# SSL应用安全网关测试计划

**2015年1月**

目录

[SSL应用安全网关测试计划 1](#_Toc413694665)

[1. SSL系统测试产品组成 3](#_Toc413694666)

[1.1. SSL系统测试产品清单 3](#_Toc413694667)

[1.2. SSL系统测试示意图 3](#_Toc413694668)

[2. 测试计划 3](#_Toc413694669)

[2.1. 各产品需支持的环境列表 3](#_Toc413694670)

[2.2. 测试环境准备 4](#_Toc413694671)

[2.3. 测试目标 4](#_Toc413694672)

[2.4. 测试用例 4](#_Toc413694673)

[2.4.1. KEY厂商测试用例 4](#_Toc413694674)

[2.4.2. 国产浏览器厂商测试用例 5](#_Toc413694675)

[2.4.3. 功能与兼容性测试用例 5](#_Toc413694676)

# SSL系统测试产品组成

## SSL系统测试产品清单

1. 安全网关（支持RSA算法和SM2算法的SSL访问）
2. 支持国密算法的浏览器
3. 支持国密证书的USB KEY
4. 支持RSA证书的USB KEY

## SSL系统测试示意图

USB KEY，支持国密算法的浏览器，SSL网关



# 测试计划

## 各产品需支持的环境列表

* 主流IE浏览器（IE6，IE7，IE8，IE9，IE10，IE11）（RSA算法）
* 主流windows系统（Windows XP 32位，Windows 7 32位，Windows 7 64位，Windows 8 32位，Windows 8 64位）

## 测试环境准备

服务器端环境：

单向RSA算法SSL通道：https://公网IP:4436

双向RSA算法SSL通道：https:// 公网IP:4437

单向SM2算法SSL通道：https:// 公网IP:4438

双向SM2算法SSL通道：https:// 公网IP:4439

## 测试目标

* 通过IE浏览器和USB KEY可以实现双向SSL握手，并访问web后台数据（RSA算法）
* 通过国密浏览器和USB KEY可以实现双向SSL握手，并访问web后台数据（RSA、SM2算法）
* 完成国密浏览器和USB KEY的兼容性测试

## 测试用例

### KEY厂商测试用例

各KEY厂商自行设计产品测试用例，需保证KEY在以下操作系统与IE版本中可用，并支持RSA证书与SM2双证书（签名证书与加密证书）。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 系统版本 IE版本 | IE6 | IE7 | IE8 | IE9 | IE10 | IE11 |
| Windows XP |  |  |  | —— | —— | —— |
| Windows 7 32位 | —— | —— |  |  |  |  |
| Windows 7 64位 | —— | —— |  |  |  |  |
| Windows 8 32位 | —— | —— | —— | —— |  |  |
| Windows 8 64位 | —— | —— | —— | —— |  |  |

### 国产浏览器厂商测试用例

浏览器厂商自行设计产品测试用例，需保证浏览器在以下操作系统可用：Windos XP，Windows 7 32位，Windows 7 64位，Windows 8 32位，Windos 7 64位。可使用浏览器进行单向RSA算法SSL访问，双向RSA算法SSL访问，单向SM2算法SSL访问，双向SM2算法SSL访问（SM2算法的SSL访问参照标准《GM/T 0024-2014 SSL VPN技术规范》）

### 功能与兼容性测试用例

#### IE浏览器单向RSA算法SSL（TLS1.0协议）访问

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **IE浏览器单向RSA算法SSL访问（TLS1.0协议）** | | |
| 功能描述 | 支持用户采用单向RSA算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放RSA证书、网关服务器单向RSA算法端口443 | | |
| 测试工具 | IE（TLS1.0协议） | | |
| 测试步骤 | 1. 将IE浏览器设置为只支持TLS1.0协议  2. 打开IE浏览器,在地址栏输入地址：https://公网IP:443  3. 输入正确用户名密码点击登录  4. 登录成功  5. 点击界面上的下载链接  6. 点击页面上的500k页面测试  7. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### IE浏览器单向RSA算法SSL（TLS1.2协议）访问

