# 4 安全要求

本章包含的部分安全功能要求以及附加的扩展功能组件来自于 Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4。

## 4.1 规定

CC 将安全功能组件的操作定义为：{{assignment}}，{{selection}}，{{selection}}下的{{assignment}}，{{refinement}}。这篇文档使用以下规定字体用于标识 CC 定义的这些操作。

* {{assignment}}：*斜体*；
* PP 作者制定的{{refinement}}：**粗体**的“{{refinement}}”，在元素编号之后，带有**粗体**标识的附加文字和删除线标识的删除部分（如有需要）；
* {{selection}}：下划线；
* {{selection}}下的{{assignment}}：*斜体* + 下划线；
* {{iteration}}：{{iteration}}号带有括号。

扩展的安全功能要求则使用 在对应的安全功能要求的名称后面加上“EXT”标签 的方法进行标识。

## 4.2 安全功能要求

本节列举 TOE 可能需要满足的安全功能要求。

### 4.2.1 类：用户数据保护（User Data Protection, FDP）

访问控制功能

FDP\_ACF\_EXT.1 扩展：本地存储和会话存储的区分

FDP\_ACF\_EXT.1 TOE 应基于域名、协议和端口对本地（永久）存储和会话（临时）存储进行区分：

* 会话存储只能被发起会话的标签页或 window 对象所访问；
* 本地存储只能被运行同一 web 应用的标签页或 window 对象所访问。

***Application Note:***

*本地存储和会话存储的区分在 World Wide Web Consortium (W3C) 的提案推荐标准（PR） "Web Storage" 中有被描述。*

*在本文中，域名是互联网上的权限管理控制的范围，子域名则表示为顶级域名加个前缀；协议是计算机内部或之间数据传输的数字规则系统，在 web 环境中典型的协议是 HTTP 和 HTTPS；端口是种“应用特定”构造，用于在主机的操作系统中充当通信端点，在 web 环境中80端口是 HTTP 通信的默认端口（也可以使用其他端口），在一个 web 地址中端口跟在域名或子域名的后面（如 http://www.cnn.com:80）。*

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以确保其阐明了 TSF 如何区分本地存储和会话存储。

**Guidance**

评估者应检验操作指南以确保其阐明了文件系统中用于本地存储的位置和用于会话存储的位置。

**Tests**

评估者应进行以下测试：

* 测试1：评估者应获得或创建 Javascript 脚本用于向本地/会话存储中存入信息并从中获取；还应搭建一个 web 服务器，包含两个或多个网页，使用不同的协议或端口。评估者应将脚本合并进网页中。评估者应使用两个或多个浏览器窗口打开同一个网页。评估者应验证，一个窗口中访问会话存储的脚本无法访问另一个窗口的会话存储。
* 测试2：用相同的 web 服务器，评估者应使用两个或多个浏览器标签页打开同一个网页。评估者应验证，一个标签页中访问会话存储的脚本无法访问另一个标签页的会话存储。
* 测试3：用相同的 web 服务器，评估者应使用两个或多个浏览器窗口打开同一个网页。评估者应验证，一个窗口中访问本地存储的脚本能够访问另一个窗口的本地存储。
* 测试4：用相同的 web 服务器，评估者应使用两个或多个浏览器标签页打开同一个网页。评估者应验证，一个标签页中访问本地存储的脚本能够访问另一个标签页的本地存储。
* 测试5：用相同的 web 服务器，评估者应使用浏览器窗口和标签页打开不同的网页。评估者应验证，运行在一个窗口或标签页中的一个域名/协议/端口下的网页上下文的脚本无法访问另一个窗口或标签页中的另一个域名/协议/端口下的存储信息。

cookie 管理

FDP\_COO\_EXT.1 扩展：cookie 阻止

FDP\_COO\_EXT.1.1 TOE 应能够阻止网站存储第三方 cookie。

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以确保其阐明了 TSF 如何阻止第三方 cookie 以及何时会阻止（例如，显然的是当此阻止功能被打开时）。

**Guidance**

评估者应检验操作指南以确保其为阻止第三方 cookie 提供了配置选项说明。

**Tests**

评估者应进行以下测试：

* 测试1：评估者应清除所有 cookie 然后配置 TOE 以允许第三方 cookie 的存储。评估者应载入一个存储第三方 cookie 的网页。评估者应前往 cookie 存储的位置并验证 cookie 是否已存在。
* 测试2：评估者应清除所有 cookie 然后配置 TOE 以禁止第三方 cookie 的存储。评估者应载入一个试图存储第三方 cookie 的网页并验证 cookie 是否未被存储。

信息删除

FDP\_DEL\_EXT.1 扩展：浏览器数据的删除

FDP\_DEL\_EXT.1.1 TOE 应能够让用户选择删除 TOE 的 [{{selection}}：浏览器缓存、历史、密码、web 表单信息、cookie、扩展程序、插件]。

FDP\_DEL\_EXT.1.2 TOE 应能够在浏览器退出时删除 TOE 的 [{{selection}}：浏览器缓存、历史、密码、web 表单信息、cookie、扩展程序、插件]。

***Application Note:***

*如果扩展程序或插件在上面 {{selection}} 中被选中，附录 C 里相应的基于 selection 的要求必须也被包含在 ST 的主体中。*

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以确保其阐明了浏览器内容存储在哪里、什么内容可被删除。TSS 也应描述浏览器退出时浏览器内容的删除过程。

