



## China Cyber Security

# Common Security Requirements

Version 1.1

UNCONTROLLED COPY IF PRINTED

**FORD CONFIDENTIAL**



## Revision History

| Date      | Version | Created/Modified By     | Notes   |
|-----------|---------|-------------------------|---|
| 8/13/2021 | 1.0     | JSHAO13/XZHAN221/CSUN26 | Initial Version   |
| 8/26/2021 | 1.1     | JSHAO13/XZHAN221/CSUN26 | Updated with more specific definition on PII and other info |

CONFIDENTIAL



# CONTENTS

|                             |           |
|-----------------------------|-----------|
| <b>1. 客户端</b>               | <b>4</b>  |
| 1.1 安全开发(App)               | 4         |
| 1.1.1 代码安全                  | 4         |
| 1.1.2 签名                    | 4         |
| 1.1.3 下载、安装、卸载和更新           | 4         |
| 1.1.4 权限控制                  | 5         |
| 1.2 安全运行                    | 5         |
| 1.2.1 安全启动(App)             | 5         |
| 1.2.2 Cert Pinning/CTL(App) | 5         |
| 1.2.3 防 HOOK 及反调试(App)      | 5         |
| 1.2.4 身份认证                  | 6         |
| 1.2.5 安全登出                  | 7         |
| 1.2.6 输入/输出                 | 7         |
| 1.2.7 白盒/密钥                 | 8         |
| 1.2.8 其他安全防护（截屏、剪切板、键盘）     | 8         |
| 1.2.9 监控日志                  | 8         |
| 1.3 数据保护                    | 8         |
| 1.3.1 PII 识别与采集             | 8         |
| 1.3.2 PII 存储                | 9         |
| 1.3.3 PII 传输                | 9         |
| 1.3.4 PII 删除                | 9         |
| <b>2. 云端</b>                | <b>10</b> |
| 2.1 云端服务器                   | 10        |
| 2.2 云端应用框架/中间件/第三方组件        | 10        |
| 2.3 云端应用配置                  | 10        |
| 2.3.1 通讯                    | 10        |
| 2.3.2 防火墙                   | 10        |
| 2.3.3 云端攻击防护                | 10        |
| 2.3.4 管理后台                  | 11        |
| 2.3.5 数据库                   | 11        |
| 2.3.6 数据备份和恢复               | 12        |
| <b>3. 通讯</b>                | <b>13</b> |
| 3.1 客户端（App）                | 13        |
| 3.2 客户端与云端                  | 13        |
| 3.2.1 TLS                   | 13        |
| 3.2.2 TLS 超时                | 13        |
| 3.2.3 TLS 密码套件              | 13        |
| 3.2.4 TLS 压缩                | 13        |
| 3.2.5 TLS 证书颁发机构            | 13        |
| 3.2.6 MTLS 证书锁定             | 14        |
| 3.2.7 主机认证                  | 14        |
| 3.2.8 验证对等方                 | 14        |
| 3.2.9 证书安全                  | 14        |
| 3.3 云端与云端                   | 14        |
| 3.3.1 身份认证                  | 14        |
| 3.3.2 输入/输出                 | 14        |



## 1. 客户端

### 1.1 安全开发(APP)

#### 1.1.1 代码安全

##### 1.1.1.1 代码混淆加固

建议客户端代码应做混淆处理和加壳保护，包括但不限于福特开发部分、第三方库（网络层调用及计算）等。

##### 1.1.1.2 代码安全

客户端代码不应含有关键信息（包括但不限于：密钥、令牌、不必要的URL及IP地址），不应存在后门，不应允许备份和调试。应具备安全机制防止被反编译。

谨慎使用WebView，应仅加载白名单中内容(如特定URL/IP地址)：

1. 不使用searchBoxJavaBridge\_，accessibility，accessibilityTraversal等接口（易引起远程代码执行）
2. 不明文存储密码：WebSettings.setSavePassword(false)
3. 对于不需要使用file协议的应用，禁用file协议。如需要使用file协议的应用，禁止file协议加载JavaScript。
4. 强化证书校验
  - a. 通过方法setHostnameVerifier设置严格的主机名校验；
  - b. 如证书校验错误，对于方法onReceivedSslError、SslErrorHandler，检查其处理方式应该为SslErrorHandler.cancel()，而不是sslErrorHandler.proceed()；

不应存在于Google安全性平台（<https://source.android.com/security>）、CVE平台发布的CVSS≥7高危安全漏洞（“中国汽车行业漏洞共享平台（CAVD）”、“国家信息安全漏洞共享平台（CNVD）”平台上发布的高危安全漏洞也建议修复）。不应含有非授权收集或泄露用户信息、非法数据外传等恶意行为。

