上上签安全白皮书

版本：V3.0

发布时间：2020 年 04 月

目录

【声明】

本文档基于现状编写，仅供读者了解上上签安全体系参考。对于本文档中的信息，上上签不作明示、默示的保证。

由于服务的迭代和升级，本文档内容会不定期进行更新，恕不另行通知。上上签保留直接对文档内容进行修改的权利，并在官网入口进行发布。请从上上签官网获取本文档的最新版本。

1 前言

上上签，中国电子签约云平台领跑者，以构建智能时代的诚信规则为使命，致力于打造以电子签名为纽带的生态服务体系。

2019 年 4 月，上上签品牌安全战略升级，行业首创“终身 SaaS”商业模式，并提出“电子签约上上签，合同终身保安全”的全新口号。在高度关注用户隐私和数据安全的责任下，上上签结合业界先进的云安全理念和安全实践，构建了纵深防御和合规遵从的安全保障体系。

借此白皮书，我们将向大家介绍上上签品牌价值背后：具备高度安全意识的团队组织，指导体系防护思维的政策方针，实践纵深防御落地的技术方法。将上上签在电子签约领域积累的安全经验，分享给用户，分享给业界，相互了解，相互监督，共同推动电子签约行业的发展。

2 组织与人员安全

2.1 组织安全

上上签自成立以来，充分认识到安全对业务的支撑作用，一直坚定“企业安全需要全员的配合与努力”，并在工作中积极调动大家的积极性。为此，公司设立了：

（1）信息安全委员会：决策和审批公司的安全战略；

（2）信息安全小组：执行主机安全、网络安全、应用安全等基础安全工作，保障系统可靠运行；

（3）安全审计小组：关注公司内部对安全法律法规和流程的遵从度，积极实施合规审计、风险评估等工作，监控、排查潜在威胁；

（4）应急响应小组：负责疑似信息安全事件的应急响应组织和协调工作；

（5）体系小组：负责公司安全制度的管理与发布等工作。

各团队高效协同，推动业务安全合规地发展，切实保障上上签广大用户的利益。

2.2 人员安全

2.2.1 背景调查

上上签在国家法律法规允许的情况下，会仔细考察候选人的能力与职业素养，验证候选人的个人背景与工作经历的真实性，确保候选人的品行与职业道德符合要求。

2.2.2 保密协议

员工入职后必须签署保密协议，并参加“信息安全意识培训”，学习保密要求与安全工作守则。保密协议对于员工履行职责中知悉的秘密信息有严格的保密要求，员工在职时和离职后均有效。

2.2.3 安全教育

让员工接受持续的安全教育是上上签信息安全策略的重要组成部分。上上签致力于建设活力与包容的安全文化，并将其渗透至招聘流程、员工入职、在职员工培训以及日常业务运营之中。上上签持续开展的安全教育工作包括：

（1） 全员安全意识培训：面向全员开展信息安全活动周，宣贯安全的工作行为准则；

（2） 技术部安全研发培训：面向技术部成员提供安全技能培训，提升研发过程中的安全水平；

（3） 我司在办公环境布置了安全意识宣传海报，时刻提醒员工树立安全责任意识。

3 安全合规

3.1 合规认证

上上签建立的安全体系得到了国内外权威机构的认可，我们积极解读众多合规标准要求，并将其融入到上上签安全体系的执行程序中。截止目前，上上签先后获得了如下表所示的合规资质：

国际标准		
资质	测评/颁证机构	意义
ISO/IEC 27001 信息安全管理体系认证	BSI（英国标准协会）	ISO/IEC 27001 是被广泛采用的全球安全标准，上上签是国内首家获得 ISO/IEC 27001 认证的电子签约服务提供商。通过此认证，体现了上上签对安全的承诺，表明上上签建立了系统的、持续的方法来管理信息安全风险，以保障自身及客户信息的保密性、完整性和可用性。
ISO/IEC 27018 公有云个人身份信息处理器保护个人身份信息管	BSI（英国标准协会）	ISO/IEC 27018 是专注于云中个人数据保护的国际行为准则，标准所制定的指引基于 ISO/IEC 27002，同时考虑了可能适用于公有云服务提供商信息安全风险环境范围内有关 PII 保护的要

