AF VFL 客户端训练 API 的安全分析

本报告的其他语言版本：English。

19.2.0 · ProVerif+ Agent 报告

文稿	5G System; Application Function Artificial Intelligence/Machine Learning (AI/ML) Services; Stage 3 （协议定义）
检查的性质	12 条：7 条成立，5 条不成立（12 个攻击）
发现	1

目录

1 协议和范围
2 发现
3 检查过的性质
4 本次分析的局限
附录 A：逐条性质的解读
附录 C：主张和证明器的答案
附录 D：分析是怎么跑的

1 协议和范围

Naf_VFLTraining 服务是可信 Application Function 作为 VFL 客户端对外暴露的接口，NWDAF 作为 NF 服务消费者可以通过它订阅 VFL 训练报告。AF 持有订阅并发出训练通知；NWDAF 创建、更新和删除自己的订阅，并在其指定的 URI 上接收通知。二者是同一运营商的 NF，都从 NRF 获取服务范围 naf-vfl-train 的访问令牌。

该交互包括：创建订阅（指定通知 URI 和关联标识），更新订阅以激活上报，AF 发出一次通知，消费者确认该通知，最后删除订阅。交互结束后，AF 确信其接受的请求来自它已验证过凭据和令牌的 NF，NWDAF 确信 201 响应和通知来自 AF 且对应它创建的订阅。但本 API 中没有任何机制能让 AF 确信，操作某个订阅的 NF 就是创建该订阅的 NF。

参与方：

- **NWDAF**：可信场景下的 NF 服务消费者。持有：NF 实例身份、TLS 凭据、OAuth2 客户端凭据。
- **AF**：可信 VFL 客户端、服务生产者。持有：它所持有的订阅、用于验证令牌的 NRF 密钥。
- **NRF**：授权服务器。持有：NRF 签名密钥。

图 1 展示了文稿规定的交互流程。

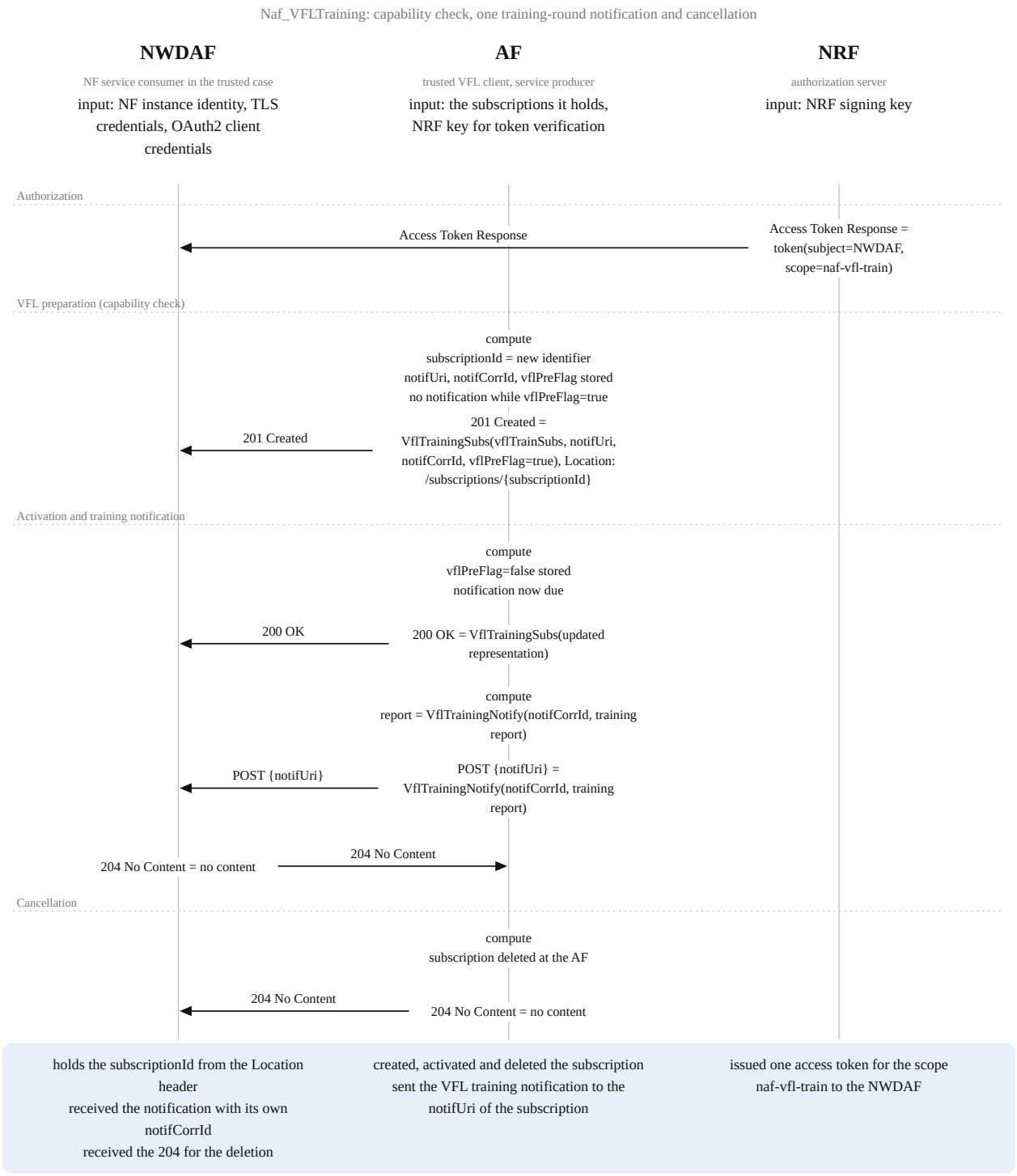


图 1. 文稿规定的协议。

分析范围见附录 D：分析了什么、省略了什么，以及依据文稿的哪些章节。

2 发现

本次分析有 1 个发现：以下内容文稿中没有写明。其中 1 项是否在文稿中写明尚不明确。

该 API 仅对只控制网络的攻击者提供其设计目标的保证：认证、参数一致性、令牌有效性和准备标志在该场景下均成立。但对另一个已授权 NF 则不成立：一个合法 NF 可以接管另一个消费者的订阅、接收其 VFL 训练通知并将其删除。这就是唯一的发现；作为一条陈述它是新的，尽管文稿已经写明了两个要素：单一

服务范围，以及资源服务器上不存在令牌到客户端的绑定。这些结果基于一个模型，该模型将 TLS 简化为按端点加密、不保留会话状态，固定两个 NF 身份，并假设 subscriptionId 可知；删除性质是在展开四步的模型上求解的。Tamarin+ Agent 按 TLS 记录和状态的本来面貌建模，可以解决 ProVerif 模型留作 artifact 的重放问题，并能在四步之外确认删除行为。

攻击图沿用图 1 的列。红色表示攻击者的行为。黄色标记某方发送了消息，但规定的交互在该位置并没有这条消息，以及攻击所破坏的结果。

2.1 一个已授权 NF 可以接管另一个消费者的 VFL 训练订阅

类型	协议规范本身的弱点
是否新发现	不确定：文稿只写了一部分，或没能检索
价值	高
涉及的性质	A08, Z03, Z04, U02, U03 （见第 3 节）
原文	s0045, s0061, s0074, s0144, s0276
依据	ProVerif attack queries `z03_update`, `z03_delete`, `z03_notif`, `a08_origin`, `a08_owner`; Figures 2, 3, 4, 5 and 6

发生了什么。 一个合法 NF 从 NRF 获取自己的访问令牌，服务范围为单一范围 naf-vfl-train。它通过资源 URI 定位另一个消费者的个体订阅，并发送 PUT 或 PATCH。AF 验证令牌、范围和 subscriptionId，但从不将令牌主体与创建该订阅的 NF 进行比较，因此接受该更新，并替换已存储的 notifUri、notifCorrId 和准备标志。该订阅的下一条 VFL 训练通知就被投递到攻击者的 URI，并用攻击者自己的 TLS 密钥解密；同一处缺失的检查还让攻击者可以删除订阅并抑制其上报。

攻击者能得到什么。 攻击者代替消费者接收该消费者订阅的 VFL 训练通知，可以通过将准备标志改回原值来抑制上报，还可以通过删除订阅彻底终止上报。双方都不会察觉：消费者只是不再收到通知，而 AF 接受的请求确实由其令牌和范围授权。

