SYBASE®

Feature Guide

Sybase mBanking 365®

3.0

DOCUMENT ID: DC00785-01-0300-01

LAST REVISED: June 2010

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

Contents

CHAPTER 1

Features and Functionality

This chapter describes Sybase® mBanking 365® features and functionality.

Introduction

Increasingly, users are demanding access to a broad array of financial services centered around convenience and ease-of-use. At the fore of such demand is the desire for mobile access to banking services. Financial institutions must work to meet consumer demands while, at the same time, improving their return on investment (ROI).

Sybase mBanking 365 enables financial institutions to satisfy user demands while improving ROI. mBanking 365 provides users with access to bank services such as payments, transfers, alerts, and summaries through their mobile devices, ensuring mobility and convenient banking access. It also enables your financial institution to provide the features and functions that users demand for mobile banking technology, including multiple delivery channels and enhanced security. mBanking 365 provides complete flexibility and control through its fully customizable interface, configuration options, and built-in internationalization capabilities:

- Improved customer retention – personal and immediate interaction with customers, directly through their mobile devices.
- Increased customer contact points – allows users to track their accounts at their convenience without using a computer, adding value and increasing loyalty.
- Fraud reduction – mobile alerts give customers increased confidence by notifying them immediately about possible fraudulent account activity.
- Differentiation – enables banks to increase market share by offering a unique and valuable service.
- Cost reduction – a lower-cost channel of customer interaction for customers without access to Internet banking.
- Increased Profits – decreased demand on call centers and fewer customer branch visits.

New Features

Sybase mBanking 365 version 3.0 introduces the following features:

Alert Management – Bank employees can configure certain types of alerts to aggregate, configure an alert override, designate certain alert types to high priority, and can designate the lifetime of an alert type. For more information, see “Alert Configuration” on page 8.

ATM Branch Locator – Allows users to locate ATM kiosks using all channels. For more information, see “ATM Branch Locator” on page 17.

Audit Customization – Enables easier audit logging customization.

Authentication Framework – Leverages externally generated and validated credentials, such as RSA tokens. For more information, see “Authentication Framework” on page 11.

Carrier Based Entitlements – Some services (such as funds transfers) are restricted by certain carriers, and some services differ between carriers. mBanking 365 provides service-level configuration to supports these differences.

Contact Points – Users can now register multiple devices as well as set email and fax contact points to receive alerts. For more information, see “Contact Points” on page 8.

Mobile Self-Enrollment – Enables users to register devices using WAP or SMS channels. Once the devices are registered, users can use the device to receive alerts and perform mobile banking operations.

Alert File Processing – Flat files are created to avoid multiple calls to the backend to retrieve alert information for each alert being fired. This feature is capable of reading and processing any type of file. For more information, see “File based Alerts” on page 8.

File Processing – Provides generic file uploading and processing capabilities. It allows any type of file processing through the use of configurable processing plug-ins. For more information, see “File processing” on page 13.

Financial Product Information – Enables the user to request product information, for instance deposit rates, interest rates, and foreign exchange rates, through SMS and WAP.

Merchant Network Integration – Provides integration with networks supporting ISO 8583 protocol for Visa and MasterCard. For more information, see “ISO 8583 protocol support” on page 15.

Payment Scheduling – Lets WAP users view, delete, and edit scheduled and pending bill payments and transfers.

Schedule Management – Lets users manage system jobs such as database purge operations, alert file processing, and so on. Users can run a set of system-defined jobs, modify jobs, delete, or create their own jobs. For more information, see “Schedule management” on page 12.

Ported, Retired, and Restricted MSISDNs – Bank employees can upload a file of restricted numbers or add them one at a time. For more information, see “Ported, retired, and restricted MSISDNs” on page 13.

Reporting – More reports are provided to inspect the activities performed both by customers and employees. For more information, see “Customizable reports” on page 17.

