

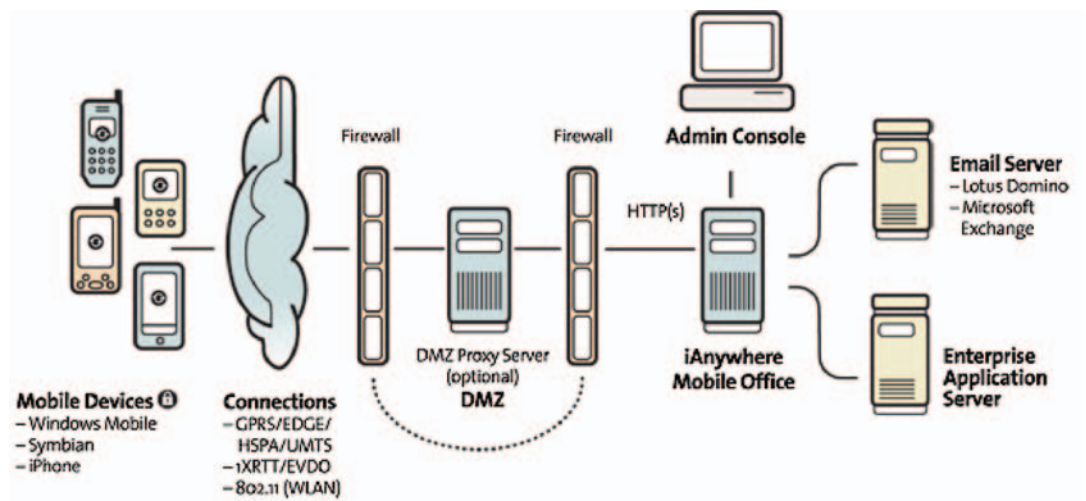
iAnywhere Mobile Office for iPhone Security Overview

TECHNICAL BRIEF

With the increasing popularity of the Apple iPhone (and its Wireless LAN cousin, the iPod Touch), pressure has mounted on enterprise IT to allow these devices to access corporate data. From a user perspective this may be a great thing, but for corporate IT there are numerous challenges that have to be overcome in order to provide services that meet the strict standards for the protection of sensitive data while still being useful for the end user.

The purpose of this whitepaper is to describe the secure messaging and collaboration infrastructure provided by iAnywhere Mobile Office.

iAnywhere Mobile Office, a product of Sybase, is specifically designed for today's mobile business workforce. It combines fully integrated wireless email and PIM data with on-device security and business process mobilization. iAnywhere Mobile Office enables organizations to manage critical, time-sensitive workflow business processes. iAnywhere Mobile Office offers key features that provide the foundation for a company's "mobile inbox of the future".



Operating on the networks of all major carriers worldwide, iAnywhere Mobile Office extends email and PIM data to iPhone and iPod Touch devices as well as the latest Windows Mobile and Symbian powered devices.

- Usability – iAnywhere Mobile Office provides instant email delivery and rich PIM functionalities without requiring any special software knowledge. Highly optimized protocols ensure minimal impact to battery life.
- Administration – Over-the-air client provisioning and deployment, automatic unattended software upgrades and intuitive configuration tools make day to day operation easy. iAnywhere Mobile Office allows the use of standard service monitoring tools.

- Low cost of ownership – Optimized protocols minimize wireless air time requirements and data transfer costs. The use of standards for service monitoring and the automatic client upgrades reduce support costs. The iAnywhere Mobile Office architecture allows for extended scalability to reduce hardware requirements for globally distributed enterprise deployments

The purpose of this document is to address the mechanisms provided within iAnywhere Mobile Office that allow enterprises to securely provide a messaging and collaboration solution to a broad and diverse fleet of mobile and wireless devices. In particular, the following questions will be answered:

1. How can an enterprise provide access to wireless email to some users without providing it to everyone?
2. How access to email from rogue devices be controlled?
3. How can an enterprise deliver email in a way that is not susceptible to eavesdropping?
4. What architecture can an enterprise use that meets the needs of enterprise security?
5. How does an enterprise ensure that, once email is delivered, that the risks of unauthorized access and/or device loss are minimized?
6. In the event that a device is lost, how can an enterprise remove corporate data remotely?

The iPhone represents a layer of challenges over and above those present on other devices. Some are technical in nature, but other challenges are psychological, having to do with a conflict between what IT and the users view as the core use case of the device. Understanding the Sybase solution for iPhone requires a deeper understanding of our approach on the device, beginning with the definition of an enterprise sandbox.

ENTERPRISE SANDBOX – DEFINING THE SECURITY BOUNDARY

Prior to the introduction of the iPhone, the majority of enterprises pursued a strategy of purchasing devices and airtime plans for their users. There are numerous benefits in that approach, from more advantageous pricing discounts to an increased likelihood that the user will report the device stolen if it is indeed lost. However, it carries with it an obvious financial burden on the enterprise. The iPhone has allowed, and indeed in some cases required, enterprises to approve and support devices that are owned by employees.

The acceptance of the iPhone in the enterprise does not come without some risk. In general the risks are associated with the mindset of the user. While it's often the case regardless of who purchases the device, an iPhone user tends to regard the device as personal property. As such, he views that there should be limits to what levels of control that IT should be able to enforce in managing and securing the device. But in order to allow enterprise data on a device, enterprise IT must be able to do so in a manner that represents an acceptable level of risk.