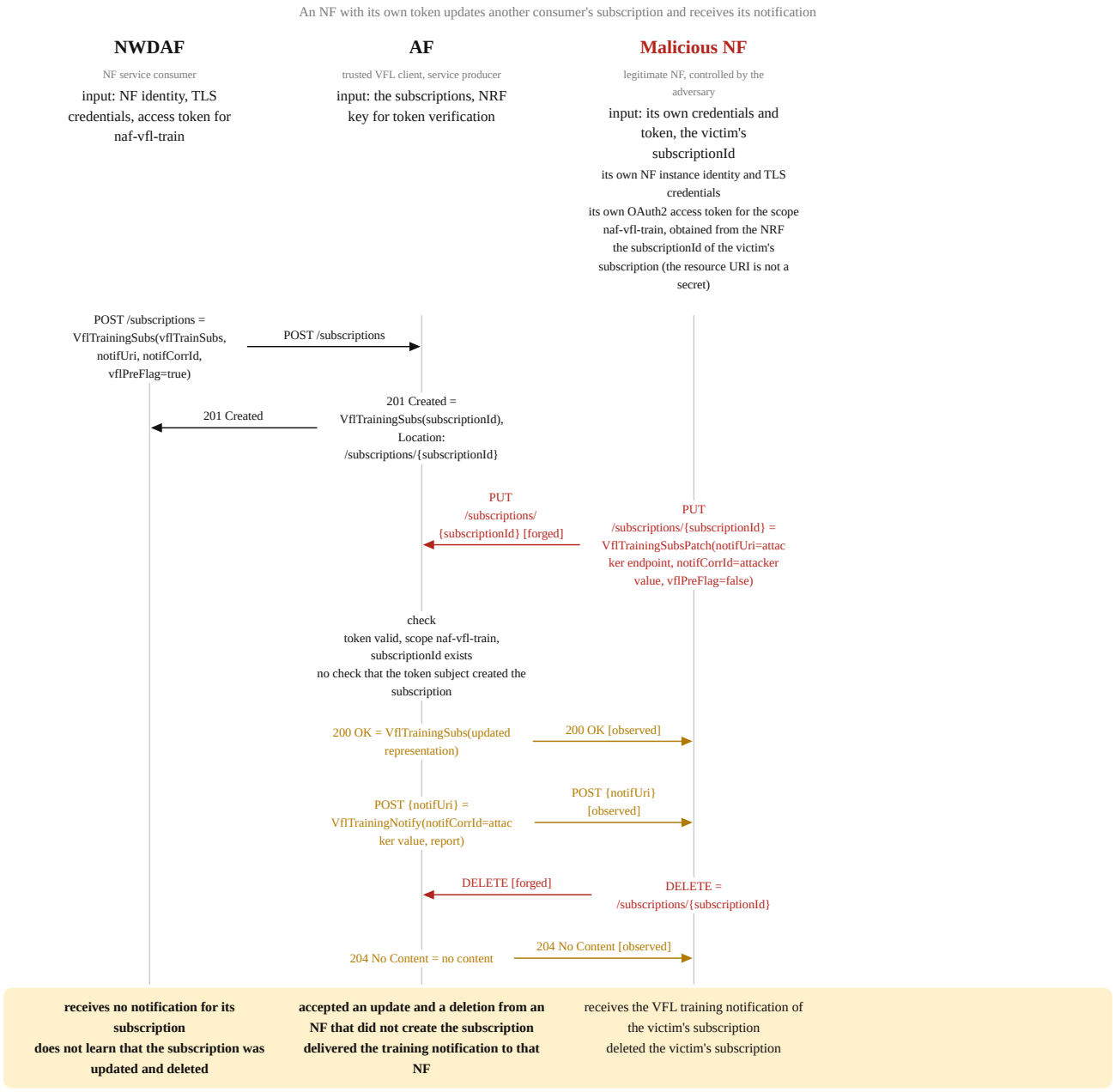


图 2. 一个持有自己令牌的 NF 更新另一个消费者的订阅并接收其通知。性质 U03；攻击查询 z03_delete, z03_notif, z03_update。

