



数据加密实施指南

淘子王

2017/04/17



• 目录

一、接入介绍

二、接入演示

三、常见问题

四、支持资源

1

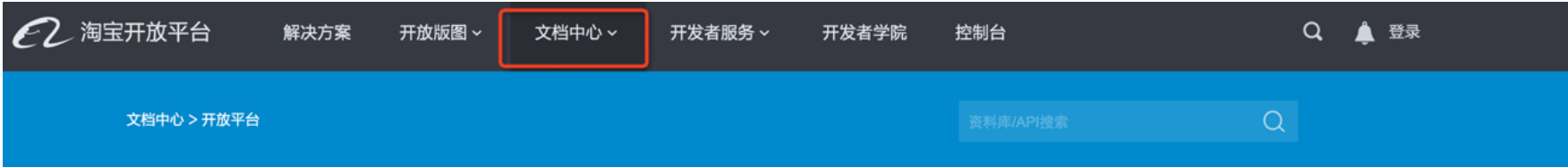
接入介绍



• 接入介绍

数据存储加密的整改范围 是包括所有涉及获取消费者隐私数据的服务商应用。

可在开放平台查看数据加密相关文档获得帮助。



文档内容：

- 1、数据加密产品简介：产品介绍；
- 2、实施指南：流程操作详解；
- 3、典型方案：加密开发过程各种方案详解；
- 4、常见问题：日常问题解答；
- 5、加密培训视频：产品操作及开发讲解视频；



数据加密简介

更新时间：2017/01/11 访问次数：277

一. 产品背景

- 1、安全事件频发：消费者订单泄漏、数据价值被盗等
- 2、业务核心资产：数据、数据、还是数据…
- 3、现有管控局限：生态链路中不可控的系统或应用，管控成本越来越高
- 4、安全技术瓶颈：已有加密技术场景简单且无法满足三方应用场景、去中心化的新兴加密技术还无法商业化应用

二. 产品用途

本产品提供针对消费者敏感数据存储的加密能力，用于防止因外部或内部安全威胁所导致的数据泄露问题，从而提高数据安全的防护水平。

三. 产品架构

解决数据安全的一个重要的手段，就是敏感数据的加密。为了让保护范围覆盖到流通和存储等各个环节，本产品设计的方案将加密范围从源头、一直涵盖到ISV的持久化存储。

使用本产品的加密服务后，从开放平台输出的数据从流出源头开始就是加密的。这包括含敏感

- 一. 产品背景
- 二. 产品用途
- 三. 产品架构
- 四. 产品功能
- 五. 产品特点

【流程概述】

第1阶段：“接入须知”阶段需该应用的开发者，了解本次安全整改的背景、要求明确安全整改的内容和方法，以便于开发者做好安全整改的准备。

第2阶段：“方案确认”阶段需该应用的开发者，指定本项目相关的接口人联系方式，并明确本应用的技术架构、应用部署以及存储的数据规模等相关信息，以便与开放平台做好后续的协同与沟通。并且针对该应用的加解密处理需求，开发者应进行相关详细的技术方案设计与问卷报备。

第3阶段：“店铺加密”阶段需该应用的开发者，依据本产品的 [接入方案](#) 和 [开发文档](#)（如涉及数据的模糊查询时，请参考 [密文检索](#)），对其应用的数据加解密实现逻辑进行代码的开发、测试和上线，以便满足本次安全整改的应用功能要求。
并且通过用户（卖家）的白名单或黑名单的功能，逐步将用户（卖家）的数据接入到已开发好的加解密应用功能中，最终保障该应用所需获取的所有用户（卖家）数据能进行正常的加解密。

第4阶段：“数据迁移”阶段需该应用的开发者，依据本产品的 [数据迁移文档](#)，将其存储的历史明文数据迁移加密为密文，以避免敏感的明文存储风险。

第5阶段：“验收上线”阶段需该应用的开发者，确认方案信息的完善性和有效性，全店铺的隐私数据已加密和历史数据加密迁移的完成情况，对其应用的系统处理逻辑和数据处理过程进行安全自评估与平台小二确认本次安全整改的所有任务是否满足要求。

「2」

接入演示

└──────────┘

√

• 接入演示-入口

【入口】

登陆开放平台控制台—应用管理—安全中心—数据存储加密，点击进入产品页面如下图：

The screenshot shows the Alibaba Open Platform console interface. The top navigation bar includes the '应用管理' (Application Management) tab, which is highlighted with a red box. The left sidebar contains a '安全中心' (Security Center) section, also highlighted with a red box, with a red arrow pointing to the '数据存储加密' (Data Storage Encryption) option. The main content area displays the 'APP证书' (APP Certificate) section, which includes fields for App Key, Random Number, App Secret, and Application Security Level. A '提示' (Notice) box on the right states that the application is not online and provides instructions for API usage and user limits. Below this, the '功能场景' (Function Scenarios) table lists various scenarios and their status.

