AF 训练服务器订阅的安全分析

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	10 条：6 条成立，2 条不成立（3 个攻击），2 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

Naf_Training 服务是充当 VFL 服务器的应用功能所提供的基于服务的接口。网络数据分析功能，或在 AF 不受信任时的网络开放功能，订阅一个已有训练任务的训练事件，在它注册的回调 URI 上接收训练报告，更新订阅，随后将其删除。AF 持有训练订阅和报告；NRF 签发 OAuth2 访问令牌，消费者凭借该令牌获得授权。

消费者确信，它接受的每条通知都是 AF 为它自己的订阅发送的。AF 确信，它处理的每个请求都携带 NRF 为出示该令牌的消费者签发的令牌。两者都不确信发送请求的消费者就是创建该订阅的那个消费者，交换正是在这里被破坏。

参与方：

- **NWDAF（或 NEF）**：NF 服务消费者。持有：访问令牌（naf-train 范围）、它的 notifUri、它的 notifCorreId。
- **AF**：VFL 服务器，NF 服务生产者。持有：订阅、训练报告。
- **NRF**：授权服务器。持有：令牌密钥。

图 1 展示了文稿所规定的交换过程。

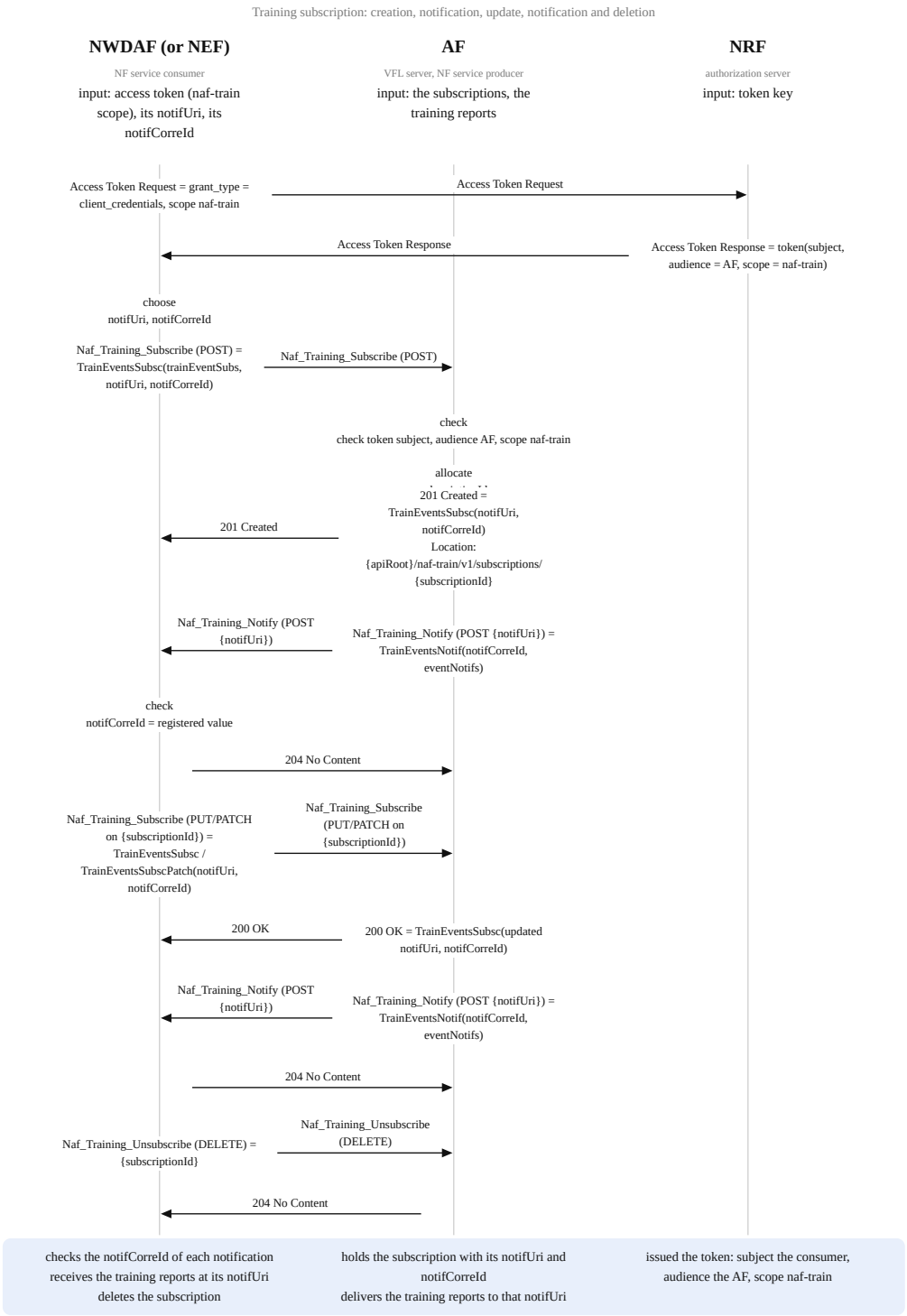


图 1. 协议如规范所定义。

分析的范围见附录 D：分析了什么、省略了什么，以及它所依据的文稿章节。

2 发现

分析有 1 个发现：以下内容文稿并未写明。其中 1 项不确定文稿是否写明。

授权要求成立，通知绑定也成立：AF 只有在持有 NRF 为请求消费者签发的令牌时才执行创建、更新或删除，并且每条通知都发往为其订阅登记的端点和关联标识符，无论有多少会话。发现的是授权的另一半：由于 API 只定义了一个服务级范围而不定义资源级范围，第二个合法 NF 只要知道另一消费者的订阅 URI，