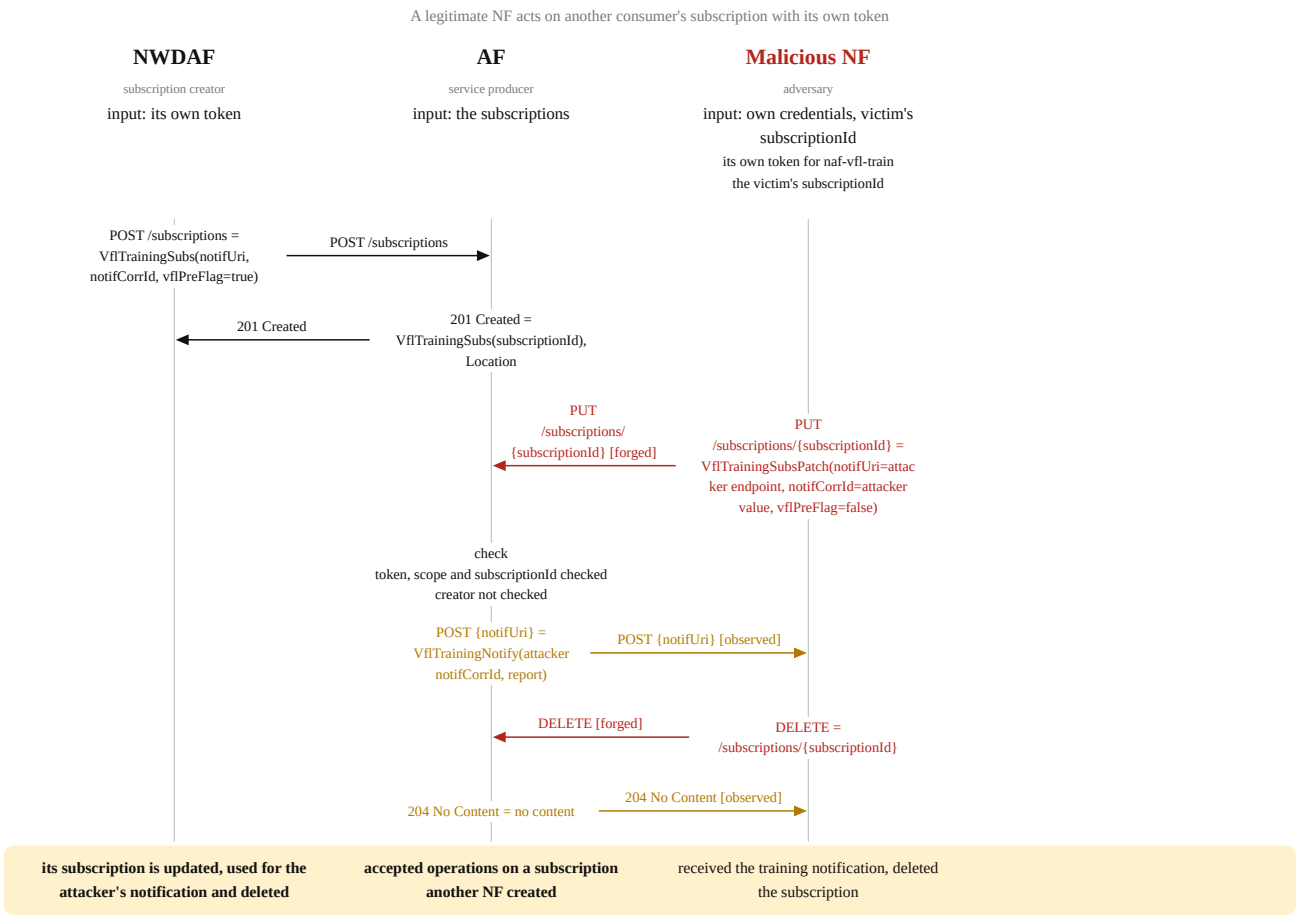


图 3. 一个合法 NF 用自己的令牌操作另一个消费者的订阅。性质 Z03；攻击查询 z03_delete, z03_notif, z03_update。

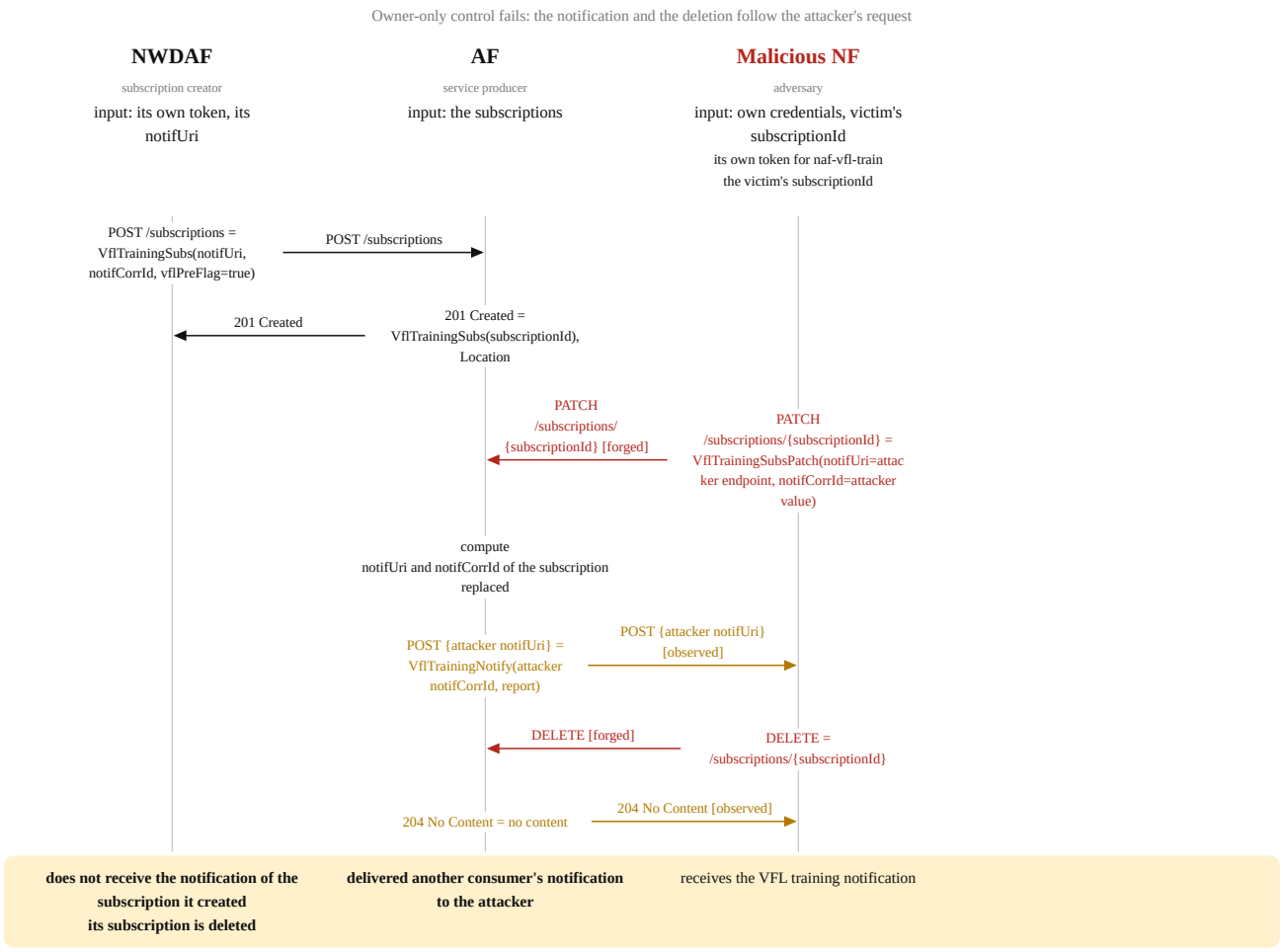


图 4. 仅所有者可控制失败：通知和删除都跟随攻击者的请求。性质 U02；攻击查询 z03_delete, z03_notif, z03_update。

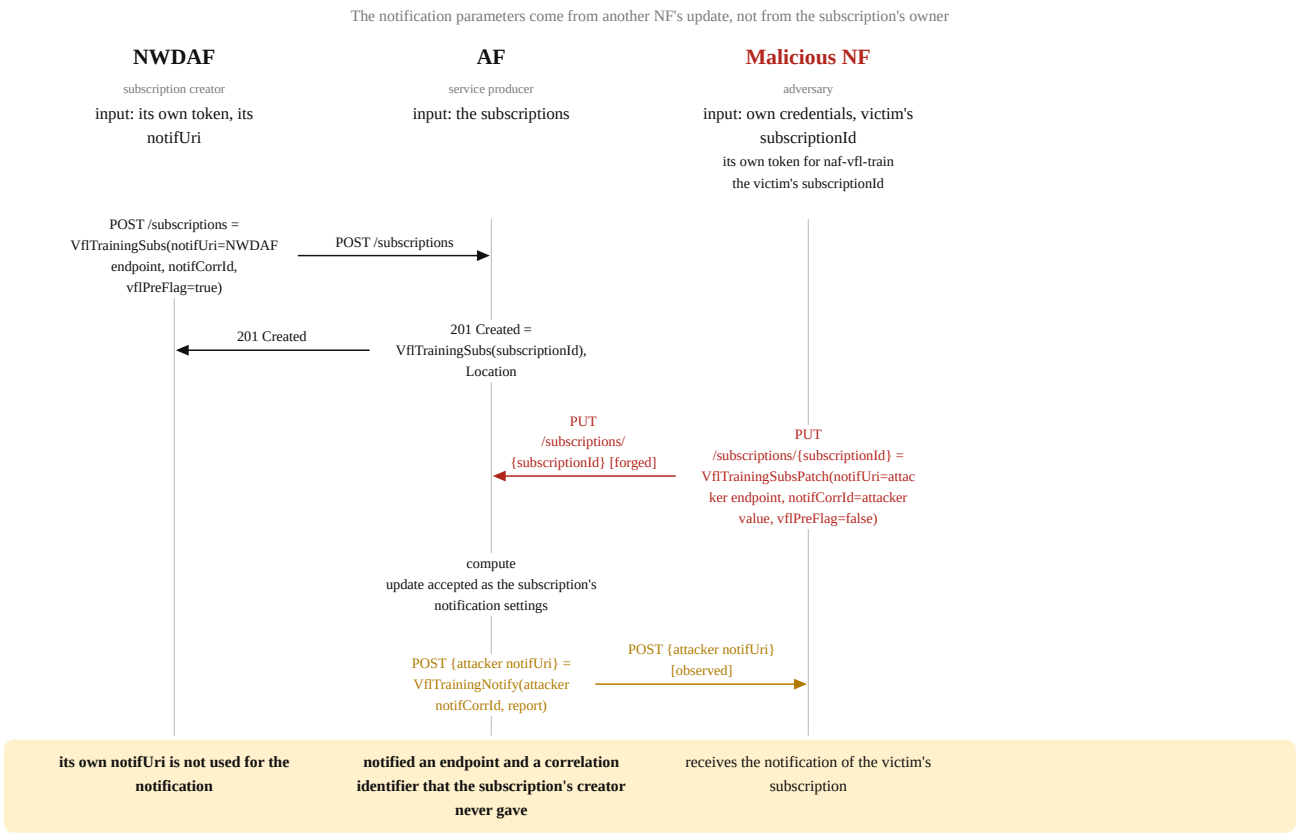


图 5. 通知参数来自另一个 NF 的更新，而不是来自订阅的所有者。性质 A08；攻击查询 a08_origin, a08_owner。

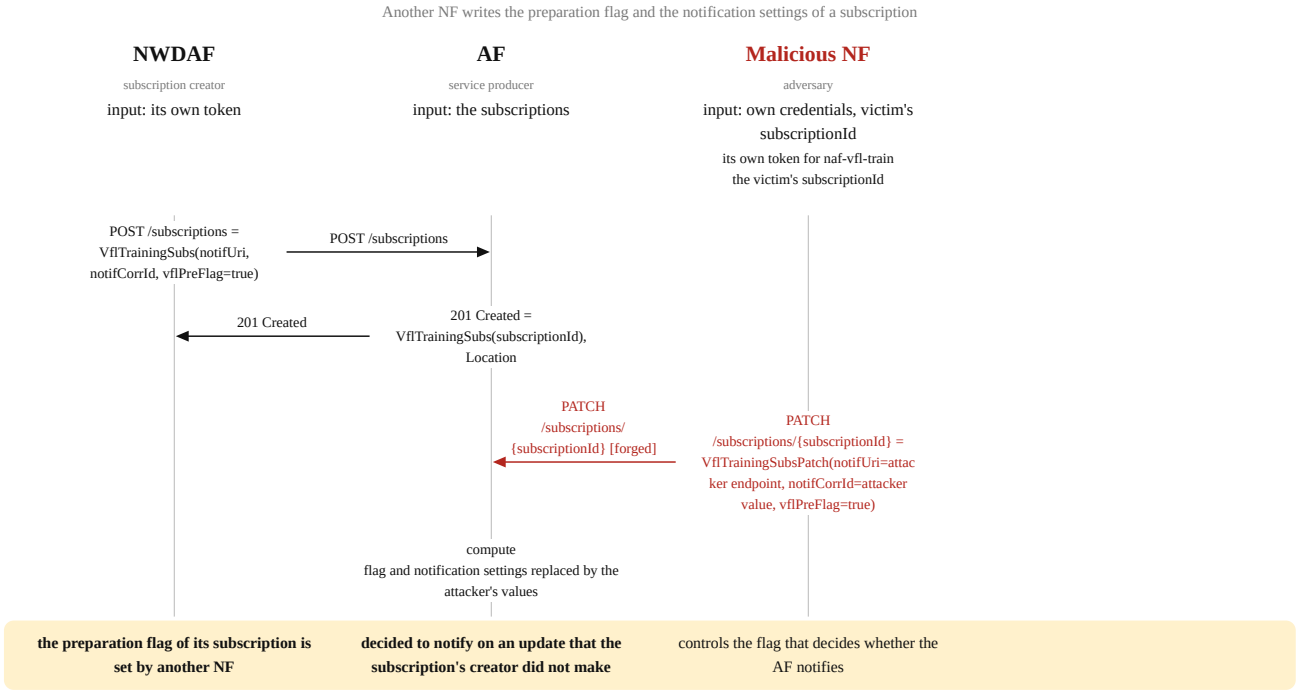


图 6. 另一个 NF 写入某订阅的准备标志和通知设置。性质 Z04；攻击查询 a08_origin。

拟议修改。 让 AF 记录创建每个订阅的 NF 实例身份，当访问令牌的主体不是该身份时拒绝 PUT、PATCH 和 DELETE；只有 notifUri 是同一身份的端点时才接受。静态层面，在资源级定义授权，而不是对整个服务使用一个范围，使 NRF 签发的令牌指明消费者可以操作哪个订阅。

用 ProVerif 复核。 未检查：该修改的模型需要 AF 保存每个订阅的创建者身份并与令牌主体比较，还需要 API 在令牌中携带该身份；这改变了协议的检查和授权，我没有在本次会话中作为变体构建。

本发现下这些攻击没有配图： A08: z03_delete, A08: z03_notif, A08: z03_update, U02: a08_origin, U02: a08_owner, U03: a08_origin, U03: a08_owner, Z03: a08_origin, Z03: a08_owner, Z04: a08_owner, Z04: z03_delete, Z04: z03_notif, Z04: z03_update。

3 检查过的性质

每一行是一条提交给 ProVerif 的性质。结果是 ProVerif 对分析者所建协议模型的答案；价值和文稿是否已写明该结果属于分析者的判断，理由见附录 A。

ID	性质	假定的泄露	结果	价值	文稿是否已写
A02	**VFL 请求对端认证。** 每当 AF 接受一个订阅/更新/删除请求，或消费者接受一条通知时，都存在一个以本方身份为对象的真实对端运行。	无	成立	中	是
A03	**订阅参数的一致性。** 每次 AF 接受订阅创建/更新，或消费者接受通知时，都存在一个匹配的对端运行，双方对订阅标识、notifUri、notifCorrId、vflTrainSubs 与 vflPreFlag 的取值一致。	无	成立	低	是
A04	**请求与通知的新鲜性。** 每次 AF 成功创建订阅或消费者成功接受通知，都对应一个此前未使用过的对端运行；同一请求不能被重复接受为新的订阅或新的通知。	无	成立	低	是
A08	**通知绑定到已批准的订阅。** AF 接受的通知投递参数（notifUri、notifCorrId、vflTrainSubs、vflPreFlag）必须来自该消费者此前获批的订阅，且准备阶段标志为 true 时不得发出通知。	无	不成立（2 个攻击）	高	不确定
Z01	**每个操作的令牌与范围。** 每次订阅创建/更新/删除或通知投递被接受，都必须有来自授权服务器（NRF）的有效 token，且 token 的 scope 覆盖 naf-vfl-train 服务。	无	成立	中	是
Z03	**按订阅授权。** 用于订阅更新/删除或通知投递的授权，必须绑定到该消费者自己的订阅资源与对应操作，不能被用于其他消费者的订阅。	无	不成立（3 个攻击）	高	不确定
Z04	**删除后无通知。** 订阅被删除（或 vflPreFlag 由 true 更新为 false 之前）之后，AF 不得再依据该旧订阅向消费者投递通知。	无	不成立（1 个攻击）	中	不确定
S05	**已删除订阅不产生通知。** 订阅删除生效之后，使用该订阅的旧 notifUri、notifCorrId 或 subscriptionId 不能触发新的通知投递。	无	在界内成立（变化值展开到 4 步）	低	不确定
U01	**AF 身份与关联绑定。** AF 接受订阅或消费者接受通知时，AF 身份、subscriptionId、notifCorrId 与训练轮次标识必须与匹配的对端运行一致。	无	成立	低	是
U02	**仅所有者可控制订阅。** 对某 subscriptionId 的更新/删除只能由该订阅的创建者发起；通知只能投递给该订阅者提供的 notifUri 且 notifCorrId 一致。	无	不成立（3 个攻击）	高	不确定
U03	**恶意 NF 被限制在自身订阅内。** 持有自身合法凭据的恶意 NF 不能使 AF 接受跨训练轮次的订阅内容替换，也不能对其他消费者的订阅执行更新或删除。	无	不成立（3 个攻击）	高	不确定
X01	**OAuth2 令牌传输机密性。** 网络攻击者永远无法获知 NF 消费者从 NRF 为 naf-vfl-train 范围获取的访问令牌。	无	成立	低	是