公共场景			
基础	已获得	查看详情	
	已获得	查看详情	了解更多
	已获得	查看详情	了解更多

接入演示-入口

淘宝 · 开放平台 / 控制台

资料库/API搜索

🔍

🔔

👤

▼

changchun_test

应用管理

服务管理

资源管理

开发运维

监控中心

+ 创建应用

概览

SDK下载

应用设置

安全中心

应用安全指数

IP白名单设置

操作日志

缺陷列表

违规问题列表

数据存储加密

沙箱数据存储加密

报表中心

消息服务

插件管理

应用管理_new

数据流转

淘宝小程序

1 接入须知

2 方案确认

3 店铺加密

4 数据迁移

5 验证上线

🔔 您的数据加密整改工作正处于安全验收阶段，进度延迟 [点击进入安全整改](#)

您在安全验收阶段的数据加密整改任务，需在2017.01.17前完成，目前还剩余0天
您所有阶段的数据加密整改任务，需在2017.01.25前完成，目前还剩余0天

本次加密整改工作的实施排期表

排期	接入须知	方案确认	店铺加密	数据迁移	验证上线
计划排期	2017.01.10	2017.01.10	2017.01.10	2017.01.14	2017.01.25
完成进度	2017.04.14	2017.04.14	未完成	未完成	未完成

上次（已完成）加密整改工作的实施进度表

排期	接入须知	方案确认	店铺加密	数据迁移	验证上线
已完成进度	2017.04.14	2017.04.14	2017.04.14	2017.04.14	2017.04.14

如图所示：

- ① 是您当前的整改进度在什么阶段，还有多少未完成，进度是否有延迟。
- ② 是平台要求的整改时间与当前应用的改造进度，完成情况。
- ③ 如果上期已经参加过整改，会出现上期整改的进度表。

• 接入演示-接入须知

• 【第1阶段】 ‘接入须知’ 第一步 如下图所示：

该步骤主要介绍了应用本次的整改范围，整改的隐私API，处罚规则和支持资源，如下图所示：

淘宝 · 开放平台 / 控制台

应用管理 服务管理 资源管理 开发运维 监控中心

chanq

创建应用

概览
SDK下载
应用设置
安全中心
应用安全指数
IP白名单设置
操作日志
缺陷列表
违规问题列表
数据存储加密
沙箱数据存储加密
报表中心
消息服务
插件管理
应用管理_new
数据流转
淘宝小程序

1 接入须知 2 方案确认 3 店铺加密 4 数据迁移 5 验证上线

帮助文档 最佳实践

一、整改须知

1. 整改范围

当您的应用获取平台中涉及消费者的隐私数据（包括但不限于：消费者的昵称、姓名、电话、Email、身份证号、车牌号、支付宝账号、用户id 以及收货地址等）时，您的应用就应对这些敏感的消费者的隐私数据进行存储加密，具体可参考平台定义的敏感 [API列表](#)。

2. 整改要求

平台已明确要求对涉及存储消费者隐私数据获取的应用进行存储加密，否则将依据其平台相关规则对违规者进行处罚，具体请参加《[服务市场安全违规行为及处罚规范](#)》和《[开放平台安全违规行为及处罚规范](#)》中相关内容。

1) 处罚依据：该应用系统通过appkey或相关权限获取并存储淘宝平台用户的隐私数据时，未按照官方认可的安全方案对其存储的用户隐私数据进行安全加密。

2) 处罚措施：对该应用的安全分进行3分的扣除，并在服务市场上对该应用进行服务冻结；同时，由开放平台发出其警告通知，并罚款1万元和对其API调用进行模糊化处理，若限期已到未完成整改，则延长处罚至整改完成。

3) 处罚周期：10个工作日，如仍未按期完成整改，再根据实际情况升级平台的处罚力度。

3. 该应用在本次安全整改中需涉及的敏感API列表(15天调用记录，仅供参考)

taobao.cainiao.station.order.sendmail.query、taobao.logistics.order.query、taobao.logistics.orders.detail.get、taobao.vmarket.taoma.merchant.consume、cainiao.logistics.station.order.cp.create、cainiao.logistics.station.order.query、taobao.cainiao.station.order.locker.ext.mailno.query、taobao.cainiao.station.order.locker.mailno.query、taobao.cainiao.station.order.locker.package.put、taobao.cainiao.station.order.sendmail.reccode.query、cainiao.endpoint.locker.spi.order.query、cainiao.endpoint.locker.spi.order.state.sync、cainiao.endpoint.locker.spi.order.subscribe、

