A. 安全

# OCPP 安全

此功能块描述了 OCPP 协议的安全要求。安全部分的开发是为了加强和完善 OCPP的未来发展和 标准化。 它基于 LaQuSo的端到端安全设计[21]。充电站和CSMS的安全措施中包括了安全要求，以支持OCPP的用户。

## 安全 目标

*本节仅供参考。*

OCPP 安全性 旨在 满足 以下 安全 目标：

1. 允许在 CSMS和充电站之间创建安全的通信通道。 应使用强加密措施 保护此通道 上消息的完整性和机密性。
2. 在充电站和 CSMS 之间 提供相互身份验证。 双方都 应该能够 识别 他们正在与谁沟通。
3. 通过允许 充电站 检查 固件映像的来源和 完整性，并允许 这些映像的不可否认性， 来提供安全的固件更新过程。
4. 允许记录 安全事件，以方便监控 智能充电系统的安全性。 附录中 提供了 安全相关事件 及其“关键性”的列表。

## 设计 注意事项

*本节内容丰富。*

安全功能块 旨在 适应OCPP中采用 的方法。 尽可能 使用标准 Web 技术 ，以便使用可用的 Web 库和软件实现经济高效的实现。 不包括任何应用层 安全措施。基于这些注意事项，OCPP 安全性基于使用 X.509 证书的 TLS 和公钥加密。 由于CSMS通常充当服务器，因此该标准中没有实现充电站上的不同用户或基于角色的访问控制。为了缓解这种情况，建议在CSMS上实现访问控制。为了确保在那里实施的机制不能 被绕过， OCPP不应该 由合格的 人员使用，以便在充电站本地对充电Stations进行维护，因为 其他协议 可用于 本地维护目的。

## 安全 配置文件

本节定义 不同的 OCPP 安全配置文件及其 要求。 OCPP 2.0.1 支持三种安全配置文件： 下表显示了哪个配置文件使用哪些 安全措施。

*表 11. OCPP 安全配置文件*  *概述*

|  |  |  |  |
| --- | --- | --- | --- |
| **轮廓** | **充电 站 认证** | **网信**  **认证** | **通信 安全** |
| **1. 使用基本身份验证的不安全传输** | 基本身份验证 | - | - |
| **2. 带基本身份验证**的 **TLS** | 基本身份验证 | 使用证书进行 TLS 身份验证 | 传输 层 安全性 （TLS） |
| **3. 带有客户端 证书的 TLS** | 使用证书进行 TLS 身份验证 | 使用证书进行 TLS 身份验证 | 传输 层 安全性 （TLS） |

* “使用基本身份验证配置文件的不安全传输 ” 不包括 对 CSMS 的身份验证，也不包括设置 安全通信通道的措施。 因此， 它 只应在受信任的网络 中使用， 例如在CSMS和充电站之间有VPN的网络中。 对于现场操作， 强烈建议 将安全配置文件与 TLS 结合使用。
* 在某些情况下 （例如实验室安装、测试设置等） 人们可能更喜欢 使用OCPP 2.0.1而不实现安全性。 虽然 这是 可能的，但它 不被视为有效的 OCPP 2.0.1 实现。

### 通用 安全 配置文件 要求

*表 12. 通用 安全 配置文件 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.001 |  | 充电站和CSMS一次只能使用一个安全配置文件 |
| 答00.FR.002 | 如果充电站尝试使用与 CSMS 使用的配置文件不同的配置文件进行连接 | 网吧点点通应终止 连接。 |
| 答00.FR.003 | 如果 CSMS 尝试使用与充电站使用的配置文件不同的配置文件进行连接 | 充电站应终止 连接。 |
| 答00.FR.004 |  | 应在 OCPP 通信开始之前配置安全配置文件。 |
| 答00.FR.005 |  | 将使用的安全配置文件降低到安全性较低的配置文件是出于安全原因，而不是 OCPP 规范的一部分，并且必须 通过另一种方法完成，而不是通过 OCPP 完成。OCPP 消息不得 用于此目的（例如 SetVariablesRequest 或 DataTransferRequest）。 |
| 答00.FR.006 | 当CSMS与具有不同安全配置文件或不同版本的OCPP 的充电站进行通信时。 | CSMS可以通过 不同的地址或  网吧点点通的端口。  例如， CSMS 服务器可能有 一个用于 TLS 的 TCP 端口，用于基本端口  身份验证，以及用于具有客户端 证书的 TLS 的另一个端口。  在这种情况下 ， CSMS 的每个端口 仅使用一个安全配置文件，这是 允许的。 |

### 使用基本身份验证配置文件的不安全传输 - 1

*表 13. 安全配置文件 1 - 具有基本身份验证的不安全传输*

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **1** | **名字** | 具有基本身份验证的不安全传输 |
| **2** | **型 材编号** | 1 |
| **3** | **描述** | “带基本身份验证的不安全传输”配置文件提供 的安全级别较低。 充电站身份验证 通过 用户名和密码完成。 未包含 任何措施来保护 通信通道。 |
| **4** | **充电 站 认证** | 对于 充电 站 身份验证 ，使用 HTTP 基本 身份验证 。 |

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **5** | **网吧点点 通认证** | 在此配置文件中， CSMS 不会 向充电站验证自身身份。 充电 站必须 相信 它 所连接的服务器确实是CSMS。 |
| **6** | **通信 安全** | 配置文件中 不包含任何通信安全措施 。 |

充电 站

网信

|  |  |
| --- | --- |
| HTTP GET / ProtectedData （明 文 通信） | |
|  | 需要 HTTP/401 授权 |
|  | HTTP GET / ProtectedData Authorization 基本 用户名 / 密码 |
|  | HTTP 200 / 受保护的数据 |
|  | 应用程序 数据 |
|  | |

*图 2. 序列 图： HTTP 基本 身份验证 序列 图*

|  |  |  |
| --- | --- | --- |
| **7** | **备注** | 不适用 |

### 使用基本身份验证配置文件的不安全传输 - 要求

*表 14. 安全配置文件 1 - 使用基本身份验证的不安全传输 - 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.201 |  | “具有基本身份验证配置文件的不安全传输” 应仅在 受信任的网络中使用。 |
| 答00.FR.202 |  | 充电站应使用HTTP基本身份验证向CSMS 验证自身身份[18] |
| 答00.FR.203 | 答00.FR.202 | 客户端（即 充电站）应在 每次连接请求中提供 用户名和密码。 |
| 答00.FR.204 | 答00.FR.203 | 用户名应 等于 充电站标识，该标识是充电站的标识字符串，因为它在 OCPP-J 连接 URL 中使用它。 使用基本身份验证 时，充电站标识可能 不包含 字符“：”。 否则，网吧点点通 可能无法将用户名与 密码分开。 |
| 答00.FR.205 | 答00.FR.203 | 密码应存储在基本密码配置变量中。它应是随机选择的标识符字符串，具有 足够高的熵，由最少16个字符和最多40个字符组成（字母数字字符和标识符字符串允许的特殊字符）。密码 SHALL 以 UTF-8 编码字符串的形式发送（未编码为八位字节字符串或 base64）。 |
| 答00.FR.206 | 答00.FR.203 | 使用 HTTP Basic，用户名和密码以明文形式传输，仅以 base64 编码。因此，建议 仅通过 已使用其他方式（如 VPN ）保护的 连接使用此机制。 |

