China Cyber Security

IVI Security Requirements

Version 1.5

UNCONTROLLED COPY IF PRINTED

FORD CONFIDENTAL

Revision History

Date	Version	Created/Modified By	Notes
4/9/2020	1.0	JSHAO13/JXU125/CSUN26	Initial Version
11/9/2020	1.1	CSUN26	Update 3.4.4 – Add version control on OTA
2/5/2021	1.2	CSUN26	Add cyber security requirements on non-connected module
18/5/2021	1.3	CSUN26	Update 5.2.4.4 – Update approved TLS Cipher Suites
21/12/2021	1.4	CSUN26	Update chapter 3.3/5 – Added fuzzing test requirement on USB and communication protocols
10/3/2022	1.5	CSUN26	Updated chapter 4.1.6, 4.2.6, 4.3.1, 4.3.3, 4.5, 5.2.1, 5.2.2.1.2 based on new published GB/T 40856-2021 and GB/T 40861-2021

CONTENTS

1. INTRODUTION

1.1 EXECUTIVE SUMMARY

此文档旨在提供福特汽车对于车载娱乐系统（IVI）的网络安全要求。

1.2 PURPOSE OF DOCUMENT

本文档概述了福特汽车公司对于车载娱乐系统的网络安全基本要求，除另外说明，否则此文档应作为供应商一般指南。

本文档主要关注以下几个方面：

- ECU网络安全基本要求
- IVI硬件安全
- IVI软件安全
- IVI通讯安全

1.3 REFERENCES

此章节包含了所有相关国家标准（及征求意见稿），国标中相关网络安全要求都必须满足（征求意见稿一旦变为国标，其相关网络安全要求也必须满足）。在国标的基础上，本文档定义了福特汽车对于网络安全的公司要求。

标准号	标准名称
GB/T 35273-2020	信息安全技术 个人信息安全规范
GB/T 20008-2005	信息安全技术 操作系统安全评估准则
GB/T 28452-2012	信息安全技术 应用软件系统通用安全技术要求
GB/T 32927-2016	信息安全技术 移动智能终端安全架构
GB/T 40856-2021	车载信息交互系统信息安全技术要求及实验方法
GB/T 40861-2021	汽车信息安全通用技术要求

征求意见稿名称
信息安全技术 车载网络设备信息安全技术要求
汽车整车信息安全技术要求与试验方法

1.4 TERMINOLOGY AND ABBREVIATIONS

Term	Description
IVI	In-Vehicle Infotainment
SPID	Security Package Identifier
FESN	Ford Electronic Serial Numbers
TLS	Transport Layer Security
OSCP	Open Source Contribution Process
POSIX	Portable Operating System Interface
SE	Secure element
FNOS	Ford Network Operating System
CMAC	Cipher-based Message Authentication Code
TEE	Trusted execution environment

2. 非联网模块的基本网络安全需求

IVI应满足非联网模块的基本网络安全需求并依照相应测试方法提供测试报告。

2.1 基本网络安全需求及检测方法

2.1.1 RQT-001403-020627 网络安全ESOW合规性-网络安全

供应商应提供《福特供应商保证书》的收据和遵守证明工作说明书（FSCA-SOW）。

注意：FSCA是通用eSOW软件包的一部分，将作为采购软件包的一部分提供文档。 eSOW附件可以从官方通用以下链接ESOW存储库下载：

文件链接：
https://pd1.spt.ford.com/sites/VCSE/NonCoreContributors/ESOW/ESOW/Current/b.%20General%20Attachments / B.10%20Ford_CyberAssurance-SOW_ReleaseV1.1.doc

eSOW主站点：
https://pd1.spt.ford.com/sites/VCSE/NonCoreContributors/ESOW/Forms/AllItems.aspx?RootFolder = / sites / VCSE / NonCoreContributors / ESOW / ESOW / Current /

检测方法 TM-00.14-E-11225 FSCA-SOW合规性

验收标准：车载安全组的审查和批准的清单表

所需数据：完成eSOW清单

2.1.2 RQT-001403-020628 安全算法评审-网络安全

ISO14229 SecurityAccess（0x27）的任何实现均应使用标准安全算法。SecurityAccess类型 0x01至0x41是制造商范围，应被用于支持福特所请求的SecurityAccess类型。供供应商使用的SecurityAccess类型应使用0x61至0x7E。

建议的算法应由福特安全团队审查和批准。作为审查的一部分，供应商应：

1. 提供有关算法类型及其实现的详细信息
2. 定义实施所需的所有安全属性
3. 验证秘密密钥是否受到保护，防止未经授权的访问，并且没有以明文形式存储在RAM / EEPROM
4. 确保加密模块安全失败
    a. 无效的输入不应得到授权回应
    b. 微重置应始终以未经授权的状态开始
5. 建立并利用策略和流程来管理密码密钥

基于供应商的密钥生成应具有定义的密钥管理策略，该策略应由福特审查和批准安全团队。

对于新的福特钥匙管理流程，申请者应提供管理密钥和对ECU性能要求/影响方面的策略和流程的文档。

注意：Vector作为Autosar的一部分提供的SecurityAccess子功能0x01和0x03算法或CANBedded OS库已由福特审查和批准，除非经过修改，否则不需要重新验证。

检测方法 TM-00.14-E-11120 安全算法验证

验收标准：审核

所需数据：完成检测方法

2.1.3 RQT-001403-020629 通过DID访问安全关键数据防护-网络安全

通过ISO14229 0x22（ReadDataByIdentifier）的所有服务请求和ISO14229 0x2E（WriteDataByIdentifier）用于读取/写入存储安全关键数据的DID应通过ISO14229 0x27（SecurityAccess）身份验证机制防止外部来源的攻击。
每当添加新的受保护DID时，都应执行此DVM。
注意：在RQT-001403–020617上标识了安全关键数据列表

检测方法 TM-00.14-E-11121 所有存储安全关键数据的DID的访问控制
验收标准：
所需数据：供应商遵守所有DID的规定证明

2.1.4 RQT-001403-020655 通过诊断程序31的安全功能输入及控制的防护

所有诊断服务程序（ISO14229 RoutineControl 0x31初始化，终止，配置和访问安全关键功能和安全关键数据应通过ISO14229 SecurityAccess（0x27）认证保护免受外部调用机制。
安全关键功能被添加通过常规控制0x31进行访问时，都应执行DVM。
注意：请参阅RQT-001503-020617上确定的安全关键功能列表

检测方法 TM-00.14-E-11122 通过0x31（RoutineControl）调用安全功能服务防护
验收标准：
所需数据：演示对通过诊断常规程序访问的安全性至关重要的I / O输入的适当保护

2.1.5 RQT-001403-020656 通过HEX 2F输入安全功能防护-网络安全

所有调用ISO14229 InputOutputControlByIdentifier 0x2F修改ECU安全关键功能的输入或输出的功能都应受到保护，以免通过ISO14229 SecurityAccess（0x27）身份验证机制进行外部调用。
安全关键功能被添加通过服务0x2F进行访问时，都应执行DVM。

检测方法 TM-00.14-E-11124 通过诊断例程（0x2F）对安全功能输入和控件安全防护
验收标准：演示通过诊断常规程序$ 2F访问关键功能输入的防护
所需数据：DV测试报告

2.1.6 RQT-001403-020657 网关上的消息控制-网络安全

ECU只能放行车载网络与给定消息的任何网络（车载或其他方式）且在福特批准预定义的白名单上的通信。
定义：
白名单是允许在网络之间传输的邮件的完整列表（包括CAN、LIN、以太网、BT、WI-FI等）。福特CMDB是福特批准的白名单。对于特定的ECU，任何超出CMDB以外的内容需记录在白名单中。
定义：
福特批准的白名单包括但不限于

- NetCom发布福特批准的白名单（CMDB）
- LIN具有福特D＆R批准的LDF文件
- SYNC / TCU团队批准无线白名单

福特批准白名单的方向：

- 仅批准对功能至关重要的消息
- 批准功能所需的最少ISO14229诊断消息
- 除非已加密，否则避免存储PII
- 避免使用安全关键数据，除非已对其进行加密/数字签名
- 其他特殊情况下的获取/擦除密钥（例如制造/服务）。

检测方法 TM-00.14-E-11125 网关模块上的消息控制（测试方法）

验收标准：测试证明未在白名单中的通信被成功阻止

所需数据：DV测试结果

2.1.7 RQT-001403-020661 通过安全关键数据的地址进行内存读/写-网络安全

在量产ECU（TT及更高版本）上，所有用于直接读取安全关键数据的内存方法应仅允许ISO14229 SecurityAccess（服务0x27安全级别0x03或更高）。

在量产ECU（TT及更高版本）上，所有直接写入内存方法应仅允许被授权的ISO14229 SecurityAccess（服务0x27安全级别0x03或更高）。

这包括但不限于：

- ISO14229 ReadMemoryByAddress（0x23）
- ISO14229 WriteMemoryByAddress（0x3D）
- XCP（通用测量和校准协议）
- CCP（CAN校准协议）