A solution that addresses the needs of both end users as well as enterprise IT therefore has several challenges to overcome:

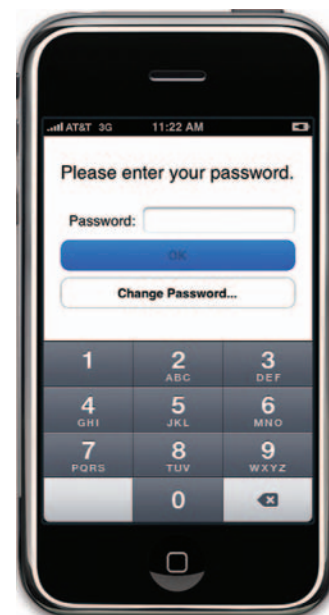
- How to “secure” the enterprise data without controlling the device
- In the event that a company needs to remove the “enterprise” data on a user’s iPhone they need to be able to do so without affecting the users “personal” data and applications on that same iPhone

Sybase was able to overcome both of these challenges at once through the introduction of iAnywhere Mobile Office and its unique enterprise sandbox approach. The concept of a “sandbox” originated in the Java development world, and basically referred to the ability for a program to have full access to its own environment (the sandbox), while at the same time being restricted, either completely or at least partially from the outside environment, such as the operating system and system resources.

By using a similar sandbox approach within iAnywhere Mobile Office, Sybase is able to delineate between what is corporate owned and delivered and what is employee owned and delivered. There is a natural separation between the two types of data. Enterprise IT can enforce security policies, but they only apply to the enterprise sandbox. IT can enforce encryption, but it only applies to the sandbox. IT can wipe a device, but only wipes the sandbox. The rest of

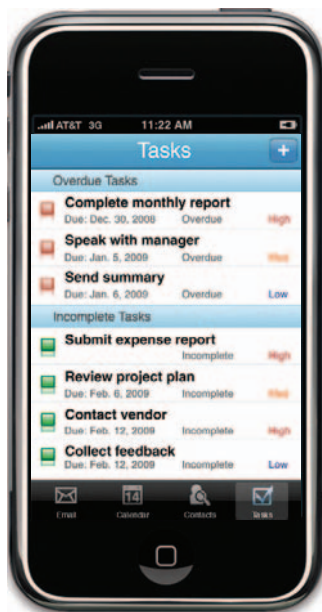
the device, the “consumer half” of the device is untouched, allowing Sybase to walk the difficult line of providing enterprise security services to a personally owned device.

How is that implemented on the device? Simple. Sybase provides an application that is free to download from Apple’s App Store. A search for “iAnywhere” or “Sybase” will return a single application that can be installed onto the device. Once configured, the user accesses the iAnywhere Mobile Office application:



Once authenticated, the user is permitted to access the iAnywhere Mobile Office application and the protected contents stored within. The application contains several components: email, contacts, calendar and tasks. All data stored within the application sandbox is protected with multiple measures, and no data can be stored outside the sandbox on the device.

The enterprise sandbox is only the first of many security-focused features in the iAnywhere Mobile Office solution.



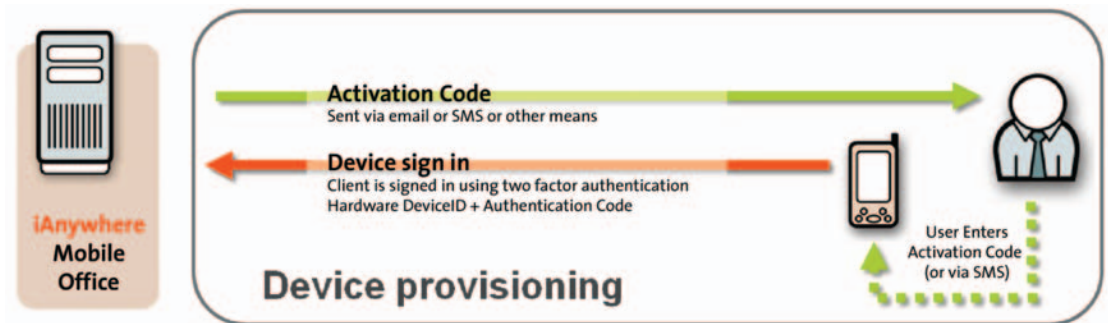
SECURE ACTIVATION

The first step in providing a secure architecture is ensuring that only the devices desired to be part of the system are allowed in. iAnywhere Mobile Office delivers this capability through its enterprise provisioning mechanism. This is built on a basic white-list paradigm where, by default, no access is provided unless explicitly granted by an administrator. The process works as follows:

1. A user requests access to his corporate email.
2. In the Mobile Office Administration tool, an administrator searches through either the Domino or Exchange directory for the user requesting registration.
3. As part of the registration process, an activation code is generated. This code can either be automatically generated or manually entered by the administrator. There are several key features of the activation code process:
 - a. The code expires (the default expiration period is 72 hours but can be manually changed by the administrator).
 - b. The administrator, at his discretion, can choose to include or not include the registration code in the device notification. If the registration code is not included as part of the device notification, another secure out-of-band communication sequence would take place.