### 带基本身份验证配置文件的 TLS - 2

*表 15. 安全配置文件 2 - 具有基本身份验证*的  *TLS*

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **1** | **名字** | 带基本身份验证的 TLS |
| **2** | **型 材编号** | 2 |
| **3** | **描述** | 在具有基本身份验证的 TLS 配置文件中，使用传输层安全性 （TLS） 保护通信通道。 网吧点点通使用 TLS 服务器证书对自身进行身份验证。 充电站使用 HTTP 基本身份验证进行 自我身份验证。 |

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **4** | **充电 站 认证** | 对于 充电 站 身份验证 ，使用 HTTP 基本 身份验证 。  由于在此配置文件 中使用了 TLS，因此密码 将以加密方式发送，从而降低了使用此 身份验证方法的风险。 |
| **5** | **网吧点点 通认证** | 充电站通过 TLS 服务器证书对 CSMS 进行身份验证。 |
| **6** | **通信 安全** | 充电站和CSMS 之间的通信使用TLS进行保护。 |

充电 站

网信

|  |  |
| --- | --- |
| 客户 您好 | |
|  | 服务器 Hello 服务器 证书 服务器 Hello Done |
|  | ClientKeyExchange [ChangeCipherSpec] 已完成 |
|  | [更改密码规格] 完成 |
|  | HTTP GET / ProtectedData （Encrypted Communication） |
|  | 需要 HTTP/401 身份验证 |
|  | HTTP GET / ProtectedData Authorization 基本 用户名/密码 |
|  | HTTP 200 / 受保护的数据 |
|  | 应用程序 数据 |
|  | |

*图 3. 序列图：具有基本身份验证序列图*的  *TLS*

|  |  |  |
| --- | --- | --- |
| **7** | **备注** | TLS 允许多种 配置，但并非所有 配置都提供足够的安全性。 以下要求 描述了 OCPP 允许的配置。  充电站应包含与基本身份验证 RFC 2617 中使用的标头相同的标头，同时请求将 http 连接升级到 websocket 连接，如 RFC 6455 中所述。  在升级 连接之前，服务器首先需要 验证授权标头。  **例：**  *GET /ws HTTP/1.1*  *Remote-Addr： 127.0.0.1 升级： websocket 连接： 升级 主机： 127.0.0.1：9999 来源： http://127.0.0.1:9999*  *SEC-WEBSOCKET-KEY： Pb4obWo2214EfaPQuazMjA== SEC-WEBSOCKET-VERSION： 13*  授权： 基本 *<Base64 编码（<ChargePointId>：<授权密钥>）>* |

### 具有基本身份验证配置文件的 TLS - 要求

*表 16. 安全配置文件 2 - 带基本身份验证*的  *TLS - 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.301 |  | 充电站应使用HTTP基本身份验证向CSMS 验证自身身份[18] |

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.302 | 答00.FR.301 | 客户端（即 充电站）应在 每次连接请求中提供 用户名和密码。 |
| 答00.FR.303 | 答00.FR.302 | 用户名应 等于 充电站标识，该标识是充电站的标识字符串，因为它在 OCPP-J 连接 URL 中使用它。 使用基本身份验证 时，充电站标识可能 不包含 字符“：”。 否则，网吧点点通 可能无法将用户名与 密码分开。 |
| 答00.FR.304 | 答00.FR.302 | 密码应存储在基本密码配置变量中。它应是随机选择的标识符字符串，具有 足够高的熵，由最少16个字符和最多40个字符组成（字母数字字符和标识符字符串允许的特殊字符操作符）。密码应以 UTF-8 编码字符串的形式发送（不编码为八位字节字符串或 base64）。 |
| 答00.FR.306 |  | CSMS应充当 TLS 服务器。 |
| 答00.FR.307 |  | 网吧网服务使用网吧作为服务器端证书进行自我认证。 |
| 答00.FR.308 |  | 充电站应根据 [3] 第6节建立的路径验证规则，验证CSMS证书的认证路径。 |
| 答00.FR.309 |  | 充电站应验证 公用名是否包含 网吧点点通的FQDN。 |
| 答00.FR.310 | 如果 CSMS 不拥有有效的证书，或者 证书路径无效 | 充电站应触发 InvalidCsmsCertificate 安全事件（有关 安全事件的完整列表 ，请参阅第 2 部分附录）。 |
| 答00.FR.311 | 答00.FR.310 | 充电站应终止 连接。 |
| 答00.FR.312 |  | 应使用传输层安全性 （TLS） [4] 保护通信通道。 |
| 答00.FR.313 |  | 充电站和网吧点点通系统只能使用TLS v1.2或更高版本。 |
| 答00.FR.314 |  | 这两 个 端点 都应 检查 所使用的 TLS 版本。 |
| 答00.FR.315 | 答00.FR.314 和  CSMS 检测到充电 站仅允许 使用较旧版本的 TLS 进行连接，或者 仅 允许 SSL | 网吧点点通应终止 连接。 |
| 答00.FR.316 | 答00.FR.314 和  充电站检测到 CSMS仅允许使用旧版TLS进行连接，或仅允许SSL连接 | 充电站应触发 无效TLSVersion安全事件并终止 连接（有关安全事件的完整列表 ，请参阅第2部分附录）。 |
| 答00.FR.317 |  | TLS 应按照[4] 或其后续标准的规定实施，不得进行任何修改。 |
| 答00.FR.318 |  | CSMS应至少支持 以下四个密码套件：**TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384**  注意：CSMS 必须 提供 2 个不同的证书来支持 这两个密码套件。 此外，在使用安全配置文件 3 时， CSMS 应该能够 为两个密码套件生成客户端证书。 |

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.319 |  | 充电站应 至少支持密码套件：（**TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256**  和 **TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384**） 或  （**TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256** 和 **TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384**）  注1：TLS\_RSA 不支持 前向保密，因此建议TLS\_ECDHE。此外，如果充电站检测到使用的算法不安全，则应触发 InvalidTLSCipherSuite 安全事件（有关完整事件 ，请参阅第 2 部分附录）  安全事件列表）。  注2：请注意，ISO15118-2规定为EV和Charge之间的通信实施以下密码套件  站：  TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_**CBC**\_SHA256， TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_**CBC**\_SHA256 |
| 答00.FR.320 |  | 充电站和CSMS不得使用使用在[1]中标记为 不适合传统使用的加密基元的密码套件。 这意味着，当本规范 中描述的一个或多个密码套件 被标记为不适合旧版使用时，将不再 使用。 |
| 答00.FR.321 |  | TLS 服务器和客户端不得使用 TLS 压缩方法来避免压缩侧信道攻击 并确保互操作性，如 [10] 第 6 节所述。 |
| 答00.FR.322 | 答00.FR.321 和  CSMS检测到充电站仅允许使用这些 套件之一进行连接 | 网吧点点通应终止 连接。 |
| 答00.FR.323 | 答00.FR.321 和  充电站检测到 CSMS仅允许使用这些 套件之一进行连接 | 充电站应触发无效 TLSCipherSuite安全事件并终止 连接（有关安全事件的完整列表 ，请参阅第2部分附录）。 |