文稿写明、但起草清单中没有、由分析者补充的目标（见附录 D）：X01。

所提的问题及分析者的回答：

问题	回答	依据
Q1: AF/client 身份与 VFL correlation/round 绑定	AF 与消费者确实绑定了 subscriptionId 和 notifCorrId：消费者只接受来自 AF 的 201 或通知，且只针对自己创建的订阅和 correlation 标识，ProVerif 针对网络攻击者证明了这一点。训练轮次在此 API 中没有对应字段：轮次号承载于 TS 29.520 的 VflTrainingNotify 数据中，因此模型只通过订阅的通知内容来绑定轮次；持有凭据的一方进行的替换无法被阻止，这就是针对 U03 报告的攻击。	U01, A03, U03
Q2: 训练订阅控制者和通知接收者绑定	否。AF 会验证 token 和 subscriptionId，但 API 未定义按资源的授权，AF 也从不将 token 主体与创建订阅的 NF 进行比较，因此第二个合法 NF 可以更新或删除该订阅，并能使 AF 将通知投递到其自己的 notifUri，而非订阅者给出的 notifUri。	U02, Z03, Z04
Q3: 恶意合法 NF 的跨轮次替换与跨订阅操作	是，两者都可以。凭借其自身对单一服务范围的有效 token，它可以替换另一个消费者订阅的 notifUri、notifCorrId 和准备标志，接收该订阅者的 VFL 训练通知，并可以删除该订阅；替换某一轮次的内容就是对同一条记录的同一操作，因此下一次通知的轮次会跟随攻击者的更新。	U03, U02, Z03, A08

4 本次分析的局限

这里的结果是关于协议模型的结果：它说明的是所规定的消息和检查给出了什么或未能给出什么，密码学被视为理想的，与实现无关。

正如分析者所述，本分析不覆盖以下内容：

- TLS 被建模为发送方长期密钥下的 MAC 加上接收方长期密钥下的加密；握手、会话密钥和记录序列号未建模，因此录制记录的 replay 留给抽象处理。
- 模型有两个 NF 身份（一个诚实消费者、一个恶意 NF）和一个 AF 身份；对任意数量 NF 成立的内容是从这两个身份论证而来，而非证明。
- subscriptionId 被建模为消费者身份的函数，因此被视为攻击者可获知的；subscriptionId 为不可猜测标识符的部署不在覆盖范围内，同一消费者的并发会话也不在覆盖范围内。
- OAuth2 在源文中是可选的（对 API 的访问可以被授权）；模型始终让 AF 验证 token，因此回答针对的是使用 OAuth2 的配置。
- AF 的记录一次只建模一个订阅：model.pv 不检查其状态，bounded.pv 将其展开为四步（创建、更新和通知、删除、一次重复更新）。
- 错误处理（403 OVERLOAD、NOT_AVAILABLE_FOR_VFL_PROCESS、VFL_REQS_NOT_MET）、经由 SCP 的 HTTP 重定向、NEF 与不可信 AF 分支，以及 VflTrainingSub 和 VflTrainingNotify 的内容（定义于 TS 29.520）均在被分析的流程之外。
- 密码学强度、NRF 签名密钥的保密性和可用性未分析。

宿主记录的内容：

- Z04、S05 的回答依赖于模型所做的一项简化（附录 D）。
- 没带对照查询的证明（附录 C）：Z01: z01_create, Z01: z01_update, Z01: z01_delete, Z03: z03_imp, U03: z03_imp。对照查询是这条性质的一个必然不成立的变体；没有它，就没有东西表明这条性质照现在的写法在模型里有可能不成立。

每条性质还有哪些未决之处，以及什么能解决它，见附录 A。

附录 A：逐条性质的解读

这是分析者自己对证明器回答的解读，而非证明器的回答：这些回答对协议意味着什么，解读依据什么，能否按原样使用，以及它的价值如何。

A02: VFL 请求对端认证

每当 AF 接受一个订阅/更新/删除请求，或消费者接受一条通知时，都存在一个以本方身份为对象的真实对端运行。

AF 仅在请求确实来自其所指名的 NF 时才接受订阅创建、更新或删除，消费者仅在 201 或通知确实由 AF 发送时才接受。该保证正是 TLS 和 OAuth2 客户端凭据旨在提供的，且对任意数量的会话都成立。

- 结果：成立；回答了所问：是；可在有保留的情况下使用
- 价值 中：这是流程的核心认证保证，已通过机械化方式证明，但没有简化触及它，且文稿要求它，因此这是确认而非新发现。
- 文稿中已陈述：是。文稿中陈述之处：s0038, s0045, s0061, s0074, s0098, s0273
- 依据：TLS 被建模为发送方长期密钥下的 MAC 加上接收方长期密钥下的加密，不含握手或会话状态。；仅建模了两个 NF 身份；主张是针对诚实身份提出的，而恶意 NF 按其构造就是其自身运行的真实对端。；token 格式与 NRF 的签名被建模为 NRF 与 AF 共享密钥下的 MAC。

A03: 订阅参数的一致性

每次 AF 接受订阅创建/更新，或消费者接受通知时，都存在一个匹配的对端运行，双方对订阅标识、notifUri、notifCorrId、vflTrainSubs 与 vflPreFlag 的取值一致。

双方对 subscriptionId、notifUri、notifCorrId 和准备标志达成一致：消费者在 201 和更新响应中读到的内容就是 AF 为其订阅所接受的内容，而其接受的通知携带其自身订阅的 correlation 标识。

- 结果：成立；回答了所问：是；可在有保留的情况下使用
- 价值 低：API 在请求和响应中携带相同的值，因此一致性直接来自消息格式；该结果确认模型与源文一致。
- 文稿中已陈述：是。文稿中陈述之处：s0039, s0048, s0074, s0241
- 依据：更新响应被建模为携带 correlation 标识，正如更新后资源的 200 OK 表示所应携带的。；TLS 与 token 建模同 A02。

A04: 请求与通知的新鲜性

每次 AF 成功创建订阅或消费者成功接受通知，都对应一个此前未使用过的对端运行；同一请求不能被重复接受为新的订阅或新的通知。

攻击者无法仅凭网络使一条通知被接受两次，也未发现同一消费者运行的同一请求被接受两次，除非 replay 录制的记录，而模型接受它仅仅是因为它将 TLS 加密视为确定性的。因此 API 的新鲜性完全依赖于 TLS：订阅请求和通知中都不携带 nonce、序列号或时间戳。

- 结果：成立；回答了所问：部分；可在有保留的情况下使用
- 价值 低：ProVerif 发现的唯一失败是模型产物，剩下的事实是 API 对 TLS 的新鲜性没有任何补充；文稿已要求 SBI 层的 replay 保护。
- 文稿中已陈述：是。文稿中陈述之处：s0038, s0074, s0098

- 依据：创建操作的 replay 是将 TLS 建模为确定性加密所产生的产物；TLS 1.3 记录属于一次握手，攻击者没有消费者的密钥就无法重复该握手。；未建模序列号或轮次号，因此无法表达通知跨轮次的新鲜性。
- 未决：录制的 TLS 记录在部署中能否被 replay 由 TLS 决定，而非由 API 决定；API 本身未定义请求 nonce 或序列号。

A08: 通知绑定到已批准的订阅

AF 接受的通知投递参数（notifUri、notifCorrId、vflTrainSubs、vflPreFlag）必须来自该消费者此前获批的订阅，且准备阶段标志为 true 时不得发出通知。

AF 仅在接受了将准备标志设为 false 的更新之后才通知，且始终使用该更新的 notifUri 和 notifCorrId。对于仅拥有网络的攻击者，这意味着消费者自己的值；对于另一个合法 NF，这意味着攻击者的值，因为该 NF 可以使 AF 接受该更新。

- 结果：不成立（2 个攻击）；回答了所问：部分；可在有保留的情况下使用
- 价值 高：该攻击是对另一消费者训练报告的真实窃取，所用凭据是每个授权 NF 都可以拥有的；文稿未陈述此点。
- 文稿中已陈述：不明确。所依据的源文：s0074, s0213, s0241, s0276
- 依据：假设 subscriptionId 可被攻击者获知，因为它是资源 URI 而非秘密。；AF 检查 token 和服务范围，但不做按资源的授权，因为源文未定义任何此类授权。
- 未决：AF 是否必须接受属于另一个 NF 的 notifUri；源文未说明。

Z01: 每个操作的令牌与范围

每次订阅创建/更新/删除或通知投递被接受，都必须有来自授权服务器（NRF）的有效 token，且 token 的 scope 覆盖 naf-vfl-train 服务。

AF 接受的每次创建、更新和删除都依赖于 NRF 向同一 NF 身份为 naf-vfl-train 范围签发的 token，这既针对仅拥有网络的攻击者，也针对持有自身 token 的合法 NF。该 token 不能用于另一个 NF 的身份。

- 结果：Holds；所问是否得到回答：是；可用但有保留
- 价值中：它证明了授权步骤按预期工作，这本身有价值，但它依赖于 OAuth2 已部署这一假设，而原文将此留给本地配置。
- 文稿中已说明：是。文稿中的位置：s0273、s0274、s0276
- 依据：AF 被建模为始终验证令牌，而原文将 OAuth2 设为可选。；NRF 的签名密钥被建模为与 AF 共享的 MAC 密钥，令牌被建模为没有生命周期或受众。
- 待定：原文称访问可使用 OAuth2 授权，因此该保证对使用 OAuth2 的配置成立。

Z03: 按订阅授权

用于订阅更新/删除或通知投递的授权，必须绑定到该消费者自己的订阅资源与对应操作，不能被用于其他消费者的订阅。

任何 NF 都不能以另一个 NF 的身份行事：只有当 AF 验证的令牌是签发给在传输层完成认证的身份时，AF 才接受该操作。AF 没有检查的是该身份是否拥有它所指的订阅，因此任何持有服务范围令牌的 NF 都可以更新或删除另一个消费者的订阅并接收其通知。

- 结果：Fails（3 个攻击）；所问是否得到回答：部分；可用但有保留

- 价值高：该攻击会导致另一个消费者的订阅和训练报告丢失，同一运营商的每个已授权 NF 都可实施，而按规范定义的 API 没有任何检查能阻止它。
- 文稿中已说明：不明确。所依据的原文文本：s0144、s0276、s0045、s0061
- 依据：假设攻击者能够知道 subscriptionId；模型中有两个 NF 身份。；AF 的查找和授权按原文描述建模：令牌、范围与资源 URI，没有所有者比较。
- 待定：部署是否应添加 API 未定义的资源级检查。

Z04: 删除后无通知

订阅被删除（或 vflPreFlag 由 true 更新为 false 之前）之后，AF 不得再依据该旧订阅向消费者投递通知。

在准备标志仍为 true 时，AF 不发送通知；删除之后，AF 拒绝重复更新同一订阅，而不是再次通知。谁可以写该标志和通知参数仅由令牌与服务范围决定，因此另一个合法 NF 可以抑制或重定向某个订阅的通知。