**Guidance**

评估者应检验操作指南以确保其阐明了用户如何删除存储的内容以及哪些类型的内容可被选择删除。操作指南也应阐明以确保浏览器内容可在浏览器退出时被删除。

**Tests**

评估者应对每种类型的存储内容进行以下测试：

* 测试1：评估者应建立一个与 web 服务器的 web 会话（该会话创建并存储了内容）。评估者应验证：浏览器支持的类型的内容已被存储于（操作指南所阐明的）指定位置。然后评估者通过浏览器将内容删除，并验证：被存储的内容已从（操作指南所阐明的）指定位置被删除。
* 测试2：评估者应验证浏览器内容在文件系统特定位置。评估者应调用 TOE，通过它将内容删除，然后将 TOE 退出。评估者应前往（操作指南所阐明的）内容所在指定位置，验证存储的内容是否已被删除。

沙盒

FDP\_SBX\_EXT.1 扩展：渲染进程的沙盒机制

FDP\_SBX\_EXT.1.1 TOE 应确保网页渲染发生于一个符合以下限定条件的进程中：

* 渲染进程无法直接访问 TOE 平台所处的文件系统；
* 渲染进程无法直接和非 TOE 的进程进行进程间通信；
* The rendering process has reduced privilege with respect to other TOE processes [selection: [assignment: *methods by which the principle of least privilege is implement for rendering processes*], in no other ways].

***Application Note:***

*浏览器实现了多种方法以确保渲染 HTML 并解释执行 Javascript 的进程运行在一个受限的环境中，以降低该渲染进程被其处理的 HTML 或 Javascript 搞崩溃的风险。这个组件要求 TSF 确保渲染进程无法直接访问主机的文件系统而且无法参与主机提供的进程间通信机制（即不能与主机上非 TOE 的进程进行通信），以此降低渲染进程的权限。典型地，如果一个渲染进程需要访问一个文件或与一个非 TOE 进程通信，它必须通过 TSF 请求这样的访问（这是被这一安全要求所允许的）。*

*除了要求的两种措施，其他措施可以依赖 TOE 和主机平台进行实现。可能包含这些做法：将渲染进程的所有者换成一个低权限用户，或减弱渲染进程的平台定义级别（platform-defined）的权限。ST 作者填写 TOE 实现的这些额外措施。*

***Assurance Acitivity:***

**TSS**

评估者应检验 TSS 以确保其阐明了 TOE 在进程的角度上（进程是执行代码的有效实体）如何渲染 HTML 和解释执行 Javascript。对于渲染 HTML 和执行 Javascript 的进程，评估者应检验 TSS 以确保其阐明了这些进程是如何被阻止访问所在平台文件系统的。评估者应检验 TSS 以确保其阐明了平台提供的各种 IPC （进程间通信）机制，并对每种机制阐明渲染进程是如何被禁止使用该机制与非 TOE 进程通信的。评估者还应确认 TSS 阐明了 IPC 和文件系统如何可访问（如果 TOE 实现了这种可访问），例如可通过一个不负责网页渲染的更高权限的 TOE 进程。评估者应确保 TSS 中的这些阐述涵盖（适用） ST 中声明的所有平台。

对于 ST 作者在本组件的第三 bullet 中所列的每个附加的机制，评估者应检验 TSS 以确保：

1) 该机制被阐明了；2) 对该机制的详细阐述足够体现其对（渲染进程所实现的）最低权限原则（the principle of least privilege）的作用；3) TSS 适当提供了相应的辅助信息（或对这类信息资料的指向），为提到的最低权限原则提供上下文理解。

**Guidance**

评估者应检验操作指南以确保其阐明了对渲染进程的限制机制。此外，如果这样的机制可配置（例如，用户可以选择“启用”哪些机制），评估者应检验操作指南以确保“启用”和“禁用”这些机制的方法有被提供，并且这些操作的对应结果也有被描述。

**Tests**

注意：以下测试需要开发者提供给评估者一个测试平台，包括（普通消费者用户的平台版本中所没有的）调试和测试工具。

评估者应对 ST 中声明的每个平台进行以下测试：

* 测试1：评估者应使用调试或测试工具，向一个渲染进程导入代码，试图直接访问当前平台的文件系统，然后直接执行代码。评估者应确认这段代码的执行没能访问 TOE 文件系统。
* 测试2：对于 TSS 中阐述的每种 IPC 机制，评估者应使用调试或测试工具，向一个渲染进程导入代码，试图直接与平台上另一个非 TOE 的进程通信，然后直接执行代码。评估者应确认这段代码的执行没能达成目的。
* 测试3：对于 ST 中提到的每个附加机制，评估者应设计一个测试来证明这一机制的实际作用如 TSS 中所述。如果这样的测试无法做到，评估者应在测试报告中解释为什么这个机制无法测试。
* 测试4：对于每个可配置或可启用/禁用的机制，评估者应进行测试以确认这一机制配置起来和操作指南所说的一致。

同源策略

FDP\_SOP\_EXT.1 扩展：同源策略

FDP\_SOP\_EXT.1.1 TOE 应确保从一个源获取的内容无法与从另一个源获取的内容交互（在正被获取的内容的源没有允许的情况下）。

FDP\_SOP\_EXT.1.2 TOE 不应允许对不同域名有同源策略例外。

***Application Note:***

*同源策略的概念在 RFC 6454 的 "The Web Origin Concept" 中有相关描述。*

*源的定义是域名、协议、端口的组合。两个 URI 享有相同的域名、协议和端口，则被认为是同源。*

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以确保其阐明了其对同源策略的实现以及解释了其对 RFC 6454 的遵守。如果 TSF 允许对不同标签页或窗口的子域名放宽同源策略，则 TSS 应阐明这样的例外是如何实现的。

