PostgresConf.CN 2022

中国PostgreSQL数据库生态大会

云原生数据库 PieCloudDB ：Unbreakable 安全特性剖析

王渼舟

PieCloudDB 资深技术专家

OpenPie | 拓数派

PCC POSTGRESCONF CN 2022 / 2023.2.17-19 /

OpenPie

CHINA POSTGRESQL ASSOCIATION

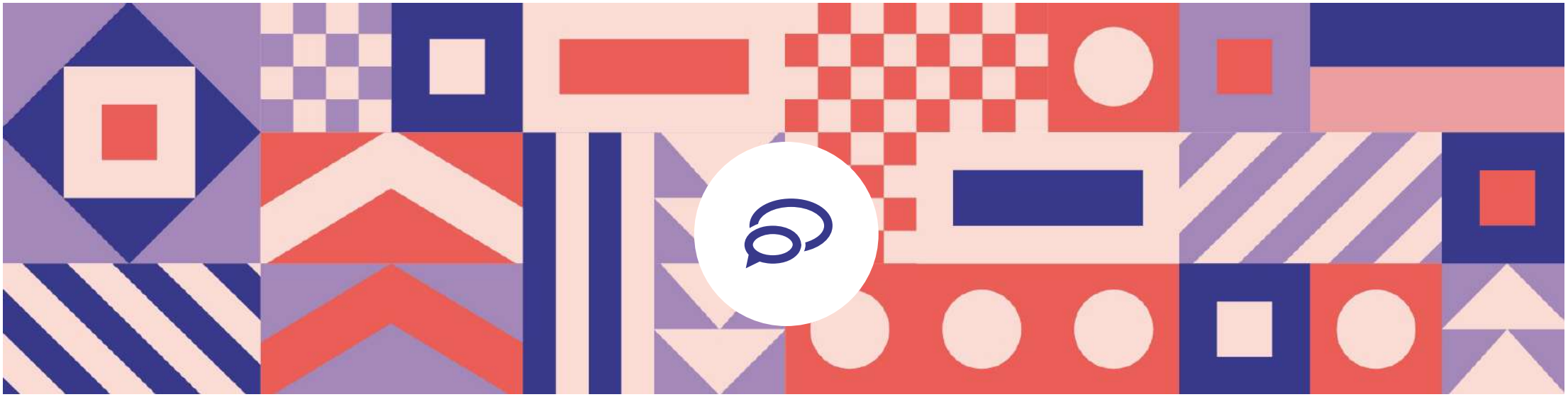
Data Computing for New Discoveries

数 据 计 算 ， 只 为 新 发 现

打造立足于国内 基础数据计算领域的世界级高科技创新驱动机构

杭州拓数派科技发展有限公司（又称“OpenPie”），以“Data Computing for New Discoveries”「数据计算，只为新发现」为使命，成立后的短短10个月时间内，完成了包括头部产业基金、东吴证券、元禾重元和政府科创平台在内的**连续三轮战略融资**。

旗下云原生分析型数据库 **PieCloudDB**，以云计算架构为设计基础，**首创全新 eMPP 分布式技术**，帮助企业建立竞争壁垒的同时，实现数据价值最大化，并在新基建中承担可靠和可控的世界级云数据库底座。



PART 01

元CloudDB的安全特性

三大区域

- 云原生安全
  - 传输层加密
  - 缓存数据加密
- 存储安全
  - 元数据持久化存储
  - 用户数据多副本加密储存
- 计算安全
  - 集群失效不影响用户数据
  - ACID保证

三大区域

- 云原生安全
  - 传输层加密
  - 缓存数据加密
- 存储安全
  - 元数据持久化存储
  - 用户数据多副本加密储存
- 计算安全
  - 集群失效不影响用户数据
  - ACID保证

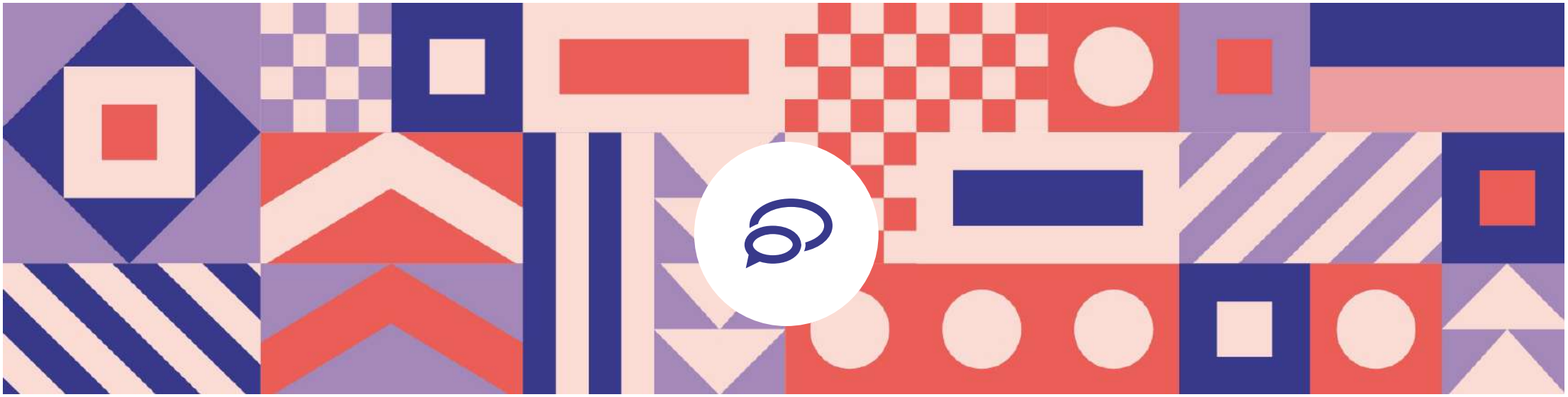
透明加密的定义

- 目标
  - 加密用户数据
- 使用高强度加密算法
  - AES-GCM 128 bit，AES-GCM 256 bit …
- 特点
  - 用户无感知
  - 数据写入自动加密，读取自动解密

透明加密的作用

- 将数据库数据从明文存储转为加密存储
  - 避免数据被系统运维人员直接读出
  - 不依赖公有云/私有云/系统加密

- 用户合规需求
  - 数据安全审计
  - 业务安全审计



PART 02

需求和挑战

来自用户的需求（1）

- 密钥自主可控
  - 主密钥存储于安全区域中
  - 密钥不出区
- 加密密钥支持轮换
  - 按时间/条件进行密钥轮换
  - 无需停机，不中断服务
- 对性能影响小
  - 避免额外造成查询延迟
  - 不影响批量读取，流式数据写入性能