理体系认证		求。上上签是业内首家获得 ISO/IEC 27018 认证的电子签约服务提供商。通过此认证，体现了上上签在保护企业数据、知识产权、个人信息等方面达到了高标准的行业实践。
ISO 38505-1 数据治理认证	BSI（英国标准协会）	上上签非常重视用户数据安全，是全球首家通过 ISO 38505-1 认证的公司，我们构建了先进的数据治理框架，通过建立业务需求、技术研发、安全管理的协同机制，驱动数据中台的建设，提升公司的数据安全能力，保障客户数据安全。

国内权威		
证书名称	测评/颁证机构	意义
可信云认证	中国信息通信研究院、数据中心联盟	可信云服务（TRUCS）认证是我国针对云服务，由数据中心联盟和云计算发展与政策论坛联合组织发起，由中国信息通信研究院测评认证的权威认证体系。上上签是国内首家获得可信云服务认证的电子签约服务提供商。获得可信云服务认证意味着上上签在企业信息和业务基本信息披露的真实性、云服务指标（含 SLA）的完备性、规范性和真实性等方面满足国家权威认证机构的认证要求，也意味着上上签的产品质量、技术实力、用户权益保障、运营和服务能力获得权威认证机构的认可，是为用户智选云服务商的重要依据。
信息系统安全等级保护三级认证	杭州市公安局	上上签是国内首家通过三级等保测评的电子签约服务提供商。通过等级保护测评意味着上上签重视国家在信息安全方面的制度，积极配合公安部门开展等级保护方面的工作，遵循国家在信息系统安全建设方面的技术保障要求和安全管理要求，接受监管部门的监督检查。
云计算服务能力标准符合性认证	中国电子工业标准化技术协会	通过云计算服务能力标准符合性认证标志着上上签云服务能力在安全、技术、人员、管理等方

		面达到国家标准（GB/T 36326-2018）的要求。

3.2 内控审计

为确保安全体系在公司快速发展的同时保持规范化、持续化的运行，上上签会定期开展如下安全审计工作，以确保及时发现合规风险，全面推行安全政策：

审计名称	描述
IT 运行审计	检查 IT 运行策略配置是否合规。
信息系统权限审计	检查内部系统权限配置是否合理。
内部体系运行审计	检查安全制度执行情况与适用性。
风险评估	评估关键资产的风险。
管理评审	评价与决策制度和程序的适用性。

4 系统安全

4.1 基础设施

上上签电子签约平台底层采用阿里金融云。阿里金融云符合等级保护四级要求，遵从金融级的安全监管与合规要求，使上上签电子签约平台更加安全可靠。

4.2 主机安全

为加强主机安全管理，上上签遵循最小化原则开启业务所需的服务和端口，并部署了主机 IDS，实现异常登录检测、异常行为检测等能力。

同时，我司启用了阿里金融云安全中心，实现系统化的基线检查、补丁管理、漏洞管理、抗 DDoS 等安全能力，保障平台安全运行。

4.3 网络安全

上上签的生产网络、测试网络和办公网络物理隔离。生产网络采用了 VPC，并部署了网络 IDS、WAF 应用防火墙，有效识别异常。在各独立网络内部，上上签利用行业标准防火墙或访问控制列表（ACL）实现更细化的逻辑隔离。

4.4 安全研发流程(SDL)

为了在产品的快速成长中持续保障应用安全，上上签在项目开发流程中引入了安全研发规范，结合企业级安全需求及上上签自身的项目开发流程，控制项目整体的安全风险。

安全开发流程详情如下：

（1） 人员培训环节：研发人员接受代码安全规范、安全意识等培训；

（2） 需求分析环节：安全人员根据需求文档进行安全需求分析，针对业务内容、业务流程、数据流进行合规、风险等方面的评价；

（3） 安全开发环节：研发人员遵守安全编码规范要求进行开发，并使用代码扫描工具进行自动化扫描；

（4） 安全测试环节：通过扫描工具进行黑盒扫描，并结合人工验证漏洞。

5 数据安全

5.1 数据治理

我司依据业务战略，制定了数据战略来指导数据使用计划；依据数据战略，拟定了数据责任地图，覆盖收集、存储、报告、决策、分发、处置的生命周期，明确各阶段对数据的价值、风险、约束。基于责任地图，我们建立管理体系与数据绩效，引入技术手段，解决：数据在哪、数据去哪、谁用数据、如何管数据的问题，并建立对应监督机制。

