



CM 证书管理解决方案

亚数信息科技有限公司（上海）有限公司

主目录

01

企业现状

02

企业证书管理痛点

03

证书管理需求

04

行业趋势

05

CM 解决方案

06

CM 功能

07

CM 优势

企业现状

当今，企业对安全的需求越来越高，SSL 证书大规模使用

证书申请过程复杂，周期长，限制了业务快速上线

错综复杂的证书部署，一台设备可能部署多张证书，一张证书可能部署在多台设备上

证书管理不善，证书过期，损失资金，信誉受损

持续不断的证书到期，人工更新繁琐且存在风险

企业内部员工对密钥保护没有安全意识

企业证书管理痛点

由于证书过期导致的停机

01

不知道他们拥有多少证书和密钥

02

企业担心他们无法在整个生命周期的各个阶段都确保密钥的安全

03

无法保护密钥和证书的安全性会使信任大打折扣（CA 厂商确认企业密钥泄露，有权吊销企业证书）

04

证书管理需求

安全性

私钥和证书的
安全存储

01

可见性

所有私钥和证书及
相关活动的审计

02

有效性

避免意外
失效或中断

03

一站式

证书全生命
周期管理服务

04

行业趋势

美国 NIST NCCoE 联合上下游安全厂商发布了 [Securing Web Transactions: Transport Layer Security \(TLS\) Server Certificate Management](#) 草案，NIST NCCoE 认识到保护组织客户端和服务端之间的Web事务和其他通信至关重要，该实践指南旨在指导企业更好地管理TLS服务器证书。