来自用户的需求（2）

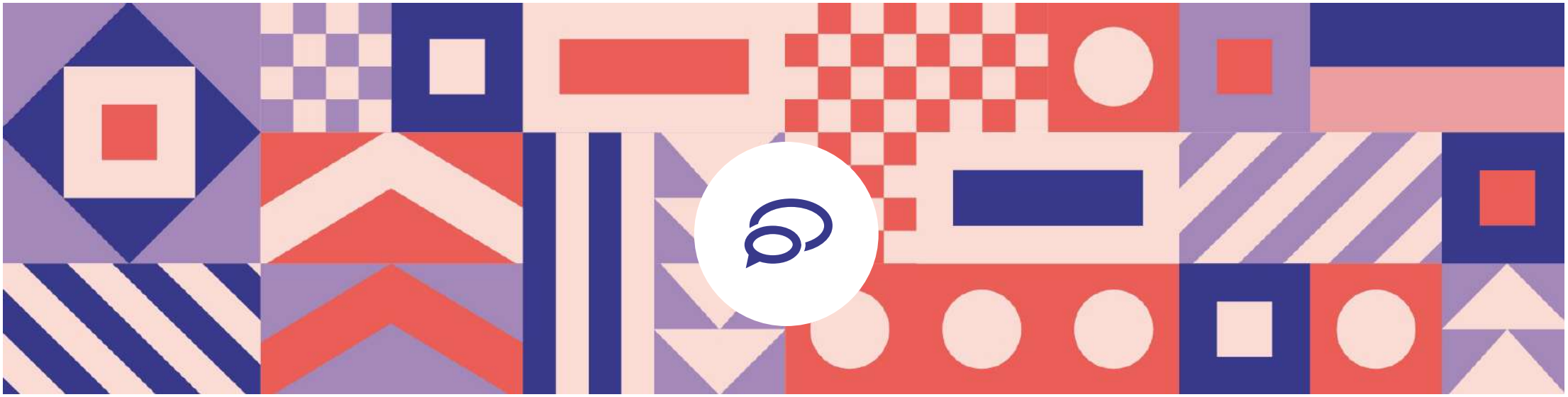
- 支持国密标准
  - 合规
  - 加密算法可选
- 免配置
  - 开箱即用

技术挑战（1）

- 不可避免的性能损失
  - 选用支持硬件加速的加密算法
  - SIMD 支持
- 减少因为密钥泄露而造成的损失
  - 多级密钥
  - 密钥加密密钥
- 用户无感知
  - 自动生成次级密钥
  - 密钥自管理
  - 分区加密

技术挑战（2）

- 和数据库存储结合
  - 不影响数据库内核（执行器，优化器）
  - 不修改/添加元数据表格式
- 业务拟合
  - 不影响原有用户的查询\业务
  - 不影响外围组件（ETL）