注意：供应商EOL操作可能允许例外或使用XCP和CCP控件。 这些例外情况必须由福特SME或D＆R和福特汽车安全部门审查并批准。

注意：有关JTAG访问要求，请参考RQT-001403 – 020667

检测方法 TM-00.14-E-11149 通过安全关键数据的地址进行读写

验收标准：

所需数据：DV测试

2.1.8 RQT-001403-020665 RAM中安全关键数据处理-网络安全

危及或规避ECU /车辆安全保护机制的安全关键数据使用后，决不能以明文形式存储在RAM中超过100毫秒。 该信息可以被擦除，散列或加密。

这包括但不限于

- 密码

- 代码内或代码外值
- 车辆进入/启动PIN
- 预先计算的响应

注意：PII数据是可选的

注意：RAM包括调用堆栈

注意：Vector作为Autosar或CANBedded库的一部分提供福特安全访问算法的内部变量豁免。 预先计算的响应不应被存储，其应按需计算。

检测方法 TM-00.14-E-11183 通过诊断方法访问RAM

验收标准：供应商证明安全关键数据的所有瞬时变量都满足此要求。

所需数据：DV测试结果

2.1.9 RQT-001403-020666 随机数生成器-网络安全

允许使用基于硬件或基于软件的随机数生成器。 至少所有随机数生成器都应符合NIST SP-800-90A或AIS 31 DRG.2（首选NIST SP-800-90C）。 RNG必须通过NIST统计测试套件（NIST SP-800-22）中的所有适用测试。 PRNG的种子方式应确保重置（UDS $ 11）和电源循环不会导致重复的随机值。

注意：不需要由独立实验室对NIST-SP-800-90A / B / C进行认证

注意：其他RNG标准也可以接受，需经福特安全团队进行审查和批准，并向NIST统计测试套件提交证据。

目标：确保用于保护安全功能的RNG达到最低质量并经过测试。

理由：RNG产生的数字对于确保良好的安全强度（包括种子/密钥挑战）至关重要。 产生可预测或重复的数字可能会削弱RNG支持的安全协议。

检测方法 TM-00.14-E-11184 随机数生成器

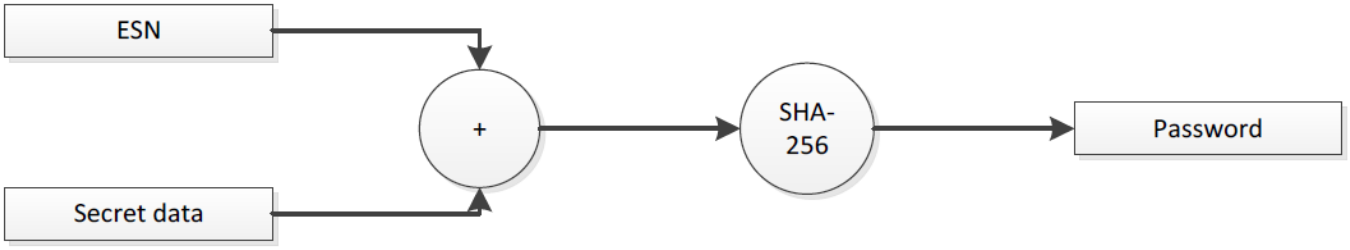
验收标准：随机数生成器通过NIST基准测试

所需数据：DV测试结果

2.1.10 RQT-001403-020667 微调试接口的访问控制-网络安全

在量产ECU（TT及更高版本）上，访问硬件的调试接口（例如JTAG，BDM）必须禁用或使用模块唯一的序列号（而非安装PN）密码防护。密码应符合最小密码复杂度策略或微控制器允许的最大长度。如果可以，最好使用片上硬件安全模块（HSM）功能来保护ECU内部的密码。当存储在非福特数据库中时，所有密码均应加密并安全受保护的存储。

或者，可以使用可接受的算法（例如SHA256，AES等）通过输入序列号+“秘密数据”（可在模块之间共享）输入密码。该算法应确保没有重复的密码。 “秘密数据”是由供应商选择的非零值，例如UUID。



注意：对于备用密码生成方法，不需要在ECU上实现用于生成密码的算法。密码可以生成为模块配置的一部分，并安全地存储在模块中，并防止其被读出。

注意：断开硬件端口与微型ECU的连接或减少量产ECU上的填充不足以满足此要求

注意：供应商应向福特SME提供有关其密码生成/存储的实施详细信息，以满足这一要求。

检测方法 TM-00.14-E-11185 访问调试接口

验收标准：所有量产模块均应禁用或保护调试端口

所需数据：DV测试结果

2.1.11 RQT-001403-020668 移除硬件和软件后门访问-网络安全

在交付服务或量产（TT）时，模块应仅响应福特汽车批准的输入。 这包括特殊的供应商EOL配置功能，软件后门如未定义的仅供供应商使用的DID，硬件后门和CCP / XCP等。

注意：密码保护的JTAG / BDM /串行端口不被视为后门（请参阅RQT-001403-020667）

注意：由RQT-001403 – 020626中指定的3级或更高保护等级保护的CCP / XCP /调试接口不视为后门程序。

检测方法 TM-00.14-E-11186 移除硬件和软件后门

验收标准：移除或充分保护所有后门

所需数据：所有软件和硬件后门的枚举

2.1.12 RQT-001403-020669 ECU内的访问定义-网络安全

在量产模块（TT及更高版本）中，诊断工具只能通过以下批准的方法修改应用程序/策略，主引导加载程序或EEPROM：

批准的方法	应用程序	FlashData文件	主引导程序	EEPROM/DataFlash
解锁JTAG，BDM，串行接口	X	X	X	X
辅助引导加载程序（SBL，由福特软件下载规范定义）	X	X		
批准的ISO14229诊断服务				X

检测方法 TM-00.14-E-12927 软件访问控制

验收标准：

所需数据：DV测试报告

2.1.13 RQT-001403-020671 模块重置后的安全默认状态-网络安全

在进行任何复位之后，ECU应用程序/策略应以安全状态启动，并且应维护保留组件安全性的系统功能。 所有外部xmit / recv缓冲区应初始化为默认值

定义：安全状态是一种对安全关键功能和安全关键数据的所有保护都在起作用并阻止访问的状态。

定义：安全状态包括但不限于：

- 阻止对安全关键功能响应的安全机制
- 阻止访问对安全至关重要的数据进入内存的安全机制
- 读/写保护级别（请参阅RQT-001403 – 020626）

定义：维护组件或车辆安全性的系统功能包括但不限于：

- 周边警报已开启
- 车辆处于“锁定”状态
- 车辆防盗器

检测方法 TM-00.14-E-11230 重置后的安全默认状态

验收标准：设计验证

所需数据：DV测试

2.1.14 RQT-001403-020672 授权软件下载-网络安全

量产ECU（TT和更高版本）应仅接受包含有效数字签名的SBL和应用软件（包括配置和校准文件）。如果一个ECU有一个以上的微控制器，则应在最终的目的地微处理器上验证SW签名。

定义：有效签名是由授权实体发布的签名：

1） 在开发ECU上，可以将软件开发团队（Tier1或福特）指定为授权实体来签署软件以进行测试

2） 对于量产ECU，福特安全后端是唯一签署生产软件的授权实体

注意：App_Signing_requirement文档中描述的过程适用于具有真正RTOS的ECU。具有传统操作系统（QNX，Linux等）的ECU将使用标准的PKI签名创建/验证（即x509）进行软件完整性验证。

注意：请参考签名章节以获取流程定义和可接受的文件格式（VBF）。假设HSM或ECU中不存在其他安全元件时，建议的实施方案应将其视为ECU上软件验证的基准。只要满足以下假设，就可以接受其他实现方法：

1）文件格式符合福特规范

2）福特是生产文件的唯一签名机构

3）哈希和签名算法符合福特规范

4）如果福特签名失败，则不允许在量产ECU上安装软件

检测方法 TM-00.14-E-12929 软件签名验证

验收标准：量产ECU仅接受福特批准的证书颁发机构（CA）签署的软件

所需数据：DV测试

2.1.15 RQT-001403-705880 不使用公开的密钥-网络安全

先前公开的加密机密材料不得在开发或量产软件版本中使用。在整个产品生命周期中，加密密钥应：

- 包含根据NIST准则唯一生成的值。
- 不可重用或使用默认值。（例如，空白密码，“密码”，“ 1234”，全0或全1，在已发布的标准中用作示例的密钥/密码）。
- 在支持用户角色的系统中，必须在量产中禁用根帐户。

