NWDAF VFL 客户端训练 API 的安全分析

本报告的其他语言版本：English。

19.8.0 · ProVerif+ Agent 报告

文稿	5G System; Network Data Analytics Services; Stage 3 （协议定义）
检查的性质	17 条：6 条成立，1 条不成立（3 个攻击），10 条没有答案
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

Nnwdaf_VFLTraining 服务让 NF 服务消费者（AF、NEF 或 NWDAF）把 NWDAF 当作 VFL 客户端使用。消费者持有 NRF 为单一范围 nnwdaf-vfltraining 签发给它的 OAuth2 访问令牌，NWDAF 持有训练状态并分配订阅标识符。

消费者以 vflPreFlag 为 true 创建一个订阅，作为能力检查；随后以 vflPreFlag 为 false 将其更新为训练订阅；通过它提供的回调 URI 接收训练报告；最后用 DELETE 取消订阅。两个端点都是同一网络的 NF，通过基于服务的接口上双向认证的 TLS 互相通信。

各方：

- **NF 服务消费者（VFL 服务器）**：运行 VFL 训练的 AF / NEF / NWDAF。持有：客户端凭证；notifUri；notifCorrId；vflCorrId。
- **NRF**：授权服务器，客户端凭证授权。持有：NF 配置文件；本地授权策略。
- **NWDAF（VFL 客户端）**：NF 服务生产者，保存订阅和训练状态。持有：自己的 NF 身份；订阅存储。

图 1 展示了文稿所规定的交互流程。

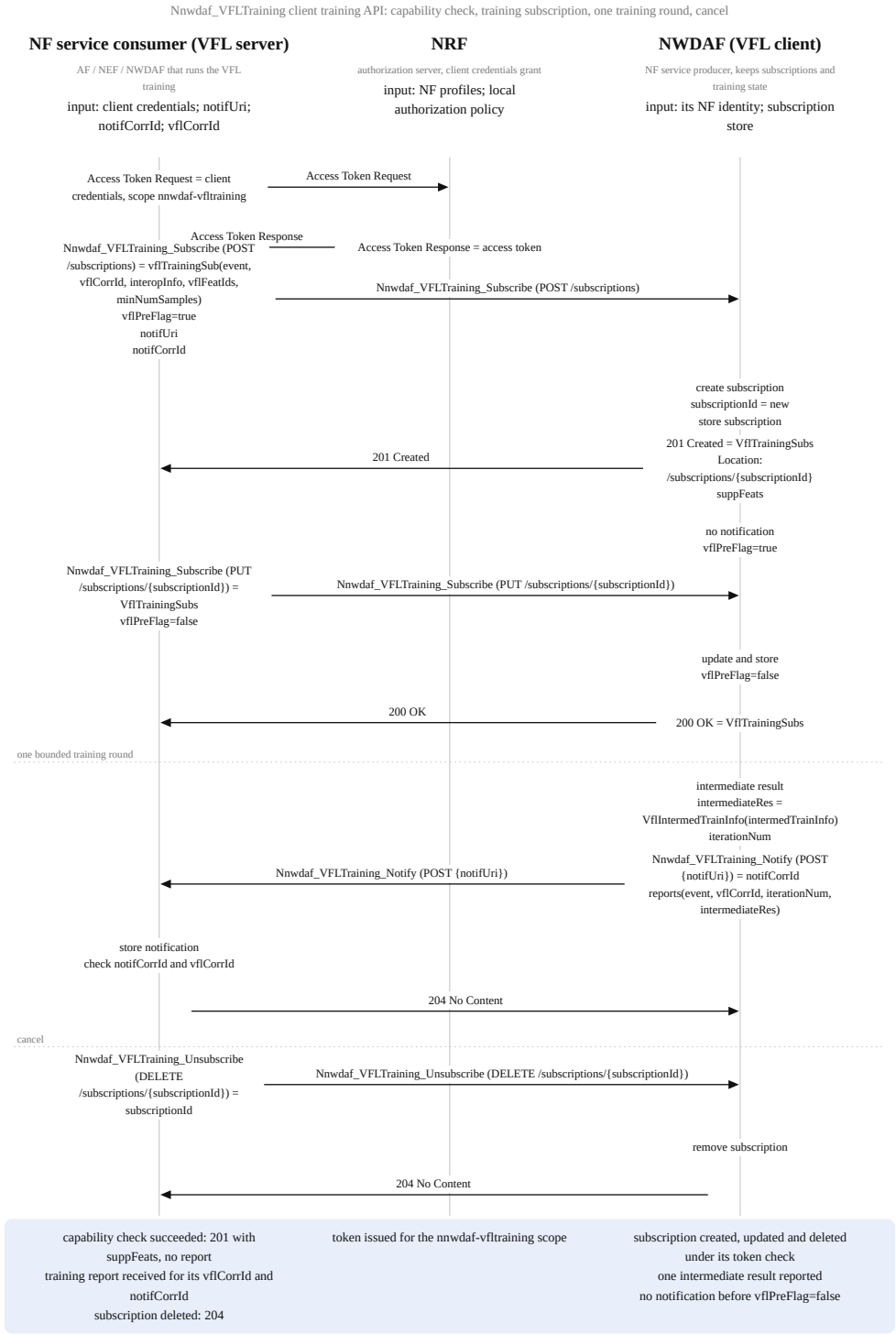


图 1. 所规定的协议。

分析的范围见附录 D：分析了什么、省略了什么，以及它依据的文稿章节。

2 发现

分析共有 1 个发现：以下内容并未在文稿中写明。其中 1 个发现，文稿是否写明并不明确。

模型中的授权是健全的：NWDAF 接受的每一次创建、修改和删除，都由 NRF 为 nnwdaf-vfltraining 范围签发、并由其指名的 NF 出示的令牌作为依据；泄漏给另一个 NF 的令牌无法被用来冒充其所有者行事。仍有一个发现：该 API 没有定义资源级范围，也没有任何操作条款要求所有权检查，因此任何持有服务范围令

牌的 NF，只要知道订阅 URI，就能修改、修补或删除另一个消费者的订阅。通知关联、准备标志和能力检查成立，但这只是因为消费者检查的是它自己选定的关联值。关于新鲜度和通知发送者的三个目标没有答案：ProVerif 的复制请求处理程序让一个创建请求能建立两个订阅。在 17 个目标中，10 个已证明或已到达，4 个带有攻击，3 个没有答案。

攻击图使用图 1 的列。红色表示攻击者的行为。黄色标记某一方在指定交互流程中本不该在该位置发送的消息，以及攻击所破坏的结果。

2.1 持有服务范围的 NF 可以劫持或取消另一个消费者的 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 (ts-29-500:4996, ts-29-500:5000)
价值	高
涉及的性质	Z03 （见第 3 节）
原文	s0048, s0049, s0072, s0073, s0293
依据	ProVerif attack queries `z03_update`, `z03_delete`, `z03_patch`; Figure 2

发生了什么。 该 API 为整个服务定义了单一的 OAuth2 范围，没有资源级范围。NWDAF 校验令牌、其受众和范围，然后仅凭 subscriptionId 查找订阅，并直接执行 PUT、PATCH 或 DELETE，而不询问请求方 NF 是否创建了该订阅。因此，任何持有服务范围令牌并知道另一个消费者订阅 URI 的 NF，都能替换其内容、通过设置 vflPreFlag 停止其训练，或将其删除，而 NWDAF 会像对待所有者一样返回 200、204 或 204。

攻击者需要什么。 本网络的一个 NF 实例身份、NRF 为 nnwdaf-vfltraining 签发的访问令牌，以及受害者订阅的 subscriptionId。文稿并未声明该 ID 保密，它出现在 Location 头以及后续每个请求的 URI 中。

攻击者能得到什么。 攻击者取消另一个 AF 或 NWDAF 的 VFL 训练运行，或把订阅重定向到自己的 notifUri 和关联值，使消费者不再收到它所订阅的报告。