**Guidance**

N/A

**Tests**

评估者应进行如下测试：

* 测试1：评估者应获得或创建可从指定地址获取内容的脚本，并搭建一个 web 服务器（包含两个或多个网页代表不同域名）。评估者应将脚本合并入网页中。评估者应将每个页面关联到一个不同的协议和/或端口。评估者应打开两个或多个浏览器窗口并在各个窗口中打开网站的不同页面。评估者应运行脚本并验证：在一个窗口中运行的脚本无法访问另一个窗口中获取的内容。
* 测试2：使用同样的 web 服务器，评估者应打开两个或多个浏览器标签页并在各个标签页中打开网站的不同页面。评估者应运行脚本并验证：在一个标签页中运行的脚本无法访问另一个标签页中获取的内容。
* 测试3：如果 TSF 支持对子域名放宽同源策略，评估者应为 web 服务器配置子域名，重复测试1和测试2。评估者应验证：脚本能够从另一个窗口/标签页（其 URI 位于另一个子域名）获取内容。

安全的数据传输

FDP\_STR\_EXT.1 扩展：cookie 数据的安全传输

FDP\_STR\_EXT.1.1 TOE 应确保那些在 set-cookie 头中包含 "secure" attribute 的 cookie 是通过 HTTPS 发送的。

***Application Note:***

*set-cookie 头功能在 RFC 6265 "HTTP State Management Mechanism" 中有被阐述。*

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以验证其阐明了 TOE 依据 RFC 6265 支持在 set-cookie 头中包含 "secure" attribute 的 cookie 并通过 HTTPS 发送。

**Guidance**

N/A

**Tests**

评估者应进行如下测试：

* 测试1：评估者应将 TOE （通过 HTTPS）连到一个（实现了 HTTPS 的）“cookie 允许”（指该网站未被禁用 cookie）的测试网站，且该网站赋予了 TOE 一个 "secure" cookie。评估者应检验 TOE 的 cookie 缓存，确认包含那个 secure cookie。
* 测试2：评估者应再次连上那个 cookie 允许的网站，这次是通过不安全通道，确认没有 secure cookie 被发送。

用户跟踪信息

FDP\_TRK\_EXT.1 扩展：跟踪信息收集

FDP\_TRK\_EXT.1.1 TOE 应支持（即允许）网站收集关于 TOE 用户的 [{{selection}}: 所访问的网站，地理位置信息，系统配置，系统状态，出错情况，崩溃情况，[{{assignment}}: *其他跟踪信息*]]。

FDP\_TRK\_EXT.1.2 当一个网站请求跟踪信息时，TOE 应通知用户。

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以确保其描述了 TSF 对跟踪信息的支持并指明了 TOE 允许网站收集的关于 TOE 用户的跟踪信息。

**Guidance**

评估者应检验操作指南以确保其阐明了当一个网站请求跟踪信息时用户会收到的所有通知，以及收到通知后可作出的选择。

**Tests**

评估者应对 TSS 中列出的每种类型的跟踪信息进行如下测试：

- 测试1：评估者应配置一个请求用户跟踪信息的网站并导航到（即在浏览器中打开）该网站。评估者应确认用户收到了关于跟踪信息请求的通知，并且在用户选择允许后，网站获得了跟踪信息。

### 4.2.2 类：TSF 保护（Protection of the TSF, FPT）

TOE 的下载内容

FPT\_DNL\_EXT.1 扩展：下载的可执行内容的启动

FPT\_DNL\_EXT.1.1 TOE 应阻止下载的可执行内容的自动启动。

FPT\_DNL\_EXT.1.2 TOE 应给用户下载或丢弃可执行内容的选择。

***Application Note:***

*在本文中，可执行内容是一个包含了某个软件程序的编译后的代码（一旦启动将进行程序的安装）的文件。它的调用是独立的、在 TOE 的环境之外的，并不含有移动代码（mobile code）、脚本或插件。*

*本组件（即要求）不包括已安装在 TOE 平台的程序的调用。*

*本组件确保，如果用户故意（通过点击一个链接）或无意地开始下载一个可执行内容，TSF 会进行干预，例如打开一个对话框让用户选择是保存可执行内容到文件系统还是不下载它。*

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以确保其阐明了当用户开始下载可执行内容时 TSF 的行为。

**Guidance**

评估者应检验操作指南以确保其阐明了当下载开始时出现的对话框以及对话框中呈现的选项的含义。

**Tests**

评估者应进行如下测试：

* 测试1：评估者应导航到一个含有可执行内容的网站并试图下载、启动若干个可执行内容。评估者应验证，TOE 总能呈现一个对话框让用户选择将可执行内容下载到文件系统或丢弃。

FPT\_DNL\_EXT.2 扩展：下载位置

FPT\_DNL\_EXT.2.1 TOE 应能指明下载内容的保存位置。

***Assurance Activity:***

**TSS**

N/A

**Guidance**

评估者应检验操作指南以确保其阐明了下载内容的默认保存位置以及如何（由用户）修改该位置。

**Tests**

评估者应进行如下测试：

* 测试1：评估者应导航到一个提供文件下载的网站并下载一个文件。评估者应检查操作指南中指定的默认下载位置并确认下载内容是在该位置。
* 测试2：评估者应修改下载文件的保存位置。评估者应试着从一个提供文件下载的网站下载一个文件，确认该文件被保存到之前配置的位置。