在开发或量产期间的任何时候，加密密钥都会被暴露或泄露，应根据NIST准则重新生成替换值，并在包括开发在内的所有版本中将其替换。

注意：安全访问固定字节应遵循GGDS规范中定义的生成要求，而JTAG密码应遵循RQT-001403-020667微调试接口的访问控制生成要求。

注意：此要求不适用于客户设置的PIN码或密码，例如门密码。

目标：防止量产软件意外地包含具有已知值或先前已公开的密钥。

定义：密码密钥是用于身份验证，加密或解密的任何信息或参数。

- 密码/密码
- 对称密钥/私钥
- 初始化向量

定义：先前公开的加密密钥是旨在对应用程序秘密材料但已暴露给潜在攻击者的任何加密元素或密码。这包括但不限于：

- 在标准中合法发布，例如标准中包括的Bluetooth L2Cap加密示例密钥
- 偶然的，例如在公开可访问的GitHub中意外发布的密钥
- 提取的机密，例如黑客从DVD硬件提取的DVD解密密钥

理由：默认和公开的密码秘密是公共知识，并且将提供访问权限给恶意攻击者，从而破坏了预期目的。通过要求即使在开发过程中也必须唯一地生成加密密钥，可以降低在量产软件中意外包含已公开机密的风险。

检测方法 TM-00.14-E-705085 不使用公开的密钥-网络安全

验收标准：设计中未使用默认密钥或PIN

所需数据：DV测试

2.1.16 RQT-001403-706883 识别和保护安全关键功能和数据-网络安全

所有安全关键数据和安全关键功能（请参阅下面的定义）都应得到标识。子系统中影响（即启动/终止/提供/命令的输入）安全关键功能，并通过诊断命令/请求存储/传输安全关键数据的每个组件，均应采用适合风险级别的安全机制进行保护。福特SME / D&R，功能所有者，一级供应商应根据感知到的风险级别为所有安全关键功能和数据提出适当的保护级别。防护机制应由车载安全团队审查和批准。

对于每个数据或功能，工程团队应：

- 创建并跟踪唯一的ID
- 提供功能或数据用途的简要说明
- 确定潜在的攻击机制
- 提出适当的保护机制（下面的IAW定义）
- 识别和分配用于读取和写入的保护级别（下面的IAW定义）
- 识别将在其中测试或检查该机制的DVM
- 审查并获得福特安全团队的批准。

以上要求的摘要应记录在“安全关键功能和数据”模板中。

每当模块合并了新功能，连接更改，更新/添加/删除安全控制措施时，均应对安全关键功能和数据进行重新评估。即使对程序的审查已完成并获得批准，但功能或安全控制发生了变化，也应进行重新评估。

推荐保护级别3的供应商应确定支持保护级别且不依赖福特系统的后端系统，除非福特安全团队另行同意。

目标：记录模块中包含的安全关键功能和数据，并确保实施了适当的保护方法以防止恶意篡改或激活。

注意：此要求取代RQT-001403-020617-安全功能的标识-网络安全和RQT-001403-020626-识别和查看安全保护机制-网络安全。仅需要一个模块即可完成（RQT-001403-020617和RQT-001403-020626）或（此要求），而无需同时完成。 RQT-001403-020617和RQT-001403-020626最终将被废弃以支持此要求。

定义：关键安全功能是可以影响车辆安全性的车辆功能或诊断操作（例如，偷车，偷PII，欺诈性控制汽车等）。

以下是被视为安全关键功能的某些功能类别：

- 控制进入车辆内部的通道（例如，锁定/解锁，远程解锁等）
- 控制外部进入点（例如，加油口，注油口等）
- 控制车辆的启动（例如点火控制，燃油泵等）
- 控制安全特定功能（例如防盗警报，被动防盗）
- 控制车辆动态（例如转向，刹车，油门等）
- 控制车辆诊断命令/控制（例如，校准转向角传感器，放气ABS，ECU重置，I / O控制等）
- 存储/读取基本或敏感（PII）等级的个人可识别信息
- 通过诊断，服务，制造或其他实用程序提供写访问权限的所有功能（出厂诊断服务）
- 可以在服务器外发送数据或使用无线通信链接（例如Wifi，蓝牙）与移动设备（例如手机，平板电脑，笔记本电脑等）进行通信的功能
- 保护获利功能或服务的功能（例如，启用付款，升级付款，集成的车辆付款系统或直接支持付款的功能）
- 法规要求的功能

定义：安全关键数据是系统中的值（影响汽车或其用户的安全性）。安全关键数据包括但不限于：

- 安全凭证（例如密码，密钥代码）
- 在加密或解密过程中使用的临时变量，用于存储可以推断出秘密值的值
- PII和位置信息
- 福特专有的安全算法或例程。

- 用于配置车辆安全关键功能的状态或处于降级状态的数据（例如，高级警报，CAN消息身份验证，网关网络保护，SOA TLS等）
- 法规要求的数据

定义：个人身份信息（PII）是有关个人的任何信息，可用于区分或追踪个人的身份以及与个人链接或可链接的任何其他信息。（根据NSIT SP 800-53）。排名越高，数据越敏感。

- 如果明显降低了PII数据的数量，则所有非PII数据（大多数技术传感器数据），VIN（机载），体重和身高（除非生物识别精确），个性化设置（例如，座椅位置，无线电预设，闪电偏好）均会提高 模块中存在数据元素。
- 基本的P.I.I. 例如 GPS，驾驶行为（随时间变化的存储模式（例如时间戳，存储缓冲区）），显示驾驶员的操作习惯（例如转向，安全带，制动，加速），姓名，地址，电话号码，可视图像
- 敏感的P.I.I. 例如 带时间戳（或随时间存储）的GPS，信用卡，DOB，SSN，生物识别数据，医疗数据

定义：适当的保护机制是一种功能，可以保留所需的数据和常规安全性。这包括：

- 身份验证机制（确定是否允许代理访问特定资源）
- 完整性机制（防止未经授权的消息修改/写入）
- 机密性机制（防止未经授权的数据读取）

定义：保护级别是根据已确定的安全关键功能或数据元素进行的访问的分类。保护级别定义如下：

- 级别0：（PL0）- 无。在正常操作条件下允许访问
- 级别1：（PL1）- 仅在扩展诊断会话有效时才允许访问。
- 级别2：（PL2）- 仅当授予标准安全访问权限时才允许访问（ISO14229 $ 0x27安全级别$ 01或$ 03）。
- 级别3：（PL3）- 仅当授予增强的安全访问权限时，才允许访问（ISO14229 $ 0x27 安全级别$ 3B）。在允许访问之前，需要进行后端服务器身份验证（例如FIMCO或其他将来的系统）
- 4级：（PL4）- 在所有情况下都拒绝访问。

注意：保护级别与安全访问子功能不同（例如，服务$ 27子功能$ 01，服务$ 27子功能$ 03或服务$ 27子功能$ 3b）。

注意：保护级别3需要后端身份验证系统才能提供访问权限（例如，安全令牌），但是福特通常不提供此系统。福特FIMCO（$ 3b）预留给PATS和某些物理访问系统。

注意：对底盘系统，有冲突情况下，RQT-060900-006128取代了此要求。

Ford Motor Company
Security Critical Functions and Data Form

Identification	
Module Name:	
Module Acronym:	
Vehicle Program(s):	
Supplier:	
Part Number:	

	DVP Team #:	
	CPSC:	
	Revision:	
Preparer	Name:	
	Company:	
	Phone:	
	Email:	
	Date:	
Reviewer	Name:	
	Company:	
	Phone:	
	Email:	
	Date:	

Security Critical Function						
ID	Function	Description	Potential Attack Methods/Scenario	UDS PL Read/Write	Protection Method	DVM

Security Critical Data						
ID	Data	Description	Potential Attack Methods/Scenario	UDS PL Read/Write	Protection Method	DVM

Review Actions			
Item ID	Findings	Recommended actions	Owner

检测方法 TM-00.14-E-703144 识别和保护安全关键功能和数据-网络安全

验收标准：

所需数据：完成表格

3. IVI Hardware

3.1 关键安全数据

关键安全数据包括但不限于用户身份凭据、密钥、证书、系统配置文件等。
车端具备硬件实现的安全区域或安全模块（比如TEE、SE），实现车载端设备关键安全数据安全存储与隔离。
在安全区域或安全模块中一次性写入的敏感信息，应保证无法非授权获取或者篡改。
安全区域或安全模块应具备检测与处置非授权访问的能力，对抗暴力破解。

3.2 安全调试端口/服务管理

原则上，所有调试端口（比如ADB, UART, JTAG）及不使用的服务协议都应被禁用（物理禁用，如无电源；软件禁用）或移除以防止固件代码被提取或被篡改。如有需要启用或访问调试端口和服务，必须为其分配一个唯一的身份验证证书。 当包含多个微控制器时，每个微控制器应具有唯一的身份验证凭据（如密码、证书、调试令牌）。唯一身份凭证可以从批准的随机或伪随机函数派生。调试端口访问和启用事件应被记录并报告。

3.3 可移动存储介质或USB设备的过滤

应建立严格的USB和存储设备筛选机制（比如白名单），并成功通过福特认可的模糊测试，以使得仅允许安装或使用具有已知配置的受信任设备。

3.4 PCB板/芯片安全防护

车载端系统的电路板不能存在用以标注芯片、端口和管脚功能的可读丝印。
车载端系统所使用的芯片不能存在可以非法对芯片内存进行访问或者更改芯片功能的隐蔽接口。芯片在设计验证阶段使用的调试接口应在上市产品中禁用。
车载端系统芯片之间敏感数据的通信线路应尽量隐蔽（例如：使用多层电路板的车载端系统采用内层布线方式隐藏通信线路），对抗针对车载端内部数据传输的窃听和伪造攻击。
车载端所使用的关键芯片应尽量减少暴露管脚（例如：采用 BGA/LGA 封装的芯片）。