- c. The activation code data is now stored in the encrypted database, the secure sandbox on the iPhone, on initial connection. A “dummy” activation code is put in the settings screen in place of the real activation code once it has been moved. This eliminates any potential risk of special software that can be used to break Apple’s built-in operating system security.
4. During the registration process, the administrator has the ability to send the server settings (and optionally the registration code) to the device via an SMS or email message. For non-iPhone devices that information would be automatically read by the device client and provisioned into the device application. For iPhone, the settings must be entered manually.
5. Once registered, the status will display in the Mobile Office Admin tool. Additional hardware and software information is collected. If at any point an administrator decides that the account should cease to receive email, he can simply right click on the client and select either “Remove” or “Send Kill Pill”. Removing the device simply deletes the entry from the admin view, rendering the activation code invalid. The device is unaffected with the exception that it will no longer receive email.

The following diagram illustrates the process.



Implementing this secure activation procedure ensures that only approved devices are allowed access to the iAnywhere Mobile Office solution.

NETWORK ARCHITECTURE

As with any mobile and wireless solution, enterprise IT and in particular firewall administrators are faced with a dilemma – how do I provide access to enterprise data in a way that doesn’t a) open up unnecessary inbound ports into the environment and/or b) doesn’t allow the staging of data anywhere except for the device and the secure network space?

Sybase has two solutions that independently address both of these requirements. The native solution, included as part of the iAnywhere Mobile Office core architecture, is the Mobile Office DMZ Proxy. The second is the Sybase Relay Server. While essentially the same security challenge, the solutions approach and solve the problem differently – one approach is specific to Mobile Office in particular, while the other is a shareable component, reusable across all Sybase mobile and wireless solutions.

The right solution for a particular enterprise depends largely on its specific requirements, but the concept for both solutions contains the same key elements:

1. The client device does not connect directly to the iAnywhere Mobile Office server, but instead is routed through an intermediary component hosted in a DMZ.
2. The DMZ component requires no inbound ports to be opened into the real network space, and doesn’t stage any sensitive data.
3. In order for the solution to function, the iAnywhere Mobile Office server must first initiate a connection to the DMZ component. All client-to-server communications are subsequently tunneled through this outbound initiated, bi-directional communication.
4. Client communications are encrypted at the packet level, thus eliminating any vulnerability introduced by protocol conversion (e.g. the WAP Gap issue).

iAnywhere Mobile Office DMZ Proxy

iAnywhere Mobile Office uses a token/proxy relationship that provides the enterprise with an additional level of protection. A token is a user-defined string that is configured on the iAnywhere Mobile Office server. The token effectively acts as a license, allowing the machine that is running the iAnywhere Mobile Office server to connect to one or more DMZ proxies. Each iAnywhere Mobile Office server must have its own token. Once it is used on a server, a token cannot be transferred or reused on a different server.

The token must match a separate user-defined string within the proxy settings access list on the DMZ proxy. If the token for iAnywhere Mobile Office does not exist on the DMZ proxy that it is configured to connect to, communications between the two machines will be disallowed, preventing unauthorized intrusion.

How the DMZ Proxy Works

The DMZ proxy component can be installed within a corporate DMZ or Firewall gateway to increase security for devices connecting to the email server from outside the corporate network. The DMZ proxy is a proxy server, or an application-specific firewall, for iAnywhere Mobile Office. Because it functions as a reverse proxy, the DMZ proxy simplifies setup of filters and firewalls, enhances security, and facilitates auditing, intrusion detection, or usage monitoring.

Note: A reverse proxy dispatches in-bound traffic to a set of servers, presenting a single interface to the client. A reverse proxy is useful for load-balancing a cluster of servers. In contrast, a forward proxy acts as a proxy for outbound traffic.

The DMZ proxy understands the iAnywhere Mobile Office protocol, examines and authenticates each connection, and checks iAnywhere Mobile Office protocol packets for validity. Invalid connections from the Internet to the corporate network are disallowed. The iAnywhere Mobile Office server can be configured to define which DMZ proxy to connect to, which ports are used to connect to the proxy, and which protocol is used (HTTP or HTTPS). If configured to do so, the iAnywhere Mobile Office server connects to the DMZ proxy from the corporate LAN, eliminating the need to allow connections from the DMZ or Internet to the LAN for iAnywhere Mobile Office traffic.

Tokens

Each server connecting to the proxy must have a unique token value that is known to the proxy. The token must be configured on both the iAnywhere Mobile Office server and the DMZ proxy to allow communications.

The Token Management screen (Install Wizard) is used during the iAnywhere Mobile Office server installation to configure the server's token. Valid tokens are registered using the Proxy Settings utility. By default, the server token is Token_o. If a proxy is to be used, the default token should be changed during installation. The DMZ proxy will not only validate the token but also associate the token with its connecting server. The same token cannot be used by more than one server. Also, once used on a server, tokens cannot be transferred or reused on a different server.