SMPP Adapters – The SMPP communication framework supports heavy SMS traffic volumes (sending and receiving). For more information, see “SMPP Adapters” on page 6.

SMS Account History – Ability to send account history as SMS. For more information, see “Simple Messaging Service” on page 4.

SMS Confirmation for Payment Transaction – Users can receive SMS confirmation of payment transactions, including adding, editing, deleting, payments and transfers. For more information, see “Simple Messaging Service” on page 4.

Stop Check Payments – Users have the ability to place stop check payment requests and to view stop summaries. For more information, see “Stop Check Payments” on page 16.

Suspicious Transaction Pattern Detection – Implemented by defining a new report type which shows “suspicious” transactions by configurable data. Banking employees set reporting criteria through the Mobile Operations Manager. For more information, see “Suspicious Transaction Pattern Detection” on page 18.

Multiple delivery channels

Sybase mBanking 365 is equipped with multiple delivery channels to connect mobile users to your financial institution’s banking system.

Simple Messaging Service

Simple Messaging Service (SMS) receives and processes requests from end-user mobile devices. SMS processing manages secure device sessions, validates and executes commands, delivers SMS response messages, and delivers both scheduled and event-based alerts.

SMS transactions and supported formats include:

- Account balances, using either a short numeric code for an account or an account nickname such as “Savings”

- Funds transfers between accounts
- Bill payments to a selected list of payees
- Statements for user accounts
- Accounts and payees lists
- Account history
- Enabling and disabling a user mobile device from receiving alert messages
- Enabling and disabling the issuance of SMS commands from a user mobile device
- Enabling users to self-enroll their devices using SMS commands
- Allows users to access financial product and foreign exchange rate information by sending a HELP SMS

Intelligent SMS

In addition to standard SMS communication, mBanking also supports intelligent SMS, or SMS conversations. An SMS conversation is initiated by an actionable alert such as an overdraft alert. Rather than simply sending an alert indicating that an account is overdrawn, an SMS conversation asks the user to perform an action, such as making a transfer. If the user opts to make a transfer, the next message in the conversation will ask for the source account, then the amount, and so on.

Actionable alerts are handled either by the mBanking server or the back-end banking system. In either case, you can engage in multiple SMS conversations simultaneously. For security, conversations time out after a specified period of inactivity.

SMS confirmation

mBanking enables customers to have payment and transfer confirmation sent through SMS after a transaction is complete. Users with multiple registered devices can receive confirmation on any number of those services. Users without a registered device cannot access the “Send as Text” button.

SMPP Adapters

The SMPP Adapters feature works with the SMPP communication framework to support heavy SMS sending and receiving traffic volumes. The SMPP service supports SMPP3.3 and 3.4, and can be installed as a plug-in, though bank users can choose an HTTP plug-in as well.

Mobile browser

The wireless application protocol (WAP) browser channel provides access to banking functions through a mobile device's mini-browser software. Users can perform actions such as transferring funds, paying bills, and managing alerts without having to download additional software. The WAP channel supports multifactor security to ensure that personal banking information is not made accessible to third parties. The WAP channel is not tied to a single handset; it can be accessed from any browser-enabled handset as long as the user has the correct login information.

The WAP channel lets users manage the different alerts they may receive for their accounts. Users with a registered mobile device can enable, disable, and view which alerts they are configured to receive.

The WAP channel allows users to self enroll their devices directly from their devices without having to use the Mobile Profile Manager.

mBanking lets users monitor their payments and transfers using the mobile browser and smart client channels. Users can access pending payments and transfers through the main screen of the mobile browser, where they can view, edit, and delete payments and transfers.

Users can request detailed information on specific financial products or foreign exchange rates offered by the bank through the WAP channel. Users can access these using either the Products / FX Rates button in the "Services" section or the corresponding links on the login page. In the latter case, information of a system-specified default bank will be serviced. The FX Rates is a currency converter, which displays foreign exchange rates to the user.