3.5 抗攻击防护

使用必要的安全机制（例如：封装），防御针对芯片的电压、时钟、电磁、激光等方式的故障注入攻击。
使用必要的防护措施，对抗针对加密芯片的简单功耗分析（SPA）攻击、一阶差分功耗分析（DPA）攻击、相关功耗分析（CPA）攻击，以及利用运行时间、温度等其它信息进行的侧信道攻击。
使用必要的防护机制，以对抗针对车载端设备内存的侵入和篡改攻击。

3.6 文件系统加密（推荐）

数据存储应使用从特定系统数据派生的密钥加密。 此数据应由处理器的受信任区域保护，或应加盖到裸片中，攻击者无法访问或读取。 重要的是，断电时设备上没有有效的安全保护，所需要的任何安全措施必须同时能够承受脱机攻击。

4. IVI Software

4.1 OS

4.1.1 安全启动

IVI中SOC及MCU均应支持安全启动。系统应使用特定方法在系统启动时验证系统软件（包括存储信号白名单的模块）未被修改，且未执行未经验证的代码。 所有模块在启动时均应验证所有引导程序和系统软件均未被修改。操作系统不得执行未经验证的代码，其可以在系统完成安全启动过程之前执行已验证的代码（经过验证的代码是指经过验签的软件或二进制文件，且自安装以来未被修改）。
此操作所需的所有密钥和证书均应存储在防篡改的集成电路中并加以保护。防篡改集成电路是HSM、SHE、TPM、ARM信任区域或其它类似设备。
MCU安全启动应支持算法：CMAC。

4.1.2 内存保护

操作系统应为应用程序的堆栈和堆实现并启用内存保护机制。 内存保护的示例包括但不限于：地址空间布局随机化（ASLR），位置独立执行（PIE），只读重定位（RELRO），无执行（nX）和数据执行保护（DEP） 。实际启用的保护应取决于操作系统的支持和网络安全团队的批准。

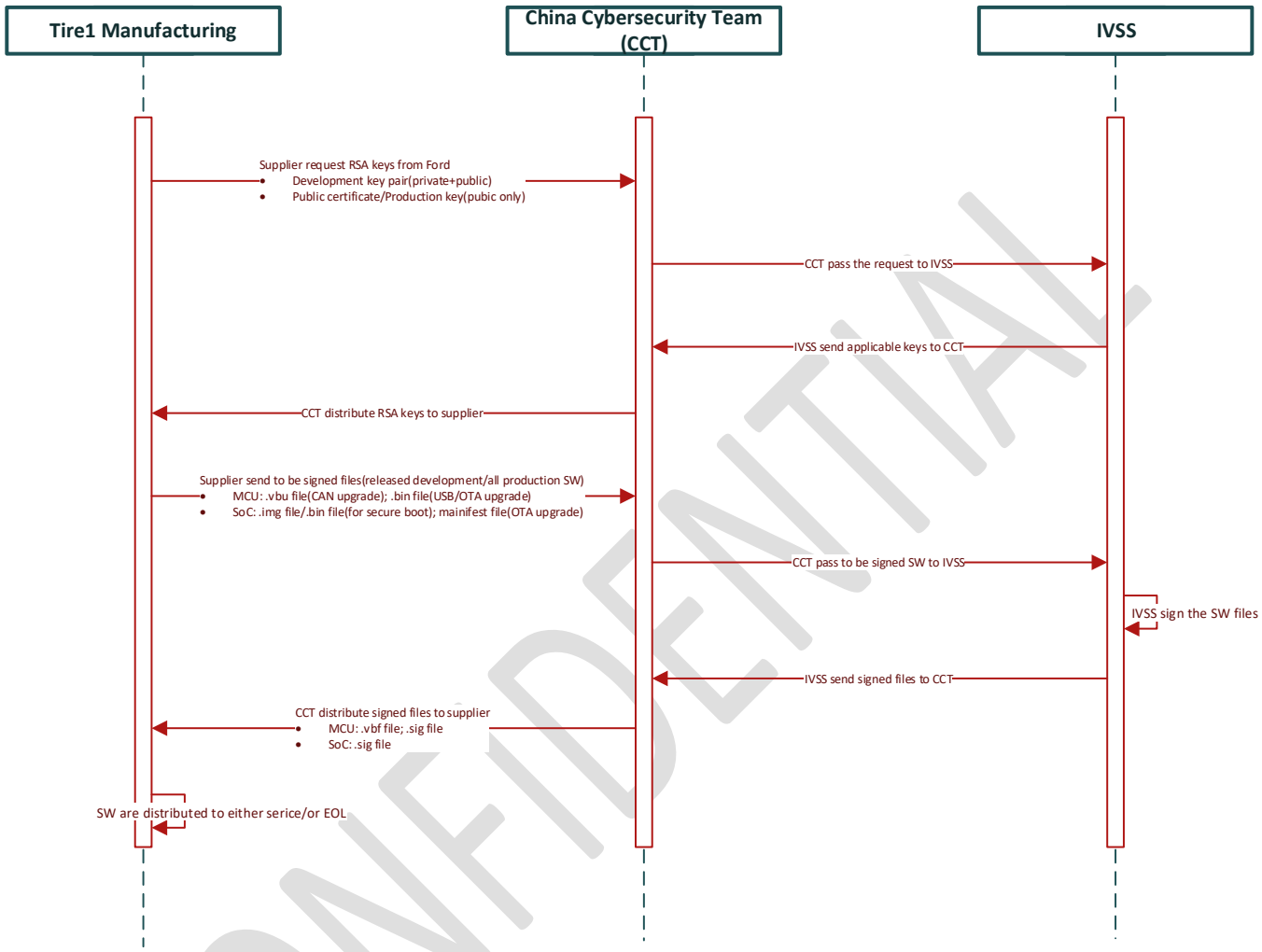
4.1.3 代码签名

模块应支持代码签名并验证要安装到该模块上的代码的签名。 仅接受由福特签名的代码才能生产。 只能使用批准的密码库，并且每个实例都应记录在案。 ECU内的每个处理域都应具有唯一的代码签名叶子证书或公私钥对。
定义：通过使用福特认可的信任链来验证代码，数据，脚本和原始发件人。 信任链机制应使用福特批准的公钥/私钥对和签名，例如：X.509证书PKCS＃7，RSA-2048。
批准的密码库包括但不限于：OpenSSL，boringSSL，TomCrypt。

4.1.3.1 签名概述

所有刷新到SOC/MCU的二进制文件（例如辅助引导程序，应用程序，校准，校准配置等）都应被签名（包括CAN或OTA软件升级），任何其他允许更新主引导加载程序（PBL）的应用程序也都应被签名。
每个模块都有一个公用密钥，以验证该特定模块上多个软件文件的签名。生产和开发密钥都应由福特生成，并将交付给Tier1供应商。福特是唯一签署包括校准和校准配置文件在内的生产阶段二进制文件的实体，相应生产阶段文件在正式发布前，均应交由福特签名。供应商可以使用开发密钥对开发阶段软件进行签名以支持软件开发。
哈希（SHA256）和加密库（RSA）应包含在主引导加载程序（PBL）中。供应商（Tier1）将编译公共密钥到主引导加载程序（PBL），并将其刷到模块中，更新/更改公钥也是通过PBL来更新。
注意：基于各模块功能及实际情况，存在多种签名验证和/或公钥存储方法。在得到福特车载网络安全团队批准的情况下，可以允许实施替代方案。

4.1.3.2 主要流程:



开发测试环境

Step 1: 供应商与福特中国网络安全团队共同审核供应商安全启动/安全升级流程，并决定合适的签名方法

Step 2: 供应商向福特中国网络安全团队申请开发环境密钥对（私钥+公钥）

Step 3: 福特中国网络安全团队向IVSS团队发送正式申请

Step 4: IVSS返回适用的开发密钥给福特中国网络安全团队

Step 5: 福特中国网络安全团队发送RSA密钥（开发公私钥对）给供应商

Step 6*: 供应商发送待签文件（发布的开发软件）给福特中国网络安全团队

Step 7*: 福特中国网络安全团队向IVSS团队发送正式申请

Step 8*: IVSS签署软件

Step 9*: IVSS返回签名后文件给福特中国网络安全团队

Step 10*: 福特中国网络安全团队将已签文件给供应商

Step 11*: 供应商将已签文件应用到开发环境，如验签失败返回到Step 6

*step 6-11仅用于测试开发软件签名流程，正常开发软件供应商可以用分发的开发私钥自行签名。

生产环境

Step 1: 供应商向福特中国网络安全团队申请生产环境证书或公钥
Step 2: 福特中国网络安全团队向IVSS团队发送正式申请
Step 3: IVSS返回适用的生产密钥给福特中国网络安全团队
Step 4: 福特中国网络安全团队发送RSA密钥(生产)给供应商
Step 5: 供应商发送待签文件（所有生产软件）给福特中国网络安全团队（Day T）
Step 6: 福特中国网络安全团队向IVSS团队发送正式申请 (Day T)
Step 7: IVSS签署软件
Step 8: IVSS返回签名后文件给福特中国网络安全团队 (Day T+3)
Step 9: 福特中国网络安全团队将已签文件给供应商 (Day T+3)
Step 10: 供应商将已签文件应用到生产环境，如验签失败返回到Step 5

