上上签安全白皮书

版本：V2.0

发布时间：2018 年 12 月 20 日

目录

1 前言

上上签，中国电子签约云平台领跑者，提供包含实名认证、在线签署、合同托管及司法举证等一站式电子签约解决方案。企业可借助电脑、手机、平板等设备，通过 API 接口、网页、APP 等方式，随时随地与企业或个人用户完成线上电子合同的实时签署并确保其安全、合规、不可篡改。

上上签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。

上上签结合业界先进的云安全理念和安全实践、以及在云安全领域的技术积累与运营实践，构建了纵深防御和合规遵从的安全保障体系，安全保障体系是上上签电子签约平台的重要组成部分，上上签高度关注用户数据的隐私性与安全性。本白皮书主要介绍上上签在安全性与合规性保障方面的策略、方法和措施。

2 术语定义

SDL：Security Development Lifecycle 的简称，即安全开发生命周期；

PII：个人可识别信息（Personal Identifiable Information），包括任何可用于确定特定用户身份的信息，比如姓名、手机号、身份证号等；

DDoS：分布式拒绝服务攻击(Distrbuted Denial of Service)，指借助于 C/S 技术，将多个计算机联合起来作为攻击平台，对目标发动流量攻击，造成目标的业务系统无法提供服务。

3 组织安全

上上签安全团队由信息安全委员会、信息安全团队、安全审计团队组成，通过高效、协同的工作为上上签广大用户提供安全保障。

3.1 信息安全委员会

信息安全委员会成员由公司 CTO、安全团队负责人、产品负责人和技术负责人等组成，监督并决策信息安全体系的建设，对上上签整体安全负责。

3.2 信息安全团队

信息安全团队由 Web 应用安全、系统和网络安全、安全开发专家组成。信息安全团队负责产品安全架构设计及安全运营工作，是上上签信息安全体系的建设者，在安全策略、安全开发流程设计、落实及执行中扮演重要的角色。

1) 设计、开发和运营入侵检测、攻击防御产品，提供 7*24 小时安全监控；
2) 依据数据类别及安全等级，设计访问控制策略，制定及实现技术隔离措施和访问控制管理流程；
3) 制定和监督执行安全开发流程；
4) 定期对上上签电子签约平台进行漏洞检测和扫描，及时修复发现的漏洞；
5) 遵循信息安全事件管理标准，依据危害程度定义安全事件类别和相应流程，提供监控识别、分析和处理信息安全事件的能力；
6) 定期进行攻防演练，评估安全策略的可靠性和控制措施的适用性；
7) 定期为上上签员工提供安全意识培训，包括个人准则、信息保护、数据安全认证和安全开发等；
8) 积极参与安全论坛和会议，吸取业界前沿的安全技术并保持与外部安全专家的交流。

3.3 安全审计团队

安全审计团队主要对上上签进行全方位的监测、控制和审查，以验证其是否满足信息安全体系及标准，满足合规性要求，如 ISO/IEC 27001:2013、ISO/IEC 27018:2014、《信息系统安全等级保护基本要求》、可信云服务认证等。

4 合规安全

4.1 安全体系

ISO/IEC 27001:2013 是被广泛采用的全球安全标准，上上签是国内首家获得 ISO 27001:2013 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 27018:2014 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 保护的要求。上上签是业内首家获得 ISO/IEC 27018:2014 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。

信息安全等级保护：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。上上签电子签约平台已达到《GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求》第三级对应的安全指标，满足等级保护三级合规相应的技术和管理要求。与此同时，信息系统在遭遇突发信息安全状况时，上上签电子签约平台具备《信息安全等级保护管理办法》中规定的所相应的安全保护能力，包括安全对抗能力和恢复能力。

可信云服务认证：可信云服务（TRUCS）认证是我国目前唯一针对云服务，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（TRUCS）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）的完备性和规范性、云服务指标的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。

4.2 政策合规

上上签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及第三方安全服务提供商之间的联络员，制定实施程序，以确保上上签电子签约平台符合国家关于知识产权相关法律和法规要求。

5 人员安全

5.1 尽职调查

在正式加入上上签的团队之前，上上签在国家法律法规允许的情况下，会验证应聘人员的个人教育背景与以往工作经历，同时执行内部与外部参考调查。背景调查的具体程度取决于应聘人员的岗位需求。