The WAP channel allows users to send their account history from the WAP Account History page to a mobile device using SMS. This feature lets users with multiple registered devices select the target device for the message. Users can also use a non-registered device to access the application and select a registered device to which the SMS Account History is sent.

Smart client

The smart client application enables users to view transaction history, transfer funds between accounts, and make bill payments using their mobile devices.

The Smart client supports self-registration and is largely integrated with the mBanking server. It is similar to the WAP channel, as users can download the Smart client to their device, install it, and login to mBanking by providing the user name and password when prompted. Once users log into mBanking, they can access all the core mBanking features such as Accounts, Payment, Transfers, Services, etc. However, access is dependent on the entitlements applicable to a user's service package.

In order to subscribe to alerts and receive alert notifications, users need to register their device using the registration features available in the Smart client application. The Mobile Operations Manager can be used to manage the registrations for all channels such as SMS, WAP, and Smart Client.

A bank employee must register the user to use the smart client application. After the user is verified and authenticated, a message containing the URL to download the smart client application is sent to the user's mobile device. When users have downloaded the smart client application, they activate it by entering an activation code, user ID, password, and PIN.

Financial institutions can disable and reenable users' access to mBanking 365 services. Users can also be locked out if they exceed the set number of login attempts.

To unregister from the smart client application, users must contact their financial institution. Unregistering from the smart client application does not unregister a user from the SMS or WAP channels.

WAP templates on mBanking supports iPhone, Palm, and Android devices. This enhances the look, feel, and usability of the application for devices.

Mobile network access

The SMS delivery channel provided by mBanking 365 requires your financial institution to be enabled within a mobile carrier network for every geographic area in which you have customers. The Sybase 365 Mobile Network, provided as part of the mBanking product suite, provides access to over 700 cellular carriers worldwide for SMS communication and enables you to provide SMS service without negotiating and managing individual carrier relationships.

While the use of the Sybase 365 Mobile Network is optional, implementing an alternate mobile network requires your financial institution to develop custom message adapters to match the specifications of the network you select.

Alerts framework

mBanking 365 has a flexible alerts framework that lets you either use mBanking as a standalone product or integrate it with an existing back-end system.

There are two types of alerts: scheduled or recurring alerts, and immediate or event-triggered alerts. You can manage scheduled alerts with either your own scheduling engine or the scheduling engine provided with mBanking 365. Immediate alerts are triggered by your back-end banking system.

File based Alerts

File-based alerts processing processes generic alert files. mBanking can read and process CSV and BAI. Batch processing allows bulk alerts to be processed.

Contact Points

mBanking provides users the option to send alerts to email and fax on top of their devices. Users manage alerts by selecting any number of contact points to a destination from the “Add Alert” page in Mobile Profile Manager. Bank employees will be enabled to manage customer contact points through the Mobile Operations Manager.

Alert Configuration

Alert configuration is available for bank employees to configure alert types through the mbanking.xml file. This option enables bank employees to send aggregated alerts. Aggregated alerts are multiple alerts of a similar type that are merged and then sent to the same device in a single SMS message. These aggregated alerts include account summary balance, account balance threshold, insufficient funds, stock portfolio, and transactions.

Alert configuration enables bank employees to control the lifetime of an alert before it expires. Users can configure their devices to receive alerts only on specified days. Alerts that expire before users want to receive them will not be sent to the users' mobile devices.

Bank employees are also enabled to designate priority to alerts. Priority alerts are delivered on a different SMS gateway than standard alerts.

Security

Sybase mBanking 365 provides several layers of security, including the security manager, second-factor authentication, and inline password protection. It is a built-in feature for mBanking 365 customers.

