超级狗身份认证使用指南

本文档描述了如何使用超级狗用于身份认证及其示例等相关信息。

产品简介

超级狗双因素身份认证可以使网络访问者经过双重认证才能获得网络访问授权。授权的访问者必须持有超级狗并且知道其口令。访问者需要把超级狗插入 USB 接口中，并且输入正确的口令，以证实自己的身份。如果身份认证服务器不能识别访问者的身份，网络访问将被拒绝。

超级狗双因素身份认证向用户提供了比传统用户名口令方式更安全的网络身份认证机制。

工作原理

超级狗利用内置算法采用查询响应的方式对访问者身份进行验证和确认。

当身份认证服务器发给超级狗查询值时，超级狗使用内置算法计算出匹配的响应值，并通过网络发送给服务器。查询值是随机的，因此拦截超级狗与服务器的通讯数据并不能帮助破解。此方式与输入口令验证方式相比更安全，更难于破解，因为口令并没有在网络上传输。

超级狗采用单向不可逆哈希算法计算响应值。超级狗内置了智能卡芯片，能够有效地防止硬件复制或伪造。超强的硬件保护，使算法不可被非法读取，从而保障了安全性。

不同开发商购买的超级狗内置的算法因子不同，可以有效防止其他人购买超级狗伪装成合法用户。

测试环境

服务器端支持 JSP、ASP.NET 和 PHP，客户端支持主流浏览器。目前已测试的平台如下：

1) Windows XP: IE8, Firefox, Google Chrome

2) Windows 7: IE8, IE9, IE10, Firefox, Google Chrome

3) Windows 8: IE10, Firefox, Google Chrome

4) Windows 8.1: IE11, Firefox, Google Chrome

5) Windows 10: IE11, Firefox, Google Chrome

目录

第一章 软件包内容

此软件包包含如下文件：

文件名	版本	描述
Tools\AuthCodeGenerator.exe	2.3.1.52711	认证代码生成工具，用来为您的认证系统生成认证代码
Tools\AuthTool.exe	2.3.0.1	认证工具，管理员可以使用此工具： 1. 修改管理员口令 2. 设置认证因子 3. 解锁并设置新的用户口令 4. 设置用户名 5. 修改用户数据
Tools\Source\AuthTool	2.3.0.1	认证工具的源文件
WebServer\dog_auth_srv.dll *WebServer\dog_auth_srv_x64.dll*	2.3.1.52712	服务器端需要用到的认证用户的动态链接库
WebServer\dog_auth_srv_php.dll	2.3.0.1	PHP 工程的服务器端需要用到的认证用户的 PHP 扩展组件
WebServer\JSP\Authentication	2.3.0.1	超级狗 Java Web 认证示例程序
WebServer\ASP.NET\Authentication	2.3.0.1	超级狗 ASP.NET 认证示例程序
WebServer\PHP\Authentication	2.3.0.1	超级狗 PHP 认证示例程序
WebServer\PHP\Source\dog_auth_srv_php	2.3.0.1	超级狗服务器端 PHP 扩展 DLL 的源文件
BrowserPlugin\DogAuthPluginSetup.exe	2.3.0.1	超级狗认证控件安装包。用于安装 客户端需要用到的支持 IE，Chrome 和 Firefox 浏览器的控件
SuperDog Authentication Sample Readme.*pdf*	无	本文档

第二章 使用示例工程

Java Web 工程（Tomcat）

使用需求

Java Web 服务器端需安装 Apache Tomcat 6.0 和 JRE 1.6 或 JRE1.7。

由于 JRE1.8 与 JDK1.8 不再包含 JDBC-ODBC Bridge，示例工程的 access 数据库将无法正常使用，所以示例工程不能使用 JRE1.8 与 JDK1.8。

客户端需安装 32-bit IE 8.0 或者以上版本，32-bit Chrome 或者 Firefox 浏览器。

如果客户端使用 IE 浏览器，客户端既可以通过网页提示下载并安装客户端控件，也可以运行 DogAuthPluginSetup.exe 安装控件；如果客户端使用 Chrome 或者 Firefox 浏览器，请运行 DogAuthPluginSetup.exe 安装控件。

编译/使用 Java Web 示例程序

Java Web 示例工程使用超级狗试用件演示。请按照如下步骤使用此软件包：

1. 在服务器端，根据您安装的 JRE 的版本是否为 64 位，选择将文件 dog_auth_srv.dll 或 dog_auth_srv_x64.dll 放到 Tomcat 安装目录的 bin 目录下。如：C:\Program Files\Apache Software Foundation\Tomcat 6.0\bin。
2. 在客户端打开 32-bit 浏览器，输入网址

   http://[服务器 IP]:8080/Authentication/Login.jsp 即可。

最终用户第一次使用请点击进入注册页面，输入用户名和用户口令进行注册。

用户名和用户口令将被写入超级狗硬件；同时，用户名和超级狗 ID 将被写入服务器端数据库中。

用户可以对用户口令进行更改。

部署您自己的 Java Web 工程

实际的工程将绑定您的开发商 ID 和认证代码。请参照如下步骤：

1. 请插入您的开发狗，使用认证代码生成工具生成认证代码，文件名默认为：auth_code.xml。文件内容包含您的开发商 ID 和认证代码。请将 auth_code.xml 拷贝至服务器端工程的目录 WEB-INF 中。
2. 使用超级狗认证初始化工具（AuthTool.exe）修改超级狗的管理员口令（SO PIN，默认为：“abcdefgh”）和认证因子（默认为：“00000000”），设置用户口令（USER PIN，默认为：“12345678”）与用户信息。也可通过 web 工程的用户注册页面让用户自行注册，设置用户名和用户口令。如果您修改了认证因子，请同时修改服务器端 WEB-INF 目录中的配置文件：auth_factor.xml。为了提高安全性，建议您修改默认的认证因子。
3. 在服务器端，将您的 web 工程按照示例工程修改后放到 Tomcat 安装目录的 webapps 文件夹下。
4. 在客户端打开 32-bit 浏览器，输入您的 web 工程的登录网址即可。

注意

1. 当您使用 64 位的 JRE 部署工程，并使用 Microsoft Access 作为数据库时，您可能会遇到如下异常信息：“java.sql.SQLException: [Microsoft][ODBC Driver Manager] Data source name not found and no default driver specified”。这是由于您没有安装 Microsoft Access Database Engine（64-bit）的原因。您可以采取如下措施：

    a. 采用其他数据库。本工程采取 Microsoft Access 作为演示数据库。在实际应用中，建议采用更常用的商业数据库。

    b. 采用 32 位的 JRE 部署本工程。

    c. 如果您继续使用 64 位的 JRE 与 Microsoft Access，您需要先确认卸载 32 位的 ODBC（可能需要卸载 Office），然后下载 64 位的 Microsoft Access Database Engine 2010 Redistributable（http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=13255）并安装。

ASP.NET 工程

使用需求

ASP.NET 服务器端需安装 Microsoft .NET Framework 4.0 和 IIS 7。

客户端需安装 32-bit IE 8.0 或者以上版本，32-bit Chrome 或者 Firefox 浏览器。

如果客户端使用 IE 浏览器，客户端既可以通过网页提示下载并安装客户端控件，也可以运行 DogAuthPluginSetup.exe 安装控件；如果客户端使用 Chrome 或者 Firefox 浏览器，请运行 DogAuthPluginSetup.exe 安装控件。

编译/使用 ASP.NET 示例程序

ASP.NET 示例工程使用超级狗试用件演示。请按照如下步骤使用此软件包：

1. 在服务器端，根据您的系统是否为 64 位，选择将文件 dog_auth_srv.dll 放到：（系统盘符:）\Windows\SysWOW64 或（系统盘符:）\Windows\System32 目录下。例如：C:\Windows\SysWOW64。（目前 64 位系统暂不支持调用 64 位动态库：dog_auth_srv_x64.dll）。
2. 使用 Visual Studio 2010 编译本工程并运行。

