Glossary

Overview

This glossary provides terms and definitions for IBM MobileFirst Foundation software and products.

The following cross-references are used in this glossary:

- **See** refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- **See also** refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (http://www.ibm.com/software/globalization/terminology/).

A

acquisition policy

A policy that controls how data is collected from a sensor of a mobile device. The policy is defined by application code.

adapter

The server-side code of a MobileFirst application. Adapters connect to enterprise applications, deliver data to and from mobile applications, and perform any necessary server-side logic on sent data.

administration database

The database of the MobileFirst Operations Console and of the Administration Services. The database tables define elements such as applications, adapters, projects with their descriptions and orders of magnitude.

Administration Services

An application that hosts the REST services and administration tasks. The Administration Services application is packaged in its own WAR file.

alias

An assumed or actual association between two data entities, or between a data entity and a pointer.

Android

A mobile operating system created by Google, most of which is released under the Apache 2.0 and GPLv2 open source licenses. See also mobile device.

API / Application Programming Interface (API)

An interface that allows an application program that is written in a high-level language to use specific data or functions of the operating system or another program.

app

A web or mobile device application. See also web application.

Application Center

A MobileFirst component that can be used to share applications and facilitate collaboration between team members in a single repository of mobile applications.

Application Center installer

An application that lists the catalog of available applications in the Application Center. The Application Center Installer must be present on a device so that one can install applications from your private application repository.

application descriptor file

A metadata file that defines various aspects of an application.

authentication

A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures.

B

Base64

A plain-text format that is used to encode binary data. Base64 encoding is commonly used in User Certificate Authentication to encode X.509 certificates, X.509 CSRs, and X.509 CRLs. See also DER encoded, PEM encoded.

binary

Pertaining to something that is compiled, or is executable.

block

A collection of several properties (such as adapter, procedure, or parameter).

broadcast notification

A notification that is targeted to all of the users of a specific MobileFirst application. See also tag-based notification.

build definition

An object that defines a build, such as a weekly project-wide integration build.

C

CA / Certificate Authority (CA)

A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate.

callback function

Executable code that allows a lower-level software layer to call a function defined in a higher-level layer.

catalog

A collection of apps.

certificate

In computer security, a digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority enterprise application

A company application that provides certificates and private keys for its client applications.

CRL / Certificate Revocation List (CRL)

A list of certificates that have been revoked before their scheduled expiration date. Certificate revocation lists are maintained by the certificate authority and used, during a Secure Sockets Layer (SSL) handshake to ensure that the certificates involved have not been revoked.

challenge

A request for certain information to a system. The information, which is sent back to the server in response to this request, is necessary for client authentication.

challenge handler

A client-side component that issues a sequence of challenges on the server side and responds on the client side.

client

A software program or computer that requests services from a server.

client-side authentication component

A component that collects client information, then uses login modules to verify this information.

clone

An identical copy of the latest approved version of a component, with a new unique component ID.

cluster

A collection of complete systems that work together to provide a single, unified computing capability.

company application

An application that is designed for internal use inside a company.

Company Hub

An application that can distribute other specified applications to be installed on a mobile device. For example, Application Center is a Company Hub. See also Application Center.

component

A reusable object or program that performs a specific function and works with other components and applications.

credential

A set of information that grants a user or process certain access rights.

D

data source

The means by which an application accesses data from a database.

deployment

The process of installing and configuring a software application and all its components.

DER encoded

Pertaining to a binary form of an ASCII PEM formatted certificate. See also Base64, PEM encoded.

device

See mobile device

device context

Data that is used to identify the location of a device. This data can include geographical coordinates, WiFi access points, and timestamp details. See also trigger.

device enrollment

The process of a device owner registering their device as trusted.

documentify

A JSONStore command used to create a document.

E

emulator

An application that can be used to run an application meant for a platform other than the current platform.

encryption

In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

enterprise application

See company application.

entity

A user, group, or resource that is defined to a security service.

environment

A specific instance of a configuration of hardware and software.

event

An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event source

An object that supports an asynchronous notification server within a single Java™ virtual machine. Using an event source, the event listener object can be registered and used to implement any interface.

F

facet

An XML entity that restricts XML data types.

farm node

A networked server that is housed in a server farm.

fire

In object-oriented programming, to cause a state transition.