Security manager

The security manager offers:

- Device authentication – verifies the user device and security entitlements for SMS requests, and either accepts or denies each request. If the request is accepted, the transaction is processed. If the request is denied, the session manager invalidates the session, removes pending actions, and sends a message to the end user indicating that authentication has been denied.
- User authentication – validates the user ID, account ID, and password entered by a user upon beginning a mobile banking session. If the user does not provide an ID and password at the beginning of the session, the manager requests reauthentication until valid information is provided. You can also configure the security manager to require a business ID number to be entered along with the password and user ID. For enhanced security, mBanking 365 uses out-of-band authentication to reauthorize users.
- Command security – provides command-specific authorization. Command security uses individual and customizable authentication policies that determine whether a command's execution is granted based on device authentication (relaxed-level), a previously-established and still-valid session (medium-level), or reauthentication (strict-level).

The security manager also provides lockout capabilities. If the user exceeds the preconfigured number of consecutive failed log in attempts, the account is locked. This includes login attempts from all channels.

Single sign-on

Single sign-on (SSO) allows for external authentication mechanisms. mBanking 365 can seamlessly integrate with existing bank platforms through arbitrary SSO systems.

This feature is developed against the Sybase back-end simulator, namely Connector RI. mBanking provides a connector framework that allows Single sign-on and other features to be easily extended or customized to any back-end core banking solution.

With SSO, users do not log in to mBanking directly. Instead, they log in to the host system. When they access an mBanking page, the mBanking server sends an authentication request to the SSO authentication system. The user does not have to log in twice, and the SSO system maintains their external banking system session so they are not logged out.

If you implement SSO with a Sybase Financial Fusion back end such as Consumer Banking or Corporate Banking, you can access mBanking 365 functionality directly within the back-end system. For example, a bank employee managing service packages within Business Central can access the mBanking 365 Mobile Operations Manager through an integrated menu option in the Business Central user interface.

Note Integration with Corporate Banking and Consumer Banking will be available in an upcoming service pack to the Banking Solutions.

Second-factor authentication

Second-factor authentication provides additional security for logging in or when performing certain transactions.

If second-factor authentication is required at login, a token is generated and sent to users by SMS message after the user name and password have been verified. Upon receipt of the message, the user enters the token in the appropriate field to access the mBanking 365 system.

Financial institutions can also require second-factor authentication for specific transaction requests, such as a transfer exceeding a certain amount. If the transaction requires second-factor authentication, a token is generated and sent by SMS to the user's mobile device. The user must enter this token to complete the transaction. Second-factor authentication can be required even if the user has already provided credentials and a second-factor token at login.

Authentication Framework

This feature allows users to secure their mBanking profile. It supports externally generated and validated credentials such as RSA tokens and scratch cards, and provides users with the opportunity to select a secret phrase to address phishing attacks. Authentication support is provided in the login process for the WAP and Mobile Profile Manager channels.

Out-of-band authentication

The out-of-band authentication mechanism is used to securely authenticate user requests originating from the SMS channel. Out-of-band authentication returns a unique URL through a process called WAP push. Users must activate the URL to complete the authentication process.

Some mobile devices support true WAP push and others do not. If true WAP push is supported, the message automatically loads the authentication URL in the mobile browser. If true WAP push is not supported, an SMS message containing the authentication URL is sent to the user, who must then manually activate the mobile browser to enter the URL.

The out-of-band authentication mechanism allows for location neutrality. In other words, it does not matter if channels are running locally or remotely. When a channel makes a normal call to the security service, it passes along a standard local callback handler. This callback handler is registered with the pluggable remote callback adapter and is replaced with a remote callback handler. The remote callback handler is passed on to the Web service proxy.

Inline password protection

Inline password protection adds a layer of security to SMS transactions. SMS commands are supplied with authentication parameters, such as a user ID and password, to allow you to set inline password protection. Configuring a command to require a user ID and password ensures that the command cannot execute without valid credentials.

If you configure a command's authentication parameters as optional and a user sends a command without providing a user ID and password, the security manager still satisfies the requirements of the configured command security level. For example, if the command is sent in a session that is not already validated, the security manager performs out-of-band authentication.