① 本期数据加密需要整改的范围（需要整改的API，API隐私字段）。

② 本期整改的平台规则和未按规定完成整改的处罚内容。

③ 本应用本期涉及到的需要整改的API列表（供参考）。

请详细确认以上要求与平台规则，确认无误请点击 ‘进入下一步’ ，该步骤可返回查看。

• 接入演示-接入须知

•【第1阶段】 ‘接入须知’ 第二步 如下图所示：

确认了整改范围和平台要求后，进入到在线培训界面，可以在这里学习存储加密的产品，实施方案，与支持的资源。

注意：开始改造前请先加入旺旺群[1640022702]，并且详细阅读项目的技术资料。

您也可以参考一下 <[典型的服务商案例](#)>，同时培训视频还会更新到单独的文档中方便查看<[培训视频](#)>。

The screenshot displays the Alibaba Open Platform (淘宝·开放平台) console. The top navigation bar includes the logo, '控制台中' (Control Center), a search bar for '资料库/API搜索' (Documentation/API Search), and user profile icons. The main navigation menu on the left lists various management options, with '数据存储服务加密' (Data Storage Encryption) highlighted. The central area shows a progress bar with five steps: 1. 接入须知 (Access Notice), 2. 方案确认 (Solution Confirmation), 3. 店铺加密 (Store Encryption), 4. 数据迁移 (Data Migration), and 5. 验证上线 (Verification and Go Live). The '接入须知' step is currently active. Below the progress bar, the content is organized into sections: '二、项目实施的技术资料' (Technical Materials for Project Implementation) with links to '1. 产品简介' (Product Introduction), '2. 实施指南' (Implementation Guide), '3. 典型方案' (Typical Solutions), and '4. 常见问题' (Common Questions); '三、整改必经之路-培训学习' (Mandatory Path for Rectification - Training and Learning) featuring three video thumbnails for '课程1.存储加密的产品介绍' (Course 1: Product Introduction), '课程2.存储加密的实施介绍' (Course 2: Implementation Introduction), and '课程3.存储加密的方案介绍' (Course 3: Solution Introduction); and '四、帮助支持' (Help and Support) with contact information for小二 (Xiao Er) and two hotlines: 7*24 hours for regular questions and 400-806-9000 for regular consultation.

学习完毕，对整改流程，技术实现基本了解，可以点击 ‘下一步’，该步骤可返回查看

接入演示-方案确认

【第2阶段】‘方案确认’ 第一步 如下图所示：

char

应用管理

服务管理

资源管理

开发运维

监控中心

+ 创建应用

概览

SDK下载

应用设置

安全中心

应用安全指数

IP白名单设置

操作日志

缺陷列表

违规问题列表

数据存储加密

沙箱数据存储加密

报表中心

消息服务

插件管理

应用管理_new

数据流转

淘宝小程序

1 接入须知

2 方案确认

3 店铺加密

4 数据迁移

5 验证上线

帮助文档

最佳实践

* 技术接口人：?

yexue_dev

12312312312

wang1

123123123123@qq.com

* 业务接口人：?

yexue_biz

12312312312

wang2

123123123123@qq.com

* 系统部署架构：?

SAAS

独立部署

SAAS+独立

* 账号方案：?

淘系帐号

自有账号

(2)自有账号注册

(3)自有账号
粒度加密

(4)历史数据逐步加密

RDS
业务库

TOP SDK

展示、查
询、输入

(1-a)加密、解密

* 使用的数据库类型：

☒

RDS-SQL Server

☒

RDS-Mysql

☐

独立部署-SQL Server

☐

独立部署-Mysql

☐

Elastic Search

☐

ODPS

☐

其他

* 使用的数据库总个数：

1

* 存储的数据量总条数（预估）：

11

步骤 (1-a)：接入TOP SDK，在订单过滤及分发的地方，将订单信息用归属的店铺密进行开发；

步骤(3)：开发测试且上线后，应通过白名单测试其店铺的加密效果，然后再逐步扩大直至打开所有店铺的加密；

步骤(4)：所有店铺都加密后，再对其历史的数据进行加密迁移。

上一步

确认

Copyright ©2015 TAOBAO.COM 版权所有

• 接入演示-方案确认

• 【第2阶段】 ‘方案确认’ 第一步

注意每个步骤右上角的小问号，里面有该步骤特别需要注意的点

上图中：

① 录入技术接口人、业务接口人联系信息，方便后续沟通联系；

注：信息请确认无误后填写 并且 填写的联系人的联系方式 确保可以正常联系。

② 请选择本应用的部署是通过SAAS服务的方式，还是软件独立部署的方式或者两种部署结构都存在的方式，来给该应用的现有用户（卖家）提供服务。

③ 选择本应用在给其用户（买家）提供软件服务时，其账号体系是使用淘系的账号体系，还是使用本应用自建的账号体系。账号方案选择介绍请参看相关文档：[账号体系接入方案详解](#)