- 结果：Fails（1 个攻击）；所问是否得到回答：部分；可用但有保留
- 价值中：标志行为如注释所述，但另一个 NF 可以写入该标志的可能性是主发现中同一缺失所有者检查的后果。
- 文稿中已说明：不明确。所依据的原文文本：s0241、s0061、s0074
- 依据：删除性质在有界模型上回答，AF 展开到四步且只有一个身份。；准备标志性质在完整模型上针对网络攻击者回答；恶意 NF 的回答即 A08 记录的攻击。
- 待定：AF 是否必须比较令牌主体与订阅的创建者；原文没有说明，API 也没有能表达这一点的资源级范围。

S05: 已删除订阅不产生通知

订阅删除生效之后，使用该订阅的旧 notifUri、notifCorrId 或 subscriptionId 不能触发新的通知投递。

在展开模型中，删除后到达的重复更新被拒绝且不产生通知，因此旧的 subscriptionId、notifUri 和 notifCorrId 本身无法让报告继续。该回答覆盖订阅生命周期的四步和一条重复消息。

- 结果：在界内成立（变化值展开到 4 步）；所问是否得到回答：部分；可用但有保留
- 价值低：它在界内确认了删除的目的，并表明该性质依赖于 AF 丢弃记录；原文没有任何与之矛盾的内容。
- 文稿中已说明：不明确。所依据的原文文本：s0054、s0061、s0062
- 依据：回答是有界的：创建、更新与通知、删除，以及一次重复更新。；有界模型只有一个身份和一个 TLS 密钥，因此对另一个 NF 在删除后自己发起的新更新不置一词。；删除被建模为 AF 不再持有该记录；如果保留记录，该性质将不成立，对照模型 bounded-buggy.pv 显示了这一点。
- 待定：在真实实现中，删除后多久重复请求仍可能被接受；模型将删除固定在展开运行的一个点上。

U01: AF 身份与关联绑定

AF 接受订阅或消费者接受通知时，AF 身份、subscriptionId、notifCorrId 与训练轮次标识必须与匹配的对端运行一致。

消费者仅从 AF 接受 201 或通知，仅针对 AF 返回给它的 subscriptionId，并且仅带有其自身订阅的 notifCorrId。轮次编号不属于该 API；轮次在 TS 29.520 的通知数据内部传递，模型仅通过订阅内容来绑定它。

- 结果：Holds；所问是否得到回答：是；可用但有保留
- 价值低：subscriptionId 与 notifCorrId 的绑定来自消息格式；问题中的轮次部分无法针对该 API 提出。

- 文稿中已说明：是。文稿中的位置：s0039、s0074、s0144、s0235
- 依据：训练轮次标识未被建模，因为所选原文单元未定义它。；TLS 和令牌建模同 A02。
- 待定：训练轮次在该 API 中没有字段，因此轮次绑定只能通过订阅的通知内容实现。

U02: 仅所有者可控制订阅

对某 subscriptionId 的更新/删除只能由该订阅的创建者发起；通知只能投递给该订阅者提供的 notifUri 且 notifCorrId 一致。

面对仅有网络的攻击者，通知只发往消费者提供的 notifUri 和 notifCorrId。面对另一个合法 NF 则不然：该 NF 可以更新或删除订阅，并让 AF 将通知投递到它自己的 URI。

- 结果：Fails（3 个攻击）；所问是否得到回答：部分；可用但有保留
- 价值高：这与主发现是同一个弱点，以订阅所有者的问题表述，而文稿未说明它。
- 文稿中已说明：不明确。所依据的原文文本：s0045、s0061、s0074、s0144
- 依据：假设攻击者能够知道 subscriptionId；模型中有两个 NF 身份。；对于对订阅的操作，AF 仅检查令牌和服务范围。
- 待定：AF 是否应记录订阅的创建者并与令牌主体比较。

U03: 恶意 NF 被限制在自身订阅内

持有自身合法凭据的恶意 NF 不能使 AF 接受跨训练轮次的订阅内容替换，也不能对其他消费者的订阅执行更新或删除。

合法 NF 无法以另一个 NF 的身份使任何操作被接受，但它可以用自己的有效令牌操作另一个消费者的订阅：替换 notifUri、notifCorrId 和准备标志，接收该订阅的训练通知，并可以删除该订阅。

- 结果：Fails（3 个攻击）；所问是否得到回答：部分；可用但有保留
- 价值高：它以文稿未说明的具体攻击回答了恶意合法 NF 的问题。
- 文稿中已说明：不明确。所依据的原文文本：s0045、s0061、s0144、s0276
- 依据：假设攻击者能够知道 subscriptionId；模型中有两个 NF 身份。；只对订阅的控制值建模；TS 29.520 的训练轮次内容未建模，因此轮次仅通过订阅字段受到影响。
- 待定：部署是否添加 API 未定义的资源级授权。

X01: OAuth2 令牌传输机密性

网络攻击者永远不会得知 NF 消费者从 NRF 为 naf-vfl-train 范围获得的访问令牌。

NWDAF 从 NRF 获得的访问令牌绝不会被仅有网络的攻击者得知：它只在到消费者的通道内传输，并绑定到该消费者的身份。对照显示同一查询确实能检测到被公开的令牌，正如恶意 NF 公开自己的令牌那样。

- 结果：Holds；所问是否得到回答：是；可用但有保留
- 价值低：它确认了 TLS 提供且文稿已要求的内容。
- 文稿中已说明：是。文稿中的位置：s0273、s0274、s0098
- 依据：令牌在建模的 TLS 通道内传输；消费者存储泄漏未建模。

附录 C：主张和证明器的答案

证明器对每个目标的记录：达到的级别、达到该级别的查询、是否检查了对照，以及分析者对每个攻击的判定。

目标	级别	界	查询	对照	攻击	主张
A02	proved		a02_create	checked		4 个 proved
A03	proved		a03_created	checked		3 个 proved
A04	proved		a04_notif	checked	a04_create（model_artifact）	1 个 proved，1 个 attack
A08	proved		a08_net	checked	a08_origin（holds_in_source）；a08_owner（holds_in_source）	1 个 proved，2 个 attack
Z01	proved		z01_create			6 个 proved
Z03	proved		z03_imp		z03_update（holds_in_source）；z03_delete（holds_in_source）；z03_notif（holds_in_source）	1 个 proved，3 个 attack
Z04	proved		a08_net	checked	a08_origin（holds_in_source）	1 个 proved，1 个 bounded，1 个 attack
S05	bounded	将变化的值展开到 4 步	s05	checked		2 个 bounded
U01	proved		u01_create	checked		2 个 proved
U02	proved		z03_notif_net	checked	z03_update（holds_in_source）；z03_delete（holds_in_source）；z03_notif（holds_in_source）	1 个 proved，3 个 attack
U03	proved		z03_imp		z03_update（holds_in_source）；z03_delete（holds_in_source）；z03_notif（holds_in_source）	1 个 proved，3 个 attack
X01	proved		x01_token	checked		1 个 proved

逐条主张，按分析者对每条主张的措辞；每个答案均由证明器给出：

目标	主张	攻击者	回答	查询	对照
A02	只有当该 NF 的真实运行发出了该创建请求时，AF 才接受以该 NF 身份发起的 VFL 训练订阅创建（对等认证），并针对仅掌握网络的攻击者成立。	`network`	proved	a02_create	checked
A02	只有当该 NF 的真实运行发出了该更新时，AF 才接受以该 NF 身份发起的订阅更新，并针对仅掌握网络的攻击者成立。	`network`	proved	a02_update	checked
A02	只有当该 NF 的真实运行发出了该删除时，AF 才接受以该 NF 身份发起的订阅删除，并针对仅掌握网络的攻击者成立。	`network`	proved	a02_delete	checked
A02	只有当 AF 确实向消费者发送了该通知时，消费者才接受该 VFL 训练通知，并针对仅掌握网络的攻击者成立。	`network`	proved	a02_notif	checked

目标	主张	攻击者	回答	查询	对照
A03	消费者接受的通知携带的是其在 AF 上自己订阅的 subscriptionId、notifUri 和 notifCorrId，并针对仅掌握网络的攻击者成立。	`network`	proved	a03_notif	checked
A03	消费者在 201 响应中读到的 subscriptionId、notifUri、notifCorrId 和 vflPreFlag 正是 AF 为该次创建所接受的这些值，并针对仅掌握网络的攻击者成立。	`network`	proved	a03_created	checked
A03	消费者在更新响应中看到的 subscriptionId、notifUri、notifCorrId 和 vflPreFlag 是 AF 为该消费者的该订阅所接受的这些值，并针对仅掌握网络的攻击者成立。	`network`	proved	a03_update	checked
A04	一次创建请求不会被接受两次：对同一 NF 的创建的两次接受必须对应两次该 NF 的运行。	`network`	attack (model_artifact)	a04_create	
A04	对于 AF 的一次发送，通知至多被接受一次：无法让消费者接受同一通知两次。	`network`	proved	a04_notif	checked
A08	通知参数来自消费者自己已批准的订阅：只有订阅所有者本人的更新才能设置这些参数。	`malicious_nf`	attack (holds_in_source)	a08_origin (the control of a08_net)	
A08	针对受害者订阅的通知绝不会被发送到另一个 NF 的 notifUri。	`malicious_nf`	attack (holds_in_source)	a08_owner	
A08	AF 发送的每条通知都使用订阅所有者本人在 vflPreFlag 设为 false 时所做的更新中的 notifUri 和 notifCorrId；在标志仍为 true 时不发送任何通知。	`network`	proved	a08_net	checked
Z01	AF 接受的每次创建都依赖于 NRF 为 naf-vfl-train 范围签发给同一 NF 身份的访问令牌，并针对仅掌握网络的攻击者成立。	`network`	proved	z01_create	none
Z01	AF 接受的每次更新都依赖于为 naf-vfl-train 范围签发给同一 NF 身份的访问令牌，并针对仅掌握网络的攻击者成立。	`network`	proved	z01_update	none
Z01	AF 接受的每次删除都依赖于为 naf-vfl-train 范围签发给同一 NF 身份的访问令牌，并针对仅掌握网络的攻击者成立。	`network`	proved	z01_delete	none
Z01	AF 接受的每次创建都依赖于 NRF 为该 NF 签发给 naf-vfl-train 范围的令牌，此处针对持有自己有效令牌的恶意 NF。	`malicious_nf`	proved	z01_create	none
Z01	AF 接受的每次更新都依赖于 NRF 为该 NF 签发给 naf-vfl-train 范围的令牌，此处针对持有自己有效令牌的恶意 NF。	`malicious_nf`	proved	z01_update	none
Z01	AF 接受的每次删除都依赖于 NRF 为该 NF 签发给 naf-vfl-train 范围的令牌，此处针对持有自己有效令牌的恶意 NF。	`malicious_nf`	proved	z01_delete	none
Z03	持有服务范围有效令牌的 NF 无法更新另一个消费者所创建的订阅。	`malicious_nf`	attack (holds_in_source)	z03_update	
Z03	持有服务范围有效令牌的 NF 无法删除另一个消费者所创建的订阅。	`malicious_nf`	attack (holds_in_source)	z03_delete	
Z03	订阅的通知只到达该订阅创建者所提供的 notifUri 和 notifCorrId。	`malicious_nf`	attack (holds_in_source)	z03_notif (the control of z03_notif_net)	