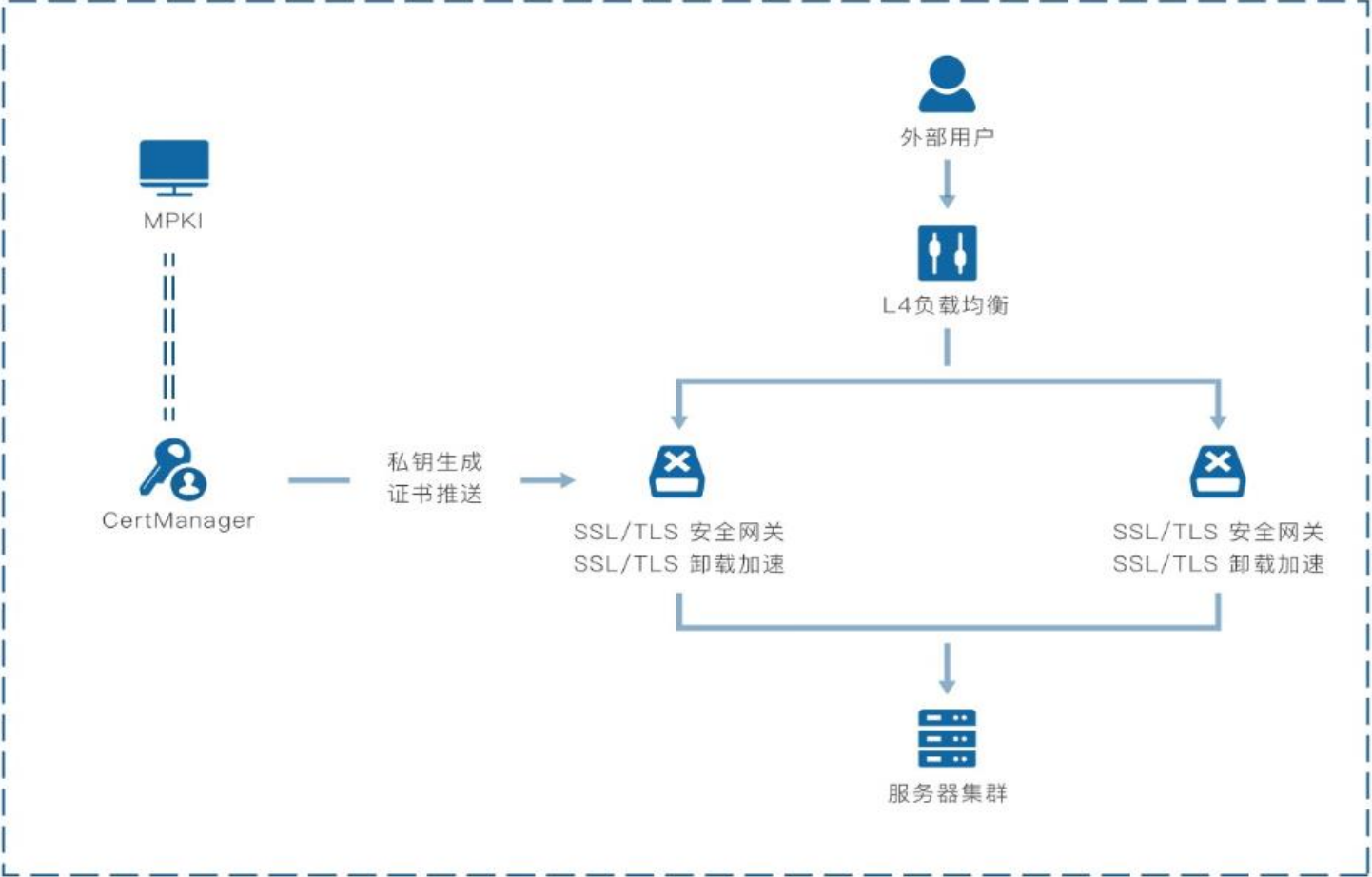


NIST TLS 证书管理最佳实践

| 证书管理策略 | CertManager |
|------------------------------|---------------|
| 集中的证书存储 | ✓ |
| 证书所有者管理 | ✓ |
| 可信的 CA | ✓ |
| 证书有效期 | ✓ |
| 密钥长度 | ✓ |
| 签名算法 | ✓ |
| Subject DN 和 SAN Contents 合规 | ✓ |
| 自动化 | ✓ |
| 证书请求审查批准 | ✓ |
| 私钥安全 | ✓ |
| 证书续期和密钥轮换 | ✓ |
| 主动证书更新 | ✓ |
| 加密敏捷性 | ✓ |
| 证书吊销 | ✓ |
| 持续监控 | ✓ |
| 记录证书管理相关的操作日志 | ✓ |