Service packages and entitlements

You can control access to mBanking 365 by setting entitlements on service packages for mBanking 365 channels, features, and alerts, and assigning mBanking 365 users to these service packages.

You can also assign entitlements & restrictions to carriers to allow or deny specific transactions for users on those carriers. This feature adds transactions and services based on restrictions through the mbanking.xml file. If a user sends a SMS command that is restricted based on carrier entitlement, the WAP channel returns a message indicating that the command is restricted.

Administration

Schedule management

The schedule management feature, available through the Mobile Operations Manager, lets employees view, add, modify, and delete scheduled jobs. It also provides the ability to load-balance between servers in a cluster. This enables jobs to fail over to a secondary server should the original server crash. Load balancing distributes requests among the servers in the cluster to prevent one server from becoming over loaded. Users also have the option of creating a local job, which performs jobs such as updating servers or server clean up of individual servers.

Terms and Conditions

Banks are given the option on whether they want users to accept their terms and conditions, as well as add the terms and conditions of the carrier before they begin using mBanking. Banks can also set a number of days in which the mBanking user has to accept the terms and conditions before their alerts are disabled.

Carrier Opt-in

mBanking 365 enables bank employees to edit carrier opt-in settings from Mobile Operations Manager by selecting the “Token required as part of device registration” option. When this option is selected, devices being registered through all delivery channels will receive a validation token.

File processing

The file processing feature enables generic file uploading and processing capabilities. Processing of generic files is easy and flexible to process a large amount of information for various tasks. The processes are audit logged, making it easier to track changes and tasks that have been completed.

Ported, retired, and restricted MSISDNs

mBanking 365 enables bank employees to manage lists of ported, retired, and restricted mobile device numbers (MSISDNs) using Mobile Operations Manager. MSISDNs that are restricted are given a “Deleted” status and cannot be registered. Retired MSISDNs are removed from the retired list and given a new entry if registered again in the future. When an MSISDNs is ported to another carrier, the ported number is validated by SMS request, the carrier is updated, and the terms and conditions are reset.

Internationalization

Sybase mBanking 365 is initially localized for U.S. English, but provides full internationalization support, allowing you to localize mBanking 365 based on date format, time zone, country, language, currency, and so on. Localization is performed as part of standard configuration and does not require advanced customization.

mBanking 365 also supports multicurrency transactions. For bill payments, the amount is remitted in the currency of the payee. For transfers, the amount is remitted in the currency of the originating, or source, account.

Commands sent through SMS are answered in the language specified during the mBanking 365 registration process. Browser mBanking requests are returned in the default language of the browser being used, or, if enabled, a language the user selects prior to login.

Integration with back-end systems

By default, mBanking 365 platform installs as a standalone product. With the standalone option, mBanking 365 is installed with a functioning demo and a connector reference implementation (connector RI) that simulates a fully functioning back-end system.

You can integrate Sybase mBanking 365 with existing back-end banking systems through connector services. These services provide a single point of access between mBanking 365 and the back-end banking system for audit, security, entitlement, administration, user mobile profile maintenance, funds transfers, and payments.

The connector services can be integrated with your financial institution's banking system through WebServices calls, EJB or remote method calls, or through a Java or native library, enabling deployment in any banking environment.

Moreover, features are developed against the Sybase back-end simulator, namely the Connector RI. mBanking provides a connector framework that allows features to be easily extended or customized to any back-end core banking solution.

Connector RI

The Connector Reference Implementation allows for mBanking 365 to run independently without having a back-end banking system integrated by acting as a reference implementation. It provides implementation for major services and is portable with mBanking and can eliminate the need for backend core banking system.

Connector RI's functionality includes implementation for all the services which is required to run front-end UIs, maintaining information between subsequent user logins, not having any dependencies on mBanking to compile, user information stored in light weight XML files, and separate XML files maintained for payees.