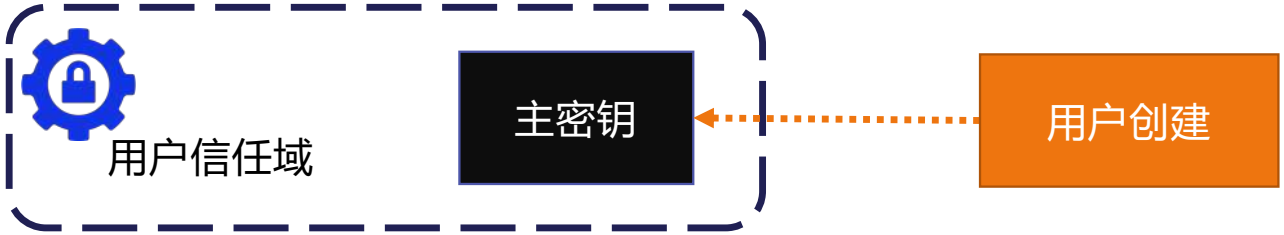
PART 03

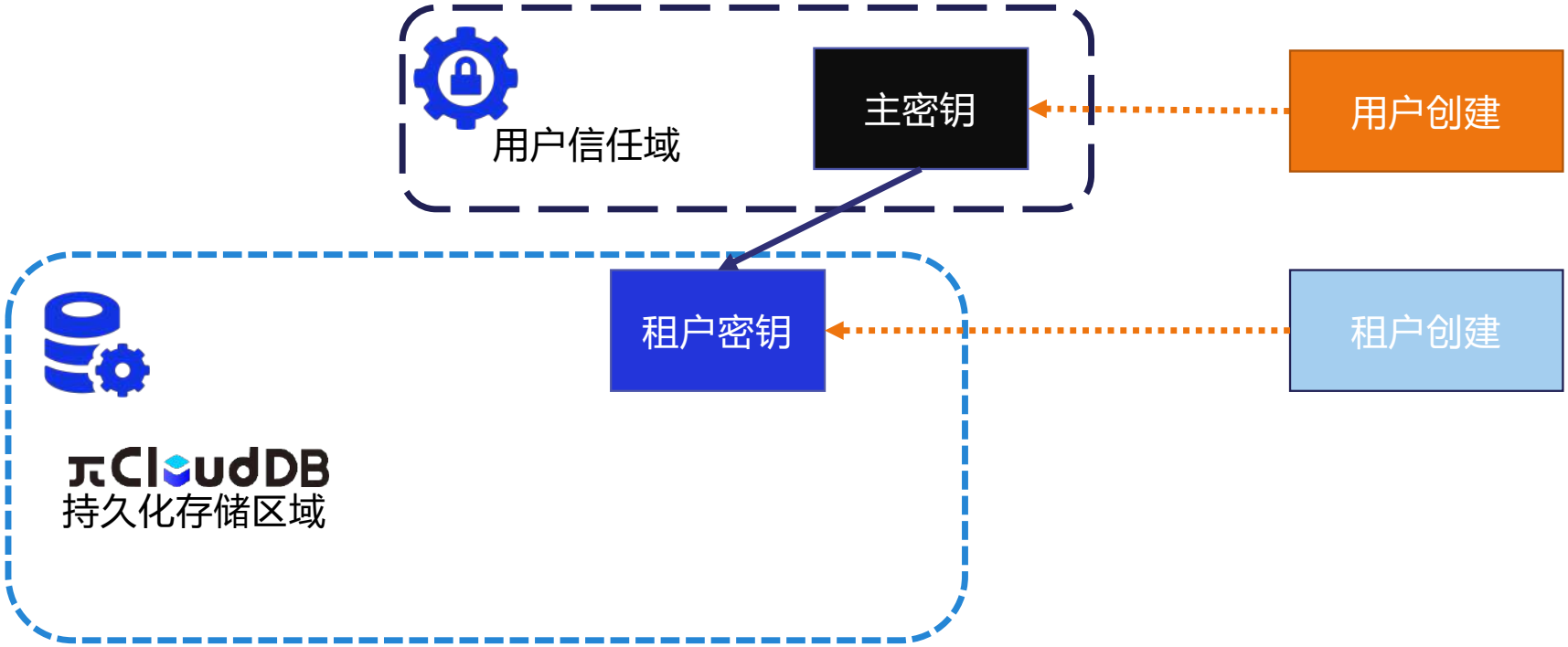
元CloudDB透明加密的实现

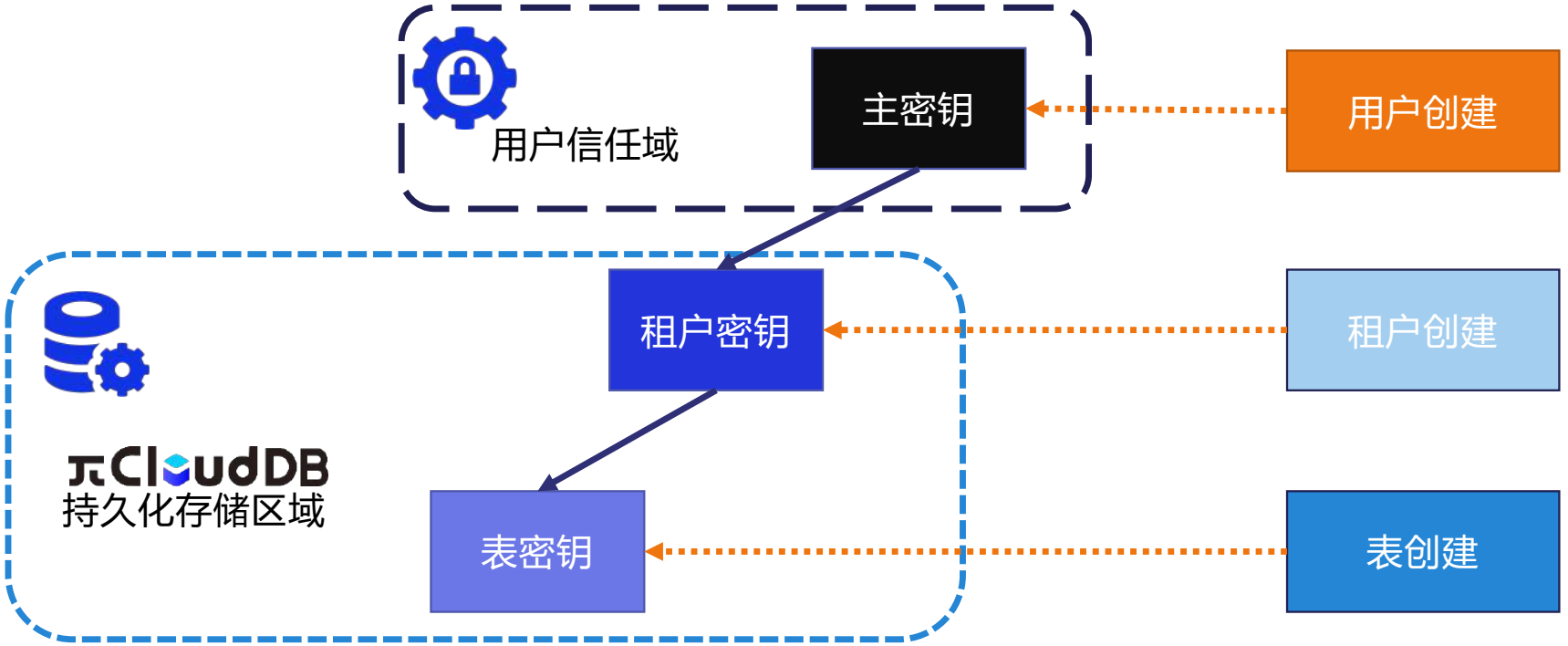
OpenPie

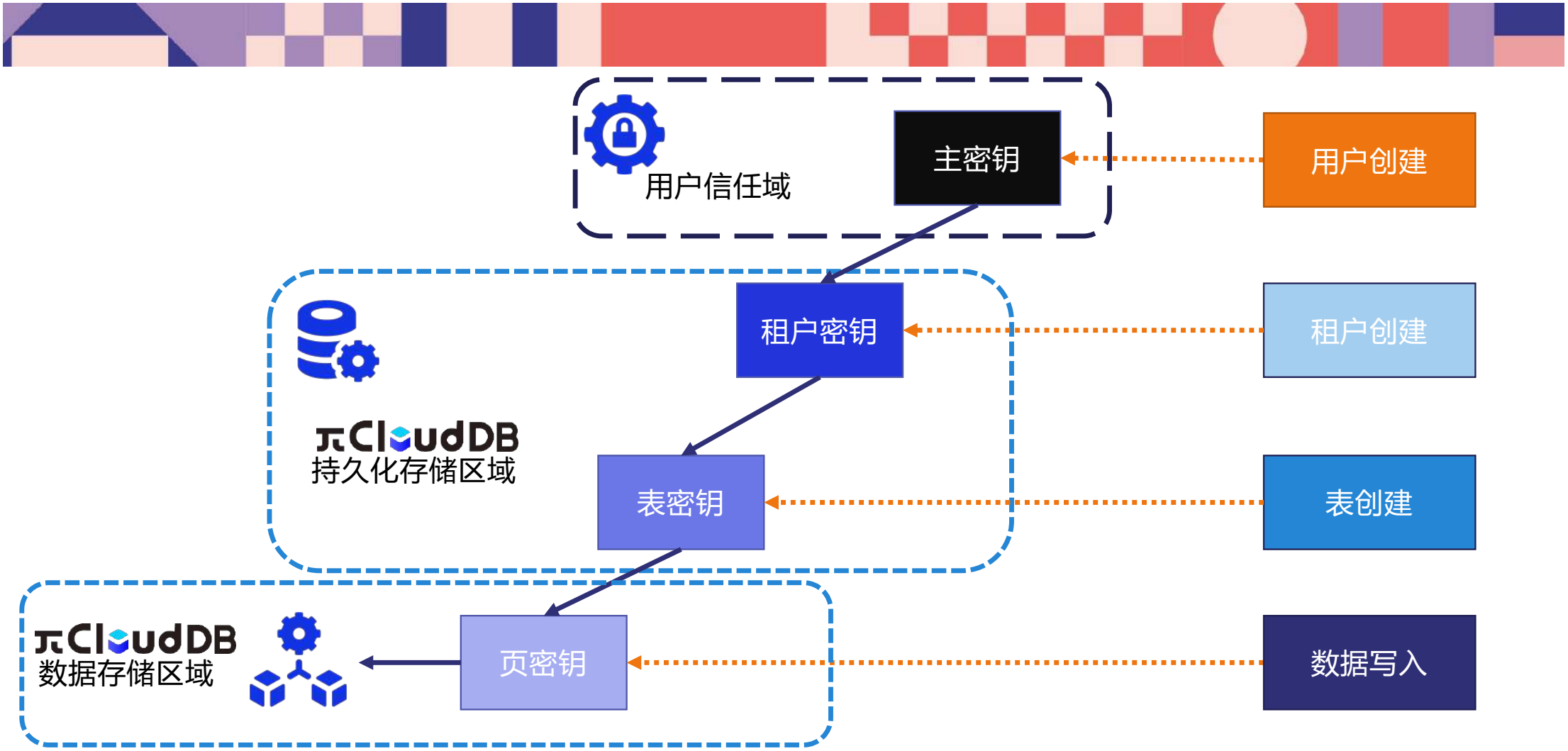
密钥管理

- 主密钥由用户提供
  - 保存于用户信任域中
  - 无需加解密主密钥
- 多级密钥
  - 单密钥加密数据为数据页
  - 轮换上级密钥无需重新加解密数据
  - 支持按页/按表轮换密钥
- 密钥保存
  - 次级密钥均在持久化存储中
  - 页级密钥与数据共存