最终用户第一次使用请点击进入注册页面，输入用户名和用户口令进行注册。

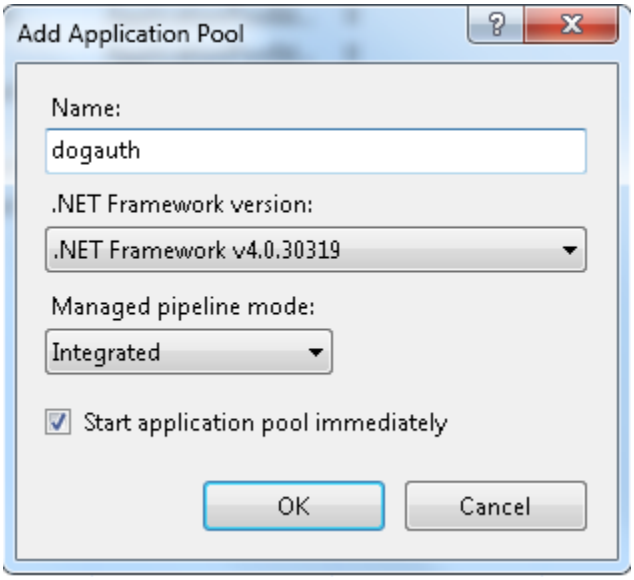
用户名和用户口令将被写入超级狗硬件；同时，用户名和超级狗 ID 将被写入服务器端数据库中。

用户可以对用户口令进行更改。

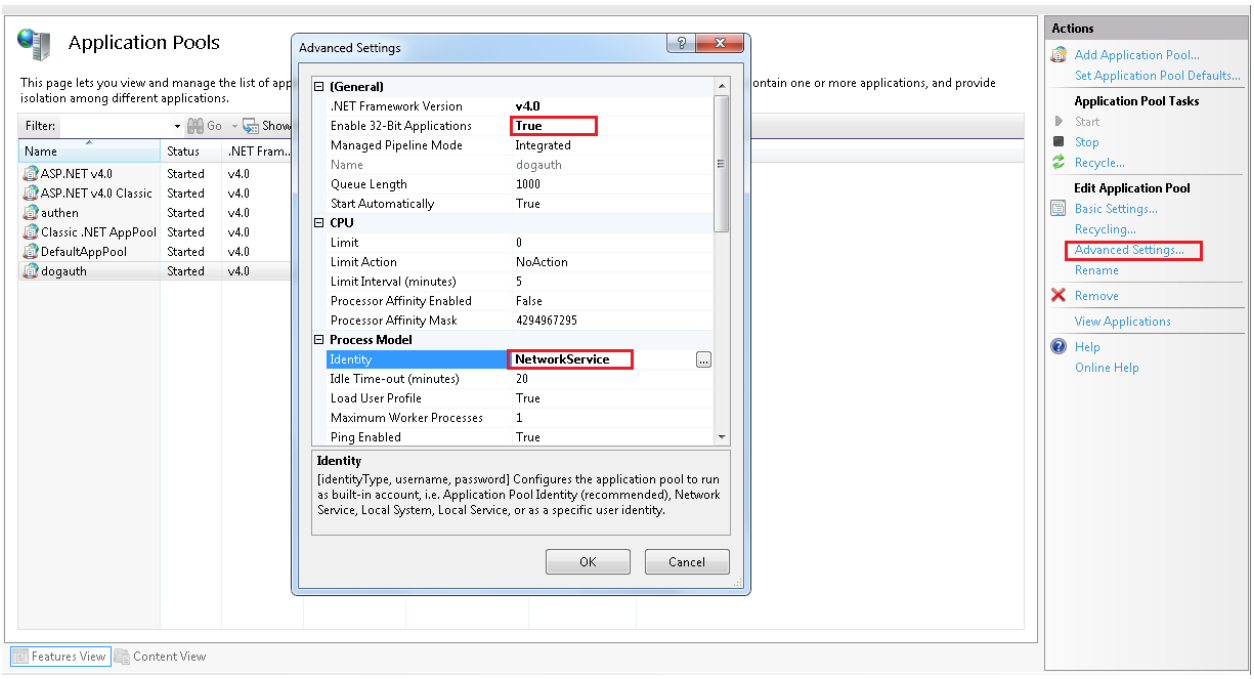
部署您自己的 ASP.NET 工程

实际的工程将绑定您的开发商 ID 和认证代码。工程部署示范采用 Windows 7 系统与 IIS 7，请参照如下步骤：

1. 请插入您的开发狗，使用认证代码生成工具生成认证代码，文件名默认为：auth_code.xml。文件内容包含您的开发商 ID 和认证代码。请将 auth_code.xml 拷贝至服务器端工程的目录 serverdata 中。
2. 使用超级狗认证初始化工具（AuthTool.exe）修改超级狗的管理员口令（SO PIN，默认为：“abcdefgh”）和认证因子（默认为：“00000000”），设置用户口令（USER PIN，默认为：“12345678”）与用户信息。也可通过 web 工程的用户注册页面让用户自行注册修改用户口令与用户名。如果您修改了认证因子，请同时修改服务器端 serverdata 目录中的配置文件：auth_factor.xml。为了提高安全性，建议您修改默认的认证因子。
3. 在服务器端，将您的 web 工程按照示例工程修改后放到一个目录中。例如：D:\Authentication。
4. 在服务器端安装 IIS 后，在控制面板中选择：Administrative Tools->Internet Information Services (IIS) Manager，双击打开。
5. 在左侧的 Application Pools 节点右键点击选择：“Add Application Pool…”，然后做出如图设置：