注：如果存在 自建和淘系的业务共存，请选择较大的账号体系。选择后不会影响后台实际实现（自建和淘系可以共存）。

④ 选择您所使用的数据库类型（可多选），数据库数量，当前数据量大小（单位：条，估算）

注：数据量指的是 数据库总量 包括业务库，当前数据量预估量。

以上信息填写完成点击 ‘确认’ 进入下一步，表单信息提交到后台供小二查看，该步骤可返回补充。

• 接入演示-方案确认

• 【第2阶段】 ‘方案确认’ 第二步 如下图所示：

针对该应用的加解密处理需求，应按照安全方案设计的规则《[安全方案设计](#)》进行相关的技术方案设计并确保完整性与真实性（需要提供相关附件）。

注意：平台小二需要了解你们的改造计划和具体的方案实现。一共8个问卷，有5个问卷必须提交附件。三个问卷按需提交附件。填写规范请按安全规范填写。否则审核时将给予驳回！

The screenshot displays the Alibaba Open Platform console interface. At the top, the navigation bar includes the '淘宝·开放平台 / 控制台' header, a search bar for '资料库/API搜索', and user profile icons. Below the navigation bar, a horizontal menu contains '应用管理', '服务管理', '资源管理', '开发运维', and '监控中心'. A '+ 创建应用' button is located on the right. The left sidebar lists various management options, with '数据储存加密' (Data Storage Encryption) highlighted. The main content area shows a progress bar with five steps: 1. 接入须知, 2. 方案确认 (active), 3. 店铺加密, 4. 数据迁移, and 5. 验证上线. Below the progress bar, a yellow box contains instructions for the '方案确认' step, including a warning icon and three numbered points. The first point asks for a questionnaire regarding data encryption and decryption. Below this, a text input field contains the placeholder 'TB1iC7XXXXXXXjXpXXXXXXXXXX'. An '上传附件' (Upload Attachment) button is present, with a note that attachments should be text files (doc, docx, xls,xlsx, pdf, ppt, pptx) not exceeding 5MB. At the bottom, another questionnaire point is visible, asking about custom key caching.

点击 ‘提交与报备’ 后设计方案将提交到后台，小二会进行审核，该步骤可返回补充。

• 接入演示-方案确认

• 【第2阶段】 ‘方案确认’ 第三步 如下图所示：

char 应用管理 服务管理 资源管理 开发运维 监控中心 + 创建应用

概览
SDK下载
> 应用设置
√ 安全中心
 应用安全指数
 IP白名单设置
 操作日志
 缺陷列表
 违规问题列表
 数据存储加密
 沙箱数据存储加密
> 报表中心
> 消息服务
 插件管理
> 应用管理_new
> 数据流转
> 淘宝小程序

1 接入须知 2 方案确认 3 店铺加密 4 数据迁移 5 验证上线

帮助文档 最佳实践

✓ 您已完成本次安全整改的方案报备，整改实施计划如下：

接入须知阶段的完成日期：	2017-01-10 00:00:00
方案确认阶段的完成日期：	2017-01-10 00:00:00
店铺加密阶段的完成日期：	2017-01-10 00:00:00
数据迁移阶段的完成日期：	2017-01-14 00:00:00
验证上线阶段的完成日期：	2017-01-17 00:00:00