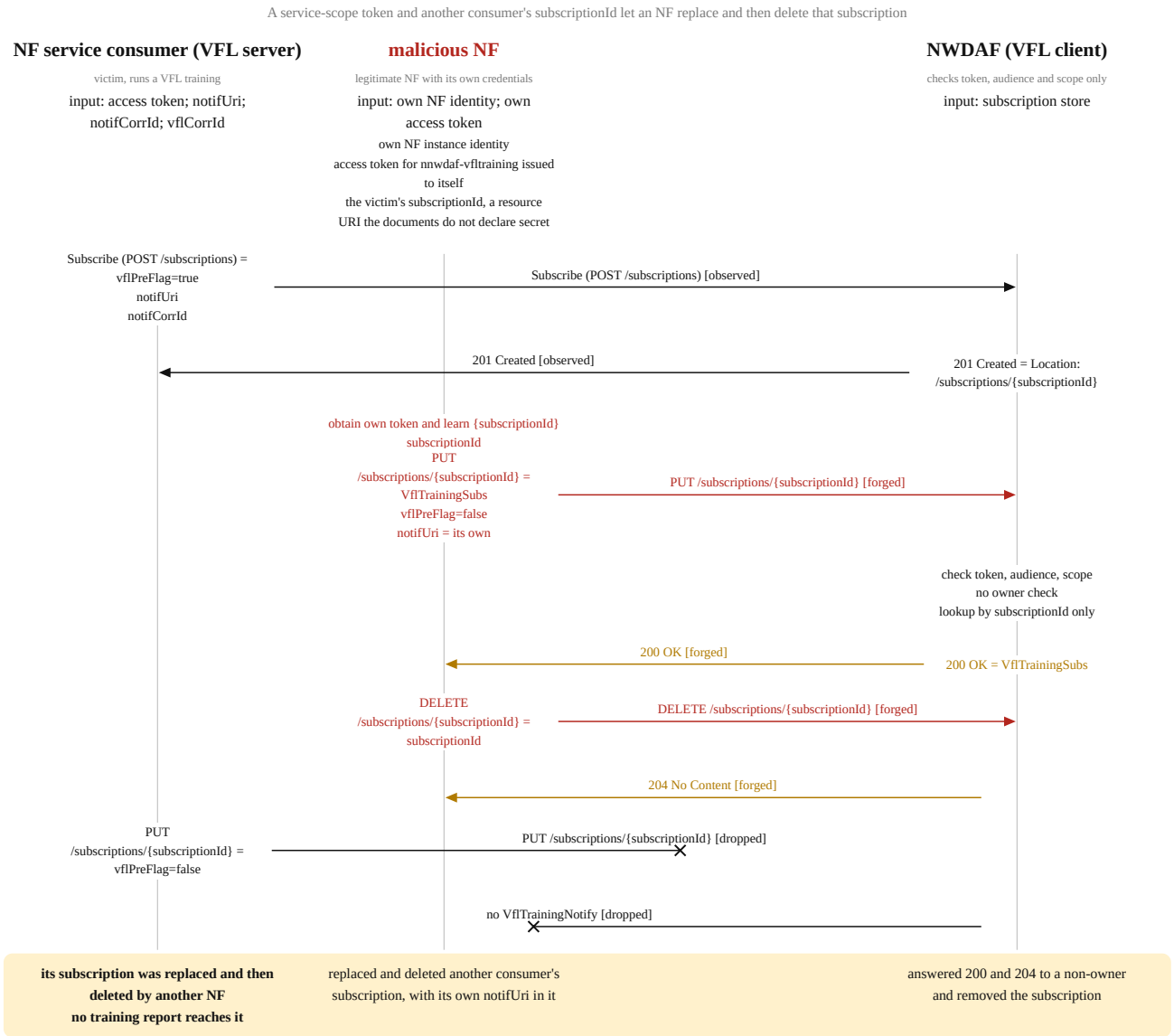


图 2. 服务范围令牌加上另一个消费者的 subscriptionId，使一个 NF 能够替换并随后删除该订阅。性质 Z03；攻击查询 z03_delete、z03_patch、z03_update。

拟议修改。 对于记录的所有者不是所出示访问令牌主体的单个订阅，NWDAF 必须拒绝对其的 PUT、PATCH 或 DELETE，返回 403 Forbidden 且不产生任何副作用；在 4.10.2.2.3、4.10.2.2.4 和 4.10.2.3.2 中写明这一点，并按 TS 29.500 第 6.7.3 条的规定为单个订阅定义资源级范围。在仅添加该检查的模型副本上验证：三个攻击查询变为已验证，正常流程仍能找到，其余已记录的答案不变。

用 ProVerif 复核。 该修改被放入模型副本：对于记录的所有者不是所出示访问令牌主体的单个 VFL 训练订阅，NWDAF 拒绝对其的 PUT、PATCH 或 DELETE；请求返回 403 Forbidden，且不施加任何副作用。在修改后的模型上，ProVerif 证明了 `z03_update`、`z03_delete`、`z03_patch`：该攻击在那里不再可能。协议的正常流程仍能找到。其余已记录的答案中，16 个仍然成立，7 个发生变化：`z01_notify`（Z01，原为无答案）现在为不确定；`x01_notify`（X01，原为无答案）现在为不确定；`x01_notify`（A03，原为无答案）现在为不确定；`a04_create`（A04，原为无答案）现在为不确定；`r02_report`（R02，原为无答案）现在为不确定；`a04_create`（R03，原为无答案）现在为不确定；`r02_report`（U02，原为无答案）现在为不确定。这是对模型的首次检查：它表明该修改在那里消除了此攻击，而非表明它不会引入其他问题。修改后的模型：`records/fixes/0050-fix-owner.pv`。

3 检查过的性质

每一行都是一条交给 ProVerif 的性质。结果是 ProVerif 对分析者所建协议模型给出的答案；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
Z01	**每个操作均由有效令牌覆盖。** 每次订阅创建/修改/删除或通知投递被 NWDAF 或消费者接受时，都必须存在由 NRF 作为授权服务器签发的、覆盖 nnwdaf-vfltraining scope 且未过期的有效授权。	无	无答案	中	不明确
Z03	**订阅绑定至其获授权主体。** 对某个 subscriptionId 的修改/删除，以及对某个 notifCorrId 的通知，只能由该订阅的授权主体在其令牌覆盖的上下文内完成；令牌、subscriptionId 与 notifUri/notifCorrId 不能被移植到其他主体或其他订阅。	无	不成立（3 个攻击）	高	不明确
A03	**消费者与NWDAF基于真实运行行事。** NWDAF 接受订阅创建时，存在消费者以相同身份和相同 VflTrainingSubs 内容发起的真实运行；消费者接受通知时，存在 NWDAF 针对该订阅、相同 notifCorrId 与 reports 的真实通知运行。	无	无答案	中	是
A04	**每次真实运行使用新鲜标识符。** 每次 NWDAF 成功创建订阅（新的 subscriptionId）都对应消费者一次不同的真实订阅运行；每次消费者接受通知都对应 NWDAF 一次不同的真实通知运行。	无	无答案	低	不明确
R02	**每个通知实例仅接受一次。** 同一 notifCorrId 的通知实例至多被消费者接受一次；同一订阅创建请求至多产生一个订阅资源。	无	无答案	低	不明确
R03	**每个逻辑操作仅产生一次副作用。** 同一逻辑订阅创建、订阅删除或通知存储操作在消费者与 NWDAF 之间至多提交一次安全相关副作用。	无	无答案	低	不明确
S05	**已删除的订阅保持删除状态。** 在 DELETE 成功（204）之后，该 subscriptionId 不再接受修改，也不再产生通知；旧订阅上下文不能重新触发这些操作。	无	只确认可达	低	是
S04	**准备、轮次与报告字段一致。** 准备阶段订阅（vflPreFlag=true）在更新为 false 之前不产生通知；检查点恢复使用其引用的迭代号；通知中的 termCause、intermediateRes、vflNotOnTimeInd 至多出现一个，且与前序订阅上下文一致。	无	成立	中	是
A08	**通知值与订阅匹配。** 消费者接受的通知中，event、vflCorrId、iterationNum 与 notifCorrId 必须对应其已创建或修改的订阅中同一组值；NWDAF 接受的订阅参数必须对应消费者真实提议的值。	无	无答案	中	否
K02	**训练数据仅留存于双方。** 中间训练信息、中间结果与样本标识（SUPI/GPSI）只对订阅的消费者和 NWDAF 可见，SCP/SEPP 等中间转发者不能读取其内容。	无	只确认可达	无	不明确
K01	**访问令牌对攻击者保密。** OAuth2 访问令牌只对签发它的 NRF 与获得它的 NF service consumer 可知，攻击者不能推导出可用于访问 Nnwdaf_VFLTraining API 的有效令牌。	无	成立	低	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
U01	**通知关联来自消费者。** 消费者接受的通知中 vflCorrId 与 iterationNum 必须来自该消费者自己提交的订阅。	无	成立	中	否
U02	**训练报告仅接受一次。** 同一训练报告（notifCorrId, vflCorrId, iterationNum）至多被消费者接受一次，不跨会话、不跨轮次。	无	无答案	低	不明确
Q3	**能力检查与训练完成相区分。** 问题涉及能力检查与训练完成的语义区分以及取消后的有限状态一致性。	无	成立	中	是
X01	**SBI交换的相互认证。** NWDAF 仅对来自其已认证对等方 NF 身份的订阅请求行事，NF service consumer 仅接受来自该对等方的通知；任何一方都不会对持有自身凭据的第三方 NF 的消息行事	同一网络中属于它自己的 NF 实例身份，以及 NRF 在运行前签发给它的、用于 nnwdaf-vfltraining scope 的访问令牌	无答案	中	是
X02	**无效请求被拒绝。** NWDAF 拒绝未指明任何现有 subscriptionId 的创建、修改或删除请求，或拒绝不携带令牌、携带过期令牌、或携带面向其他受众或 scope 的令牌的请求，并以错误应答而不是采取行动	同一网络中属于它自己的 NF 实例身份，以及 NRF 在运行前签发给它的、用于 nnwdaf-vfltraining scope 的访问令牌	成立	中	是
X03	**访问令牌不可被其他NF使用。** 泄露给另一个 NF 的访问令牌无法被用来以该令牌签发对象 NF 的名义行事，因为生产者要求令牌主体必须是它在连接上认证的身份	NRF 签发给合法 NF service consumer 的、用于 nnwdaf-vfltraining scope 的访问令牌，但不包含消费者的 TLS 凭据	成立	中	是

文稿写明而起草的清单里没有、由分析者补充的目标（见附录 D）：X01, X02, X03.