外部交互

FPT\_INT\_EXT.1 扩展：与后台进程的交互

FPT\_INT\_EXT.1.1 扩展：TOE 应在退出时关闭所有由 TOE 产生的后台进程。

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以确保其阐明了 TOE 运行时所有由 TOE 产生的进程，以及 TOE 退出时能够关闭这些进程。TSS 还应阐明这些后台进程的实质、何种情况下会产生、与其相关联的 process/image 名字以及期望的生命周期。

**Guidance**

N/A

**Tests**

评估者应进行如下测试：

* 测试1：评估者应启动一个 TOE 实例。评估者应检查 TOE 平台正在运行的进程并识别哪些与 TOE 实例相关联。评估者应关闭 TOE 实例并确认 TOE 后台进程都已经终结。

移动代码

FPT\_MCD\_EXT.1 扩展：移动代码

FPT\_MCD\_EXT.1.1 TOE 应能执行签名的 [{{selection}}: ActiveX、Flash、Java、JavaScript、[{{assignment}}: TOE 支持的其他类型移动代码]] 移动代码。

FPT\_MCD\_EXT.1.2 TOE 应能执行未签名的 [{{selection}}: ActiveX、Flash、Java、JavaScript、[{{assignment}}: TOE 支持的其他类型移动代码]] 移动代码。

FPT\_MCD\_EXT.1.3 TOE 应能执行不可信或未验证的来源的 [{{selection}}: ActiveX、Flash、Java、JavaScript、[{{assignment}}: TOE 支持的其他类型移动代码]] 移动代码。

FPT\_MCD\_EXT.1.4 当遇到未签名的、不可信的或未验证来源的移动代码时，TOE 应通知用户。

FPT\_MCD\_EXT.1.5 TOE 应能让用户可选择丢弃未签名的、不可信的或未验证来源的移动代码而不去执行它。

***Application Note:***

*ST 作者必须指明浏览器支持的所有的移动代码类型。如果它们没被列出，ST 作者必须将缺失的移动代码类型填写在 assignment 中。*

*一个经授权的签名者（？）可能直接将代码自身签名，或者代码可能通过一个验证的 HTTPS 连接随着一个经授权的实体被传送。*

*FIA\_X509\_EXT.2 对签名的移动代码的执行作了说明。*

***Assurance Activity:***

**TSS**

评估者应检验 TSS 以确保其列出了 TSF 支持的签名的移动代码的类型。TSS 应阐明 TSF 如何处理未签名的移动代码、不可信来源的移动代码和未验证来源的移动代码。

**Guidance**

评估者应检验操作指南以确认其为每种支持的移动代码类型都提供了配置说明。操作指南还应阐明当遇到未签名的、不可信的或未验证的移动代码时 TOE 会显示怎样的警告以及用户可以采取怎样的措施。

**Tests**

评估者应对 TSS 中指定的每种移动代码的类型进行如下测试：

* 测试1：评估者应构建一个包含未签名的、正确验证的、不正确验证的移动代码，并确保：当 TOE 遇到未能通过验证的移动代码时 TOE 对用户发出了警报并让用户能选择丢弃移动代码而不执行它，若遇到正当验证的移动代码则执行它。

## 4.3 TOE 或 TOE 平台安全功能要求

本节列举了 TOE 本身、TOE 平台或两者结合可能需要满足的安全功能要求。

### 4.3.1 类：密码支持（Cryptographic Support, FCS）

密钥管理

FCS\_CKM.1 密钥生成

FCS\_CKM.1(1) 密钥生成（用于建立钥匙（key establishment））

FCS\_CKM.1.1(1) 细化：[{{selection}}: TOE，TOE 平台] 应该生成不对称密钥**用于建立钥匙**，根据：

* NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [{{selection}}: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")
* NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes

[{{selection}}:

* NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes
* 无其他方案

]

以及指定的密钥大小（大于等于一个112位的对称密钥强度）。

***Application Note:***

*本组件要求 TSF 或 TOE 平台能够为 TOE 的多种加密协议（cryptographic protocol，如 trusted channel）生成用于建立钥匙的公钥私钥对。如果支持多种方案，那么 ST 作者应该重复本要求，以实现这样的能力（？）。所用的方案会被 ST 作者从 {{selection}} 中选择。由于 the domain parameters to be used are specified by the requirements of the protocol in this PP，不需要 TOE 生成 domain parameters，因此当 TOE 遵守本 PP 中指定的协议时没有必要对 domain parameter 额外验证。*

*生成的2048位 DSA 和 RSA 密钥强度（？）需要大于等于一个112位的对称密钥强度。同等密钥强度的信息参见 NIST Special Publication 800-57, "Recommendation for Key Management"。*

*RSA 和基于椭圆曲线的方案是需要的，为了遵守 FCS\_TLCS\_EXT.1 中要求的密码套件（**ciphersuites）。*

***Assurance Activity:***

**TSS**

TOE 平台满足的要求：评估者应检验平台的 ST 以确保该平台的 ST 中声明的钥匙建立包含 Web 浏览器的 ST 中的钥匙建立要求。评估者还应检验 Web 浏览器的 ST 的 TSS 以确认其（对每个支持的平台）阐明了钥匙建立功能是怎样调用的（应当注意，这个调用可能是通过一个不是由 Web 浏览器所实现的机制，但这个机制会在 TSS 中作为 assurance activity 中的一部分被说明）。