ISO 8583 protocol support

ISO 8583 protocol support allows mBanking 365 to be used as a standalone application. Since most banks provide ISO 8583 protocol support in their ATM networks, out-of-the box integration with this protocol results in reduced implementation times at most institutions; rather than designing a custom integration with your backend directly, the implementation team can simply establish connectivity between the mBanking application and the ISO 8583 server.

Merchant Network Integration

Merchant Network Integration enables users to integrate with networks supporting ISO 8583 protocol, namely VISA and MasterCard. It uses the jPOS Transaction Switch (JPTS) plug-in to convert ISO 8583 messages from one variant to another.

OFX support

OFX support, like ISO 8583 protocol support, allows mBanking 365 to be used as a standalone application. Open Financial Exchange (OFX) is a transaction format standard used by most financial institutions to support transaction interactions between the Quicken and Microsoft Money Personal Financial Manager (PFM) applications. Sybase mBanking 365 provides out-of-the-box integration through OFX. This allows for greatly reduced integration time since implementation requires only that you connect to your existing OFX server.

Transaction Support

Payment transaction

mBanking lets users monitor their payments and transfers through mobile browser and smart client enabled devices. Users can access pending payments and transfers through the main screen of the smart client or mobile browser, and can view, edit, and delete payments and transfers.

Stop Check Payments

The Stop Check Payments feature enables users to perform self-serving operations such as placing a stop on a payment or transfer. Users have the ability to place a stop check payment request through WAP, SMS, and Smart Client channels, and can also retain the request receipts. The Stop summary lists the status of stop payments requests. Bank employees activate this feature through the Mobile Operations Manager.

ATM Branch Locator

The ATM Branch Locator feature allows users to locate their bank's kiosks and branches using the WAP, SMS, and Smart Client channels. Users have the ability to search ATM Branch details based on fields such as type (ATM/Branch), city, state, and zip code. Furthermore, the implementation of the ATM Branch Locator allows users more flexibility to integrate other systems such as the "Answer Anywhere" to provide narrower search results in the future.

Users do not require authentication in order to utilize the Branch locator within the WAP channel. They can search their default bank when logged out, and their affiliated bank after logging in.

Customizable reports

Sybase mBanking 365 allows for a wide variety of customizable reports that are easily accessible for bank users. Users can generate reports from a template that uses default values, customize their reports, or generate reports from a saved custom report.

Available reports include:

- Employee
  - Employee Activity
- Customer
  - Customer Activity
  - Customer Authentication Summary
  - Device Authentication Exception
- Operation
  - Transaction
  - Transaction Volume
  - Active Customers
  - Suspicious Transaction Pattern Detection
  - Current User Login
  - Login Usage Pattern

- Customer Activity Statistics
- Employee Activity Statistics
- Customer Login Statistics
- Registration
- Retired/Restricted MSISDNs

Suspicious Transaction Pattern Detection

Suspicious Transaction Pattern Detection is a report type that outlines suspicious payments and transfers. mBanking 365 enables bank employees to manage Suspicious Transaction reporting criteria through Mobile Operations Manager. The output from this reporting feature can be exported to a file for transmission, and the report can be run automatically on a periodical basis. Bank employees can manage report scheduling from the Mobile Operations Manager ADMIN section.

Customization and configuration

Sybase mBanking 365 offers many customizable features to provide additional flexibility for your bank's needs:

- SMS channel command language – financial institutions can change the commands for performing actions, such as requesting an account balance, to any desired custom command. mBanking 365 includes a list of default commands you can add to, restrict, or revise.
- Security details – such as second-factor authentication for individual actions.
- Custom alerts – sent to customers as certain events occur within the electronic banking solution.
- The mbanking.xml file – customize the interaction between mBanking 365 and backend banking systems, as well as the interactions between the mBanking server and the mBanking channel client.

CHAPTER 2 Architecture and Technology

This chapter provides an architectural overview of Sybase mBanking 365 and describes the supporting applications, functions, and databases that form the foundation of mBanking 365.

