

**Functional Overview:
Anywhere Platform**

Contents

Introduction	4
Platform Feature Summary	6
Security.....	6
Administration Console.....	7
Audit and Reporting	8
Web Services Integration	8
Service Management	8
Customer/User Management	8
Multi Language Support	9
Branding	10
Customer Segmentation	11
Application and Configuration Management.....	11
Device Support.....	12
Application Type Support.....	12
Operations and Management.....	12
Billing.....	13
Secure Mobile Services (Mobile Banking)	14
Define Your Own Functions.....	14
Defining Functions.....	15
Mobile Application	15
iPhone and Android	18
Web Channel	18
Customer Segmentation	19
Possible Mobile Banking Functions.....	19
Security Features.....	20
Messaging Services	22



Customisation	22
Multi Language Support	23
Short code management	23
Message Priorities	24
Message error handling	24
Possible Messaging Functions	25
Alerting Services	28
Alert categories	28
TwoSecure	30
Functions	31
Domains and Identity Management	31
Highly Configurable	31
Mobile Application	32
Using TwoSecure	34
Using Transaction Signed OTP	35
SMS TwoSecure	35
Integration	36
Radius Integration	36
Mobile Ordering and Payments	38
Merchants	39
Product Ordering	40
Pay Only	42
Payment Providers	43
Security Features	43
Registration Process	44
Administration console registration	44
Business registration channels	44
Registration process	45



Registration for Messaging Services	50
Registration for Alerting Services	51
Software as a Service (SAAS) Platform.....	52
Segmentation of Data	52
Administration	52
Glossary.....	54

Introduction

The Anywhere platform is designed to help companies transform the way they engage with their customers by providing secure anytime, anywhere access to services that are directly relevant to each customer segment.

This compelling new self service channel will:

- Reduce costs by shifting customers from other more expensive channels.
- Provide customer contact anytime, anywhere
- Enhance customer experience and access to information
- Facilitate targeted and relevant up-selling and cross-selling of products and services.
- Provide brand awareness and promotion opportunities

The Anywhere product suite includes a comprehensive set of modules that deliver a complete range of mobile services. The full suite includes:

- Secure mobile services (Mobile Banking)
- Mobile ordering and payments
- Two Factor authentication using a mobile application or messaging (SMS or email)
- Mobile originated SMS services (SMS pull)
- Mobile terminated messaging services (Alerts via SMS or Email)

Each module can be purchased independently and then offered to customers via a single instance of the platform. The entire suite shares a common framework that provides the following key features out of the box:

- Comprehensive device side and server side security
- Web based administration console for customer and service management
- Web Service interfaces for easy integration
- Reporting
- Multi language support
- Full branding support (colours, text and images)
- Comprehensive device support (including Blackberry, iPhone and Android)
- Isolated, pluggable modules for easy integration with existing systems
- Software as a service (SAAS) support
- System monitoring and alarm support



- Billing support

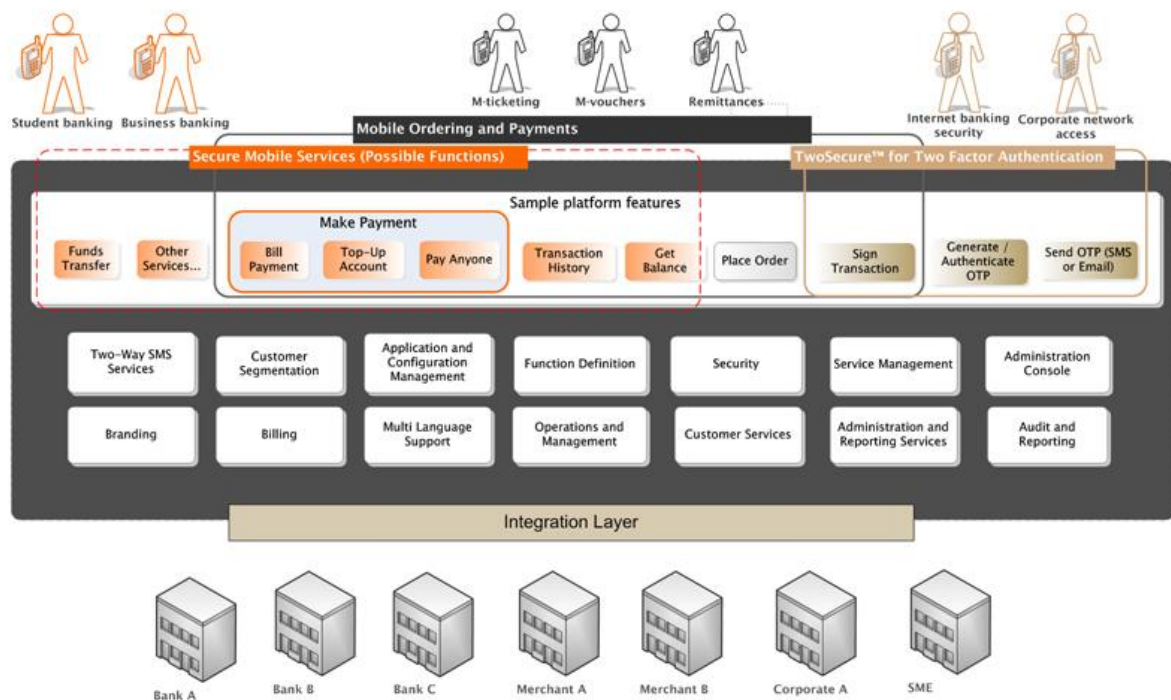


Platform Feature Summary

The Anywhere platform provides a shared set of features to each product within the suite. This section describes in some detail the features provided and how they can be configured to suit an organisation's specific requirements. The following sections describe the additional features for each of the product offerings.

This diagram provides a functional view of the Anywhere platform. The white boxes represent shared functionality across the platform. Each product in the suite adds additional functions as required (the orange and brown boxes).

The platform integrates with external entities via a pluggable integration layer. This makes it easy to develop specific integration adaptors for each external system.



Security

A key feature of the Anywhere platform is in securing the identity and data of each user on the server, over the air and within the device. Anywhere's patented security features impart multiple layers of security to every aspect of the solution.

This section provides a brief overview of some of the key features, for a full description of all the security features please refer to the Anywhere Platform Security Datasheet.



Two Factor Authentication	<p>Every customer profile on the Anywhere platform is matched to that customer's application stored on the phone using a unique signature that is embedded in to the application itself.</p> <p>Another unique token is also provided to the application during activation (see below). This is stored on the device itself and is used to login, submit a payment or generate One Time Passwords (TwoSecure). This ensures that there can only ever be one instance of the application for each customer.</p> <p>This token is changed on each successful login or payment so that it is extremely difficult for an attacker to gather enough information to steal someone's identity.</p>
Activation	<p>The Anywhere platform includes a mobile application activation process to ensure that it is delivered to the correct device, that there is a single instance that is linked to the customer and that it is the correct person using the application.</p> <p>The Anywhere platform supplies an activation code to the channel used for registration. This is displayed or read out to the customer. The customer must input the activation code into the phone prior to its first use. Further information on this process is supplied in the registration process section of this document.</p> <p>The business may configure the length of time a customer has to activate an application.</p>
URL Protection	<p>The server URL that is included in the mobile application is hashed with the unique application identifier to prevent someone changing the URL within the application.</p>
Data Protection	<p>With the exception of TwoSecure (it is not required) all communication between the mobile application and Anywhere server is encrypted using HTTPS.</p>

Administration Console

The platform includes a web based administration console that is used to manage the services and customers.

A role based security framework is used to manage administration user access; this framework may be integrated with existing user directories (such as Microsoft active directory) where required.

Where many businesses are sharing a common hosted platform, operated by a third party service provider, the service provider may provide each business with tiered levels of administration rights to their customers and services. Access is permission based and no bank will be able to view or administer customers or services associated with another bank.



Banks can define group privileges for administration users, allowing the bank to give different parts of the business unique levels of access to the system, e.g. you may require contact centre staff to have access to reports and customer details only, while a systems administrator group would be set up to have access to more functionality.

Audit and Reporting

All configuration changes committed via the administration console are audited. Reports are provided to view these audit logs.

Every customer activity is logged to the database with information about the activity, how long it took to complete and the status of the result. These activities may be viewed as reports or accessed via the web services interface. Activities may also be pushed to an external system real time via an adaptor if required.

Reports can be output in HTML, PDF or CSV format. Alternatively banks can integrate the system with a pre-existing reporting tool.

Web Services Integration

The Anywhere platform provides a comprehensive range of web services for easy integration with existing systems and processes if required. The following is a list of the services provided. Full interface specifications can be provided on request.

Customer Services: Register, Deregister, Update, Suspend, Activate

Messaging Services: Send SMS, Send Alert, Trigger Alert

Alerting Services: Subscribe, Unsubscribe, Update

Domain Services: Manage user registrations to different domains

Reporting Services: Get Activities, Get Customer Details, Get Customers

Service Management

The Anywhere administration console provides a user interface for configuring and customising the services provided. The platform is based on a service provider model, where the business is a provider of services to their set of customers.

Each service can be configured/customised independently from other services or they can share certain resources to assist with ongoing management. The services have their own configuration versions which are used to keep the applications synchronised with the server configuration.

Customer/User Management

A customer or user belongs to a particular service provider. Once registered, they can then subscribe to the services offered by that provider.

Users can be managed via the administration console or via the web service interface if integrating with an existing business or customer channel. The following management features are available:



- Register/Deregister user or service
- Suspend/deactivate/activate user
- Register/deregister a user identity
- Update registration details

Multi Language Support

All text that is shown on the mobile application is downloaded from the Anywhere server and stored on the device for easy access. Each service can define a set of supported locales or languages. The text can then be configured for each language via the administration console. When a user registers for a service they can select their locale thus defining which resource bundle to download.

The following diagram shows the administration screen that is used to define the text for a particular function and locale.

Resources can be defined at different levels within the system.

- Platform Level: Resources defined here are shared across all services on the platform. This level provides a set of defaults for the system.
- Provider Level: Resources defined at this level apply to all services within this particular provider. They over write equivalent resources defined at the platform level.
- Service Level: Resources defined at this level apply to a particular service. They over write all other equivalent resources.



Localised Resources: Platform Defaults: en_NZ				
Description	Value	Edit	Delete	Promote and Edit
Amount	Amount			
Validation message - amount	Amount should not be zero. Please check again.			
Confirmation message	You want to transfer @amount from @srcacc to @destacc today. Is this correct? Please confirm.			
Validation message - If source and destination accounts are the same	Source account and destination account should not be the same. Please check again.			
Destination Account	To Account			
Function Name	Funds Transfer to Own			
Source Account	From Account			
Message while submitting transaction	Please wait while we process your request. Call 0800 11111 to find out about our new interest rates			

Localised Resources: Provider: Not fronde staff: en_NZ				
Description	Value	Edit	Delete	Promote and Edit
Source Account	Destination Account			

Localised Resources: Service: Smartbank-Icons: en_NZ				
Description	Value	Edit	Delete	
Source Account	Payee Account			

When a resource changes on the server, the application recognises the change the next time that it connects with the server. The new resources are downloaded and the application is reconfigured. Because TwoSecure does not communicate with the server all the time it will only update resources when a customer synchronises their TwoSecure application.

Branding

All colours and images used on the mobile application are also downloaded and stored on the device. This allows the organisation to fully customise the applications to meet their own brand.

The following diagram shows the set of colours that will be used by the mobile application. They are also defined as resources so can be defined at different levels with each level over writing the previous level.



Localised Resources: Platform Defaults: en_NZ				
Description	Value	Edit	Delete	Promote and Edit
Background colour of forms	#e5e5e5			
Background colour of controls that have focus	#993300			
Colour of text on controls that have focus	#ffffff			
The colour of highlighted text on forms	#993300			
The colour of standard text on forms eg. labels	#000000			
Background colour of controls that don't have focus	#ffffff			
Colour of text on controls that don't have focus	#000000			

Localised Resources: Provider: Not fronde staff: en_NZ				
Description	Value	Edit	Delete	Promote and Edit
The colour of highlighted text on forms	#226def			

Localised Resources: Service: Smartbank-Icons: en_NZ				
Description	Value	Edit	Delete	
The colour of highlighted text on forms	#257820			

The image used as the title bar and the icon that represents the application can also be configured. The admin console is used to upload the image files to the database.

Please refer to the product feature description sections for examples of how a particular application would be displayed on a phone.

Customer Segmentation

Customers that have registered for a particular service can be categorised in to different segments.

Each segment can define a different set of functions based on the type of customer, for example a mobile banking service may have two customer segments, personal users and business users. The batch payment authorisation function may be excluded from the personal user segment.

Billing rules are also defined at the segment level. This allows the business to charge for a particular service in different ways for each customer segment.

Application and Configuration Management

Each release of a Java mobile application includes a version number. When the application accesses the mobile platform it informs the system of its version number and if it is behind the latest version then the customer will be informed of the new version. If the new version has been marked as mandatory the customer will need to initiate the download of the new application. If it is optional then the customer is asked if they wish to download.