**Guidance**

N/A

**Tests**

TOE 满足的要求：

评估者应检验钥匙生成算法实现和 TOE 使用的钥匙建立方案。

**Key Generation:**

评估者应使用以下的可行测试来检验支持的方案的钥匙生成算法（？）实现。

基于 RSA 的钥匙建立方案的钥匙生成：

评估者应使用钥匙生成测试来检验 TOE 实现的 RSA 钥匙生成。这个测试检验的是 TSF 正确产生（RSA 算法中的）关键值的能力，关键值包括：the public verification exponent e, the private prime factors p and q, the public modulus n, the calculation of the private signature exponent d。

钥匙对生成有5种特定方法生成质数 p 和 q，如下：

* 随机质数：
  + 可证质数（provable primes）
  + 可能质数（probable primes）
* 条件质数：
  + 质数 p1, p2, q1, q2, p, q 都应是可证质数
  + 质数 p1, p2, q1, q2 应是可证质数，p 和 q 应是可能质数
  + 质数 p1, p2, q1, q2, p, q 都应是可能质数

为了随机可证质数法和所有条件质数法的钥匙生成方法的测试，评估者应使用充分的数据来设计验证 TSF 钥匙生成程序（？），以可靠地生成 RSA 钥匙对。这包括随机数种子、the public exponent of the RSA key，以及期望的钥匙长度。对每个支持的钥匙长度，评估者应让 TSF 生成25个钥匙对。评估者应通过比较 TSF 生成的值和一个已有的较好的实现方法生成的值，来检验 TSF 的实现方法的正确性。

基于有限域加密（Finite-Field Cryptography, FFC）的56A方案（？）的钥匙生成

FFC 参数和钥匙生成测试

评估者应通过参数生成和钥匙生成测试来验证 TOE 实现的 FFC 参数生成和钥匙生成。这个测试验证 TSF 是否能够正确产生这些值：the field prime p, the cryptographic prime q (dividing p-1), the cryptographic group generator g, and the calculation of the private key x and public key y。

参数生成有两种特定方法生成 the cryptographic prime q 和 the field prime p：

* Cryptographic and Field Primes:
  + Primes q and p shall both be provable primes
  + Primes q and field prime p shall both be probable primes

和两种方法生成 the cryptographic group generator g：

* Cryptographic Group Generator:
  + Generator g constructed through a verifiable process
  + Generator g constructed through an unverifiable process

钥匙生成有两种特定方法生成私钥 x：

* 私钥：
  + len(q) bit output of RBG where 1 <= x <= q-1
  + len(q) + 64 bit output of RBG, followed by a mod q-1 operation where 1 <= x <= q-1

RBG 的安全强度必须至少是 FFC 参数集的安全强度。

为了测试可证质数法的 the cryptographic and field prime 生成方法，和/或一个可验证过程（？）的群生成器 g，评估者必须使用充分的数据来设计验证 TSF 参数生成程序（？），以可靠地生成参数集。

对每个支持的钥匙长度，评估者应让 TSF 生成25个参数集和钥匙对。评估者应通过比较 TSF 生成的值和一个已有的较好的实现方法生成的值，来检验 TSF 的实现方法的正确性。检验过程还必须对每个 FFC 参数集和钥匙对证实以下几点：

* g != 0,1
* q divides p-1
* g^q mod p = 1
* g^x mod p = y

基于椭圆曲线密码学（Elliptic Curve Cryptography, ECC）的56A方案（？）的钥匙生成

*ECC 钥匙生成测试*

对每种支持的 NIST 曲线，即 P-256、P-284 和 P-521，评估者应要求被测试实现（implementation under test, IUT）生成10个公钥/私钥对。私钥应使用一个受认可的随机位生成器（random bit generator, RBG）生成。为确保正确性，评估者应把生成的钥匙对提交给一个已有的较好实现方案的公钥检验（public key verification, PKV）功能（进行检验认证）。

*ECC 公钥检验（public key verification, PKV）测试*

对每种支持的 NIST 曲线，即 P-256、P-284 和 P-521，评估者应通过一个已有的较好实现方案的钥匙生成功能来生成10个公钥/私钥对，并修改其中5个公钥的值使之不正确，其他5个不变（保持正确）。评估者应（对其进行 PKV 检验，结果）得到10个 PASS/FAIL 值。

**钥匙建立方案**

评估者应通过以下可行的测试对 TOE 支持的钥匙建立方案的实现进行检验。

SP800-56A 钥匙建立方案

…………

*功能测试*

…………

*有效性测试*

…………

SP800-56 钥匙建立方案

…………

FCS\_CKM\_EXT.1 扩展：加密存储

FCS\_CKM\_EXT.1.1 [{{selection}}：TOE，TOE 平台] 应在平台提供的密钥存储库中存储持久隐私、私钥、[{{assignment}}：*敏感的 web 表单数据*] 和 "secure" cookies （当这些数据不在被使用）。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

N/A

**Tests**

N/A

FCS\_CKM\_EXT.4 扩展：密钥归零

FCS\_CKM\_EXT.4.1 [{{selection}}：TOE，TOE 平台] 应将所有明文隐私数据、密钥和加密服务提供者（Cryptographic Service Provider, CSP）置零（当这些不再被需要）。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