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **IE浏览器单向RSA算法SSL访问（TLS1.2协议）** | | |
| 功能描述 | 支持用户采用单向RSA算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放RSA证书、网关服务器单向RSA算法端口443 | | |
| 测试工具 | IE（TLS1.2协议） | | |
| 测试步骤 | 1. 将IE浏览器设置为只支持TLS1.2协议  2. 打开IE浏览器,在地址栏输入地址：https://公网IP:443  3. 输入正确用户名密码点击登录  4. 登录成功  5. 点击界面上的下载链接  6. 点击页面上的500k页面测试  7. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### IE浏览器双向RSA算法SSL访问（TLS1.0协议）

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **IE浏览器双向RSA算法SSL访问（TLS1.0）** | | |
| 功能描述 | 支持用户采用双向RSA算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放RSA证书、用户ukey存放RSA证书、网关服务器单向RSA算法端口444 | | |
| 测试工具 | IE（TLS1.0协议） | | |
| 测试步骤 | 1. 将IE浏览器设置为只支持TLS1.0  2. 打开IE浏览器在地址栏输入地址：https://公网IP:444  3. 提示输入USBKEY pin码  4. 输入正确pin码确认后，访问成功显示应用列表  5. 点击界面上的下载链接  5. 点击页面上的500k页面测试  6. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### IE浏览器双向RSA算法SSL访问（TLS1.2协议）

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **IE浏览器双向RSA算法SSL访问（TLS1.2）** | | |
| 功能描述 | 支持用户采用双向RSA算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放RSA证书、用户ukey存放RSA证书、网关服务器单向RSA算法端口444 | | |
| 测试工具 | IE（TLS1.2协议） | | |
| 测试步骤 | 1. 将IE浏览器设置为只支持TLS1.2  2. 打开IE浏览器在地址栏输入地址：https://公网IP:444  3. 提示输入USBKEY pin码  4. 输入正确pin码确认后，访问成功显示应用列表  5. 点击界面上的下载链接  5. 点击页面上的500k页面测试  6. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |
|  |  | | |

#### 国产浏览器单向RSA算法SSL（TLS1.0协议）访问

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **国产浏览器单向RSA算法SSL访问（TLS1.0协议）** | | |
| 功能描述 | 支持用户采用单向RSA算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放RSA证书、网关服务器单向RSA算法端口443 | | |
| 测试工具 | 国产浏览器（TLS1.0协议） | | |
| 测试步骤 | 1. 将浏览器设置为只支持TLS1.0协议  2. 打开国产浏览器,在地址栏输入地址：https://公网IP:443  3. 输入正确用户名密码点击登录  4. 登录成功  5. 点击界面上的下载链接  6. 点击页面上的500k页面测试  7. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### 国产浏览器单向RSA算法SSL（TLS1.2协议）访问

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **国产浏览器单向RSA算法SSL访问（TLS1.2协议）** | | |
| 功能描述 | 支持用户采用单向RSA算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放RSA证书、网关服务器单向RSA算法端口443 | | |
| 测试工具 | 国产浏览器（TLS1.2协议） | | |
| 测试步骤 | 1. 将浏览器设置为只支持TLS1.2协议  2. 打开国产浏览器,在地址栏输入地址：https://公网IP:443  3. 输入正确用户名密码点击登录  4. 登录成功  5. 点击界面上的下载链接  6. 点击页面上的500k页面测试  7. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### 国产浏览器双向RSA算法SSL访问（TLS1.0协议）

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **国产浏览器双向RSA算法SSL访问（TLS1.0协议）** | | |
| 功能描述 | 支持用户采用双向RSA算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放RSA证书、用户ukey存放RSA证书、网关服务器单向RSA算法端口444 | | |
| 测试工具 | 国产浏览器（TLS1.0协议） | | |
| 测试步骤 | 1. 将浏览器设置为只支持TLS1.0  2. 打开国产浏览器在地址栏输入地址：https://公网IP:444  3. 提示输入USBKEY pin码  4. 输入正确pin码确认后，访问成功显示应用列表  5. 点击界面上的下载链接  5. 点击页面上的500k页面测试  6. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### 国产浏览器双向RSA算法SSL访问（TLS1.2协议）