The questions asked, and the analyst's answers:

问题	回答	依据
Q1: VFL correlation ID/iteration ID 与参与者身份绑定	在已建模的运行中是：订阅绑定到消费者生成的 vflCorrId 与 notifCorrId，NWDAF 将两者复制到每份报告中，消费者仅在两者都匹配时才接受报告。该绑定仅依赖这些值本身，而不依赖发送者的身份，因为 notify 操作未经令牌授权。	A08, U01, Z03
Q2: 训练报告不会跨会话或跨轮次接受	在此模型上无法定论：每份报告使用新的 notifCorrId 和新的迭代号，使重复在正常流程中不可能发生，但 ProVerif 的复制发送者允许一个创建请求构建两个订阅，因此单射查询无法得出结论，既未主张攻击也未主张证明。	U02, R02, A04
Q3: 能力检查成功不等于训练完成，取消后有限状态一致性	能力检查是一次准备阶段订阅，在订阅被更新为 vflPreFlag false 之前不产生任何报告，因此检查成功并不等于训练完成。删除之后，NWDAF 拒绝通知已删除的订阅，但文稿未说明在途报告是否会被投递，且另一个 NF 可以强制触发该删除，这就是发现。	Q3, S04, S05, Z03

4 本次分析的局限

这里的结果是协议模型上的结果：它说明所规定的消息与检查能给出或不能给出什么，其中密码学被视为理想的，且与任何实现无关。

正如分析者所述，本次分析不覆盖以下内容：

- TLS 被建模为端点之间的私有通道，因此终止连接并可能读取或重新发起消息的中继未被建模；TS 33.501 5.9.2.4 规定所有参与方都必须信任 SCP。
- 订阅存储是单调的：删除被记录为一个标记，不移除任何内容，因此无法确定一个请求的副作用计数以及删除前后在途报告的命运。

- notifUri 是每个订阅的私有通道，因此第三方向消费者回调 URI 发送伪造 notify 请求的情况未被建模；消费者在此的唯一保护是 notifCorrId 与 vflCorrId 的保密性和检查，而规范并未要求它们不可猜测。
- 令牌过期未被建模，因此授权目标中未过期这一部分未被测试。
- 训练本身以及不透明字段 intermedTrainInfo、interopInfo、vflFeatIds 和 accuMonInfo 未被分析；收敛性、抗投毒鲁棒性和差分隐私超出了符号模型的范围。
- SUPI 与 GPSI 样本标识的订户隐私超出任务范围。
- 模型是符号性的：它不说明 TLS、令牌格式或 HTTP/2 传输的计算强度。

宿主记录的内容：

- 无答案的有：Z01, A03, A04, R02, R03, S05, A08, K02, U02, X01。
- 解读写完之后答案发生变化的有：A08, X01。
- 证明器没有给出结论的查询（附录 C）：Z01: z01_notify, A03: x01_notify, A04: a04_create, R02: r02_report, R03: a04_create, A08: a08_notify, U02: r02_report, X01: x01_notify。这条性质问过了，证明器既没有证明它也没有找到攻击，所以结果写“无答案”。
- 分析者为性质设定了攻击者条件，但既没有证明也没有攻击的（附录 D）：S05 在 `network` 下; S05 在 `nf_scope_resource_uri` 下; K02 在 `network` 下; K02 在 `nf_scope_resource_uri` 下。
- 没带对照查询的证明（附录 C）：Z01: z01_create, Z01: z01_update, Z01: z01_delete, Z03: x02_foreign, A03: z01_create, S04: s04_preflag, A08: z03_notify, K01: k01, U01: z03_notify, Q3: s04_preflag, X01: z01_create, X01: x01_request_c, X02: x02_foreign, X03: x02_foreign。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。

每条性质还有哪些问题悬而未决、什么能解决它，见附录 A。

附录 A：逐条性质的解读

以下是分析者自己对证明器答案的解读，而非证明器的回答：这些答案对协议意味着什么、解读依据是什么、能否按现状使用，以及它的价值几何。

Z01: 每个操作均由有效令牌覆盖

每次订阅创建/修改/删除或通知投递被 NWDAF 或消费者接受时，都必须存在由 NRF 作为授权服务器签发的、覆盖 nnwdaf-vfltraining scope 且未过期的有效授权。

NWDAF 仅对其能够针对自身 NF 类型和 nnwdaf-vfltraining scope 验证令牌、且令牌主体是它在连接上认证的 NF 的请求行事，因此每一次被接受的创建、修改和删除都有 NRF 签发的令牌作为支撑。通知投递是基线刻意留作无令牌的操作，因此该主张的这一半按设计就不成立，证明器也无法判定它。

- 结果：无答案；回答了所问：部分；可带保留地使用
- 价值中：证明表明生产者执行了基线要求的检查，这并非新结果；通知这一半是有文档记载的设计选择，而非弱点。
- 文稿是否已写：不明确
- 依据：TS 29.500 第 6.7.3 条是唯一被建模的授权规则；令牌是不透明的，只有 NRF 能铸造它，因此其格式、声明和过期未被分析。；notify 操作按 TS 29.500 第 6.7.3 条的规定被建模为无令牌。
- 待解决：可预测的 notifCorrId，或不检查它的消费者，是否会让第三方注入报告
- 下一步：将回调建模为带逐连接加密的公开端点，并使用可猜测的 notifCorrId。

Z03: 订阅绑定至其获授权主体

对某个 subscriptionId 的修改/删除，以及对某个 notifCorrId 的通知，只能由该订阅的授权主体在其令牌覆盖的上下文内完成；令牌、subscriptionId 与 notifUri/notifCorrId 不能被移植到其他主体或其他订阅。

令牌的主体绑定被强制执行：签发给一个 NF 的令牌不能被用来以另一个 NF 的名义行事，因为生产者要求令牌主体等于它在连接上认证的身份。资源所有权未被强制执行：持有自己有效令牌的 NF 可以替换、修补或删除它知道 URI 的任何订阅，而 NWDAF 的应答与对所有者无异。

- 结果：不成立（3 个攻击）；回答了所问：是；可用
- 价值 高：文稿陈述了使该攻击成为可能的范围模型，但从未陈述该失败。
- 文稿中是否陈述：不明确
- 依据：假定攻击者知道受害者的 subscriptionId；文稿既未声明其为机密，也未要求其不可猜测。；producer 完全按照操作条款的描述建模，包含 token、audience 与 scope 检查以及按 subscriptionId 的查找，且不含所有权检查，因为没有任何条款陈述该检查。；TLS 为每个 NF 提供各自经过认证的连接，身份检查通过请求到达的连接来建模。
- 待定：是否期望运维人员为此 API 配置资源级 scope
- 下一步：检查一项拟议修改，该修改增加资源级 scope 并对单个 subscription 进行所有者检查。

A03: 消费者与NWDAF基于真实运行行事

NWDAF 接受订阅创建时，存在消费者以相同身份和相同 VflTrainingSubs 内容发起的真实运行；消费者接受通知时，存在 NWDAF 针对该订阅、相同 notifCorrId 与 reports 的真实通知运行。

创建这一半成立：NWDAF 仅将验证过 token 的身份记录为所有者，因此没有其他 NF 能以消费者的身份创建订阅。通知这一半无法判定：证明器既不能证明也不能证伪被接受的上报是由 NWDAF 针对该订阅发送的。

- 结果：无答案；回答了所问：部分；带保留可用
- 价值 中：TS 33.501 第 5.9.2.1 条要求 consumer 与 producer 之间进行双向认证，这正是创建这一半所展示的内容。
- 文稿中是否陈述：是。文稿中的位置：ts-33-501:2871
- 依据：双向认证取自 TLS，并建模为携带对端身份的连接。；关于通知发送方的一致性未判定。
- 待定：关于通知发送方的一致性
- 下一步：将每个通知绑定到一个复制后的发送方无法共享的会话值，并询问单射形式。

A04: 每次真实运行使用新鲜标识符

每次 NWDAF 成功创建订阅（新的 subscriptionId）都对应消费者一次不同的真实订阅运行；每次消费者接受通知都对应 NWDAF 一次不同的真实通知运行。

单射对应关系无法判定：证明器通过复制后的处理器的两个副本，由单个创建请求构建出一个订阅，这一过近似阻断了查询。

- 结果：无答案；回答了所问：否；不可用
- 价值 低：未判定的答案来自复制抽象，而非协议本身。
- 文稿中是否陈述：不明确
- 依据：subscriptionId 来自每次请求的新鲜值，但复制后的处理器在抽象中仍允许一个请求产生两个订阅。
- 待定：重试的 POST 是否会创建两个订阅，文稿未讨论这一点
- 下一步：用幂等键对创建建模，并再次询问单射查询。