目标	主张	攻击者	回答	查询	对照
Z03	没有 NF 能让以另一个 NF 的身份发起的操作被接受：只有当 AF 所验证的令牌签发给了在传输层完成认证的同一身份时，AF 才接受更新。	`network`	proved	z03_imp	none
Z04	只有在订阅所有者通过更新把 vflPreFlag 设为 false 之后，才会为该订阅发送通知。	`malicious_nf`	attack (holds_in_source)	a08_origin (the control of a08_net)	
Z04	订阅删除后，对同一订阅的重复（重放）更新不会导致通知：AF 会拒绝它。	`network`	bounded (the changing value unrolled to 4 steps)	s05	checked
Z04	订阅的 vflPreFlag 仍为 true 期间不会发送任何通知：AF 只在标志设为 false 的更新之后才发送通知。	`network`	proved	a08_net	checked
S05	删除生效后，携带旧 subscriptionId、notifUri 和 notifCorrId 的重放更新不会产生新通知。	`network`	bounded (the changing value unrolled to 4 steps)	s05	checked
S05	删除生效后，无论是重放的更新，还是来自另一个 NF、携带旧 subscriptionId 的新更新，都不会产生新通知。	`malicious_nf`	bounded (the changing value unrolled to 4 steps)	s05	checked
U01	消费者只接受来自 AF 的 201，且针对的是 AF 为其创建的 subscriptionId 以及它自己发送的 notifCorrId。	`network`	proved	u01_create	checked
U01	消费者只接受来自 AF 的通知，且针对的是自己的 subscriptionId 和自己订阅的 notifCorrId。	`network`	proved	u01_notif	checked
U02	在网络攻击者下，通知只会发送到其订阅所属消费者所提供的 notifUri 和 notifCorrId。	`network`	proved	z03_notif_net	checked
U02	只有创建了订阅的 NF 才能更新该订阅。	`malicious_nf`	attack (holds_in_source)	z03_update	
U02	只有创建了订阅的 NF 才能删除该订阅。	`malicious_nf`	attack (holds_in_source)	z03_delete	
U02	通知只发往该订阅创建者所提供的 notifUri 和 notifCorrId。	`malicious_nf`	attack (holds_in_source)	z03_notif (the control of z03_notif_net)	
U03	除网络之外没有其他凭据时，没有 NF 能让以另一个 NF 的身份发起的操作被接受。	`network`	proved	z03_imp	none
U03	持有自己凭据的合法 NF 无法替换另一个消费者订阅的内容。	`malicious_nf`	attack (holds_in_source)	z03_update	
U03	持有自己凭据的合法 NF 无法删除另一个消费者的订阅。	`malicious_nf`	attack (holds_in_source)	z03_delete	
U03	持有自己凭据的合法 NF 无法让 AF 把另一个消费者的训练通知投递给它。	`malicious_nf`	attack (holds_in_source)	z03_notif (the control of z03_notif_net)	
X01	NWDAF 从 NRF 为 naf-vfl-train 范围获取的访问令牌绝不会被仅掌握网络的攻击者所知。	`network`	proved	x01_token	checked

附录 D：分析是怎么跑的

LLM 分析者根据文稿构建协议模型，并把每个性质交给 ProVerif；第 3 节中的每个结果都是证明器的回答。

ProVerif+ Agent 会话 session-20261114T232842，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：51，证明器 11 秒，总耗时 13 分钟，费用 0.129 USD。

ProVerif：运行 86 次证明，86 次得出结论，0 次无答案，10 秒，记录 57 个回答。

分析了什么

协议	AF VFL client training API
版本	19.2.0
分析范围	可信 AF 作为 VFL client，NWDAF server 直接调用 Naf_VFLTraining；一次能力检查、一个训练轮次通知及取消，排除 NEF/不可信 AF 分支和全局多客户端调度。
不在范围内	符号模型不证明算法的计算安全或抗量子安全；攻击轨迹只在明确假设下成立，不直接等同规范漏洞。每个性质必须有可达性/正例控制。 固定 Rel-19。分别区分外部网络攻击者与持有自身凭据的恶意合法 NF；TLS 认证加密按端点建模，合法 NF 不能读取其他 NF 的 TLS 会话。 OAuth2 subject/audience/scope/expiry 及 TLS 身份绑定依照所附基线；服务 scope 不自动等于资源所有权。单调表不能模拟真实删除，有限状态生命周期必须明确界定。目标是指定 API 子流程，不是完整 5G 安全。 这是同一协议范围在修正表格定位后的实现版本下重跑；前次在准备阶段被实现版本锁拒绝，不能绕过版本锁续用旧输入。
原文	来自下列章节的 322 个编号原文单元（153032 字节）。本报告中的 s0001 之类的引用即为这些原文单元之一

构建分析所依据的文稿章节：

文稿	章节	标题
main	5.2	Naf_VFLTraining 服务
main	5.2.1	服务描述
main	5.2.1.1	概述
main	5.2.1.2	服务架构
main	5.2.1.3	网络功能
main	5.2.1.3.1	应用功能（AF）
main	5.2.1.3.2	NF 服务消费者
main	5.2.2	服务操作
main	5.2.2.1	引言
main	5.2.2.2	Naf_VFLTraining_Subscribe
main	5.2.2.2.1	概述
main	5.2.2.2.2	VFL 训练订阅创建
main	5.2.2.2.3	VFL 训练订阅更新
main	5.2.2.3	Naf_VFLTraining_Unsubscribe
main	5.2.2.3.1	概述

文稿	章节	标题
main	5.2.2.3.2	VFL 训练订阅删除
main	5.2.2.4	Naf_VFLTraining_Notify
main	5.2.2.4.1	概述
main	5.2.2.4.2	VFL 训练通知
main	6.1	Naf_VFLTraining 服务 API
main	6.1.1	引言
main	6.1.2	HTTP 的使用
main	6.1.2.1	概述
main	6.1.2.2	HTTP 标准头
main	6.1.2.2.1	概述
main	6.1.2.2.2	内容类型
main	6.1.2.3	HTTP 自定义头
main	6.1.3	资源
main	6.1.3.1	概述
main	6.1.3.2	资源：VFL 训练订阅
main	6.1.3.2.1	描述
main	6.1.3.2.2	资源定义
main	6.1.3.2.3	资源标准方法
main	6.1.3.2.3.1	POST
main	6.1.3.2.4	资源自定义操作
main	6.1.3.3	资源：单个 VFL 训练订阅
main	6.1.3.3.1	描述
main	6.1.3.3.2	资源定义
main	6.1.3.3.3	资源标准方法
main	6.1.3.3.3.1	GET
main	6.1.3.3.3.2	PUT
main	6.1.3.3.3.3	PATCH
main	6.1.3.3.3.4	DELETE
main	6.1.4	无关联资源的自定义操作
main	6.1.5	通知
main	6.1.5.1	概述
main	6.1.5.2	VFL 训练通知
main	6.1.5.2.1	描述
main	6.1.5.2.2	目标 URI
main	6.1.5.2.3	标准方法
main	6.1.5.2.3.1	POST

文稿	章节	标题
main	6.1.6	数据模型
main	6.1.6.1	概述
main	6.1.6.2	结构化数据类型
main	6.1.6.2.1	引言
main	6.1.6.2.2	类型：VflTrainingSubs
main	6.1.6.2.3	类型：VflTrainingSubsPatch
main	6.1.6.3	简单数据类型与枚举
main	6.1.6.3.1	引言
main	6.1.6.3.2	简单数据类型
main	6.1.6.4	描述备选数据类型或数据类型组合的数据类型
main	6.1.6.5	二进制数据
main	6.1.6.5.1	二进制数据类型
main	6.1.7	错误处理
main	6.1.7.1	概述
main	6.1.7.2	协议错误
main	6.1.7.3	应用错误
main	6.1.8	特性协商
main	6.1.9	安全
main	6.1.10	HTTP 重定向

源文包所定位的协议目的：可信 AF 作为 VFL client，NWDAF server 直接调用 Naf_VFLTraining；一次能力检查、一个训练轮次通知及取消，排除 NEF/不可信 AF 分支和全局多客户端调度。

对照文稿定性质

在写出查询之前，分析者把草拟的性质清单与文稿本身对协议目的的说明做了对照。名称、性质所针对的对象以及文稿的说法均属分析者的解读；所列位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
A02	VFL 请求对端认证	AF（可信 VFL client）确信其接受的订阅创建/更新/删除请求来自它所声明的真实 NWDAF；消费者确信通知来自该 AF。	TS 29.500/TS 33.501 要求 NF 到 NF 的直接通信进行双向认证；该 API 对可信 AF 使用 TLS 和 OAuth2 客户端凭据。	ts-33-501:2871, main:931, s0009, s0011, s0038, s0045, s0061, s0074, s0098, s0099
A03	订阅参数的一致性	AF 与消费者对双方共同操作的订阅在 subscriptionId、notifUri、notifCorrId、vflTrainSubs 和 vflPreFlag 上达成一致。	VflTrainingSubs 表示携带 notifUri、notifCorrId 和 vflPreFlag，AF 会回显这些参数并在之后使用；通知投递使用该订阅的 notifCorrId。	main:1126, s0038, s0039, s0074, s0241, s0244
A04	请求与通知的新鲜性	AF 对每次请求的接受、消费者对每条通知的接受都对应一次未使用的对端运行；同一个请求不能被接受两次。	TS 33.501 要求对 SBI 信令进行重放保护；该 API 本身未定义请求 nonce 或序列号。	ts-33-501:2865, ts-33-501:2915, s0038, s0061, s0074