##### 1.1.1.3 组件安全(安卓)

应严格设置安卓组件（Activity、Broadcast、Service、Content Provider）访问权限，以限定外部调用权限、接受/发送外部应用数据，应指定发送/接受方，避免外部攻击（如恶意调用、数据泄露等）。

#### 1.1.2 签名

每个（iOS或Android）应用必须使用福特批准的唯一数字签名，防止安装包被重新打包。

#### 1.1.3 下载、安装、卸载和更新

##### 1.1.3.1 下载及更新

各版本软件应发布在福特批准的应用商店供用户下载，如福特官网、福特官方微博/微信、腾讯应用宝、苹果App Store等。



### 1.1.3.2 安装

应用安装应取得用户明确授权，其安装过程应满足以下要求：

- 检查系统环境，如系统已root/jailbroken，应禁止安装或给用户相应风险提示，用户接收后(应记录在日志中)方可安装
- 安装时应提示用户对其使用的系统资源及数据进行确认
- 不应应对系统及其他应用程序的正常运行造成影响

### 1.1.3.3 卸载

卸载应满足以下要求：

- 删除安装和使用过程中产生的资源文件、配置文件和本地用户数据
- 删除用户数据之前应有相应提示
- 不应应对系统及其他应用程序的正常运行造成影响

## 1.1.4 权限控制

客户端应遵循最小化及必要原则授予权限，避免数据泄露、非法提权等安全问题。对于因实际需要调用系统敏感资源（如位置信息、麦克风、照相机、通讯录、日历等），应采取显式方式告知用户并获得用户确认，并说明使用目的及业务场景。

## 1.2 安全运行

### 1.2.1 安全启动(APP)

客户端在启动时应执行自检，检查程序运行时所必须的条件，确保程序自身和所处运行环境的安全性。运行期间，应具备运行验证及相应防护机制，以防止运行数据被非法分析、非法调试或代码被非法执行。

### 1.2.2 CERT PINNING/CTL(APP)

建议应用实施证书锁定(Cert Pinning)或证书透明度（CTL）校验机制来确保客户端和云端通信的唯一性和安全性，该验证机制应持续性校验，以覆盖登录及登录之后相关应用场景，以防止被绕过。

证书锁定可以有两种实现方式：证书锁定（Certificate Pinning）和公钥锁定（Public Key Pinning）。

证书锁定验证应包括整个证书链（Certificate Chain）。

### 1.2.3 防HOOK及反调试(APP)

建议应用实施防HOOK和反调试检测，可以通过第三方工具实现（如Arxan,Bangle, etc.）。



## 1.2.4 身份认证

### 1.2.4.1 登录

用户登录应有身份认证机制。对于某些敏感应用场景（如支付、远控、更改用户名和密码等），应设置多因子的验证机制（如PIN、短信验证码、电话验证、生物识别等）。

#### 1.2.4.1.1 密码

建议的密码政策：

- 不低于8位，包括大小写字符、数字、特殊字符
- 定期强制修改（修改密码应验证原始密码）
- 尝试错误限制（如5次错误账号锁定等）
- 完善的密码重置流程（包括但不限于二次验证机制）

福特ISP要求：

所有没有特别访问权限的用户帐户都需要至少12个字符的密码。所有具有特别访问权限的用户帐户都需要至少16个字符的密码。

#### 1.2.4.1.2 验证码

建议的验证码政策：

- 至少六位
- 有效期应低于5分钟（推荐一分钟）
- 单次有效
- 尝试错误次数限制（3~5次，如超出错误限制次数，应锁定账户30s - 1min）
- 短信验证码调用接口应做相应限制（如具有抗机器识别能力的图形验证码）

#### 1.2.4.1.3 PIN

应增加PIN码机制，作为另一层的身份认证机制。PIN码应由用户在第一次成功登录后立即设置，PIN码输入时必须要有屏蔽机制以防止PIN泄露。应用闲置超过十分钟应要求重新输入PIN。