用户信任域
主密钥
用户创建


用户信任域
主密钥
用户创建
租户密钥
租户创建
CloudDB
持久化存储区域

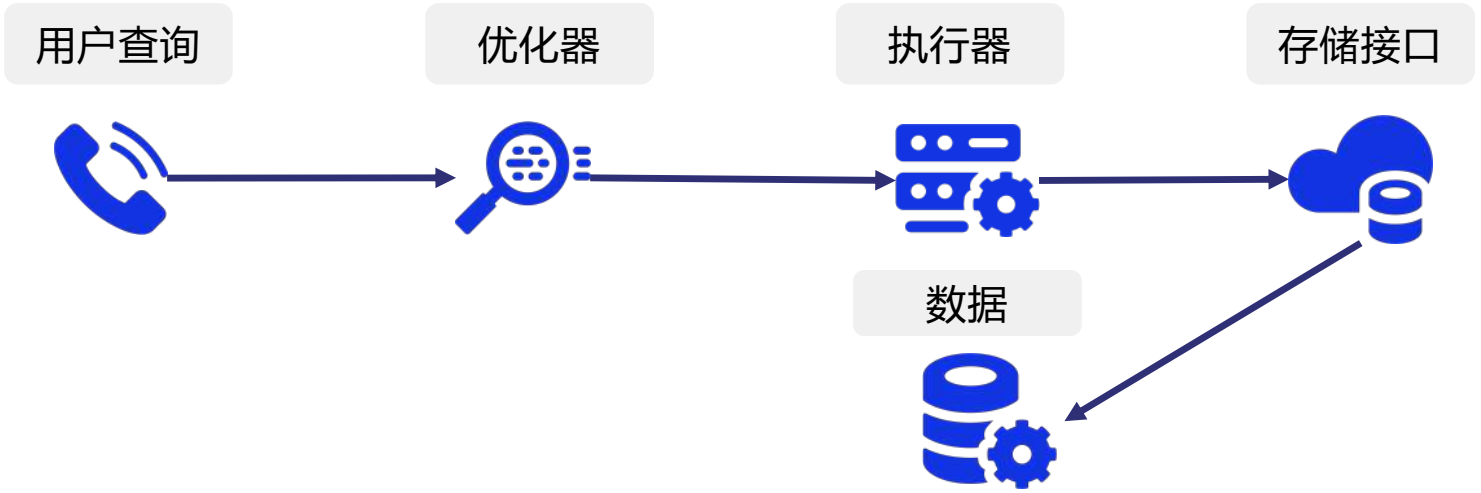

用户信任域
主密钥
用户创建
租户密钥
租户创建
PolarDB
持久化存储区域
表密钥
表创建


用户信任域
主密钥
用户创建
租户密钥
租户创建
PolarDB
持久化存储区域
表密钥
表创建
PolarDB
数据存储区域
页密钥
数据写入

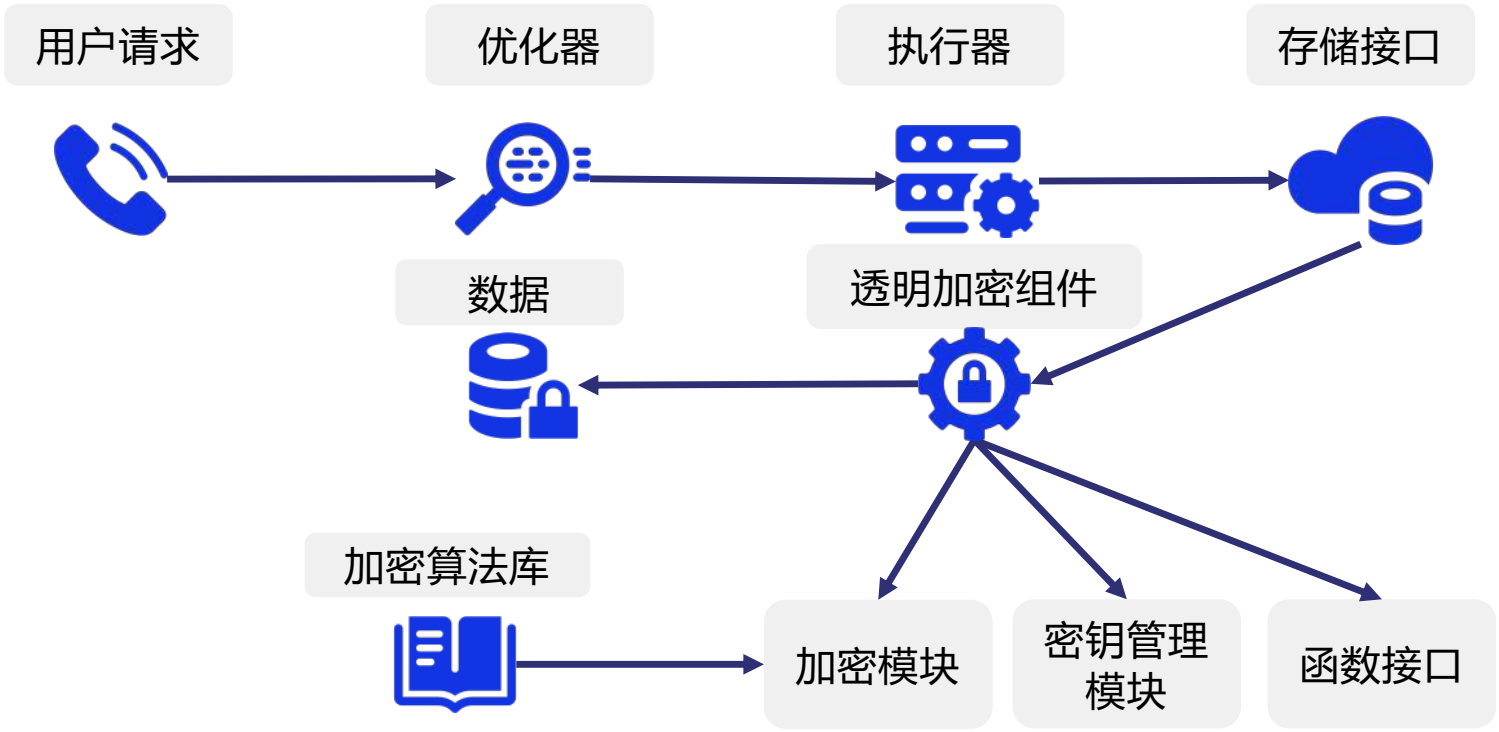
透明加密实现细节

- 模块化实现
  - 优化器、执行器不感知
  - 模块完美支持自研存储
- 可插拔加密算法库
  - 支持不同硬件加密算法
  - 支持国密算法
- 不影响用户业务
  - 原有业务无需变化
  - 不影响ETL数据导入导出