就能更新该订阅以接收其训练报告，并将其删除。文稿既未写明也未禁止这一点，因此这是规范中需要弥补的缺口。所有依赖 AF 订阅记录的内容都只对三个未展开的步骤作答，重试的创建和删除之后的时间至多只能由可达性作答，没有任何证明带有对照变体，且建议的修复未在模型上验证。

攻击图使用图 1 的列。红色表示攻击者的行为。黄色标记的是某参与方发送的消息，而规范交换在该时点并没有这条消息，以及攻击所破坏的结果。

2.1 一个合法 NF 可以接管另一消费者的训练订阅并接收其报告

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 (main:5855, ts-29-500:4996, rfc6749:2827)
价值	高
涉及的性质	Z01.10, Z03 （见第 3 节）
原文	s0045, s0061, s0134, s0288
依据	ProVerif attack queries `z0110_upd`, `z0110_del`; Figures 2, 3 and 4

发生了什么。 第二个 NF 服务消费者用自己有效的 naf-train 令牌，向另一消费者的个体训练订阅发送 PUT，并要求将该订阅的 notifUri 设为自己的端点；AF 验证令牌，找到预期的受众和范围，然后应用更新，因为它是唯一应用的是服务级范围。随后 AF 把该订阅的通知发送给第二个 NF。用同一个令牌，第二个 NF 还可以对该订阅发送 DELETE，AF 便会将其删除。

攻击者需要什么。 一个合法的 NF 服务消费者，持有自己针对 naf-train 范围的 OAuth2 令牌（NRF 会向任何消费者签发），以及另一消费者的个体训练订阅 URI。该 URI 具有固定的公开形式 {apiRoot}/naf-train/v1/subscriptions/{subscriptionId}，规范中没有任何要求 subscriptionId 不可猜测或保密。

攻击者能得到什么。 该订阅的训练报告——分析事件、准确度、终止原因、VFL 关联标识符——被投递给另一个 NF，而且订阅可以在其所有者的名义下被移除。没有任何东西告知所有者：它只是不再收到报告。