### 具有客户端 证书配置文件的 TLS - 3

*表 17. 安全配置文件 3 - 具有客户端 证书的 TLS*

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **1** | **名字** | 具有客户端 证书的 TLS |
| **2** | **型 材编号** | 3 |
| **3** | **描述** | 在具有客户端证书的 TLS 配置文件中，使用传输层安全性 （TLS） 保护通信通道。 充电站和CSMS都使用证书对自己进行身份验证。 |
| **4** | **充电 站 认证** | 网吧点点通通过TLS 客户端证书对充电站进行认证。 |
| **5** | **网吧点点 通认证** | 充电站通过 TLS 服务器证书对 CSMS 进行身份验证。 |
| **6** | **通信 安全** | 充电站和CSMS 之间的通信使用TLS进行保护。 |

充电站

网信

|  |  |
| --- | --- |
| 客户 您好 | |
|  | 服务器 Hello 服务器 证书  证书 服务器请求 服务器 你好 完成 |
|  | 客户端证书 客户端 密钥 交换 证书验证 [更改密码规范] 已完成 |
|  | [更改密码规格] 完成 |
|  | 应用程序 数据 （经过 身份验证和 加密的 通信） |
|  | |

*图 4. 序列图：具有客户端 证书的 TLS*

|  |  |  |
| --- | --- | --- |
| **7** | **备注** | 不适用 |

### 具有客户端证书配置文件的 TLS - 要求

*表 18. 安全配置文件 3 - 具有客户端 证书的 TLS - 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.401 |  | 充电站应使用 充电站证书向CSMS认证。 |
| 答00.FR.402 |  | 充电站证书应 用作 TLS 客户端证书 |
| 答00.FR.403 |  | CSMS应 根据 [3]第6节建立的路径验证规则验证充电站证书的认证路径。 |
| 答00.FR.404 |  | CSMS 应通过检查证书 主题字段中 的 O（组织名称）RDN 是否包含 CSO 名称来验证证书是否归 CSO（或 CSO 信任的组织） 所有。 |
| 答00.FR.405 |  | 网信通系统 应通过检查证书 主题字段中的 CN（通用名称）RDN是否包含充电站的唯一 序列号来验证证书是否属于该充电站。 （请参见证书属性）。 |
| 答00.FR.406 | 如果充电站证书不属于 CSO， 例如 在安装后立即 | 建议 在继续与 充电站通信之前更新证书（另请参阅安装） |
| 答00.FR.407 | 如果充电站 不拥有有效的证书，或者证书路径无效 | 网吧点点通应终止 连接。 |
| 答00.FR.408 | 答00.FR.407 | 建议 在网吧点点通中 记录安全事件。 |
| 答00.FR.409 |  | CSMS应充当 TLS 服务器。 |
| 答00.FR.410 |  | 网吧网服务使用网吧作为服务器端证书进行自我认证。 |
| 答00.FR.411 |  | 充电站应根据 [3] 第6节建立的路径验证规则，验证CSMS证书的认证路径。 |
| 答00.FR.412 |  | 充电站应验证 公用名是否与 网吧点点通的FQDN相匹配。 |
| 答00.FR.413 | 如果 CSMS 不拥有有效的证书，或者 证书路径无效 | 充电站应触发 InvalidCsmsCertificate 安全事件（有关 安全事件的完整列表 ，请参阅第 2 部分附录）。 |
| 答00.FR.414 | 答00.FR.413 | 充电站应终止 连接。 |

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.415 |  | 应使用传输层安全性 （TLS） [4] 保护通信通道。 |
| 答00.FR.416 |  | 充电站和网吧点点通系统只能使用TLS v1.2或更高版本。 |
| 答00.FR.417 |  | 这两 个 端点 都应 检查 所使用的 TLS 版本。 |
| 答00.FR.418 | 答00.FR.417 和  CSMS 检测到充电 站仅允许 使用较旧版本的 TLS 进行连接，或者 仅 允许 SSL | 网吧点点通应终止 连接。 |
| 答00.FR.419 | 答00.FR.417 和  充电站检测到 CSMS仅允许使用旧版TLS进行连接，或仅允许SSL连接 | 充电站应触发 无效TLSVersion安全事件并终止 连接（有关 安全事件的完整限制 ，请参阅第2部分附录）。 |
| 答00.FR.420 |  | TLS 应按照[4] 或其后续标准的规定实施，不得进行任何修改。 |
| 答00.FR.421 |  | CSMS应至少支持 以下四个密码套件：**TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384**  注意：CSMS 必须 提供 2 个不同的证书来支持 这两个密码套件。 此外，当使用 security 配置文件 3 时， CSMS 应该能够为两个密码套件生成客户端 证书。 |
| 答00.FR.422 |  | 充电站应 至少支持密码套件：（**TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256**  和 **TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384**） 或  （**TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256** 和 **TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384**）  注1：TLS\_RSA 不支持 前向保密，因此建议TLS\_ECDHE。此外，如果充电站检测到使用的算法不安全，则应触发 InvalidTLSCipherSuite 安全事件（有关完整事件 ，请参阅第 2 部分附录）  安全事件列表）。  注2：请注意，ISO15118-2规定为EV和Charge之间的通信实施以下密码套件  站：  TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_**CBC**\_SHA256， TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_**CBC**\_SHA256 |
| 答00.FR.423 |  | 充电站和CSMS不得使用使用在[1]中标记为 不适合传统使用的加密基元的密码套件。 这意味着，当本规范 中描述的一个或多个密码套件 被标记为不适合旧版使用时，将不再 使用。 |
| 答00.FR.424 |  | TLS 服务器和客户端不得使用 TLS 压缩方法来避免压缩侧信道攻击 并确保互操作性，如 [10] 第 6 节所述。 |

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.425 | 答00.FR.424 和  如果 CSMS 检测到充电站仅允许使用这些套件之一进行连接 | 网吧点点通应终止 连接。 |
| 答00.FR.426 | 答00.FR.424 和  充电站检测到 CSMS仅允许使用这些 套件之一进行连接 | 充电站应触发无效 TLSCipherSuite安全事件并终止 连接（有关安全事件的完整列表 ，请参阅第2部分附录）。 |
| 答00.FR.427 |  | 每个充电站 应 使用唯一的充电站证书。 |
| 答00.FR.428 |  | 充电站证书 可能与 ISO15118-2中的SECC证书 相同，用于在充电站和电动汽车之间建立TLS连接。 |