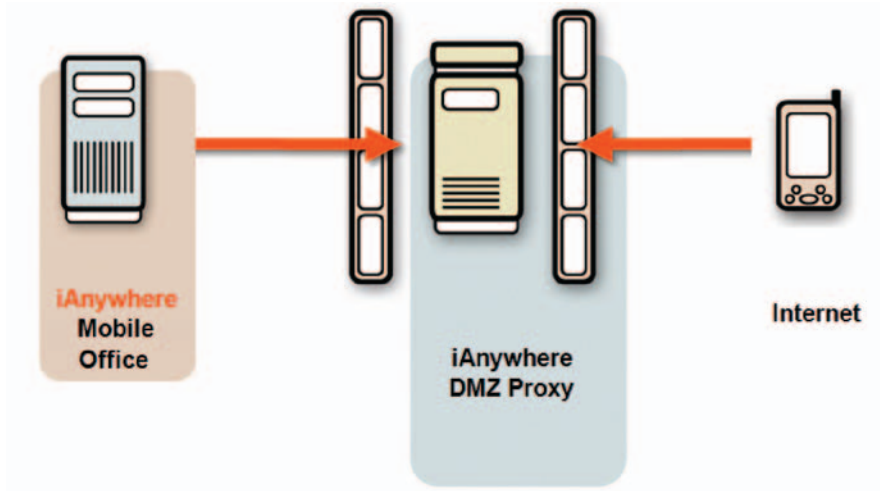
Company ID

Company IDs are used to route client traffic to a specific server. The Company ID is a string that is entered during configuration of the server and the user's mobile device to identify the iAnywhere Mobile Office server to which the device will connect. Whenever a device sends iAnywhere Mobile Office data to an iAnywhere Mobile Office DMZ proxy, the Company ID is attached. The proxy uses this information to route the traffic to the correct server.

The Company ID is considered an attribute of the server. It is configured wherever the port is configured, both on the server and on the device. On the server, it is modified in the HTTP Settings application where the server listening port (or ports) is edited. On the client, it is modified in the Connections dialog where the port and server name are also edited.

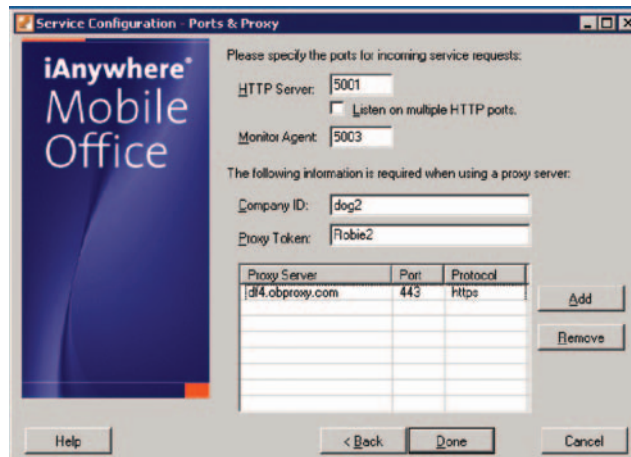
By default, the value of the Company ID is 0. Any server or device that does not explicitly configure a different Company ID will use 0. This permits out-of-the-box functionality for the default proxy/server/client configuration without the need to specifically configure the Company ID settings on the mobile device.

Note: The Company ID must be a string consisting of characters A through Z (upper or lower case) or numbers 0 through 9.

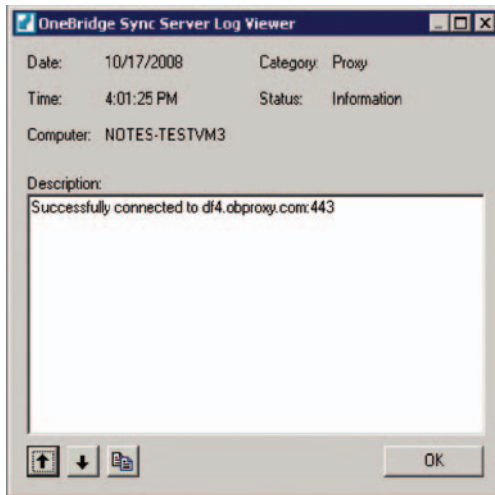


DMZ Proxy Registration Process

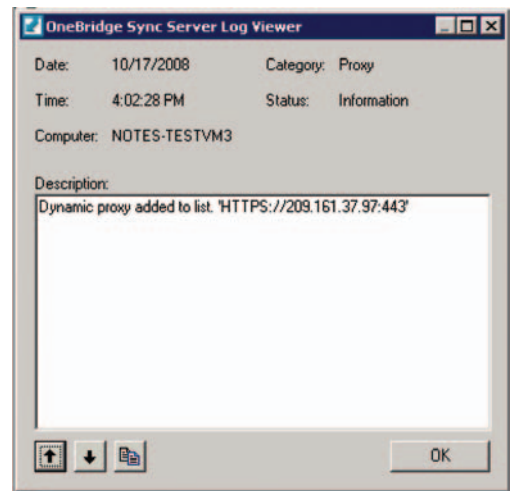
When the iAnywhere Mobile Office Server starts, it must register itself with a particular DMZ Proxy. Ensuring availability however will often require that a single Mobile Office server be able to communicate with one of several DMZ Proxy Servers. This process is accomplished as follows:



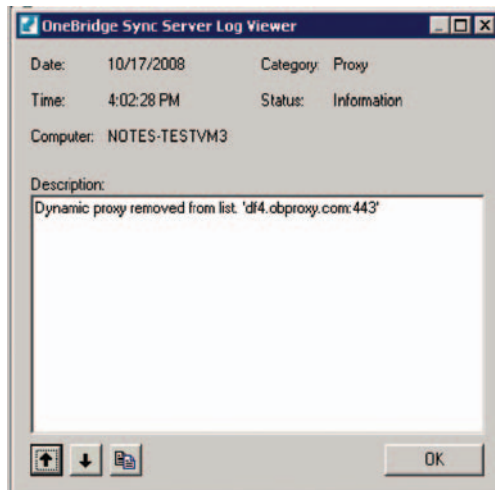
1. As part of the setup process, an administrator enters proxy and token information for a specific DMZ proxy. In evaluations, this is often a proxy server hosted by Sybase but in a production environment this would be one server in the DMZ:



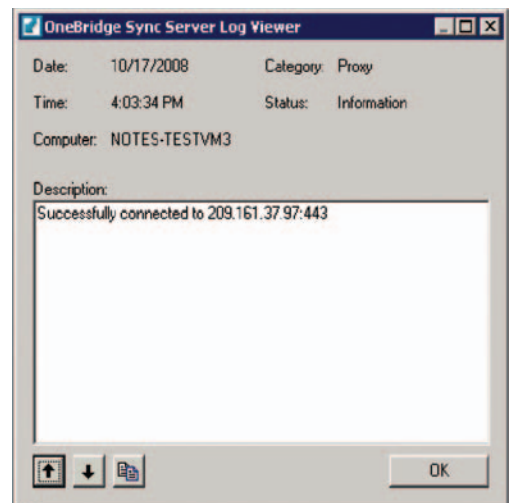
2. When the server service starts, the proxy defined during the setup process is contacted, and the token information is verified.



3. The Mobile Office Server receives a new list of valid Proxies from the initially contacted DMZ Proxy and dynamically adds those entries to its initial list.



4. The Mobile Office server removes the Proxy from the list that was entered as part of the setup process:



5. The Mobile Office server establishes a connection to all Proxies that were downloaded from the initially configured Proxy server:

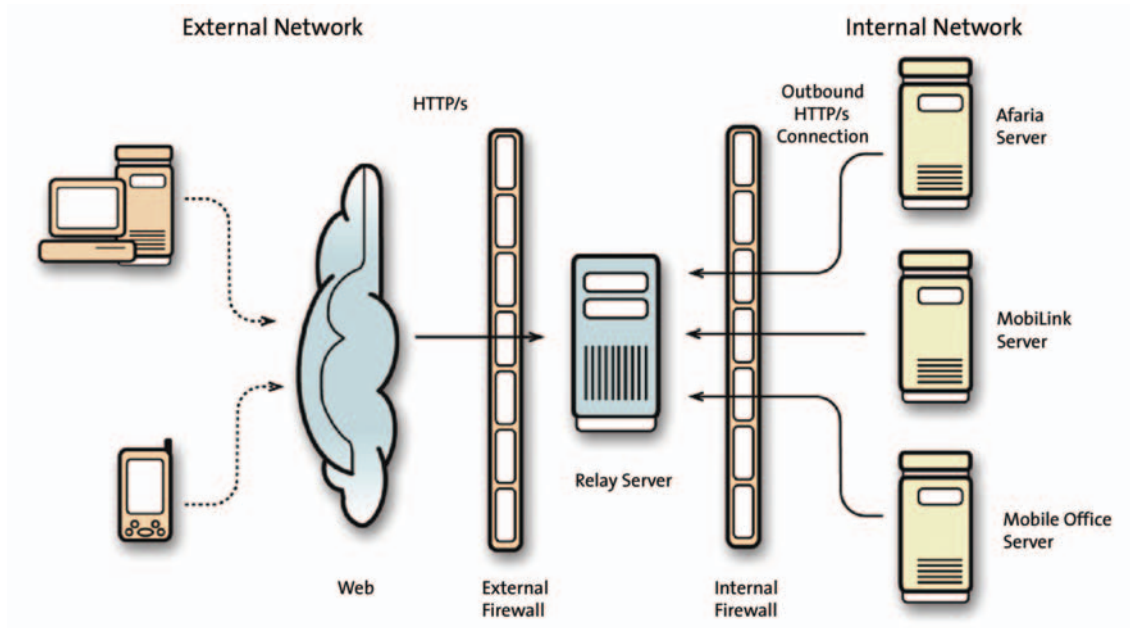
Sybase Relay Server

The Sybase Relay Server represents a more product-independent approach to solving the connectivity and data staging issues. As mentioned previously, preventing inbound ports and the staging of interim data outside of the secure network space while still delivering a viable solution is not an issue that is isolated to iAnywhere Mobile Office. Sybase recognized this fact, and the Relay Server addresses the issue not only for iAnywhere Mobile Office, but for the other industry-leading Sybase products – Afaria, SQL Anywhere/MobiLink and Sybase Unwired Platform.

Architecturally speaking, the Sybase Relay has four basic parts:

1. Client software designed to recognize that a relay may be part of the environment.
2. The relay itself, which is essentially a web plug-in for either IIS or Apache. A key element to a secure implementation is a data file configuring the number and types of backend servers that will be connected to. The Relay Server architecture supports both the use of Tokens, as well as MAC address restrictions to prohibit unknown backend systems from being exposed. Connectivity to the Relay Server can be accomplished through either HTTP or HTTPS.
3. The Outbound Enabler. This process, which is independent from the backend solution being supported, ultimately is what provides end-to-end connectivity. The Outbound Enabler (OE) must make a successful connection to the Relay Server, passing the correct configuration information (such as Token, a valid MAC Address and Certificate information if SSL is being used) to establish a handshake with the Relay. Only once established will information be able transfer to and from the remote client to the backend system.
4. The backend system itself. Communication comes from client systems, routes through the relay to the outbound enabler, and ultimately terminates at the backend system.