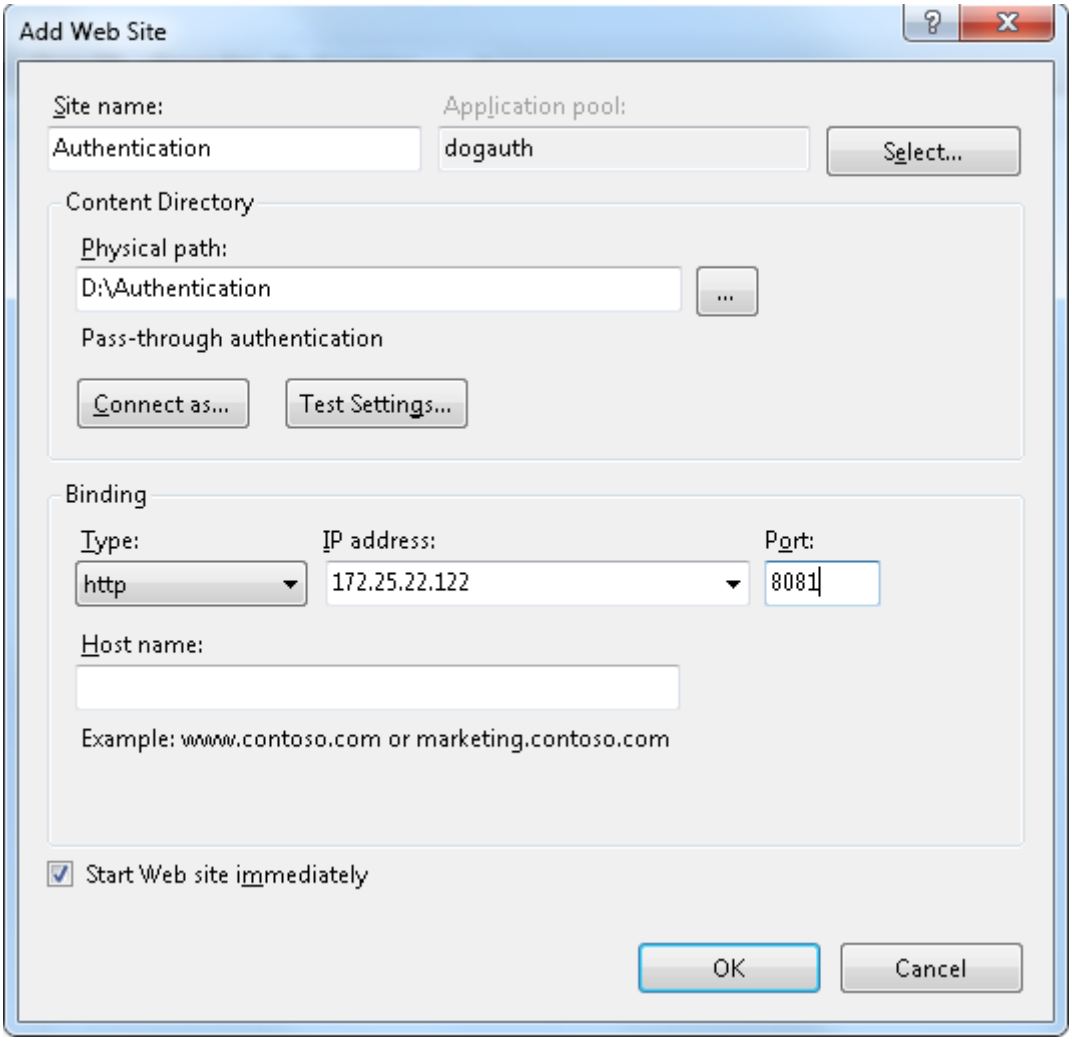


点击“OK”确认。然后点击右侧的“Advanced Settings…”，打开“Advanced Setting”对话框，做出如下图设置：



点击“OK”确认。

6. 在左侧的 Sites 节点右键点击选择：“Add Web Site…”，在弹出的对话框中，做出相关设置，例如：在“Application pool：”中选择上面设置的“dogauth”；在“Physical path”中设置为工程的存放路径；在“IP Address”中设置一个可用的 IP 地址，选择一个不会跟其他应用程序冲突的端口。如图：



点击“OK”确认。

PHP Web 工程

使用需求

PHP Web 服务器端需下载并配置 Apache 和 PHP。

本例中通过测试版本：

Apache 2.4.12 vc9 x86 和 php-5.4.36-Win32-VC9-x86

客户端需安装 32-bit IE 8.0 或者以上版本，32-bit Chrome 或者 Firefox 浏览器。

如果客户端使用 IE 浏览器，客户端既可以通过网页提示下载并安装客户端控件，也可以运行 DogAuthPluginSetup.exe 安装控件；如果客户端使用 Chrome 或者 Firefox 浏览器，请运行 DogAuthPluginSetup.exe 安装控件。

使用 PHP 示例程序

PHP 示例工程使用超级狗试用件演示。请按照如下步骤使用此软件包：

1. 下载 Apache 与 PHP 压缩包并部署。

2. 在服务器端，将超级狗认证服务器端 PHP 扩展组件 dog_auth_srv_php.dll 放到：（盘符:）\（PHP 安装文件夹）\ext 目录下。例如：D:\php\ext。在 PHP 的配置文件（php.ini）中添加“extension=dog_auth_srv_php.dll”。该组件对应 php 源码版本为：5.4.36 版本，请使用相应版本的 php 二进制包进行部署。

   如果用户使用其他 php 版本部署工程，请使用超级狗认证服务器端 PHP 扩展组件源代码工程（目录：WebServer\PHP\Source\dog_auth_srv_php）链接相应的 php 源代码版本，编译出对应的 PHP 扩展组件。该组件提供了对客户端进行身份认证的相关功能。

3. 本工程无需编译，使用 Apache 部署本工程后，在客户端打开 32-bit 浏览器，输入网址：

   http://[服务器 IP]:（Apache 中部署的端口号）/Login.php 即可。

最终用户第一次使用请点击进入注册页面，输入用户名和用户口令进行注册。

用户名和用户口令将被写入超级狗硬件；同时，用户名和超级狗 ID 将被写入服务器端数据库中。

用户可以对用户口令进行更改。

部署您自己的 PHP 工程

实际的工程将绑定您的开发商 ID 和认证代码。工程部署示范采用 Windows 7 系统与 Apache 2.4.10 x86 版本，请参照如下步骤：

1. 请插入您的开发狗，使用认证代码生成工具生成认证代码，文件名默认为：auth_code.xml。文件内容包含您的开发商 ID 和认证代码。请将 auth_code.xml 拷贝至服务器端工程的目录 serverdata 中。

2. 使用超级狗认证初始化工具（AuthTool.exe）修改超级狗的管理员口令（SO PIN，默认为：“abcdefgh”）和认证因子（默认为：“00000000”），设置用户口令（USER PIN，默认为：“12345678”）与用户信息。也可通过 web 工程的用户注册页面让用户自行注册修改用户口令与用户名。如果您修改了认证因子，请同时修改 serverdata 目录中的配置文件：auth_factor.xml。为了提高安全性，建议您修改默认的认证因子。

3. 在服务器端，按照常规方法部署在 Apache 与 PHP 运行环境。在 Apache 配置文件（Apache 文件夹）\conf\httpd.conf 中，设置您的 web 工程路径，例如：

   ```
   DocumentRoot "E:/Authentication/php"
   <Directory "E:/Authentication/php">
   ```

注意

1. 在 Windows 系统部署 PHP 环境需要安装 Visual C++ Redistributable Package。请按照您选择的 PHP 版本中的说明文档安装对应版本的 Visual C++ Redistributable Package。

2. 示例工程中提供的 PHP 扩展组件 dog_auth_srv_php.dll 对应 php 源码版本为：5.4.36 版本，如果使用其他 php 版本部署工程，请使用超级狗认证服务器端 PHP 扩展组件源代码工程（目录：WebServer\PHP\Source\dog_auth_srv_php）链接相应的 php 源代码版本，编译出对应的 PHP 扩展组件。否则可能将导致 dog_auth_srv_php.dll 无法正常加载。