ID	简称	对象	文稿怎么说	出处
A08	通知绑定到已批准的订阅	AF 使用的通知参数（notifUri、notifCorrId、vflTrainSubs）是消费者已接受订阅的参数；当 vflPreFlag 为 true 时不发送任何通知。	VflTrainingNotify 请求发送到在相应订阅创建/更新期间收到的 notifUri；关于 vflPreFlag 的说明禁止在该标志置为 false 之前发送通知。	main:1126, main:1103, s0074, s0213, s0241
Z01	每个操作的令牌与范围	每次被接受的创建、更新、删除和通知投递都依赖于 NRF 为该消费者身份签发的、具有 naf-vfl-train 范围的访问令牌。	对 API 的访问可用 OAuth2 客户端凭据授权，NRF 作为授权服务器，仅有单一范围 naf-vfl-train。	rfc6749:2859, s0273, s0274, s0276
Z03	按订阅授权	持有该服务范围有效令牌的 NF 只能更新、删除其创建的订阅，或接收这些订阅的通知。	该 API 只定义了单一的服务级范围，没有资源级或操作级范围；OAuth2 不提供资源服务器核查令牌是否签发给出示方客户端的方法。	rfc6749:2879, s0144, s0276
Z04	删除后无通知	订阅被删除后，或在 vflPreFlag 置为 false 之前，AF 不为其发送任何通知。	Unsubscribe 请求在 AF 处删除该订阅；通知只发给先前已订阅的消费者。	main:1126, s0054, s0061, s0062, s0074, s0241
S05	已删除订阅不产生通知	删除生效后，旧的 subscriptionId、notifUri 和 notifCorrId 不能引发新的通知。	删除会移除 AF 处的单个订阅资源；通知只发给先前已订阅的消费者。	main:1126, s0054, s0061, s0062, s0074
U01	AF 身份与关联绑定	消费者只接受来自 AF 的 201 或通知，且携带其所获得的 subscriptionId 和自己订阅的 notifCorrId；通知的训练轮次是该订阅所对应的轮次。	201 响应携带所创建资源的 Location；通知发送到 notifUri，并携带由订阅建立的关联。	main:1126, s0039, s0074, s0144, s0241
U02	仅所有者可控制订阅	只有创建了订阅的 NF 才能更新或删除该订阅，通知也只发往该 NF 提供的 notifUri 和 notifCorrId。	单个订阅资源由 AF 管理；除服务范围外未定义按资源的授权。	rfc6749:2879, s0045, s0061, s0074, s0144, s0276
U03	恶意 NF 被限制在自身订阅内	持有自身凭据的合法 NF 不能替换另一消费者订阅的内容（notifUri、notifCorrId、训练轮次），也不能更新或删除该订阅。	同一信任域内的 NF 相互认证，但该 API 仅基于单一服务范围进行授权。	ts-33-501:2859, ts-33-501:2875, rfc6749:2879, s0045, s0061, s0144, s0273, s0276
X01	OAuth2 令牌传输机密性	NF 服务消费者的 OAuth2 访问令牌，必须在 NRF、消费者和 AF 之间保持机密。	RFC 6749 要求访问令牌凭据在传输中保持机密，且只能通过 TLS 使用；该 API 依赖 NF 之间的 TLS。	rfc6749:2859, main:1141

分析者依据文稿补充的性质：X01。

文稿里的安全表述，逐段去向

宿主把文稿里说明协议保护什么、防什么的章节逐段列出，共 398 段；分析者对每一段说明了去向：定为性质、定为攻击者条件，或者为什么都不选。选了 27 段，没选 371 段。列哪些段落由标准的章节结构决定；每一段的去向是分析者的判断。

段落	出处	定为	不选的原因
P001 至 P002	rfc6749:2778-2786	没有陈述目标	这是框架层面的指导，指向各节的威胁；并未对 API 提出任何要求。

段落	出处	定为	不选的原因
P003 至 P006	rfc6749:2790-2823	Z01, `malicious_nf`	
P007 至 P010	rfc6749:2827-2850	Z01, `malicious_nf`	
P011 至 P014	rfc6749:2859-2877	Z01, `malicious_nf`	
P015	rfc6749:2879-2881	Z03, Z01, `malicious_nf`	
P016 至 P021	rfc6749:2885-2917	没有陈述目标	本 API 授权所用的 client-credentials 授权不使用刷新令牌。
P022 至 P025	rfc6749:2921-2943	没有陈述目标	SBI 的 client-credentials 流程不使用授权码授权。
P026 至 P029	rfc6749:2947-2980	没有陈述目标	重定向 URI 操纵属于授权码授权，本 API 不使用该授权。
P030 至 P033	rfc6749:2984-3003	没有陈述目标	不使用资源所有者口令授权。
P034 至 P035	rfc6749:3013-3019	Z01, `network`	
P036	rfc6749:3023-3028	A02, U01, `network`	
P037 至 P039	rfc6749:3032-3041	没有陈述目标	凭据猜测攻击针对用户自选的口令；SBI 客户端用证书认证，因此流程中不存在可猜测的秘密。
P040 至 P042	rfc6749:3045-3066	没有陈述目标	钓鱼攻击涉及资源所有者和用户代理；二者都不参与本 SBI 流程。
P043 至 P048	rfc6749:3070-3110	没有陈述目标	CSRF 针对携带环境凭据的浏览器请求；本流程不涉及浏览器，消费者在 TLS 和 OAuth2 层完成认证。
P049 至 P050	rfc6749:3119-3138	没有陈述目标	点击劫持属于用户代理的问题，不属于本流程。
P051 至 P052	rfc6749:3142-3150	没有陈述目标	代码注入和输入校验针对 API 实现，不是本消息流程的性质。
P053 至 P054	rfc6749:3154-3167	不在范围内	开放重定向针对 HTTP 重定向，本流程中的重定向由 SCP 完成，不在所建模的子流程之内。
P055 至 P062	rfc6749:3170-3210	没有陈述目标	隐式授权的令牌误用不适用于 client-credentials 授权。
P063	ts-33-501:2491-2491	没有陈述目标	降级协商针对安全特性的协商；Naf_VFLTraining API 在 Rel-19 中没有定义任何可选特性（表 6.1.8-1 为空）。
P064 至 P074	ts-33-501:2495-2517	不在范围内	这些是对订阅认证以及 UE 的 5GC/NG-RAN 密钥的要求，本 API 子流程不涉及。
P075 至 P213	ts-33-501:2523-2853	不在范围内	这些是对 UE、gNB、ng-eNB 和 NG-RAN 密钥处理的要求；它们属于 TS 33.501 的无线和 UE 部分，本任务不予考虑。
P214	ts-33-501:2859-2859	U03, `malicious_nf`	
P215	ts-33-501:2865-2865	A04, `network`	
P216	ts-33-501:2867-2867	Z01, `malicious_nf`	

段落	出处	定为	不选的原因
P217	ts-33-501:2869-2869	没有陈述目标	拓扑隐藏是发现的性质，不是此处分析的订阅与通知流程的性质。
P218	ts-33-501:2871-2871	A02, U01, `network`	
P219	ts-33-501:2873-2873	A02	
P220	ts-33-501:2875-2875	U02, Z03, A08, `malicious_nf`	
P221 至 P222	ts-33-501:2879-2881	没有陈述目标	这是描述 NRF 做什么的文字；除 P223-P227 外没有提出其他要求。
P223 至 P225	ts-33-501:2883-2887	Z01, `malicious_nf`	
P226 至 P227	ts-33-501:2889-2891	Z01, `malicious_nf`	
P228 至 P234	ts-33-501:2895-2907	不在范围内	NEF 安全要求属于不可信 AF 分支，本任务将其排除。
P235 至 P241	ts-33-501:2911-2923	不在范围内	SCP 要求针对间接通信，本任务不予考虑。
P242 至 P312	ts-33-501:2929-3075	不在范围内	端到端互联、SEPP 和漫游中介要求属于跨 PLMN 漫游，本单运营商子流程不涉及。
P313 至 P314	ts-33-501:3079-3081	不在范围内	IPUPS 是跨 PLMN 边界功能，不在所分析的子流程之内。
P315 至 P318	ts-33-501:3085-3091	没有陈述目标	3gpp-Sbi-Originating-Network-Id 头要求未陈述本订阅与通知流程的任何性质。
P319 至 P327	ts-33-501:3097-3115	不在范围内	信令监测要求针对监测基础设施，本任务不予考虑。
P328 至 P337	ts-33-501:3121-3141	不在范围内	安全可见性和可配置性针对运营商部署，不是 API 消息流程。
P338 至 P375	ts-33-501:3149-3231	不在范围内	算法标识符与选择、5G-RG 和 NSSAAF 要求属于 TS 33.501 的其他部分。
P376 至 P398	ts-33-501:6540-11901	不在范围内	N3、EAP-TLS 附录、IAB、MBS 和 NEF 附录要求属于本任务不予考虑的系统部分。

参与方和受保护的值，逐项是否设为攻击者条件

宿主把起草的性质里点到的参与方和受保护的值逐项列出，共 20 项；分析者对每一项说明了哪个攻击者条件控制这个参与方或持有这个值，或者为什么不设。设了攻击者条件的 12 项，没设的 8 项。清单来自性质本身；每一项怎么处理是分析者的判断。

ID	参与方或值	类别	攻击者条件	不设的原因
S01	AF	参与方	按定义全部失守	AF 持有订阅并发出通知；不诚实的 AF 会破坏针对服务生产者提出的每一条性质，而文稿没有针对可信 AF 提出任何性质（s0009）。
S02	NWDAF	参与方	`malicious_nf`	
S03	NRF	参与方	按定义全部失守	NRF 是令牌的信任根；一旦它被控制，按定义令牌性质即丢失，而文稿没有在它失守的情况下提出任何性质。
S04	恶意合法 NF	参与方	`malicious_nf`	