## OCPP 中使用的密钥

*本节是规范性的。*

OCPP 使用许多公钥私钥对来确保其安全性，请参阅下表。为了管理充电站上的密钥，已将消息添加到 OCPP。在 CSMS 或制造商处更新密钥超出了 OCPP 的范围。如果使用带有客户端 证书的 TLS ， 则充电站需要一个“充电站证书”，以便针对 CSMS 进行身份验证。

*表 19. OCPP 安全规范 中使用的证书*

|  |  |  |
| --- | --- | --- |
| **证书** | **私钥存储在** | **描述** |
| 网信 认证证书 | 网信 | 用于对网吧点点通进行身份验证的密钥。 |
| 充电 站 证书 | 充电 站 | 用于对充电站进行身份验证的密钥。 |
| 固件 签名 证书 | 制造者 | 用于验证固件签名的密钥。 |
| 美国环保总会 证书 | 充电 站 | ISO15118-2 用于在充电站和 电动汽车之间建立 TLS 连接的证书。 |

### 证书 属性

*本节是规范性的。*

*表 20. 证书 属性 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.501 |  | 所有证书都应使用私钥 ，根据 [17] 的第 5.6.1 节，该私钥提供 的安全性相当于 至少 112 位的对称密钥。 这是 NIST 为 2011-2030 年期间建议的密钥大小。 |
| 答00.FR.502 | 答00.FR.501 和  RSA 或 DSA | 这转化为 一个密钥，该密钥的长度应至少为2048位。 |
| 答00.FR.503 | 答00.FR.501 和  椭圆 曲线 密码学 | 这转化为 一个密钥，该密钥的长度应至少为224位。 |
| 答00.FR.504 |  | 对于所有加密操作，应仅使用 BSI在[12]中推荐的适合在未来系统中使用的 算法。此限制包括在 证书层次结构中对证书进行签名 |
| 答00.FR.505 |  | 对于 由证书颁发机构进行签名， 应使用 RSA-PSS 或 ECDSA。 |
| 答00.FR.506 |  | 对于计算哈希值， 应使用 SHA256 算法。 |
| 答00.FR.507 |  | 证书 应以X.509格式存储和传输，并以隐私增强邮件（PEM）格式编码。 |

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.508 |  | 所有 证书 应 包括 一个 序列号 。 |
| 答00.FR.509 |  | 证书 的使用者字段应包含 O（组织名称）RDN 中证书所有者的组织名称。 |
| 答00.FR.510 |  | 对于 CSMS 证书， 使用者字段应包含 CN（公用名）RDN 中 服务器终结点的 FQDN。 |
| 答00.FR.511 |  | 对于充电站证书， 主题字段应包含 CN （通用名称）RDN，该 RDN 由充电站的唯一序列号组成。此序列号不得采用 URL 或 IP 地址的格式，以便充电站证书可以  与 CSMS 证书不同。  注意： According to RFC 2818， if a subjectAltName extension of type dnsName 存在，必须用作标识。这将 不符合 OCPP 和 ISO 15118。 因此 ， 不应 使用它  在 充电 站 和 CSMS 证书中。  当CSMS有多个网络路径可以到达它时， 允许对CSMS 使用 dnsName 类型的subsEdName扩展（例如，通过 专用APN + VPN使用其在 VPN中的IP地址和 通过使用 命名 URL 通过公共互联网）。 |
| 答00.FR.512 |  | 对于所有证书，应 使用 X.509 密钥用法扩展 [19] 将证书的使用限制为将要使用的操作。 |
| 答00.FR.513 |  | 如果充电站证书在 ISO 15118协议中也用作SECC证书，则该证书 还应符合ISO15118-2的要求。 |
| 答00.FR.514 |  | 对于所有 证书，强烈建议不要使用 X.509 扩展密钥用法扩展，以便与 ISO 15118 标准兼容。 有 可用的替代机制。 |

### 证书 层次结构

*本节是规范性的。*

OCPP 协议支持 使用 两个单独的证书层次结构：

* + - 1. 包含 CSMS 和充电站证书的充电站操作员层次结构 。
      2. 包含固件签名证书的制造商层次结构。

CSMS 可以使用 InstallCertificateRequest 消息更新 存储在 充电站上的 CSO 根证书。

*表 21. 证书 层次结构 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.601 |  | 充电站运营商可以 充当 充电站运营商层次结构的证书颁发机构 |
| 答00.FR.602 | 答00.FR.601 | 例如，充电站运营商 MAY 遵循 ISO15118-2 附录 E 和 F 中描述的证书层次结构，并使用 CSO 子 CA 2 证书对 CSMS 和充电站证书进行签名。这可以带来充电 站客户端 证书 的在线验证 可以在充电站运营商的网络内完成的优势，从而简化网络。 建筑。 |
| 答00.FR.603 |  | 属于 CSO 根证书的私钥 必须得到很好的保护。 |
| 答00.FR.604 |  | 由于制造商通常是 与充电站运营商 分开的组织，因此应使用受信任的第三方作为证书颁发机构。 这对于 固件映像的 不可否认性至关重要。 |

## 证书 吊销

*本节是规范性的。*

在某些情况下，证书可能会在有效期到期之前失效。此类情况包括更改组织名称，或 证书 私钥的泄露或可疑泄露。 在这种情况下，需要吊销证书 或指示它不再 有效。 吊销 证书 并不意味着 需要关闭连接 ，因为连接可以保持打开状态超过 24 小时。

证书 吊销建议 使用不同的方法，请参见 下表。

*表 22. 针对不同证书*  *的建议吊销方法*。

|  |  |
| --- | --- |
| **证书** | **撤销** |
| 网信 认证证书 | 快速 过期 |
| 充电 站 证书 | 在线 验证 |
| 固件 签名 证书 | 在线 验证 |

*表 23. 证书 吊销 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.701 |  | 应使用快速过期 来吊销 CSMS 证书。 （请参阅注释 1） |
| 答00.FR.702 |  | 网信通应使用在线证书验证来验证 充电站证书的有效性。 |
| 答00.FR.703 |  | 建议 使用单独的证书颁发机构服务器来管理 证书。 |
| 答00.FR.704 | 答00.FR.703 | 此服务器还应 跟踪 哪些证书已被 吊销。 |
| 答00.FR.705 |  | 网吧网服务应通过 证书颁发机构服务器验证 证书的有效性。 （请参阅注释 2） |
| 答00.FR.707 |  | 在向充电站提供固件验证证书之前 ，CSMS 应同时验证证书和签名的 固件 更新。 |

注意1：由于 快速过期， 证书 仅在短时间内有效，少于 24小时。 之后，服务器 需要从证书颁发机构请求新证书，这可能是 CSO 本身（请参阅证书层次结构部分）。这可以防止充电站 需要 实施吊销列表或在线证书验证。 这简化了 充电站证书管理 的实施 ，并降低了充电站端的通信成本。 通过要求快速