3. PHP 部署时需要指定一个会话缓存目录，并将该路径设置到 PHP 的配置文件中。例如：在 php.ini 文件中设置：

   ```
   session.save_path = "D:/tmp"
   ```

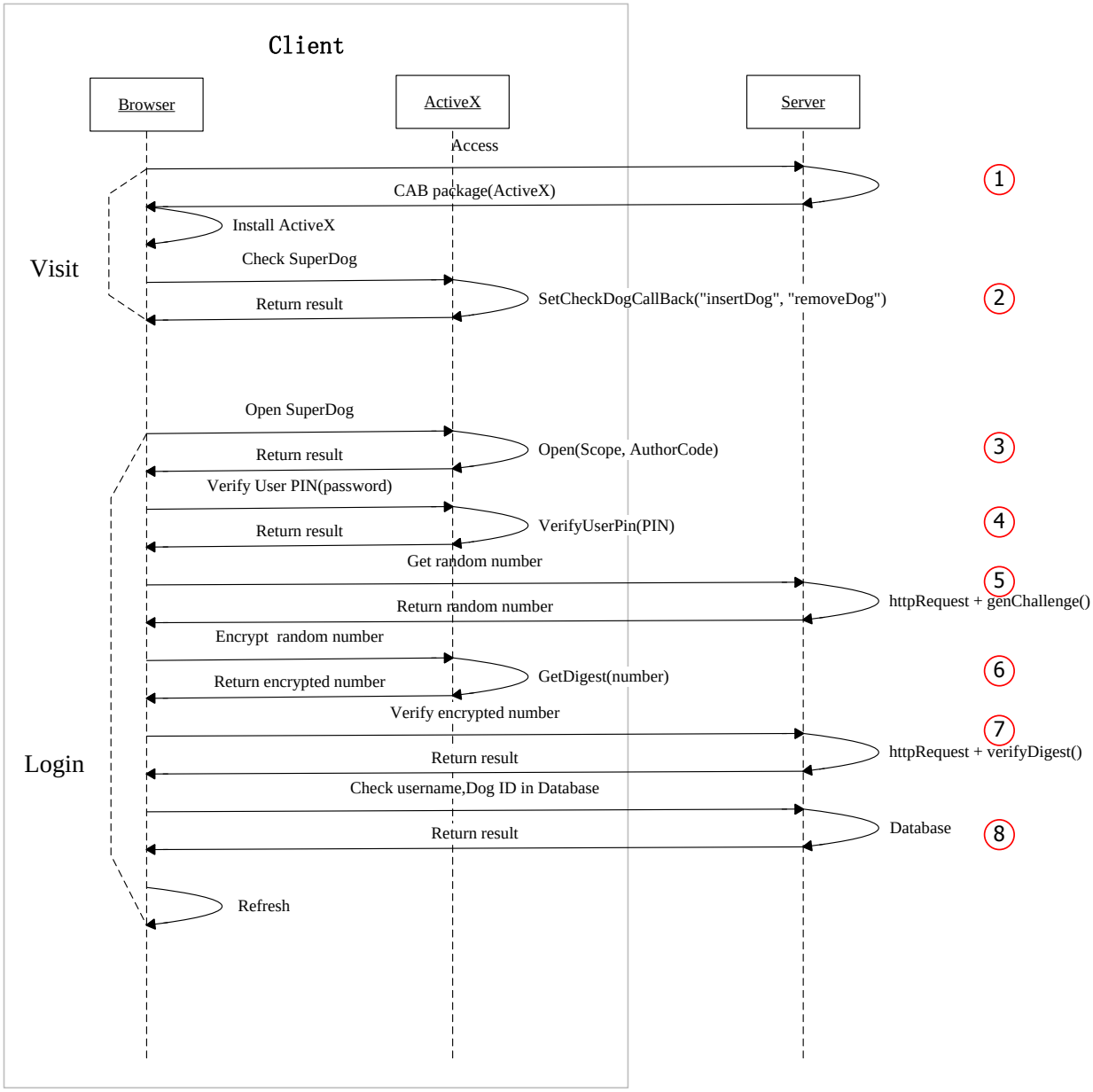
   没有正确设置将影响 PHP 工程的正常使用。

实际应用注意事项

1. 管理员可以使用认证工具 AuthTool.exe 修改默认的管理员口令（SO PIN），默认的管理员口令是：“abcdefgh”。为了提高安全性，强烈建议您修改默认的管理员口令。
2. 管理员可以使用超级狗认证初始化工具 AuthTool.exe 修改默认的认证因子（Authenticate Factor），默认的认证因子是“00000000”。如果您修改了认证因子，请同时修改服务器端配置文件：auth_factor.xml。为了提高安全性，建议您修改默认的认证因子。
3. 连续输入 15 次错误的管理员口令，管理员口令会被锁定。管理员口令被锁定后不影响用户使用超级狗进行认证操作。
4. 用户连续输入 15 次错误的用户口令，用户口令会被锁定。如果要解除锁定，用户需要将超级狗寄给管理员，管理员可以使用认证工具 AuthTool.exe 解锁并设置新的用户口令。
5. 如果用户使用 DogAuthPluginSetup.exe 安装控件，控件将被安装到如下目录：
   a. 如果是 64 位系统，C:\Program Files (x86)\Common Files\SafeNet Dog\SuperDog Auth
   b. 如果是 32 位系统，C:\Program Files\Common Files\SafeNet Dog\SuperDog Auth
6. 用户名、口令、用户数据等信息将被加密存储于超级狗默认的数据文件中（文件 ID 为 65524）。如果您还将超级狗用于软件保护，请不要调用 API 更改此文件。您可以使用许可设计工具设计并写入其它的数据文件。

第三章 认证流程

用户登录流程



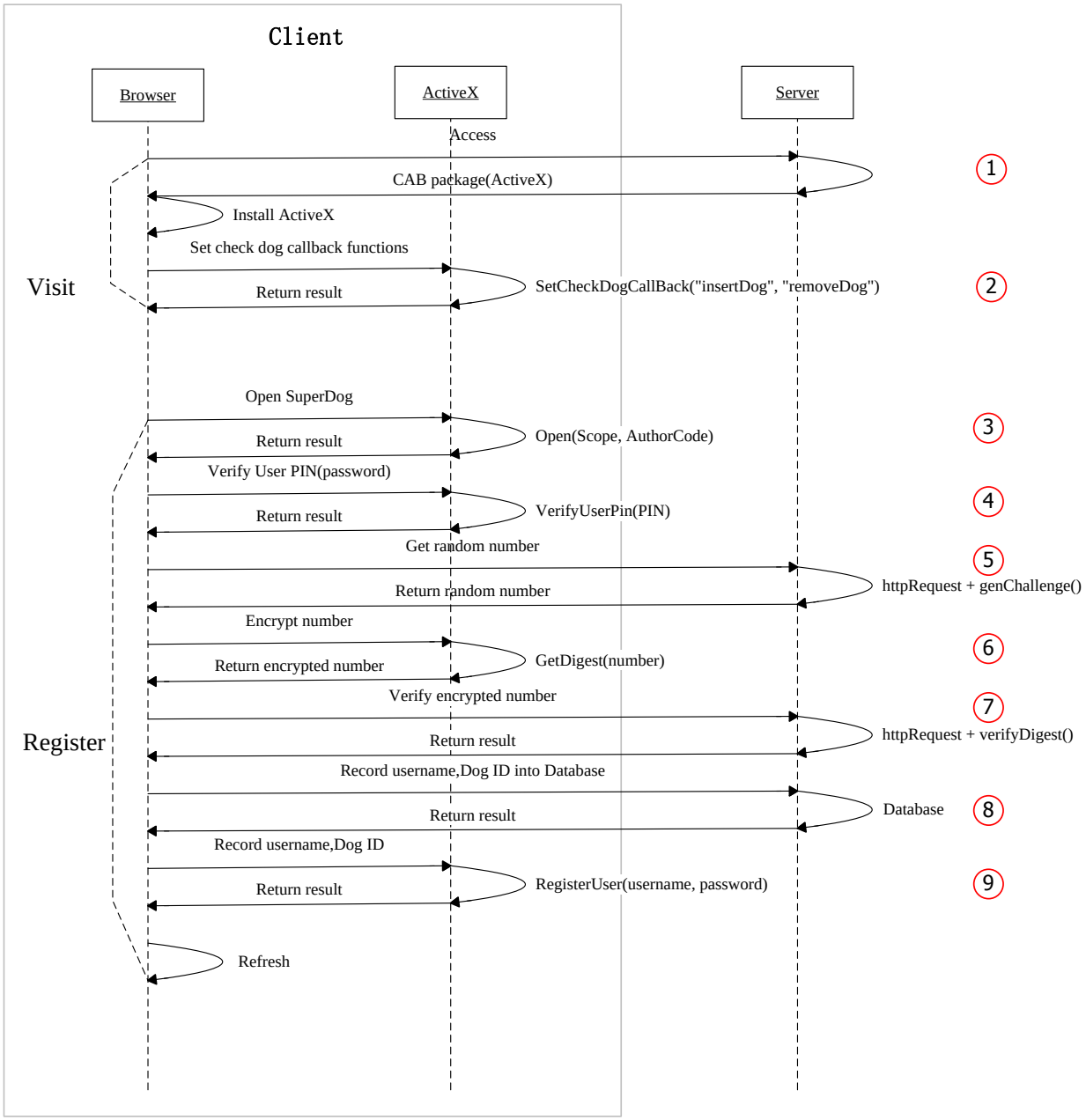
图（一）

流程说明

1. 浏览登录页面，如 `http://localhost:8080/Authentication/Login.jsp` 。客户端会自动加载提示安装 `ActiveX` 控件，点击安装，完成控件的安装，如果已经安装了控件则不会提示。