ID	参与方或值	类别	攻击者条件	不设的原因
S05	NF 实例身份	值	`malicious_nf`	
S06	订阅资源	值	`malicious_nf`	
S07	subscriptionId	值	`malicious_nf`	
S08	notifUri	值	攻击者得不到更多	知道 notifUri 并不能送达通知，通知经 TLS 发往该 URI 所指的端点；替换成自己的 URI 是 Z03/U02 的更新主张。
S09	notifCorrId	值	攻击者得不到更多	知道 notifCorrId 并不能访问通知；消费者只是用它来匹配自己的订阅。
S10	vflTrainSubs	值	攻击者得不到更多	没有目标要求训练集描述的机密性；它的意义在于 AF 必须接受其所有者提供的值，读取它并不改变这一点。
S11	vflPreFlag	值	`malicious_nf`	
S12	通知请求	值	`malicious_nf`	
S13	suppFeat	值	攻击者得不到更多	Rel-19 没有为本 API 定义任何可选特性（表 6.1.8-1 为空），因此该属性不携带任何内容。
S14	OAuth2 access token	值	`malicious_nf`	
S15	naf-vfl-train scope	值	`malicious_nf`	
S16	access token 主体与受众	值	`malicious_nf`	
S17	AF 身份	值	按定义全部失守	AF 身份是消费者认证的信任锚；一旦它被持有，按定义关于生产者的所有保证即丢失。
S18	训练轮次标识	值	`malicious_nf`	
S19	订阅创建者身份	值	`malicious_nf`	
S20	订阅内容	值	攻击者得不到更多	订阅内容的意义在于 AF 必须接受其所有者提供的值（A03/A08）；读取它并不改变此处提出的任何性质。

每条性质在各攻击者条件下的答案

攻击者是分析者在写查询之前设定的；每个答案都是在其中一个攻击者条件下记录的。单元格是证明器在该攻击者条件下对该性质给出的答案；“无答案”是指为该性质设定了一个攻击者条件，但在该条件下证明器留下了未决的主张，或者没有记录任何内容；空单元格是指分析者没有为该性质设定该攻击者条件。

攻击者	持有什么	依据	出处
`network`	仅拥有网络：它能读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`malicious_nf`	自己的 NF 身份、自己的 TLS 凭据，以及从 NRF 合法取得的、用于 naf-vfl-train scope 的自己的 OAuth2 access token	任何已授权 NF 都可以取得服务 scope 的令牌；TS 33.501 假定存在信任区并要求 NF 校验传入消息，因此合法但不诚实的 NF 在范围内。	ts-33-501:2859, ts-33-501:2875, main:1147

ID	`network`	`malicious_nf`
A02	成立	
A03	成立	
A04	成立	
A08	成立	不成立

ID	network	malicious_nf
Z01	成立	成立
Z03	成立	不成立
Z04	成立	不成立
S05	成立	成立
U01	成立	
U02	成立	不成立
U03	成立	不成立
X01	成立	

原文和目标

来源：322 个原文单元，153032 字节，冻结在 source-delivery-01.json 中。 目标：11 个已批准（A02, A03, A04, A08, Z01, Z03, Z04, S05, U01, U02, U03）；提出的问题：3 个。 目标清单事先按草稿批准，使用的是 --approve-targets。

宿主按文档默认值（任务 `decisions: auto`）做出的决定，请你核对：

- approve_package: 批准源文包 protocol-1e783448602f196b8ceaeba2251f

本步骤自报：1 次请求（1 次失败），0.000 USD，输入 81443 tokens，输出 5532 tokens，262 秒。

关于证明器和模型的说明

- Z04：在 ProVerif 中作答，分析者为该目标指定了 changing_state
- S05：在 ProVerif 中作答，分析者为该目标指定了 changing_state

对代数做简化的 ProVerif 模型（xor、dh_algebra、other_algebra）给攻击者的能力弱于真实操作：在此模型中的证明是针对更弱攻击者的证明，在此模型中的攻击则就是攻击。省略对会变化的值所做检查的 ProVerif 模型（changing_state）让各方接受更多内容：其中的证明成立，其中的攻击可能只是缺失的检查。Tamarin+Agent 按原样对这些建模。

按步数给出的界是对 bounded.pv 的回答：这是分析者的第二个 ProVerif 模型，其中持有会变化的值的一方被展开到该步数，并且其检查保留在原位。该模型所做的事少于协议所做的事，因此该性质只在这些步数内成立、不再往外延伸，而在其中发现的攻击就是攻击。步数由分析者声明。

分析者的状态审查

这部分是分析者自己对原文的解读，不是证明器的回答。ProVerif 所示的“是”表示 ProVerif 在展开模型中找到了具有这些步数的轨迹，因此这些步数是可能的；这些步数是否破坏某个目标，只由答案表中的攻击说明，而它们的其他代价属于分析者的解读。“未发现”说明查看了哪些模式，不证明任何东西。

值	由谁保存	何时变化	何时检查	引用
AF 处的 VFL 训练订阅记录（vflTrainSubs、notifUri、notifCorrId、vflPreFlag、creator）	AF（VFL 客户端、服务生产者）	由对集合资源的 POST 创建（s0038、s0039），由对单个资源的 PUT/PATCH 修改（s0045、s0048），由 DELETE 删除（s0061、s0062）	对发往该单个订阅的每个请求：AF 按 subscriptionId 查找资源并检查令牌，但不比较令牌主体与 creator（s0144、s0273、s0276）	s0038、s0039、s0045、s0061、s0144、s0267、s0276

值	由谁保存	何时变化	何时检查	引用
vflPreFlag（订阅的准备标志）	AF	创建时对 VFL 准备置为 true，由激活通知的更新置为 false（s0241）	在 AF 发送通知之前：在标志为 false 之前不发送通知（s0241 NOTE）	s0241、s0045
notifCorrId（通知相关标识符）	AF 和 NWDAF	创建时设置，或可由 PUT/PATCH 替换（s0241、s0244）	消费者将通知的 notifCorrId 与其自己的订阅进行匹配	s0241、s0244、s0074

模式	结果	目标	ProVerif 所示	步数
replay	未发现			所记录的更新在删除之后被再次投递；展开后的 AF 读取它并拒绝它（bounded.pv 查询 refdel 被伪证，因此该步骤确实发生），且之后没有通知（查询 s05 验证通过）。重放的创建之所以被接受为第二个订阅，只是因为模型的 TLS 是确定性加密；这是记录在 A04 下的模型伪影。
repeat_one_time_action	未发现			通知阶段对每个订阅运行一次，随后 AF 只接受删除；在展开模型中，第二次更新不会在其位置上被接受。
desynchronisation	未发现			该模式对订阅记录而言是真实的，但它在无界模型上展示：另一个 NF 的更新替换了记录的 notifUri 和 notifCorrId，消费者永远看不到其仍拥有的订阅的通知。它被记录为 U03 和 Z03 的攻击答案（对 model.pv 的查询 z03_notif）；bounded.pv 不包含第二个身份，因此同一运行无法在那里展示。
update_before_check	未发现			AF 在更新时修改存储的记录，却不检查令牌主体是否为该订阅的 creator；这被记录为 Z03 的攻击答案（对 model.pv 的查询 z03_update）。在 bounded.pv 中，唯一的写入者是其密钥加密该更新的消费者，因此缺失的检查在那里没有可见效果。
no_rollback_on_failure	未发现			在删除之前被放弃的运行会保留订阅及其 notifUri，但在该点之后、在订阅自身生命周期内不会发出通知；原文没有提及重试，因此不再主张其他内容。
race_between_sessions	未发现			模型为每个消费者身份给出一个 subscriptionId，因此一个消费者的两个会话无法区分，同一记录上的竞争也未被建模。在一个消费者针对每次创建发放一个 subscriptionId 的部署的并发会话，超出了本模型所能说明的范围。
distinguishable_failure	未发现			AF 的 403 原因（OVERLOAD、NOT_AVAILABLE_FOR_VFL_PROCESS、VFL_REQS_NOT_MET）未被建模，原文也没有说明它们是否向请求者透露关于该订阅的任何信息；模型中只有接受和不回复。
wrap_or_window	未发现			该 API 不携带计数器、序列号或接受窗口；subscriptionId 是标识符，不是数字，因此没有任何东西可以回绕。

分析者为目标命名的内容：

步骤	目标	特征	理由
38	Z04、S05	changing_state	AF 保存一条状态会变化的订阅记录：在准备阶段创建（vflPreFlag 为 true），由更新激活，发出一次通知，然后被删除。Z04 和 S05 询问在删除之后到达的消息会发生什么，而这正是跨步骤会变化的值；model.pv 省略了该检查，bounded.pv 将 AF 展开四步。
38	A02、A03、A04、A08、Z01、Z03、U01、U02、U03、X01	plain_primitives、many_sessions	模型只对 TLS 风格端点信道使用对称加密、MAC 和私钥派生函数，并对 NRF 的令牌使用 MAC；没有异或或 Diffie-Hellman 代数。查询针对消费者和 AF 的任意数量的会话提出；唯一的固定界是单个诚实身份和单个恶意身份。

分析者的结尾说明

模型：model.pv 给出受信任 AF 和 NWDAF 的 Naf_VFLTraining 流程（以 notifUri/notifCorrId/vflPreFlag 作为能力检查的创建、激活更新、一次带确认的通知、删除），其中 TLS 建模为按端点的 MAC 加加密，OAuth2 客户端凭据以 NRF 作为授权服务器并使用单一范围 naf-vfl-train，另有一个持有自己令牌的恶意但合法的 NF。bounded.pv 将 AF 展开为四步（创建、更新/通知、删除、一次重复更新）；bounded-buggy.pv 是省略删除检查的对照。

已确立：针对网络攻击者，AF 和消费者的认证（A02，四个主张带对照），对 subscriptionId/notifUri/notifCorrId/vflPreFlag 的一致（A03），通知不会被重复接受（A04 的第二个主张），通知只在所有者更新且 vflPreFlag 为 false 之后发出（A08 网络主张、Z04 标志主张），每个被接受操作对应的令牌有效性和主体绑定（Z01，两种攻击者），消费者侧对 AF 和相关标识符的绑定（U01），没有操作会在另一个 NF 的身份下被接受（Z03/U03 网络主张），以及令牌保密性（X01，对照被伪证）。S05 和 Z04 的删除主张在 4 步的有界模型上成立，而对照表明它们依赖于 AF 丢弃该记录。

发现（一项，高，新颖性不明确）：一个持有单一服务范围令牌的合法 NF 可以更新或删除另一个消费者的订阅，并让 AF 将该消费者的 VFL 训练通知投递到它自己的 notifUri，还可以通过改写 vflPreFlag 来抑制上报。文稿给出了其中的要素（单一服务范围、没有资源级范围；RFC 6749 关于资源服务器无法将令牌绑定到客户端的陈述），但没有给出其后果。建议：记录 creator 身份并与令牌主体比较，或定义资源级范围；未在变体模型上检查。

限制：TLS 没有握手或记录状态，因此 ProVerif 发现的创建重放是模型伪影（按此提交）；只有两个身份；subscriptionId 被视为可知；OAuth2 被假定已部署，尽管原文将其设为可选；删除在四步展开内得到回答。Tamarin+ Agent 可以解决 TLS 重放问题以及超出界的删除行为。