1.数字标牌简介

板卡厂商为其上运行的业务提供了两项特色安全功能，有需要的业务可以通过板卡的SDK 和相关工具/库进行开发，实现业务的安全增强。特色安全功能包括安全显示和态势感知两项，其中态势感知技术复杂度较高，前端业务需要对接安全库整合。

2.安全显示

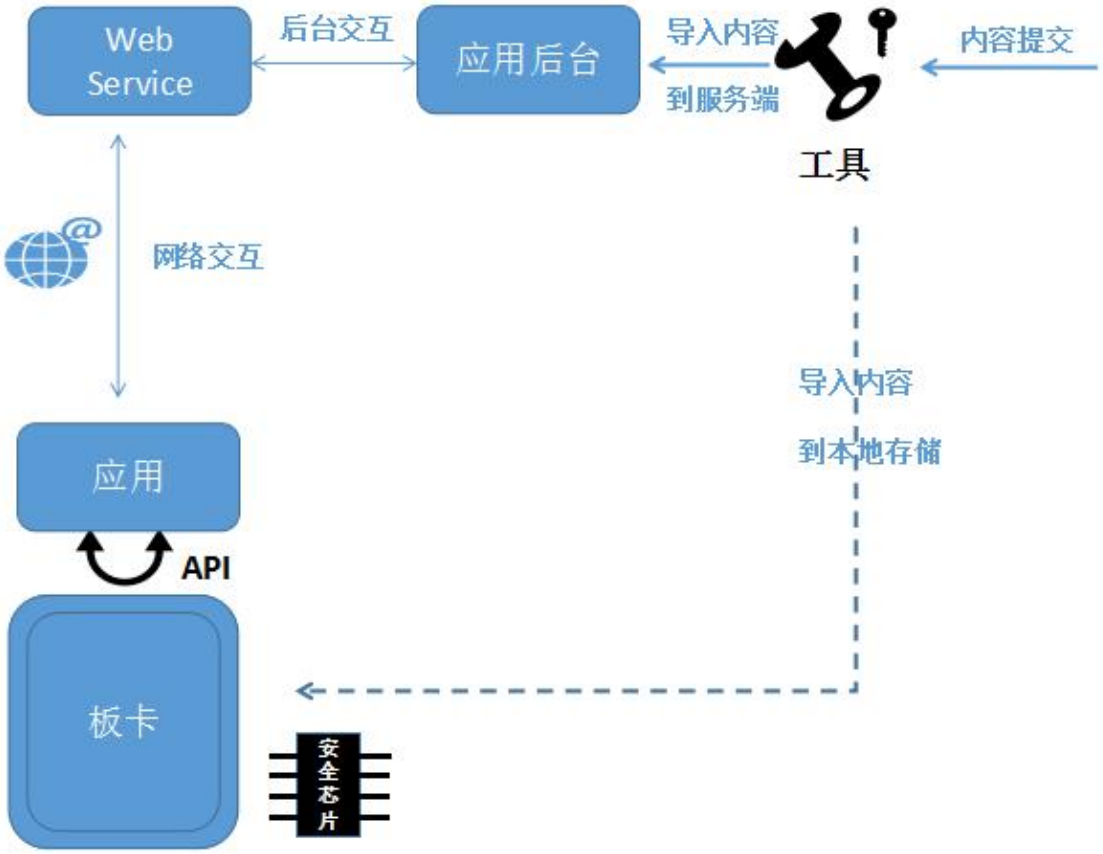
安全显示主要是针对服务端安全保护不足问题。目前商显行业主要是 C/S 模型，传统的安全假设都是基于服务端是安全的这个前提，大多数终端系统管理和功能都依赖于服务器，当服务器被攻击，成片的终端都将沦陷。事实上，目前针对商显行业的攻击已经是客观事实，在第三方安全反馈平台乌云上通过“数字标牌”“广告机”“商业显示屏幕”等关键字搜索，可搜出一系列服务器安全事件，可对商显服务器实现任意终端控制，内容任意播放，服务端信息修改，机密数据库信息获取等方法。尤其是目前服务有云化趋势，当所有的终端都联网且由唯一的云服务器进行控制时，云服务器业务的安全就显得尤其重要。安全显示方案顺应“服务云端化”趋势，提出了安全显示方案，实现“内容线下可控”效果，这样内容的显示将由最终客户自身控制，即使服务器或个别终端被攻击，影响都将比较小。

方案的简单结构如下图：

- 最终用户端到终端方案，板卡厂商通过线下证书发放和用户密钥发放实现商显功能控制。
- 用户使用在线或离线工具，输入强认证密钥，对内容进行发布。强认证密钥被安装到浏览器上（体验好）或者 USB key（安全性好）上，需要输入口令。只有持有该密钥且知道口令的人员才有能力对内容资源进行发布，实现密钥控制内容。用户密钥和操作的离线性保证了针对在线服务器的攻击效果有限。
- 在线服务器可以减少被攻击的危害，在线服务器只是内容发布和编辑的一个通道。减少服务器安全的运营成本和风险。在线服务器可通过与板卡厂商分成方式获取收益。

- 终端对内容的认证基于安全芯片的强认证方式，保证只有持有私钥的用户发布的内容才可以在终端显示和执行。

目前，开发套件只支持对文件（音视频，图片，文件）的内容安全显示，可通过与业务方定制的方式实现更细，如指令，流媒体等的安全显示功能。安全显示功能默认集成到板卡厂商系统中，需要证书才可以激活。



3.态势感知

态势感知，是板卡厂商为了保护承载业务的安全而设计的认证协议，默认集成到板卡厂商 SDK 中，该协议使得板卡厂商的终端系统有能力向应用服务端如实报告当前终端的状态，业务服务商可以依据此报告进行安全判断，攻击告警，以及状态利用。态势感知基于安全芯片，是基于攻防对抗实践下的通用防御方法。具有以下安全效果：

- 报告当前的 APK 身份：业务服务端可防止应用被篡改；防止应用被重打包调试；只允许许可应用连接服务端后台。
- 报告当前的终端身份：身份与安全芯片绑定唯一，应用服务端可对终端身份进行业务信息绑定或监视，而无需担心终端身份篡改和克隆

- 报告当前的连接信息：若业务系统已部署 TLS 服务，则该机制可防止 TLS 攻击和其他中间人攻击，保护通信安全。TLS 的攻击可参考我们整理的《SSL/TLS 安全最佳实践》。
- 报告当前系统的时间：防止针对时间类的攻击实践，如重放攻击。

为了业务开发的便利性，我们整合了协议的两侧，SDK 和服务端安全库，并各提供一个接口供业务者使用，应用开发者也只需要调用 SDK 的一个 API 即可实现该协议内容，保护业务安全。

该安全协议相对于可信计算的完整性报告协议更加贴近应用，实践性更强。相对于 FIDO 类的承载 TLS 之上的 Token binding 协议功能更丰富，可部署性更强，更适合商业显示行业的业务保护。