过期时，如果证书 泄露，则影响将减少到仅短时间。

当证书链 受到损害时，攻击者可以使用 伪造的证书来诱骗充电站 连接到 “假”CSMS。 通过使用快速过期，充电站 易受攻击 的时间大大减少。

充电站始终通过 CSMS与 证书颁发机构通信 ，这样，如果充电站受到威胁，充电站无法直接攻击CA。

注2：这允许立即吊销充电站证书。 例如，当充电站 被移除时，将撤销充电站证书。 这比吊销 CSMS 证书 更常见，后者通常仅在证书受到威胁时才进行。

## 安装

*本节是规范性的。*

应使用唯一凭据向 CSMS 验证每个充电站，无论它们是用于 HTTP 基本身份验证的密码（请参阅充电站身份验证）还是 充电站证书。 这些独特的凭据必须在 制造或安装过程中的某个时刻放在充电站 上。

*表 24. 证书 安装 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 答00.FR.801 |  | 建议 制造商在制造过程中使用唯一凭据初始化充电站。 |
| 答00.FR.802 | 答00.FR.801 | 凭据 应使用 加密随机数生成器 生成，并安装在安全的环境中。 |
| 答00.FR.803 | 答00.FR.801 | 它们 应该 通过安全通道发送给CSO，以便 CSO可以将它们导入CSMS中 |
| 答00.FR.804 | 如果使用 充电 站 证书 。 | 制造商可以使用 自己的证书对这些证书进行签名。 |
| 答00.FR.805 | 答00.FR.804 | 建议 CSO 在 安装后立即使用 A01 节 - 更新 HTTP 基本身份验证的充电站密码 或 A02 - 根据 CSMS 请求更新充电站证书中描述的方法更新凭据。 |
| 答00.FR.806 | 在“工厂凭据” 更新之前 | 网吧点点通系统可能会限制 充电站可以使用的功能。网吧点点通则可以使用“引导通知”状态：“挂起”。 在“挂起”状态下，网吧点点通可以更新 凭证。 |

# 2. 用例 和 要求

## A01 - 更新 HTTP 基本身份验证的充电站密码

*表 25. A01 - 密码 管理*

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **1** | **名字** | 更新 HTTP 基本身份验证的充电站密码 |
| **2** | **编号** | 答01 |
|  | *功能 块* | A. 安全 |
| **3** | **目标** | 此用例 定义了如何使用 BasicAuthPassword，即用于对基本身份验证安全配置文件中的基本和 TLS 中的充电站进行身份验证的密码。 |
| **4** | **描述** | 若要使 CSMS 能够为 HTTP 基本身份验证配置新密码，CSMS 可以为 基本密码配置变量发送 新值。 |
|  | *演员* | 充电 站， 网吧点点通 |
|  | *场景 描述* | 1. CSMS将SetVariablesRequest（ComponentName=SecurityCtrlr，VariableName=BasicAuthPassword）发送到 充电站。 2. 充电站以 SetVariablesResponse 和 状态*“已接受”进行*响应。 3. 充电站断开其当前连接。 （存储任何排队的消息） 4. 充电站使用 新密码连接到 CSMS。 |
| **5** | **先决条件** | 安全配置文件：基本安全配置文件或正在使用基本身份验证的 TLS。 |
| **6** | **后置条件** | **成功的 后置条件：**  充电站已使用 新密码重新连接到 CSMS。  **故障 后置条件：**  如果充电站使用 状态不是*“已接受*”的 SetVariablesResponse 响应 SetVariablesRequest 来响应 SetVariablesRequest，则充电站将继续 使用旧凭据。CSMS可能会以不同的方式对待充电站，例如不接受充电站的启动通知。 |

网信

充电 站

SetVariablesRequest（BasicAuthPassword）



SetVariablesResponse（status = Accepted）

断开

连接 （使用 新 密码）

*图 5. 更新 HTTP 基本身份验证的充电站密码（快乐流）*

|  |  |  |
| --- | --- | --- |
| **7** | **错误 处理** | 不适用 |
| **8** | **备注** | 不适用 |

### A01 - 更新 HTTP 基本身份验证的充电站密码 - 要求

*表 26. A01 - 更新 HTTP 基本身份验证的充电站密码 - 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 解答 01.法国01 |  | 密码 应存储在配置变量中  BasicAuthPassword. |

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 解答 01.FR.02 |  | 要 通过OCPP 设置 充电站的基本授权密码，网信通应向充电站发送带有BasicAuthPassword Configuration Variable的SetVariablesRequest消息。 |
| 解答 01.FR.03 | 解答 01.FR.02 和  充电站 通过状态为*“已接受*”的 SetVariablesResponse 响应此 SetVariablesRequest 来响应此 SetVariablesRequest。 | 网信服务应假定授权密钥变更 成功，不再 接受充电站之前使用的凭证。 |
| 解答 01.FR.04 | 解答 01.FR.02 和  充电站通过 SetVariablesRespons 响应此 SetVariablesRequest，其状态不是*“已接受”* | 网信系统应 假定 充电站未 更改密码。因此，CSMS应继续接受旧的凭据。 |
| 解答 01.法国05元 | 解答 01.FR.04 | 虽然CSMS仍应接受来自充电站的连接，但它可能会限制充电站可以使用的功能。网吧点点通则可以使用“引导通知”状态：“挂起”。 在 “挂起”状态下，CSMS 可以重试 更新凭据。 |
| 解答 01.法国06元 |  | 不同的充电站应使用 不同的密码。 |
| 解答 01.FR.07 |  | 密码 应随机生成， 以确保 密码具有足够的熵。 |
| 解答 01.FR.08 |  | CSMS 应该只存储加盐的密码哈希，而不是 密码 本身。 |
| 解答 01.法国09 |  | 网吧网服务不应该 把密码明文放在日志文件 或 调试信息中。这样，如果CSMS受到损害，并非所有充电站密码都会 立即受到损害。 |
| 解答 01.FR.10 |  | 在充电站上，密码 需要以 明文形式存储。 应格外小心，以安全地存放它。 但是， 如何安全存储凭据的机制的定义不在 OCPP 安全配置文件的范围内。 |
| 解答 01.法国11 | 解答 01.FR.02 | 充电站应记录  安全日志中的基本身份验证密码。 |
| 解答 01.FR.12 | 解答 01.法国11 | 充电站不得在其日志中披露BasicAuthPassword的内容。 这是为了防止 密钥材料暴露给 可能 有权访问诊断文件的人员。 |