R02: 每个通知实例仅接受一次

同一 notifCorrId 的通知实例至多被消费者接受一次；同一订阅创建请求至多产生一个订阅资源。

通知实例的唯一性因同样的抽象原因无法判定：复制后的发送方与重复的订阅使证明器能够两次到达同一份上报。

- 结果：无答案；回答了所问：否；不可用
- 价值 低：该答案关乎模型的多重性，而非协议。
- 文稿中是否陈述：不明确
- 依据：未对重试或去重规则建模，因为文稿没有定义任何此类规则。
- 待定：NWDAF 是否会对 204 丢失的通知进行重试
- 下一步：将通知交互展开为每轮一份上报，并在那里询问单射查询。

R03: 每个逻辑操作仅产生一次副作用

同一逻辑订阅创建、订阅删除或通知存储操作在消费者与 NWDAF 之间至多提交一次安全相关副作用。

每个逻辑操作的安全相关副作用计数无法判定；模型允许一个创建请求被复制后的处理器消费两次。

- 结果：无答案；回答了所问：否；不可用
- 价值 低：该答案不能对协议给出任何可靠结论。

- 文稿中是否陈述：不明确
- 依据：存储是单调的，且请求处理器是复制的，因此多重性被过近似。
- 待定：POST 与 DELETE 的重试语义
- 下一步：为每个新鲜会话值建模一个逻辑操作，并统计其副作用。

S05: 已删除的订阅保持删除状态

在 DELETE 成功（204）之后，该 subscriptionId 不再接受修改，也不再产生通知；旧订阅上下文不能重新触发这些操作。

该情形可到达：订阅被删除后，NWDAF 被要求对其发送通知并拒绝，因为它记录了已删除的 subscriptionId 并在每次上报前检查它。对于删除到达时已在途的上报，没有给出任何结论，且该发现表明另一 NF 可以促成该删除。

- 结果：仅可到达；回答了所问：部分；带保留可用
- 价值 低：TS 29.520 第 4.10.2.3.2 条规定 DELETE 被接受时订阅即被移除，这正是所到达情形检查的内容。
- 文稿中是否陈述：是。文稿中的位置：main:32691
- 依据：删除标记是单调的：模型记录删除，但无法移除条目。；在途上报未被建模为丢失，因此删除之后它们的投递未定。
- 待定：在途上报能否在删除后存活
- 下一步：将删除建模为移除条目，加入一个在途上报，并询问消费者是否会接受它。

S04: 准备、轮次与报告字段一致

准备阶段订阅（vflPreFlag=true）在更新为 false 之前不产生通知；检查点恢复使用其引用的迭代号；通知中的 termCause、intermediateRes、vflNotOnTimeInd 至多出现一个，且与前序订阅上下文一致。

准备订阅在更新为 vflPreFlag false 之前从不产生上报，而直接创建为训练订阅的订阅会立即通知。三个报告字段的互斥性是一条静态良构规则，在本模型中任何迹都无法违反。

- 结果：成立；回答了所问：是；带保留可用
- 价值 中：VflTrainingSubs 表中的 NOTE 恰好陈述了证明所检查的规则。
- 文稿中是否陈述：是。文稿中的位置：main:32691
- 依据：通知前检查 vflPreFlag 为 false 的代码写在 NWDAF 中，正如数据类型 NOTE 所要求。；按构造，上报被建模为恰好携带三个可选字段之一。
- 下一步：标志无需下一步；字段互斥性需要对报文体而非迹建模。

A08: 通知值与订阅匹配

消费者接受的通知中，event、vflCorrId、iterationNum 与 notifCorrId 必须对应其已创建或修改的订阅中同一组值；NWDAF 接受的订阅参数必须对应消费者真实提议的值。

本目标的答案在本解读撰写之后发生了变化。

被接受的上报属于消费者自己创建并更新为训练状态的订阅，其 event、vflCorrId、notifCorrId 与迭代号均来自该订阅，因为只有当消费者自己选择的值匹配时它才会接受上报。关于 NWDAF 确实发送了该上报的一致性无法判定。

- 结果：无答案；回答了所问：部分；带保留可用

- 价值 中：我在安全条款和数据模型中查找 vflCorrId 的绑定规则，未找到；文稿只定义了该字段，因此消费者自身检查是唯一绑定这一事实未被陈述。
- 文稿中是否陈述：否
- 依据：消费者对 notifCorrId 与 vflCorrId 的检查就是保护；模型只将这两个值交给消费者。；关于上报发送方的一致性未判定。
- 待定：关于通知发送方的一致性
- 下一步：如 A03 那样在模型中将通知绑定到会话。

K02: 训练数据仅留存于双方

中间训练信息、中间结果与样本标识（SUPI/GPSI）只对订阅的消费者和 NWDAF 可见，SCP/SEPP 等中间转发者不能读取其内容。

模型仅表明恶意 NF 会收到它自己创建并更新的订阅的结果，这是 API 设计上允许的；消费者自己的上报留在其 TLS 回调上，因为攻击者无法提供消费者的 notifCorrId 或 vflCorrId。所记录的攻击是查询的产物，并未表明消费者训练数据对另一 NF 的机密性会失效。

- 结果：仅可到达；回答了所问：否；不可用
- 价值 无：该攻击迹是攻击者自己的订阅，对协议的机密性没有任何说明。
- 文稿中是否陈述：不明确
- 依据：回调被建模为只有订阅者可读的通道，这在机密性上强于 TLS。；终止 TLS 的转发者未被建模，因此对 SCP 或 SEPP 读取上报没有任何结论。
- 待定：转发者能否读取通知，以及 Z03 的劫持是否能让攻击者获得消费者的上报
- 下一步：将回调建模为任何 NF 都可到达的公开端点，并再次询问机密性查询。

K01: 访问令牌对攻击者保密

OAuth2 访问令牌只对签发它的 NRF 与获得它的 NF service consumer 可知，攻击者不能推导出可用于访问 Nnwdaf_VFLTraining API 的有效令牌。

网络上的攻击者永远无法获知消费者的访问令牌：令牌只在其两个持有端点的连接上传输，恶意 NF 持有的令牌是它自己的。

- 结果：成立；回答所问：是；可用但有保留
- 价值低：RFC 6749 第 10.3 条要求访问令牌在传输和存储中保密。
- 文稿中已说明：是。文稿中说明位置：rfc6749:2859
- 依据：令牌是不透明的，只有 NRF 能创建它们；其格式、签名和有效期未建模。；TLS 被建模为私有信道，因此传输中的保密性是假设而非证明。
- 下一步：无。

U01: 通知关联来自消费者

消费者接受的通知中 vflCorrId 与 iterationNum 必须来自该消费者自己提交的订阅。

已接受报告的 vflCorrId 和迭代编号来自消费者自己的订阅：消费者插入一个新的 vflCorrId，并且只有当同一值返回时才接受报告，因此关于其他订阅的报告不会被接受。

- 结果：成立；回答所问：是；可用但有保留
- 价值中：数据模型将 vflCorrId 定义为关联值，但未说明生成或绑定规则，安全条款也未提及它。

- 文稿中已说明：否
- 依据：消费者检查自己的 vflCorrId 和 notifCorrId；文稿不要求该检查，只定义了字段。；vflCorrId 被视为消费者选择并对其余 NF 保密的值。
- 未决：跨订阅复用一个 vflCorrId 的消费者是否仍受保护
- 下一步：建模一个复用同一 vflCorrId 的消费者，并再次询问一致性。

U02: 训练报告仅接受一次

同一训练报告（notifCorrId, vflCorrId, iterationNum）至多被消费者接受一次，不跨会话、不跨轮次。

训练报告跨会话和轮次的唯一性无法判定；复制的发送者和重复的订阅使证明器两次到达同一报告。

- 结果：无答案；回答所问：否；不可用
- 价值低：答案来自模型的多重性，而非协议本身。
- 文稿中已说明：不明确
- 依据：模型在建模运行中每个订阅只发送一份报告，因此答案主要受复制抽象影响。
- 未决：当迭代编号重复时，两轮的报报告是否可能混淆
- 下一步：展开两个具有不同迭代编号的轮次，并在那里询问单射查询。

Q3: 能力检查与训练完成相区分

问题涉及能力检查与训练完成的语义区分以及取消后的有限状态一致性。

成功的能力检查是准备订阅，在消费者将 vflPreFlag 更新为 false 之前不产生报告，因此该检查不会被误认为训练完成；删除后，NWDAF 拒绝通知已删除的订阅。文稿未定义进一步的状态机，且另一个 NF 可以强制触发删除。

- 结果：成立；回答所问：是；可用但有保留
- 价值中：能力检查的目的在 4.10.1.1 和 4.10.2.2.1 中说明，不通知规则在 VflTrainingSubs NOTE 中说明。
- 文稿中已说明：是。文稿中说明位置：main:32691
- 依据：建模的唯一状态规则是 vflPreFlag NOTE 和删除标记。；模型将训练限制为一份报告，且未建模检查点恢复。
- 未决：检查点恢复，以及恢复的轮次是否可能以过时的迭代编号报告
- 下一步：建模 chkPoint 和 resIterNum，并询问恢复的轮次。