PIN政策

- PIN应最少4位。推荐6位或更多位数。
- 4位PIN码不可以为相同数字。（如1111等）
- 尝试错误限制（如5次错误PIN锁定等）

### 1.2.4.2 会话管理(TOKEN, SESSIONID等)

用户在登录之后建立会话应生成随机的身份认证凭证（如session id、token或secret key等），且该身份识别凭证应做到：

1. 随机性
2. 足够长（至少16字节）



3. 登录前后不同（每次登录也应不同）
4. 不同用户不同（以防止水平/垂直越权）
5. 加签，验签时间推荐为小于5分钟（推荐使用SHA256）
6. 不应暴露在URL中
7. 具有一定时效性及失效机制，token访问范围和有效时间应根据业务需要控制在最低限度（30 mins for access token, 1 year for refresh token）
8. 令牌提供者和客户应采用安全的、基于互联网的标准和协议（例如，OAuth 2.0、OpenID Connect 和 SAML 2.0）。
9. 保持令牌信息的机密性。（本地加密存储，云端KeyVault存储）
10. 令牌的真实性和完整性经过验证。
11. 令牌通讯渠道必须使用https, TLS1.2以上。
12. Refresh token必须是可撤销的。（如token泄露主动撤销和用户登出撤销）
13. Token中仅包括业务用例场景所必需的数据，不可包括PII

#### 1.2.4.3 设备授权

某些业务场景(需要用户同意)，可能需要用户和设备都经过身份验证。设备唯一标识符（UUID）可用于识别用户和设备

- 唯一性
- 不可重复
- 不可共享也不可被用于追踪
- 在安装或使用新功能时安全的生产并配置给设备
- 如应用卸载，该设备UUID也应失效
- 推荐同一用户同一时间仅可单设备登录

#### 1.2.5 安全登出

用户登出应用时，相应身份认证凭证（如session id、token或secret key等）应立即失效。

#### 1.2.6 输入/输出

为防止恶意、错误信息被传输到系统后台或被执行，应对所有用户输入信息实施后台云端验证机制（不可接受仅客户端验证），包括但不限于：

- 白名单/黑名单
- 字符编码（特殊字符）
- 字符长度及格式

服务端错误返回信息应保持一致统一，并做相应编码，且不应显示敏感信息（如服务器数据库相关信息等）。对返回到前端的敏感信息应做脱敏及加密处理，以防止数据泄露。



### 1.2.7 白盒/密钥

密钥必须使用安全存储（如KeyChain或KeyStore, HSM或者key vault），不能存放在应用配置文件中，且有定期更换和撤销、销毁机制，必须严格限制对密钥的访问，以防止密钥泄露。推荐使用白盒对传输敏感数据进行加解密。对于私钥应存放在TEE或Secure Enclave中。关键数据（如key, 密码等）在内存存放不应超过100ms。

### 1.2.8 其他安全防护（截屏、剪切板、键盘）

对于应用的关键操作或页面应禁止截屏，且采用相应错误屏蔽PII。对于关键操作的输入应禁止调用第三方键盘，禁止使用剪切板等。

### 1.2.9 监控日志

系统应监视并记录与安全性有关的事件，每个事件都应写入系统日志。系统应实现一个事件专用计数器，并且每个事件都应增加计数器。安全日志客户端应至少保留10天，云端应至少保留6个月。敏感日志应加密存储。

如需要应支持日志上传功能，上传时对云端进行认证；根据云端管理需求，采取安全的方式传输日志，确保数据的安全性、完整性、可认证性和可被审计。

操作系统应具有检测未经授权修改日志事件的能力。只能通过批准和授权的方法提取日志。

安全日志定义为与安全性相关的事件包括但不限于：

- 软件安装、更新
- 用户登入登出
- 关键功能操作
- 尝试访问敏感或关键数据
- 权限升级尝试
- 定义之外的事件
- 密钥管理相关事件

## 1.3 数据保护

### 1.3.1 PII识别与采集

PII包括但不限于：姓名、地址、电话号码、信息娱乐个性设置、GPS、信用卡号码、出生日期、驾驶行为、VIN、GUID、生物识别或医疗信息、个人证件号（如身份证、驾驶证、护照等）等。

所采集的与用户身份、位置信息等相关的PII，应通过单独显式的方式（不应放在用户使用条款和条件内）告知用户并获得用户确认，应说明数据采集所依据的国家法律法规或者业务需求。

对用户数据的采集应在提供相应服务的同时进行。若出于业务需要而必须事先采集相关数据，应向用户明示事先采集的目的和范围，并且只有在用户同意的情况下方可继续。

采集用户使用行为等用户数据时，应提示用户并向用户提供关闭数据采集的功能。在执行此类操作前，应首先对用户身份进行认证。

应具备支持国家监管部门依法进行数据采集工作的能力。





### 1.3.2 PII存储

PII不得以明文形式存储在客户端。

在将用户PII（例如：用户身份、位置信息）存储在系统时，应为保存数据的文件设置适当的权限，以防止未授权的访问和篡改。

存储涉及用户生物特征的数据时，应仅采取特征值，且应采用本地加密形式保存，原始数据及特征值不可以上传云端，原始数据在采集完成后应删除且不可恢复。

不应有未向用户明示且未经用户同意，擅自修改、删除用户数据的行为。

### 1.3.3 PII传输

若出于业务需要必须对PII进行传输，应向用户明示传输数据的范围和目的，并且只有在用户同意的情况下方可执行。PII传输应对信息进行加密，并对传输通道进行加密且有相应身份认证机制。