N/A

**Tests**

…………

加密操作

FCS\_COP.1(1) 加密操作（对于加密/解密）

FCS\_COP.1.1(1) [{{selection}}：TOE，TOE 平台] 应执行 [加密/解密]，依据一个指定的加密算法：

* AES-CBC（如 NIST SP 800-38A 中所定义）模式；

[{{selection}}:

* AES-GCM（如NIST SP 800-38D 中所定义）
* 无其他模式

]

并且密钥大小为128位、256位。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

N/A

**Tests**

…………

FCS\_COP.1(2) 加密操作（对于哈希加密）

FCS\_COP.1.1(2) [{{selection}}：TOE，TOE 平台] 应执行哈希加密，依据一个指定的加密算法：

* SHA-1;
* SHA-256;
* SHA-384;
* [{{selection}}: SHA-512，无其他算法] 并且消息摘要（message digest）的大小为160、256、384和 [{{selection}}: 512，无其他大小]，满足：FIPS PUB 180-4。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

N/A

**Tests**

…………

FCS\_COP.1(3) 加密操作（对于数字签名）

FCS\_COP.1.1(3) [{{selection}}：TOE，TOE 平台] 应依据以下指定的加密算法执行加密签名服务：

* RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater that meets FIPS PUB 180-2 or FIPS-PUB 186-4, "Digital Signature Standard";
* Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater that meets FIPS PUB 186-4, "Digital Signature Standard" with "NIST curves" P-256, P-384 and [{{selection}}: P-521，无其他曲线]（如 FIPS PUB 186-4, "Digital Signature Standard" 中所定义）；

[{{selection}}:

* Digital Signature Algorithm (DSA) with a key size (modulus) of 2048 bits or greater that meets FIPS-PUB 186-4, "Digital Signature Standard";
* 无其他加密签名服务

]。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

N/A

**Tests**

…………

FCS\_COP.1(4) 加密操作（密钥相关的哈希运算消息认证（Keyed-Hash Message Authentication））

FCS\_COP.1.1(4) [{{selection}}：TOE，TOE 平台] 应执行密钥相关的哈希运算消息认证，依据一个指定的加密算法：

* HMAC- SHA-256

[{{selection}}:

* SHA-1
* SHA-384
* SHA-512
* 无其他算法

]，

密钥大小为 [{{assignment}}: *key size (in bits) used in HMAC*]，并且消息摘要（message digest ）大小为256和 [{{selection}}: 160，384，512，无其他大小] 位，满足：FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code" 和 FIPS Pub 180-4, "Secure Hash Standard"。

***Application Note:***

*…………*

***Assurance Activity:***

…………

**Guidance**

N/A

**Tests**

…………

安全超文本传输协议（HTTPS）

FCS\_HTTPS\_EXT.1 扩展：HTTPS 实现

FCS\_HTTPS\_EXT.1.1 [{{selection}}：TOE，TOE 平台] 应遵照 RFC 2818 实现 HTTPS 协议。

FCS\_HTTPS\_EXT.1.2 [{{selection}}：TOE，TOE 平台] 应使用 FCS\_TLSC\_EXT.1 中说明的 TLS 实现 HTTPS。

***Assurance Activity:***

…………

随机位生成（Random Bit Generation, RBG）

FCS\_RBG\_EXT.1 扩展：随机位生成

FCS\_RBG\_EXT.1.1 [{{selection}}：TOE，TOE 平台] 应执行所有确定性随机位生成服务，依据 [{{selection}}: 二选一：NIST Special Publication 800-90A using [{{selection}}: Hash\_DRBG (any), HMAC\_DRBG (any), CTR\_DRBG (AES), Dual\_EC\_DRBG (any)]；FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES]。

FCS\_RBG\_EXT.1.2 确定性随机位生成的随机种子应取自一个熵源（entropy source），熵源累积的熵来自 [{{selection}}: 一个基于软件的噪声源（noise source），一个基于平台的 RBG]，其最小的熵是 [{{selection}}: 128位，256位] 的，至少同等于它会生成的密钥和 hash 的最大安全强度（根据 NIST SP 800-57）。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

N/A

**Tests**

…………

传输层安全（TLS）

FCS\_TLSC\_EXT.1 扩展：传输层安全

FCS\_TLSC\_EXT.1.1 [{{selection}}：TOE，TOE 平台] 应实现 TLS 1.2 (RFC 5246)，支持以下密码套件（ciphersuites）：

**强制支持的密码套件：**

* TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA，如 RFC 3268 中所定义
* TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256，如 RFC 5289 中所定义
* TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384，如 RFC 5289 中所定义

**可选支持的密码套件：**

[{{selection}}:

* TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA，如 RFC 3268 中所定义
* TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA，如 RFC 3268 中所定义
* TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA，如 RFC 3268 中所定义
* TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA，如 RFC 4492 中所定义
* TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA，如 RFC 4492 中所定义
* TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA，如 RFC 4492 中所定义
* TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA，如 RFC 4492 中所定义
* TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256，如 RFC 5246 中所定义
* TLS\_RSA\_WITH\_AES\_256\_CBC\_ SHA256，如 RFC 5246 中所定义
* TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_ SHA256，如 RFC 5246 中所定义
* TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_ SHA256，如 RFC 5246 中所定义
* TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256，如 RFC 5289 中所定义
* TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384，如 RFC 5289 中所定义
* 无其他密码套件

]。

***Application Note:***

*…………*

FCS\_TLSC\_EXT.1.2 如果一个证书中包含的别名（distinguished name, DN）和端的期望的别名不相匹配，TOE 不应建立可信通道。

