



Feature Guide

Sybase mBanking 365™

2.1

DOCUMENT ID: DC00785-01-0210-01

LAST REVISED: March 2009

Copyright © 2009 by Sybase, Inc. All rights reserved.

This publication pertains to Sybase software and to any subsequent release until otherwise indicated in new editions or technical notes. Information in this document is subject to change without notice. The software described herein is furnished under a license agreement, and it may be used or copied only in accordance with the terms of that agreement.

To order additional documents, U.S. and Canadian customers should call Customer Fulfillment at (800) 685-8225, fax (617) 229-9845.

Customers in other countries with a U.S. license agreement may contact Customer Fulfillment via the above fax number. All other international customers should contact their Sybase subsidiary or local distributor. Upgrades are provided only at regularly scheduled software release dates. No part of this publication may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without the prior written permission of Sybase, Inc.

Sybase trademarks can be viewed at the Sybase trademarks page at <http://www.sybase.com/detail?id=1011207>. Sybase and the marks listed are trademarks of Sybase, Inc. ® indicates registration in the United States of America.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Unicode and the Unicode Logo are registered trademarks of Unicode, Inc.

All other company and product names mentioned may be trademarks of the respective companies with which they are associated.

Use, duplication, or disclosure by the government is subject to the restrictions set forth in subparagraph (c)(1)(ii) of DFARS 52.227-7013 for the DOD and as set forth in FAR 52.227-19(a)-(d) for civilian agencies.

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

Contents

CHAPTER 1	Features and Functionality	1
	Introduction	1
	New Features	2
	Multiple delivery channels	3
	Simple Messaging Service	3
	Alerts framework	4
	Mobile browser	4
	Smart client	5
	Mobile network access	5
	Security	6
	Security manager	6
	Single sign-on	6
	Second-factor authentication	7
	Out-of-band authentication	7
	Inline password protection	8
	Service packages and entitlements	8
	Internationalization	9
	Integration with back-end systems	9
	Connector RI	10
	ISO 8583 protocol support	10
	OFX support	10
	Customizable reports	11
	Customization and configuration	11
 CHAPTER 2	 Architecture and Technology	 13
	Architectural overview	13
	Core mBanking modules	14
	Messaging module	14
	mBanking module	15
	Operational module	15
	Mobile network	16
	mBanking services	16

Features and Functionality

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

Topic	Page
Introduction	1
New Features	2
Multiple delivery channels	3
Mobile network access	5
Security	6
Internationalization	9
Integration with back-end systems	9
Customizable reports	11
Customization and configuration	11

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 2.1 introduces the following features:

- SMS Conversation – enables the mBanking server to exchange a series of SMS messages with a user's mobile device based on message context and user response. See “Simple Messaging Service” on page 3.
- SMS Enhancements - Additional enhancements allow backend applications to send reliable SMS conversation through Web Service Interfaces. See “Simple Messaging Service” on page 3.
- Integration with back-end systems – out-of-the-box integration through either OFX or ISO 8583 Protocol. See “Integration with back-end systems” on page 9.
- Remote access to out-of-band authentication – in previous versions of mBanking 365, out-of-band authentication was available only to local channels. Now, any channel, whether local or remote, can use out-of-band authentication. See “Out-of-band authentication” on page 7.
- WAP alert management – appropriately entitled users are now able to manage their alerts through the mobile browser banking channel (WAP). See “Mobile browser” on page 4.

- Customizable reports – the Operational module provides access to several customizable reports that help you maintain records on mBanking 365 usage. See “Customizable reports” on page 11.

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
- Enabling and disabling a user mobile device from receiving alert messages
- Enabling and disabling the issuance of SMS commands from a user mobile device

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.

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.

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.

Smart client

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

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.

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.

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.

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 Operational module 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.

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.

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

The mBanking connector, provided with mBanking 365, provides a single point of integration with any banking system. The connector is required to enable communication between mBanking 365 and your financial institution's banking system. The connector 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, making it deployable in any banking environment.

If you have an existing Sybase Financial Fusion back-end system such as Corporate Banking or Consumer Banking, you can integrate with this system directly during the installation process. If you have a different back-end banking system, you can install mBanking 365 as a standalone application and integrate with your back-end system using several different methods including the connector layer, ISO 8583 protocol, and OFX protocol.

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

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.

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.

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

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.

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.

Topic	Page
Architectural overview	13
Core mBanking modules	14
Mobile network	16
mBanking services	16

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 Operational module.

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.
- Profile management module – enables customers to manage customer profiles, register their devices, and configure their alert preferences.

Operational module

The mBanking Operational module enables financial institution employees to monitor and manage mBanking tasks including customer management, entitlement management, device management, reporting, and so on. The operational module 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.