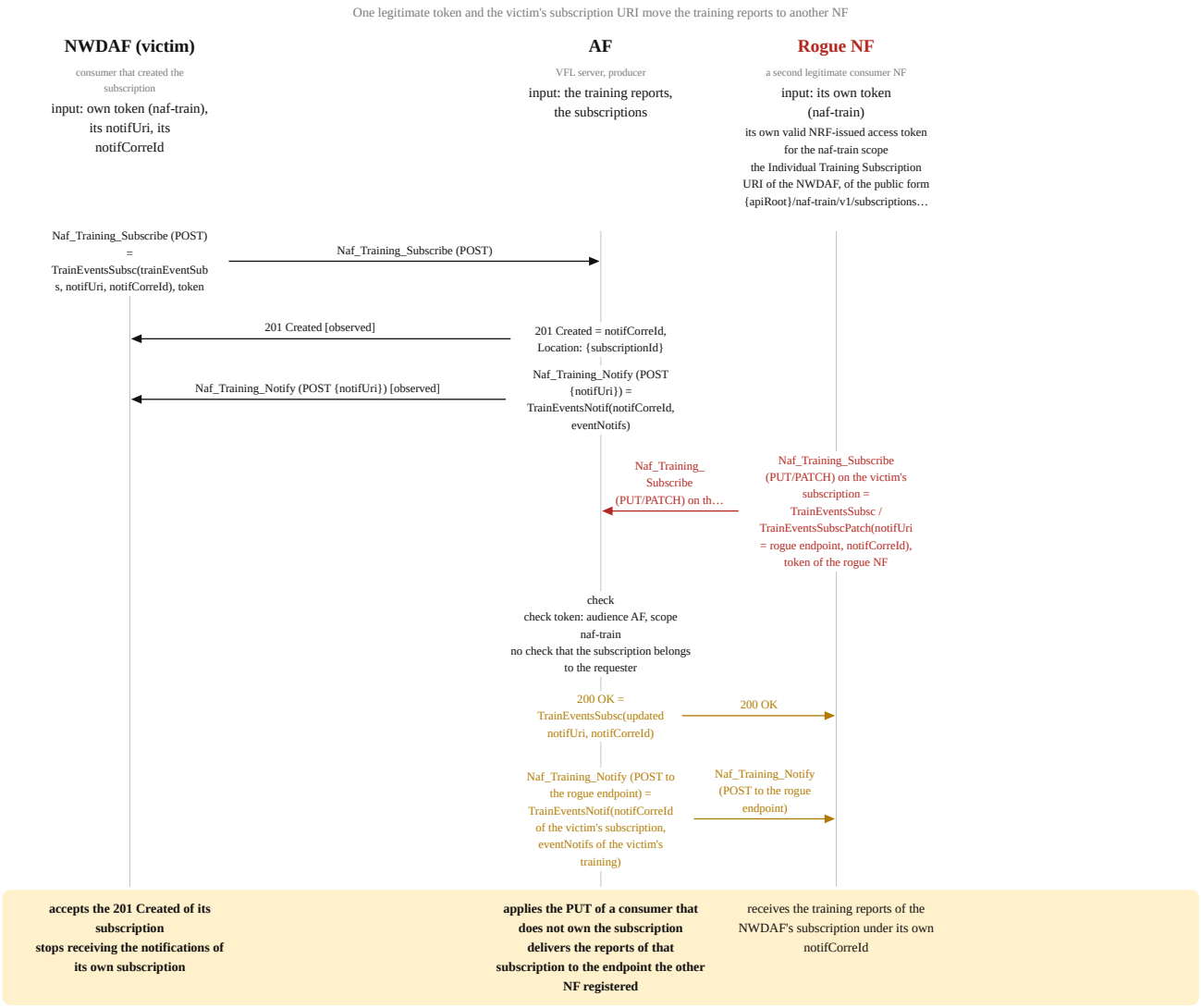


图 2. 一个合法令牌加上受害者的订阅 URI 就能把训练报告转移到另一个 NF。性质 Z01.10；攻击查询 z0110_upd。

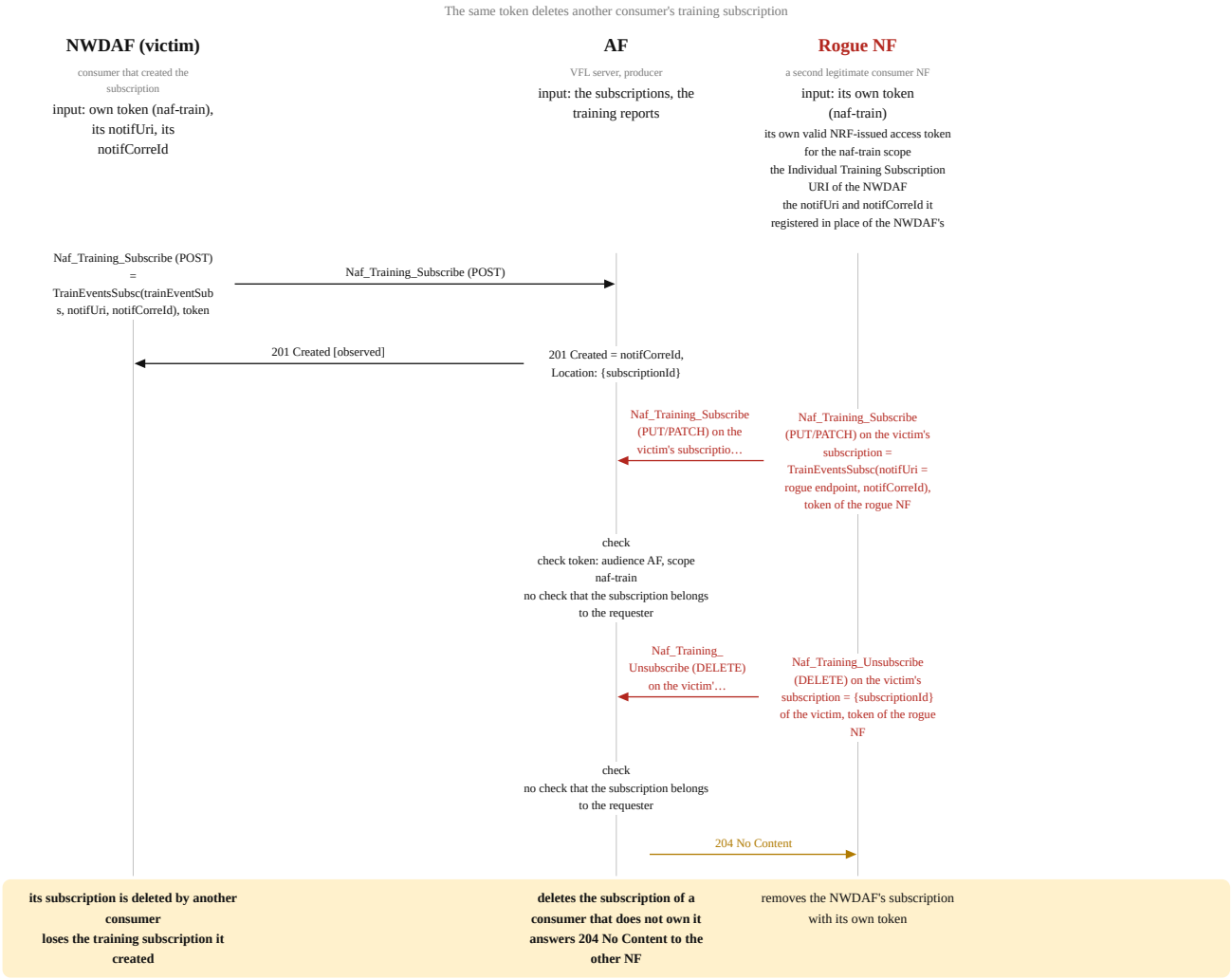


图 3. 同一个令牌删除了另一消费者的训练订阅。性质 Z01.10；攻击查询 z0110_del。

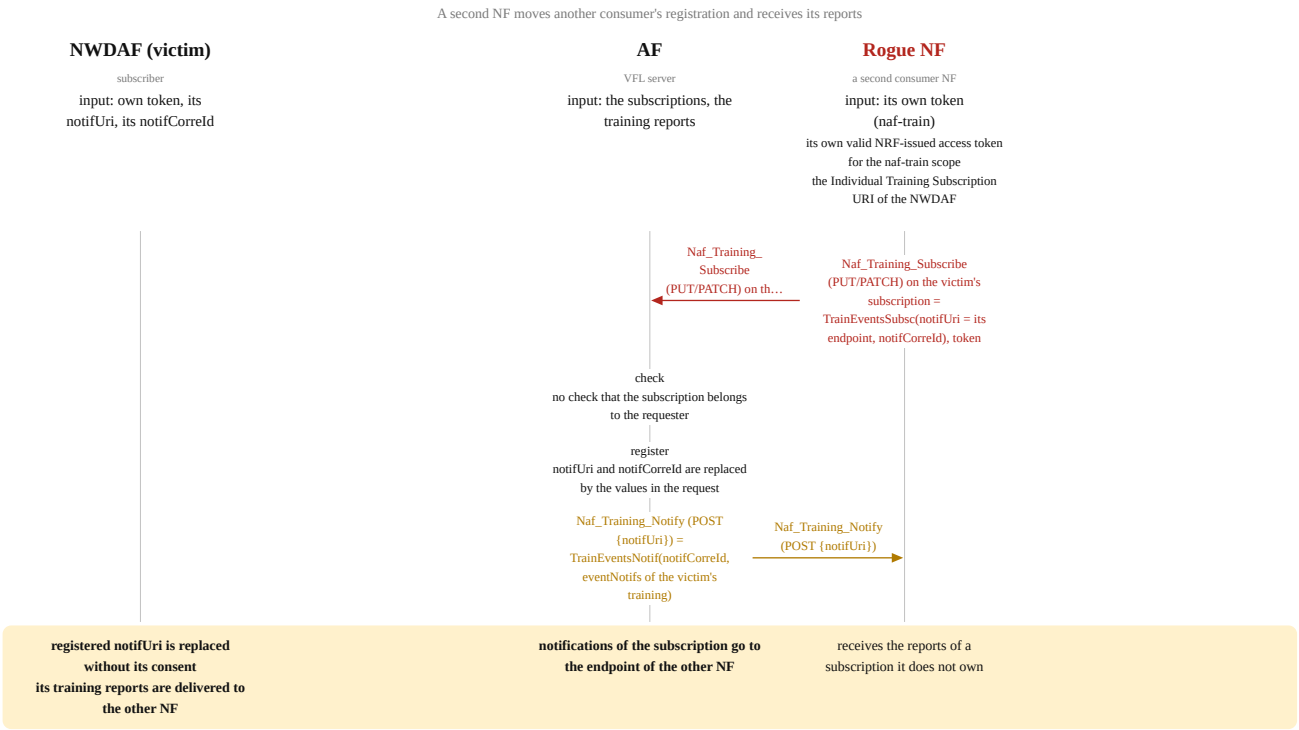


图 4. 第二个 NF 转移了另一消费者的注册并接收其报告。性质 Z03；攻击查询 z0110_upd。

拟议修改。 将每个训练订阅绑定到创建它的消费者，并在之后的每个请求上检查该绑定：AF 保存成功 POST 的令牌主体，并在个体训练订阅的 PUT、PATCH、GET 和 DELETE 上要求令牌主体等于所保存的主体。或者，第 6.3.9 条为这些操作定义操作级和资源级范围（如 TS 29.500 在需要特定授权时所允许的），AF 在个体训练订阅资源上要求该范围。

用 ProVerif 复核。 未检查：该修改需要在 AF 处为每个订阅保留所有者记录，并在 PUT、PATCH、GET 和 DELETE 上进行比较。bounded.pv 为三步保留了这样的记录，但没有携带创建它的消费者的身份，因此必须先对该修复建模；这超出了本次会话的范围，因此该修改未经验证。