4.1.3.3 数字签名密钥管理

4.1.3.3.1 生产KEY生成

生产RSA密钥应由Ford HSM（IT）生成，而私钥应安全地存储在后端基础架构（例如HSM）中。

4.1.3.3.2 开发KEY生成

开发RSA密钥应由福特HSM（IT）且公私钥都将分发给供应商。 开发密钥仅用于签署开发阶段软件（TT前）

4.1.3.3.3 生产KEY更新

在特殊情况下（例如私钥泄露），福特保留向模块发行新的RSA密钥的权利。任何PBL更新申请在提交签名之前应由网络安全团队审核。

4.1.3.3.4 模块间密钥分配

福特根据以下规则发布不同的签名密钥：
1）同一模块的不同供应商应具有不同的密钥
2）每个模块系列应具有不同的密钥
3）硬件变化较大且软件不兼容
4）在特殊情况下，例如在多个硬件部件使用相同的软件时，可以共享同一个密钥对，以降低整体软件复杂性
5）拥有单独处理器的模组作为最小送签单元

4.1.3.3.5 签名方法

所有适用的SW文件均应签名：

a）开发SW文件（TT之前的版本）应使用开发密钥签名，福特网络安全团队可能会提出替代方案来满足此要求并最大程度地减少影响开发过程。 这些方案应经由网络安全团队审核并批准。

b）生产（TT及更高版本）软件，例如应用程序的二进制文件，SBL，校准和配置文件应仅由福特使用有效的生产证书（私钥）签名。

4.1.3.3.6 私钥签署生产软件

福特安全后端（IVSS）应使用该模块的专有私钥来签署所有适用于生产的软件。

4.1.3.3.7 验证结构

软件作者（例如Tier1 / Ford SW）应为每个数据段计算哈希值，将它们包括在验证结构（VS）块中（HexView或任何可以使用的兼容VBF创建器工具都可以）。 VS将成为VBF文件的一部分，而福特IVSS将提取该文件以创建签名。软件作者应确保验证结构涵盖计划要刷到模块的二进制文件的所有数据段。VS组件的版本、长度、数据段的地址和长度均应为Big-Endian格式。

4.1.3.3.8 公钥存储

公钥应安全地存储在模块中，并应加以保护以免未经授权的修改。

主/福特引导加载程序应仅包含一个集成在PBL代码中（开发或生产）密钥。公钥不允许通过诊断或模块内部应用程序修改。任何通过应用程序写入或通过诊断重新刷写生产主引导程序均应由福特网络安全团队批准并签名。

4.1.3.3.9 代为验签

当模块具有多个微控制器/模块时，目标微控制器将是唯一的实体来验证自己的软件签名。车载网络安全团队会基于详细审核适当的补偿控制措施的基础上，考虑其他建议。

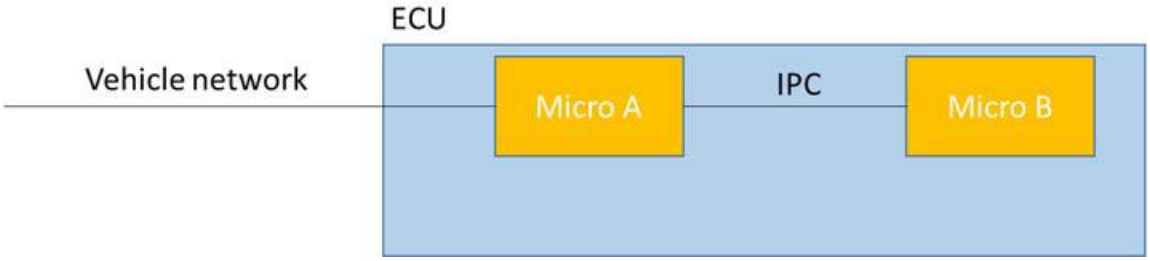
示例：满足以下所有条件时，可以允许主模块（模块A）验证辅助模块（模块B）的软件签名（模块A、B在同一/不同控制单元）。

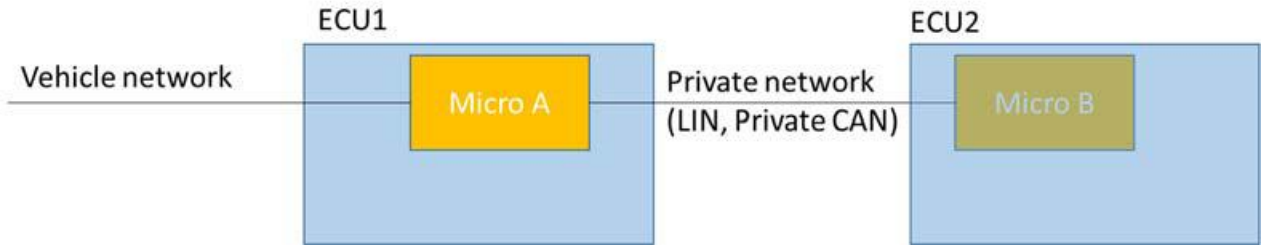
1）模块B的资源（RAM，闪存）有限，并且无法实施软件签名

2）模块B尚未实施FNOS

3）模块B没有直接的外部连接（CAN，串口，Wi-Fi，蓝牙，RF等）

4）模块A有比较完善的补偿性控制（例如通过白名单方法来管控所有传递进车载网络数据）





4.1.3.3.10 诊断模式故障分析(公钥)

模块应报告公共密钥的哈希（SHA256）并通过诊断请求提供通过DID $ D03F（使用中的应用程序签名公共密钥哈希）。 DID $ D03F应可支持引导加载程序（PBL）和应用程序。

4.1.3.3.11 签名验证失败反馈

如果签名验证失败，模块需将结果反馈给刷写工具(OTA/CAN)。模块应实施DID $ D028以支持SW签名故障分析。

4.1.3.3.12 加密标准

软件签名应使用带有RSA2048的PKCS＃1 v.2.2标准（PSS填充）生成密钥、签名和签名验证。应使用SHA256来创建验证结构和根哈希

4.1.3.3.13 待签及已签文件格式

提交给福特的待签文件应包含以下内容：

1）具有.vbu扩展名
2）在VBF标头中填充了正确的哈希值的“ public_key_hash”字段
3）VS位置的地址（填充在VBF标头的Verification_structure_address中）
    a.请注意，Verification_structure_address始终指向的最高有效字节VS版本
4）合适的验证结构
5）文件中不存在签名（VBF数据部分）
6）VBF头中不存在“ sw_signature”字段

从福特返回的已签文件应包含以下内容：

1）具有.vbu扩展名
2）在VBF标头中填充了正确的哈希值的“ public_key_hash”字段
3）VS位置的地址（填充在VBF标头的Verification_structure_address中）
    a.请注意，Verification_structure_address始终指向的最高有效字节VS版本
4）合适的验证结构
5）文件中存在的签名（数据部分）
6）VBF标头中的“ sw_signature”字段具有与数据段匹配的有效签名值

4.1.4 代码检查

操作系统应在每次应用程序执行之前，通过将应用程序和数据与已知和受信任的签名或哈希值进行比较来验证应用程序、持久性数据和共享库是否得到授权。 如果这些值不匹配或该值不能被信任，则该应用程序将不执行。 该事件应被记录并报告。

4.1.5 权限控制

4.1.5.1 强制访问控制

应用程序应基于最小化原则授予权限。 对资源（包括但不限于系统接口，数据和消息路径）的访问应受到限制和审核。 应生成包含枚举所有应用程序及其MAC列表的清单，并交由网络安全团队审查。

4.1.5.2 自主访问控制

对文件和可执行文件的访问应进行管理和审核。 基于POSIX的系统中的权限应为744、755，或以只读配置（例如，只读分区）托管。 非基于POSIX的系统必须使用等效权限文件，目录或进程的所有者确定该对象的访问控制， 这样可以保护文件和进程免受未经授权的访问和操纵。

4.1.5.3 对于安卓系统访问控制要求 - SE LINUX

SE Linux 要求使用强制模式

4.1.5.4 工程模式

原则上工程模式应该在生产件中移除，不使用的库及可调试工具和文件也应一并移除。操作系统不得留有任何后门。如因实际需要在生产环境保留工程模式，应有相应访问身份认证，并由网络安全团队审核批准。