2. 页面的 javascript 代码调用控件的 SetCheckDogCallBack ("insertDog","removeDog") 方法设置 js 回调函数。"insertDog"插入超级狗的响应函数，"removeDog"拔出超级狗的响应函数。
3. 页面的 javascript 代码调用控件的 Open (Scope, AuthorCode) 方法，打开超级狗。只有打开狗以后才可访问后续的处理函数，使用结束后需调用 Close () 方法关闭超级狗。参数 Scope 表示在多个超级狗同时存在的情况下，可以打开特定的狗；参数 AuthorCode 是从服务端的 auth_code.xml 配置文件中读取的算法数据。
4. 页面的 javascript 代码调用控件的 VerifyUserPin(PIN) 方法，验证用户输入的口令与超级狗中的口令是否一致。
5. 页面的 javascript 代码调用 getChallenge() 方法发送 httpRequest 请求，获取服务端随机生成的挑战数据，服务端同时把数据记录到 session 中。
6. 页面的 javascript 代码调用控件的 GetDigest (PIN) 方法，对挑战数据进行加密处理。
7. 页面的 javascript 代码调用 doAuth () 方法发送 httpRequest 请求，把从 ActiveX 控件中获取的 DogID 和加密的挑战数据发送给服务端。服务端的 verifyDigest()方法对数据进行比对。
8. 对登录的用户进行数据库（Access Database）的查询匹配，如果匹配成功则可以访问主页。

用户注册流程



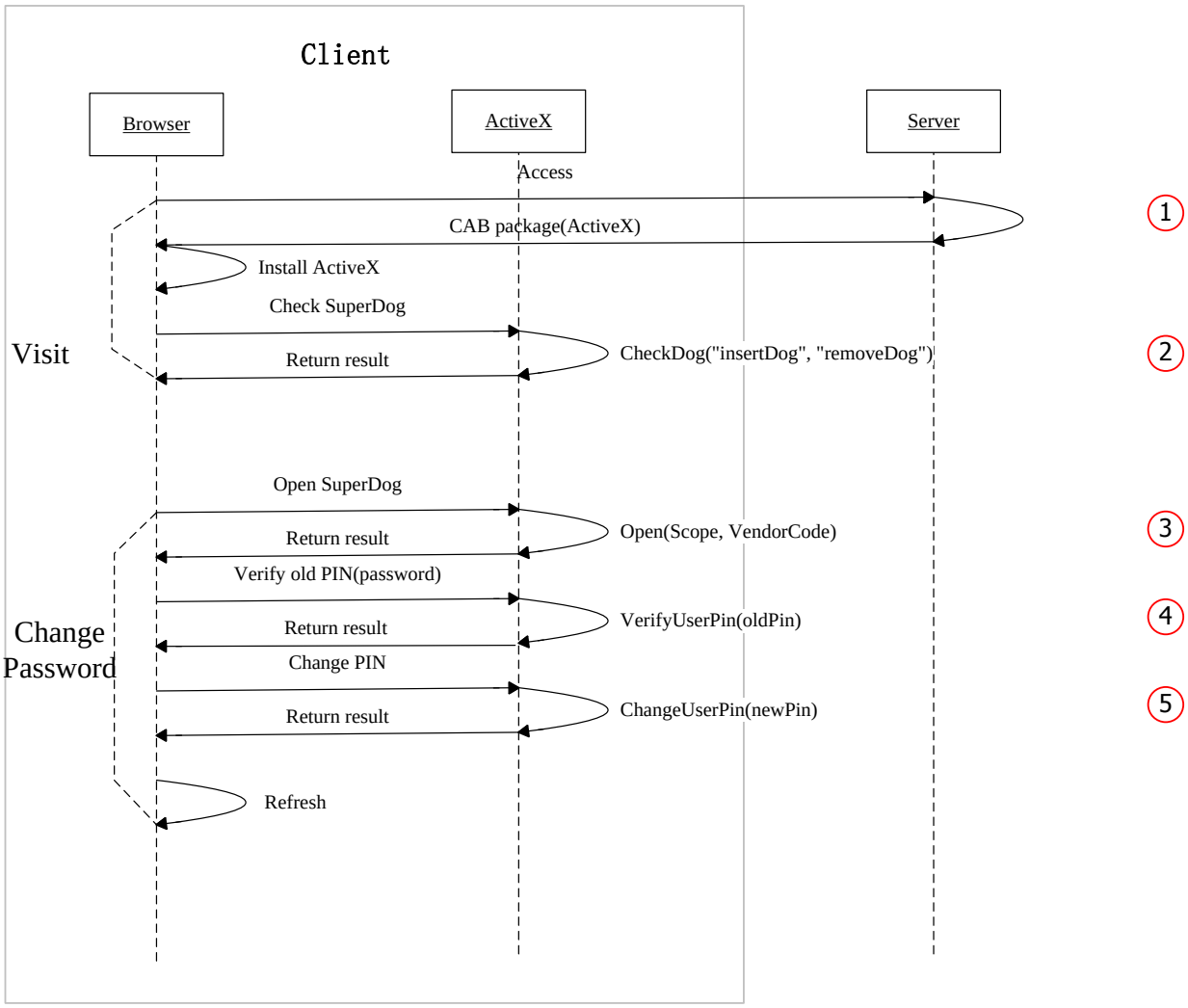
图（二）

流程说明

1. 浏览登录页面，如：`http://localhost:8080/Authentication/Register.jsp` 。客户端会自动加载提示安装 `ActiveX` 控件，点击安装，完成控件的安装，如果已经安装了控件则不会提示。

2. 页面的 javascript 代码调用控件的 SetCheckDogCallBack ("insertDog","removeDog") 方法设置 js 回调函数。"insertDog"，插入超级狗的响应函数，"removeDog"拔出超级狗的响应函数。
3. 页面的 javascript 代码调用控件的 Open (Scope, AuthorCode) 方法，打开超级狗。只有打开狗以后才可访问后续的处理函数，使用结束后需调用 Close () 方法关闭超级狗。参数 Scope 表示在多个超级狗同时存在的情况下，可以打开特定的狗；参数 AuthorCode 是从服务端的 auth_code.xml 配置文件中读取的算法数据。
4. 页面的 javascript 代码调用控件的 VerifyUserPin(PIN) 方法，对于新注册的超级狗需要先验证，输入初始参数"12345678"。
5. 页面的 javascript 代码调用 getChallenge() 方法发送 httpRequest 请求，获取服务端随机生成的挑战数据，服务端同时把数据记录到 session 中。
6. 页面的 javascript 代码调用控件的 GetDigest (PIN) 方法，对挑战数据进行加密处理。
7. 页面的 javascript 代码调用 doAuth () 方法发送 httpRequest 请求，把从 ActiveX 控件中获取的 DogID 和加密的挑战数据发送给服务端。服务端的 verifyDigest()方法对数据进行比对。
8. 对新注册的用户记录用户信息，把信息写入数据库（Access Database）。
9. 数据库写入成功后，调用 ActiveX 控件的 RegisterUser(username, PIN)方法，把注册信息写入到超级狗里。

用户修改口令流程



图（三）

流程说明

1．浏览登录页面，如：`http://localhost:8080/Authentication/ModifyPin.jsp` 。客户端会自动加载提示安装 `ActiveX` 控件，点击安装，完成控件的安装，如果已经安装了控件则不会提示。