Each application is highly customisable via configuration data that is downloaded and stored on the phone. This data is versioned, so that when something is changed on the server the application recognises this change and downloads a new set of data behind the scenes. The application configures itself using this data and stores it on the phone.

Device Support

A key feature of the platform is the ability to support a large number of different devices using a single Java application instance. This makes device management much easier because we do not need to administer different applications for different device types.

Each product has been tested on a range of devices including Blackberry, Symbian, NokiaOS, Motorola, Sony Ericsson, Sanyo, Palm, HTC, Okta, Samsung, Panasonic, LG, Sharp and Alcatel.

All JME applications require MIDP 2 because they use HTTPS for secure communication with the server.

In the latest version of the Anywhere platform, support has been added for Android and iPhone. TwoSecure and SmartBank applications are now available on Android and iPhone devices.

Android TwoSecure is available on any Android device with Android 1.5 or above. iPhone TwoSecure is available on any iPhone OS 3.0 or above.

Android SmartBank is available on any Android device with Android 2.0 or above. iPhone SmartBank is available on any iPhone OS 3.0 or above.

Application Type Support

A key feature of the version 4 platform is the introduction of multiple application delivery channels. Previously applications could only be provisioned from the Anywhere platform. Now external repositories can be configured to serve applications, for example Apple's App Store.

- + Local Applications: allows JME application downloads directly from the Anywhere platform.
- + Remote Applications: allows the platform to direct users to external systems in order to download their application. For instance the Apple App Store for accessing the iPhone applications.

Operations and Management

Use of Java (JEE) based application servers thus providing standard (known) out of box operations support of the platform.

Comprehensive multi level file logging is provided, as well as activity logging to the database.

Support tools are provided to test the platform and provide feed back on issues.

Load and performance tested in IBM labs using various hardware and configurations. Results of this testing can be provided on request.

The platform includes built-in alarm threshold management to ensure that support staff are notified if there are issues with the platform. When a system error occurs, an alarm is raised which can be pushed to support via email or SMS. Alarm thresholds can be configured via the



administration console thus allowing full control on when they are triggered. Alarms can also be pushed to an external system via an integration adaptor if required.

Alarm message types

The administration console allows the bank to configure the destination addresses for support alarms; and to set the criteria for triggering alarms. Alarms may be generated on an escalating basis.

- + Component – the bank may define which system components will trigger an alarm. The Anywhere support guide contains a list of components.
- + Threshold – the bank can define the number of events (or Threshold) that are required to trigger an alarm
- + Duration – the bank can define the number of seconds within which the threshold can be reached before an alarm is generated.

The ability to apply multiple alarm settings per component is provided to allow more control over the generation of alarms.

Billing

The platform includes a billing module that can be used to rate customer usage. The following billing rules can be defined for each customer segment (may want to charge some customer differently to other customers):

- One off registration charge
- Subscription charge (fixed charge every billing period)
- Transaction charge (applied to any activity)
- Number of free transactions
- Discount
- Can also define different charges for each type of activity

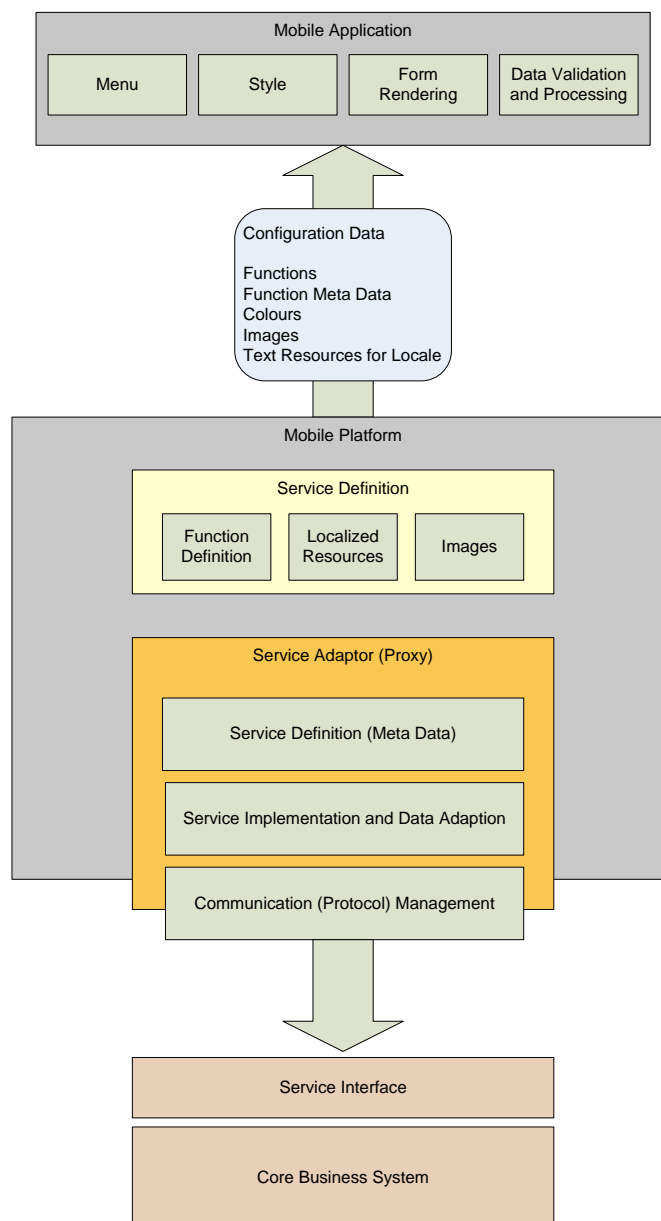
A billing period may be defined as weekly, fortnightly, monthly or quarterly at which point a billing run is executed. Billing records are created for each customer based on their usage. These records can be pushed to an external system for settlement.

Secure Mobile Services (Mobile Banking)

Secure mobile services provide customer access to business services via Java, iPhone, Android applications or a web browser. While this includes mobile banking, the flexibility provided by this module means that the technology can be applied to any business service.

Define Your Own Functions

Many mobile banking solutions define a set of functions and data that can be offered using the product, or customisation of the product is required to meet a bank's requirements. A key feature of the Anywhere platform is that the set of functions and data required for each function can be defined through the use of an adaptor without the need to change the core product itself. This saves time, money and ensures an easy to manage upgrade path over time.





The service adaptor (in orange) is developed to the businesses specific requirements and technical specifications of the core systems to which it is integrating. Once developed the meta data for each function is exposed to the platform. This data is used to define the menus, functions and text that will be downloaded to the phone.

Defining Functions

The following diagram shows the configuration of a particular function. The type of functions are extracted from the adaptor meta data and displayed in a drop down list. The administrator selects which menu will hold this function, the sequence (defines the order of the functions), the icon and focused icon and if there are minimum and maximum limits that should be applied to the amount field.


Application Function Information

Type:

Menu*:


Sequence*:

Icon:

Current Icon: 
Transfer to Own

Clear Icon:

Focus Icon:

Current Focus Icon: 
Transfer to Own

Clear Focus Icon:

Min Limit*:

Max Limit*:

Localised Resources

Edit the: resources for Locale:

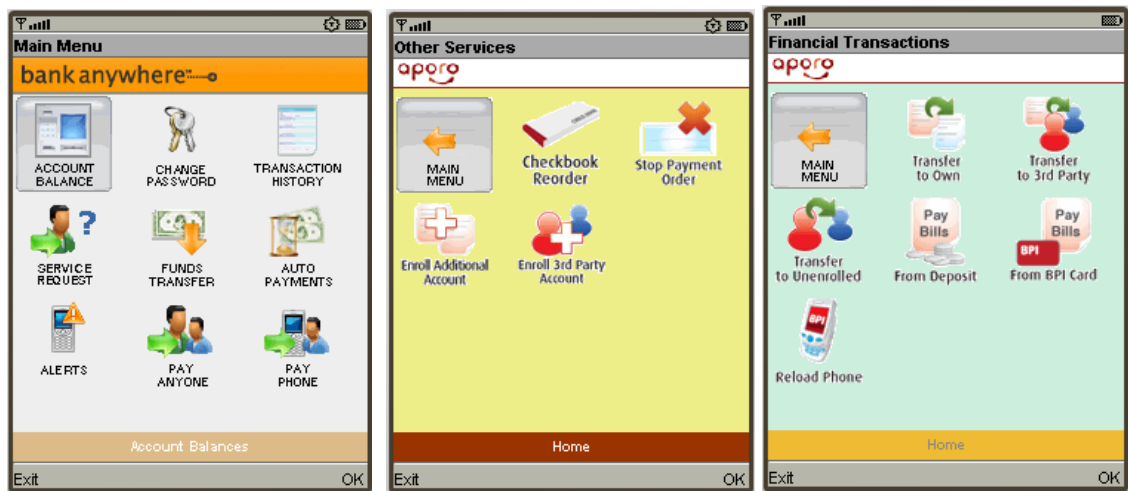
These functions may be added or removed at any time. The next time that a customer logs in they will download the new configuration data and the menu will be adjusted accordingly. This feature is useful where a bank chooses to roll out functionality over time.

Mobile Application

During log in, the mobile application will download the meta data and resources. This data is stored on the device and used to configure the look and feel of the application itself.



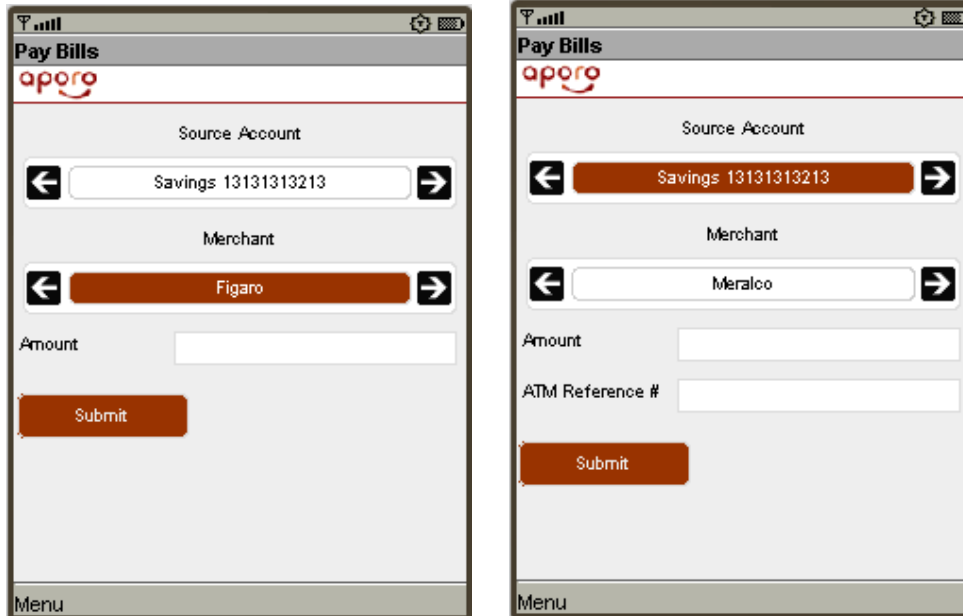
The following shows three mobile banking services. Each one has their own set of functions, icons and colour schemes.



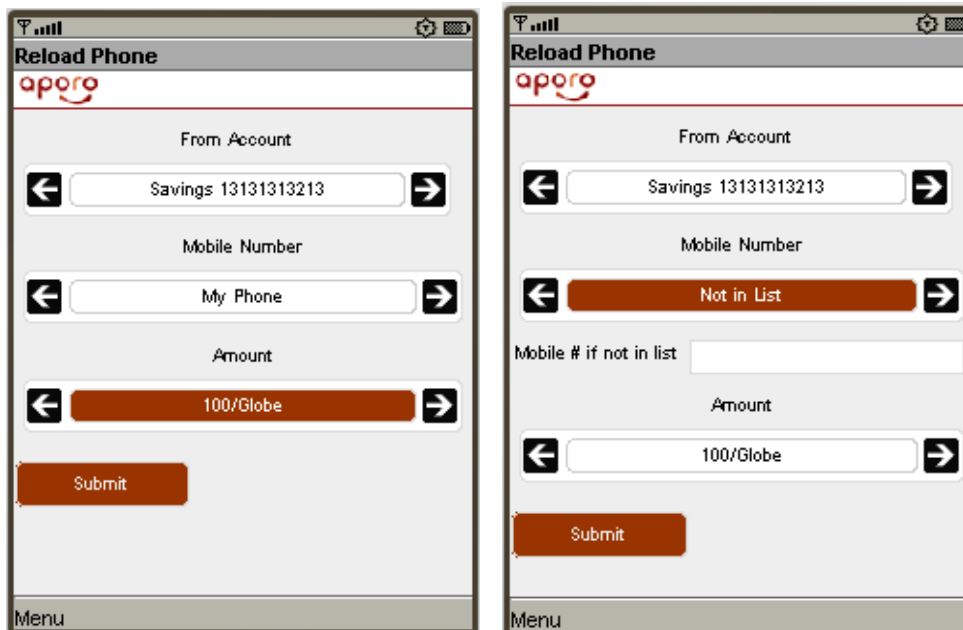
The following shows an example of a funds transfer. Everything shown on this form is customised for this particular bank. The first image shows the fields required to transfer from the customer's CHQ account to their home loan account. The second image shows how the form changes if the customer selects their VISA account. The data required to make the transfer now includes the Expiry Date and CCV.