Once a successful communication pathway is established, the actual operation of the relay in the iAnywhere Mobile Office environment is relatively simple in that it acts as a forwarding mechanism for traffic originated from client systems.



TRANSPORT ENCRYPTION

Email can and often does contain sensitive information. Protecting that information in a way that is not susceptible to eavesdropping or tampering, even if the data has to go through an intermediation point, is critical to delivering a secure solution.

iAnywhere Mobile Office uses a combination of symmetric and asymmetric key encryption to ensure data privacy. Asymmetric key encryption is accomplished using a 1024-bit key along with RSA OAEP encryption. Bulk, or symmetric key encryption, is accomplished through the use of industry-standard and FIPS 140-2 compliant 128-bit AES-CFB for payload encryption.

Encryption keys are based and rotated on a “per message” basis versus a “per session” basis. A “session” can be thought of as the communication required to transmit one PIM item, such as an email. A typical session to receive one email will contain between two and four individual messages, each encrypted with its own encryption key. This method ensures key rotation and avoids the type of key stagnation challenges typically associated with wireless technologies such as WEP.

The following example is a step-by-step overview of iAnywhere Mobile Office’s transport encryption. For simplicity sake, it assumes either a direct connection to the iAnywhere Mobile Office server or one that is proxied through the Relay Server architecture:

1. When the client starts up if it doesn’t already have public key info for the server (or proxy) it is configured for, it sends a GetKeys command to the server.
2. The server responds with its public key.
3. Upon the initiation of the dialogue the client generates a symmetric (currently AES 128-bit) key, C1. For the iPhone, this key is generated via the built in iPhone SDK API SecRandomCopyBytes. It also generates the “next” symmetric (currently AES 128-bit) key to be used in the revolving key chain sequence, C2.
4. The client encrypts C1 along with some other client header information with the server’s public key. A “private header” is created.
5. The client appends C2 to the rest of the payload and encrypts the entire contents with C1.
6. When the server receives the message, it decrypts the private header with its private key. With the newly decrypted C1, it decrypts the payload, including C2.
7. The server creates its own AES 128-bit key, S1.
8. The server encrypts the private header with C2.
9. The server appends S1 to the rest of the payload and encrypts the entire contents with C2.
10. When the client receives the message, it decrypts the private header with C2, which it already had. It also decrypts the message payload, giving it access to S1.
11. The client creates a third key, C3.
12. The client encrypts the private header with S1, appends C3 to the payload and encrypts the entire contents with S1.
13. When the server receives the message, it decrypts the private header with S1, which it already had. It also decrypts the message payload, giving it access to C3.

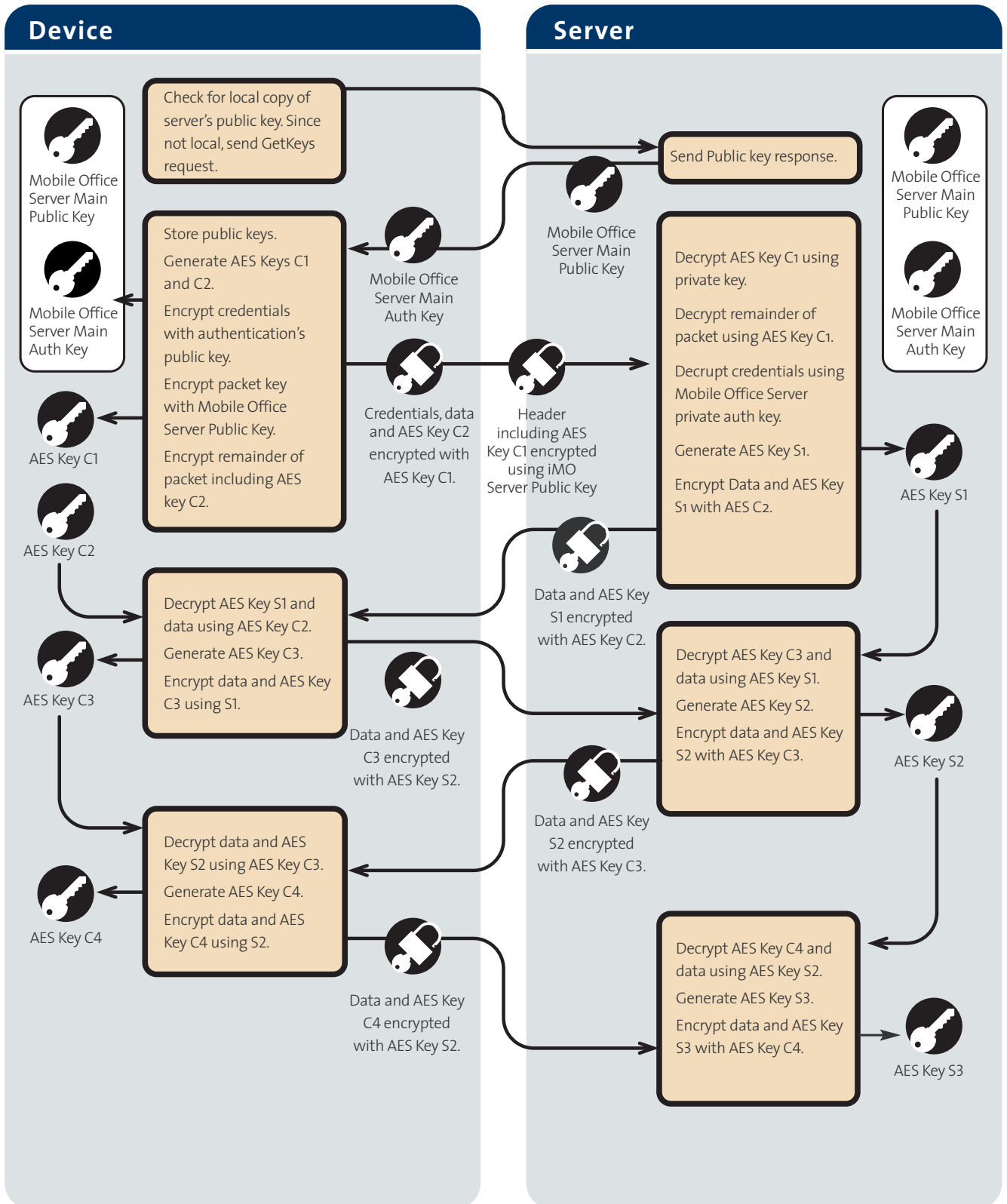
This process of revolving symmetric keys occurs until the session is over. When a new session begins the complete process is repeated excluding the “GetKeys” call as the client already has the server’s public key.