对于某个发现的这些攻击，未给出图：Z03: z0110_del。

3 检查过的性质

每一行是一条提交给 ProVerif 的性质。结果是 ProVerif 对分析者协议模型的回答；价值和文稿是否已写明该结果是分析者的判断，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	**对每个订阅操作的授权。** AF 每次接受一次训练订阅的创建、更新或删除，都必须有该请求消费者持有的、由授权服务器签发的有效许可。	无	成立	中	是
Z03	**通知与其订阅绑定。** AF 发出的每条训练通知都发往该订阅创建/更新时登记的 notifUri，并携带与该订阅对应的 notifCorreId；许可不能被移到其他消费者或其他订阅上使用。	无	不成立（1 个攻击）	高	不确定
D01	**仅在真实发送后发送通知。** 消费者每次接受一条训练通知，都存在 AF 对该消费者的真实发送，且 notifCorreId 与 eventNotifs 内容一致。	无	成立	低	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
A03	**匹配通知投递，无重放。** 消费者每次接受通知，都存在 AF 的一次匹配发送，消费者身份、notifUri、notifCorreId 与事件内容一致。	无	成立	低	是
A08	**创建的资源与请求匹配。** AF 返回的订阅资源与 Location 对应消费者提交的 TrainEventsSubsc 参数；后续通知使用该订阅登记的 notifUri 与 notifCorreId。	无	成立	低	是
R03	**每个操作一个副作用。** 同一逻辑订阅创建/更新/删除操作在 AF 侧至多提交一次副作用。	无	只确认可达	低	不确定
S05	**删除后无任何内容。** 订阅删除生效之后，AF 不再向该订阅的 notifUri 发送该订阅的通知，旧订阅标识不能重新触发通知。	无	无答案	低	不确定
Z03.8	**notifUri和notifCorreId绑定（Q1）。** AF 发出的每条训练通知都发往该订阅登记的 notifUri，并携带与该订阅对应的 notifCorreId。	无	成立	低	是
U01	**报告与其训练任务绑定（Q2）。** 消费者接受的每条训练报告都对应 AF 针对同一训练任务（event、vflCorrId）的真实发送，报告类别一致。	无	成立	低	是
Z01.10	**无跨消费者订阅控制（Q3）。** AF 每次接受订阅更新或删除，都必须有该请求消费者持有的有效许可；持有自身令牌的 NF 不能在没有针对该订阅的授权时更新或删除其他 NF 的订阅。	无	不成立（2 个攻击）	高	不确定