## A02 - 根据CSMS的要求 更新充电站证书

*表 27. A02 - 根据CSMS的要求 更新充电站证书*

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **1** | **名字** | 根据CSMS的要求更新充电站证书 |
| **2** | **编号** | 答01 |
|  | *功能 块* | A. 安全 |
| **3** | **目标** | 为了便于管理 充电站客户端证书，提供了证书更新过程 。 |
| **4** | **描述** | CSMS 请求充电站使用 TriggerMessageRequest 更新其密钥，并将*请求的消息*字段设置为 SignChargingStationCertificate（或 SignV2GCertificate，用于单独的 15118 证书）。 |
|  | *演员* | 充电 站、 网吧点点通、 证书 颁发机构 服务器 |

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
|  | *场景 描述* | 1. CSMS 请求充电站使用 TriggerMessageRequest 更新其证书，并将  *请求的消息*字段设置为 SignChargingStationCertificate   （或 SignV2GCertificate 用于 单独的 15118 证书）。   1. 充电站 使用触发消息响应进行响应 2. 充电站生成新的 公钥/私钥 对。 3. 充电站向 CSMS 发送 SignCertificateRequest，其中包含适用的 CertificateSigningUse 。 4. CSMS 以 SignCertificateResponse 进行响应，状态为  *“已接受*”。 5. CSMS 将 CSR 转发到 证书颁发机构服务器。 6. 证书颁发机构服务器对证书进行签名。 7. 证书颁发机构服务器将签名证书返回到 CSMS。 8. CSMS 将 CertificateSignedRequest 发送到 充电站。 9. 充电站验证签名证书。 10. 充电站以证书签名响应 CSMS， 状态为   *已接受* 或 *已拒绝*。 |
| **5** | **先决条件** | 必须 设置标准配置变量组织名称。 |
| **6** | **后置条件** | **成功的 后置条件：**  充电站中 安装了新的客户端 证书。  **故障 后置条件：**  新的 客户端 证书 将 被拒绝 并 丢弃。 |

网信

充电 站

证书 颁发机构 服务器

CS 证书 即将 到期



TriggerMessageRequest（SignCertificate）

触发器消息响应（已接受）

生成 新增功能

SignCertificateRequest（csr）

公钥 / 私钥 对

SignCertificateResponse（已接受）

前进 企业社会责任

标志 证书

返回 签名 证书

证书签名请求（证书）

验证 有效性

签名证书的数量

证书签名响应 （已接受/已拒绝）

**[键 有效]**

**选择**

切换到新证书

*图 6. 更新 充电 站 证书*

|  |  |  |
| --- | --- | --- |
| **7** | **错误 处理** | CSMS 接受 来自充电站的 CSR 请求，然后再将其转发到 CA。 但是，当无法到达CA或拒绝CSR时，充电站将永远不会知道。 CSMS 可能会对 CSR 执行一些检查，但不能执行 CA 所做的所有检查，并且不会阻止与 CA 的连接超时。 根据 CA 的说法，当 此类 事情出错时，要么是 CA 处于脱机状态，要么是充电站发送的 CSR 不正确。 在这两种情况下 ， 这都是CSO 的操作员 需要 通知的事情。 然后，操作员需要  调查问题。 解析后， 操作员可以重新运行 A02。  不建议 在 X 分钟或小时内未发送证书时让充电站重试。当 CSR 不正确时，不会自动解决。 可能 只有 新固件才能解决此问题。 |
| **8** | **备注** | 充电站运营商可以 充当 充电站运营商层次结构的证书颁发机构。  适用的证书颁发机构应检查 CSR 中 的信息。  如果 正确，证书颁发机构应签署 CSR，将其发送给CSO， CSO将其发送  返回到 CertificateSignedRequest 消息中的 充电站。  证书颁发机构应实施强措施来确保 证书签名私钥 的安全。  尽管消息 CertificateSignedRequest（请参阅用例 A02 和 A03）和 InstallCertificateRequest（用例 M05 - 在充电站中安装 CA 证书）都用于 发送证书，但它们的用途是不同的。 证书签名请求 用于 返回 充电站自己的公共证书和由 证书签名的 V2G 证书  柄。 InstallCertificateRequest 用于 安装 根 证书。  有关 V2G 证书处理的信息，请参阅用例 M03 - 从 充电站检索可用证书的列表、M04 - 从充电站中删除特定证书和 M06 - 获取充电站证书状态。 |

### A02 - 根据CSMS的要求 更新充电站证书 - 要求

*表 28. A02 - 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 解答 02.法国01 |  | 安装充电站 后，应执行密钥更新 ，以更改制造商最初提供的密钥 （可能是默认密钥）。 |
| 解答 02.FR.02 | 发送触发消息响应后。 | 充电站应 使用[16]第4.2.1.3节中描述的密钥生成功能之一生成新的公钥/私钥 对。 |
| 解答 02.FR.03 | 解答 02.FR.02 | 充电站应按照 RFC 2986 [22] 中所述，以证书签名请求 （CSR） 的形式 发送 公钥，然后使用 SignCertificateRequest 消息对 PEM 进行编码。 |
| 解答 02.FR.04 |  | CSMS 不应 对证书本身进行签名，而是将 CSR 转发到管理充电站基础结构的证书的专用证书颁发机构服务器。专用权限服务器 可由 CSO 操作。 |
| 解答 02.法国05元 |  | 充电站在 密钥更新过程中 生成的 私钥不得在任何时候离开充电站，也不得通过OCPP或任何其他（远程）通信连接读取。 |
| 解答 02.法国06元 |  | 充电站应在 CertificateSignedRequest 消息中验证已签名证书 的有效性，至少 检查证书有效的时间段，在证书属性，并且 它是 充电站运营商证书层次结构的一 部分，如证书层次结构中所述。 |
| 解答 02.FR.07 | 如果证书 无效。 | 充电站应丢弃证书，并触发无效充电站证书安全事件（有关安全事件的完整列表 ，请参阅第2部分附录）。 |
| 解答 02.FR.08 |  | 充电 站应在当前 日期和时间位于证书中的“之前无效” 字段之后立即切换到新证书。 |

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 解答 02.法国09 | 如果充电站包含多个  *充电站证书*类型的有效证书。 | 充电站应使用 最新的证书，以 有效期开始时为准。 |
| 解答 02.FR.10 | 解答 02.法国09  并且当充电站已 验证新证书 是否正常工作时 | 充电站可能会丢弃旧证书。 建议将旧证书 存储一个月，作为回退。 |
| 解答 02.法国11 | 收到  SignCertificateRequest AND  它 能够处理 请求 | 网信服务在 SignCertificateResponse 中应将状态设置为*“已接受*”。 |
| 解答 02.FR.12 | 收到  SignCertificateRequest AND  它 无法处理 请求 | CSMS 应在 SignCertificateResponse 中将状态设置为*“已拒绝*”。 |
| 解答 02.FR.13 | 对 15118 连接和 充电站到 CSMS 连接使用不同的证书时 | 充电站应将 SignCertificateRequest 中的 certificateType 字段设置为 触发更新的证书。 |
| 解答 02.14节 | 收到包含证书 类型的 SignCertificate 请求时 | 建议 CSMS 将 CertificateSignedRequest 中的 certificateType 字段设置为 SignCertificateRequest 中的证书类型。 |
| 解答 02.15节 | 如果充电站包含多个从同一根证书派生的有效 V2G 证书。 | 充电站应使用 最新的证书，以 有效期开始时为准。 |
| 解答 02.法币16 | 如果 配置 变量 MaxCertificateChainSize 是  已实施 和  充电站接收 CertificateSignedRequest 消息 ，其中包含一个大小超过 MaxCertificateChainSize 中配置的设置值的证书（链） | 充电站应使用状态为*“已拒绝*”的“证书签名响应”消息进行响应。 |

