Ant Technology

Overview

User Guide

Document Version: 20230209

蚂蚁集团
ANT GROUP

Legal disclaimer

Ant Group all rights reserved©2022.

No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Ant Group.

Trademark statement

蚂蚁集团 ANT GROUP and other trademarks related to Ant Group are owned by Ant Group. The third-party registered trademarks involved in this document are owned by the right holder according to law.

Disclaimer

The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Ant Group reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through channels authorized by Ant Group. You must pay attention to the version changes of this document as they occur and download and obtain the latest version of this document from Ant Group's authorized channels. Ant Group does not assume any responsibility for direct or indirect losses caused by improper use of documents.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is mPaaS ---------- 05

2.Basic concepts ---------- 08

1.What is mPaaS

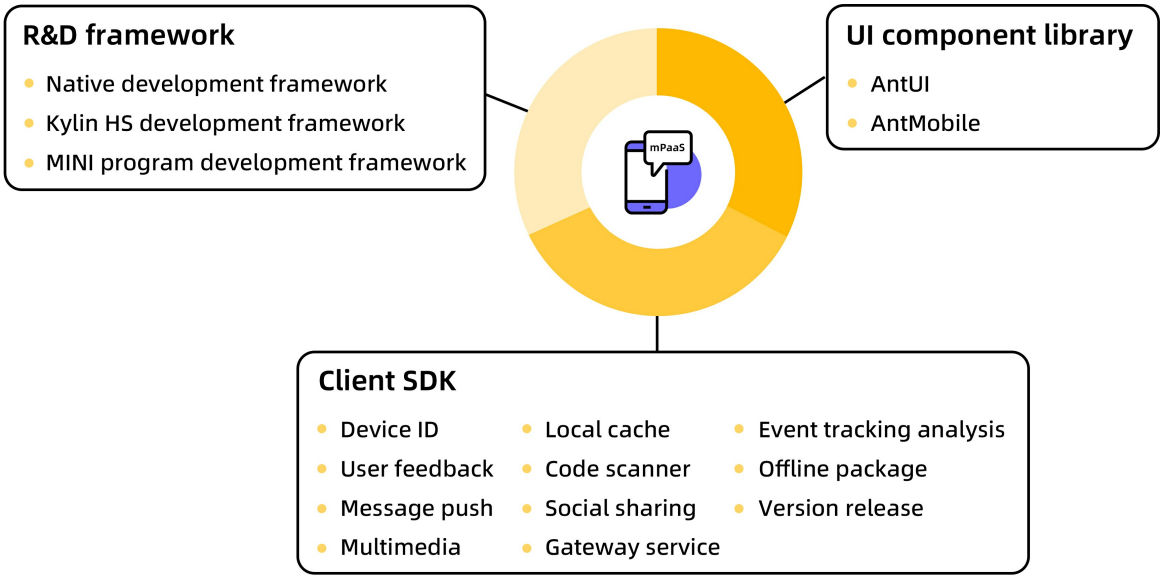
mPaaS (Mobile PaaS) is a mobile development platform originated from AliPay App, providing cloud-to-end one-stop solution for mobile development, testing, maintenance, and operation. mPaaS can effectively lower technological barrier, reduce R&D cost, improve development efficiency and facilitate the enterprise to build a stable high-quality mobile App rapidly.