所提出的问题，以及分析者的回答：

问题	回答	依据
Q1: 训练事件订阅者与 notification URI/相关标识绑定	这种绑定在 AF 控制的方向上成立：每条通知都发往为该订阅登记的 notifUri，并携带其 notifCorreId，对任意数量的会话均已证明。未绑定的是注册本身：另一个合法 NF 可以向并非由它拥有的订阅 PUT 一个新的 notifUri，随后报告就在它自己的 notifCorreId 下发往它。规范从未说明 AF 如何检查 notifUri 是否属于提交它的消费者。	Z03.8, Z03, Z01.10
Q2: 成功/失败/终止报告不可跨训练任务混用	网络上的参与方无法在任务之间混淆报告：消费者接受的每条报告都对应 AF 发出的一条通知，事件相同、notifCorreId 相同、VFL 关联标识也相同，且每条通知对应一次不同的发送。混淆只通过接管产生：第二个 NF 收到的另一个任务的报告已经按其自己的 notifCorreId 整理好，因此无法与它自己的报告区分开。	U01, A03, Z01.10
Q3: 持有自身 token 的 NF 是否可更新/取消其他订阅，按规范区分策略条件	凭借自己的 token 和另一消费者的订阅 URI，一个合法 NF 可以更新该订阅并接收其报告；token 检查会通过，因为 API 只定义了一个服务级 scope，资源级没有 scope。因此消费者之间的隔离依赖于第 6.3.9 条留给本地配置的策略，以及订阅 URI 不被知晓，而非 AF 能够检查的授权。问题的删除部分未能确定。	Z01.10, Z01, Z03

4 本次分析的局限

这里的结果是关于协议模型的结果：它说明规范规定的消息和检查给出了什么、未能给出什么，其中密码学被视为理想化的，不涉及任何实现。

按分析者的陈述，本分析未覆盖以下内容：

- AF 的订阅记录在 bounded.pv 中被展开为三步（创建、更新、删除），且未复制；对同一条记录的第四次及以后的请求，以及两个订阅的交错，都不在分析范围内。
- 在 model.pv 中，AF 每个进程实例只服务一个订阅，因此那里没有涉及在其持有的生命周期之后到达的请求，删除路径在那里根本无法到达。
- TLS 是每个端点一条私有通道，token 是只有 NRF 才能生成的 MAC；token 过期、TLS 密钥材料以及任一原语的强度均未建模。

- 单个订阅 URI 被视为另一个 NF 可以知晓的标识符；如果 subscriptionId 不可猜测且从未泄露，接管就需要额外披露该 URI，而规范对此既不要求也不禁止。
- AF 的训练计算、VFL 客户端、不可信的 AF 或 NEF、HTTP 重定向（307、308）、SCP、特性协商，以及与 NRF 之间除签发 token 之外的 OAuth2 交换，均在模型之外。
- 通知投递是每条通知一次 POST 并返回 204 确认；重试、每个订阅多条通知，以及删除与在途通知之间的顺序均未建模。
- 证明未携带对照查询变体，因此报告对每项性质都指出：没有任何东西表明该性质在本模型中可能不成立；唯一尝试的对照查询在模型被缩减后变成了证明。
- 建议的修复未在模型上验证，重试创建（R03）只能在可达性层面回答，因为此处的模型都没有发送两次创建请求。

宿主记录的内容：

- 无答案：R03、S05。
- 在解读写成之后答案发生变化的：R03。
- Z01、R03、S05、Z01.10 的答案依赖于模型简化的一项操作（附录 D）。
- 证明器没有给出结论的查询（附录 C）：S05: s05, Z01.10: z0110_del。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）：R03 在 `legal_nf` 下。
- 没带对照查询的证明（附录 C）：Z01: z01_upd, Z01: z01_create, Z01: z01_del, Z03: z03_reg, D01: d01, A03: a03, A08: a08, A08: z03_reg, Z03.8: z03_reg, U01: d01。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。

每项性质仍待解决的问题，以及怎样才能解决它，见附录 A。

附录 A：逐条性质的解读

这是分析者本人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、能否按现状使用，以及它的价值何在。

Z01: 对每个订阅操作的授权

AF 每次接受一次训练订阅的创建、更新或删除，都必须有该请求消费者持有的、由授权服务器签发的有效许可。

AF 所执行的每一次创建、更新和删除，都由 NRF 为请求中指定的消费者签发的访问 token 支撑，该 token 以 AF 为受众并具有 naf-train scope；没有 token 的 NF 无法让 AF 接受其中任何一项。在展开模型上，删除也得到了覆盖，该模型中记录被创建、替换和移除。该检查说明的是 token 属于谁，而不是该消费者有权对被命名的资源做什么。

- Result: Holds; answers what is asked: yes; usable with caveats
- Value medium: 它确认了规范与 TS 29.500 所陈述的 token 要求，并表明该检查对其所检查的内容成立；对读者而言没有多少新内容。
- Stated in the documents: yes. Where the documents say it: main:5849, main:5855
- Rests on: token 是 NRF 与 AF 共享密钥下的 MAC；其过期、格式以及与 NRF 之间的通道均未建模。; token 主体被当作 TLS 对端的身份，与基线绑定方式一致；不携带客户端证书。; 删除是针对记录展开的三步来回答的，而非针对任意数量的请求。