## A03 - 更新充电站启动的充电站证书

*表 29. A03 - 更新充电站启动 的充电站证书*

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **1** | **名字** | 更新充电站 启动的充电站证书 |
| **2** | **编号** | 答03 |
|  | *功能 块* | A. 安全 |
| **3** | **目标** | 为了便于管理 充电站客户端证书，提供了证书更新过程 。 |
| **4** | **描述** | 充电站检测到它正在使用的证书（ChargingStationCertificate或V2GCertificate for 15118）将在一个月后过期。 充电站使用 SignCertificateRequest 启动 更新其密钥 的过程，并在 CertificateSigningUse 字段中指示请求的证书。 |
|  | *演员* | 充电 站、 网吧点点通、 证书 颁发机构 服务器 |

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
|  | *场景 描述* | 1. 充电站检测到 充电站证书 即将 过期。 2. 充电站生成新的 公钥/私钥 对。 3. 充电站向 CSMS 发送包含适用证书签名用途的 SignCertificateRequest。 4. CSMS 使用 SignCertificateResponse 进行响应， 状态*为“已接受*”。 5. CSMS 将 CSR 转发到 证书颁发机构服务器。 6. 证书颁发机构服务器对证书进行签名。 7. 证书颁发机构服务器将签名证书返回到 CSMS。 8. CSMS 将 CertificateSignedRequest 发送到 充电站。 9. 充电站验证签名证书。 10. 充电站使用 证书签名响应 CSMS， 状态为   *已接受* 或 *已拒绝*。 |
| **5** | **先决条件** | 必须 设置标准配置变量组织名称。 |
| **6** | **后置条件** | **成功的 后置条件：**  充电站中 安装了新的客户端 证书。  **故障 后置条件：**  新的 客户端 证书 将 被拒绝 并 丢弃。 |

充电 站

网信

证书 颁发机构 服务器

CS 证书 即将 到期



生成 新的 公钥 / 私钥 对

SignCertificateRequest（csr）

SignCertificateResponse（已接受）

向前 企业社会责任

证书签名请求（证书）

标志 证书

返回 签名 证书

验证 签名证书的有效性

证书签名响应 （已接受/已拒绝）

**[键 有效]**

**选择**

切换到新证书

*图 7. 更新充电站启动的 充电站证书*

|  |  |  |
| --- | --- | --- |
| **7** | **错误 处理** | CSMS 接受 来自充电站的 CSR 请求，然后再将其转发到 CA。 但是，当无法到达CA或拒绝CSR时，充电站将永远不会知道。 CSMS 可能会对 CSR 执行一些检查，但不能执行 CA 所做的所有检查，并且不会阻止与 CA 的连接超时。 当 此类 情况出错时，CA 处于脱机状态，或者充电站发送的 CSR 不正确，符合 CA 的要求。 在这两种情况下 ， 这都是CSO 的操作员 需要 通知的事情。 然后，操作员需要  调查问题。 解析后， 操作员可以重新运行 A02。  不建议 在 X 分钟或小时内未发送证书时让充电站重试。当 CSR 不正确时，不会自动解决。 可能 只有 新固件才能解决此问题。 |
| **8** | **备注** | 与A02中相同的说明 - 根据CSMS的请求 更新充电站证书适用。 |

### A03 - 更新充电站启动的充电站证书 - 要求

*表 30. A03 - 要求*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 解答 03.法国01 |  | 安装 充电站后，可以执行密钥更新，以更改制造商最初提供的密钥（可能是默认密钥）。 |
| 解答 03.FR.02 | 当充电站检测到当前充电站证书将在 一个月后过期时。 | 充电站应 使用[16]第4.2.1.3节中描述的密钥生成功能之一生成新的公钥/私钥 对。 |
| 解答 03.FR.03 | 解答 03.FR.02 | 充电站应按照 RFC 2986 [22] 中所述，以证书签名请求 （CSR） 的形式 发送 公钥，然后使用 SignCertificateRequest 消息对 PEM 进行编码。 |
| 解答 03.FR.04 |  | CSMS 不应 对证书本身进行签名，而是将 CSR 转发到管理充电站基础结构的证书的专用证书颁发机构服务器。专用权限服务器 可由 CSO 操作。 |
| 解答 03.法国05元 |  | 充电站在 密钥 udate过程中生成的私钥不得在任何时候离开充电站，并且不得通过OCPP或任何其他（远程）通信连接读取。 |
| 解答 03.法国06元 |  | 充电站应在 CertificateSignedRequest 消息中验证已签名证书 的有效性，至少 检查证书有效的时间段，在证书属性，并且 它是 充电站运营商证书层次结构的一 部分，如证书层次结构中所述。 |
| 解答 03.FR.07 | 如果证书 无效。 | 充电站应丢弃证书，并触发无效充电站证书安全事件（有关安全事件的完整列表 ，请参阅第2部分附录）。 |
| 解答 03.FR.08 |  | 充电 站应在当前 日期和时间位于证书中的“之前无效” 字段之后立即切换到新证书。 |
| 解答 03.法国09 | 如果充电站包含多个  *充电站证书*类型的有效证书。 | 充电站应使用 最新的证书，以 有效期开始时为准。 |
| 解答 03.FR.10 | 解答 03.FR09  并且当充电站已 验证新证书 是否正常工作时 | 充电站可能会丢弃旧证书。 建议将旧证书 存储一个月，作为回退。 |
| 解答 03.法国11 | 收到  SignCertificateRequest AND  它 能够处理 请求 | 网信服务在 SignCertificateResponse 中应将状态设置为*“已接受*”。 |
| 解答 03.FR.12 | 收到  SignCertificateRequest AND  它 无法处理 请求 | CSMS 应在 SignCertificateResponse 中将状态设置为*“已拒绝*”。 |
| 解答 03.FR.13 | 对 15118 连接和 充电站到 CSMS 连接使用不同的证书时 | 充电站应在 SignCertificateRequest 中包含 certificateType 字段，以指定 要 更新的证书。 |
| 解答 03.14节 | 收到包含证书 类型的 SignCertificate 请求时 | 建议 CSMS 将 CertificateSignedRequest 中的 certificateType 字段设置为 SignCertificateRequest 中的证书类型。 |
| 解答 03.15节 | 如果充电站包含多个从同一根证书派生的有效 V2G 证书。 | 充电站应使用 最新的证书，以 有效期开始时为准。 |