4.1.6 CVE

系统不应存在于CVE平台发布超过6个月的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）。

4.1.7 主复位

4.1.7.1 主复位前提条件

车辆主复位事件仅在满足以下前提时才能执行：

- 引擎状态必须处于运行/附件模式。
- 点火信号必须设置为运行
- 代客模式不能激活
- 驾驶员限制为关闭状态

4.1.7.2 个人身份识别信息（PII）移除

当执行主复位事件时，应从车辆系统中清除所有PII数据。
例外：安全日志永远不应该被移除（具体参见3.5条目）

4.1.7.3 IVI配对设备数据移除

当执行主复位事件时，应从车辆系统中清除通过配对设备获得的所有客户信息（例如，手机名称，电话簿列表等）。

4.1.7.4 系统动态数据移除

当执行主复位事件时，应从车辆系统中清除所有系统动态数据（如动态车辆数据等）。

4.1.7.5 缓存数据清除

车辆主复位完成后，所有缓存数据均应被清除。

4.1.7.6 EULA(END USER LICENSE AGREEMENT)接受标识

执行主复位后，EULA接受标志应复位为默认值。

4.1.7.7 系统主复位日志

系统主复位事件应始终记录成日志。 执行主复位时，日志中应包含以下信息：

- 日期和时间
- 执行初始化的方法（即本地，远程）
- 事件结果（即成功与否）

4.1.7.8 确认提示

在执行主复位事件之前，应提示用户进行确认。

4.1.8 ROOT用户权限控制

应基于最小化原则授予权限，尽量减少应用程序使用ROOT权限。如因实际需要使用到ROOT权限的应用/进程，也应根据使用场景及最小化原则授予权限，并由网络安全团队审核批准。

4.1.9 关闭不使用的端口

对于不使用的端口，应该禁用。比如：22-ssh; 25-smtp; 53-domain; 110-pop3; 514-shell等。

4.1.10 浏览器及应用商店（禁用）

在IVI系统内，禁止浏览器、应用商店等App，以减少受攻击风险。

4.2 APP

4.2.1 代码混淆加固

未经防篡改IC或批准的加密功能保护的关键数据应通过代码混淆保护，不得以明文形式存储。关键数据是指私钥，对称密钥，私钥证书，凭据和关键代码。应与网络安全团队协调以获取批准的代码混淆方法。
批准的加密功能包括：AES，RSA，ECC，国密。
对于系统中关键的应用程序应进行加固保护，加固方法包含但不限于：加壳、代码混淆等。

4.2.2 APP签名

应用软件应采用代码签名认证机制（福特或第三方），且代码签名机制符合相关标准要求。

4.2.3 APP访问权限控制

4.2.3.1 登录

登录token应具有合适的有效期，登出后token应立即失效。登录token建议具有refresh功能、token应加密存储
如有多账户绑定功能，建议采取oauth2的方式。

4.2.3.2 系统资源调用（麦克风/GPS/通讯录等）

应采取适用于汽车各应用场景的告知和控制方式，实现当应用对系统敏感资源调用（例如：使用位置信息，麦克风）时用户可知。并提供设置开关，供用户同意或者拒绝该项调用。

4.2.3.3 应用软件权限

使用安全机制，防止和检测应用软件之间不必要的访问，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。

4.2.4 APP启动自检

关键应用程序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。应用软件运行期间，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或代码被非法执行。

4.2.5 SANDBOX沙盒（安卓系统）

系统应为App配置沙盒，将不同的应用程序彼此隔离，以使得每个应用在其单独虚拟机的隔离环境中运行，可以确保系统整体的安全。应用程序的资源访问权限应基于系统赋予的uid（每个应用程序的uid应唯一且保持不变），应用程序因实际需要共享数据和访问系统服务时，也可以通过共享uid来实现。系统将所有uid和GID资源统一为辅助工具（system/core/include/private/android_filesystem_config.H）。

4.2.6 后门及CVE

通用应用软件不应存在后门，也不应存在于CVE平台发布超过6个月的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）。
应用软件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。

4.3 数据保护

4.3.1 敏感数据识别与采集

敏感数据包括但不限于：姓名、地址、电话号码、信息娱乐个性设置、GPS、信用卡、出生日期、驾驶行为、生物识别或医疗信息、社会保障号等
车端所采集的与用户身份、位置信息等相关的敏感数据，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。
车端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。
车载端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。
车载端应具备支持国家监管部门依法进行数据采集工作的能力。
当用户输入个人敏感数据时，应采取安全措施确保个人敏感信息不被其他应用窃取，并通过安全键盘等防止录屏。

4.3.2 敏感数据存储

敏感数据不得以明文形式存储在系统中。
车端在将用户敏感数据（例如：用户身份、位置信息）存储在车内系统时，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，应采用加密形式保存。
车端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。
禁止在HMI上，通过CAN或其他连接接口向未经授权的用户透露敏感数据。

4.3.3 敏感数据传输

若出于业务需要必须对敏感数据进行传输，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。敏感数据传输应对信息进行加密，并对传输通道进行加密且有相应双向身份认证机制，以保证传输数据的保密性、完整性、可用性。
通过车载端采集的用户数据，在传送到云端服务器后，应具备相应的脱敏措施，防止用户隐私信息泄露。

4.3.4 敏感数据删除

删除关联的配对设备或系统主复位后，应立即从系统中删除相应的敏感数据。

4.4 OTA

4.4.1 OTA 升级保护

OTA升级包应以处理器为最小单位制包（如SoC和MCU应单独制包），每个单独升级包应由福特分别签名。
整个OTA升级包应由OTA服务供应商做相应加密保护，至少每个版本一个密钥。加密要求不低于AES256。推荐增加一机一授权。

4.4.2 OTA 云端

OTA升级包的签名、加密密钥及证书应存储在安全环境内（如key vault或HSM）。

4.4.3 OTA 下载身份验证及加密

IVI与Server之间需要做双向认证，并一机一密。触发升级请求及下载升级包时应验证车机身份。下载OTA升级包应对信息层做相应加密。

4.4.4 OTA 升级包检查

软件更新时，应能够对提供更新软件包的来源进行鉴别，并对接收到的更新文件进行完整性校验，并做签名验证。同时应对更新软件包版本加以校验，系统不应支持刷回比当前版本更低的软件版本。

4.4.5 升级失败补救方案

4.4.5.1 重试

系统应提供失败重试机制，并对连续升级行为进行记录，设定一段时间内升级尝试次数上限，避免通过车载端升级尝试对车辆资源进行过度消耗。

4.4.5.2 回滚

系统应具有备份和恢复能力（如A、B区），能够在软件更新发生异常时进行必要的操作，避免更新失败导致系统失效。

4.4.6 本地升级(USB/CAN)

本地USB升级包至少每个版本一个密钥，推荐一机一密授权和使用工程U盘
诊断（CAN）升级应遵循FNOS VECTOR升级要求（0x27服务）

4.4.7 升级条件及安全保护

系统OTA升级检测可以在系统开机5分钟后自动进行，并提供用户手动检测升级选项。下载及安装升级包应支持静默升级，并在此过程中不得影响系统正常功能运行。安装完成后切换至新系统（重启操作）必须在熄火状态或用户预设的时间段执行。

推荐在升级过程中考虑以下要求：
只接收在约定的工况（例如：非行驶状态）和车辆系统状态（例如：电瓶电量满足要求）下发起的车载端操作系统和应用等软件的更新请求，并在用户确认后执行更新操作。
车辆升级前需对车辆当前状态进行检测，确保整个升级过程中车辆处于驻车状态且电池电量能够保障整个升级过程及下一次启动使用。同时，升级包安装前需要考虑升级时间、车辆位置是否适合进行升级操作，尽量避免车辆在用车高峰、十字路口、限停区域、高速公路等位置进行升级包安装操作，避免误操作引发交通问题。

4.5 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。安全日志车机端应至少保留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，确保数据的保密性、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，对日志的访问权限应基于最小化原则授予。只能通过批准和授权的方法提取日志，至少应保留2MB的循环安全日志。
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
- 尝试软件安装
- 尝试启动沟通渠道
- 尝试启动诊断会话
- 尝试访问敏感或关键数据
- 权限升级尝试
- 应用执行尝试
- 系统重置
- 尝试直接访问内存
- 定义之外的事件

批准的日志提取方法包括：由福特批准的实体（例如Hancock）签发的签名实用程序

5. IVI communication

对于所有通讯协议（包括但不限于CAN, LIN, Ethernet, WiFi, 蓝牙等）均应使用福特认可的工具进行模糊测试。

5.1 车内通讯

5.1.1 CAN

建议IVI与CAN通讯应实施身份认证机制，以确保通讯安全。
车载端具备冗余备份和重发机制，保证对电子电气系统发送重要数据时（例如：ECU固件升级包），传输数据的可靠性。
车载端向车内电子电气系统发送数据和转发数据时，应采用相应技术避免大量集中发送数据包导致的总线拥塞和拒绝服务。
车载端应建立监测模块，实时监测向车内电子电气系统发送数据的数量与质量，对于异常情况应及时发现并告警。