透明加密组件架构



透明加密组件架构



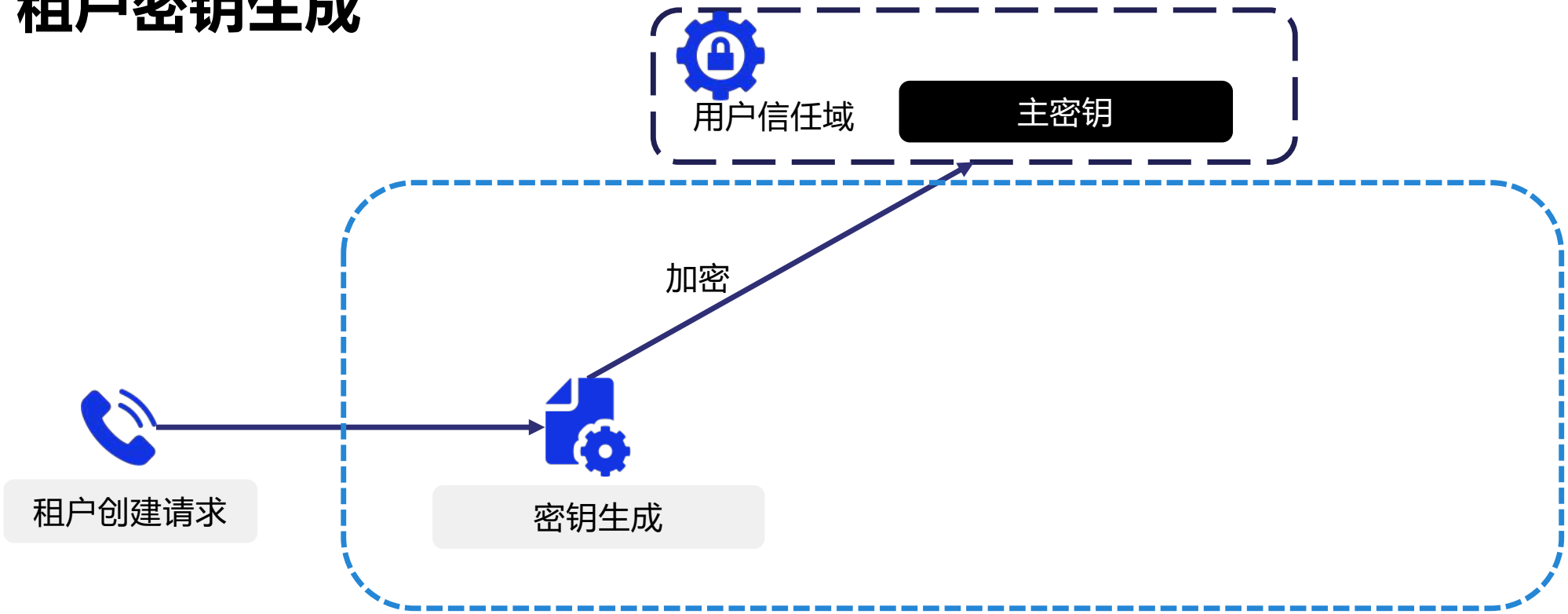
租户密钥生成

用户信任域

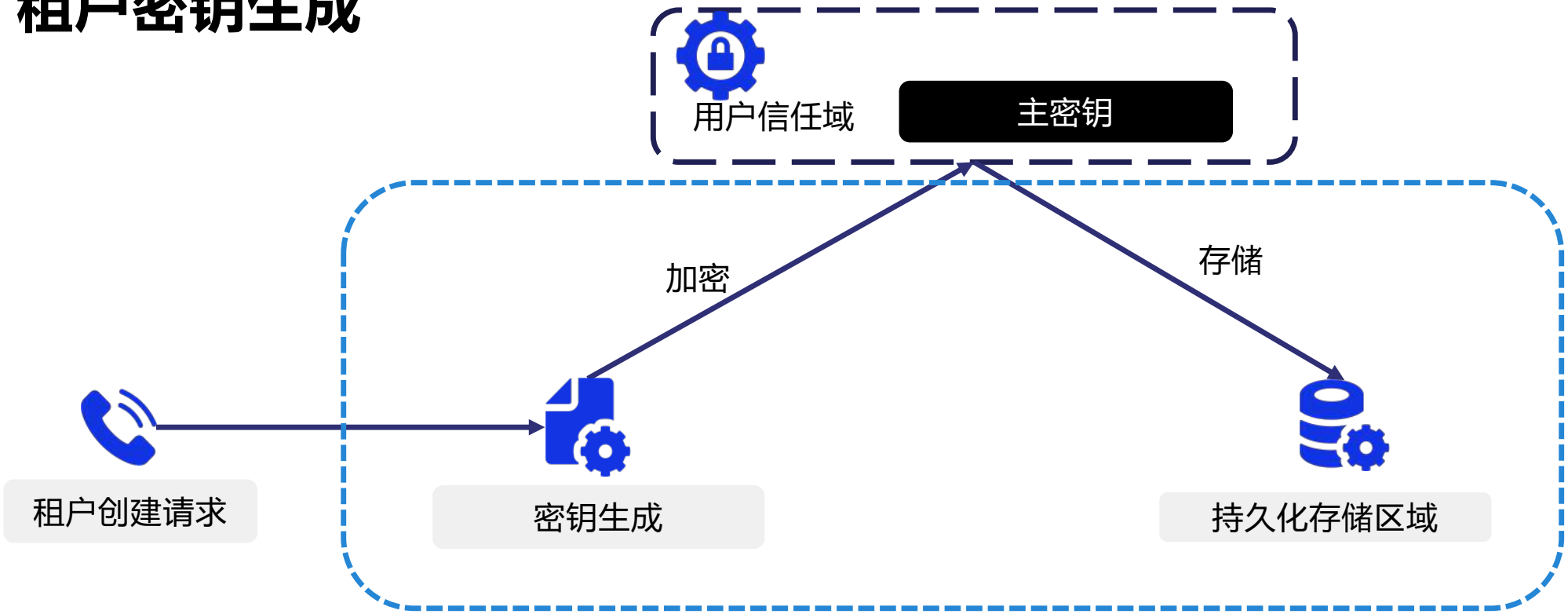
主密钥

租户创建请求

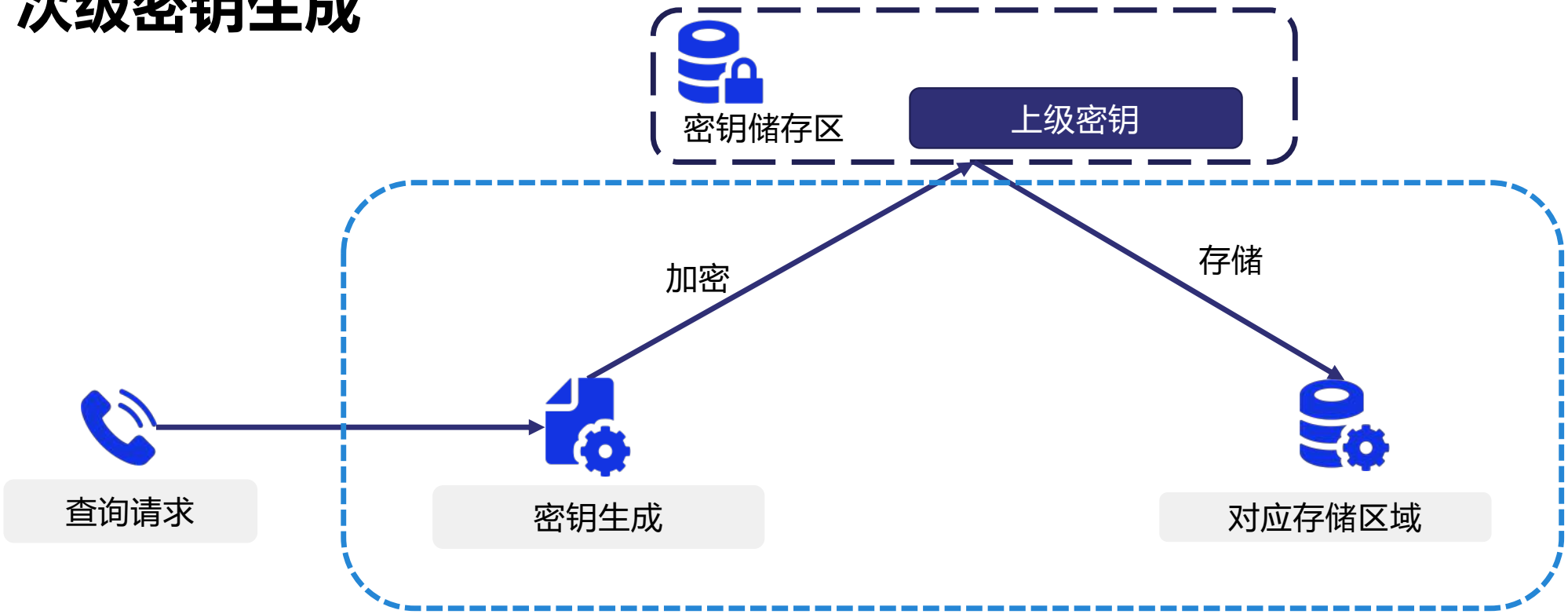
租户密钥生成