上一步 无异议，进入下阶段工作

① 确认本期平台要求的整改时间，调整最佳的改造进度安排。

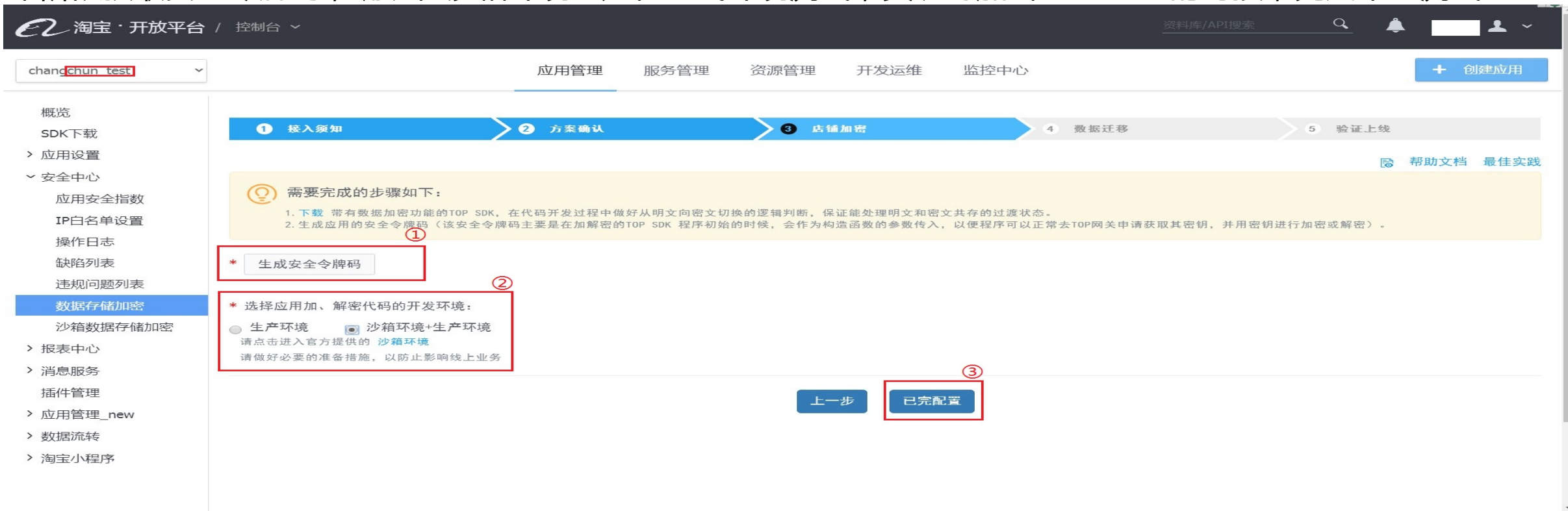
注意：改造进度如果延迟会有处罚，如果有问题请提早联系小二。

点击 ‘无异议，进入下阶段工作’ 进入测试，店铺加密阶段。确认对平台要求整改时间无异议，该步骤可返回查看。

● 接入演示-店铺加密

●【第3阶段】‘店铺加密’ 第一步 如下图所示：

本阶段获取安全令牌码，确认在沙箱环境还是在正式环境测试，实现与加密TOP SDK的对接，完成常量测试：



① 需要点击生成安全码（每个应用都有一个唯一的安全码，沙箱的和线上的都不同）

注：这里是正式环境的安全码。正式环境与沙箱环境的安全码不同，使用错误的话会报错，安全码无效。

② 选择这个应用需要代码开发的环境，建议优先进行沙箱环境测试。

注：沙箱环境与线上环境完全隔离，在沙箱环境中进行的相关操作不会影响到线上的正常的业务。

③ 生成下载带有加解密功能的SDK。

点击‘已完成配置’进入下一步，该步骤可返回修改。

● 接入演示-店铺加密

● 【第3阶段】 ‘店铺加密’ 第二步 如下图所示：

chan

应用管理 服务管理 资源管理 开发运维 监控中心

+ 创建应用

概览
SDK下载
应用设置
安全中心
应用安全指数
IP白名单设置
操作日志
缺陷列表
违规问题列表
数据存储加密
沙箱数据存储加密
报表中心
消息服务
插件管理
应用管理_new
数据流转
淘宝小程序

1 接入须知 2 方案确认 3 店铺加密 4 数据迁移 5 验证上线

帮助文档 最佳实践

需要完成的步骤如下：

1. 确定是否需要支持字段的密文检索功能。
2. 修改RDS推送库交易表、退款表buyer_nick字段长度，业务库涉及到的加密字段自行修改。

选择应用需要支持密文检索的数据库字段：?

☒ 买家nick ☐ 姓名 ☐ 联系人手机号码 ☐ 电子邮箱

请添加该应用所涉及RDS数据库的字段长度修改计划。如不修改，影响数据推送库的写入：?