| TLS 流量监控 | ✓ |
| CAA | ✓ |
| 证书透明度 | 即将支持，利用CT的大数据 |
| 证书黑名单 | ✓ |

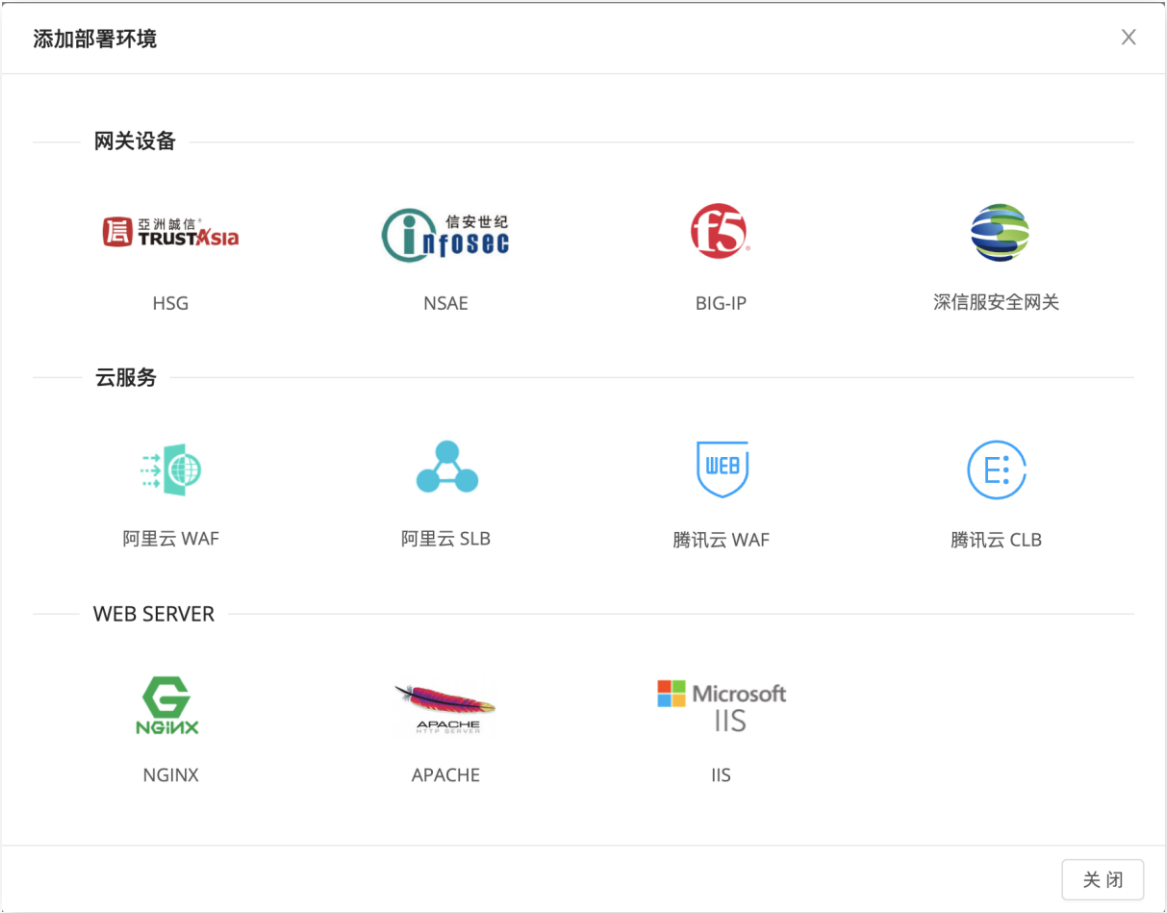
| 证书管理服务 | CertManager |
|-----------------|-------------|
| CAs | ✓ |
| 证书存储 | ✓ |
| 证书发现和导入 | ✓ |
| 证书管理界面 | ✓ |
| 证书自动申请和安装 | ✓ |
| RA/证书审核流程管理 | ✓ |
| 报表和分析 | ✓ |
| 被动解密支持 | ✓ |
| 持续监控 | ✓ |
| 教育和培训 | ✓ |
| 服务台支持 | ✓ |
| GMT 0024-2014 | ✓ |
| 《SSL VPN技术规范》检测 | ✓ |
| 国密SM2证书 | ✓ |