2．页面的 `javascript` 代码调用控件的 `SetCheckDogCallBack("insertDog","removeDog")` 方法设置 `js` 回调函数。“`insertDog`”，插入超级狗的响应函数，“`removeDog`”拔出超级狗的响应函数。

3. 页面的 javascript 代码调用控件的 Open (Scope, AuthorCode) 方法，打开超级狗。只有打开狗以后才可访问后续的处理函数，使用结束后需调用 Close () 方法关闭超级狗。参数 Scope 表示在多个超级狗同时存在的情况下，可以打开特定的狗；参数 AuthorCode 是从服务端的 auth_code.xml 配置文件中读取的算法数据。
4. 页面的 javascript 代码调用控件的 VerifyUserPin(PIN) 方法，验证用户输入的旧口令与超级狗中的口令是否一致。
5. 页面的 javascript 代码调用控件的 ChangeUserPin (newPIN) 方法，修改新口令为 newPIN。

第四章 客户端浏览器控件

IE 浏览器控件

超级狗认证 IE 浏览器控件是一个经过签名的 ActiveX 形式的 COM 控件，它的文件名是 SuperDogAuth.ocx。浏览器控件与初始化工具相对应，向 web 前端开发者提供了一组可以利用超级狗内部的默认数据文件进行身份认证的函数接口。

超级狗认证 IE 浏览器控件的 CLSID 为“05C384B0-F45D-46DB-9055-C72DC76176E3”，并能够响应超级狗的硬件插拔消息。在网页中，可以这样对它定义：

```
<object id="AuthIE" name="AuthIE" width="0px" height="0px"
            codebase="DogAuth.CAB"
            classid="CLSID:05C384B0-F45D-46DB-9055-C72DC76176E3">
</object>
```

下面对超级狗认证 IE 浏览器控件的所有的接口函数进行说明：

- **LONG Open([in]BSTR strScope, [in]BSTR strAuthCode)**

说明：打开目前系统中的一个超级狗。如果有多个超级狗连接到当前系统中，请在第一个输入参数中，指定要搜索超级狗 ID 的 XML 格式定义。更多信息，参阅超级狗帮助文档中 《超级狗 Licensing API 帮助》的“范围输入 XML 标记”一节。

输入数据：

strScope：要搜索的数据的 XML 格式定义。更多信息，参阅超级狗帮助文档中 《超级狗 Licensing API 帮助》的“范围输入 XML 标记”一节。

strAuthCode：认证代码字符串。该内容从认证代码生成工具生成的 xml 文件中取出。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.Open(scope, auth_code);
```

注：这里的 AuthIE 是网页内定义的超级狗认证 IE 浏览器控件的名称（ID），开发中应根据实际命名进行改变。下同。

- **LONG Close()**

说明：从当前的一个会话环境中注销。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.Close();
```

- **LONG VerifyUserPin([in]BSTR strpin)**

说明：校验超级狗的用户口令。

输入数据：

strPin：用户口令字符串。范围：6-16 字节。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.VerifyUserPin("12345678");
```

- **LONG ChangeUserPin([in]BSTR strdstpin)**

说明：修改超级狗的用户口令。需要先校验超级狗的用户口令成功。

输入数据：

strdstpin：用于替换的用户口令字符串。范围：6-16 字节。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.ChangeUserPin("111111");
```

- **LONG GetUserName()**

说明：获取超级狗的用户名字符串。需要在调用该函数之后再通过控件属性 UserNameStr 获取用户名。最大长度：32 字节

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.GetUserName();
var name = AuthIE.UserNameStr;
```

- **LONG GetDogID()**

说明：获取当前会话环境中的超级狗 ID 号。需要在调用该函数之后再通过控件属性 DogIdStr 获取 ID 号。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.GetDogID();
var idinfo = AuthIE.DogIdStr;
```

- **LONG GetDigest([in]BSTR strChallenge)**

说明：根据输入的字符串生成加密的摘要字符串。需要在调用该函数之后再通过控件属性 DigestStr 获取加密的摘要字符串。需要先校验超级狗的口令成功。

输入数据：

strChallenge：用于生成加密摘要的字符串。即从服务器端获取的挑战数据。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.GetDigest("3702032AA96A457CB619C523E1126340");
var repn = AuthIE.DigestStr;
```

- **LONG SetCheckDogCallBack([in]BSTR strinstfun, [in]BSTR strrmvfun)**

说明：开启服务检测超级狗的插拔。通过参数传递响应超级狗插拔设备的 javascript 函数名称。

输入数据：

strinstfun：用于响应超级狗接入到系统的 javascript 函数名称。

strrmvfun：用于响应拔掉超级狗的 javascript 函数名称。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.SetCheckDogCallBack("insertfunc", "pullfunc");
```

- **LONG RegisterUser([in]BSTR struser, [in]BSTR strpin)**

说明：注册用户信息。第一次使用超级狗时，将用户名和用户口令写入超级狗默认的数据文件中。

输入数据：

struser：用户名字符串。最大长度：32 字节。

strpin：用户口令字符串。范围：6-16 字节。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.RegisterUser("Edward", "12345678");
```

- **LONG SetUserData([in]LONG idatatype, [in]LONG ioffset, [in]BSTR strdata)**

说明：设置自定义用户信息。需要管理员口令或用户口令验证通过。

输入数据：

idatatype：字符串类型为：16 进制格式或普通可显示字符串。

ioffset：存储到超级狗中的偏移量。

Strdata：自定义用户数据。

16 进制格式字符串，类似："EFD9AE38"，长度必须为偶数，函数内部会把该字符串转换为对应的 ASCII 码存储到超级狗中。字符串长度/2 + ioffset 必须小于或等于 50；

普通可显示字符串，类似："SafeNet"，字符串长度 + ioffset 必须小于或等于 50。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.SetUserData(1, 30, "SafeNet Inc");
```

- **LONG GetUserData([in]LONG idatatype, [in]LONG ioffset, [in] LONG iDataSize)**

说明：获取自定义用户信息。需要在调用该函数之后再通过控件属性 UserDataStr 获取用户信息。

输入数据：

idatatype：字符串类型为：16 进制格式或普通可显示字符串。

ioffset：存储到超级狗中的偏移量。

iDataSize：获取用户数据的大小。需要比欲取到的数据长度大一个字节。

16 进制格式字符串，类似："EFD9AE38"，(idatatype - 1)/2 + ioffset 必须小于或等于 50；

普通可显示字符串，类似："SafeNet"，(idatatype - 1) + ioffset 必须小于或等于 50。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
AuthIE.GetUserData(1, 30, 11);
var datainfo = AuthIE.UserDataStr;
```

Chrome 和 Firefox 浏览器控件

超级狗认证 Chrome 和 Firefox 浏览器控件是一个经过签名的基于 NPAPI 的控件，它的文件名是 npDogAuth.dll。浏览器控件与初始化工具相对应，向 web 前端开发者提供了一组可以利用超级狗内部的默认文件进行身份认证的函数接口。

超级狗认证 Chrome 和 Firefox 浏览器控件能够响应超级狗的硬件插拔。在网页中，可以这样对它定义：

```
var temp = document.body.innerHTML;
var embed_tag = "<embed id=\"Authplg\" type=\"application/x-dogauth\"
width=0 height=0 hidden=\"true\"></embed>";
document.body.innerHTML = embed_tag + temp;
```

下面对超级狗认证 Chrome 和 Firefox 浏览器控件的所有的接口函数进行说明：

- **int Open([in]NPSTRING strScope, [in]NPSTRING strAuthCode)**

说明：打开目前系统中的一个超级狗。如果有多个超级狗连接到当前系统中，请在第一个输入参数中，指定要搜索超级狗 ID 的 XML 格式定义。更多信息，参阅超级狗帮助文档中 《超级狗 Licensing API 帮助》的“范围输入 XML 标记”一节。

输入数据：

strScope：要搜索的数据的 XML 格式定义。更多信息，参阅超级狗帮助文档中 《超级狗 Licensing API 帮助》的“范围输入 XML 标记”一节。

strAuthCode：认证代码字符串。该内容从认证代码生成工具生成的 xml 文件中取出。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.Open(scope, auth_code);
```