***Application Note:***

*…………*

FCS\_TLSC\_EXT.1.3 TOE 应在客户端问候消息（the Client Hello）中的签名算法扩展（the signature\_algorithm extension）中采用以下 hash 算法：[{{selection}}: SHA256, SHA384, SHA512] 并且没有其他 hash 算法。

***Application Note:***

*…………*

FCS\_TLSC\_EXT.1.4 TOE 应在客户端问候消息（the Client Hello）中支持的椭圆曲线扩展（the Supported Elliptic Curves Extension）中采用以下 NIST 曲线：[{{selection}}: secp256r1, secp384r1, secp521r1] 并且没有其他曲线。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

…………

**Tests**

…………

### 4.3.2 类：识别与认证（Identification and Authentication, FIA）

X509 证书

FIA\_X509\_EXT.1 扩展：X509 验证（validation）

FIA\_X509\_EXT.1.1 [{{selection}}：TOE，TOE 平台] 应根据以下规则验证证书：

* RFC 5280 证书认证和证书路径认证。
* TSF 应确保基本约束扩展（the basicConstraints extension）存在、CA 标记对所有CA证书都设成 TRUE，以此验证一个证书路径。
* TSF 应使用 [{{selection}}: RFC 2560中指定的在线证书状态协议（Online Certificate Status Protocol, OCSP），RFC 5759中指定的一个证书废止列表（Certificate Revocation List, CRL）] 来验证证书的撤销状态。
* TSF 应验证 extendedKeyUsage 字段，依据以下规则：
  + 用于可信更新和可执行代码完整性检验的证书，应带有代码签名目的（the Code Signing purpose）(id-kp 3 with OID 1.3.6.1.5.5.7.3.3)。
  + 提交给 TLS 的服务器证书，应在extendedKeyUsage 字段中带有服务器身份认证目的（the Server Authentication purpose）(id-kp 1 with OID 1.3.6.1.5.5.7.3.1)。

***Application Note:***

*…………*

FIA\_X509\_EXT.1.2 如果基本约束扩展存在并且 CA 标记被设为 TRUE，[{{selection}}：TOE，TOE 平台] 应只把一个证书当作一个 CA 证书。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

N/A

**Tests**

…………

FIA\_X509\_EXT.2 扩展：X509 认证（authentication）

FIA\_X509\_EXT.2.1 [{{selection}}：TOE，TOE 平台] 应按照 RFC 5280 中的定义，使用 X.509v3 证书来支持 HTTPS、TLS 和 [{{selection}}: DTLS，无其他协议] 协议下的认证，和 TOE 更新的代码签名、用于移动代码安装的代码签名和 [{{selection}}: 用于扩展安装的代码签名，用于插件安装的代码签名，无额外用途]。

***Application Note:***

*…………*

FIA\_X509\_EXT.2.2 当 [{{selection}}：TOE，TOE 平台] 无法建立连接以确定证书的有效性，[{{selection}}：TOE，TOE 平台] 应 [{{selection}}: 允许管理员选择是否在这种情况下接受证书，接受证书，不接受证书]。

***Application Note:***

*…………*

FIA\_X509\_EXT.2.3 如果端证书在可信信道建立过程中被认为无效，[{{selection}}：TOE，TOE 平台] 应通知用户。

***Application Note:***

*…………*

FIA\_X509\_EXT.2.4 如果代码签名证书被认为无效，[{{selection}}：TOE，TOE 平台] 不应安装运行代码。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

…………

**Tests**

…………

### 4.3.3 类：安全管理（Security Management, FMT）

TSF 功能管理

FMT\_MOF.1 Management of Functions Behavior

FMT\_MOF.1.1 [{{selection}}：TOE，TOE 及其平台] 应根据管理员策略，将执行以下功能的能力限定于管理员：

1. 启用/禁用 敏感 web 表单信息的存储；
2. 移动代码的配置：
   1. 安装移动代码的能力；
   2. 卸载移动代码的能力；
   3. 更新移动代码的能力；
   4. 执行未签名移动代码的能力；
   5. 从不可信或未认证的发布者处执行移动代码的能力

[{{selection}}:

1. 启用/禁用 第三方 cookie 的存储；
2. 扩展程序的配置：
   1. 安装扩展的能力；
   2. 卸载扩展的能力；
   3. 更新扩展的能力；
   4. 禁用扩展的能力
3. 插件的配置：
   1. 安装插件的能力；
   2. 卸载插件的能力；
   3. 更新插件的能力；
   4. 禁用插件的能力
4. 启用/禁用 OSCP（Online Certificate Status Protocol，在线证书状态协议）获得一个 X.509 证书的撤销状态；
5. 配置 HTTP 头中 user-agent 信息的夹带内容；
6. 允许/禁止 网站收集关于用户的跟踪信息；
7. 删除存储的浏览数据（缓存、web 表单信息）：
   1. 指定哪些内容应删除的能力；
   2. 删除所有存储内容的能力；
   3. 浏览器会话终止时自动删除内容
8. 启用/禁用 敏感信息在持久存储中的存储；
9. 指定下载文件保存到磁盘的位置的能力；
10. 配置 cookie 缓存（？）的大小；
11. 允许/禁止 与 GPU（Graphic Processing Units）交互；
12. 配置在 X.509 证书无效或未验证时访问网站的能力；
13. 启用/禁用隐私浏览会话（private browsing session）；
14. 配置使用一个应用程序评价服务（application reputation service），用于在下载之前检测出恶意程序；
15. 配置使用一个 URL 评价服务（URL reputation service），用于检测含有恶意或钓鱼内容的站点；
16. 允许/禁止 软件更新和补丁的自动安装；
17. 允许/禁止 建立可信通道，如果 TSF 无法建立连接验证证书；
18. 允许/禁止 网站注册协议处理器（protocol handler）