Advantages

Dynamic and flexible client capabilities

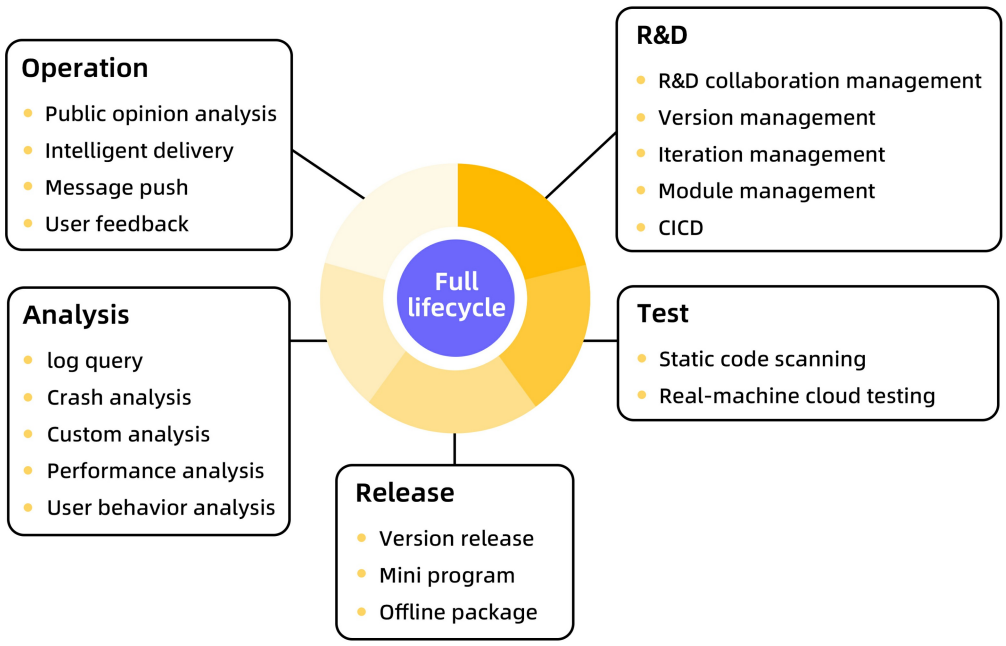
As a developer, you can effectively improve development efficiency and create an ultimate App experience with the help of the following dynamic and flexible client capabilities:

- 3 development frameworks: Native development framework, Kylin HTML5 development framework, and Mini development framework.
- 20+ functional components, such as gateway service, event tracking analysis, user feedback, message push, offline package.
- 100+ UI controls, including AntUI and AntMobile.



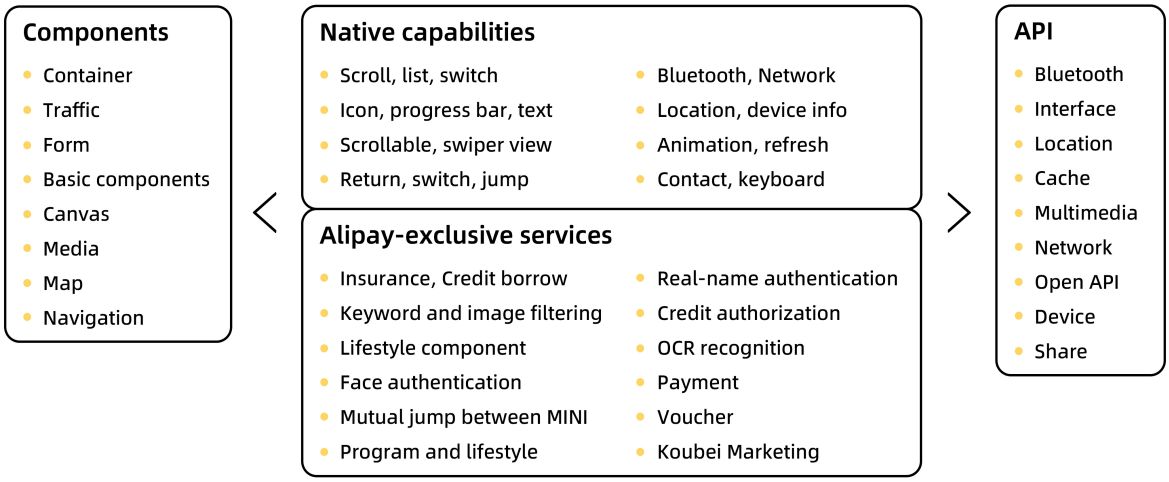
Solid mobile middle office capability

This capability covers the entire lifecycle of the App, provides strong support to ensure a stable and efficient operation of the client, and to perform rapid change and innovation.



Future-oriented research and development: Mini program

Achieves one-development-and-multi-delivery and a smoother user experience. At the same time, Alipay capabilities are fully opened for quickly building new businesses and new ecosystems.

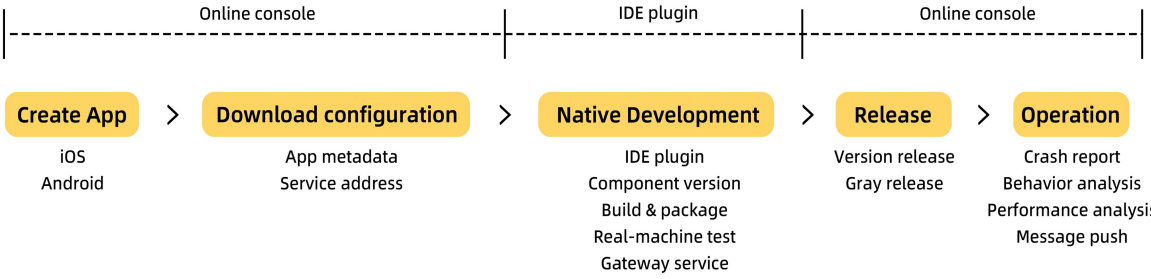


Component functions

To make the development more convenient, mPaaS encapsulates many high-performance components which cover every stage of mobile development. The components can either be used together with the framework to fast develop new Apps or be independently integrated into an existing App.