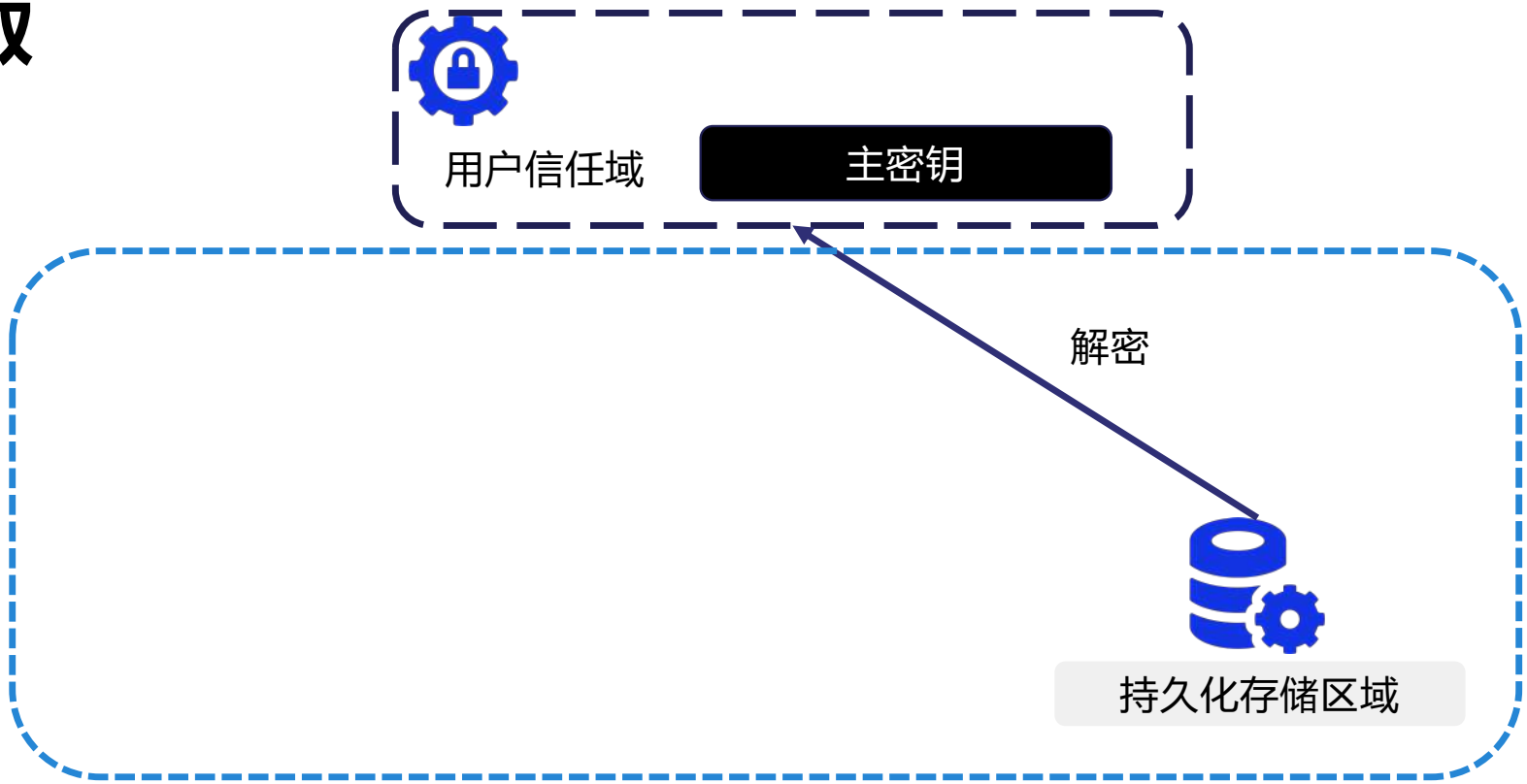
租户密钥生成



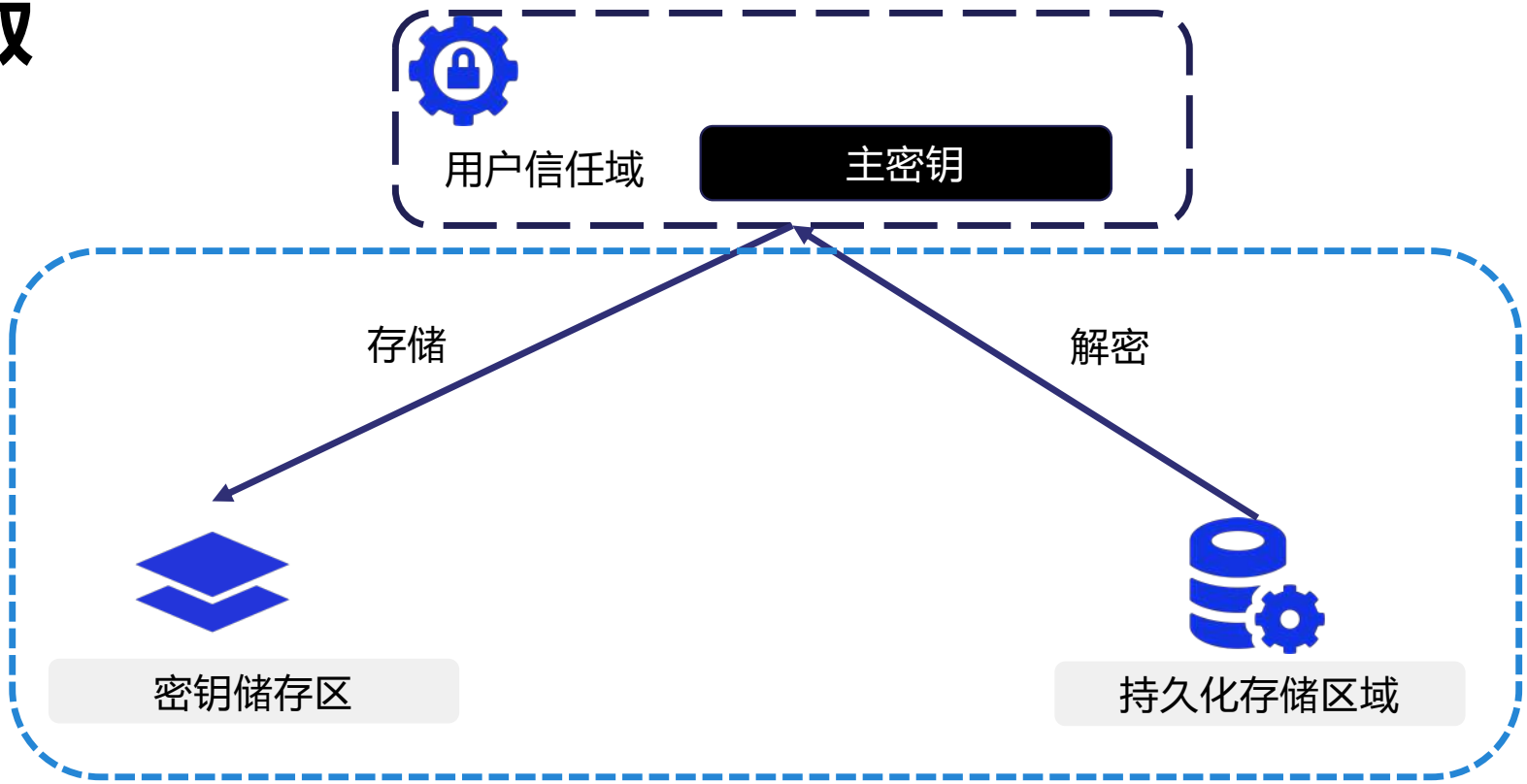
次级密钥生成



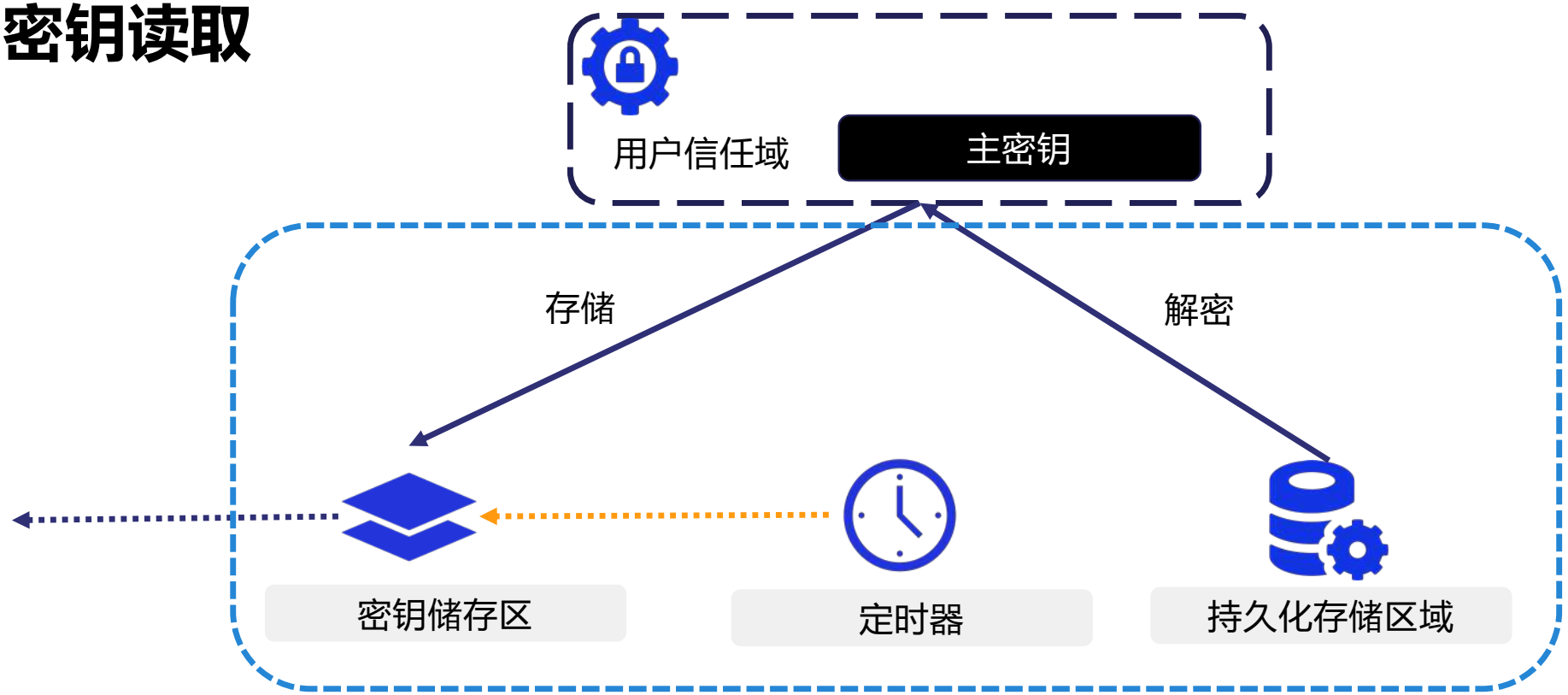
租户密钥读取



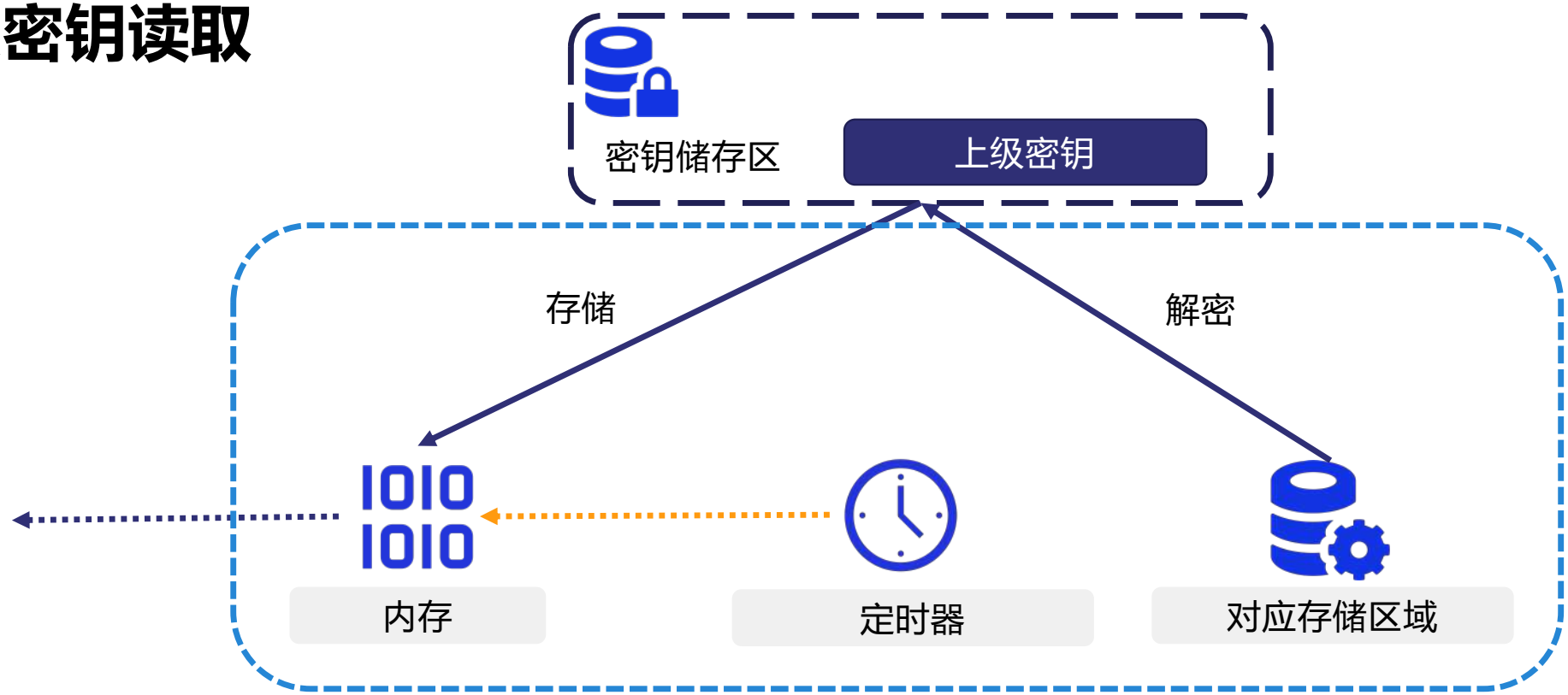
租户密钥读取