☐ 批量设置计划

☐ asjd.mysql.com	1234-11-22	日期格式：yyyy-MM-dd
☐ asjd.mysql.com2	输入加密字段长度修改时间	日期格式：yyyy-MM-dd
☐ asjd.mysql.com2	2234-11-22	日期格式：yyyy-MM-dd

配置多个RDS实例名时，以“;”分隔

Copyright ©2015 TAOBAO.COM 版权所有

① 选择需要密文检索的字段，请根据实际的业务需求进行选择，如果本应用不需要支持密文检索的功能，可不选择；

注：如果需支持时，应谨慎选择且核实选择是否准确，因为选择后该字段在数据库的字段长度将发生变化且不可回退。不可修改。密文检索可以查看详细的文档：密文字段检索方案

② RDS数据库字段长度修改设定，当该计划设定后，将由平台根据您所设定日期进行自动的字段修改，执行时间将在凌晨2点-凌晨5点间完成。

注：如果推送库buyer_nick字段不是255长度的都需要添加修改与是否检索需求无关，平台会自动判断是否需要修改，如果不需要修改的RDS不会再进入修改流程，未修改字段长度的RDS可能导致数据无法正常写入数据库。

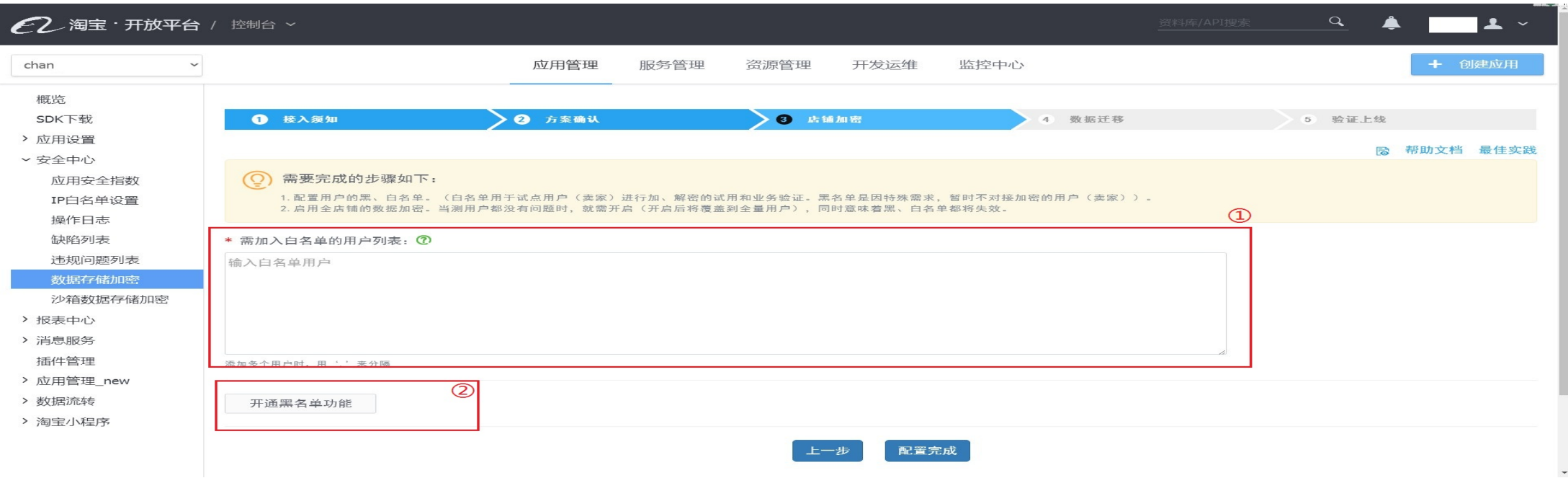
每个框中可同时填写多个RDS实例，建议一个框中填写的数量不要大于50个，每个实例id使用“;”分隔。

点击“已完成并提交”，生效密文检索字段和RDS改造计划，密文检索勾选后无法取消，并且RDS字段长度修改排期中，无法进行其他操作，需要等待字段长度修改完成。该步骤可返回，只能修改RDS实例，无法修改密文检索字段。

● 接入演示-店铺加密

●【第3阶段】 ‘店铺加密’ 第三步 如下图所示：

配置用户（卖家）的白、黑名单：在本应用的用户（卖家）加密切换过程中，可通过白名单的功能将其试点的用户（卖家）数据进行加解密的试用和业务验证；如果用户（卖家）数据在加密切换过程中有特殊需求时，也可以临时使用黑名单来保障个别用户（卖家）的数据不做加密。代码开发阶段，可以查看下面的代码开发方案（**注意：代码规范编码**）：



① 白名单：填写白名单就是配置测试店铺，点击确定后，会在五分钟内逐渐生效，所有隐私出参会为密文。测试店铺配置可以同时配置多个店铺，使用“,”分隔，注意配置的店铺不要超过 512个。