X01: SBI交换的相互认证

the NWDAF acts on a subscription request only from a peer whose NF identity it has authenticated, and the NF service consumer accepts a notification only from that peer; neither party acts on a message of a third NF that holds its own credentials

本目标的答案在此解读撰写后发生了变化。

NWDAF 只对来自其对等方的请求采取行动，该对等方的身份已经过认证且所出示令牌是签发给它的，因此第三方 NF 无法以另一个 NF 的身份驱动它。对消费者而言，相应的约定——它只接受来自其所订阅的 NWDAF 的通知——无法判定。

- 结果：无答案；回答所问：部分；可用但有保留
- 价值中：TS 33.501 第 5.9.2.1 条是请求方向所示的要求。
- 文稿中已说明：是。文稿中说明位置：ts-33-501:2871

- 依据：相互认证取自 TLS 并建模为连接身份。；通知侧未决。
- 未决：通知方向
- 下一步：将回调建模为公共端点，并询问是否接受来自另一个 NF 的报告。

X02: 无效请求被拒绝

the NWDAF refuses a create, modify or delete request that names no existing subscriptionId, or that carries no token, an expired token, or a token for another audience or scope, and answers with an error instead of acting

NWDAF 从不对令牌主体与其已认证身份不同的请求采取行动，因此以自己令牌声称另一个 NF 身份的请求会被拒绝；命名不存在的 subscriptionId 的请求永远不会匹配存储。

- 结果：成立；回答所问：是；可用但有保留
- 价值中：TS 33.501 第 5.9.2.1 条要求每个 NF 验证传入消息，TS 29.500 第 6.7.3 条要求令牌检查。
- 文稿中已说明：是。文稿中说明位置：ts-33-501:2875
- 依据：未知订阅的情况是结构性的：查找无法匹配且进程停止，ProVerif 将其建模为无应答的拒绝。；令牌过期未建模。
- 未决：对拒绝请求的错误应答，模型不产生该应答
- 下一步：建模 401 和 403 应答，并检查拒绝不会泄露哪个检查失败。

X03: 访问令牌不可被其他NF使用

an access token that leaked to another NF cannot be used to act in the name of the NF it was issued to, because the producer requires the token subject to be the identity it authenticated on the connection

泄露给另一个 NF 的访问令牌不能用于以签发它的 NF 的名义行事，因为 NWDAF 要求令牌主体是其在连接上认证的身份；攻击者保留令牌，但没有以所有者身份建立的连接。

- 结果：成立；回答所问：是；可用但有保留
- 价值中：TS 29.500 第 6.7.5 条要求当主体声明与客户端凭据断言不匹配时返回 403，模型展示了等效检查。
- 文稿中已说明：是。文稿中说明位置：ts-29-500:5068
- 依据：模型只给泄露令牌的攻击者令牌，而不给消费者的 TLS 凭据，这正是 RFC 6749 10.3 和 TS 29.500 6.7.5 所假设的。；主体声明检查在 NWDAF 中建模为比较。
- 未决：NF 的 TLS 凭据也泄露的情况，不在攻击者集合内
- 下一步：添加一个同时持有令牌和客户端凭据的攻击者。

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，以及攻击及分析者对每项攻击的裁定。

目标	级别	界	查询	对照	攻击	主张
Z01	proved		z01_create			4 proved, 1 undecided
Z03	proved		x02_foreign		z03_update (holds_in_source); z03_delete (holds_in_source); z03_patch (holds_in_source)	2 proved, 3 attack
A03	proved		z01_create			1 proved, 1 undecided
A04	none					1 undecided
R02	none					1 undecided
R03	none					1 undecided
S05	reachable		s05_delete			3 reachable
S04	proved		s04_preflag			1 proved
A08	proved		z03_notify			1 proved, 1 undecided
K02	reachable		k02_reach		k02_result (model_artifact)	2 reachable, 1 attack
K01	proved		k01			1 proved
U01	proved		z03_notify			1 proved
U02	none					1 undecided
Q3	proved		s04_preflag			1 proved
X01	proved		z01_create			3 proved, 1 undecided
X02	proved		x02_foreign			2 proved
X03	proved		x02_foreign			1 proved

逐条主张，按分析者对每条主张的措辞；每条主张的答案是证明器的：

目标	主张	攻击者	回答	查询	对照
Z01	NWDAF 接受的每次订阅创建（AcceptedCreate）都有 NRF 签发给其所记录主体的令牌作为依据；攻击者持有自己的 NF 身份和面向 nnwdaf-vfltraining scope 的自己的令牌	`nf_service_scope`	proved	z01_create	none
Z01	NWDAF 接受的每次修改（PUT/PATCH）都有 NRF 签发的、面向该服务 scope 的令牌作为依据，并由其所指明的主体出示	`nf_service_scope`	proved	z01_update	none
Z01	NWDAF 接受的每次删除都有 NRF 签发的、面向该服务 scope 的令牌作为依据，并由其所指明的主体出示	`nf_service_scope`	proved	z01_delete	none

目标	主张	攻击者	回答	查询	对照
Z01	消费者接受的每次通知投递都由有效令牌授权：notify 操作不携带令牌（TS 29.500 第 6.7.3 条），因此能问的是：所接受的报告是由 NWDAF 为消费者自己的订阅投递的	`nf_service_scope`	undecided	z01_notify	
Z01	NWDAF 接受的每次订阅创建都有 NRF 签发给其所记录主体的令牌作为依据，在面对仅位于网络上的攻击者时也成立	`network`	proved	z01_create	none
Z03	只有订阅所属的主体才能修改它：对另一个 NF 的 subscriptionId 发起完整 PUT 会被接受	`nf_scope_resource_uri`	attack (holds_in_source)	z03_update	
Z03	只有订阅所属的主体才能删除它：对另一个 NF 的 subscriptionId 发起 DELETE 会被接受	`nf_scope_resource_uri`	attack (holds_in_source)	z03_delete	
Z03	只有订阅所属的主体才能部分修改它：对另一个 NF 的 subscriptionId 发起 PATCH 会被接受	`nf_scope_resource_uri`	attack (holds_in_source)	z03_patch	
Z03	签发给一个 NF 的令牌不能被用来冒充另一个 NF：生产者会拒绝主体声明与已认证对端不一致的请求	`nf_scope_resource_uri`	proved	x02_foreign	none
Z03	签发给一个 NF 的令牌不能被用来冒充另一个 NF；在面对仅位于网络上的攻击者时，生产者也会拒绝主体声明与已认证对端不一致的请求	`network`	proved	x02_foreign	none
A03	NWDAF 将消费者用于认证的身份记录为所创建订阅的所有者，因此第三方无法以消费者的身份创建订阅	`network`	proved	z01_create	none
A03	所接受的通知是由 NWDAF 为该订阅发送的，且 notifCorrId 和报告均相同	`network`	undecided	x01_notify	
A04	每次以新 subscriptionId 被接受的创建都对应消费者一次不同的真实订阅运行	`network`	undecided	a04_create	
R02	一个通知实例（notifCorrId、vflCorrId、迭代编号）最多被接受一次	`network`	undecided	r02_report	
R03	一次逻辑上的创建、删除或通知在对方最多产生一个与安全相关的副作用	`network`	undecided	a04_create	
S05	消费者的订阅被删除后，NWDAF 被要求向其发送通知并拒绝（达到了目标所述的情形）	`network`	reachable	s05_delete	
S05	订阅被删除后，NWDAF 被要求向其发送通知并拒绝（在删除消费者自己的订阅的情形下达到该情形）	`network`	reachable	s05_delete	
S05	订阅被删除后，NWDAF 被要求向其发送通知并拒绝；当另一个持有该服务 scope 和该订阅 URI 的 NF 执行删除时也成立	`nf_scope_resource_uri`	reachable	s05_delete	
S04	准备订阅（vflPreFlag=true）在被更新为 vflPreFlag=false 之前不产生报告	`network`	proved	s04_preflag	none
A08	被接受的通知属于消费者自己创建并更新为训练状态的订阅，因此事件、vflCorrId、notifCorrId 和迭代编号都来自其自己的订阅	`network`	proved	z03_notify	none
A08	只有当消费者已将订阅更新为训练状态时，报告才会被接受，因此报告与其订阅上下文一致	`network`	undecided	a08_notify	
K02	中间训练结果只有消费者和 NWDAF 知道：一个订阅的结果绝不会到达另一个 NF	`nf_scope_resource_uri`	attack (model_artifact)	k02_result	