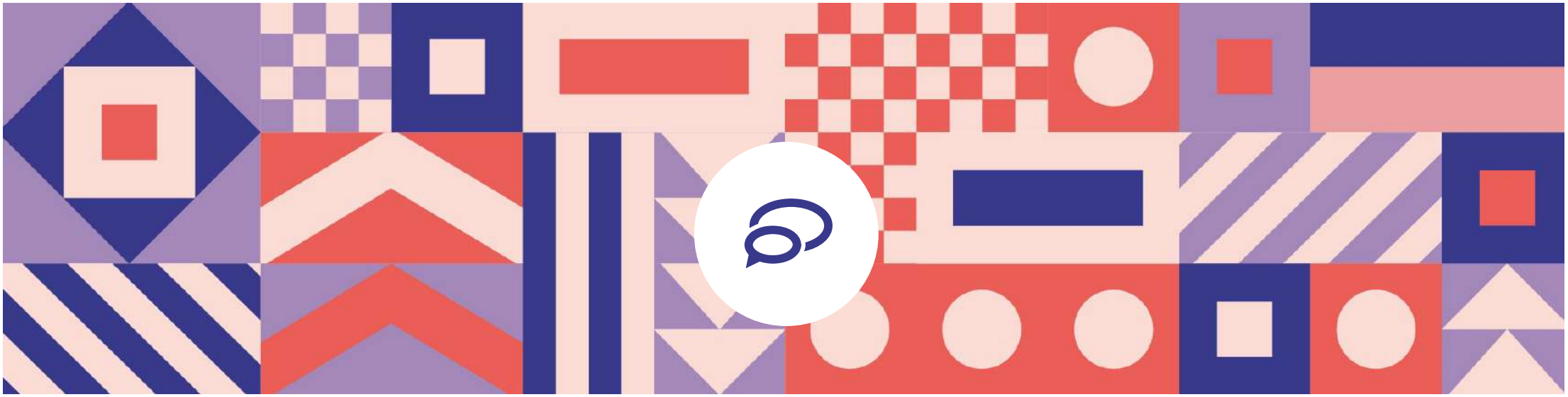


租户密钥读取



次级密钥读取





PART 04

总结

总结

- 用户侧
  - 符合审计流程
  - 用户无感知
  - 业务不变化
- 研发侧
  - 不影响内核迭代
  - 独立模块，方便后续扩展
  - 无历史包袱

加入我们！

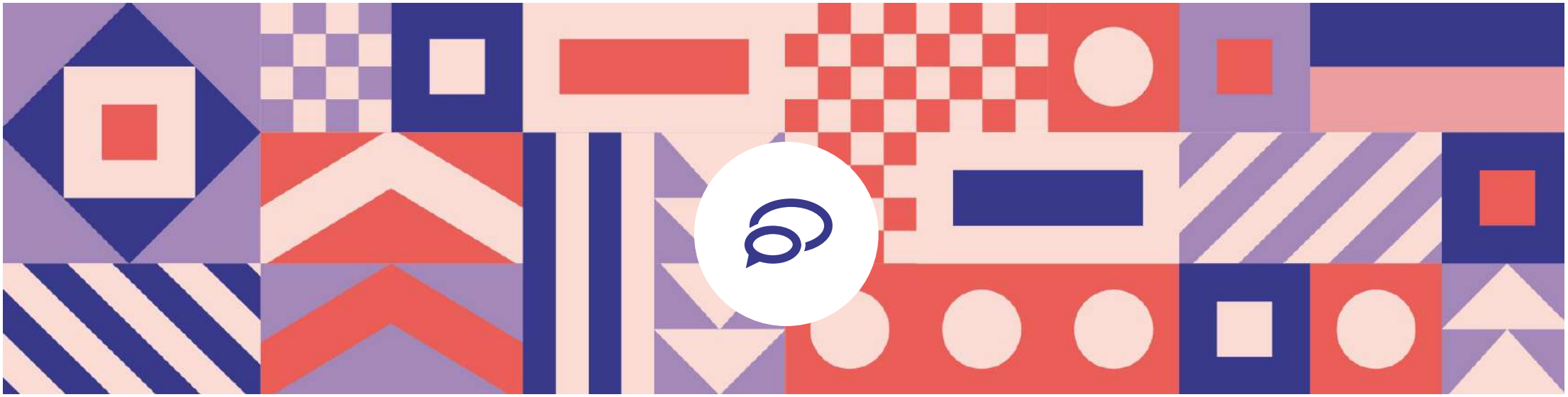
- **官　　网：** https://www.openpie.com
- **公 众 号 ：**PieCloudDB | 拓数派
- **技术社群：**扫码添加入群助手

扫码加入 PieCloudDB 技术群

PCC POSTGRESCONF CN 2022

CHINA POSTGRESQL ASSOCIATION

OpenPie



谢谢！

OpenPie