5.1.2 ETHENET

Ethenet通讯应满足使用TLS1.2以上，并实现双向认证。

5.1.3 MCU白名单（CAN/LIN）

MCU应包含一个信号白名单，该白名单枚举系统可以读取或写入车辆网络的信号。MCU应禁止未在信号白名单中的信号读取或写入系统网络。
安全启动验证应包括包含信号白名单内存模块的验证。
包括在MCU信号白名单中的所有信号清单均应由福特网络安全团队审核和批准。 在每次发布之前，都应对清单进行审核。
MCU应包含一个独立于系统应用的微处理器，以处理与系统之间传输的消息。

5.1.4 SOC与MCU之间通讯(推荐)

如MCU有对外部远控及查询指令有独立处理能力的情况下，建议SOC与MCU之间通讯应加密，并有相应身份认证机制。

5.2 车外通讯

5.2.1 蓝牙

车机应只允许用户发起的显式配对请求连接，禁止连接任何未事先配对的设备。配对方式：经典蓝牙应为SSP模式，低功耗蓝牙应为低功耗安全连接模式（LE Secure Connection）。配对过程是唯一可能受到攻击的时期。当外部设备未连接时，车机不可以暴露任何敏感信息。

5.2.1.1 蓝牙安全模式

允许蓝牙连接的设备应使用可用的最强安全模式。 应该使用最新的蓝牙版本，但是如果不可用，则以下列表定义了每个适用版本应使用的安全模式：

•支持BR（Basic Rate），EDR(Enhanced Data Rate)和高速（HS）的Bluetooth 1.4设备应使用安全模式4，级别4
•蓝牙2.1至5.0设备应使用安全模式4，级别3
•蓝牙2.0和较旧的设备应使用安全模式3
•绝不能使用安全模式1
•对于低功耗蓝牙，设备在可用时应使用安全模式1级别4，蓝牙4.0和4.1设备应使用安全模式1，级别3

5.2.1.2 蓝牙配置设置

蓝牙设备不得使用默认配置设置，包括默认PIN码。 每个设备应配置为使用随机生成的PIN码，并且PIN在每个模块中均应唯一。

5.2.1.3 安全模式4兼容性

连接到不支持安全模式4的设备时，处于安全模式4的蓝牙设备可以回退到较低的安全模式。即使在安全模式4不可用的情况下，设备也不得使用安全模式1。 如果为了兼容，处于安全模式4的蓝牙设备必须回落到较低级别，则应使用安全模式3

5.2.1.4 链路密钥(LINK KEYS)

链路密钥(Link keys)不应被重复使用，也不应基于单元密钥(unit keys)，相反，配对应使用基于每个设备配对时生成的组合密钥。

5.2.1.5 设备应设置未不可发现

蓝牙设备应默认配置为不可发现，并且在非配对状态时仍不可发现。

5.2.1.6 链路加密

链路加密应用于确保通过蓝牙的所有数据传输的安全。 加密密钥的大小应配置为最大允许值。

5.2.1.7 相互认证

除非无法使用PIN配对，否则所有设备连接都必须进行相互身份验证。 在PIN配对不可用的情况下可能会出现例外，例如BLE。

5.2.1.8 不使用时禁用广播

不使用时，除BLE应用外，所有蓝牙功能均应禁用。

5.2.1.9 模糊测试

所有蓝牙设备均应使用福特认可的工具进行模糊测试。

5.2.1.10 蓝牙MAC地址

蓝牙MAC地址不得与相应的WLAN MAC地址相同或在其一位数之内。

5.2.2 车机热点及WIFI连接

5.2.2.1 车机热点要求

5.2.2.1.1 加密

热点应配置为仅接受使用WPA2或更高安全协议的连接。 不允许使用WPS或WPA协议甚至无安全协议配置热点。

5.2.2.1.2 预共享密钥

默认的预共享密钥应由所使用的安全协议指定的最小长度的随机字母和数字生成，且不可预测，不同车机应不一样。（密码应不低于8位，至少包含阿拉伯数字、大小写拉丁字母。如用户设置密码不符合复杂度要求，应向用户提示风险）

5.2.2.1.3 SSID

对于AP模式，共享的SSID必须包括唯一的命名约定，格式为“ HotspotXXXX”，其中“ XXXX”是TCU ESN的后四位。

5.2.2.2 车机连接WIFI要求

5.2.2.2.1 热点认证

在WiFi模式下，车机只能连接到车主认可或福特预设的网络。 在主重置期间，应删除所有者认可的热点列表。

5.2.2.2.2 不安全的网络

车机在尝试连接到任何不受WPA2 +保护的WiFi网络之前, 应提示用户进行确认。

5.2.3 蜂窝网络

车载端应使用安全机制，识别伪基站，确保接入真实可靠的蜂窝网络。
车载端与核心业务平台的通信应采用专用网络或者虚拟专用网络通信，与公网隔离。
车载端应能够识别来自蜂窝网络的非法连接请求，过滤恶意数据包。
车载端应采取技术措施，禁用业务所不需要的蜂窝网络通信功能。

通过蜂窝网络传送的针对车载端的关键操作（例如：用户号码写入），应采用强验证手段，确保只有授权的主体可以实施相应的操作。
应根据不同应用的重要性划分优先级，保障关键业务（例如：监管平台信息采集）具有网络通信的优先使用权。

5.2.4 车到云端通讯

5.2.4.1 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。

5.2.4.2 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。

5.2.4.3 信息层加密

发送至车辆和从车辆发送的指令和控制消息应使用福特专有的SyncP标准进行签名和加密。

5.2.4.4 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证书的有效期最长为30年（后端的单个证书的有效期应较短，例如1年）。

5.2.4.5 TLS压缩

不得使用TLS级压缩。

5.2.4.6 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。

5.2.4.7 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。

5.2.4.8 主机认证

连接到外部系统的模块应验证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。

5.2.4.9 验证对等方

协商TLS连接时，连接到外部系统的任何模块均应使用“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，则模块应拒绝连接。

5.3 密钥证书管理

5.3.1 密钥证书类别及生成

车内密钥及证书的类别、生成推荐满足下表要求：

密钥证书用途	应用场景	密钥/证书类型	密钥生成
验签	升级	SoC 公钥	福特提供并预埋
		MCU 公钥	福特提供并预埋
	安全启动	SoC 公钥	福特提供并预埋
		MCU 对称密钥	福特/供应商提供并预埋，一机一密
车端到云端通讯	TLS 证书	SoC 私钥证书	福特/供应商提供并预埋
		云端公钥证书	福特/供应商提供
车内通讯	SoC/MCU 认证	公私钥证书	福特/供应商提供并预埋
	Ethernet	ECG 公钥、IVI 公私钥	福特提供并预埋

5.3.2 密钥证书存储

5.3.2.1 密钥存储

作为基本要求，设备上存储的所有私钥都应存储在HSM或其他安全存储中。除非另有说明，否则福特汽车公司应独自拥有并管控与系统结合使用的所有密钥。

涉及存储在安全密钥存储中的密钥的操作（加密，解密，签名验证等）应完全包含在静止的安全密钥存储中，并且在实际操作中应在使用期间通过诸如ARM Trust Zone之类的机制进行保护。如果加密功能托管在安全密钥存储之外，则设备应不允许密钥/证书在RAM中保留超过100ms。