]。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

…………

**Tests**

…………

管理功能规范

FMT\_SMF.1 管理功能规范

FMT\_SMF.1.1 [{{selection}}：TOE，TOE 及其平台] 应能够执行以下管理功能：

1. 启用/禁用 敏感 web 表单信息的存储；
2. 启用/禁用 第三方 cookie 的存储；
3. 配置 HTTP 头中 user-agent 信息的夹带内容；
4. 允许/禁止 网站收集关于用户的跟踪信息；
5. 删除存储的浏览数据（缓存、web 表单信息）：
   1. 指定哪些内容应删除的能力；
   2. 删除所有存储内容的能力；
   3. 浏览器会话终止时自动删除内容
6. 移动代码的配置：
   1. 安装移动代码的能力；
   2. 卸载移动代码的能力；
   3. 更新移动代码的能力；
   4. 执行未签名移动代码的能力；
   5. 从不可信或未认证的发布者处执行移动代码的能力
7. 指定下载文件保存到磁盘的位置的能力；
8. 配置 cookie 缓存（？）的大小；
9. 允许/禁止 在 X.509 证书无效或未验证时访问网站；
10. 允许/禁止 软件更新和补丁的自动安装；

[{{selection}}:

1. 扩展程序的配置：
2. 安装扩展的能力；
3. 卸载扩展的能力；
4. 更新扩展的能力；
5. 禁用扩展的能力
6. 插件的配置：
7. 安装插件的能力；
8. 卸载插件的能力；
9. 更新插件的能力；
10. 禁用插件的能力
11. 启用/禁用 敏感信息在持久存储中的存储；
12. 启用/禁用 OSCP 获得一个 X.509 证书的撤销状态；
13. 允许/禁止 与 GPU 交互；
14. 启用/禁用隐私浏览会话；
15. 配置使用一个应用程序评价服务，用于在下载之前检测出恶意程序；
16. 配置使用一个 URL 评价服务，用于检测含有恶意或钓鱼内容的站点；
17. 允许/禁止 建立可信通道，如果 TSF 无法建立连接验证证书；
18. 允许/禁止 网站注册协议处理器（protocol handler）

]。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

…………

**Tests**

…………

FMT\_SMR.1 安全管理角色

FMT\_SMR.1.1 [{{selection}}：TOE，TOE 平台] 应维护角色：管理员。

FMT\_SMR.1.2 [{{selection}}：TOE，TOE 平台] 应能够将用户和角色结合。

***Assurance Activity:***

**TSS**

…………

**Guidance**

…………

**Tests**

…………

### 4.3.4 类：TSF 保护（Protection of the TSF, FPT）

TSF 自检（Self-Test）

FPT\_TST\_EXT.1 扩展：TSF 自检

FPT\_TST\_EXT.1.1 [{{selection}}：TOE，TOE 平台] 在打开电源初次启动过程中应该运行一套自检程序，以确保其完整的可执行性和数据。

***Assurance Activity:***

**TSS**

…………

**Guidance**

N/A

**Tests**

…………

可信更新

FPT\_TUD\_EXT.1 扩展：可信的软件更新和补丁

FPT\_TUD\_EXT.1.1 [{{selection}}：TOE，TOE 平台] 应能够（让用户）查询TOE 软件，[selection: 扩展，插件，无其他附加组件] 的当前版本号。

FPT\_TUD\_EXT.1.2 [{{selection}}：TOE，TOE 平台] 应能够启动对TOE 软件，[selection: 扩展，插件，无其他附加组件] 的更新和补丁。

FPT\_TUD\_EXT.1.3 [{{selection}}：TOE，TOE 平台] 应有办法在安装 TOE 的软件更新和补丁、[{{selection}}: 扩展更新，插件更新，无其他更新] 之前，使用一个数字签名机制和 [{{selection}}: published hash，无其他方法] 对其进行验证。

FTP\_TUD\_EXT.1.4 [{{selection}}：TOE，TOE 平台] 应能够让 TOE 的更新和补丁、[{{selection}}: 扩展，插件，无其他附加组件] 验证后自动安装。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

…………

**Tests**

…………

### 4.3.5 类：可信路径/通道（Trusted Path/Channel, FTP）

可信通道

FTP\_ITC.1 TSF 间的可信通道

FTP\_ITC.1 **Refinement**: [{{selection}}：TOE，TOE 平台] 应使用 **[selection: HTTPS, TLS, DTLS]** 协议在自身和另一个可信的 IT 产品之间提供一个在逻辑上（？）不同于其他通信通道的**可信的**通信通道，并能提供结束点的明确标识、保护通道数据不被暴露、检测通道数据的修改。

FPT\_ITC.1.2 [{{selection}}：TOE，TOE 平台] 应允许 TSF 通过可信通道发起通信。

FPT\_ITC.1.3 [{{selection}}：TOE，TOE 平台] 应通过可信通道发起通信，为所有通过该连接的通信量。

***Application Note:***

*…………*

***Assurance Activity:***

**TSS**

…………

**Guidance**

…………

**Tests**

…………