5.2 数据收集

当您使用上上签的服务时，为保障您正常使用我们的服务，我们会在您同意的前提下收集必要的个人数据。上上签在数据收集方面遵守公开透明和最小必要原则，我们在《隐私政策》中披露了具体的收集与使用规则。

5.3 数据传输

上上签电子签约平台采用 SSL/TLS 协议，实现全站 HTTPS 数据传输。平台所有开放接口在前述加密传输的基础上还实现了双向签名及认证，保障数据传输的保密性和完整性。

5.4 数据存储

上上签通过数据加密和密钥管理为敏感数据提供保护，上上签采取的数据存储策略如下：

（1）个人敏感数据：如个人/法人证件号，采用国密算法 SM4 加密存储；

（2）合同文件：采用高强度对称加密算法 AES256 一文一密加密存储。

5.5 数据使用

上上签不会用真实用户的个人身份信息进行测试，除非用户主动要求并授权。

所有客户在使用产品过程中产生的临时数据，均会被不可撤销地自动清除。

上上签系统运行日志中的个人身份信息都会被脱敏处理。

5.6 数据销毁

上上签保障用户删除数据的权利，如数据主体要求销毁数据，并提供了合规的销毁申请，上上签审核通过后，会遵循严格的数据销毁流程执行销毁程序。法律另有规定的除外。

5.7 KMC 密钥管理中心

密钥管理中心（KMC）是上上签电子签约平台的关键系统之一，为核心业务应用提供密钥管理服务，主要负责密钥的生成、使用、存储，并提供数据加解密服务。

KMC 的设计与管理符合行业合规要求，是上上签电子签约平台实现密钥明文不落地策略的核心基础设施。

6 安全运营

6.1 漏洞管理

上上签包括但不限于通过以下几种途径高效、全面地发现与识别信息漏洞：

（1） 内部安全团队的测评与评估；

（2） 第三方安全服务提供商的渗透测试；

（3） 上上签 SRC 收录的漏洞；

（4） 阿里金融云安全中心披露的漏洞情报。

我司对漏洞进行分级管理，高危漏洞会在 24 小时内完成修复。安全团队负责识别、定义和追踪漏洞，并监督漏洞的修复工作，保障业务系统稳定运行。

6.2 供应商管理

上上签设置了供应商准入程序，对第三方服务供应商进行安全评估：

（1） 由安全组进行安全相关的审查工作，如数据加密、合规资质等；

（2） 在合同中限制数据的使用范围；

（3） 在合同中明确双方的保密责任和义务；

（4） 在合同中保留我方对供应商的审计权利。

同时，为保障业务连续性，我司采取了供应商冗余备份策略。

6.3 业务连续性与灾难恢复

上上签电子签约平台采用同城双活，异地跨云容灾架构，采用全负载均衡策略，所有服务均冗余部署无单点。

其中，同城双活数据中心和异地容灾数据中心均通过专线实时同步数据。

上上签制定了 SLA，承诺服务可用性不低于 99.99%，同时，上上签提供 7×24 小时的运行维护，具备完善的秒级故障监控、业务可用性监控、可视化监控大盘、语音/IM/短信/邮件多重告警、快速定位、快速恢复等一系列故障响应机制。故障快速恢复及预防手段包括弹性伸缩、在线扩容、在线/停机迁移、自动切换以及柔性限流等。

6.4 信息安全事件管理

针对网络攻击、数据泄露等类型的信息安全事件，上上签制定了信息安全事件管理程序，会由应急响应小组快速确认事件性质、影响范围、风险等级，如识别到信息安全事件，我司会根据标准流程通知相关客户，以便客户及时采取行动将损失降到最低。

6.5 访问控制与运维安全

为保障电子签约平台安全稳定运行，我司部署了堡垒机，运维人员必须通过堡垒机开展工作，实现统一授权、统一认证、统一审计。其中，堡垒机设置了包括但不限于限制下载、打印映射、键盘记录等策略，以贯彻“生产数据不出生产”的原则。

上上签运维同事的权限开通均需通过特定流程审批，并且会由审计小组定期实施审计。

7 结语

信息安全是上上签的生命线，上上签将持续以优质的产品与服务、健全的安全体系保障用户的数据安全，树立电子签约行业的安全标杆，推动行业的不断进步。