisync Mobile Suite Platform. Intellisync customers using the Secure Gateway do not need to implement a Reverse-Proxy, but if one exists it can be used in place of the Secure Gateway.

Situated in the DMZ, the reverse proxy can be easily configured to handle all your synchronization traffic. Just like the other models, the Intellisync Mobile Suite Platform maintains a constant connection to your Exchange, IMAP, or Domino server looking for new information. When new information is received, it sends update notifications using one outbound TCP connection to the carrier network, which then immediately sends a push notification to the mobile device. The mobile device will then establish a connection to your existing enterprise reverse proxy in your DMZ using either HTTP or HTTPS. Information retrieved from the reverse proxy is immediately routed to the Intellisync Mobile Suite Platform and is synchronized with the Exchange, IMAP, or Domino server.

On the reverse proxy in the DMZ setup, the internal firewall requires inbound ports to be open so that it is able to talk to the Intellisync Server. However, the firewall can restrict the incoming connections to the DMZ machine (and that machine only.) The reverse proxy takes connections and “pretends” to be the internal server. This means that a potential hacker does not know the location of the real server. This is a perfectly acceptable way to publish web applications and is also very secure when properly configured.

During a sync operation, the mobile device routes traffic through the reverse proxy to the Intellisync Mobile Suite Platform. The user will not be able to authenticate to the Intellisync Mobile Suite Platform if he is not already connected to the reverse proxy. Data is routed immediately from the mobile device to the server creating the path across which a sync can be performed.

Deployment Strengths

The Intellisync Secure Gateway has all the capability needed to protect the corporate intranet and all applications accessed by the Intellisync Mobile Suite Platform. A definite advantage of the Secure Gateway compared to the reverse proxy method is that the Secure Gateway looks at incoming traffic to make certain it is received in an expected format that complies with normal Intellisync Mobile Suite Platform traffic. This level of packet inspection makes certain that the data stream is not falsified or spoofed by a malicious attack.

Advanced Options for More Complex Networks

The network deployment of the Intellisync Mobile Suite Platform solution is completely customizable to meet the strict requirements of every enterprise. No matter how complex the enterprise firewall configuration is, an option is available to tailor the network deployment of Intellisync Mobile Suite Platform. The value of the Intellisync Mobile Suite Platform is the ability to support advanced firewall configurations or meet strict VPN requirements.

PART 3: DATA SECURITY

How Information is Safely Transferred

Each device used with Intellisync Mobile Suite Platform requires an Intellisync Mobile Suite Platform Client. The Intellisync Mobile Suite Platform Client manages secure communication of data to and from the Intellisync Mobile Suite Platform Server and the target data store on the device. The client software includes encryption libraries for the encryption and decryption of data sent over the air.

An RSA public key that was generated during installation of the Intellisync Mobile Suite Platform is stored on the device upon installation of the Intellisync Mobile Suite Platform Client. Each client is issued the server's RSA public key upon device setup and the server securely holds its own private key. Data encrypted with the server's public key can only be decrypted with the server's private key.

Every point in the Intellisync Mobile Suite Platform architecture is secured to industry standards. For example:

- All data from a mobile device to the Intellisync Mobile Suite Platform is secured with 128-bit AES (Advanced Encryption Standard) encryption and travels via HTTP or HTTPS over TCP/IP.
- Data sent to a device connecting to the Web Portal (for PIM & email access or account management) is protected using SSL (Secure Sockets Layer) encryption in the Intellisync Mobile Suite Platform model.

Session-Based Key Exchange

Each synchronization session can generate new encryption keys to ensure security. Key exchange can be configured either to occur at every session or at pre-defined time intervals configured by the server administrators depending on the requirements of the individual enterprise. Given the nature of synchronization sessions, i.e. typically short and frequent, this makes it difficult to compromise the encryption in a meaningful way.

Password Storage

It is not required or necessary to store user passwords on the device. Since many users may synchronize more than twenty times per day, some users/companies find it helpful to cache the users' authentication credentials on the device, so that users are not required to enter a password each time they synchronize. It is not uncommon that users demand this functionality to maintain an acceptable level of usability.

If this functionality is desired, administrators can configure Intellisync Mobile Suite Platform to place a highly encrypted package of authentication credentials on the client device; this is referred to as an authentication token. If the administrator has configured the server to store the authentication credentials on the client, an expiration timestamp will be included in this token. The expiration timestamp is configured by the administrator in the profile settings of the Intellisync Mobile Suite Platform Security Section and can be configured to last minutes, hours, days or indefinitely.