As another example the following shows an example of a function for paying bills. The merchant Meralco requires an ATM Reference so when that merchant is selected this field appears on the form.



Finally, the following is an example of mobile phone top up. If the customer has a set of preconfigured phones then these are downloaded and displayed in a list (first image). Alternatively they may want to enter a new phone number so they select not in list and the mobile number field is displayed.





iPhone and Android

The iPhone and Android applications utilise the same functions, features and security as the JME application, but are provisioned to the users mobile device in a different fashion. Both the iPhone and Android applications can be provisioned from external application stores. For iPhone this is via the Apple App Store, whilst for Android it can be via the Android Market. Android devices can also accept an Android application directly from the Anywhere platform, provided the users mobile device is configured to allow unknown application sources.

These applications simply wrap the web channel described below. This provides the convenience and security of an application with the flexibility and management of a web interface.

Web Channel

The Anywhere platform now allows the delivery of Secure Mobile Services over the web using XHTML standards.

The web channel can also be configured with its own branding and language. While the same adaptor is used for integration with the backend, the web channel defines its own set of functions. This allows the bank to define different functions for each channel (application versus browser).

The following shows the mobile banking browser version.





Customer Segmentation

The Anywhere platform includes the ability to categorize customers in to segments. Certain functions can be excluded from particular segments if the business wishes to provide a slightly different service to different customer groups.

Possible Mobile Banking Functions

As described, this module allows a business to easily expose any secure mobile service to their customers. As an example the following table provides a list of possible functions that a bank or financial institution may wish to provide.

Name	Description
Account Balances	View a list of accounts and balances
Transaction History	View transactions for a particular account
Change Password	Change a customer's password
Bill Payment	Make a bill payment to a merchant or organisation
Funds Transfer	Transfer money between own accounts
Person to Person Payment	Transfer money to another person's account
Order Cheque Book	Order a new cheque book
Mobile Phone Topup	Put money on my prepaid mobile phone account
Pay a Phone Number	Transfer money to the account of the person with this phone number
Manage Automatic Payment	View and manage my list of automatic payments
Stop cheque	Stop a cheque immediately
Report Stolen Card	Report that my card has been stolen and needs to be cancelled
Enrol Account	Enrol a new account for a particular function, eg. setting up



	payees.
View rates and fees	The customer can view bank interest rates and fees. These are automatically retrieved from bank systems via an exposed XML web services interface.
Calculators	The customer can calculate repayment amounts and timeframes using a mortgage calculator.
Secure mail	The customer may submit requests for information or feedback to the bank using a secure mail feature.
Account top-up	The customer may select a prepaid merchant account to top-up direct from their bank account. The most popular account tends to be the mobile phone account, additional accounts may include any other prepaid account such as the prepaid energy account.
Dual authorisation for payments	Dual authorisation for payments will be offered via a separate, standalone business mobile banking module. This feature will allow small businesses to mandate approval of payments by two authorised approvers from the business accounts.
Business Batch Payments	Set up and execute a set of payments.

Security Features

Every session is supplied with a single use unique identifier in the form of a “token” or “one time password” (OTP) that is embedded into the application on the phone. Login requires the correct user name, password, jar signature and customer token to be submitted. This ensures the application is correct (jar signature), the customer token is correct and the person knows the customer’s password.

When the customer logs on, the user id, jar signature and token are passed to the server over HTTPS. If the three pieces of data are all verified as correct the user name and password are then validated, the customer is logged on only when all data used to identify the customer has been validated. Once logged on, a new token is passed back to the phone for the next login.

The initial jar signature and token is supplied to the phone during the download and activation process. The input of the activation code initiates the request to the server for the initial customer token (or embedded OTP) used to log in. This function enables the bank to offer embedded multi-factor authentication to the customer, and helps prevent unauthorised copying of the application.

Certain functions can be defined as requiring a signature. This triggers the generation of a transaction signature that is unique to the end user and the transaction being submitted. when the server receives the transaction the signature is checked before passing it through to the bank for processing.



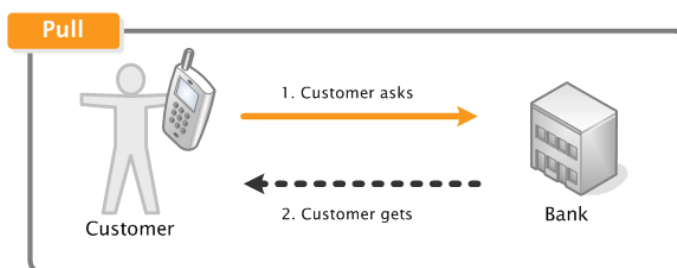
All communication with the server is encrypted using HTTPS protocol.

For a full description of the security features please refer to the Anywhere Security Datasheet.

Messaging Services

Messaging Services allow customers to request or be pushed information using text messaging from their mobile phone.

Text services are commonly restricted to information-based enquiries such as queries about account balances or transaction history. This module allows businesses to offer customers cost effective, efficient and easily accessible access to their details. All devices on the market support text messaging.



Customisation

Messaging Services utilize the same mechanism as Secure Mobile Services (described above) to customise the set of the functions offered via this service. An adaptor is developed to integrate the Anywhere platform with core business systems to expose a set of functions. Meta data is defined for each function and these are exposed to the administration console.

The administrator configures a set of functions and resources using this meta data. The following diagram shows the configuration screen for an account balance function.

SMS Function

Service Definition:

Type:

Sequence*:

Regular Expression*:

Alert Command:

Use Billable Address:

SMS Function

Please select the type of function, the name, the sequence and the regular expression for the incoming message

Save

SMS and Email Message Templates

Edit SMS Templates for Locale*: **Edit**



Every function uses a regular expression to match it with the text message submitted by the customer. Regular expression is a technical term for the definition of rules for matching text inputs to a particular query.

Each function defines a set of message templates that can be configured via the administration console. This allows the bank to define the messages that are sent to the customer. As shown below the administrator can set up both SMS and email templates for each function and supported locale.

The message template defines the content of the response message for your customers. Some templates have parameters which are tags in the message. These tags are replaced with specific information returned from business core systems such as the bank account name, balance or transaction info.

Localised Resources: Platform Defaults: en_NZ				
Description	Value	Edit	Delete	Promote and Edit
- Email HTML	Your account balances are for(@accname: @accbal)endfor			
- Email Subject	Email Subject			
- Email Text	Your account balances are for (@accname: @accbal)endfor			
- SMS Message	for(Account: @accname with balance @accbal)endfor			

Localised Resources: Provider: Fronde: en_NZ				
Description	Value	Edit	Delete	Promote and Edit

Localised Resources: Service: TextBanking: en_NZ			
Description	Value	Edit	Delete

Multi Language Support

Messaging Services can be offered in multiple languages from the same deployment. The administrator sets up message templates for each language via the admin console.

The customer selects a particular language during registration and will receive messages in that language for this service.

Short code management

Text messages are requested via a “short code” or short mobile phone number. In order to ensure that enterprises have a common short code (e.g. 2265 for “BANK”) in their market, the short code must be registered to the business by every local mobile operator.

Typically businesses will connect into a single message aggregator who provides connections into all the local mobile operators, and will register the preferred short code(s) on the behalf of the business.

Message Priorities

The Anywhere platform provides the ability to apply priorities to certain services or customer segments. This is significant where a business is offering a range of services including some that are time-critical to customers.

Most mobile operators throttle the delivery of messages into their network (usually at around 30 messages per second maximum). If the business is delivering batch files including thousands of messages at a particular time, these messages may hold-up more critical services or customers. The platform will scan messages for priority rules, and will move higher priority messages to the front of the queue for delivery.

Message error handling

Spelling and formatting

When customers enter content into the body of a text message, spelling and formatting errors are common as this is a free text query. To ensure that business systems receive consistently formatted queries from text users, the Anywhere platform includes comprehensive message parsing and error handling functionality. Typical user errors include:

- + Substitution of upper and lower case characters
- + Substitution of letters for numbers and vice versa (eg O for zero or L for 1).
- + Incorrect spelling, e.g. BLANCE for BALANCE
- + Additional words or phrases, e.g. MY NAME IS PIERRE AND I WOULD LIKE MY ACCOUNT BALANCE.
- + Inclusion of punctuation, e.g. BALANCE! Or "BALANCE".

The platform will scan every message received from a user, handle standard formatting errors such as punctuation and casing, and determine which query they are trying to execute. A cleanly formatted query is then passed through to the business systems for processing.

Definition of standard query formats

The Anywhere platform's administration console provides a user interface to enable the business to configure and define the specific wording for allowable requests by the user and to define any alternative wording that will be accepted. It is recommended that the business be flexible about what it will accept, for example it could accept BAL or BLA for balance requests regardless of where these characters are inserted in a sentence.

- + BAL
- + BALance
- + I would like my account BALance
- + "BALance"
- + BLAnce.

The contents of this field are not case sensitive and the wild card character [*] can be used. For example the regular expression for an account balance request could be BAL. BAL* is mapped to the request account balance function, in this example any message containing the first 3 characters BAL would return account balances to the end user.



The business can optionally mandate specific formatting such as, BALANCE for account balance, and refuse to accept incorrectly formatted requests from the customer. It is strongly recommended that the business be flexible about what it accepts from the customer.

It is possible to set up multiple rules to cater for common user error scenario's that become apparent after the system has gone into production. An example of this may be where the regular expression BAL* is mapped to the balance request function, if users were regularly substituting the number 1 for the letter l, you could create a new function that mapped the regular expression BA1* to the 'account details' function.

Generic error responses to the customer

Where the Anywhere platform can not interpret the customer's request, a standard "help" response can be sent to the customer. This is configurable by the business via the administration console. In general it is recommended that the response contains useful information to the customer to enable them to gain a successful transaction.

- + Not recommended: "Your query was incorrectly formatted. Please format it correctly so we can send you a response."
- + Recommended: "Sorry, we could not work out what info you were requesting, to get your balance text BAL to 2265, or text HELP to 2265."

Business system errors

Where the core business system returns an error, the platform will send the customer a standard system error response. Bank systems can return many different error conditions and in general these can be interpreted to the customer as: "We apologise as the mobile banking service is currently unavailable, please try again in 10 minutes."

Reporting of errors

All messages sent to and from the customer are logged. These can be viewed via standard reports supplied with the administration console. It is recommended that the bank review the reports regularly during early rollout of the service in order to review whether customers are consistently misspelling a particular phrase or struggling with a certain query type. The service can then be configured to handle these additional error conditions via the administration console.

Possible Messaging Functions

As described, this module allows any business to easily expose any service to their customers using text messaging. As an example the following table provides a list of possible functions that a bank or financial institution may wish to provide.

Feature	Description
Account balance	The customer may request the balance of one or more accounts using SMS. In general most banks allow the customer to select which accounts they would like to view balances from, and then all balances are returned in a



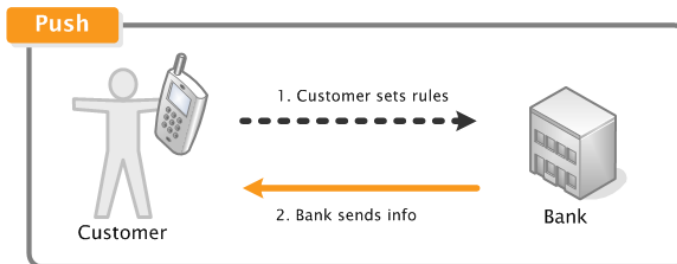
Feature	Description
	<p>single response.</p> <p>The bank can define the required phrase for example:</p> <p>BAL</p> <p>BALANCE</p> <p>The system parses (or scans) the message received from the customer and sends a “clean” query to bank systems.</p>
Funds transfer between own accounts	The customer may transfer funds between their own accounts.
Transaction history	<p>The customer may request transaction history of particular accounts. The last five transactions will be returned. The bank may configure or define the allowable phrases for transaction history requests, for example:</p> <p>TH SAV</p> <p>HISTORY SAV.</p>
View rates and fees	<p>The customer may request information on current interest rates and fees by texting a defined phrase. For example:</p> <p>RATES</p> <p>MORTGAGES</p> <p>INTEREST.</p>
Stop Cheque	<p>The customer may request that a specific cheque be stopped by texting a phrase including the cheque number, such as:</p> <p>STOP 123456789</p> <p>The bank returns confirmation that the cheque has been stopped, and the fee that has been charged for this service.</p>
Cheque status	<p>The customer may request the status of specific cheques by texting a phrase including the cheque number, such as:</p> <p>STATUS 123456789</p> <p>The bank will return the payment status of that cheque.</p>



Feature	Description
Chequebook request	The customer may request a new chequebook for a specific account. The bank can configure the required phrase, such as: REQUEST CURRENT
Help	The customer may request help at any time via texting HELP. The system will respond with suggestions on how to format a successful response.