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 解答 03.法币16 | 如果 配置 变量 MaxCertificateChainSize 是  已实施 和  充电站接收 CertificateSignedRequest 消息 ，其中包含一个大小超过 MaxCertificateChainSize 中配置的设置值的证书（链） | 充电站应使用状态为*“已拒绝*”的“证书签名响应”消息进行响应。 |

## A04 - 安全 事件 通知

*表 31. A04 - 安全 事件 通知*

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **1** | **名字** | 安全 事件 通知 |
| **2** | **编号** | 答04 |
|  | *功能 块* | A. 安全 |
| **3** | **目标** | 将 关键安全事件通知 CSMS。 |
| **4** | **描述** | 此 用例允许充电站立即 通知CSMS系统安全性的变化。 |
|  | *演员* | 网吧点点通， 充电 站 |
|  | *场景 描述* | 1. 发生 *严重* 安全 事件 。 2. 充电站向 CSMS 发送安全事件通知请求。 3. CSMS 以安全事件通知响应向 充电站做出响应。 |
| **5** | **先决条件** | 不适用 |
| **6** | **后置条件** | 充电站 通过向CSMS 发送安全事件通知请求*，成功地*通知CSMS关键安全事件。 |

充电 站

网信



发生了与安全相关的事件

请参阅第 2 部分 安全性附录

相关 活动

SecurityEventNotificationResponse（）

**[严重 安全 事件]**

SecurityEventNotificationRequest（）

**选择**

*图 8. 安全 事件 通知*

|  |  |  |
| --- | --- | --- |
| **7** | **错误 处理** | 不适用 |
| **8** | **备注** | 附录（ *附录 1. 安全事件*） |

### A04 - 安全 事件 通知 - 要求

*表 32. A04 - 安全 事件 通知 - 要求*

|  |  |  |  |
| --- | --- | --- | --- |
| **编号** | **前提** | **需求 定义** | **注意** |
| 解答 04.法国01 | 发生*严重*安全事件时 | 充电站应通过向网信系统发送安全通知请求，将安全事件通知网信处。 |  |
| 解答 04.FR.02 | 解答 04.FR.01 和  充电站已断开连接。 | 安全事件通知 必须在 CSMS 上排队，并保证传递。 |  |
| 解答 04.FR.03 | 解答 04.法国01 | 网信服务网服务应使用 安全通知回复消息确认 收到 通知。 |  |
| 解答 04.FR.04 | 发生 安全事件时 （也是 非关键事件） | 充电站应将 安全事件存储在 安全日志中。 | 建议以 滚动格式实现此日志。 |

## A05 - 升级 充电 站 安全 配置文件

*表 33. A05 - 升级 充电 站 安全 配置文件*

|  |  |  |
| --- | --- | --- |
| **不。** | **类型** | **描述** |
| **1** | **名字** | 升级 充电 站 安全 配置文件 |
| **2** | **编号** | 答05 |
|  | *功能 块* | A. 安全 |
| **3** | **目标** | CSO希望 提高CSMS和 充电站之间OCPP连接的安全性。 |
| **4** | **描述** | 从不带安全配置文件的 OCPP 1.6 迁移到 具有安全配置文件的 OCPP 1.6 或 OCPP 2.0.1 时的用例 在 迁移到安全配置文件之前，先决条件（如已安装的证书） 或 需要配置密码。 |
|  | *演员* | 网吧点点通， 充电 站 |
|  | *场景 描述* | 1. CSMS 通过 SetVariablesRequest 为网络配置优先级配置变量设置新值 ，以便 新的（更高）安全配置文件的 NetworkConnectionProfile 成为列表中的第一个，而现有连接配置文件变为   列表。   1. 充电站 以 SetVariables 响应 状态*“已接受”* 2. CSMS 发送 ResetRequest（OnIdle） 3. 充电站重新启动并通过 新的主网络连接配置文件进行连接 |
| **5** | **先决条件** | CSO 确保 已使用（更高的）安全性配置文件设置了网络连接配置文件  和  在 发送 命令以更改为更高的安全性配置文件之前，满足转到更高安全性配置文件的先决条件。 |
| **6** | **后置条件** | 充电站 已成功升级到 更高的安全配置文件。 |

算子

网信

充电 站

更改 网络 配置



SetVariablesRequest（NetworkConfigurationPriority）

SetVariablesResponse（status： RebootRequired）

ResetRequest（OnIdle）

重置响应（已接受）

重新启动

使用具有更高安全性配置文件的（新）网络连接配置文件进行连接

BootNotificationRequest（...）

BootNotificationResponse（...）

*图 9. 升级 充电 站 安全 配置文件*

|  |  |  |
| --- | --- | --- |
| **7** | **错误 处理** | 不适用 |
| **8** | **备注** | 出于安全 原因，不允许 使用 OCPP 恢复到较低的安全配置文件。 |

### A05 - 升级 充电 站 安全 配置文件 - 要求

*表 34. A05 - 升级 充电 站 安全 配置文件*

|  |  |  |
| --- | --- | --- |
| **编号** | **前提** | **需求 定义** |
| 解答 05.FR.02 | 充电站接收 SetVariablesRequest for NetworkConfigurationPriority，其中包含一个用于 NetworkConnectionProfile 的 配置文件插槽 ，其中包含  “安全性配置文件” 值 高于 当前 值 AND  新 值为 2 或 3  和  未安装有效的 CSMSRootCertificate | 充电站应以SetVariablesResponse（Rejected）进行响应， 并且不会更新 SecurityProfile 的值和/或重新连接到 CSMS。 |
| 解答 05.FR.03 | 充电站接收 SetVariablesRequest for NetworkConfigurationPriority，其中包含一个用于 NetworkConnectionProfile 的 配置文件插槽 ，其中包含  “安全性配置文件” 值 高于 当前 值 AND  新 值为 3  和  未安装有效的充电站证书 | 充电站应以SetVariablesResponse（Rejected）进行响应， 并且不会更新 SecurityProfile 的值和/或重新连接到 CSMS。 |
| 解答 05.FR.04 | 充电站接收 SetVariablesRequest for NetworkConfigurationPriority，其中包含 NetworkConnectionProfile 的 配置文件插槽，其“securityProfile”值等于或大于 the current  值 和  满足所有先决条件 | 充电站应以SetVariablesResponse（已接受）响应 |
| 解答 05.法国05元 | 解答 05.FR.04 和  重新启动后 | 充电站应开始 连接到网络配置优先级的第一个条目 |
| 解答 05.法国06元 | 解答 05.FR.05 和  充电站使用 （新）网络连接配置文件成功连接到 CSMS | 充电站应更新配置变量 SecurityProfile 的值，并应 删除 所有安全性低于 SecurityProfile 存储的“网络连接 配置文件”，并相应地更新“网络配置优先级”。 |
| 解答 05.FR.07 | 解答 05.法国06元 | CSMS将不再允许 充电站以较低的安全配置文件连接 。 |