注：这里的 Authplg 是网页内定义的超级狗认证 Chrome 和 Firefox 浏览器控件的名称（ID），开发中应根据实际命名进行改变。下同。

- **int Close()**

说明：从当前的一个会话环境中注销。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.Close();
```

- **int VerifyUserPin([in]NPSTRING strpin)**

说明：校验超级狗的用户口令。

输入数据：

strPin：用户口令字符串。范围：6-16 字节。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.VerifyUserPin("12345678");
```

- **int ChangeUserPin([in]NPSTRING strdstpin)**

说明：修改超级狗的用户口令。需要先校验超级狗的用户口令成功。

输入数据：

strdstpin：用于替换的用户口令字符串。范围：6-16 字节。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.ChangeUserPin("111111");
```

- **int GetUserName()**

说明：获取超级狗的用户名字符串。需要在调用该函数之后再通过控件属性 UserNameStr 获取用户名。最大长度：32 字节

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.GetUserName();
var name = Authplg.UserNameStr;
```

- **int GetDogID()**

说明：获取当前会话环境中的超级狗 ID 号。需要在调用该函数之后再通过控件属性 DogIdStr 获取 ID 号。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.GetDogID();
var idinfo = Authplg.DogIdStr;
```

- **int GetDigest([in]NPSTRING strChallenge)**

说明：根据输入的字符串生成加密的摘要字符串。需要在调用该函数之后再通过控件属性 DigestStr 获取加密的摘要字符串。需要先校验超级狗的口令成功。

输入数据：

strChallenge：用于生成加密摘要的字符串。即从服务器端获取的挑战数据。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.GetDigest("3702032AA96A457CB619C523E1126340");
var repn = Authplg.DigestStr;
```

- **int SetCheckDogCallBack([in]NPSTRING strinstfun, [in]NPSTRING strrmvfun)**

说明：开启服务检测超级狗的插拔。通过参数传递响应超级狗插拔设备的 javascript 函数名称。在调用该函数之后，需要通过控件属性 InsertFunc 与 RemoveFunc 分别传入响应超级狗插拔的 javascript 函数名称。

输入数据：

strinstfun：用于响应超级狗接入到系统的 javascript 函数名称。

strrmvfun：用于响应拔掉超级狗的 javascript 函数名称。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.SetCheckDogCallBack("insertfunc", "pullfunc");
Authplg.InsertFunc = insertfunc;
Authplg.RemoveFunc = pullfunc;
```

- **int RegisterUser([in]NPSTRING struser, [in]NPSTRING strpin)**

说明：注册用户信息。第一次使用超级狗时，将用户名和用户口令写入超级狗默认的数据文件中。

输入数据：

struser：用户名字符串。最大长度：32 字节。

strpin：用户口令字符串。范围：6-16 字节。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.RegisterUser("Edward", "12345678");
```

- **int SetUserData([in]int idatatype, [in]int ioffset, [in]NPSTRING strdata)**

说明：设置自定义用户信息。需要管理员口令或用户口令验证通过。

输入数据：

idatatype：字符串类型为：16 进制格式或普通可显示字符串。

ioffset：存储到超级狗中的偏移量。

Strdata：自定义用户数据。

16 进制格式字符串，类似："EFD9AE38"，长度必须为偶数，函数内部会把该字符串转换为对应的 ASCII 码存储到超级狗中。字符串长度/2 + ioffset 必须小于或等于 50；

普通可显示字符串，类似："SafeNet"，字符串长度 + ioffset 必须小于或等于 50。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.SetUserData(1, 30, "SafeNet Inc");
```

- **int GetUserData([in]int idatatype, [in]int ioffset, [in]int iDataSize)**

说明：获取自定义用户信息。需要在调用该函数之后再通过控件属性 UserDataStr 获取用户信息。

输入数据：

idatatype：字符串类型为：16 进制格式或普通可显示字符串。

ioffset：存储到超级狗中的偏移量。

iDataSize：获取用户数据的大小。需要比欲取到的数据长度大一个字节。

16 进制格式字符串，类似："EFD9AE38"，(idatatype – 1)/2 + ioffset 必须小于或等于 50；

普通可显示字符串，类似："SafeNet"，(idatatype – 1) + ioffset 必须小于或等于 50。

返回数据：

DOG_STATUS_OK： 请求已成功完成

JavsScript 调用示例：

```
Authplg.GetUserData(1, 30, 11);
var datainfo = Authplg.UserDataStr;
```

第五章 服务器端组件

动态链接库

超级狗认证服务器端动态链接库分为 32 位版本（dog_auth_srv.dll）和 64 位版本（dog_auth_srv_x64.dll）。该动态库向服务器端开发者提供了一组可以对客户端进行身份认证的函数接口。

下面对超级狗认证服务器端动态链接库的接口函数进行说明：

- **public native static String getChallenge(int status[])**

说明：生成一个随机的挑战字符串。

输出数据：

status：用于获取函数执行结果。如果执行成功，status[0]返回值为：DOG_STATUS_OK。

返回数据：

生成的随机挑战字符串。

调用示例：

```
String challenge = getChallenge(status);
```

- **public native static int verifyDigest(**
  int vendor_id,
  int dog_id,
  String challenge,
  String digest,
  String factor)

说明：验证输入的挑战字符串与生成的加密摘要字符串是否能够正确匹配。

输入数据：

vendor_id：开发商 ID。

dog_id：超级狗 ID。

challenge：随机生成的挑战字符串。

digest：由客户端生成的加密的摘要字符串。

factor：认证因子。

返回数据：

DOG_STATUS_OK： 验证成功

调用示例：

```
int ires = verifyDigest(37515, 591751299,
"4B2E2D1266241012460276532052663 8",
"288692145D2C611861A26093318F86437F0151A7", "00000000");
```

PHP 扩展组件

超级狗认证服务器端 PHP 扩展组件为 32 位版本（dog_auth_srv_php.dll）。该组件向 PHP 工程的服务器端开发者提供了一组可以对客户端进行身份认证的函数接口。该组件提供源代码工程（目录：WebServer\PHP\Source\dog_auth_srv_php），用于开发者链接相应的 php 源代码版本，编译出对应版本的 PHP 扩展组件。

下面对超级狗认证服务器端 PHP 扩展组件的接口函数进行说明：

- **char* dog_auth_get_challenge()**

说明：生成一个随机的挑战字符串。

返回数据：

生成的随机挑战字符串。如果执行成功，将返回包含 32 个 Base16 字符的字符串。

PHP 调用示例：

```
$strchallenge = dog_auth_get_challenge();
```

- **int dog_auth_verify_digest(**
  int vendor_id,
  int dog_id,
  char challenge,
  char digest,
  char factor)

说明：验证输入的挑战字符串与生成的加密摘要字符串是否能够正确匹配。

输入数据：

vendor_id：开发商 ID。

dog_id：超级狗 ID。

challenge：随机生成的挑战字符串。

digest：由客户端生成的加密的摘要字符串。

factor：认证因子。

返回数据：

DOG_STATUS_OK： 验证成功。

PHP 调用示例：

