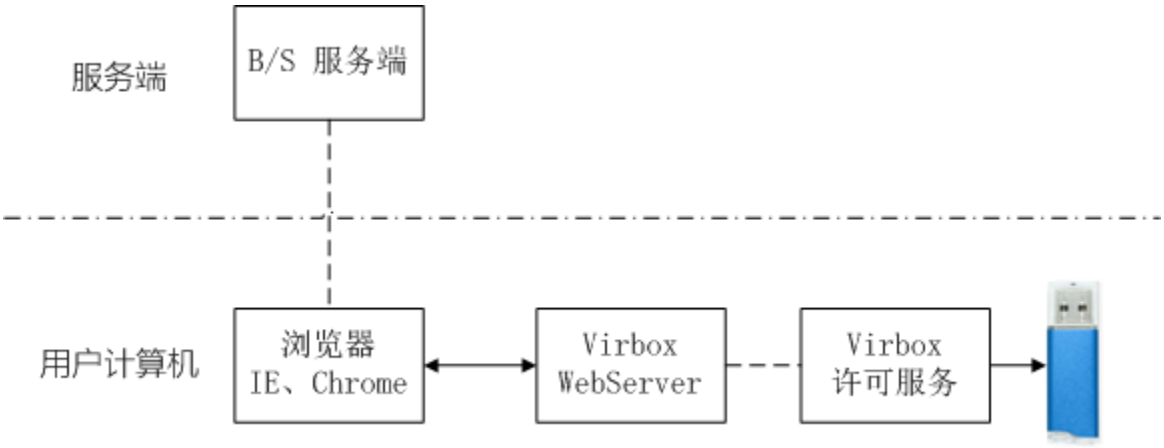
精锐5身份认证

一、产品简介

深盾精锐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（**不需要访问互联网**），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



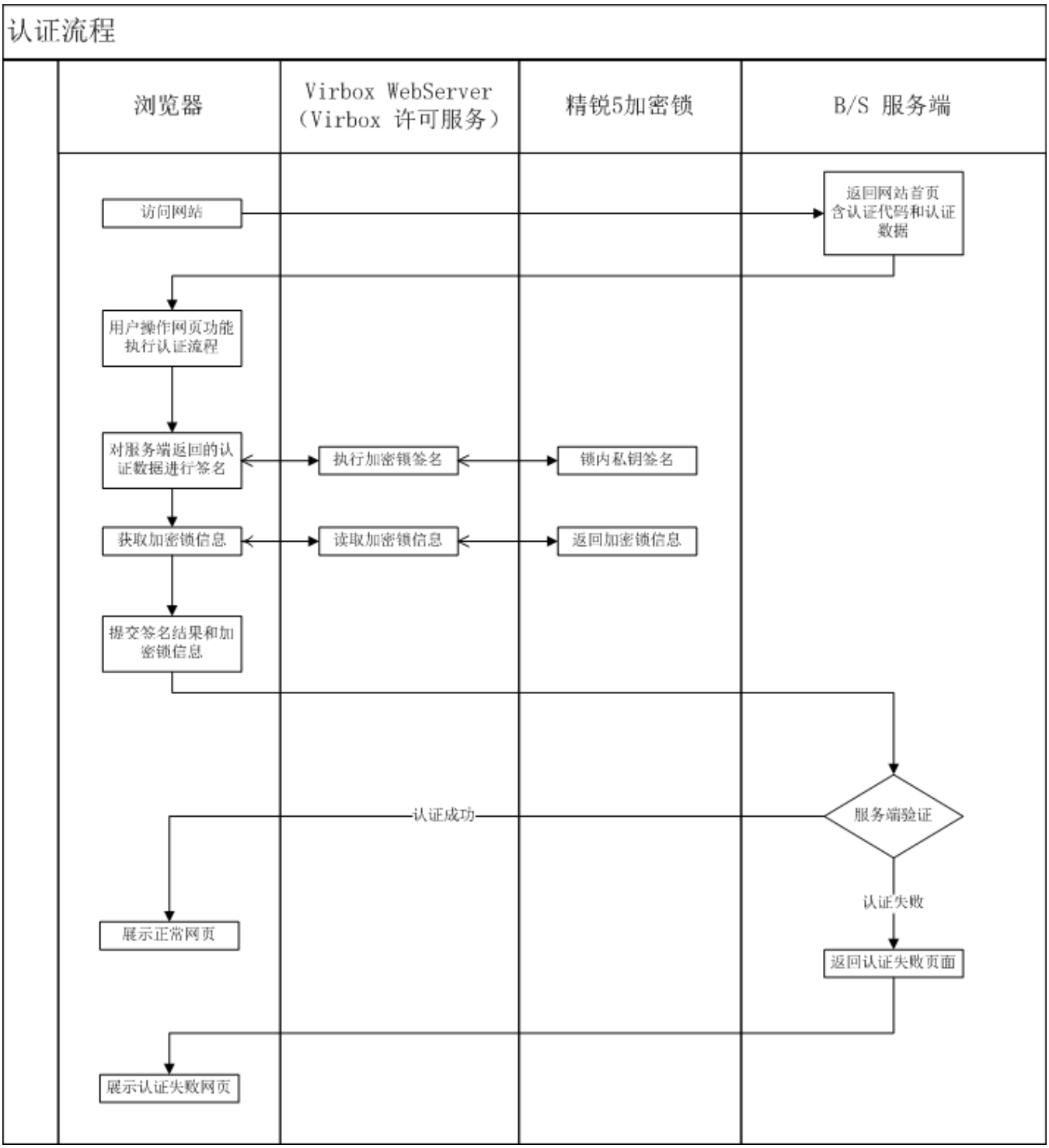
- **B/S 服务端**：开发者 B/S 架构应用程序（网站）服务端，向用户提供服务。
- **浏览器（客户端）**：用户通过浏览器访问指定域名的网站，包括主流的浏览器：IE、Chrome、360安全浏览器、360极速浏览器、猎豹浏览器等。
- **Virbox WebServer**：身份认证核心组件，提供访问加密锁的 Web 接口。
- **Virbox 许可服务**：访问深盾精锐5加密锁、云锁、软锁，提供抽象访问锁（含硬件锁、云锁、软锁）接口。
- **精锐5加密锁**：身份认证的物理介质，锁内存有唯一的设备私钥，提供不可伪造的设备签名。每一把精锐5加密锁在出厂前由锁内安全芯片生成全球唯一密钥和证书，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 用户工具（身份认证）定制版，可以通过联系深盾的技术人员获取最新版本。