Operation flow

As a developer, you can use the functions of mPaaS through mPaaS console and mPaaS plugin. A complete process includes the following steps:



Related links

- Access method introduction - Android
- Access method introduction - iOS

2.Basic concepts

This term list is presented in lexicographical order.

#|A|B|C|D|E|F|H|I|J|L|M|N|O|P|R|S|T|U|V|W|

#

95th percentile

The percentile is a measure in which all values are sorted in ascending order and the first N% value is the N% percentile. The 95th percentile represents the first 95 data among 100 data which is sorted in ascending order.

A

Active promotion activity

It refers to a direct promotion event for the targeted population, such as pushing a message notifying a daily login reward event to users who had not logged in for the last 15 days.

Advertisement space

It refers to a position in a booth where advertisement materials are displayed. An advertisement space can display an advertisement. A booth can contain multiple advertisement spaces.

Advertisement space frames

It refers to the number of advertisement spaces in a booth, that is, the number of advertisements displayed in the booth when the booth is occupied for event purposes.

Ad-token

It refers to the unique identifier of an Android device and is frequently used in client-side SDKs.

Application Not Responding (ANR)

Application Not Responding (ANR) is a dialogue box displayed on an Android device when the App is unresponsive.

Anti-debugging

It refers to a method of examining the current runtime environment based on the knowledge of the debugger features to hamper the execution of JavaScript code in the debugging mode.

Anti-formatting

It forces the code to be displayed in a single line. This code will fail to be executed if it is formatted or renamed.

Apache Dubbo (Dubbo)

Dubbo is an open-source and distributed service framework that provides capabilities targeted at interface proxies such as high-performance RPC call and microservice governance.

API group

A group of APIs with a common attribute. The API group name can be a specific system name, a component name, or an abstract identifier.

APK/ABB package reinforcement

It enhances the security of APK/ABB packages by providing the following capabilities: anti-decompilation for APK/ABB packages, encapsulation for DEX files, anti-tamper for DEX files, anti-white-box attacks, secure shell encryption algorithms, anti-debugging, anti-tamper of memory, anti-hook, anti-emulator, anti-repackaging for APK/ABB packages, and anti-dumping of memory.

appId

The appId is an identifier generated when a mPaaS app is created. You can view the appId in the download configuration file page on the console.

AppId

It identifies a unique app and is generated when the app is created.

Attribute

An event contains information such as the ID of a user who triggered an event, the app version, and the device model. The abovementioned are collectively referred to as attributes. The mobile analysis platform provides some built-in attributes that are frequently used, and you can custom your own attributes as needed.

Attribute ID

It is a unique identifier of an attribute that is a global concept in an app. Therefore, the attribute ID must be unique in the same mPaaS app.

B

Background

It refers to a state when the App is running in the background, that is, when the phone is on the home screen or black screen, or the user is operating another App.

Binding relationship

It refers to the mapping relationship between a device and a user identifier. It corresponds to the operations of binding and unbinding.

BizType

It indicates the business type and is the unique identifier of a business scenario. After data is pushed, the client-side data synchronization SDK uses Biztype to distribute data to corresponding service components.

Booth

It refers to the area on an app page that is used to display an advertisement.

Branch forgery

The branch forgery is a method used for control flow obfuscation based on opaque predicates, and its component is built in the safe compiler. It can reorganize the control flow at relatively low costs (with performance scarcely affected and file size slightly increased).

Broadcast push

It refers to a method of pushing the same message to all devices connected to the network. The message content is obtained by replacing the parameter values in a message template.

Build

Website building is a process of assembling components into a web page, involving operations such as adding, duplicating, deleting, and reordering components on the page as well as configuring data.

Business dimension

The business dimension of the synchronization service falls into the user dimension and the device dimension. For the user dimension, data is pushed according to userId. For the device dimension, data is pushed according to utdId.