注：白名单用户列表是添加店铺的主账号。并且添加后无法取消（如果手动取消了将获取不到秘钥之前的密文数据将解密不了）

② 黑名单：黑名单中的店铺是不加密的，而且黑名单优先级大于白名单，如果同时配置会处于不加密的状态。

注：开启全店铺加密后黑白名单都会失效，本应用下的所有店铺隐私出参都会为密文。

点击 ‘配置完成’ ，生效白名单中的店铺隐私字段数据出参为密文，白名单建议只增加不删除，添加测试店铺可重复到当前步骤添加。

• 接入演示-店铺加密

• 【第3阶段】 ‘店铺加密’ 第四步 如下图所示：

注意：该阶段可以重复配置店铺，建议配置多个店铺充分测试，通过 ‘上一步’ 在白名单中增加新的店铺。
(只可添加店铺 不可删除店铺，如果删除了，删除的这个店铺之前的密文数据将无法解密)。



建议充分测试配置的测试店铺能达到50个以上，并且选择多种不同的用户来进行测试。

• 接入演示-店铺加密

• 【第3阶段】 ‘店铺加密’ 第五步 如下图所示：

开启全店加密配置，请在多个测试店铺充分的测试后，确保应用明密文兼容，数据流转没有问题在开启，开启后应用的全部授权店铺将隐私数据出参皆为密文。

全店铺加密开启后黑白名单将全部失效，并且无法退回到未开启全店状态，请谨慎操作！



[帮助文档](#) [最佳实践](#)

✓ 您已经完成部分店铺的数据加密

上一步

全部店铺加密

全店铺加密请充分配置测试店铺，充分测试后在点击开启全店铺。开启后应用的全部店铺隐私字段将全是密文。应用中也需要做好明密文兼容



[帮助文档](#) [最佳实践](#)

✓ 您已经完成全部店铺的数据加密

上一步

下一步

点击 ‘下一步’ 会进入数据迁移阶段，全店铺加密开启后无法回退到部分店铺加密阶段。

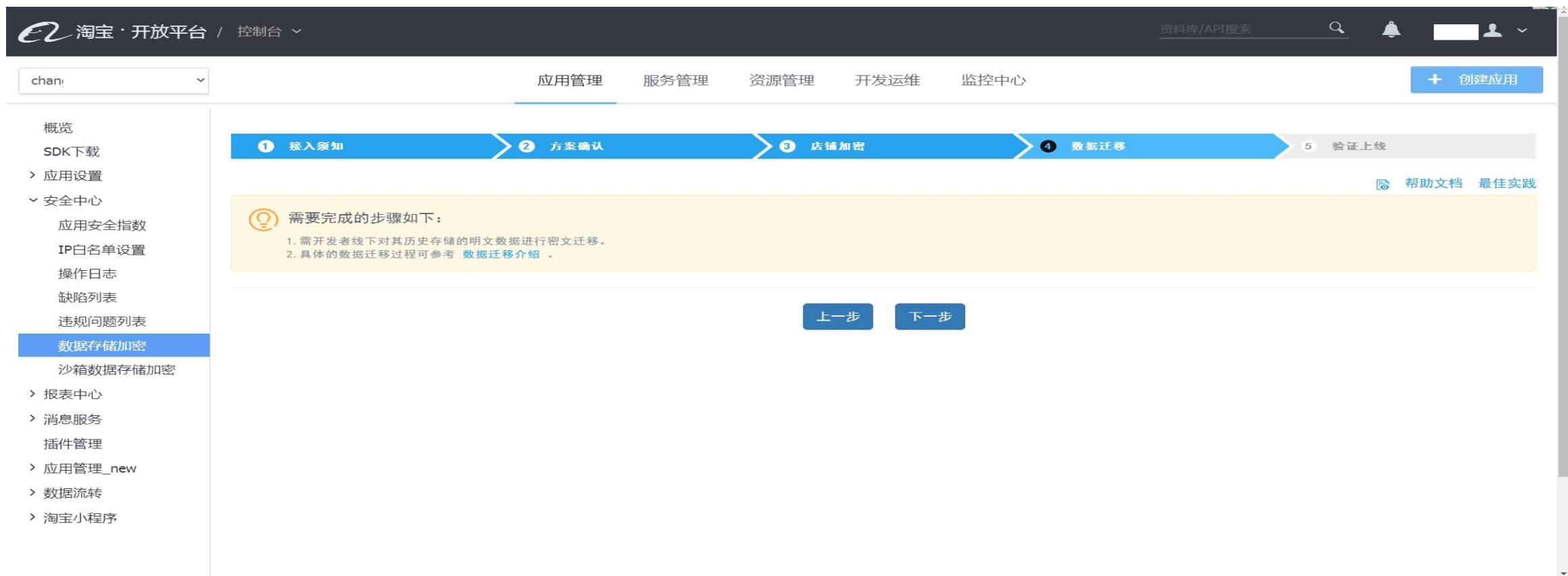
• 接入演示-数据迁移

• 【第4阶段】 ‘数据迁移’ 如下图所示：

1) 需开发者线下对其历史存储的明文数据进行密文迁移。

2) 具体的数据迁移过程可参考文档：[数据迁移方案](#)