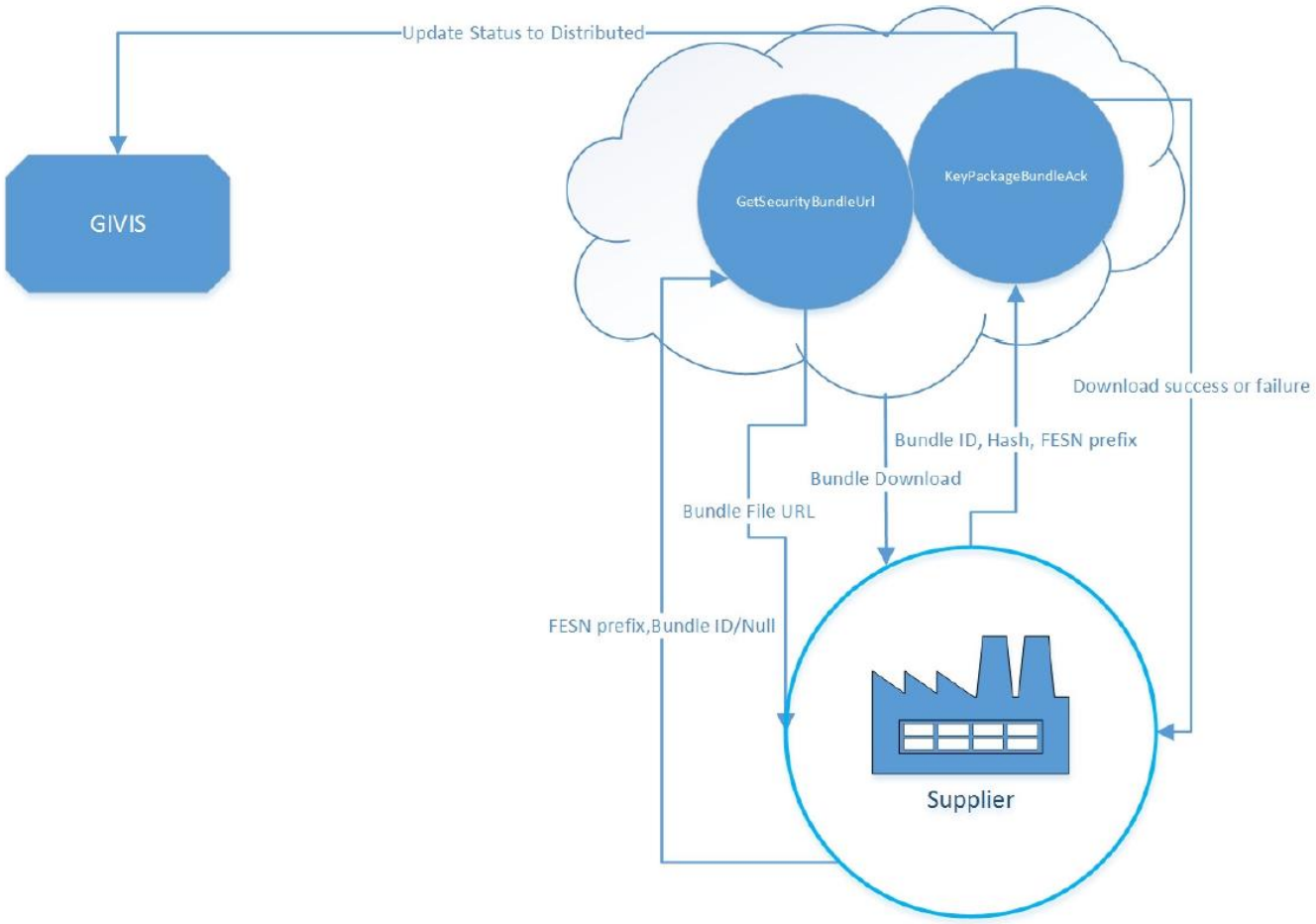
5.3.2.2 证书存储

用于TLS和车内通信及软件安装的证书应存储在设备上。 代码签名公钥/证书应存储在主引导程序中，并且仅通过经过验证的镜像进行编程。 用于TLS连接的证书应存储在只读存储位置。
除非另有说明，所有使用的证书均应来自福特根CA。

5.3.3 KEY INJECTION AND SUPPLIER FEED

5.3.3.1 安全软件包发放(一机一密)流程

安全软件包的一般流程如下：



- 福特根据模块需求创建安全对象并打包：
  - 福特生成FESN(大部分情况下)
  - 每单个的FESN模块会打包相对应的所有安全对象
  - 安全软件包含XML清单文件、安全对象及其他用于加解密的数据
  - 每个安全软件包应包含唯一的安全软件包ID（SPID）

福特会通过以下部署在Azure云上的网络服务将安全软件包发送给供应商，该网络服务应使用TLS双向认证。

- 供应商应使用*GetSecurityBundleUrl*网络服务下载下一版的安全软件包，该网络服务请求参数如下：

Request	**GetSecurityBundleUrl**
URL	https://usivssspd.cv.ford.com/GetSecurityBundleUrl/FESN_prefix/[BundleID]
Method	Get
URL Parameters	Required (string) FESN prefix Optional (string) Bundle ID
XML Return Response	Bundle download URL
Success Return Codes	*HTTP* 200 *Application* 000
Error Return Codes	*HTTP* Any code other than 200 *Application* Any code other than 000

  - 如果仅使用FESN前缀调用该网络服务，将会返回下一版安全软件包的URL；
  - 如果使用FESN前缀、包ID参数调用该网络服务，将会返回对应版本安全软件包的URL（该请求仅在包发布7天内可用，超过7天的重新下载请求需走特别流程）；
- 供应商将下载的安全软件包生成SHA-256哈希值、包ID及FESN前缀等参数，通过*KeyPackageBundleAck*网络服务发送给福特验证，下载结果（成功/失败）将会返回给供应商。成功验证后，福特会将密钥包的状态设置为“已发送“。

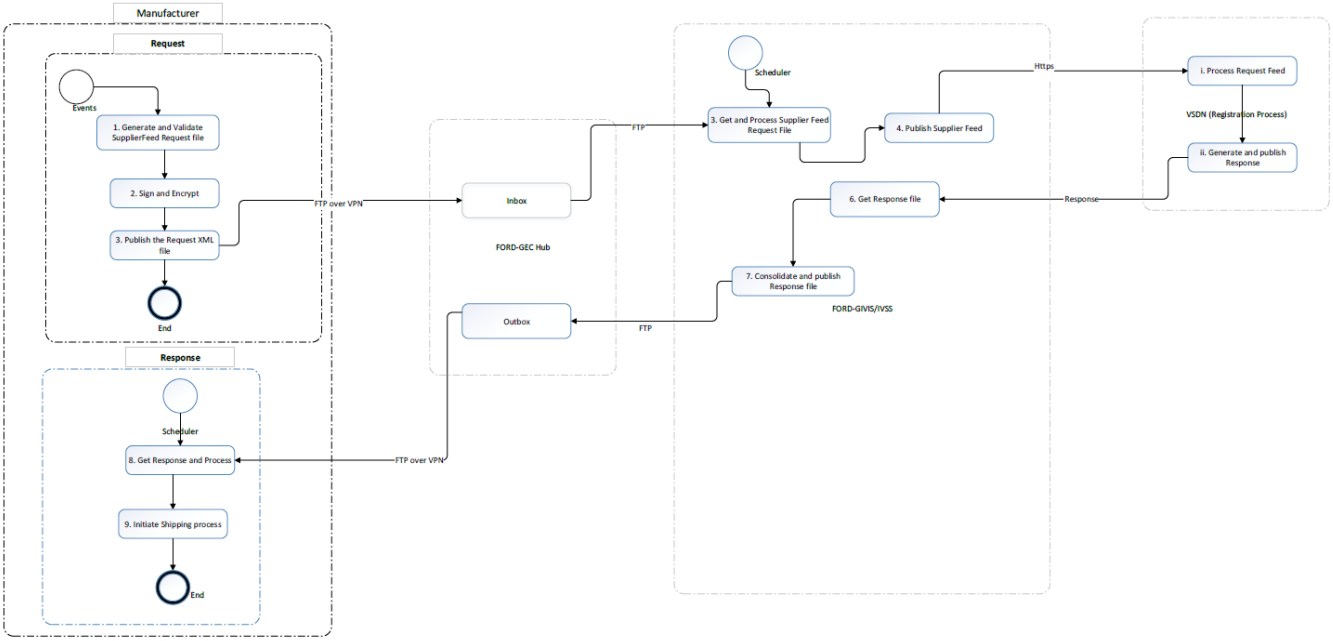
Request	**KeyPackageBundleAck**
URL	https://usivssspd.cv.ford.com/KeyPackageBundleAck/BundleID/BundleFileHash/FESN_prefix
Method	Get
URL Parameters	Required (string) Bundle ID (string) Bundle file SHA-256 hash, hex encoded uppercase with no separator (string) FESN prefix
XML Return Response	Success or Failure
Success Return Codes	*HTTP* 200 *Application* 000
Error Return Codes	*HTTP* Any code other than 200 *Application* Any code other than 000

供应商有责任确保以下事项：

- 密钥包中包含的数据必须视为秘密数据
- 未使用的密钥包必须加密存储在安全的网络中且有严格的权限控制
- 未加密的安全对象绝不能传输到工厂网络。
- 必须安全地将安全软件包转移到工厂现场进行配置。
- 安全软件包解密必须安全进行，以最大程度地缩短解密安全对象暴露的时间。
- 安全软件包必须在一个且仅此一个模块上配置。

- 供应商必须验证包中的每个安全对象均已被正确配置在模块上
- 供应商必须验证FESN和SPID及DID是否正确编写
- 安全软件包成功预埋并验证后，必须立即清除
- 供应商必须跟踪密钥包的使用情况。对于每个模块，供应商必须能够确定密钥包状态：
    - 已配置（密钥预埋，模块已发货）
    - 未使用（密钥由于某些原因未预埋成功–损坏，丢失等）
    - 报废（密钥预埋，但模块在出厂前已报废）
- 用于存储密钥包的设备必须能够确保数据删除后无法恢复

5.3.3.2 SUPPLIER FEED流程：



签名证书：

- 供应商应使用供应商的公私钥证书对文件内容签名
- 上述证书对的公钥证书将通过安全的加密电子邮件或此过程之外的其他通信传递给福特SDN

加密证书：

- 应使用福特公钥证书来解密供应商提供的文件内容
- 福特将私钥证书保存在其信任库中，并且应通过安全的加密电子邮件或此过程之外的其他通信将公钥证书交付给供应商

5.3.4 密钥/证书更新撤销

密钥应定期更新，并且在泄露后有及时的密钥/证书撤销更新机制。