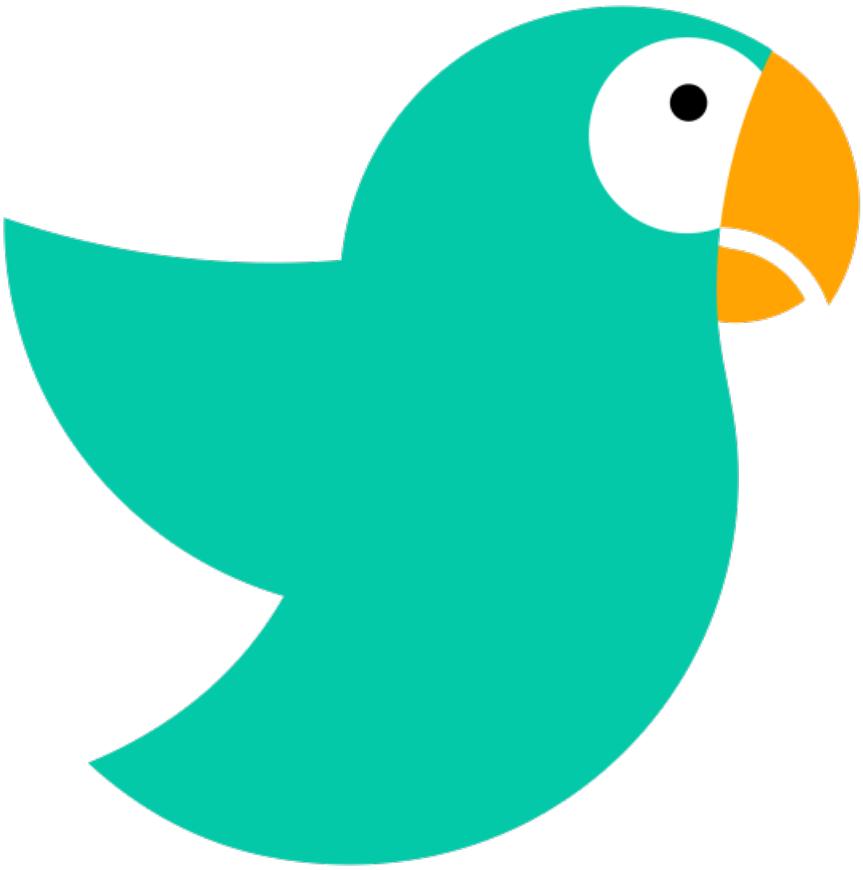

Baklib安全白皮书

版本（v1.0）

前言

Baklib 是成都探码科技旗下的一款专注企业知识人工智能的 SaaS 云服务系统。我们的使命是帮助知识创新型企业，实现向内知识协同和对外产品宣传的网站内容管理。我们相信，现代文档技术可通过改善用户体验来提高用户试用率和客户留存率，从而使公司增加收入。通过易于导航的在线文档、产品说明、培训手册和教程来获得此结果。

我们致力于使 Baklib 成为面向未来的最佳智能知识助理，通过 Baklib 只需三步即可创建一个结构清晰、易导航、易检索的产品介绍网站。

Baklib 采用业界领先的技术，对产品、用户数据进行全生命周期的安全保障，同时具有高度的可扩展性与可用性。Baklib 产品的设计、开发和运营充分考虑了合规性以及用户个人信息隐私性要求。

1、合规安全

1.1、安全体系认证

探码科技高度重视产品的合规性，积极对标国内和国际最高标准合规性要求。目前 Baklib 已通过公安部等级 2.0 保护三级、ISO27001。标志着我们在信息安全管理、 服务质量管理、IT 服务管理等方面达到了更规范化、更标准化的水平，为公司全面质量体系的改进和完善奠定坚实的基础。

1.2、政策合规

Baklib 根据国家信息安全相关法律、法规要求，设置与信息安全监控机构之间的联络员，制定实施程序，以确保提供的产品符合国家关于知识产权相关法律和法规要求。 Baklib 同所有企业及开发者签署保密协议，并通过定期检查识别、记录、评审保密协议中数据安全的相关控制要求（如访问控制、防泄露及完整性要求），防止不正当披露、篡改和破坏数据。

2、组织及人员安全

2.1、安全团队及职能

Baklib 作为 SaaS 服务提供商，一直都把用户业务和数据的安全保护列为最高优先级工作。公司具有完善的基础架构安全以及用户业务、数据安全保护体系，可以为用户提供从物理到应用层面的全方位防护。

Baklib 产品安全团队是 CTO 直接领导，由安全团队负责人、产品负责人及技术负责人组成。工作内容包括产品设计安全评估、代码安全审阅、漏漏洞洞扫描、渗透测试、威胁情报、入侵检测、应急响应、数据安全、安全合规等。