```
$ires = dog_auth_verify_digest(37515, 591751299,
"4B2E2D1266241012460276532052663 8",
"288692145D2C611861A26093318F86437F0151A7", "00000000");
```

第六章 超级狗认证动态链接库

超级狗认证动态链接库的文件名是 dogauthdsp.dll。该动态库由初始化工具调用，向开发者提供了一组可以利用超级狗内部的默认文件进行身份认证的函数接口。

下面对超级狗认证动态链接库的接口函数进行说明：

- **dog_status_t DOG_CALLCONV dog_auth_open(**
  const char *scope,
  const char *auth_code,
  auth_handle_t *handle)

说明：打开目前系统中的一个超级狗。如果有多个超级狗连接到当前系统中，请在第一个输入参数中，指定要搜索超级狗 ID 的 XML 格式定义。更多信息，参阅超级狗帮助文档中 《超级狗 Licensing API 帮助》的“范围输入 XML 标记”一节。

输入数据：

scope：要搜索的数据的 XML 格式定义。更多信息，参阅超级狗帮助文档中 《超级狗 Licensing API 帮助》的“范围输入 XML 标记”一节。

auth_code：指向认证代码的指针。该内容从**认证代码生成工具**生成的 xml 文件中取出。

handle：指向生成的会话句柄的指针。

返回数据：

DOG_STATUS_OK：请求已成功完成

调用示例：

```
dog_auth_open(scope, auth_code, &handle);
```

- **dog_status_t DOG_CALLCONV dog_auth_close(**
  auth_handle_t handle)

说明：关闭与当前会话关联的超级狗。

输入数据：

handle：指向会话句柄的指针。

返回数据：

DOG_STATUS_OK：请求已成功完成

调用示例：

```
dog_auth_close(handle);
```

- **dog_status_t DOG_CALLCONV dog_auth_verify_pin(**
  auth_handle_t handle,

dogauth_pin_t pin_type,

const char *current_pin)

说明：校验超级狗的管理员口令或用户口令。

输入数据：

handle：会话句柄。

pin_type：口令类型，可以是管理员口令或者用户口令。

current_pin：欲验证的口令字符串。范围：6-16 字节。

返回数据：

DOG_STATUS_OK：请求已成功完成

调用示例：

校验管理员口令

```
dog_auth_verify_pin(handle, PINTYPE_SO_PIN, "abcdefgh");
```

校验用户口令

```
dog_auth_verify_pin(handle, PINTYPE_USER_PIN, "12345678");
```

- **dog_status_t DOG_CALLCONV dog_auth_change_pin(**

  auth_handle_t handle,

  dogauth_pin_t pin_type,

  const char *new_pin)

说明：修改超级狗的口令。需要先校验超级狗的口令成功。校验超级狗管理员口令成功后，可以修改管理员口令与用户口令。校验超级狗用户口令成功后，只能修改用户口令。

输入数据：

handle：会话句柄。

pin_type：管理员口令或者用户口令。

new_pin：用于替换的口令字符串。范围：6-16 字节。

返回数据：

DOG_STATUS_OK：请求已成功完成

调用示例：

```
dog_auth_change_pin(handle, PINTYPE_SO_PIN, "111111");
```

- **dog_status_t DOG_CALLCONV dog_auth_get_digest(**

  auth_handle_t handle,

  const char *challenge,

  char *digest,

  dog_size_t *digest_size)

说明：根据输入的挑战字符串生成加密的摘要字符串。调用此函数之前需要先成功校验超级狗的口令。

输入数据：

handle：会话句柄。

challenge：从服务器端获取的挑战字符串，用于生成加密的摘要字符串。挑战字符串长度为 32 字节。

digest_size：指定存储获取的摘要字符串缓冲区的大小。长度至少为 41 字节。

输出数据：

digest：指向获取的加密摘要字符串的指针。生成的摘要字符串的长度为 40 字节。

返回数据：

DOG_STATUS_OK： 请求已成功完成

调用示例：

```
dog_auth_get_digest(handle, challenge, digest, 41);
```

- **dog_status_t DOG_CALLCONV dog_auth_set_factor(**
  auth_handle_t handle,
  const char *factor)

说明：设置认证因子。认证因子将在生成加密的摘要字符串中使用。需要先校验超级狗的管理员口令成功。

输入数据：

handle：会话句柄。

factor：认证因子字符串。长度为 8 字节。

返回数据：

DOG_STATUS_OK： 请求已成功完成

调用示例：

```
dog_auth_set_factor(handle, "cv6ejrbj");
```

- **dog_status_t DOG_CALLCONV dog_auth_get_dogid(**
  auth_handle_t handle,
  char *dog_id,
  dog_size_t *id_size)

说明：获取当前会话的超级狗 ID。

输入数据：

handle：会话句柄。

id_size：指定存储获取的超级狗 ID 字符串的缓冲区的大小。

输出数据：

dog_id：指向存储获取的超级狗 ID 字符串的缓冲区的指针。

返回数据：

DOG_STATUS_OK： 请求已成功完成

调用示例：

```
dog_auth_get_dogid(handle, dogid, id_size);
```

- **dog_status_t DOG_CALLCONV dog_auth_set_username(**
  auth_handle_t handle,
  const char *user_name)

说明：设置用户名。最大长度：32 字节。需要管理员口令或用户口令验证通过。

输入数据：

handle：会话句柄。

user_name：要设置的用户名字符串。

返回数据：

DOG_STATUS_OK：请求已成功完成

调用示例：

```
dog_auth_set_username(handle, "demouser");
```

- **dog_status_t DOG_CALLCONV dog_auth_get_username(**
  auth_handle_t handle,
  char *user_name,
  dog_size_t *name_size)

说明：获取用户名。最大长度：32 字节。

输入数据：

handle：会话句柄。

name_size：用于存储获取的用户名的缓冲区的大小。

输出数据：

user_name：指向存储获取的用户名的缓冲区的指针。

返回数据：

DOG_STATUS_OK：请求已成功完成

调用示例：

```
dog_auth_get_username(handle, tmpbuf, buf_size);
```

- **dog_status_t DOG_CALLCONV dog_auth_set_userdata(**
  auth_handle_t handle,

```
    dog_data_t data_type,
    dog_size_t offset,
    const char *user_data)
```

说明：设置自定义用户信息。需要管理员口令或用户口令验证通过。

输入数据：

handle：会话句柄。

data_type：字符串类型为：16 进制格式或普通可显示字符串。

offset：存储到超级狗中的偏移量。

user_data：自定义用户数据。

16 进制格式字符串，类似："EFD9AE38"，长度必须为偶数，函数内部会把该字符串转换为对应的 ASCII 码存储到超级狗中。字符串长度/2 + offset 必须小于或等于 50；

普通可显示字符串，类似："SafeNet"，字符串长度 + offset 必须小于或等于 50。

返回数据：

DOG_STATUS_OK： 请求已成功完成

调用示例：

```
dog_auth_set_userdata(handle, DATA_TYPE_STRING, 3, "SafeNet Inc");
```

- ```
  dog_status_t DOG_CALLCONV dog_auth_get_userdata(
  auth_handle_t handle,
  dog_data_t data_type,
  dog_size_t offset,
  dog_size_t length,
  char *user_data)
  ```

说明：获取自定义用户信息。

输入数据：

handle：会话句柄。

data_type：字符串类型为：16 进制格式或普通可显示字符串。

offset：用户信息块的偏移量。

length：想要获取用户信息的长度。

注意：请预留足够的空间以存储获取的用户信息。根据数据类型的不同，需要的大小计算如下：

16 进制格式字符串，类似："EFD9AE38"，空间须大于 length * 2

普通可显示字符串，类似："SafeNet"，空间须大于 length

输出数据：
  ```

user_data：指向存储获取的用户信息的缓冲区的指针。

返回数据：

DOG_STATUS_OK： 请求已成功完成

调用示例：

```
dog_auth_get_userdata(handle, DATA_TYPE_STRING, 0, 7, buffer, 8);
```