Alerting Services

Alerting Services allows customers to subscribe to alerts that are delivered to their mobile phones using text messages. This module offers two main types of alerts – time based alerts, and event based.



This module is an extension to the Messaging Services module described in the preceding section. It shares the same customisation, function and message template functionality described above.

The following sections describe additional functionality that is specific to alerting services.

Alert categories

Time based or subscription alerts

The Anywhere platform allows customers to subscribe to alerts that are triggered at specific recurring times. For example a customer subscribes to get their account balance at 9am every morning.

With subscription alerts, the customer registers for that alert and it is stored within the Anywhere platform. When the alert is due to be delivered, the platform requests and retrieves the information from the core business system, applies the configured message template and sends the text message to the customer's mobile phone.

If Messaging Services are already implemented as part of the solution, then this module can share the same adaptor that is used to integrate with the core business systems.

Event based or business alerts

Event based alerts are triggered by events that occur within business systems and therefore outside of the Anywhere domain. This type of alert generally requires some form of development work to be undertaken within the business systems to enable the event to be



triggered. Some software products provide standard event based alerts for email or SMS as a standard part of the offering.

The Anywhere platform provides a set of web services for initiating these types of alerts. The business can integrate with these services and manage the scheduling and delivery of the messages. The following events are examples of this type of alert:

- + Account goes into overdraft or below a certain threshold
- + Mortgage/Interest rate changes
- + Salary deposit
- + Transaction over certain size occurs
- + Credit Card payment due
- + Payments have been against a particular credit card account
- + Special offers and promotions.

Message scheduling

The Anywhere platform includes message scheduling (store and forward) capability. When subscribing to a particular alert, the customer may choose to define a window within which they want the messages to be delivered, eg. between 8am and 10pm.

The business may also define a delivery time for particular event based alerts. The Anywhere platform will store these messages and send them at the requested time. This feature is particularly important where certain alerts are likely to be triggered via events occurring during the night. Most customers will not be grateful to receive notifications at 3am.



TwoSecure

TwoSecure™ is a multi factor authentication solution that provides secure identity verification. TwoSecure™ generates One Time Passwords (OTP) that can be used to secure log-ins and/or transactions.

TwoSecure™ may be integrated with a web site such as Internet Banking to provide additional security at log-in or applied to specific transactions, eg. payments over \$500.00.

TwoSecure™ may also be integrated with an enterprises network equipment to protect remote access to networks or specific resources within a network.

OTPs can be generated using a Java Application which is downloaded to the user's mobile device or sent to the user via SMS or Email.

Key benefits of TwoSecure are:

1. **Secure Identity verification:** TwoSecure supports tiered security models including transaction signing, a function which is unique to TwoSecure and differentiates it from similar hardware solution.

The product has been independently audited against US FFIEC guidelines and passed internal security audits for two of the largest financial institutions in Europe.

The TwoSecure mobile application uses a time based algorithm based on a highly secure digest and two unique security codes generated during registration. This ensures that each OTP generated is unique to the credentials of that user. Fronde Anywhere has patents granted for the elements of the security model.

2. **Easy and convenient for users:** TwoSecure is easy and intuitive for customers to use providing a better user experience than competing products. TwoSecure offers increased convenience for users as they do not have to carry additional security devices.

End-user feedback on the experience has uniformly been that the user refuses to give up the product and go back to hardware offerings.

3. **Good for large volumes of users:** TwoSecure is easy to support and distribute to large numbers of customers or staff. It is extremely cost effective as there are no distribution or unit costs as the mobile phone replaces the need for token generators.

TwoSecure is an out-of-the-box solution that supports the requirements of many geographic markets and offers a high degree of configurability as standard.

TwoSecure™ provides web service interfaces for integrating user management and OTP services. This allows for easy integration with registration channels such as IVR or Internet as well as web sites for authentication.

TwoSecure™ also provides a Radius interface for OTP validation to provide integration with network appliances such as firewalls, proxies and domain controllers.

Functions

TwoSecure provides a set of functions for generating OTPs. These functions may be turned on or off at a service level depending on what the business requires.

Each function can be configured with or without a pass code.

Standard OTP	No additional seeds; simply generate a one time password.
Challenge OTP	Request a challenge that is used as a seed in the OTP generation. The challenge represents a piece of information that is specific to a transaction or resource, therefore the OTP can only be used for this transaction.
Transaction Signed OTP	OTP includes transaction details (account details and amount) as seeds in the OTP generation. The OTP is only valid for this particular transaction thus preventing man in the middle or man in the browser attacks.

Domains and Identity Management

The Anywhere platform supports the definition of user domains. Domains may be configured and made available to a particular TwoSecure service. Users of that service can register different identities for the different domains. This allows a user to use a single service and hence mobile application to generate one time passwords for multiple domains.

For example, if a service defined three domains such as hotmail, gmail and yahoo. A user may register for the TwoSecure service and then define an identity for each domain. When the user logs in to their hotmail account they can use the TwoSecure application to generate a one time password that can be used in this domain.

Highly Configurable

The following table lists the TwoSecure parameters that can be configured via the administration console.

OTP validity period	The length can be configured to last from 1 second to 5 minutes
Length of OTP	The length of the OTP can be configured to provide the optimal balance between security and ease of use. A typical length is 9 characters.
Character set of OTP	Hexadecimal or numeric. TwoSecure can be configured so that the OTP contains only numeric characters if used from numeric only devices (such as point of sale devices). Otherwise, the OTP will contain hexadecimal characters, which includes the digits 0-9 and the characters A-F.
Pass code	A pass code is a numeric code that is known to the user and used as a seed in the OTP generation. Therefore if a user's phone is



stolen it is not possible to generate valid OTPs. This can be turned on or off at a service level.

Length of pass code.

The pass code length can be configured. Typical length is 4.

Bulk provisioning of users

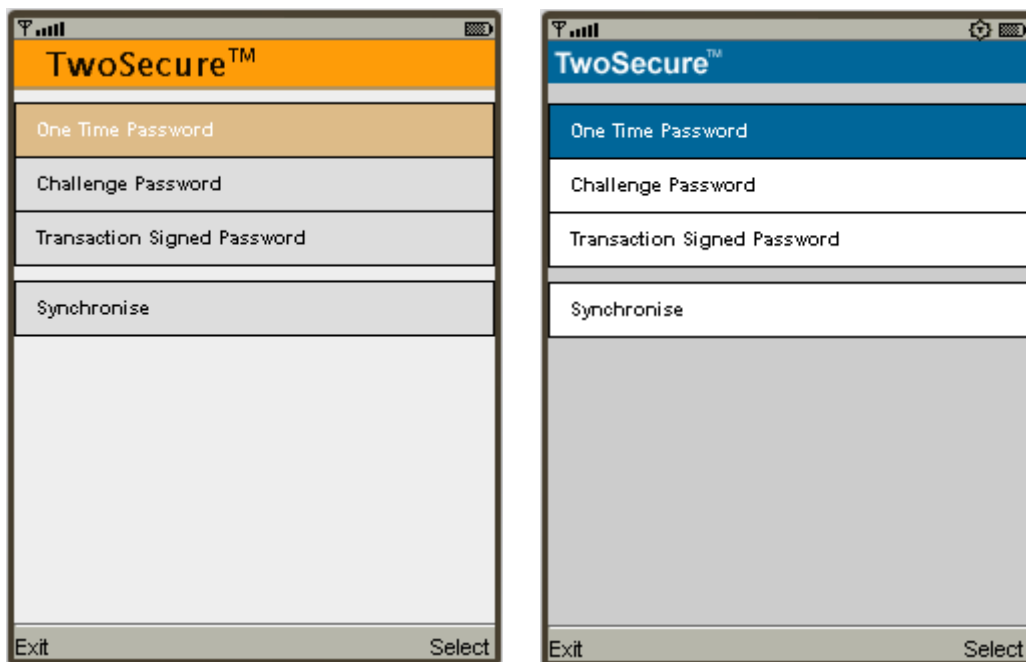
TwoSecure provides several methods for provisioning a large number of users at once. This allows an administrator to easily add or convert an existing user base to TwoSecure. The administrator can choose to manually enter a list of users directly into the administration console, to import an excel or comma delimited file containing user details, or to directly import users from an existing LDAP repository such as Active Directory.

Mobile Application

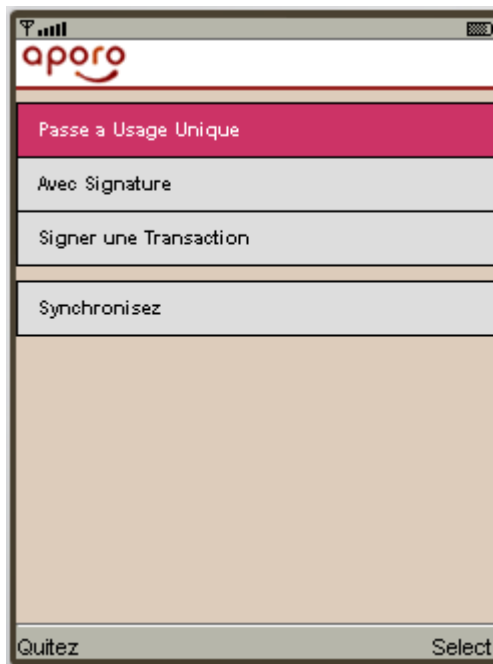
TwoSecure™ provides the option of a JME (Java), iPhone or Android application. When the end user initiates the download, the server recognises the type of phone and directs them to the appropriate application. This application contains the presentation layer, one time password (OTP) generation and validation logic.

TwoSecure does not require mobile data once it has been downloaded to the mobile phone, and can be used Anywhere in the world, any time.

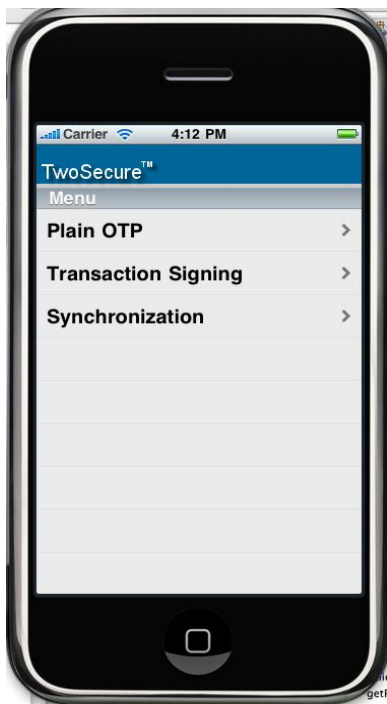
The colours and screen title bars can be configured via the administration console at run time. This allows out of the box customisation to meet any specific branding. The following examples show how the menu screen looks using two different colour schemes.



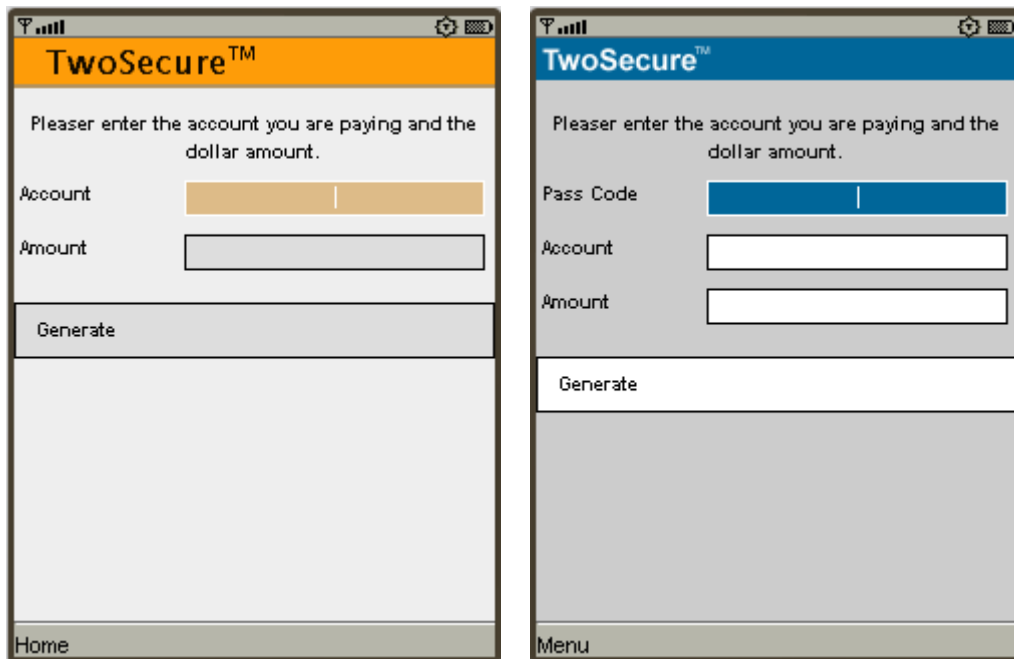
Here is another example which shows the menu in French. A business may choose to offer the service in multiple languages. Users can select the desired language during registration.



The following shows the menu screen for the iPhone and Android applications.