目标	主张	攻击者	回答	查询	对照
K02	达到了该主张所保护的情形：为某个订阅产生训练结果并投递给其订阅者	`network`	reachable	k02_reach	
K02	达到了该主张所保护的情形：为消费者拥有的某个订阅产生训练结果并投递给该订阅者	`nf_scope_resource_uri`	reachable	k02_reach	
K01	网络上的攻击者不知道消费者的访问令牌	`network`	proved	k01	none
U01	被接受通知的 vflCorrId 和迭代编号来自消费者自己的订阅	`network`	proved	z03_notify	none
U02	一个训练报告（notifCorrId、vflCorrId、迭代编号）最多被接受一次，不会跨会话或跨轮次重复	`network`	undecided	r02_report	
Q3	成功的能力检查（准备订阅）不等于训练完成：在订阅被更新之前它不产生报告	`network`	proved	s04_preflag	none
X01	NWDAF 只将这样的身份记录为新订阅的所有者：其令牌被提供给 NWDAF，且该身份是 NWDAF 在连接上认证的身份（AcceptedCreate 携带 NRF 签发的主体）	`network`	proved	z01_create	none
X01	消费者接受的每次通知（GotReport）都是由 NWDAF 为该订阅发送的（SentReport 具有相同的 subscriptionId 和迭代编号）	`network`	undecided	x01_notify	
X01	NWDAF 只将这样的身份记录为所有者：其令牌已被 NWDAF 验证，因此恶意 NF 无法以另一个 NF 的身份创建订阅	`nf_service_scope`	proved	z01_create	none
X01	NWDAF 以消费者身份接受的每次创建都对应消费者自己发送的一次创建请求	`network`	proved	x01_request_c	none
X02	令牌主体与连接上认证的身份不一致的请求不会被处理（ForeignIdentity 事件永远不会被到达）	`nf_service_scope`	proved	x02_foreign	none
X02	令牌主体与连接上认证的身份不一致的请求不会被处理，在面对仅位于网络上的攻击者时也成立	`network`	proved	x02_foreign	none
X03	指明某个订阅但携带另一个 NF 访问令牌的请求会被拒绝：生产者要求令牌主体等于连接上认证的身份（ForeignIdentity 不可达）	`nf_token_leaked`	proved	x02_foreign	none

附录 D：分析是怎么跑的

一名 LLM 分析者根据文稿构建协议模型，并将每个性质提交给 ProVerif；第 3 节中的每个结果都是证明器给出的回答。

ProVerif+ Agent 会话 session-20261114T221340，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：58，证明器 9 s，实际耗时 16 min，成本 0.168 USD。

上下文：宿主从对话中移除了过时部分 1 次，共 473732 个字符（较早的推理，以及展示模型在最新修改之前状态的内容）。轨迹文件保留了全部内容。

ProVerif：运行了 119 个证明，94 个有结论，25 个无答案，5 s，记录了 27 个回答。

分析了什么

协议	NWDAF VFL client training API
版本	19.8.0
分析范围	一个可信 AF/NWDAF VFL server 与一个 NWDAF VFL client；一次 capability check、订阅、一个有界训练轮次报告与取消；原始 feature/gradient 为 opaque，不能证明机器学习收敛、投毒鲁棒性或差分隐私。
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。
原文	来自下列章节的 293 个编号原文单元（68550 字节）。本报告中的 s0001 这类引用就是这些原文单元之一

分析所依据的文稿章节：

文稿	章节	标题
main	4.10	Nnwdaf_VFLTraining Service
main	4.10.1	服务描述
main	4.10.1.1	概述
main	4.10.1.2	服务架构
main	4.10.1.3	网络功能
main	4.10.1.3.1	网络数据分析功能（NWDAF）
main	4.10.1.3.2	NF 服务消费者
main	4.10.2	服务操作
main	4.10.2.1	引言
main	4.10.2.2	Nnwdaf_VFLTraining_Subscribe 服务操作
main	4.10.2.2.1	概述
main	4.10.2.2.2	订阅 VFL 训练信息
main	4.10.2.2.3	更新 VFL 训练信息的订阅

文稿	章节	标题
main	4.10.2.2.4	部分更新 VFL 训练信息的订阅
main	4.10.2.3	Nnwdaf_VFLTraining_Unsubscribe 服务操作
main	4.10.2.3.1	概述
main	4.10.2.3.2	取消订阅 VFL 训练信息
main	4.10.2.4	Nnwdaf_VFLTraining_Notify 服务操作
main	4.10.2.4.1	概述
main	4.10.2.4.2	关于 VFL 训练信息的通知
main	5.9	Nnwdaf_VFLTraining Service API
main	5.9.1	引言
main	5.9.2	HTTP 的使用
main	5.9.2.1	概述
main	5.9.2.2	HTTP 标准标头
main	5.9.2.2.1	概述
main	5.9.2.2.2	内容类型
main	5.9.2.3	HTTP 自定义标头
main	5.9.3	资源
main	5.9.3.1	概述
main	5.9.3.2	资源：VFL 训练订阅
main	5.9.3.2.1	描述
main	5.9.3.2.2	资源定义
main	5.9.3.2.3	资源标准方法
main	5.9.3.2.3.1	POST
main	5.9.3.2.4	资源自定义操作
main	5.9.3.3	资源：单个 VFL 训练订阅
main	5.9.3.3.1	描述
main	5.9.3.3.2	资源定义
main	5.9.3.3.3	资源标准方法
main	5.9.3.3.3.1	PUT
main	5.9.3.3.3.2	DELETE
main	5.9.3.3.3.3	GET
main	5.9.3.3.3.4	PATCH
main	5.9.3.3.4	资源自定义操作
main	5.9.4	无关联资源的自定义操作
main	5.9.5	通知
main	5.9.5.1	概述
main	5.9.5.2	VFL 训练通知

文稿	章节	标题
main	5.9.5.2.1	描述
main	5.9.5.2.2	目标 URI
main	5.9.5.2.3	标准方法
main	5.9.5.2.3.1	POST
main	5.9.6	数据模型
main	5.9.6.1	概述
main	5.9.6.2	结构化数据类型
main	5.9.6.2.1	引言
main	5.9.6.2.2	类型 VflTrainingSubs
main	5.9.6.2.3	类型 VflTrainingSub
main	5.9.6.2.4	类型 VflCheckpointInfo
main	5.9.6.2.5	类型 VflInteropInfo
main	5.9.6.2.6	类型 VflTrainingNotify
main	5.9.6.2.7	类型 VflIntermedTrainInfo
main	5.9.6.2.8	类型 VflTrainingSubsPatch
main	5.9.6.2.9	类型：VflTrainingReport
main	5.9.6.2.10	类型：VflSampleId
main	5.9.7	错误处理
main	5.9.7.1	概述
main	5.9.7.2	协议错误
main	5.9.7.3	应用错误
main	5.9.8	特性协商
main	5.9.9	安全

原文单元在文稿中给出的协议目的：一个可信 AF/NWDAF VFL server 与一个 NWDAF VFL client；一次 capability check、订阅、一个有界训练轮次报告与取消；原始 feature/gradient 为 opaque，不能证明机器学习收敛、投毒鲁棒性或差分隐私。

对照文稿定性质

在编写查询之前，分析者已把草拟的性质清单与文稿自身对协议目的的表述作了对照。名称、性质所涉及的内容以及文稿的表述均属分析者的解读；所提及的位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
Z01	每个操作均由有效令牌覆盖	NWDAF 作为 NF 服务生产者：它接受的每次订阅创建、修改或删除，都由 NRF 签发的访问令牌背书，令牌针对 nnwdaf-vfltraining 范围且未过期；通知投递是基线未附带令牌的操作	TS 29.520 5.9.9 指出，对 API 的访问可以使用 OAuth2 客户端凭据授权，NRF 作为授权服务器；TS 29.500 6.7.3 要求 NF 服务在允许访问所请求资源之前，验证令牌、其有效期及其访问范围，并指出 notify 操作不使用 OAuth2 令牌。	ts-29-500:4994, ts-29-500:5032, s0290, s0291, s0293
Z03	订阅绑定至其获授权主体	NWDAF：对某个 subscriptionId 的修改、删除和通知，仅保留给该订阅所属的主体，且在其令牌覆盖的上下文内；令牌、subscriptionId 或关联标识符不可移植到另一主体或另一订阅	TS 29.520 5.9.9 为整个服务定义一个范围，不定义资源级或操作级范围；TS 29.500 6.7.3 指出服务范围授予对 API 的通用访问权限，而资源级/操作级范围用于需要特定授权的操作。服务操作条款未规定检查请求者是否拥有该订阅。	ts-29-500:4996, ts-29-501:1795, s0042, s0072, s0085, s0143, s0293
A03	消费者与NWDAF基于真实运行行事	NWDAF 在接受订阅创建时，以及 NF 服务消费者在接受通知时：所接受的值对应于另一方的真实运行	TS 29.520 4.10.2.2.2 和 4.10.2.4.2 描述了请求和通知；TS 33.501 5.9.2.1 要求消费者与生产者之间的直接通信进行相互认证，并要求每个 NF 验证所有传入消息。	ts-33-501:2871, s0036, s0042, s0085, s0086
A04	每次真实运行使用新鲜标识符	NWDAF 的 subscriptionId 以及消费者对通知的接受：各自对应于另一方的不同运行	TS 29.520 4.10.2.2.2 规定 NWDAF 分配 subscriptionId 并存储订阅；4.10.2.4.2 规定消费者存储通知并应答 204；TS 33.501 5.9.2.1 要求 SBI 上的重放保护。	ts-33-501:2865, s0038, s0039, s0040, s0085, s0086
R02	每个通知实例仅接受一次	NF 服务消费者：具有一个 notifCorrId 和一组报告的 notification 实例最多被接受一次	TS 29.520 5.9.5.2.3.1 和 4.10.2.4.2 未给出去重或重放窗口规则；该性质依赖关联标识符。	ts-33-501:2915, s0085, s0086, s0262
R03	每个逻辑操作仅产生一次副作用	NWDAF 的订阅存储和消费者存储的通知：一次逻辑创建、删除或通知最多产生一个安全相关的副作用	TS 29.520 4.10.2.2.2（创建、分配 subscriptionId、存储）、4.10.2.3.2（移除订阅、应答 204）、4.10.2.4.2（存储通知、应答 204）；未定义重试语义。	s0038, s0039, s0040, s0073, s0074, s0086
S05	已删除的订阅保持删除状态	NWDAF：在成功 DELETE（204）之后，subscriptionId 不接受修改，也不产生通知；旧的订阅上下文不能重新触发它们	TS 29.520 4.10.2.3.2：在接受时，NWDAF 移除订阅并应答 204。未提及在途通知或标识符重用。	s0073, s0074, s0075