2.2、人员安全

在入职前，探码科技在国家法律法规允许的情况下，通过一系列背景调查手段来确保入职的员工符合公司的行为准则、保密规定、商业道德和信息安全政策，背景调查手段涉及刑事、职业履历和信息安全等方面，背景调查的程度取决于岗位需求。

在探码员工入职后，所有的员工必须签署保密协议，确认收到并遵守探码安全政策和保密要求，尤其是关于客户信息和数据的机密性要求将在入职培训过程中被重点强调。此外依据员工的工作角色进行额外信息安全培训，确保员工管理的用户数据必须按照安全策略执行。

3、数据安全

信息安全主要目标之一是保护业务系统和应用程序的基础数据安全，所以数据安全是企业的生命线。依据数据安全生命周期，Baklib 从数据创建、存储、传输、使用、共享、归档至销毁，使用了数据分级、数据加密等措施，保障了数据的保密性、完整性、可用性、真实性、授权、认证和不可抵赖。

3.1、数据传输

Baklib 为用户提供了支持强加密协议的数据传输链路，消息拉取、身份验证、操作指令等数据传输均使用 HTTPS 进行加密并使用 2048 位 RSA 密钥。

3.2、数据存储

Baklib 使用安全的密钥机制对数据进行加密存储，我们对所有消息及云文档数据都进行了加密存储。

Baklib 制定了完善的数据分类分级管理办法，对 Baklib 收集的用户信息、后台管理系统中的用户信息等都进行了严格的分类分级管理，并对所有系统中存储的敏感信息进行了加密处理，有效保障用户信息安全。

加密算法内嵌于应用源代码中，密钥由密钥管理系统（简称“ KMS 系统”）产生生，并由应用调用。KMS 服务负责密钥和敏感配置信息的全生命周期管理，包括创建、存储、分发、使用、更新、删除等。Baklib 用户的数据加密使用的主密钥和 Baklib 服务的各种其他敏感信息（如数据库账户、密码等）均存储于 Baklib 维护的 KMS 系统中，访问需通过 KMS 接入进行。KMS 系统的主密钥使用密钥共享协议生成多份密钥分量，分发给不同职能角色进行管理，提供大于总数一半以上的密钥分量才能还原 KMS 系统的主密钥。KMS 主密钥会定期轮转更新，提高 KMS 数据的安全性。

3.3、数据使用

用户数据的访问均进行了严格的权限隔离。用户之间在没有授权的情况下，无法互相访问。对数据的访问必须通过数据所有者显式的授权，比如共享操作等来完成。

Baklib 员工对用户数据的访问被严格限制和审计，员工默认没有对任何用户数据的访问权限。特殊的访问需求要经过内部严格的审批流程，才可以获得临时访问权限，在操作完成后权限将立刻被收回。Baklib 对数据的操作均有详细日志记录，并区分不同操作者角色，授予不同的权限，操作需要进行审批审计。

我们不会公开披露用户的信息，除非获得用户的同意。但根据法律法规、强制性的行政执法或司法要求，在必须提供用户个人信息的情况下，我们可能会依据要求的个人信息类型和披露方式向行政执法或司法机构披露用户的个人信息。当我们接到披露请求时，在符合法律法规的前提下，我们要求其必须出具与之相应的法律证明文件，我们仅提供执法部门因特定调查目的且有合法权利获取的数据。在法律法规许可的前提下，我们披露的文件均在加密措施的保护之下。

3.4、数据安全检测

Baklib 线上环境所有服务器的登录行为、操作行为、服务器安全基线文件变更、访问权限变更和数据访问行为都会被记录。安全团队通过建立用户行为画像和异常行为模型，实现异常行为的识别、分析和关联，自动化实时检测各种异常数据访问行为，如对数据的非法访问、恶意数据爬取、风险操作、登录异常、权限升级等，进行告警或阻断。

3.5、数据销毁

在终止对用户服务时，Baklib 管理员会删除用户账户信息，在符合当地法律法规的前提下，永久删除用户数据，确保无剩余信息。用户机构的离职员工可向用户管理员提出账号注销申请，由用户机构确认离职员工账号数据已被转移后，用户管理员联系公司，公司根据用户机构用户管理员的申请，对需注销的账号相关的数据及文档进行去删除处理。

公司在与用户机构签订合作协议时，与用户机构约定，当终止合作时，将根据用户机构提出的数据销毁要求销毁对应数据。

除供企业用户内的用户使用外，Baklib 亦支持个人用户使用。若个人用户需注销账号，须联系客服，提供账号信息提交注销账号申请，管理员根据申请，对后台数据库中该账号相关的数据及文档进行删除处理。