Z03: 通知与其订阅绑定

AF 发出的每条训练通知都发往该订阅创建/更新时登记的 notifUri，并携带与该订阅对应的 notifCorreId；许可不能被移到其他消费者或其他订阅上使用。

AF 发送的每条通知都发往其订阅登记的 notifUri，并携带该订阅的 notifCorreId，对任意数量的会话均成立。注册本身不受保护：持有自己有效 token 的第二个 NF 会覆盖并非由它创建的订阅的 notifUri，随后 AF 就把该消费者的训练报告投递给第二个 NF。

- Result: Fails (1 attack); answers what is asked: yes; usable with caveats
- Value high: 该失败未在文稿中陈述：文稿说该 API 只有一个服务级 scope，但从未说这会让另一个 NF 移动注册并接收报告。
- Stated in the documents: unclear. Source text it rests on: main:5124, s0288, s0134
- Rests on: 假定实施攻击的 NF 知晓单个订阅 URI；规范固定了其形式，但对该标识符的保密性不作任何要求。; 通知路径是每个端点一条私有通道，即 AF 与消费者之间的 TLS；网络攻击者既不能读取也不能伪造它，这部分是假定而非证明的。

D01: 仅在真实发送后发送通知

消费者每次接受一条训练通知，都存在 AF 对该消费者的真实发送，且 notifCorreId 与 eventNotifs 内容一致。

消费者接受的每条通知都是由 AF 为该消费者的订阅发送的，notifCorreId 相同，报告内容也相同。网络上的参与方无法产生消费者会接受的通知，因为回调端点绑定到 AF。

- Result: Holds; answers what is asked: yes; usable with caveats

- Value low: 它是通知路径受保护后流程所蕴含的性质，且成立；对读者没有新内容。
- Stated in the documents: yes. Where the documents say it: main:1425, main:5124
- Rests on: AF 与消费者之间的 TLS 是每个端点一条私有通道，因此网络无法在其上写入。; 每个订阅打印建模一条通知，并带 204 确认。

A03: 匹配通知投递，无重放

消费者每次接受通知，都存在 AF 的一次匹配发送，消费者身份、notifUri、notifCorreId 与事件内容一致。

消费者接受的每条通知都对应 AF 为该订阅、该报告发出的一条不同通知，因此在模型覆盖的会话中，已记录的通知不能在同一关联标识符下被出示两次。

- Result: Holds; answers what is asked: yes; usable with caveats
- Value low: 它成立的原因与上一条性质相同，且没有说出文稿尚未假定的任何内容。
- Stated in the documents: yes. Where the documents say it: main:1425
- Rests on: 响应经由 AF 自己的端点通道返回，即 TLS 绑定；规范中没有任何重放规则被建模，因为并不存在这样的规则。

A08: 创建的资源与请求匹配

AF 返回的订阅资源与 Location 对应消费者提交的 TrainEventsSubsc 参数；后续通知使用该订阅登记的 notifUri 与 notifCorreId。

消费者接受的 201 Created 所命名的订阅，是 AF 为该同一消费者创建的，回显相同的 notifCorreId 和相同的 notifUri，且该订阅的每条后续通知都使用登记的端点和关联标识符。

- 结果：Holds；是否回答了所问：是；可用但需注意
- 价值低：这是过程所要求参数的呼应，已经过证明而非假设，但并无疑问。
- 文稿中已说明：是。文稿中的位置：main:1065, main:1425
- 依据：AF 为每个被接受的 POST 创建一个新标识符；模型无法显示它如何被选择或存活多久。

R03: 每个操作一个副作用

同一逻辑订阅创建/更新/删除操作在 AF 侧至多提交一次副作用。

本解读写成后，该目标的答案发生了变化。

除以下情形外没有确立任何东西：创建请求到达 AF，并产生一个带有自己标识符的 Individual Training Subscription。AF 不保留请求标识符，规范也未定义幂等规则，因此若消费者在丢失 201 后重试，最终会有两个订阅；证明器的一个推导也如此说明，但此处没有模型发送两次请求，因此不构成一条迹。

- 结果：仅 Reachable；是否回答了所问：否；不可用
- 价值低：证明器只给出了可达性；重复副作用是对规范的解读，不是结果。
- 文稿中已说明：不明确
- 依据：AF 为每个被接受的 POST 创建一个订阅，并且不保留产生该订阅的请求的任何记录。; 未建模重试、超时和请求标识符。
- 未决：重试的 POST 是否会创建第二个订阅，这正是目标所问。