ID	简称	对象	文稿怎么说	出处
S04	准备、轮次与报告字段一致	NWDAF 和消费者：准备订阅（vflPreFlag=true）在被更新为 false 之前不产生通知；报告最多携带 intermediateRes、termCause、vflNotOnTimeInd 之一，与订阅上下文一致	TS 29.520 5.9.6.2.2 NOTE：当 vflPreFlag=true 时，生产者在订阅更新为 vflPreFlag=false 且 POST 响应中缺少 trainReports 之前不发送通知；5.9.6.2.9 NOTE 1：仅提供 intermediateRes、termCause、vflNotOnTimeInd 之一。	main:32691, s0250, s0271
A08	通知值与订阅匹配	NF 服务消费者：已接受通知中的 event、vflCorrId、iterationNum 和 notifCorrId 与其自身订阅的值相对应；NWDAF 接受了消费者提议的值	TS 29.520 5.9.6.2.3 和 5.9.6.2.9 定义了相关属性；4.10.2.4.2 规定 NWDAF 使用 notifUri，报告携带 notifCorrId。未给出 vflCorrId 的生成或绑定规则。	s0253, s0262, s0271, s0085
K02	训练数据仅留存于双方	NF 服务消费者和 NWDAF：中间训练信息、中间结果和样本标识符（SUPI/GPSI）只能由它们读取，其他 NF 和中继均不可读取	TS 29.520 5.9.6.2.7 和 5.9.6.2.9 携带中间结果，5.9.6.2.10 携带 SUPI/GPSI；TS 33.501 5.9.2.4 要求 SCP 与 NF 之间的机密性和完整性；任务范围指出，合法 NF 无法读取另一 NF 的 TLS 会话。	ts-33-501:2915, s0265, s0271, s0274
K01	访问令牌对攻击者保密	NRF 和 NF 服务消费者：可在 Nnwdaf_VFLTraining API 上使用的访问令牌仅被 NRF 和被签发该令牌的 NF 知晓	TS 29.520 5.9.9 将令牌签发和保护委托给 OAuth2 基线；RFC 6749 10.3 要求访问令牌在传输和存储中保持机密且不可猜测，10.8 禁止以明文发送它们。	rfc6749:2859, rfc6749:3013, s0290, s0291
U01	通知关联来自消费者	NF 服务消费者：已接受通知的 vflCorrId 和 iterationNum 来自其提交的订阅	TS 29.520 5.9.6.2.3 在订阅中定义 vflCorrId，5.9.6.2.9 在报告中定义它；未给出绑定规则。	s0253, s0271, s0085
U02	训练报告仅接受一次	NF 服务消费者：一个训练报告（notifCorrId、vflCorrId、iterationNum）最多被接受一次，且不跨会话或轮次	TS 29.520 5.9.6.2.6 和 5.9.6.2.9 定义了报告标识符；29.520 未给出去重规则，TS 33.501 要求 SBI 上的重放保护。	ts-33-501:2865, s0262, s0271, s0086
Q3	能力检查与训练完成相区分	NF 服务消费者和 NWDAF：成功的能力检查（准备订阅，vflPreFlag=true）不是训练完成，已取消的订阅留下一致的有限状态	TS 29.520 4.10.1.1 和 4.10.2.2.1 将能力检查作为其自身目的；5.9.6.2.2 NOTE 禁止准备订阅产生通知；4.10.2.3.2 在 DELETE 时移除订阅。除这些之外，文稿未定义状态机。	s0006, s0031, s0075, s0250

ID	简称	对象	文稿怎么说	出处
X01	SBI交换的相互认证	NF 服务消费者和 NWDAF，针对网络中的任何其他 NF	TS 33.501 5.9.2.1 要求 NF 服务消费者与生产者之间的直接通信进行相互认证，并要求每个 NF 验证所有传入消息；TS 29.500 6.7.2 要求基于服务的接口使用 TLS。	ts-33-501:2871, ts-29-500:4980
X02	无效请求被拒绝	NWDAF，针对持有自身凭据的任何 NF	TS 33.501 5.9.2.1：每个 NF 应验证所有传入消息，并拒绝或丢弃无效消息；TS 29.500 6.7.3 要求验证令牌、有效期和范围，并给出 401/403 应答。	ts-33-501:2875, ts-29-500:4994
X03	访问令牌不可被其他NF使用	NWDAF，持有合法消费者的令牌	RFC 6749 10.3 指出，OAuth 2.0 未给资源服务器提供任何方法来验证客户端出示的令牌是签发给该客户端的；TS 29.500 6.7.5 要求访问令牌的 subject 声明与请求 NF 的客户端凭据断言相匹配。	rfc6749:2879, ts-29-500:5068

分析者依据文稿补充的性质：X01, X02, X03.

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 39 段，没选 359 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	RFC 6749 安全考虑一节的开头说明了这些章节面向哪些客户端类型，并指向 OAuth 威胁模型；其中没有陈述本 API 的任何性质
P003 至 P006	rfc6749:2790-2823	Z01, K01	
P007 至 P010	rfc6749:2827-2850	Z01, Z03, `nf_service_scope`	
P011 至 P015	rfc6749:2859-2881	K01, Z03	
P016 至 P033	rfc6749:2885-3003	不在范围内	在基于 SBI 的客户端凭据授予中不存在 refresh token、授权码、重定向 URI 和资源所有者口令凭据
P034 至 P035	rfc6749:3013-3019	K01, K02	
P036	rfc6749:3023-3028	A03	
P037 至 P039	rfc6749:3032-3041	K01	
P040 至 P062	rfc6749:3045-3210	不在范围内	钓鱼、跨站请求伪造、点击劫持、代码注入、开放重定向和隐式授予涉及用户代理流程；本 API 由持有客户端凭据的 NF 使用

段落	出处	定为	不选的原因
P063	ts-33-501:2491-2491	不在范围内	AS/NAS 安全特性的降级涉及无线接口，而不是本 SBI API
P064 至 P074	ts-33-501:2495-2517	不在范围内	订阅和拜访网络认证、UE 授权以及 5G 密钥要求属于接入层性质，不在本文分析的 API 范围内
P075 至 P213	ts-33-501:2523-2853	不在范围内	对 UE、gNB、ng-eNB、SEAF、UDM、SIDF、UDR 和用户隐私的要求属于接入层和用户层，任务未纳入
P214	ts-33-501:2859-2859	没有陈述目标	信任边界这一段只说明哪些要求适用于跨越信任区的消息；其中没有陈述本 API 的任何性质
P215 至 P220	ts-33-501:2865-2875	A03, A04, Z01, R02, `nf_service_scope`	
P221 至 P227	ts-33-501:2879-2891	Z01, K01	
P228 至 P234	ts-33-501:2895-2907	不在范围内	这些要求涉及 NEF-AF 接口，而不是本文分析的接口
P235 至 P241	ts-33-501:2911-2923	K02	
P242 至 P303	ts-33-501:2929-3055	不在范围内	核心网端到端互连、SEPP 和漫游中介涉及跨 PLMN 漫游，本文的单 PLMN API 分析未纳入
P304 至 P318	ts-33-501:3059-3091	不在范围内	漫游属性的保护和 IPUPS 要求涉及网络间互连，不在本 API 范围内
P319 至 P375	ts-33-501:3097-3231	不在范围内	信令监控、安全可见性、算法选择、5G-RG 和 NSSAAF 要求涉及系统的其他部分
P376 至 P398	ts-33-501:6540-11901	不在范围内	N3 安全、EAP-TLS 附录、IAB、MBS 和 NEF 要求涉及用户面、接入层或其他接口