通过采集的用户数据，在传送到云端服务器后，防止用户隐私信息泄露。

当第三方服务访问车辆或人员时，对于PII信息（如 GUID、VIN、ESN 或个人信息）应加密或使用其别名。

绝不能通过备用渠道（短信、彩信等）发送PII；

URL 中不得包含PII；

不得缓存PII；

### 1.3.4 PII删除

用户提出删除PII信息要求后，应及时从系统（云端/客户端）中删除该用户相应的PII。



## 2. 云端

### 2.1 云端服务器

WebServer相关信息不应返回给客户端（如服务器请求错误时，不应返回给客户端关于服务器使用框架及服务相关敏感信息），应关闭不必要的端口及服务，不得将内网IP暴露给客户端。

### 2.2 云端应用框架/中间件/第三方组件

Web应用框架、中间件及第三方组件不应存在公开平台（CVE，CAVD,CNVD）披露的已知高危漏洞（如CVSS $\geq$ 7），并更新至最新版本。

### 2.3 云端应用配置

#### 2.3.1 通讯

##### 2.3.1.1 通讯协议

系统应强制使用HTTPS链接并实施TLS1.2以上版本，不得使用TLS压缩，并使用安全的密码套件（见3.2.3章节）。

##### 2.3.1.2 信息加密

传输的机密信息（如身份识别信息、密钥secret key等，见1.3.1章节）应加密传输，不低于AES256(AES/ECB除外)和RSA2048，并且使用SHA256以上算法防篡改。

#### 2.3.2 防火墙

应根据网络请求类型（如：GET, POST, PUT, DELETE等）设置过滤规则，设置相应白名单或黑名单。

应在网站系统和互联网之间的网络边界部署边界隔离设备，如防火墙等，并应配置合理的边界访问控制策略（白名单/黑名单），实现网站系统和互联网之间的逻辑隔离；

应仅允许互联网用户和内部用户访问指定的服务和端口，如web服务器提供的HTTP服务等，默认禁止访问不必要的服务和端口。（比如：22-ssh; 110-pop3; 514-shell等）。

#### 2.3.3 云端攻击防护

应具备以下WEB攻击防护功能：（以下一并列举了部分攻击防护建议措施）

##### 1. SQL注入攻击防护：

- 应对客户端提交的数据进行校验（包括但不限于字符格式类型及长度、特殊字符过滤、白名单/黑名单校验）
- 使用预编译绑定变量的SQL语句
- 使用参数化的sql查询，禁止使用动态拼接sql
- 避免直接返回错误信息，应返回统一的错误信息，不应包含数据库信息
- 对数据库敏感信息进行加密



## 2. XSS注入攻击防护:

- 应对客户端提交的数据进行校验（包括但不限于字符格式类型及长度、特殊字符过滤、白名单/黑名单校验）
- Set the X-XSS-Protection: 1, mode=block
- 使用自动转义的XSS框架，如Ruby on Rails, React JS
- 避免动态写入第三方数据到HTML（防止DOM型XSS注入）

## 3. XML/XXE注入攻击防护

- 对输入的XML元字符进行HTML编码
- 禁用加载外部实体

## 4. XPATH注入攻击防护

- 白名单机制验证用户输入，阻止任何可能破坏XPath查询的字符（如"(", ")", "\*", "/"等）

## 5. LDAP注入攻击防护

- 白名单机制验证用户输入，阻止任何可能破坏LDAP查询的字符（如"(", ")", "\*", "|", "&"等）
- 基于必要且最小化原则授予账号LDAP权限

## 6. SSI注入攻击防护

- 不建议在WEB站点中使用SSI
- 清理用户输入 - 禁止可能支持 SSI 的模式/字符

## 7. 命令注入攻击防护

- 对于用户输入进行编码处理
- 白名单机制验证用户输入

## 8. 文件上传防护

- 文件上传的目录设置为不可执行
- 判断文件类型（结合使用MIME Type、后缀检查等方式，白名单方式）
- 使用随机数改写文件名和文件路径
- 单独设置文件服务器的域名