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **国产浏览器双向RSA算法SSL访问（TLS1.2协议）** | | |
| 功能描述 | 支持用户采用双向RSA算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放RSA证书、用户ukey存放RSA证书、网关服务器单向RSA算法端口444 | | |
| 测试工具 | 国产浏览器（TLS1.2协议） | | |
| 测试步骤 | 1. 将浏览器设置为只支持TLS1.2  2. 打开国产浏览器在地址栏输入地址：https://公网IP:444  3. 提示输入USBKEY pin码  4. 输入正确pin码确认后，访问成功显示应用列表  5. 点击界面上的下载链接  5. 点击页面上的500k页面测试  6. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### 国产浏览器单向SM2算法SSL访问

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **国产浏览器单向SM2算法SSL访问** | | |
| 功能描述 | 支持用户采用单向SM2算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放SM2证书、网关服务器单向SM2算法端口445 | | |
| 测试工具 | 国产浏览器，增加白名单 | | |
| 测试步骤 | 1. 增加国产浏览器白名单https://公网IP:445  2. 打开国产浏览器,在地址栏输入地址：https://公网IP:445  3. 输入正确用户名密码点击登录  4. 登录成功  5. 点击界面上的下载链接  6. 点击页面上的500k页面测试  7. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### 国产浏览器双向SM2算法SSL访问

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **国产浏览器双向SM2算法SSL访问** | | |
| 功能描述 | 支持用户采用双向SM2算法SSL方式访问应用服务 | | |
| 预设条件 | 网关服务器存放SM2证书、用户ukey存放SM2证书、网关服务器双向SM2算法端口446 | | |
| 测试工具 | 国产浏览器，增加白名单 | | |
| 测试步骤 | 1. 增加国产浏览器白名单https://公网IP:446  2. 打开国产浏览器在地址栏输入地址：https://公网IP:446  3. 提示输入USBKEY pin码  4. 出现web界面，提示双向SM2算法SSL访问成功  5. 点击界面上的下载链接  5. 点击页面上的500k页面测试  6. 点击页面上的50个图片测试 | | |
| 预期结果 | 登录成功，下载文件成功，500k页面访问成功，50个图片测试访问成功 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

#### Crl验证

|  |  |  |  |
| --- | --- | --- | --- |
| **测试功能** | **Crl验证** | | |
| 功能描述 | 通过设置的CRL文件验证证书的有效性 | | |
| 预设条件 | 作废证书：zuofei.pfx 密码1，对应作废列表为crl7.crl，本地测试可采用将CRL导入方式进行校验、过期证书：guoqi123.pfx 密码1、正常证书：CHSG123.pfx 密码12345678 | | |
| 测试工具 | IE | | |
| 测试步骤 | 1. 网关后台设置为通过设置的CRL文件验证证书的有效性  2. 打开IE浏览器在地址栏输入地址：https://公网IP:444  3. 证书列表  4. 选择作废证书zuofei.pfx  5. 选择正常证书CHSG123.pfx | | |
| 预期结果 | 过期证书guoqi123.pfx不显示在证书列表，作废证书zuofei.pfx无法登录提示已被吊销或已作废，正常证书CHSG123.pfx登录正常 | | |
| 测试结果 |  | 是否通过 |  |
| 备注 |  | | |

以上测试用例需在以下环境通过测试：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 系统版本 IE版本 | IE6 | IE7 | IE8 | IE9 | IE10 | IE11 |
| Windows XP |  |  |  | —— | —— | —— |
| Windows 7 32位 | —— | —— |  |  |  |  |
| Windows 7 64位 | —— | —— |  |  |  |  |
| Windows 8 32位 | —— | —— | —— | —— |  |  |
| Windows 8 64位 | —— | —— | —— | —— |  |  |