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 28 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 7 项，没设的 21 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	NF service consumer	参与方	`nf_service_scope`	
S02	NWDAF	参与方	按定义全部失守	NWDAF 计算并持有全部训练结果，因此它自身不诚实按定义就使保密性性质失效，而且在该假设下文稿没有对它提出任何性质
S03	NRF	参与方	按定义全部失守	控制授权服务器的攻击者可以签发任意令牌，因此这里要求的每一项授权性质都按定义失效
S04	SCP/SEPP	参与方	不在范围内	模型对每个端点采用 TLS，因此终止另一个 NF 连接的转发节点未被建模；TS 33.501 5.9.2.4 规定所有参与方都必须信任 SCP
S05	attacker	参与方	攻击者得不到更多	目标列表中的 attacker 条目就是模型中的网络攻击者，除网络之外没有任何能力
S06	OAuth2 access token	值	`nf_token_leaked`	
S07	nnwdaf-vfltraining scope	值	攻击者得不到更多	scope 名称是公开的，按设计就携带在令牌中

ID	参与方或值	类别	攻击者条件	不设的原因
S08	subscription resource	值	`nf_scope_resource_uri`	
S09	access token	值	`nf_token_leaked`	
S10	subscriptionId	值	`nf_scope_resource_uri`	
S11	notifUri	值	攻击者得不到更多	回调 URI 是地址，不是机密；模型只通过订阅方的 TLS 连接到达回调
S12	notifCorrId	值	攻击者得不到更多	notifCorrId 只在受 TLS 保护的订阅请求中传输，且消费者在每次通知时都会校验它；在模型中，持有它的第三方无法获得任何消息路径
S13	VflTrainingSubs	值	攻击者得不到更多	订阅体在受 TLS 保护的请求中传输，其 VFL 内容对模型是不透明的
S14	VflTrainingNotify reports	值	攻击者得不到更多	通知报告只发送到订阅方的 TLS 回调
S15	stored notification	值	攻击者得不到更多	已存储的通知留在接受它的消费者处
S16	subscription state	值	`nf_scope_resource_uri`	
S17	vflPreFlag	值	攻击者得不到更多	vflPreFlag 是携带在订阅中的公开布尔值
S18	iterationNum	值	攻击者得不到更多	迭代次数是携带在报告中的公开计数器
S19	chkPoint	值	攻击者得不到更多	checkpoint 信息是订阅的调度属性，不是机密
S20	VflTrainingReport fields	值	攻击者得不到更多	除结果之外的报告字段是公开的关联值和状态值
S21	vflCorrId	值	攻击者得不到更多	vflCorrId 是消费者自己选择的关联值；持有它无法到达回调
S22	event	值	攻击者得不到更多	分析事件标识符是公开的
S23	VflIntermedTrainInfo	值	按定义全部失守	中间训练信息是 K02 保护的值；一旦另一方持有它，保密性性质就被破坏，不再就此对本 API 提出进一步性质
S24	intermediateRes	值	按定义全部失守	intermediateRes 是受保护的训练结果；持有它就是 K02 所说的违规
S25	VflSampleId	值	不在范围内	SUPI 和 GPSI 样本标识符会引发用户隐私问题，任务未纳入
S26	VflTrainingReport	值	按定义全部失守	报告携带训练结果；持有它就是 K02 所说的违规
S27	VFL 能力检查结果	值	攻击者得不到更多	能力检查结果只返回给请求的消费者，且是公开的布尔结果
S28	订阅状态	值	`nf_scope_resource_uri`	

每条性质在各攻击者条件下的答案

攻击者由分析者设定，且在编写查询之前就已确定；每个答案都记录在其中一个攻击者下。单元格是证明器在该攻击者下对该性质给出的答案；“无答案”表示证明器在该攻击者下对该性质留有未决主张或未记录任何内容；空单元格表示分析者未为该性质设定该攻击者。

攻击者	持有什么	依据	出处
`network`	仅网络：它读取、丢弃、更改和发送消息，不持有任何参与方的机密		

攻击者	持有什么	依据	出处
`nf_service_scope`	同一网络中自己的一个 NF 实例身份，以及 NRF 在运行前签发给它的、用于 nnwdaf-vfltraining scope 的访问令牌	TS 29.520 5.9.9 为整个服务定义一个 scope，没有资源级或操作级 scope；TS 29.500 6.7.3 允许任何 NF service consumer 使用带客户端凭据的 OAuth2，且任务范围将外部网络攻击者与持有自己凭据的恶意合法 NF 区分开。	ts-29-500:4990, ts-29-500:4998, s0290, s0293
`nf_scope_resource_uri`	nf_service_scope 的凭据和令牌，以及另一个消费者的订阅的 subscriptionId（资源 URI），文稿未声明其为机密	TS 29.500 6.7.3 要求生产者在允许访问所请求资源之前校验令牌、其有效期及其访问 scope，并说明服务 scope 授予对 API 的通用访问；29.520 5.9.9 未定义资源级 scope，因此资源 URI 是唯一选择资源的东西，且 29.520 4.10.2.3.2 未陈述所有权检查。	ts-29-500:4994, ts-29-500:5000, s0042, s0143, s0293
`nf_token_leaked`	NRF 签发给合法 NF service consumer 的、用于 nnwdaf-vfltraining scope 的访问令牌，但不含消费者的 TLS 凭据	RFC 6749 10.3 将泄露的访问令牌视为典型情形，并指出资源服务器没有方法检查令牌是否签发给了出示它的客户端。	rfc6749:2859, rfc6749:2879

ID	`network`	`nf_service_scope`	`nf_scope_resource_uri`	`nf_token_leaked`
Z01	成立	无答案		
Z03	成立		不成立	
A03	无答案			
A04	无答案			
R02	无答案			
R03	无答案			
S05	无答案		无答案	
S04	成立			
A08	无答案			
K02	无答案		无答案	
K01	成立			
U01	成立			
U02	无答案			
Q3	成立			
X01	无答案	成立		
X02	成立	成立		
X03				成立

原文和目标

来源：293 个原文单元，68550 字节，冻结于 source-delivery-01.json。 目标：13 个已批准（Z01、Z03、A03、A04、R02、R03、S05、S04、A08、K02、K01、U01、U02）；提出的问题：3 个。 目标清单事先按草案获得批准，使用 --approve-targets。

宿主按其文档默认值（任务 `decisions: auto`）作出的决定，供你核查：

- approve_package：批准源文包 protocol-1a1c8dc25e8c702e2c5626af7852

本步骤的自报信息：1 个请求（1 个失败），0.000 USD，输入 46821 tokens，输出 5489 tokens，266 秒。

关于证明器与模型的说明

分析者为目标命名的内容：

步骤	目标	特征	原因
40	Z01, Z03, A03, A04, R02, R03, S05, S04, A08, K02, K01, U01, U02, Q3, X01, X02, X03	many_sessions, plain_primitives, other	该模型覆盖任意数量的并发消费者会话，以及在一个共享订阅存储上的任意数量的恶意 NF 请求，并且只使用理想化的无 MAC 原语：不透明令牌、带标签元组和私有（TLS）通道。计数、异或或 Diffie-Hellman 均未建模；TLS 被建模为端点之间的私有通道，每个回调被建模为每个订阅的私有通道，这在机密性上强于 TLS，且对终止 TLS 的中继不作任何说明。

被证伪且未提交

证明器证伪了以下性质，它们不在任何已记录的答案中。

- `a04_create`（model.pv，基于模型的较早版本，此后未再运行）：sid: subid, v: bitstring, w: bitstring; inj-event(AcceptedCreate(sid, idc, v, w)) ==> inj-event(ConsumerCreate(v, w))
- `a08_notify`（model.pv，基于模型的较早版本，此后未再运行）：sid: subid, it: bitstring; event(GotReport(sid, it)) ==> event(TrainingReady(sid))

分析者的结束说明

该模型覆盖整个 Nnwdaf_VFLTraining 客户端流程：在 NRF 处签发令牌、作为准备订阅的能力检查、训练订阅、一次中间结果通知以及删除，并包含单一服务范围、令牌的 audience/scope/subject 检查、订阅存储、持有自己令牌的恶意合法 NF，以及后来持有消费者令牌的攻击者。在 17 个目标中，11 个已证明或已到达，4 个带有攻击，3 个无答案。

唯一的发现是：API 未定义资源级范围，也没有任何服务操作条款要求所有权检查，因此一个持有服务范围令牌、并掌握另一消费者订阅 URI 的 NF 可以 PUT、PATCH 或 DELETE 该订阅，而 NWDAF 会像对所有者一样作答。在模型副本上检查了一项加入所有权检查的拟议修改：三个攻击查询变为已验证，正常流程保持不变，其他答案均无变化。

成立的内容：NWDAF 接受的每一次创建、修改和删除，都由其指名的 NF 所出示的、由 NRF 签发的令牌作为依据；泄露的令牌无法被用来冒充另一个 NF；准备标志会阻止通知，直到订阅被更新；以消费者身份进行的创建对应于该消费者发送的请求；消费者只接受自己的 vflCorrId 和 notifCorrId。被阻断的内容：通知实例的新鲜度和发送方对通知的一致意见无法判定，因为 ProVerif 的复制请求处理器允许一个创建请求构建两个订阅——这属于未展开模型或 Tamarin+ Agent 的案例。记录在通知机密性和删除上的攻击是查询和模型的产物，而非协议失败。TLS 被建模为每个端点的私有通道，因此终止连接的中继、令牌过期以及任何计数或代数细节都超出已展示的范围。