The communications process is covered under the protection of US Patent 7281128. For more detail reference <http://www.patentstorm.us/patents/7281128.html>.

The following is a graphical representation of the process:

DATA AT REST ENCRYPTION

At this point, we've accomplished the following:



1. Ensured that only authorized iPhones (all devices actually) have access to the iAnywhere Mobile Office solution.
2. Delivered a solution that does not require any inbound ports into the real network space.
3. Prevented temporary or staging data from being stored outside the real network space.
4. Delivered a secure transport mechanism, immune to the WAP Gap.

Ultimately, however, data WILL be allowed to leave the enterprise, which leaves enterprise IT with an additional challenge – how do I secure the data that resides on the iPhone? With handheld security there are typically two layers of protection (excluding tertiary mechanisms like kill-pill) of proactively protecting device data:

1. Password Protection
2. Encryption

Providing password protection is almost always considered necessary, but in many cases isn't considered sufficient protection. Combining application data encryption in addition to application password protection provides the most secure solution for the enterprise.

The inability to encrypt the native iPhone PIM stores at the application level weakens the device security model. An unlocked or "jail-broken" device allows any user full, unencrypted access to the devices data stores.

This is where the iAnywhere Mobile Office enterprise sandbox concept plays a pivotal role. On the iPhone, as with all of the iAnywhere Mobile Office enabled devices, Sybase is able to deliver BOTH password protection as well as application data at rest encryption, delivering the multi-layered approach necessary to provide enterprise security.

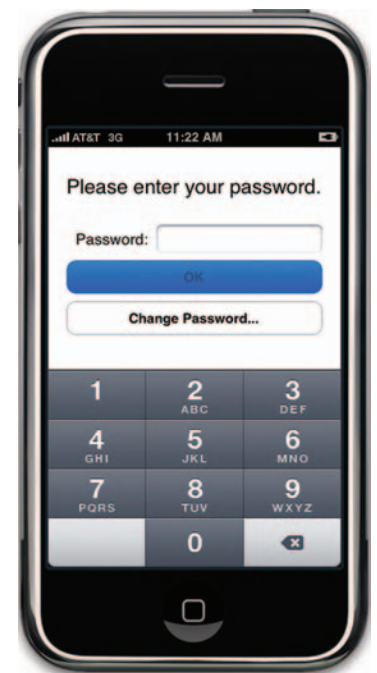
Password Protection

While encryption is handled automatically, the level of password protection is left to the administrator to define. A key differentiator to this solution is the concept of when exactly the user is prompted for the password. The iAnywhere Mobile Office password is not a device-level password – it is only required when the user attempts to enter the iAnywhere Mobile Office application:

In fact, there is nothing preventing a user from having both a device-level password and an iAnywhere Mobile Office password. They are completely independent. In terms of configuring the password, there are currently three levels of protection that are offered:

- None – this is the most basic protection and brings with it the assumption that the administrator has either deemed passwords unnecessary or has implemented a different mechanism for enforcing authentication. No sandbox password is required, although encryption is enforced.
- Medium – this mid-level password setting requires a password that is 4 digits long, and requested if there is 10 minutes of inactivity within the iPhone application. If the user enters the password incorrectly 99 times, the entire contents of the sandbox are deleted.
- High – the highest level of security, this password setting requires a password that is 6 digits long, and is requested every time the user attempts to enter the Mobile Office application. If the user enters the password incorrectly 15 times, the entire contents of the sandbox are deleted.