- If a user authentication request returns with success and the server is configured to save user credentials, then the Intellisync Mobile Suite Platform takes the username, password, device ID, and an expiry date/time and encrypts this information using Blowfish 160-bit encryption into an authentication token.
- The key used for this encryption is uniquely generated for each server installation and stored on the Intellisync Mobile Suite Platform. Therefore, only the correct Intellisync Mobile Suite Platform can decrypt this token.
- The device ID contained in the encrypted credential prevents an authentication credential from being moved from one device to another and used for authentication.
- The server then sends this token back to the client for storage and use.

Device Security

Security is the quintessential requirement with mobile devices. If lost or stolen, they can potentially cause irreparable harm without the preventative measures inherent in this solution. The Intellisync Mobile Suite Platform provides the most advanced mobile security features and policy enforcement to cover every aspect of your mobile operations. End-to-end, military-grade encryption protects your most sensitive information from prying eyes, and theft/loss protection remotely locks down and wipes clean any lost or stolen device.

The Intellisync Mobile Suite Platform provides the capability to remotely and automatically deactivate devices and destroy data. System administrators can configure varying levels of data elimination:

- Lock out the device so it cannot sync
- Delete only email and PIM data
- Delete selected applications, files, and data
- Delete data on removable storage media
- Kill (hard reset) the device to remove all data and applications

These instructions can be pushed out to addressable devices, or can be configured to take place in a variety of circumstances automatically, for instance, if network login frequency is too low.

User Disablement

Administrators are able to “turn off” a specific user, user group or device. For example, they may turn off the account of a stolen device so that no unauthorized persons are able to sync with company servers.

PART 4: KEY AUTHENTICATION

During authentication, the Intellisync Mobile Suite Platform Server will request that the user input his password. The messaging service receives the username and password, decrypts them, and passes this information to the Intellisync Mobile Suite Platform Authentication Service. This process then opens a connection to the authentication source and attempts to validate the user. Once a successful response is passed back to the Intellisync Mobile Suite Platform all other services may now proceed. Intellisync Mobile Suite Platform supports four different Authentication Sources:

- NT Domain (NTLM)
- LDAP or Active Directory
- Intellisync Mobile Suite Platform
- Domino

It is important to note that authentication traffic does not occur between the device and the authentication source. Authentication occurs between the Intellisync Mobile Suite Platform Authentication Service and the authentication source. Administrators can choose which authentication source is used on a user-by-user basis, if desired.

Encryption is established between the mobile device and the enterprise server by exchanging session keys to encrypt the wireless information flow. A random 128-bit symmetric key is used as the seed to encrypt the username, device ID, and encryption method (AES, 3DES, SSL). A public key is used for the expected encryption method. The mobile device client then uses a pre-installed 512-bit or 1024-bit RSA public key to encrypt the random key. The encrypted random key is combined with the encrypted data packet which is then sent to the server. Only the enterprise server has the RSA private key necessary in order to decrypt these packets and decode the information sent by the mobile device.

In this system, the credentials are stored for authentication purposes. When your mobile device syncs for the very first time, you enter your password during an encrypted session. If the authentication source returns with success, then the Intellisync Mobile

Suite Platform Server takes the username, password, the device ID and an expiration date/time and encrypts this information into a "token" using Blowfish 160-bit encryption. The key used for this encryption is uniquely generated for each server installation and stored on the Intellisync Mobile Suite Platform Server; only the correct Intellisync Mobile Suite Platform Server can decrypt this token. The device ID contained in the encrypted credential prevents an authentication credential from being moved from one device to another and used for authentication.

The "token" is stored on the mobile device, and is used again and again until its expiration date/time. If a hacker attempts to move the token to another mobile device, the token is rendered useless.

Summary

The Intellisync Mobile Suite Platform has strong security built into it to support the secure exchange of information from the enterprise to the mobile device. Deploying a secure architecture that relies on a Secure Gateway or reverse proxy will stand the test of time as a solution resistant to attack.

The Secure Gateway is an excellent example of a value added component that can monitor the traffic stream from the internal to the external wireless network to ensure it is not possible for anyone to spoof an authentic traffic stream for the purposes of deceiving the server's ability to identify information from valid mobile users.

The goal is to keep corporate information private. The security models described in this paper ensure that you will be able to effectively sync information with mission-critical systems without fear of interception or falsification of your data stream. Making certain that the wireless medium is secure grants you the ability to turn the problem of mobile data access into a safe solution.

APPENDIX A: INFORMATION ON ENCRYPTION ALGORITHMS

End-to-end, military-grade encryption protects your most sensitive information from prying eyes. The Intellisync Mobile Suite Platform provides highly secure end-to-end communication sessions. Anyone attempting to “eavesdrop” on communications between the Intellisync Mobile Suite Platform Server and the mobile device will not be able to successfully intercept and decode the data which is being transmitted.