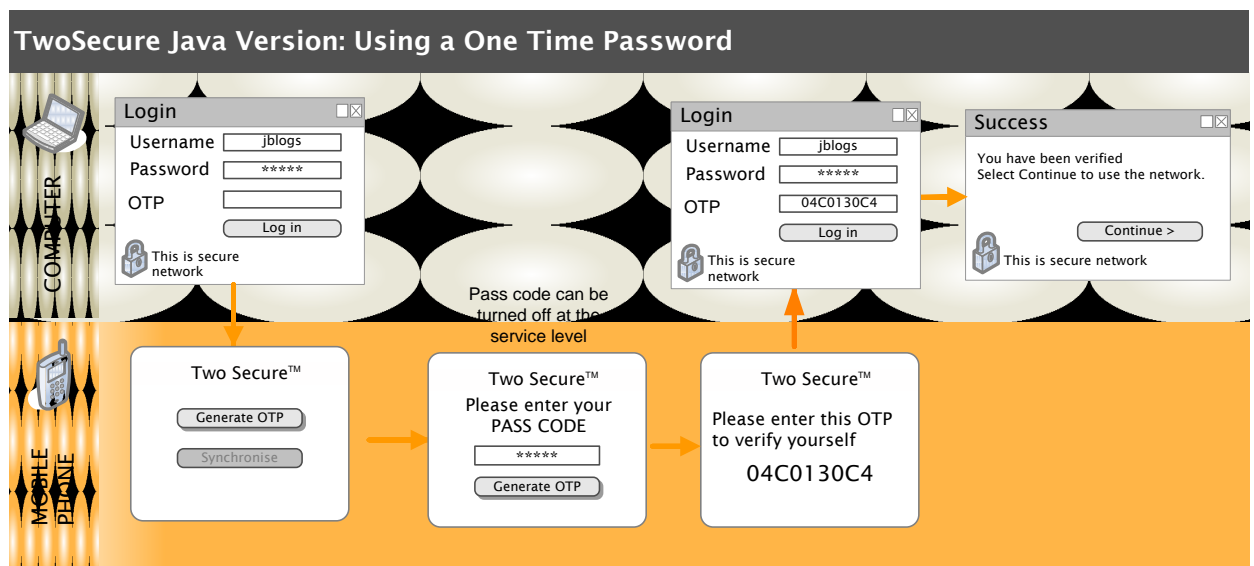


The forms for transaction signing request the account details and amount being paid. The blue example includes the pass code while the orange configuration has turned the pass code off.



Using TwoSecure

The following diagram shows how TwoSecure is used to log in to a web site or network remotely.



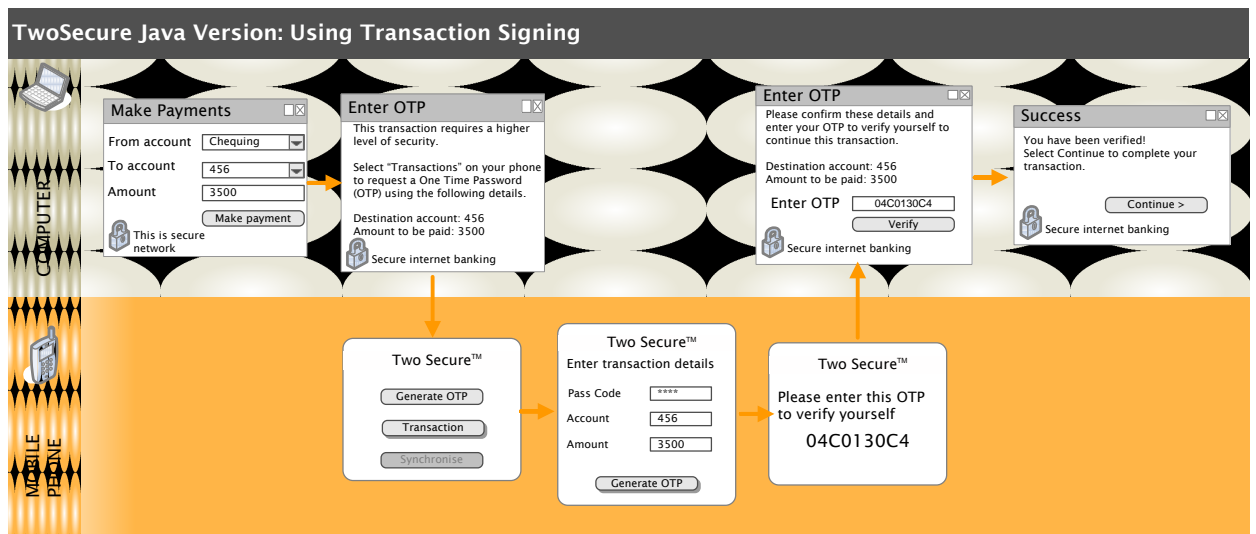
1. User is presented with a form to enter their credentials and one time password.
2. User enters their user name and password and starts TwoSecure
3. User selects generate and enters their pass code. The pass code can be turned off if not required.
4. Application generates and displays the time limited OTP



5. User enters OTP in to form and submits.
6. Server validates credentials and asks TwoSecure to validate OTP
7. User is given access

Using Transaction Signed OTP

The following diagram shows how a transaction signed OTP can be used to protect particular transactions from man in the middle attacks.



1. User submits a payment within Internet Banking
2. Because amount is above a threshold, Internet Banking requests a transaction signed OTP
3. User starts TwoSecure and selects Transaction
4. User enters pass code, account and amount and selects generate
5. User is presented with OTP which is entered in to Internet Banking
6. Internet Banking validates the OTP using TwoSecure and accepts the payment

SMS TwoSecure

The SMS version of TwoSecure provides the ability to deliver OTPs to a customer's phone via SMS. This service compliments the Java Version to include customers that do not have Java capable devices or data plans enabled.

To use SMS TwoSecure, the user must verify their phone number. TwoSecure can be configured to provide SMS based phone authorisation. If this function is set up, the customer must text in



an authorisation code before they can use TwoSecure. This validates that this customer has this phone number.

TwoSecure SMS also supports pass codes and transaction signing, whereby the customer includes their pass code or transaction details in the request for an OTP.

TwoSecure SMS supports configuration for both push and pull requests. In the SMS pull configuration, the customer requests an OTP by sending an SMS to a predefined short code. The TwoSecure server sends the customer's OTP in a text message response. This allows the customer to generate an OTP using SMS any time.

In the push configuration, an OTP is delivered to the user via SMS based on a trigger from another system, such as Internet Banking. The business system integrates with TwoSecure (using web services) to initiate sending the OTP to the specified customer. Therefore, the business has the freedom to either automatically push an OTP to the customer or provide a Generate OTP button that the customer can use.

Integration

TwoSecure provides services for validating and generating one time passwords. All generation services are accessed using web services, while validation services may be accessed via web services (for web site integration) or via Radius (for network integration).

TwoSecure interface specifications can be provided on request.

Radius Integration

TwoSecure can be used to add second factor authentication to VPN or email access. When the customer logs into a VPN or email system remotely, they will be prompted for their standard username and password, as well as a one time password. The user can generate the OTP using TwoSecure Java version or request one using TwoSecure for SMS. This one time password is then validated by TwoSecure before allowing the user access to the system.

The firewall that is providing the remote network access is integrated with TwoSecure via a standard Radius interface. Radius is a well used standard for network authentication so is supported by most existing firewalls.

In addition to the standard TwoSecure Java and SMS features, TwoSecure Radius Solution provides the following **features** out-of-the-box:

Features	Description
Multiple Deployment Configurations	<p>TwoSecure supports three deployment configurations. For a full description of each option please refer to the TwoSecure Enterprise Configuration Guide.</p> <p>Daisy Chained: TwoSecure sits along side the user authentication server. Firewall submits user name and password to authentication server and OTP to TwoSecure.</p> <p>Radius Challenge: TwoSecure sits between firewall and authentication server. User name and password is submitted to authentication server via TwoSecure. TwoSecure issues radius</p>



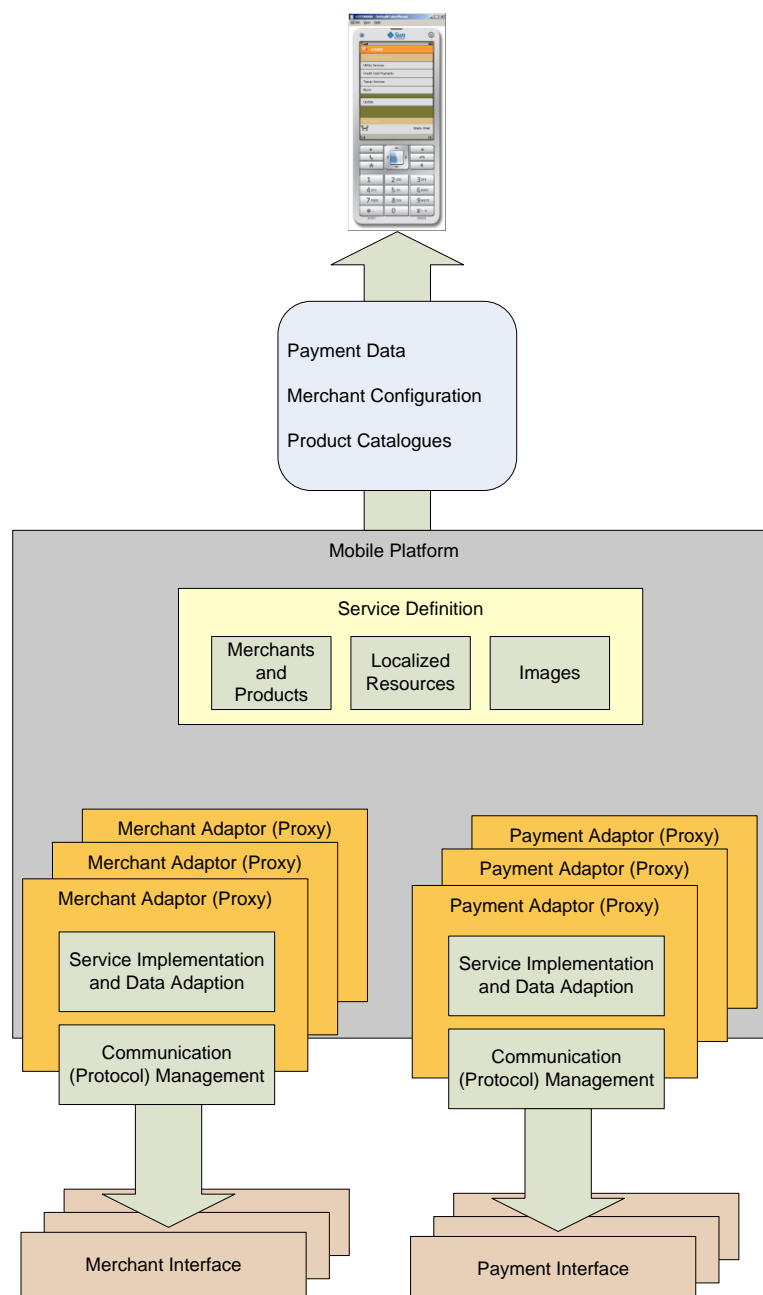
Features	Description
	<p>challenge to obtain the OTP from the user.</p> <p>Delimited: TwoSecure sits between the firewall and authentication server. The OTP is concatenated with the user name using a delimiter. TwoSecure extracts OTP and validates it before forwarding the user name and password to the authentication server.</p>
Multiple Radius Protocols	TwoSecure supports PAP, CHAP, MS CHAP and MS CHAPv2.
Create one or more radius clients	TwoSecure™ clients are the network access points that are submitting the OTP validation request (eg. Firewalls). The server will only accept requests from clients that are configured, any other requests will be ignored
Create one or more radius terminal servers (domain controllers)	Configure the Terminal Servers (Domain Controller) that the TwoSecure™ servers make Radius authentication requests to. The TwoSecure™ Radius server will try each server in the order that they were configured until it receives a response from one of them
Delimited	Configure the ability to have the username and OTP concatenated in the one field (eg. "Joeblogg;4587AB90DA1).
Permissive	Ability to use TwoSecure when only some users require two factor authentication. When Permissive is on, the server will only attempt to authenticate those users that are registered.
Challengeable	Allows the TwoSecure™ server to issue a Radius challenge to get the user to enter an OTP.
Reply message	Configures message sent to the VPN client when challengeable is set.

Mobile Ordering and Payments

The Payments module provides a Java application for ordering and paying for goods or services via the mobile phone.

Because it is part of the Anywhere suite of products it shares the same security, management and customisation features as the other modules described here. The key additional functionality provided by this module is the definition of merchants, product catalogues and payment providers.

The following diagram shows how adaptors are developed and plugged in to the platform for integration with Merchants and Payment Providers. A service is configured to use these adaptors and the configuration details are downloaded to the application installed on the phone.