C

Call graph obfuscation

A call graph indicates the calling relationships among functions, which is an important indicator used to describe the macrostructure of a program. Compared with the technique of confusing control flow graphs, the call graph obfuscation is a component-based obfuscation technique that confuses the reference relationships among functions. The call graph conversion component can compromise the macrostructure of the source code by conversing all calling commands of the source program, so that the design features of components of the source program can be removed.

Class reinforcement

It refers to a method that disarranges Java code to hide its execution flow so that the reinforced code is incomprehensible enough to counter the decompiling by using tools such as Jadx-Gui and Jeb.

Client-side message identifier

It is automatically generated by the system or customized by the user. It is used to identify a unique message in a client-side system.

Code condensation

It refers to a method of condensing the code into several lines to reduce its readability. This method is implemented by deleting unnecessary content such as spaces and line breaks or processing the part of code that is likely to be reused.

Command replacement

The command replacement component is used to transform or unfold the simple binary operations of the source code such as arithmetic operations and boolean operations. The processed operations are incomprehensible enough to counter the cracking by developers. The command replacement component has dozens of built-in replacement rules which are randomly selected for the replacement process, thus diversifying the generated commands.

Component

It refers to the minimal unit of materials used to build a page.

Confidence interval

The confidence interval is a range of estimates for the population parameter based on the observed sample parameter. A confidence interval displays the probability that a parameter will fall between a pair of values around the mean. It shows the credibility of the measured value of the observed parameter, that is, the abovementioned "certain degree of confidence".

Confidence level

It describes the credibility of the measured value of the observed parameters, that is, the "certain degree of confidence" required by the confidence interval.

Constant encryption

It supports compile-time encryption of array constants of various types. It aims to hide explicit strings such as log information to reduce the risk of information leakage and to hide static constant arrays such as AES-Sbox to complicate the recognition of static features of general algorithms.

Control flow obfuscation

It refers to a method of disarranging the execution flow of the source code and the calling relationships of functions to make the logic of the code incomprehensible.

Critical event occurrence

It refers to the occurrence of a mobile analysis event associated with an event after the user taps the event advertisement within a period of time.

Critical event occurred devices

It refers to the deduplicated devices where a mobile analysis event associated with an event occurs after the users tap the event advertisement.

Custom event

In a MAS event, it refers to a recorded action a user performs within an app. You can set a custom event for any triggered action such as tapping a button. The custom event is created by customizing conditions.

D

Debug

It refers to the debugging performed before a created test is officially implemented. It aims to check whether the test can be implemented properly.

Device Token

It refers to the unique identifier of an Apple device, which is provided by Apple.

Deduplicated share devices

It refers to the deduplicated devices that have tapped the share button on the landing page within a period of time. The implementation result depends on the accuracy of the customer-side tracking.

Display position

It refers to the position of the booth on the page, such as the top and the bottom.

Display style

It refers to the display style of the booth on the page, such as displaying it as a banner or as a bulletin.

Distributed Resource Management (DRM)

Distributed Resource Management (DRM) is a dynamic real-time configuration management framework in a distributed environment. It enables dynamic upgrades of configurations without restarting the App. It is universally applied in scenarios such as business parameter configuration and emergency switch enabling/disabling.

Dynamic booth

It refers to a booth that is integrated through dynamic configuration. The display process for such a booth must be controlled through the information issued by the server (console).

E

Event

It refers to a recorded action a user performs within an app. You can set a custom event for any triggered action such as tapping a button.

Event analysis

The event and its attribute information are stored in a local client as logs and then reported to mobile analysis servers. After completing the configuration in the console, you can view the event analysis report.

Event conversion rate

It refers to the proportion of the number of devices that triggered the mobile analysis event associated with a campaign to the number of responding devices.

Event ID

It is a unique identifier of an event which is a global concept in an app. Therefore, an event ID must be unique in the same mPaaS app.

Event unit

It refers to a set of marketing events created for a common marketing purpose. An event unit contains multiple events with the same topic.

F

Fatigue

It refers to the upper limit of reaches to a user or device during a unit time period.

Front end

It refers to a state when an app is currently open.

H

Hadoop Distributed File System (HDFS)

Hadoop Distributed File System (HDFS) provides standard HDFS access protocols. It allows users to use the distributed file system featuring unlimited storage, extended performance, unique space name, high reliability, and high availability without making any modifications to the existing big data analysis application.

HRPC

HRPC is an HTTP-based RPC scheme.