The password itself is stored within the enterprise sandbox, encrypted using 128-bit AES (described in the next section). If the user enters his password incorrectly more than the number of times allowable by the threshold, the entire contents of the sandbox, including the native contacts store, can be removed as described in the "Sandbox Wipe/Kill Pill" section.



Encryption

Rather than attempting to write iAnywhere Mobile Office data to the native PIM databases, Sybase created its own data storage facility leveraging SQLite as the underlying storage mechanism. In order to read and write encrypted data to this database, Sybase has also licensed the SQLite Encryption Extension (SEE).

This allows encryption to be managed and administered centrally to separate PIM data elements, stored essentially as tables within the database. The encrypted database has the following features:

- 128-bit AES – OFB encryption.
- The encryption key itself is generated through the use of the built-in iPhone SDK API SecRandomCopyBytes. This function reads from /dev/random to obtain an array of cryptographically-secure random bytes.
- The encryption key is stored in the iPhone equivalent of the Mac OS keychain and is accessible only via our application identifier. This is the process recommended by Apple.

Sybase reads data as necessary into memory. For example, when the application is first loaded, the first 25 email items are loaded into memory. At this initial state, all other PIM information remains encrypted. Calendar information is not loaded until the calendar is accessed, and only the information necessary to present the initial view is loaded. Only as additional information is necessary is it loaded into memory. When the application is exited, Apple native functionality causes any unencrypted information stored in memory to be flushed, leaving the data on the device completely protected.

The focus of this whitepaper has been specifically on what is stored within the iAnywhere Mobile Office iPhone encrypted sandbox. The one exception is the “contacts” data store. A user’s personal groupware contacts are synchronized to the native iPhone contacts store. This allows critical native iPhone applications such as the dialer/lookup, callerID, and call history applications to function as designed. This does however prevent the iAnywhere Mobile Office application from providing application-level encryption for the user’s personal contacts on the iPhone. If this is of major concern to the enterprise, iAnywhere Mobile Office can be configured to not deliver contact data to the device. The users would then still have access to the Corporate Directory Lookup application within the Mobile Office contacts screen. The Corporate Directory Lookup application provides users with secure dynamic access to their entire companies address book.

Even though contacts are not stored inside the iAnywhere Mobile Office sandbox, their contents are affected by the actions performed by both password validation failures as well as the Sandbox Wipe procedures.

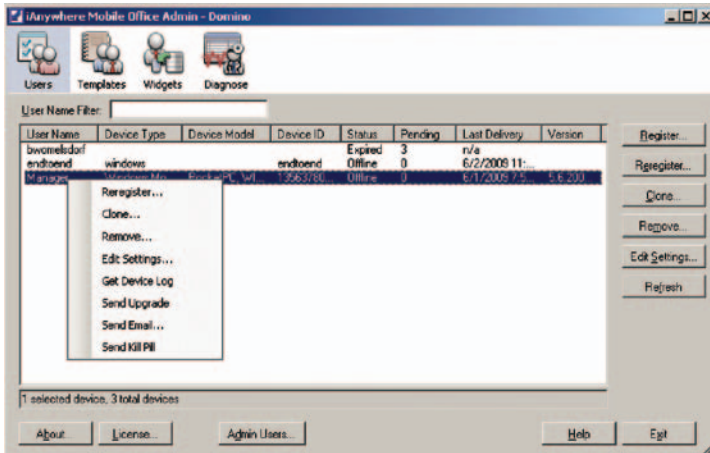
SANDBOX WIPE/KILL PILL

Undoubtedly during the course of normal operations, devices get lost. And today’s reality tells us that the individual attempting to log into a device may not be the one that is supposed to do so. For that reason, Sybase provides the capability to wipe the sandbox clean if the need arises.

iAnywhere Mobile Office stores data in the following locations as part of normal operations:

- The encrypted SQLite database
- The iPhone “keychain”
- The native Contacts db (optionally)
- The iPhone settings area

The Sandbox Wipe process is the procedure whereby the entire contents of these data stores are erased. There are two situations in which a Sandbox Wipe can be initiated, during password validation failure, and in the case of an administrator initiated Kill Pill.



The iAnywhere Mobile Office application itself is not affected. In instances where the user relocates his device, he simply requests a re-registration on the iAnywhere Mobile Office server, and he will once again begin functioning normally.

As important as it is to know what is wiped during this operation, it is also important to know what is preserved – the user’s personal data. The “user’s half” of the device, is unaffected. This allows the enterprise to protect the data that it owns, while leaving the user’s owned personal data such as iTunes songs, movies, and App Store applications alone.

SUMMARY

Mobile computing opens up a world of potential. The ability to deliver services, make real-time decisions, respond to customer requests and dynamically re-route personnel to a more effective location provides real financial and business advantages. And adding iPhone into the mix represents an exciting opportunity for both end users as well as enterprises. None of it comes, however, without risk. Enterprises must balance functional requirements with the need to protect enterprise information.

The iAnywhere Mobile Office solution allows enterprises to integrate iPhones, as well as a multitude of other device platforms, safely and securely with a variety of security features, all integrated into an industry-leading collaboration platform.

Through an effective implementation of iAnywhere Mobile Office, enterprises can enable their end users while still protecting the intellectual assets that serve to make them successful.

For more information, please visit <http://www.sybase.com/mobileoffice>.