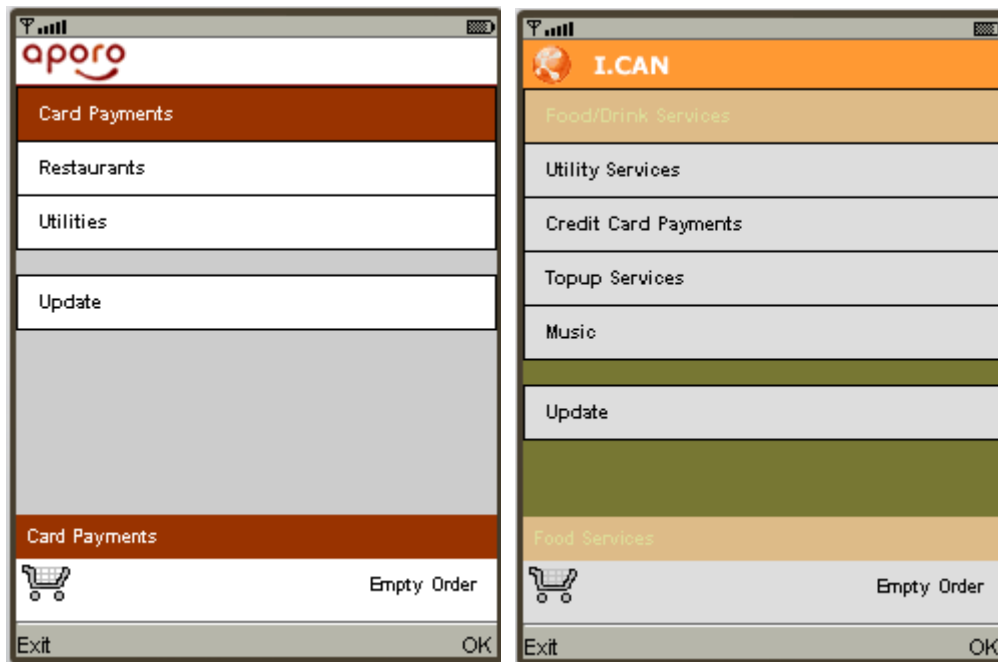




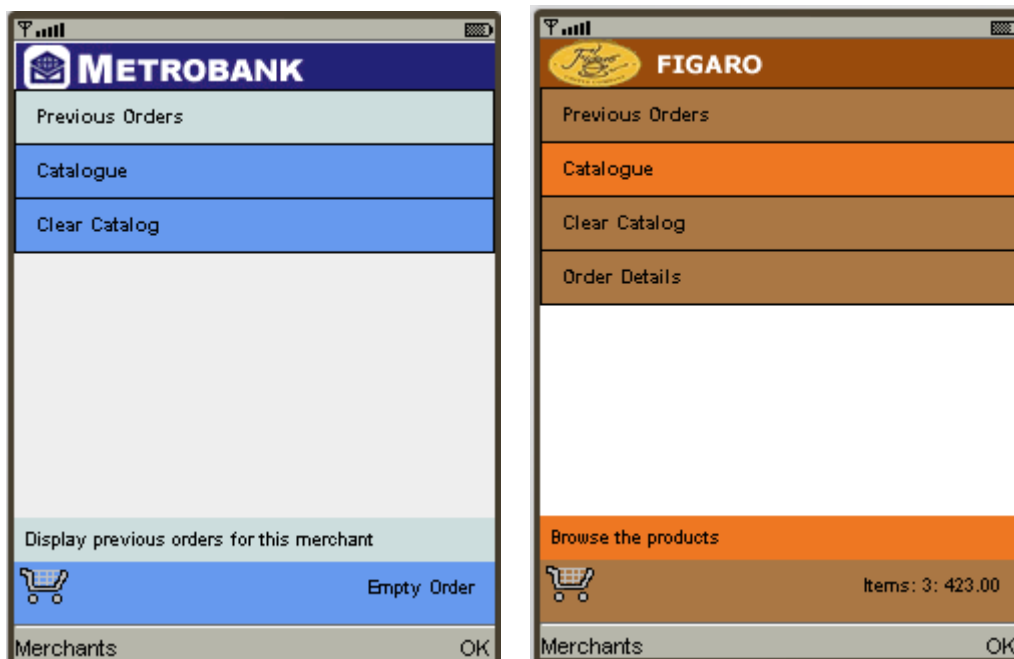
Merchants

The Payments module supports multiple merchants within a single service. The concept is to provide users with a complete shopping portal that is convenient and easy to use.

Merchants can be grouped in to categories to simplify access. The following screen shows two examples of merchant categories on the phone.



Each merchant defines their own colours and title image thus allowing them to present their brand to customers. The following screens show the main menu for two different merchants.



Two types of merchants are available, order or payment only. Order merchants allow customers to build an order by selecting from a product catalogue. These items are placed in a shopping



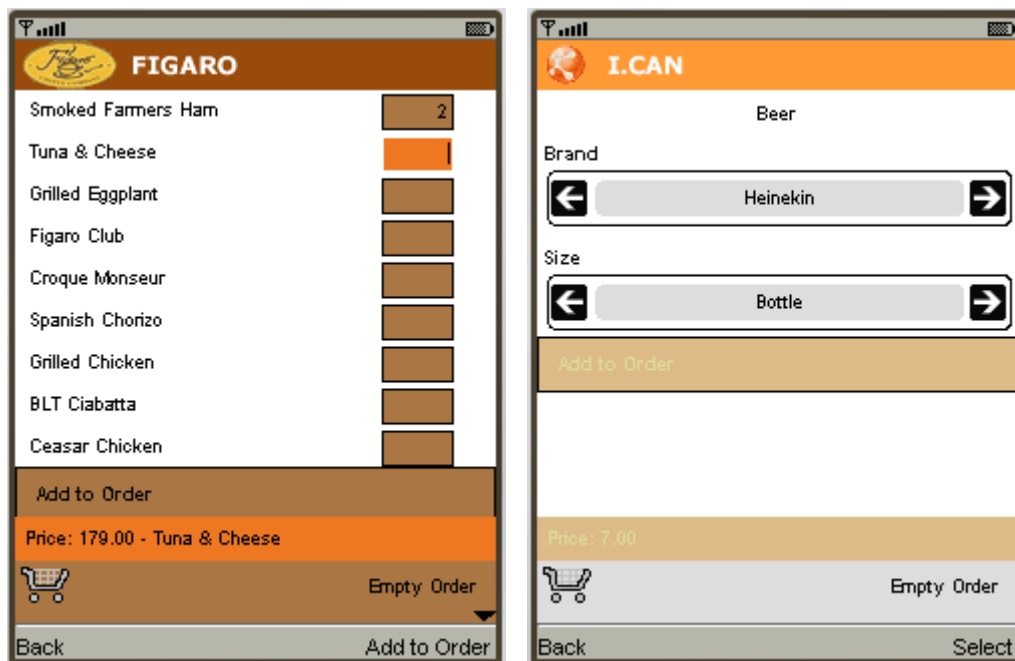
cart until the customer is ready to purchase the items. Each product item has an associated price which is calculated as the order is built.

Payment only merchants allow customers to pay for single items or services and may involve the customer determining the amount to pay. For example topping up my prepaid mobile phone or paying my gas bill.

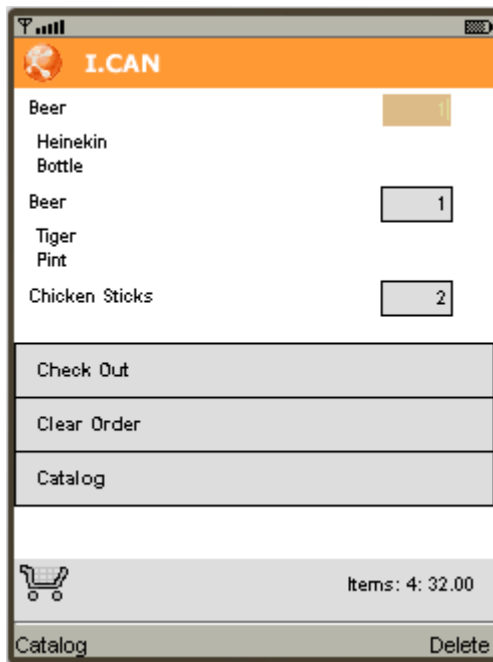
Product Ordering

Each merchant defines their product catalogue. The structure of the catalogue determines how it is presented on the phone. The product may simply be presented as a single product with a price or it may be built from a set of options. The following screen shots illustrate this difference. The First screen shows a list of products allowing the customer to select desired quantities of each product and add these to their order.

The second screen shows a particular product, beer, which has options of brand and size. The customer selects their options and can define quantities within the shopping cart itself.

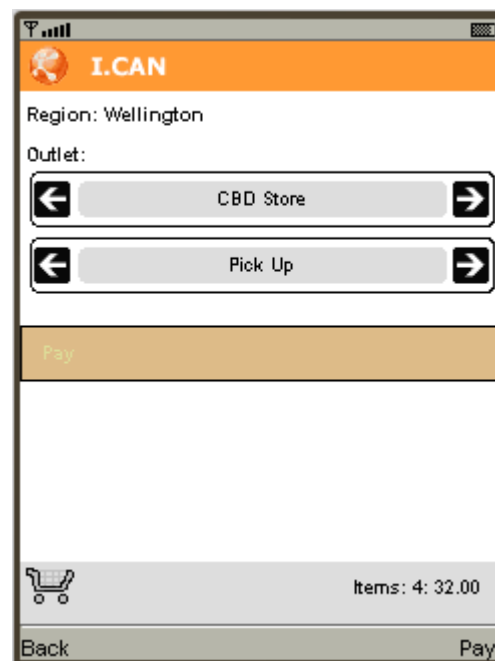
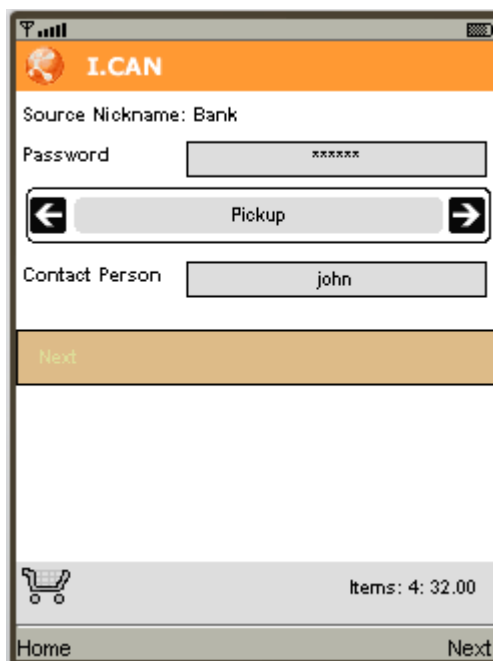


The customer selects various products and adds them to their order. The following screen shows the resulting shopping cart. The quantities for each product can be adjusted from this screen.

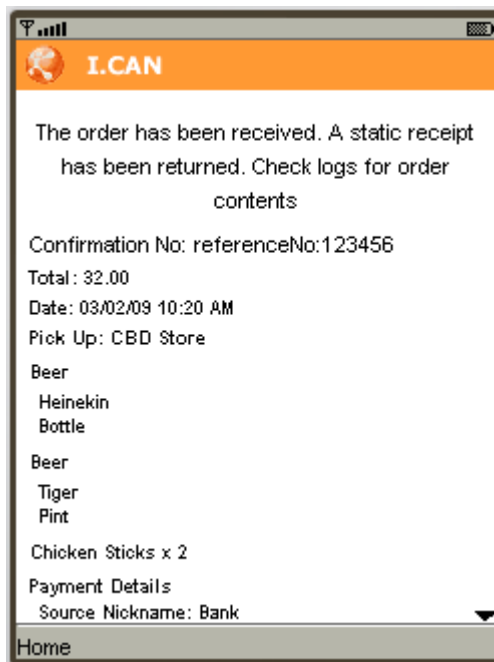


Once the customer has created the order they can check it out. This presents them with the following forms. The customer enters their payment password, the procurement option (pick up or delivery) and name of the person who will receive the order.

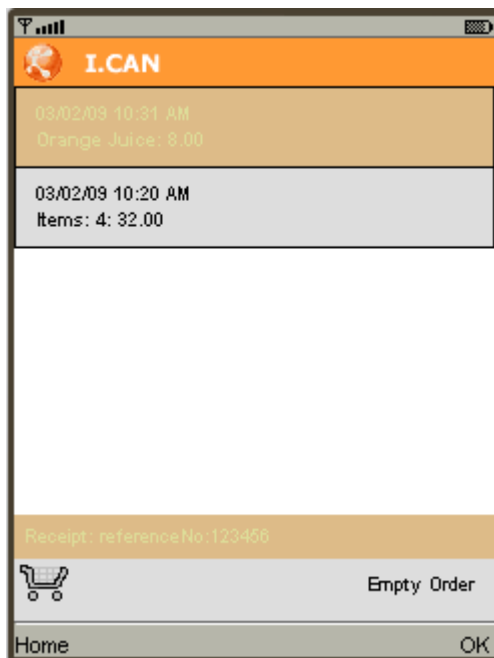
If picking up, they can select the outlet and pick up option, which may be take away, dine in, drive through etc. These options can be configured at a merchant or outlet level.