I

Idempotence

Anyone among the combination of bizType, linkToken, thirdMsgId in SyncOrder is executed multiple times while only one successful implementation is allowed to be achieved. In this process, the newly generated data will be deprecated, and the result code is DUPLICATED_BIZ_ID.

Interactive marketing event

It refers to a targeted marketing event triggered by one or more user behaviors. For instance, an active user has viewed financial products for consecutive days during a promotion period, and then an ad of financial products will be displayed on the homepage of the user's app accordingly.

J

JavaScript domain name binding

It refers to a method where the JavaScript code can only be executed under a specified domain name.

Junk code and bad code insertion

The junk code refers to the code that can be executed while interfering with analysis. The bad code refers to the illegal code that cannot be executed. The junk code and bad code insertion component is used to counter the analysis capability provided by decompilers which is capable of analyzing static instruction flow.

L

Laboratory

You can manage a group of tests in a laboratory. The laboratories fall into two types: server-side laboratories and client-side laboratories.

Location Based Services (LBS)

Location Based Services (LBS) refers to an online service that provides information resources and services to a device based on the device location obtained by using multiple positioning technologies.

M

Message template

It is a framework used to generate a message. It contains the attributes and configuration of a message, the fixed message content, and placeholder parameters.

Metric

The metric is used to determine the test result. The default system metrics are Page View (PV), Unique Visitor (UV), and the 7-day retention rate. You can also create a MAS metric or compound metric by using the custom event feature of Mobile Analysis Service (MAS).

Mobile Gateway Service

Mobile Gateway Service (MGS) is the name of the component that provides an API gateway service.

Message Identifier (MSGID)

It is used in MPS to identify a unique message and is automatically generated by the system.

MSS data

It refers to data to be pushed by data synchronization servers.

MSS push

It refers to a method of actively pushing a piece of data from servers to clients. The data will be instantly pushed when the clients that call the services are online. Otherwise, the push will not be triggered until the clients are online.

Multiple device synchronization

It means that data synchronization among multiple devices of a user is supported. Specifically, when a user logs on to another device, the data received on the previously-used device will still be sent to the currently used device. When the app is reinstalled and started on the device, the data will still be pushed.

Multiple frame booth

It refers to a booth with an advertisement displayed for more than 1 frame.

Multiple pushes

It refers to a method of pushing personalized messages to multiple target IDs. The message content is obtained by replacing parameter values in the same template according to different target IDs.

N

Network jitter

It refers to the variation in latency between packet flow from one client to another, which is a commonly used concept in Quality of Service (QoS). The jitter is the difference between the max and the min latency and describes the stability of a network. For example, if the max latency is 20 milliseconds and the min latency is 5 milliseconds, then the network jitter is 15 milliseconds.

Network latency

It refers to the time delay between when a message is sent and when it is received over a network connection. It usually consists of transmission latency and processing latency.

O

Object key replacement

It refers to a method of replacing the names of object keys to hide the calling relationships among functions.

Online

It means that there is a network available for the app on the client and a stable long-lived TCP connection can be maintained. On most Android phones, apps can keep running in the background. For an iPhone, because of the limit of the iOS system, an app can run in the background for 3 minutes.

OperationType

OperationType is the required field for creating an API. It is a unique identifier for API services.

OSS

Object Storage Service (OSS) is a cloud storage service featuring unlimited space, security, low costs, and high reliability, providing up to 99.9999999999% of data persistence and 99.995% of data availability. Multiple storage types are available.

P

Page

A page is a result generated by using Mobile Pages Building Service (MBS). One page corresponds to a URL. After the page is published, users can visit it on their phones. A page is a visible interface of an app, that is, the interface shown to general users when they use the app.

Page load time

It refers to the time it takes for a page to load on your device.

Persistence

Persistence refers to a mechanism where program data can be transformed into persistent or non-persistent data. In data synchronization services, this mechanism generates 2 types of data: persistent data and non-persistent data.

- Persistent data: when the user or device is offline, the data will be persisted and stored in the database. When the user or the device is online, the data synchronization SDK will trigger synchronization.
- Non-persistent data: when the user or device is online, data will be instantly pushed. Otherwise, the data will be deprecated. Even when the user is online later, the data will not be pushed.

Pointer encryption

The pointer encryption component is used to remove the explicit reference relationships between functions and data.

Preset booth

It refers to the booths integrated through client configuration. The display positions of such booths must be fixed by codes on the client.