G

gateway

A device or program used to connect networks or systems with different network architectures.

geocoding

The process of identifying geocodes from more traditional geographic markers (addresses, postal codes, and so on). For example, a landmark can be located at the intersection of two streets, but the geocode of that landmark consists of a number sequence.

geolocation

The process of pinpointing a location based on the assessment of various types of signals. In mobile computing, often WLAN access points and cell towers are used to approximate a location. See also geocoding, location services.

H

homogeneous server farm

A server farm in which all application servers are of the same type, level, and version.

hybrid application

An application that is primarily written in web-oriented languages (HTML5, CSS, and JS), but is wrapped in a native shell so that the app behaves like, and provides the user with all the capabilities of, a native app.

I

in-house application

See company application.

J

JMX / Java Management Extensions (JMX)

A means of doing management of and through Java technology. JMX is a universal, open extension of the Java programming language for management that can be deployed across all industries, wherever management is needed.

K

key

A cryptographic mathematical value that is used to digitally sign, verify, encrypt, or decrypt a message. See also private key, public key. One or more characters within an item of data that are used to uniquely identify a record and establish its order with respect to other records.

keychain

A password management system for Apple software. A keychain acts as a secure storage container for passwords that are used by multiple applications and services.

key pair

In computer security, a public key and a private key. When the key pair is used for encryption, the sender uses the receiver's public key to encrypt the message, and the recipient uses their private key to decrypt the message. When the key pair is used for signing, the signer uses their private key to encrypt a representation of the message, and the recipient uses the sender's public key to decrypt the representation of the message for signature verification.

L

library

A system object that serves as a directory to other objects. A library groups related objects, and allows users to find objects by name. A collection of model elements, including business items, processes, tasks, resources, and organizations.

load balancing

A computer networking method for distributing workloads across multiple computers or a computer cluster, network links, central processing units, disk drives, or other resources. Successful load balancing optimizes resource use, maximizes throughput, minimizes response time, and avoids overload.

local store

An area on a device where applications can locally store and retrieve data without the need for a network connection.

M

MBean / Managed Bean (MBean)

In the Java Management Extensions (JMX) specification, the Java objects that implement resources and their instrumentation.

mobile

See mobile device.

mobile client

See Application Center installer.

mobile device

A telephone, tablet, or personal digital assistant that operates on a radio network. See also Android.

MobileFirst adapter

See adapter

MobileFirst Data Proxy

A server-side component to the IMFData SDK that can be used to secure mobile application calls to Cloudant® by using MobileFirst Platform OAuth security capabilities. The MobileFirst Data Proxy requires an authentication through the trust association interceptor.

MobileFirst Operations Console

A web-based interface that is used to control and manage MobileFirst runtime environments that are deployed in MobileFirst Server, and to collect and analyze user statistics.

MobileFirst runtime environment

A mobile-optimized server-side component that runs the server side of your mobile applications (back-end integration, version management, security, unified push notification). Each runtime environment is packaged as a web application (WAR file).

MobileFirst Server

A MobileFirst component that handles security, back-end connections, push notifications, mobile application management, and analytics. The MobileFirst Server is a collection of apps that run on an application server and acts as a runtime container for MobileFirst runtime environments.

N

native app

An app that is compiled into binary code for use on the mobile operating system on the device.

node

A logical group of managed servers.

notification

An occurrence within a process that can trigger an action. Notifications can be used to model conditions of interest to be transmitted from a sender to a (typically unknown) set of interested parties (the receivers).

O

OAuth

An HTTP-based authorization protocol that gives applications scoped access to a protected resource on behalf of the resource owner, by creating an approval interaction between the resource owner, client, and resource server.

P

page navigation

A browser feature that enables users to navigate backwards and forwards in a browser.

PEM encoded

Pertaining to a Base64 encoded certificate. See also Base64, DER encoded.

PKI / Public Key Infrastructure (PKI)

A system of digital certificates, certification authorities, and other registration authorities that verify and authenticate the validity of each party involved in a network transaction.