Upon submission the order is processed by the Anywhere server. The payment details are submitted to the appropriate payment provider and if successful the order is submitted to the merchant. The payment details and merchant response is shown to the user and can be used at point of sale.



Each order is saved on the phone and can be accessed from the main menu. The following screen shows a list of this customer's previous orders. The customer can select an order and use it as the basis of a new order, thus providing the customer with a list of favourites for reordering.



Pay Only

Pay only merchants allow customers to pay bills or top up accounts. Unlike product ordering there is no shopping cart, but rather a list of payment options. The following payment screen illustrates how a customer may top up their prepaid mobile phone account. The customer selects the payment method, enters their password, the amount and their mobile phone number. Once submitted the customer can access their previous orders to keep topping up this phone number over time.



Payment Providers

A payment provider supplies the system with the facility to pay merchants. Users and merchants must have an account with the provider for it to be available as a payment option.

Payment providers are configured via the administration console. Each one references a specific adaptor that is developed and plugged in to the platform. The adaptor integrates with the payment system and performs any data conversion of connection as required.

Once configured these payment providers are linked to the merchants that support this provider and made available to customers for registration of payment methods. When a user submits an order the appropriate payment methods are made available for selection.

Security Features

The Payments module inherits all of the security features of the platform. This ensures that the application is linked to a specific user and there is only one instance of the application.

When an order is submitted a unique token is included and checked by the server. Upon completion of the order a new token is generated by the server and returned to the phone. This token is stored and used for the next order.

All communication between the phone and the server is encrypted using HTTPS.



Registration Process

The Anywhere platform supports flexible registration scenarios in order to maximize the uptake of mobile services.

Administration console registration

Customers can be managed via the Anywhere administration console. The following screen shot shows the customer details screen. This screen shows existing registrations for services as well as a list of service to which this customer can register.

Customer

Customer Id:* antony
Phone Number:*
Email Address:
Start Date: 26/01/09
Password:
User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)
Provider: Fronde
Authorization Code: 81856
Is Authorized: true
Status:

[Save](#)

Customer

Details for a customer, phone number (also if they are authorized or not) and status

Available Service Definitions

Available Services: [Register](#)

Existing Registrations

Service Definition	Status	Start Date	End Date	Edit
TwoSecure	Pending Activation	02/02/2009		
Aporo	Activated	26/01/2009		

Identities

Domain Alias Edit Delete

[+ New User Identity](#)

Business registration channels

The Anywhere platform exposes a set of web services for managing customers and registrations. Businesses may register their users via any channel. The channel is responsible for initial authentication of the user, collecting their mobile phone number, and passing the mobile phone number with a customer identifier to the Anywhere server.

It may be appropriate to offer customers a choice of channels for registration in order to maximise the potential user base for the service. The preferred or suggested channels are:

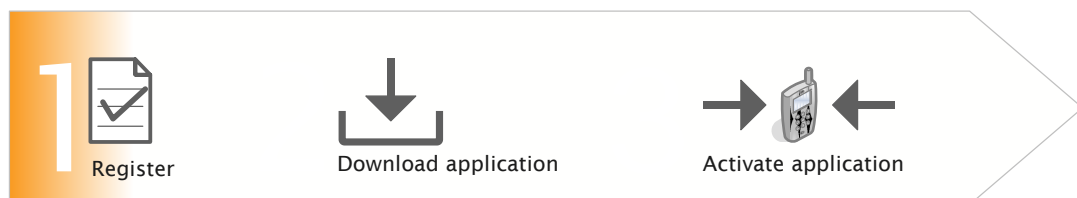
- + Existing Internet channel
- + IVR / contact centre.

Fronde Anywhere provides generic templates and help guides for recommended business process flows for registration; and recommendations for instructions and language that should be provided to end users during the registration and download process.

Registration process

Registration overview

anywhere registration process: Java Version



Before a customer can use an Anywhere mobile application, they must first register for the service. This involves three stages:

1. **customer registration** – the customer authenticates themselves with a business channel, their Anywhere profile is created on the server, and the SMS containing the URL for download is sent to their phone. If activation is enabled, the customer's activation code is returned and displayed to the customer.
2. **download application** – the customer clicks on the URL and downloads the application to their phone.
3. **activate application** – If user activation is enabled, the customer inputs the activation code into the Java application. If not enabled the activation code is embedded in the application and submitted behind the scenes. The server receives the activation code and validates that it is correct before activating the customer's registration.

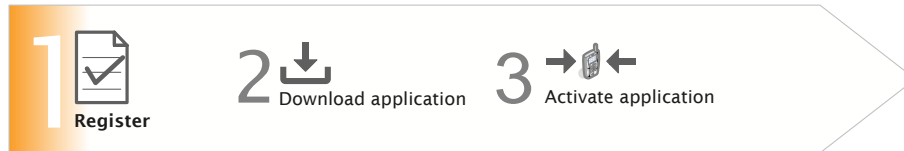
Stage 1: Registration at the channel

Anywhere registration assumes that the customer is who they say they are, or in other words, that the customer has been authenticated via a trusted channel. Possible channels for registration include the Contact Centre, interactive voice response system (IVR), ATM or Internet.

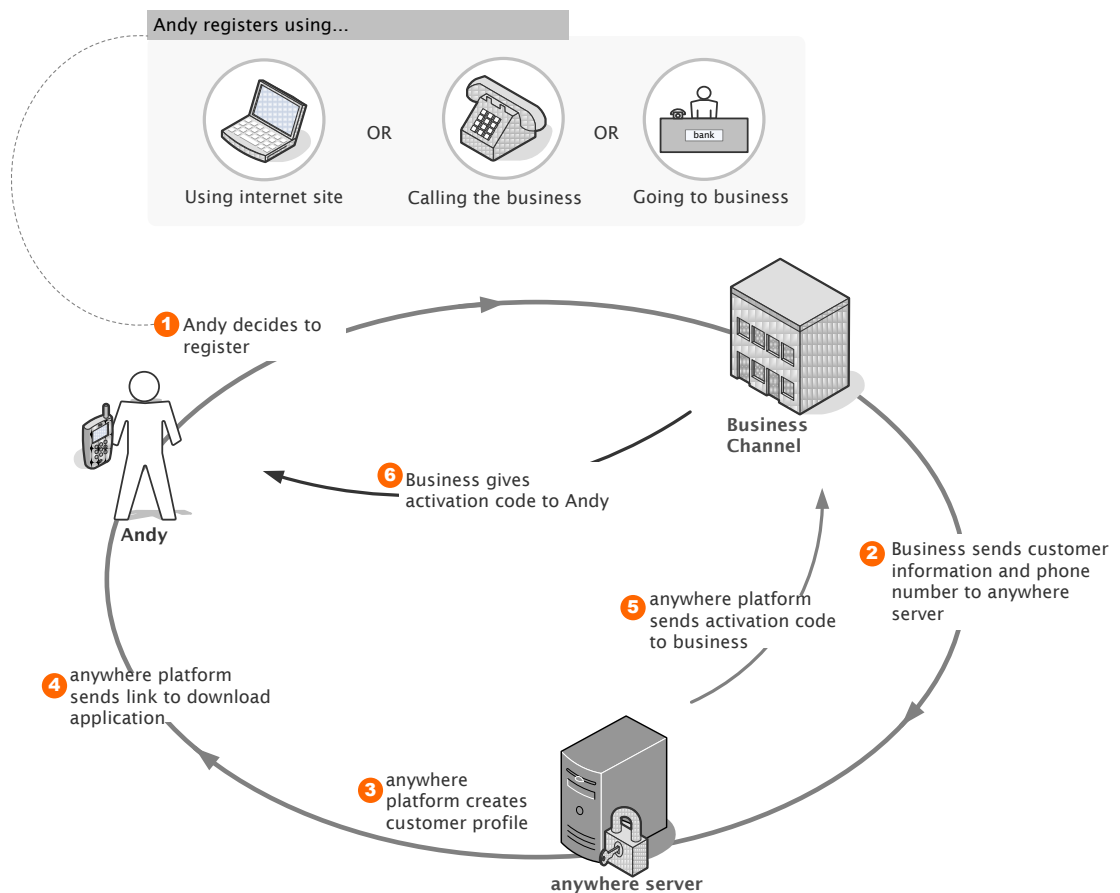
The Anywhere server exposes web service interfaces for customer registration and management. This allows a bank to integrate existing channels such as an Internet site directly with the server.



Alternatively, if it is not appropriate to implement this direct integration, the Anywhere platform provides an administration user interface for managing customer profiles. This could be used by Contact Centre staff to provision customers.



Registering for Java Version

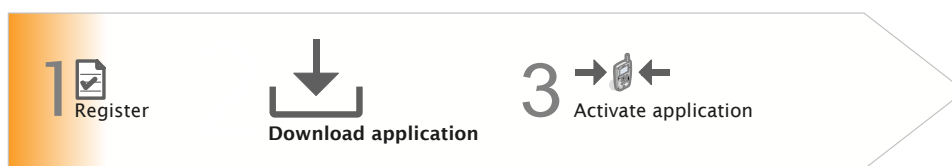


1. Customer registers for service, using existing business channel (Internet site, calling the business or going to the business).
2. Registration channel submits the relevant information to the Anywhere server via the web service interface. Alternatively, Contact Centre staff can enter customer details directly into the Anywhere administration console.
3. System creates customer profile and an activation code for that profile.
4. A unique download URL is created for this customer and it is included in an SMS message that is delivered to the supplied mobile number.

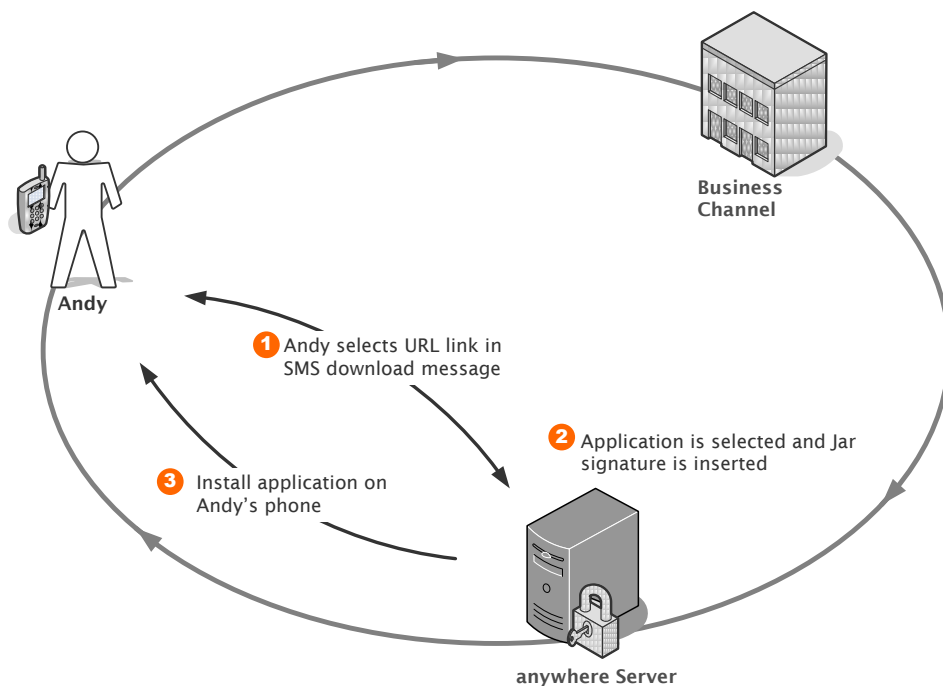
5. System sends the activation code to the bank channel.
6. Channel displays or reads out the activation code to the customer. Customer is asked to record this code to be used when activating the application. The bank can optionally configure the application to activate automatically, without customer intervention, thus saving the customer from having to remember this code.

Stage 2: Download application

After registration, the application must be downloaded and installed on the customer's mobile phone.



Downloading Java Application



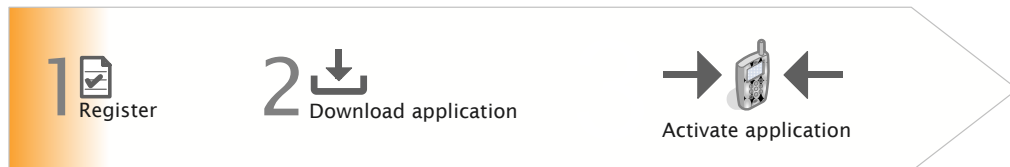
1. The customer opens the SMS message and clicks on the URL. The phone initiates a connection with the server. The customer is presented with a download page which may contain any instructions of terms and conditions. The user selects the download link.
2. The appropriate application is selected and the customer's unique signature is inserted in to the application. The application is sent to the phone.