Architectural overview

Sybase mBanking 365 is a mobile banking solution for users to manage specific banking functions using their mobile devices.

The mBanking server connects mobile users to financial institutions' banking systems through multiple channels, including SMS, wireless application protocol (WAP), and the smart client application.

The mBanking server's security manager provides security to all channels through device authentication, user authentication, and command authorization.

- Device authentication ensures that a specific device is registered with mBanking 365.
- User authentication requires users to provide authentication credentials, such as a user name and password, to verify user identity.
- Command authorization, configured on a per-command basis, enables the definition of multiple security roles including device authentication, user authentication, and reauthentication.

Each SMS command has its own security roles. For example, the SMS command for obtaining a balance may be assigned the device authentication role. When a user issues this command, the security manager authenticates the device before allowing the command to execute. If a command has re-authentication as its role, the security manager authenticates both the device and the user, even if a user session already exists.

While device and user authentication remain valid for the entire user session, you can configure each command individually with specific security roles that are performed each time the command is invoked.

The customizable mBanking interface layer provides a single integration point with any banking system. The connector consists of two functional parts, the common connector API and the connector plug-in. The common connector API defines the interface to the banking system and the services it provides. The connector plug-in lets you add specific implementations of the common connector API to the banking system.

Core mBanking modules

mBanking 365 includes three core modules: the Messaging module, the mBanking module, and the Mobile Operations Manager.

Messaging module

The Messaging module supports reports and outbound message transmissions using messaging aggregators. It includes:

- SMS sending – receives SMS messages from your back-end banking system and forwards them to the mobile network to be sent to users.
- Auditing – tracks and logs events and messages as they are processed by the mBanking server. Messages are categorized according to channel, transaction type, state of the message, and so on.
- Outbound message alerts – enable financial institutions to send two types of alerts: scheduled alerts that run daily, and event-based alerts triggered by preset alert criteria.

mBanking module

The mBanking module includes:

- Banking features – users can access Account Balance, Bill Payment, Funds Transfer, and Mini Statements.
- Two-way SMS – users can register their mobile devices with mBanking to access banking features through SMS. They can also receive SMS alerts from and participate in SMS conversations with your financial institution.
- Out-of-band authentication – authenticates user requests by providing a unique URL the user must activate to continue the process that authentication was attached to.
- Rich client support – enables customers to execute and view transactions on their mobile devices by connecting the mobile devices to the mBanking server.
- Mobile Profile Manager module – enables customers to manage customer profiles, register their devices, and configure their alert preferences.

Mobile Operations Manager

The mBanking Mobile Operations Manager enables financial institution employees to monitor and manage mBanking tasks including customer management, entitlement management, device management, reporting, and so on. The Mobile Operations Manager includes:

- Customer management – set up new or existing customers with mBanking 365 functionality, reset, or lock an mBanking account. Bank employees can add users to the mBanking system by assigning the users a mobile banking service package. In addition, bank employees can register a mobile device on behalf of a user, or change a user’s status in the system.
- Service packages and entitlements – create service packages and control access to mBanking by setting entitlements on service packages and assigning mBanking users to these service packages.
- Reporting - generate reports on employee or customer activity, mBanking transactions, and so on.

Mobile network

Sybase mBanking 365 is designed to be used with the Sybase 365 Mobile Network, which provides you with SMS connectivity to customers through over 700 carriers worldwide. While you can choose to use a different mobile network, doing so requires you to develop custom message adapters to match the specifications of the other network, as well as negotiate usage terms with cellular carriers.

mBanking services

Sybase mBanking 365 uses several services to perform tasks. Some of these services, such as the I18N Internationalization Service, are shared between the different channels that mBanking uses to communicate with end users. Others, such as the SMS receiver service, are designed for one specific channel. You can configure services through an XML configuration file within Sybase mBanking 365.