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。
    a. 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。
    b. 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。
    c. B/S 服务端验证加密锁的合法性。
    d. B/S 服务端使用加密锁证书验证签名结果的合法性。
    e. 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、加密方案

精锐5 身份认证的加密方案以加密锁设备唯一的私钥不可篡改、不可克隆为基础，使用加密锁私钥签名、加密锁公钥验签的方式进行验证。

4.1 基础方案

前提条件

1. B/S 服务端已保存发售的加密锁信息（外壳号、芯片号、设备证书）

1.B/S 服务端

当某一台客户端通过浏览器网页访问 B/S 服务端时，服务端首先校验客户端的合法性。

1. 服务端记录客户端会话GUID
2. 根据会话GUID + 随机数 + 当前的UTC时间组合生成验证数据，使用 Hash 算法计算验证数据的哈希结果，用于验证客户端的合法性。
3. 服务端将校验数据返回给客户端，等待客户端使用本地的加密锁的私钥对验证数据的 Hash 结果进行签名，并将加密锁信息和验证签名结果返回给服务端。
4. 服务端校验加密锁合法性。服务端检查客户端上传的加密锁信息（外壳号、芯片号）与数据库内容对比是否一致，验证加密锁的合法性。
5. 服务端校验验证数据的合法性。服务端在确认加密锁合法后，使用加密锁的设备公钥验签私钥签名的合法性，只有当签名结果与验证数据完全一致时，表示当前客户端的加密锁有效。

2.客户端

用户通过客户端的浏览器网页访问 B/S 服务端某些业务功能，当 B/S 服务端需要验证客户端的合法性时，客户端需要将服务端返回的数据交给本地的精锐5硬件锁进行签名，然后将签名结果返回给服务端进行验证。

1. 客户端通过 Virbox WebServer 接口获取加密锁信息（外壳号、芯片号、设备证书）。
2. 客户端通过 Virbox WebServer 接口对服务端返回的认证数据进行加密锁私钥签名。
3. 客户端将加密锁信息和加密锁私钥签名后的数据一起发给服务端进行校验审核。

4.2 双重验证方案

在实现基础方案的基础上，B/S 服务端可以同时采用 **用户名、密码** 登录认证的方式，对客户端用户进行账号认证，与硬件加密锁认证结合实现双重认证。

当客户端需要进行某些特殊操作时，进行加密锁认证，认证通过后允许客户端执行业务功能。

五、安全性

精锐5身份认证的安全性由加密方案和精锐5硬件加密锁硬件两方面保证。

从上文中可以了解到 Virbox 身份认证，由服务端针对每一个客户端生成唯一、不可重放的认证数据，再通过网络交给客户端，客户端使用加密锁私钥对认证数据进行签名，最后客户端再将认证提交给 B/S 服务端在服务端进行认证检查。