Program popularization

After a test is done, you can choose a program based on the test result to apply it to the general traffic. This process is referred to as program popularization.

Push certificate

It is used to connect with the Apple Push Notification service (APNs) servers.

Push target ID

It refers to the target that receives the push. The target ID can be the Ad-token of an Android device, the device token of an iOS device, or a userId. Its meaning depends on the context.

Push to a single device

It means that a message will be pushed only once to the single device that the user log on to most recently. When the app is reinstalled and then started on the device or the user logs on to other devices, the message will not be pushed again.

Push type

It refers to the two types of push: targeted push and global push.

- Targeted push: pushes a piece of data to a user or device that corresponds to a userId or utdId respectively.
- Global push: pushes data to all online users or devices. The pushed data is synchronized among multiple devices.

R

Reach

It refers to the sum of exposures and pushes of campaign advertisements within a certain period of time.

Reached devices

It refers to the sum of deduplicated devices as carriers of any advertisement materials as well as devices that received pushes within a promotion period.

Reinforcement

It refers to the method of achieving enhanced anti-cracking capability by recompiling and packing the app as well as modifying the executing order of commands.

Request response time

It refers to the period from when the request is sent by the client to when the response is received.

Responding devices

It refers to the sum of the deduplicated devices where an advertisement and the push are tapped over a period of time.

Response rate

It refers to the proportion of the responding devices to all reached devices.

Responses

It refers to the sum of the taps of an advertisement and the push over a period of time.

Retention rate

The retention rate is an indicator that reflects the operation of a website, app, or online game. Specifically, it refers to the average ratio of the number of daily active users to users who still start the app on the next N day within a period of statistics (week/month). Wherein, the value of N is usually set to 2, 3, 7, 14, 30, respectively corresponding to next-day retention rate, three-day retention rate, weekly retention rate, half-month retention rate, and monthly retention rate.

Remote Procedure Call (RPC)

Remote Procedure Call (RPC) is used to upgrade the OCR model online. The upgrade will take effect after the system backend is configured accordingly.

S

Security reinforcement package

It refers to the reinforced APK/AAB package. The security reinforcement package in a certain task refers to the APK/AAB package reinforced during the task.

Share rate

It refers to the ratio of the devices that have shared the push to the total devices that have received the push.

Shares

It refers to the number of shares of an event on the landing page within a period of time. The implementation result depends on the accuracy of client tracking.

Simple Push

It refers to a method of pushing one message to one target ID.

Single-frame booth

It refers to a booth with an advertisement displayed for 1 frame.

Symbol encryption

It refers to a method of encrypting the names of specified functions and variables.

SYNC

It refers to the data synchronization service, which enables data synchronization between servers and clients.

T

TaobaoRemoting (TR)

The TR framework refers to the underlying communications framework used for PRC. TR is provided by the Ant Group.

Task name

A message-pushing request is identified as a task.

Template parameter

It refers to a part in a message template that can be dynamically replaced. It can be also referred to as a template placeholder.

Template parameter value

It refers to the specific content corresponding to a template placeholder.

Template push

It refers to a method of pushing a message to one pushing target ID. The message content is obtained by replacing the template parameter.

Threshold

It refers to the upper limit of data backlog on servers. If a user or device is offline for a long time and new data is constantly generated by the MSS servers, there may be a backlog of data on the servers. In this case, only the latest data within the threshold will be retained, and the rest of the data will be deprecated.

Tracking point

The tracking point refers to a technique and its implementation process that are used to capture, process, and report specified user behaviors or events. Information of an app is collected to track the condition of the app being used so that the product and operation can be optimized based on data including visits, visitors, taps, and visit duration.

U

User identifier

It identifies a unique user and corresponds to a specified device. It is generally used in binding relationships.

UserId

Advertisements are pushed to targeted users according to their userIds. When the targeted userIds are online, the advertisements will be pushed to the corresponding users. When a user logs in on multiple devices, the advertisements will be pushed to all the devices.

UTDID

Advertisements are pushed for targeted UTDIDs. Regardless of whether the user ID is online, when the app is opened on the targeted devices, the advertisements will be displayed.

V

Variable

When a test is performed on the client side, variables are required to be pushed to the app through Mobile Delivery Service (MDS) dynamic configurations. When a test is performed on the server-side and gateway, variables should be configured.

W

workspaceId

It is an identifier of a workspace on the mobile platform. It is used to isolate different environments. You can view it on the download configuration file page on the console.