注意：数据迁移需要加密所有涉及到用户隐私的数据，包括且不仅仅为RDS，所有的业务库也同步需要加密包括CS架构的客户端数据！



确认所有历史数据加密完成后点击 ‘完成迁移’ 进入下一步，该步骤可返回查看。

• 接入演示-验收上线

• 【第5阶段】 ‘验收上线’ 第一步 如下图所示：

- 1) 请确认该应用在各个阶段里的工作是否都已完成；
- 2) 提交验收申请，等待相关小二的审核和反馈；
- 3) 平台小二会进行审核和确认，包括所有ISV提交的所有材料和项目执行情况



若全部按照整改规范整改完毕点击 ‘提交安全整改的验证申请’ 后小二会进行审核，该步骤可返回查看。

• 接入演示-验收上线

- 【第5阶段】 ‘验收上线’ 第二步 如下图所示：
验收通过，完成了本次的整改要求。

淘宝 · 开放平台 / 控制台

资料库/API搜索

应用管理 服务管理 资源管理 开发运维 监控中心

+ 创建应用

chz

应用管理

服务管理

资源管理

开发运维

监控中心

+ 创建应用

概览

SDK下载

> 应用设置

> 安全中心

应用安全指数

IP白名单设置

操作日志

缺陷列表

违规问题列表

数据存储加密

沙箱数据存储加密

> 报表中心

> 消息服务

插件管理

> 应用管理_new

> 数据流转

> 淘宝小程序

1 接入须知

2 方案确认

3 店铺加密

4 数据迁移

5 验证上线

帮助文档 最佳实践

✓ 祝贺您，您所有的数据加密整改工作都已完成！

总共实施0天0小时55分钟，完成于2017.04.14

本次加密整改工作的实施排期表

排期	接入须知	方案确认	店铺加密	数据迁移	验证上线
计划排期	2017.01.10	2017.01.10	2017.01.10	2017.01.14	2017.01.25
完成进度	2017.04.14	2017.04.14	2017.04.14	2017.04.14	2017.04.14

上次（已完成）加密整改工作的实施进度表

排期	接入须知	方案确认	店铺加密	数据迁移	验证上线
已完成进度	2017.04.14	2017.04.14	2017.04.14	2017.04.14	2017.04.14

注：如审核未通过则需要重新提交，提交过程中遇到问题请在 [支持中心](#) 提问反馈。

3

常见问题



● 常见问题

1、加解密字段有哪些？

初期主要针对订单数据中买家的昵称、姓名、电话、邮箱、地址、身份证、车牌号、支付宝账号、用户id等进行加密

2、密钥如何获取，是否要定期升级

密钥是加、解密数据的关键，密钥不会定期升级，但是如果密钥存在泄漏风险，需要您配合升级密钥。密钥的获取可以通过SDK中获取密钥的API，传入session参数和app加密安全码来获取。

3、是不是只有RDS推送才加密，API调用会加密吗？

RDS推送和API调用都会加密。

4、RDS修改字段长度有什么影响？RDS版本升级会不会停服务？

mysql5.5版本会有锁表现现象，建议升级到5.6版本（可在控制台自助升级），版本升级对用户透明的。只是最后切换的时候会闪断下。

5、数据迁移是否要终止服务

数据迁移过程中，数据库中可能存在明文、密文，老密钥和新密钥的加密数据考虑到这些因素只要做好代码的兼容性，是不需要终止服务的

● 常见问题

6、目前加解密sdk支持哪些语言

目前有.net , java , php SDK 支持加密 / 解密 , 千牛插件不会加密

7、密钥升级后还需要做那些工作？

密钥升级意味着之前的加密数据已经不再安全，所以需要以前的加密数据进行迁移工作，用新的密钥重新加密

8、加解密对计算的影响

用户密钥命中缓存情况下：单台服务器加 / 解密单条数据耗时约0.03ms。

用户密钥未命中缓存情况下：据耗时约1.5ms。

9、数据加密后，有模糊搜索的需求怎么办？

我们提供了加密数据的模糊搜索功能，如果有此需求，需要您在sql查询语句中做适当的修改

4

支持资源



如有任何疑问您可通过以下方式获得帮助：

- 1、 【数据加密整改服务支持群】旺旺群：1640022702
- 2、 支持中心提交问题
- 3、 7*24小时电话支持：4008069000



成就你的技术梦想

Thank you