4、系统及网络安全

4.1、系统软件安全

Baklib 线上服务均运行在可靠的操作系统版本上，安装软件必须由运维人员从公司统一维护的可信安装源下载和安装。对于通用的系统软件，例如 Nginx、 SSH 等，制定了对应的安全配置规范，并进行相应的维护。安全团队也会跟踪业界安全问题，评估服务器上的软件是否存在安全漏洞或隐患，一旦发现，会通过应急响应流程推动漏洞的修复。

4.2、登录授权与访问控制

Baklib 根据功能或安全级别，不同模块之间使用安全组隔离。运维人员必须通过 VPN 方式才能访问生产服务器，VPN 连接强制采用双因子认证机制。VPN 账号专人专用，员工离职或岗位变动时，对应的账号和 VPN 个人证书将被删除。

4.3、系统安全检测防御

Baklib 的服务器上统一部署了主机入侵防御系统，并依托大数据处理平台，对出入站流量进行分析，实现对入侵等安全事件的检测和预警。

4.4、网络安全

Baklib 的生产网络与办公网络完全隔离，并通过严格的审核机制以及上线流程来保证受信程序或端口的安全访问，默认不开放互联网访问端口，对外开放的端口必须经过安全团队评估。同时安全专员会定期执行网络安全扫描测试以主动发现可能存在的网络隐患。Baklib 已实现全站 HTTPS 的访问以防止各种网络窃听行为和流量劫持的发生。并与第三方安全厂商合作实现 DDOS 的攻击防护，确保第一时间发现攻击并进行流量清洗，保障用户的安全访问。

5、应用安全

5.1、Baklib SDL

Baklib 在项目开发流程中引入了 SDL，借鉴了微软推广 SDL 的经验，并结合企业级安全需求及 Baklib 自身的项目开发流程，控制项目整体的安全风险。 安全开发流程参照软件安全开发周期（Security Development Lifecycle）建立:

① 人员培训环节：安全工程师给开发人员进行安全开发规范、安全意识培训等，提高其安全意识；

② 安全需求分析环节：根据功能需求文档进行安全需求分析，针对业务内容、业务流程、技术框架进行安全评估；

③ 安全开发环节: 根据不同的开发框架，提供安全编码规范及安全框架配置规范，避免开发人员写出不安全的代码；

④ 安全测试环节：通过代码扫描工具进行白/黑盒扫描，并结合人工审核代码漏洞；
⑤ 项目发布环节：安全部门依据上述环节评价结果决定项目是否发布；
⑥ 安全运营与应急响应：安全工程师通过应急响应平台进行安全运营及事件应急响应

5.2、账号安全

用户对 Baklib 系统的访问，采用密码 + 动态密码多因素验证登录，可以有效避免因密码丢失导致的账号泄露。Baklib 密码存储为加密存放，采用的是不可逆的多重哈希混淆算法加密。当用户需要找回密码时，只能通过重置或者管理员赋予新密码来更改密码。对于未识别的设备发起的登录或短时间内多次帐号密码错误，采用图片验证码方式，进行防范机器行为的暴力破解。同时账号系统具备恶意注册、反撞库、反暴力登录破解等防护能力。

5.3、应用数据安全

Baklib 在基于 SSL/TLS 协议为应用程序供数据保密性和完整性的基础上，构建了一套完整的私有安全通信协议，通过加密用户在网络传输中的信息，防止窃听，以确保信息在网络中传输安全。

在不采用 SSL/TLS 前数据存在传输存在以下风险：

① 窃听风险（eavesdropping）：第三方可以获知通信内容；
② 篡改风险（tampering）：第三方可以修改通信内容；
③ 冒充风险（pretending）：第三方可以冒充他人身份参与通信