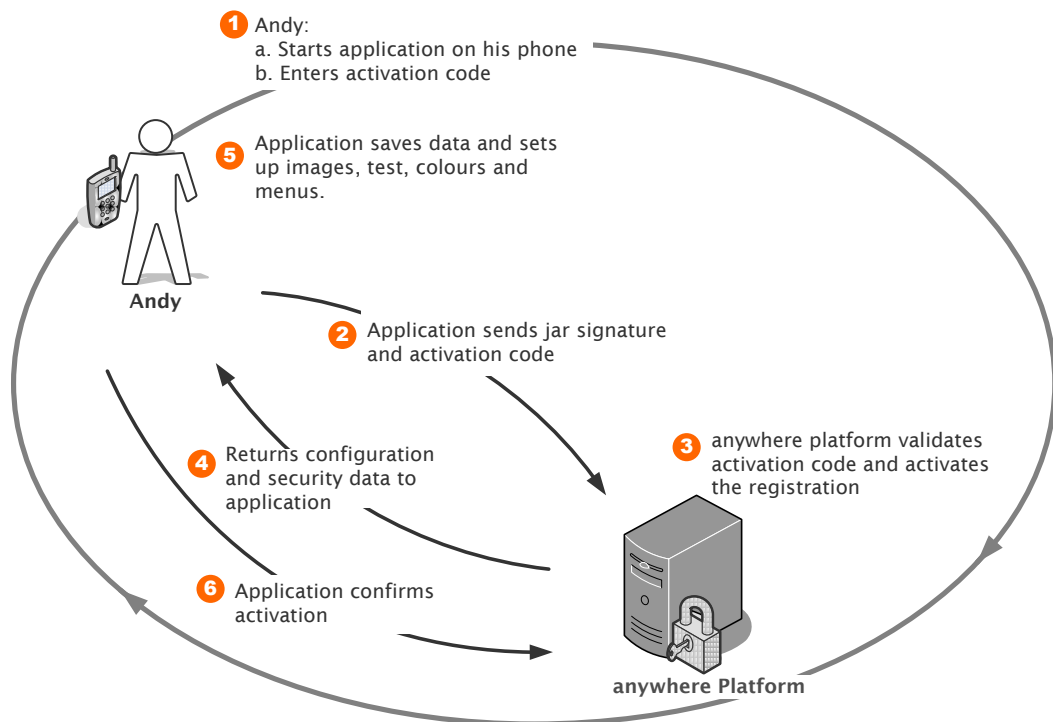
3. The phone downloads and installs the application.

Stage 3: Activation

Once installed, the application must be activated, thus associating the application instance with the customer's profile. The process verifies that the application on the phone is being used by the customer that registered via the business channel.



Activating the Java Application



1. The customer starts the application and is prompted for their activation code (if the application contains the activation code the user is not prompted).
2. The application transmits the jar signature and activation code to the Anywhere platform.
3. The Anywhere platform validates the activation code against this signature and pre-activates the registration.
4. The platform returns configuration and security data to the application.
5. The application saves the data and uses the configuration data to set up the colours, text, images and menus. The application is now activated and ready to use.



6. Application confirms the activation with the server at which point their registration profile is set to active. This ensures that nobody else can attempt to download an application or activate this registration.

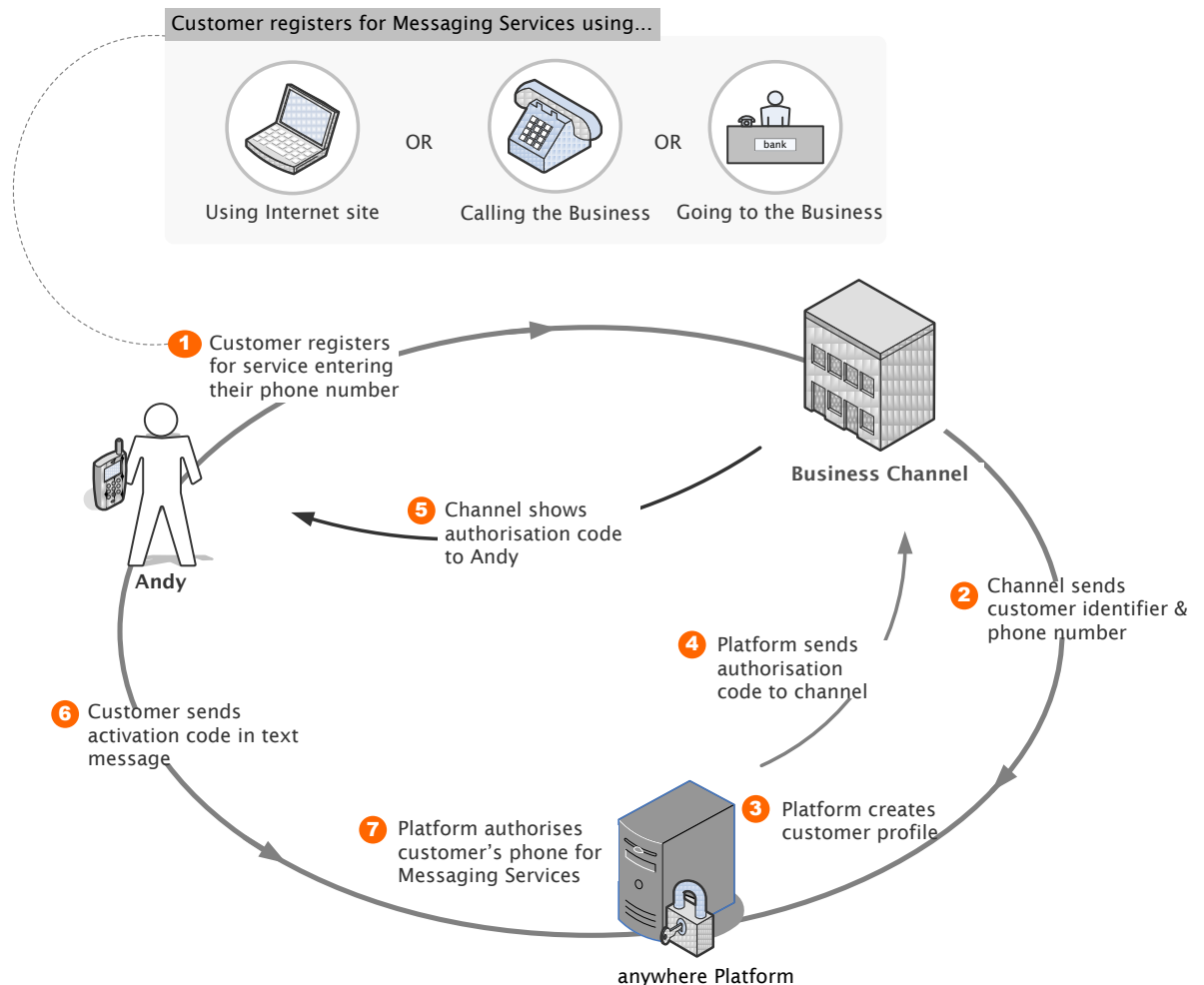
Registration for Messaging Services

As with other services offered by the Anywhere platform, the customer must first register for the service before being able to use it.

Because Messaging Services links the customer's business identifier with their mobile phone number, it is important that the customer verifies that they own the phone number being registered.

During registration, the customer is provided with an authorisation code which they must send to the platform via SMS. Upon receiving this code, the Anywhere platform authorises this phone for all messaging services.

Registering for Messaging Services



This flow describes the registration process:

1. Customer registers via existing business channel (Internet site, calling the business or going to the business).



2. The bank authenticates the customer and sends their business identifier and mobile phone number to the Anywhere platform using web services. Alternatively, Contact Centre staff can enter customer details directly into the Anywhere administration interface.
3. The Anywhere platform creates a customer profile (if required – the profile may already exist if a customer is registered for another service) and a registration record to the messaging service.
4. If the phone number is not authorised, the platform generates an authorisation code which is returned to the calling channel.
5. Channel displays or reads out the authorisation code to the customer. Customer is asked to send this code in a text message to a phone number or short code.
6. The customer sends the authorisation code as a text message.
7. Anywhere platform validates the code and authorises this phone number for all messaging services.

Registration for Alerting Services

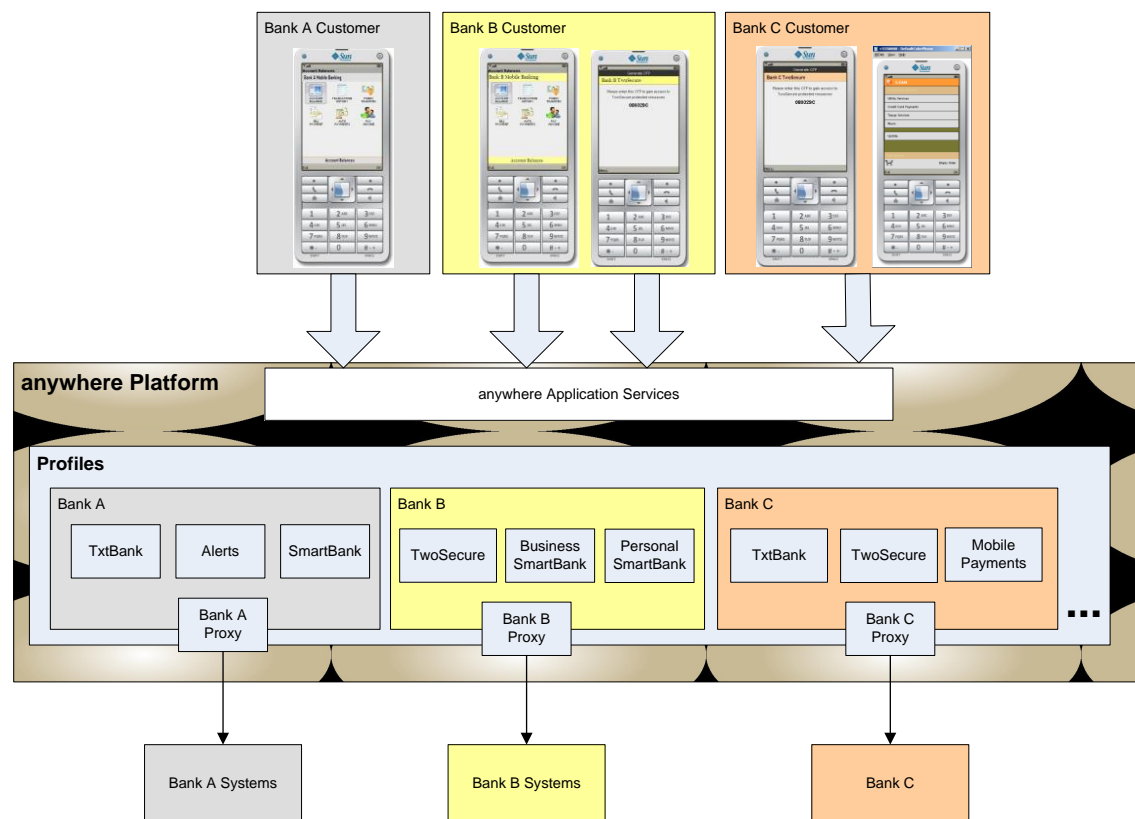
Initial registration for Alerting Services follows the same process as for Messaging Services. Once a customer is registered they can set up subscriptions for the various alerting services that are available. For time based alerts these subscriptions can be stored within the Anywhere platform; however event based subscriptions must be stored within the businesses core systems such that they can be triggered.

Software as a Service (SAAS) Platform

A single Anywhere platform can support many businesses, with any number of mobile applications and services.

This may be of particular relevance for a banking group consisting of a number of banks and/or brands; or for Software/Mobile Service providers that offer IT services to enterprise customers.

The following diagram shows a single platform hosting the entire Anywhere suite of products. Using banks as an example, each bank defines the set of services that they wish to offer. Each offering is branded for that bank and uses language appropriate to their service.



Segmentation of Data

The Anywhere platform was designed from the beginning to support this hosted service concept. This means that all business data is segmented into a provider service model. Each business customer is set up as a provider with a set of configured services. Their customers register for that provider and can then subscribe to any of the services being offered.

Because each business defines their own services they can use the extensive flexibility offered by the platform to customise their offering to their brand and market.

Administration



The Anywhere platform provides comprehensive, segmented permissions and views. The service provider may opt to provide a completely managed service, or each business may be given the ability to configure their own set of mobile offerings via the administration console. Each business will only be able to view and manage its own data.

Glossary

Term	Description of term
Web Services	Standard based on XML or more precisely SOAP for inter application communication. Has become the standard for exposing services within a Service Oriented Architecture.
HTTPS	Encrypted protocol for secure transfer of data across the Internet.
XHTML	XML compliant HTML standard used by web browsers to render web content.
URL	Uniform Resource Locator. Standard for defining the location of resources on the Internet.
JME	Java Mobile Edition. Java environment for mobile devices.
JEE	Java Enterprise Edition.
Midlet	J2ME application written for mobile devices.
Customer Token	Unique customer token stored on the phone used during login to provide a second factor of authentication.
Jar Signature	Unique signature stored within the application. Provides additional security by linking a single instance of the SmartBank™ application with a customer profile.
Download Identifier	Unique identifier that is inserted into the URL used to download the application. The server uses this to look up the customer's registration.
Activation Code	Numeric code used to activate the application once downloaded. This code can be entered by the customer or an application can be automatically activated with out customer intervention.