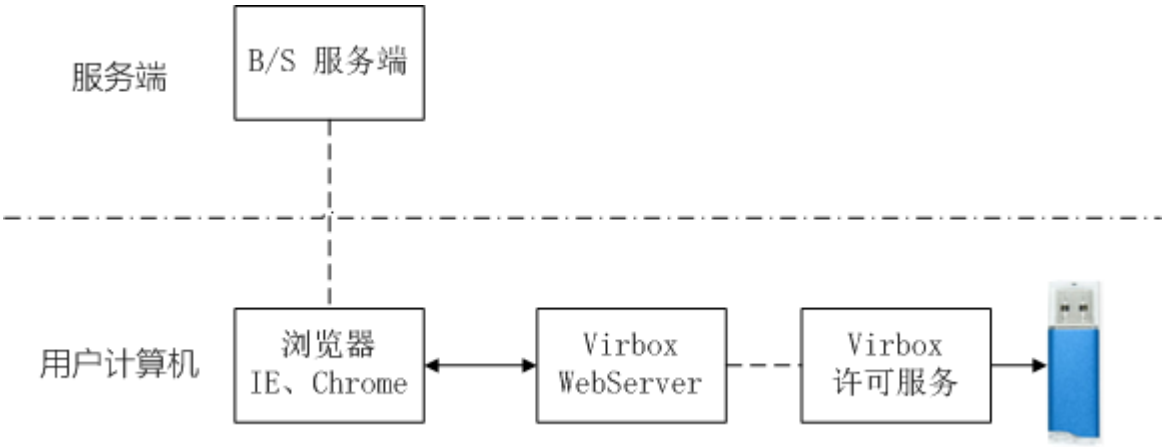
精锐5身份认证

一、产品简介

深思精锐5身份认证“组件”（Virbox WebServer），是一个运行在用户计算机的本地 Web 服务（不需要连接互联网），提供 Web 接口访问精锐5加密锁，B/S 架构的 Web
应用只需在网页代码中嵌入调用接口（跨域访问）的代码即可访问加密锁、获取加密锁信息，实现身份认证功能。

不同于 COM 组件访问加密锁的方式，本产品提供的 Web 接口可用
JavaScript 调用，开发者不需要学习额外的技能即可完成功能集成，兼容市面主流的浏览器（IE、Chrome、360、Firefox 等）。

二、产品架构



- B/S 服务端：开发者 B/S 架构应用程序（网站）服务端，向用户提供服务。
- 浏览器（客户端）：用户通过浏览器访问指定域名的网站，包括主流的浏览器：IE、Chrome、360安全浏览器、360极速浏览器、猎豹浏览器等。

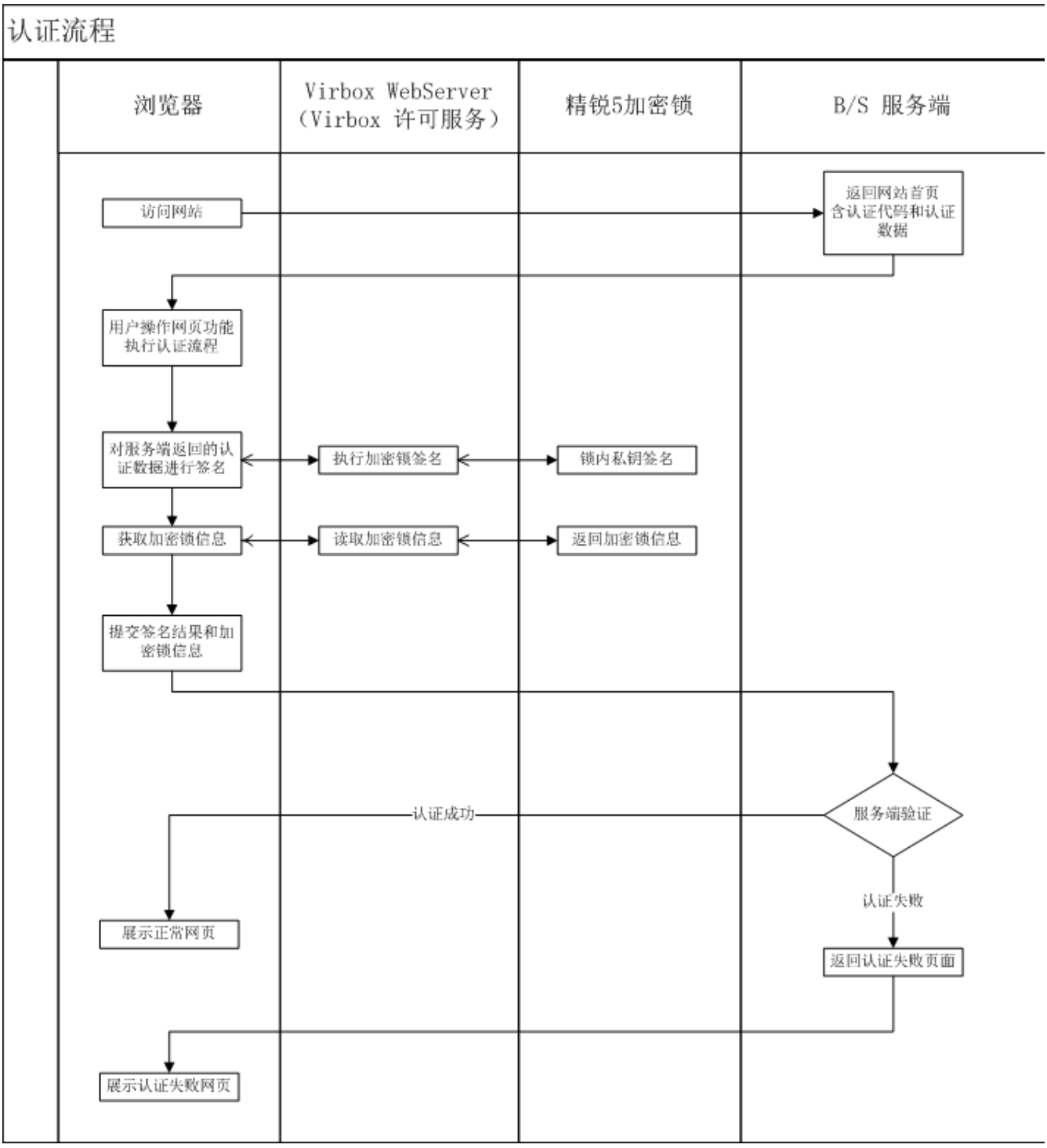
- Virbox WebServer：身份认证核心组件，提供访问加密锁的 Web 接口。
- Virbox 许可服务：访问深思精锐5加密锁、云锁、软锁，提供抽象访问锁（含硬件锁、云锁、软锁）接口。
- 精锐5加密锁：身份认证的物理介质，锁内存有唯一的设备私钥，提供不可伪造的设备签名。每一把精锐5加密锁在出厂前由锁内安全芯片生成全球唯一密钥和证书，硬件具有不可复制、密钥不可导出的安全特性，让伪造认证变得更加困难。