而采用 SSL/TLS 后，这些风险都可以规避：

① 所有信息都是加密传播，第三方无法窃听；
② 具有校验机制，一旦被篡改，通信双方会立刻发现；
③ 配备身份证书，防止身份被冒充

Baklib 的 SSL/TLS 证书见图 1：

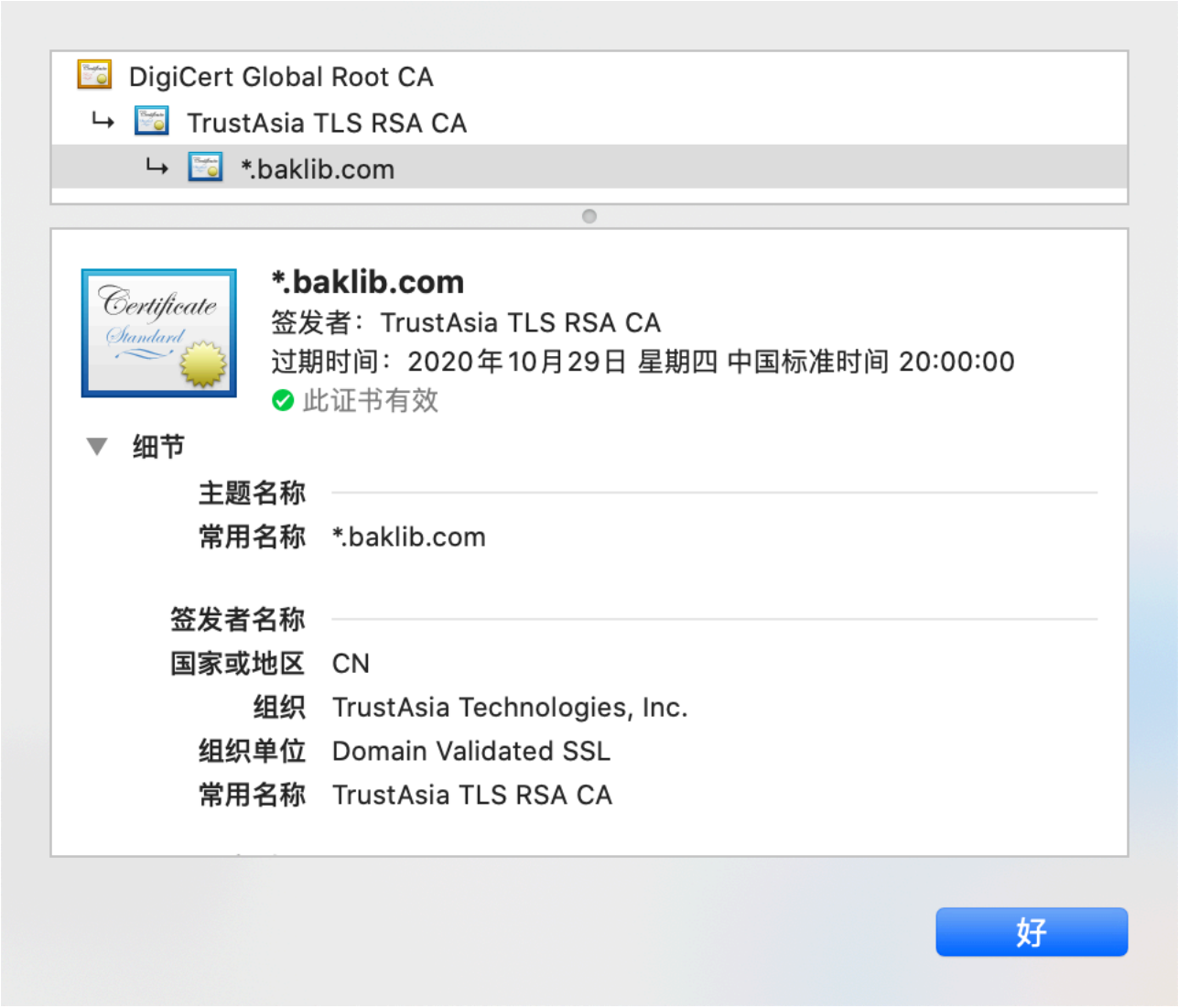

图 1 Baklib SSL 证书信息

6、物理与环境安全

Baklib 所在的 ucloud 云主机，机房建设遵从银行级的安全监管与合规要求，符合金融监管级等保要求，可以确保客户的数据从物理和环境安全上受到严格的保护。

Baklib 不定期会通过请安全服务商、白帽子进行外部安全渗透的形式来检测、巩固和提高产品、数据与服务器的安全级别。

7、灾难恢复与业务连续性

Baklib 后端采用多实例接入，保证服务的可靠性。对流量和故障做细致监控，在流量突发、或者故障时，采用降级运行方式保障业务可用性。

7.1、应急制度

Baklib 内部有一支应急处理小组，直属于 CTO，在遇到问题的时候，我们的应急处理小组将会立刻响应并处理。与此同时我们会定期进行应急演练，以保持应急状态。应急演练包含如下内容:

① 精确到每条任务与状态的应急处理；
② 数据多级别备份恢复以及异地备份恢复；
③ 灾后应急响应

7.2、灾备演练

Baklib 每季度会进行一次数据灾备演练。目的旨在针对不可预知的天灾可能带来的故障进行有效的准备，保证用户数据的安全性、一致性，并能够有效、高效的进行灾难恢复。主要从以下几个层面进行演练：

① 模拟数据库故障、服务器故障；
② 模拟故障后数据恢复流程、不断完善并找出其中的问题予以解决；
③ 模拟故障后数据恢复的可靠性和时效性