CertManager 解决方案



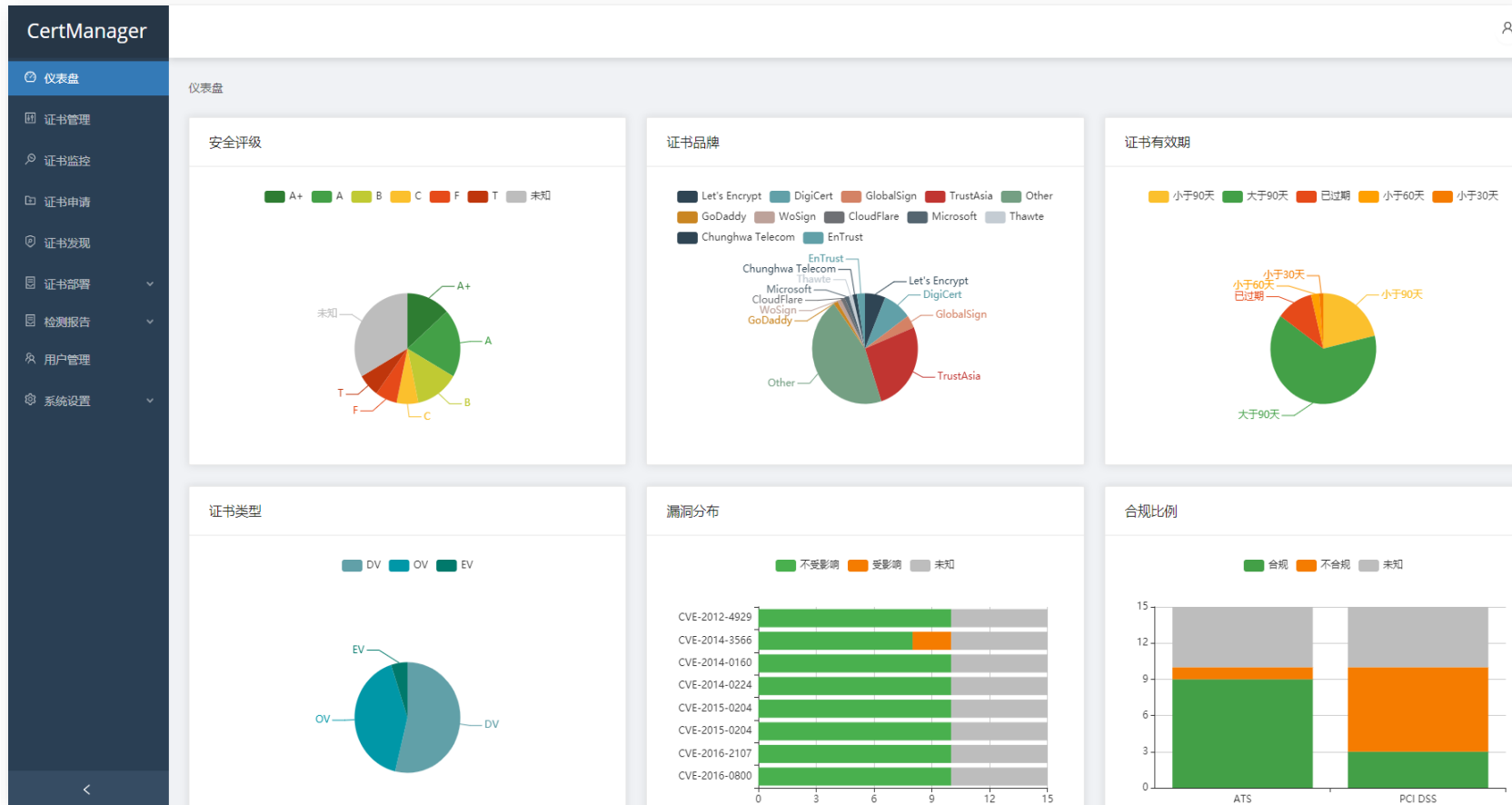
CertManager 证书部署

统一管理网关设备、云服务、WEB SERVERS 的证书部署和更新，并提供 OPENAPI 与运维系统对接。



CertManager 功能

CM 为证书的全生命周期提供管理服务：证书申请、部署、检测、发现、监控、管理、告警、更新和证书品牌切换



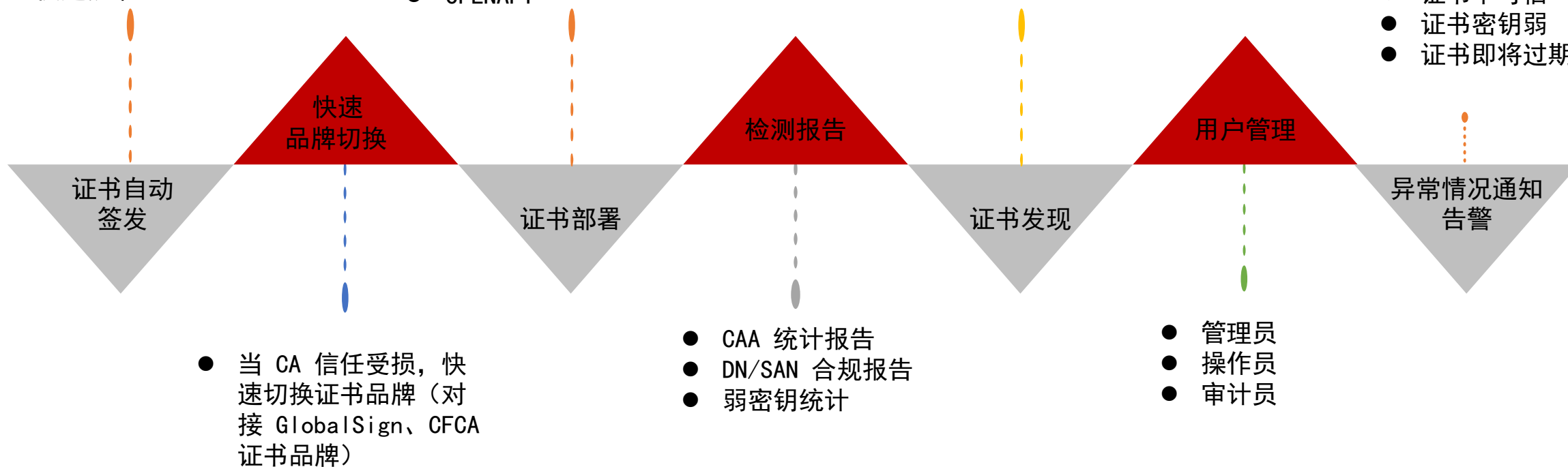
CertManager 功能

- 对接 MPKI 实现证书审核流程管理，实现 OV/EV 证书自动签发、快速获取

- 网关设备：HSG/信安/F5...
- 云服务：WAF/SLB/CDN...
- WEB SERVERS：Nginx/Apache/IIS
- OPENAPI

- 发现企业网段证书，在 CertManager 中管理发现的证书

- 连接异常
- 证书已过期
- 证书已吊销
- 证书黑名单
- 证书域名不匹配
- 证书不可信
- 证书密钥弱
- 证书即将过期



CertManager 优势



Thanks

亞數信息科技（上海）有限公司



<https://www.trustasia.com>