PKI bridge

A MobileFirst Server concept that enables the User Certificate Authentication framework to communicate with a PKI.

poll

To repeatedly request data from a server.

private key

In secure communication, an algorithmic pattern used to encrypt messages that only the corresponding public key can decrypt. The private key is also used to decrypt messages that were encrypted by the corresponding public key. The private key is kept on the user system and is protected by a password. See also key, public key.

project

The development environment for various components, such as applications, adapters, configuration files, custom Java code, and libraries.

project WAR file

A web archive (WAR) file that contains the configurations for the MobileFirst runtime environment and is deployed on an application server.

provision

To provide, deploy, and track a service, component, application, or resource.

proxy

An application gateway from one network to another for a specific network application such as Telnet or FTP, for example, where a firewall proxy Telnet server performs authentication of the user and then lets the traffic flow through the proxy as if it were not there. Function is performed in the firewall and not in the client workstation, causing more load in the firewall.

public key

In secure communication, an algorithmic pattern used to decrypt messages that were encrypted by the corresponding private key. A public key is also used to encrypt messages that can be decrypted only by the corresponding private key. Users broadcast their public keys to everyone with whom they must exchange encrypted messages. See also key, private key.

push

To send information from a server to a client. When a server pushes content, it is the server that initiates the transaction, not a request from the client.

push notification

An alert indicating a change or update that appears on a mobile app icon.

R

reverse proxy

An IP-forwarding topology where the proxy is on behalf of the back-end HTTP server. It is an application proxy for servers using HTTP.

root

The directory that contains all other directories in a system.

S

salt

Randomly generated data that is inserted into a password or passphrase hash, making those passwords uncommon (and more difficult to hack).

SDK / Software Development Kit (SDK)

A set of tools, APIs, and documentation to assist with the development of software in a specific computer language or for a particular operating environment.

security test

An ordered set of authentication realms that is used to protect a resource such as an adapter procedure, an application, or a static URL.

server farm

A group of networked servers.

service

A program that performs a primary function within a server or related software.

session

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data for the duration of the session.

sign

To attach a unique electronic signature, derived from the sender's user ID, to a document or field when a document is mailed. Signing mail ensures that if an unauthorized user creates a new copy of a user's ID,

the unauthorized user cannot forge signatures with it. In addition, the signature verifies that no one has tampered with the data while the message was in transit.

simulator

An environment for staging code that is written for a different platform. Simulators are used to develop and test code in the same IDE, but then deploy that code to its specific platform. For example, one can develop code for an Android device on a computer, then test it using a simulator on that computer.

skin

An element of a graphical user interface that can be changed to alter the appearance of the interface without affecting its functionality.

slide

To move a slider interface item horizontally on a touchscreen. Typically, apps use slide gestures to lock and unlock phones, or toggle options.

subelement

In UN/EDIFACT EDI standards, an EDI data element that is part of an EDI composite data element. For example, an EDI data element and its qualifier are subelements of an EDI composite data element.

subscription

A record that contains the information that a subscriber passes to a local broker or server to describe the publications that it wants to receive.

syntax

The rules for the construction of a command or statement.

system message

An automated message on a mobile device that provides operational status or alerts, for example if connections are successful or not.

T

tag-based notification

A notification that is targeted to devices that are subscribed for a specific tag. Tags are used to represent topics that are of interest to a user. See also broadcast notification.

TAI / Trust Association Interceptor (TAI)

The mechanism by which trust is validated in the product environment for every request received by the proxy server. The method of validation is agreed upon by the proxy server and the interceptor.

tap

To briefly touch a touchscreen. Typically, apps use tap gestures to select items (similar to a left mouse button click).

template

A group of elements that share common properties. These properties can be defined only once, at the template level, and are inherited by all elements that use the template.

trigger

A mechanism that detects an occurrence, and can cause additional processing in response. Triggers can be activated when changes occur in the device context. See also device context.

U

V

view

A pane that is outside of the editor area that can be used to look at or work with the resources in the workbench.

W

web app / application

An application that is accessible by a web browser and that provides some function beyond static display of information, for instance by allowing the user to query a database. Common components of a web application include HTML pages, JSP pages, and servlets. See also app.

web application server

The runtime environment for dynamic web applications. A Java EE web application server implements the services of the Java EE standard.

web resource

Any one of the resources that are created during the development of a web application for example web projects, HTML pages, JavaServer Pages (JSP) files, servlets, custom tag libraries, and archive files.

widget

A portable, reusable application or piece of dynamic content that can be placed into a web page, receive input, and communicate with an application or with another widget.

wrapper

A section of code that contains code that could otherwise not be interpreted by the compiler. The wrapper acts as an interface between the compiler and the wrapped code.

X

X.509 certificate

A certificate that contains information that is defined by the X.509 standard.