注意：Virbox WebServer 无法直接与精锐5加密锁通信，需要通过 Virbox 许可服务间接访问加密锁，所以在软件运行环境部署时需要安装 Virbox WebServer 和 Virbox 用户工具（含 Virbox 许可服务，可以通过深思官网下载最新版本）。

三、认证流程

1. 用户通过浏览器访问网站。
2. B/S 服务端返回包含认证数据和正版认证代码的网页给浏览器。
3. 网页被浏览器完全加载后主动（或被动）执行认证流程。
    1. 调用 Virbox WebServer 的正版认证接口，对服务端生成的认证数据使用精锐5内置设备私钥签名。
    2. 网页将接口返回的加密锁信息（唯一芯片号、加密锁设备证书链）、认证数据和签名结果返回给 B/S 服务端。
    3. B/S 服务端验证加密锁的合法性。
    4. B/S 服务端使用加密锁证书验证签名结果的合法性。
    5. B/S 服务端可根据认证结果判定是否允许用户进行后续操作。

认证流程图如下图所示：



四、功能集成

开发者参照示例（web_server_test.html）将调用 Virbox WebServer 的 JS
代码集成到业务功能的网页中，并根据业务流程在适当的情况下触发相关接口调用即可。

五、环境部署

安装组件

在用户计算机需要安装以下组件

1. Virbox 用户工具，开发者可以通过深思官网下载最新版本。

2. 身份认证组件（Virbox WebServer），联系深思获取最新发布版本。

部署验证

1. 在用户计算机插入精锐5硬件锁
2. 使用浏览器打开测试用例（web_server_test.html），点击 “查询 WebServer 版本号” ，返回当前认证服务版本号，如果未返回结果或提示错误，请根据常见问题进行排查。

六、兼容浏览器

浏览器	是否支持	备注
IE	支持	支持版本：IE8、IE9、IE10、IE11
Edge	支持	
Chrome	支持	
QQ浏览器	支持	
Firefox	支持	HTTPS 需要将证书加入信任列表
360	支持	360极速浏览器、360安全浏览器

七、常见问题

1.HTTPS 和 HTTP 协议选择

Virbox WebServer的协议必须要与 B/S 服务端保持一致，如果浏览器访问域名使用 HTTPS 协议，在返回的页面中集成调用 Virbox WebServer 接口，必须保证运行的 Virbox WebServer 也是 HTTPS，否则会在页面代码中集成的 JS 代码调用接口会返回失败；反之，如果浏览器访问域名使用 HTTP 协议，用户端部署的 Virbox WebServer 也需要设置为 HTTP 协议。

Virbox WebServer 目前支持 HTTPS 和 HTTP 两种协议。当前版本服务运行期间只能选择一种协议，服务默认配置为 HTTPS，开发者可以通过修改安装目录下的配置文件（websrv_config.ini），将 protocol=HTTPS 改为 protocol=HTTP，保存配置文件，并重启 “VirboxWebServer” ，配置即刻生效。

备注：Virbox WebServer 默认安装目录 C:\Program Files (x86)\senseshield\ss_web

2.选择 HTTPS 协议时证书是否能够兼容主流的浏览器客户端

Virbox WebServer 使用 HTTPS 协议自签名证书，在安装时将根证书添加至 Windows 证书管理 “受信任的根证书颁发机构” ，所有使用 Windows 证书管理的浏览器（IE、Edge、Chrome、360）都能够正常访问 Web 接口，不会提示 “错误的证书” 。

Firefox（火狐浏览器） 并未使用 Windows 证书管理，当前版本需要用户手动访问 Virbox WebServer 提供 Web 接口，在提示 “错误证书” 时将证书添加至信任列表即可，否则在网页中调用 JS 代码接口跨域访问时会返回失败。

3.Virbox WebServer 是否支持跨主机访问

Virbox WebServer 设置 HTTP 协议，支持跨主机使用 IP 访问。

Virbox WebServer 设置 HTTPS 协议，只支持使用 localhost 域名在本机访问 Web 接口，不支持其他域名和跨主机使用 IP 访问。