认证数据的生成和签名结果校验在服务端完成，客户端使用加密锁私钥签名后的认证数据具有不可伪造的特性，无论 B/S 服务端与客户端通信使用 HTTPS 或 HTTP 协议，传输数据是明文或者密文，都不影响认证数据的安全性。

开发者只需保证 B/S 服务端生成的认证数据以下两个特点：

1. **唯一性**。每个客户端应该具有唯一的认证数据。
2. **抗重放**。认证数据只有单次有效，过期作废，验证完毕即刻清除，防止数据被重复利用。

六、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。

深盾向开发者提供 Virbox 用户工具（身份认证）定制版安装包（内部集成 Virbox WebServer 功能），以及 Virbox WebServer 接口文档、示例代码（C#、Java）。

开发者需要参照深盾提供的示例程序完成以下工作：

1. B/S 服务端生成认证数据，调用标准密码学接口实现公钥验签功能。
2. B/S 服务端根据加密方案提供数据存储和校验逻辑。
    a. 基本方案。
        i. 服务端需要记录正式发布的加密锁信息
        ii. 客户端调用 Virbox WebServer 接口获取加密锁信息，提交给服务端。
        iii. 服务端实现检查客户端加密锁数据有效性检查功能。
    b. 双重验证方案。
        i. 服务端需要实现账号密码登录功能和相关数据存储。

七、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（身份认证）定制版，开发者联系深盾销售经理或技术人员获取最新版本。

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。

八、兼容浏览器

操作系统	CPU	协议	浏览器	支持情况	备注
Windows	x86	HTTP	Edge	✅	
		HTTPS		✅	109.0.1518.78 版本有不安全访问警告
		HTTP	Chrome	✅	
		HTTPS		✅	81.0.4044.122 及以上版本有不安全访问警告
		HTTP		✅	
		HTTPS		✅	5.1.3.22 及以上版本有不安全访问警告
		HTTP	Firefox	✅	
		HTTPS		✅	
		HTTP	IE	✅	
		HTTPS		✅	108.0.1462.54 及以上版本有不安全访问警告
	ARM	暂不支持	暂不支持	⚠️	暂不支持
Linux	x86	HTTP	Firefox	✅	
		HTTPS		✅	59.0.2 版本有不安全访问警告
	mips	HTTP	Firefox	✅	
		HTTPS		⚠️	60.10.0 及以上版本暂不支持
	ARM	暂不支持	暂不支持	⚠️	暂不支持
macOS	M1	HTTP	Safari	✅	
		HTTPS		⚠️	15.6.1 及以上版本暂不支持
		HTTP	Chrome	✅	
		HTTPS		⚠️	108.0.5359.124 及以上版本暂不支持
	x86	HTTP	Safari	✅	
		HTTPS		⚠️	部分支持，10.13.6 及以下支持，以上暂不支持。

九、服务配置

Virbox 用户工具（身份认证） 2.5.0.59543 及以上版本支持配置文件存放路径如下：

操作系统	配置文件
Windows	C:\ProgramData\senseshield\ss_service\ss_config.xml
Linux	/opt/senseshield/etc/ss_service/ss_config.xml
macOS	/Library/SCP/etc/ss_service/ss_config.xml

```
<WEB_SERVER>
    <HTTP Enable="1">
        <HTTP_PORT>9080</HTTP_PORT>
    </HTTP>
    <HTTPS Enable="1">
        <HTTPS_PORT>9081</HTTPS_PORT>
    </HTTPS>
</WEB_SERVER>
```

> *Enable 表示是否启用协议，0 不启用；1 启用；*
>
> *HTTP_PORT 与 HTTPS_PORT 表示配置协议的端口号；*

注意：配置参数修改后，需要重启服务才能生效。

十、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。开发者可根据业务需要只启用一种协议，可参考 “九、服务配置” 内容修改配置文件，保存配置后重启服务使配置生效。

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。

4.HTTPS 浏览器首次请求等待时间长

Virbox WebServer 设置 HTTPS 协议时，无论通过浏览器直接输入接口地址，或者通过 JS 调用接口，首次需要建立 HTTPS 通道，校验证书，造成请求处理时间较长，请耐心等待，但再次请求时耗时恢复与接口实际用时相当的时间。

更换浏览器首次访问 Virbox WebServer 接口都会存在访问慢的情况。
建议：1.开发者可在网页中明确标识功能仍在后台运行，请用户稍后的提示信息；2.在不考虑安全性的情况下，可改用 HTTP 协议，则不存在首次请求返回慢问题。