## 9. 高并发请求防护

- 应使用锁机制以防止客户端并发请求

## 10. 其他WEB攻击防护

### 2.3.4 管理后台

管理后台如无对外开放必要，则应限制外网访问，如因实际需要开放外网访问，应配置网络访问白名单，杜绝非授权IP访问。管理后台应基于最小化及必要原则授予权限，并设置应用较强的身份认证机制（如二次身份认证）。应配置并启用登录失败后结束会话、限制非法登录尝试次数和超时自动退出相关措施，及时更改或删除系统中默认口令、无用账号以防止管理员身份信息泄露。对管理员所作操作应有相应日志

### 2.3.5 数据库

云端数据库系统不应存在公开平台（CVE, CAVD, CNVD）已知高危漏洞（如CVSS≥7）。应采取相应措施确保数据的独立性（物理/逻辑）、安全性、完整性。应配置严格的数据库访问策略（如网络访问白名单、严格身份验证



等)。PII应加密存储和传输，并记录对PII操作事件（如查询、修改、删除等）。关闭或不使用默认数据库端口（如1434 – SQL Server、1521 – Oracle、3306 – My SQL）。

不得将存储配置为允许从公共 Internet 访问以进行读取或写入。

必须在“需要知道”的情况下授予对管理门户的访问权限，并且仅限于福特人员，特别是员工类型 F、P、A、M 和 H。

当福特内部用户进行身份验证时，Web 控制台必须与福特的 ADFS（Active Directory 联合服务）集成

### 2.3.6 数据备份和恢复

系统在应有数据备份功能，并保证备份的及时性、数据的正确性、完整性、可用性。备份可以根据业务需求采取完全备份或增量备份。备份方式应支持手动备份和自动备份，自动备份应具备一定的实时性。

系统应可以使用备份文件手动或自动恢复静态网页文件、动态脚本文件、网页目录、数据库数据等。

CONFIDENTIAL



## 3. 通讯

### 3.1 客户端 (APP)

使用安全机制，检测和防止应用软件之间不必要的访问及调用(包括但不限于广播发送/接送，activity调用等)，避免数据泄漏、非法提权等安全问题。具备识别、阻断恶意软件的能力，隔绝已经被感染的文件，拒绝软件的恶意访问。

### 3.2 客户端与云端

#### 3.2.1 TLS

实施TLS的最低版本应为TLS 1.2。除特别批准外，任何使用蜂窝连接的模块或SDN都不允许协商使用较低版本或密码套件。

#### 3.2.2 TLS超时

所有TLS会话均应在启动后六小时内超时。如果超过六个小时，则应执行新的TLS握手。

#### 3.2.3 TLS密码套件

所有TLS通信都应仅支持以下密码套件（按优先级顺序列出）：

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 \*
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 \*

\* 对于普通的Diffie-Hellman密钥交换（DHE），必须使用至少2048（DH组14）的密钥长度。如果不支持2048个密钥长度，并且不支持其他安全协议，则可以使用密钥长度1024（DH组2,5），并保证DHE密码套件位于优先级列表的底部。在技术支持下，ECDHE密钥交换应替代DHE

根CA证书的有效期限最长为30年（后端的单个证书的有效期限应较短，例如1年）。

#### 3.2.4 TLS压缩

不得使用TLS级压缩。

#### 3.2.5 TLS证书颁发机构

TLS连接只能使用福特批准的证书颁发机构。



### 3.2.6 MTLS证书锁定

如果使用双向TLS身份验证，则系统应使用带有OSCP响应的证书锁定来验证每个主机的身份。

### 3.2.7 主机认证

应验证URL主机是否与TLS服务器证书中的主机和主机备用名称字段匹配。如果证书中的主机名与URL主机不匹配，则模块应拒绝连接。

### 3.2.8 验证对等方

协商TLS连接时，均应使用“验证对等方”或类似功能来验证证书的真实性。如果验证失败，则应拒绝连接。

### 3.2.9 证书安全

确保所有证书始终是最新的

- 建议在证书到期前 6 个月轮换证书以减少意外停机时间

不得使用自签名证书

如果证书无效或不受信任，应用程序不得为用户提供继续的选项

## 3.3 云端与云端

### 3.3.1 身份认证

云对云通讯建议采取IP白名单+MTLS双向认证+APIM层级token/credential以实行完善的身份认证

### 3.3.2 输入/输出

为防止恶意、错误信息被传输到系统后台或被执行，应对所有用户输入信息实施后台云端验证机制（不可接受仅客户端验证），包括但不限于：

- 白名单/黑名单
- 字符编码（特殊字符）
- 字符长度及格式

服务端错误返回信息应保持一致统一，并做相应编码，且不应显示敏感信息（如服务器数据库相关信息等）。对返回到前端的敏感信息应做脱敏及加密处理，以防止数据泄露。