5.2 安全培训

让员工接受持续的安全培训是上上签信息安全策略的重要组成部分，上上签致力于为全体员工建立起充满活力及包容性的安全文化，并渗透至招聘流程、员工入职、在职员工培训以及日常业务运营之中。

5.3 运维安全

上上签员工入职后必须签署保密协议，保密协议对于 PII 有严格的保密要求，保密协议于员工在职时和离职后均有效。

可以接触和处理 PII 的全部为上上签正式员工。

记录客户 PII 信息的日志，只有极少数上上签员工并具备相应权限的管理员方可查看，而且这些日志只在系统中保留有限的时间。对数据的访问权限及级别由其实际工作职能与角色决定，且遵循最低权限与必要知悉原则以匹配其访问权限与责任划分，确保数据得到最大的安全保障。

工作人员对其他 PII 的访问请求需要遵循一套正式流程，对应人员必须根据上上签安全策略在审批系统中提交申请并获得批准，审批系统保留全部变更记录以便于进行审计。

6 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。依据数据安全生命周期，上上签从数据创建、存储、使用、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、真实性和不可抵赖。

6.1 数据传输

上上签电子签约平台采用 HTTPS/TLS 协议，最高 256 位密钥加密强度，实现全站加密，满足敏感数据加密传输的要求。

6.2 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可持续的信息保护，实现数据的灵活性、可靠性和可管理性，借助密钥管理中心（KMC）和加解密产品实现数据安全保护和控制，将安全技术嵌入至整个数据安全生命周期中，以保障数据安全。

6.3 密钥管理中心（KMC）

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，其主要负责密钥的存储、使用、分发和更新，并提供数据加解密及业务级别敏感数据保护。它的设计与管理符合行业合规性及审计要求，是上上签电子签约平台实现明文不落地策略的核心基础设施。

6.4 数据使用

上上签不会用真实用户 PII 进行测试，除非征得用户授权或者用户主动要求。

所有客户提交和数据处理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可能包含 PII，按要求，写入系统日志的 PII 必须加密或脱敏。

使用分包商处理 PII 时，上上签在合同和协议中明示保密要求，并对分包商安全标准的执行提出要求。

上上签根据数据的保护等级要求，对用户使用和应用展示进行了严格控制，禁止展示机密信息及未脱敏信息。

6.5 数据销毁

上上签电子签约平台部署在阿里金融云计算平台上，当客户删除数据时，遵

循严格的数据销毁标准。

7 应用安全

7.1 上上签 SDL

上上签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，提高开发人员的安全意识；
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估结果决定项目是否发布。

7.2 账户安全

上上签电子签约平台通过严格的身份认证和用户授权，以及周全的密码管理策略，确保用户账户安全。

8 运营安全

8.1 安全配置标准

线上服务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 Tomcat、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。

8.2 登录授权与访问控制

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 方式接入堡垒机才能访问生产服务器，VPN 连接强制采用双因子认证机制。

VPN 及堡垒机账号专人专用，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。

8.3 安全检测

上上签根据安全漏洞管理流程，通过商用及定制化工具、外部审计等手段主动扫描安全威胁。安全漏洞管理团队负责追踪并监督漏洞修复进展，直到确认漏洞已经得到修复。上上签亦与第三方安全服务提供商保持合作关系，不断提升及完善上上签的安全保障体系。

8.4 网络安全

上上签生产网络、测试网络和办公网络物理隔离，各网络之间的通信执行严格访问控制策略。在各自独立网络内部，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。

上上签电子签约平台部署在阿里金融云上，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。

上上签电子签约平台部署了可动态配置和扩展的 Web 应用防火墙，内置 SQL 注入、跨站攻击、远程代码执行等丰富的过滤规则集合，可在线调整和扩充防护规则。上上签电子签约平台受阿里云为金融客户提供高等级安全防护，并可随时启用数百 GB DDoS 防御。

9 物理和环境安全

上上签电子签约平台所在的阿里金融云，从物理层面完全独立于公有云，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。

10 灾难恢复与业务连续性

上上签电子签约平台采用同城双活，异地容灾架构，即两地三中心架构。

平台采用全负载均衡策略，所有应用服务均采用负载均衡，冗余部署无单点，并可进行弹性伸缩扩容。

上上签电子签约平台的数据库均采用 3 节点及以上的副本集群，数据库集群采用 MHA 高可用方案。

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、自动语音/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。故障快速恢复手段包括在线扩容、在线/停机迁移、自动切换以及降级恢复等。