The Intellisync Mobile Suite Platform allows administrators to select the encryption options that best meets their need for balancing level of security with communications efficiency. Administrators may assign different encryption options to different profiles. The following standard options are available:

- 3DES (FIPS 140-2 validated)
- AES (FIPS 140-2 validated)
- SSL

In addition, the key encryption process uses the Blowfish encryption method. Specific information on each of these encryption algorithms is outlined below.

Blowfish

Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as an alternative to existing encryption algorithms. Designed with 32-bit instruction processors in mind, it is significantly faster than DES. Since its origin, it has been analyzed considerably. Blowfish is unpatented, license-free and available free for all uses. Blowfish is currently used in over 150 products, and has been added to the mainline Linux kernel, starting with v2.5.47.

AES

AES succeeds the aging DES and Triple DES standards, which are encryption algorithms that provide 56 and 112 bits of security, respectively, and were approved for use by US Federal agencies. A new robust encryption algorithm was needed to replace them since DES, created in the 1970s, can no longer meet the demands of high security, high performance and public key cryptography systems.

AES is the only symmetric encryption algorithm providing a minimum of 128 bits of security that is approved for use by US government organizations to protect sensitive information. AES comes in three strengths: 128 bits, 192 bits and 256 bits. The 128-bit strength should provide 20 to 30 years of protection. The higher strengths are available for even greater protection.

Surprisingly, not only does AES provide more security than Triple DES, it also has better performance. Better performance and better security make AES a highly attractive alternative to 3DES.

AES, Public Key Crypto and Elliptic Curve Cryptography

In a public key cryptography environment, you must use a matching level of security for your digital signatures and key exchange as you use with the symmetric encryption scheme, such as AES (128, 192 or 256 bit). Otherwise, the symmetric encryption mechanism can be compromised through the weakness of your public-key.

There are two ways of generating public keys and digital signatures that offer AES equivalent security, but the two methods use vastly different key sizes. The first method is using RSA public-key technology and the second is using Elliptic Curve Cryptography (ECC).

At 256 bits, AES demands an RSA key size of 15,360 bits for equivalent security. This would bring almost any system to its knees. By comparison, ECC keys are only 571 bits and would have negligible impact on performance.

NIST has approved ECC as a public-key cryptography technique for digital signatures used by the US government in FIPS 186-2. The next step is for NIST to approve ECC for key management as well.

3DES

Also known as Triple DES (Data Encryption Standard) – this NIST-standard cryptographic cipher that uses a 56-bit key. Adopted by the NIST in 1977, it was replaced by AES in 2001 as the official standard. DES is a symmetric block cipher that processes 64-bit blocks in four different modes of operation, with the electronic code book (ECB) being the most popular.

3DES offers increased security by adding several multiple-pass methods; for example, encrypting with one key, decrypting the results with a second key and encrypting it again with a third. However, the extra passes added considerable computing time to the process. DES is still used in applications that do not require the strongest security.

SSL

SSL (Secure Sockets Layer) is used as the predominant security protocol on the Internet. Developed by Netscape, SSL is widely used to securely send sensitive data over a public network. When an SSL session is started, the Web server sends a digital certificate to the browser, which is used to authenticate the Web site. The browser maintains an inventory of the certificates of public certificate authorities (CA) and is able to contact the CA to see if the certificate has been revoked.

The client device (web browser) uses the public key from the Web site to encrypt a random number and send it back to the Web site. The random number may be used intact or modified to create a secret session key for the subsequent exchange of private information.



ABOUT INTELLISYNC CORPORATION

Intellisync Corporation (Nasdaq: SYNC) is a leading provider of wireless email and mobile platforms to large enterprises, mobile operators, software providers and device manufacturers. Intellisync has won the mobility industry's top awards by providing seamless synchronization; secure wireless email, device management and mobile data access software that connects nearly every device, data source and application available.



CONTACT US

For more information on Intellisync mobility solutions, please call +1.408.321.3800 or +1.800.224.5430, or visit www.intellisync.com to locate an office near you.



© Copyright 2005 Intellisync Corporation. All rights reserved. Intellisync, Mobile Suite, mobility unlimited and the Intellisync logo are trademarks of Intellisync Corporation that may be registered in some jurisdictions. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners. The specifications and features contained in this document are subject to change without notice. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means without the express written permission of:

Intellisync Corporation
Marketing Department
2550 North First Street
San Jose, CA 95131

This publication is provided as is without warranty of any kind, express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This publication could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. These changes will be incorporated in new editions of the publication. Intellisync Corporation may make improvements and/or changes at any time to the product(s) and/or the programs(s) described in this publication.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Intellisync Corporation cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.