S05: 删除后无任何内容

订阅删除生效之后，AF 不再向该订阅的 notifUri 发送该订阅的通知，旧订阅标识不能重新触发通知。

只确立了以下情形：删除会得到 204 No Content 响应，并且在展开的 AF 中，此后指名已删除订阅的请求既不产生通知也不产生应答。删除后通知是否仍能到达消费者——这正是目标所问——并未展示，因为模型无法对通知和删除进行排序。

- 结果：No answer；是否回答了所问：否；不可用
- 价值低：仅删除的可达性无法回答删除之后会发生什么；该性质本身未被确立。
- 文稿中已说明：不明确
- 依据：AF 的记录被展开为三步，删除后的请求由一个不发出任何内容的进程应答；这是建模选择，不是规范的陈述。；未建模在途通知，规范也未说明它们的顺序。
- 未决：删除生效时，AF 对在途的通知或请求如何处理；模型没有这种重叠。

Z03.8: notifUri和notifCorreId绑定（Q1）

AF 发出的每条训练通知都发往该订阅登记的 notifUri，并携带与该订阅对应的 notifCorreId。

AF 在一个订阅中发送的每条通知都发往该订阅登记的 notifUri，并携带其 notifCorreId，因此消费者仅凭通知就能识别自己的订阅，无论有多少会话。

- 结果：Holds；是否回答了所问：是；可用但需注意
- 价值低：这是过程所陈述的关联，已对任意数量的会话证明；可作为基础，但本身不是结果。
- 文稿中已说明：是。文稿中的位置：main:1425, main:5124
- 依据：消费者保留自己选择的 notifCorreId，并与通知中的值比较；模型精确匹配。；订阅更新时 AF 登记新的 notifCorreId。

U01: 报告与其训练任务绑定（Q2）

消费者接受的每条训练报告都对应 AF 针对同一训练任务（event、vflCorrId）的真实发送，报告类别一致。

消费者接受的每条训练报告都对应 AF 为同一 event 和同一报告发送的通知，因此一个任务的报告不能被当作另一个任务的报告呈现。报告与其任务的关联依赖于 AF，消费者除了 notifCorreId 之外无法检查其他内容。

- 结果：Holds；是否回答了所问：是；可用但需注意
- 价值低：它成立，且正是文稿所描述的内容；更尖锐的问题——另一个任务的报告是否会到达未请求它的消费者——由接管来回答，而不在这里。
- 文稿中已说明：是。文稿中的位置：main:5124
- 依据：报告内容是 AF 每次通知的新鲜值；模型除携带一个内容值外不区分报告类别。；vflCorrId 作为报告的一部分携带，不是消费者能验证的东西。

Z01.10: 无跨消费者订阅控制（Q3）

AF 每次接受订阅更新或删除，都必须有该请求消费者持有的有效许可；持有自身令牌的 NF 不能在没有针对该订阅的授权时更新或删除其他 NF 的订阅。

第二个 NF 持有自己有效的 naf-train 令牌和另一个消费者订阅的 URI，更新该订阅使其通知发往第二个 NF，AF 应用了该变更；用同一令牌它删除该订阅，AF 将其移除。AF 检查令牌、受众和范围，但没有任何东西将订阅绑定到创建它的消费者，因此服务级范围授权每个消费者访问每个订阅。

- 结果：Fails（2 个攻击）；是否回答了所问：是；可用但需注意
- 价值高：这是所规定授权中的弱点，文稿未说明，对训练报告和另一个消费者的订阅有具体影响；它需要订阅 URI 已知，规范既不要求也不禁止这一点。
- 文稿中已说明：不明确。所依据的原文：s0288, s0134, s0045, s0061
- 依据：假设攻击的 NF 知道另一个消费者的订阅 URI；规范固定了 URI 形式，但对 subscriptionId 的保密性没有任何要求。；AF 仅依据令牌和服务级范围进行授权，如第 6.3.9 条所述；通过本地配置检查所有权的部署不会被这些迹攻击。；删除在展开模型上展示，针对记录的三步。

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，以及各攻击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
Z01	proved		z01_create			2 proved, 1 bounded
Z03	proved		z03_reg		z0110_upd (depends_on_ambiguity)	1 proved, 1 attack
D01	proved		d01			1 proved
A03	proved		a03			1 proved
A08	proved		a08			2 proved
R03	reachable		r03			1 reachable
S05	reachable		s05			1 reachable, 1 undecided
Z03.8	proved		z03_reg			1 proved
U01	proved		d01			1 proved
Z01.10	none				z0110_upd (depends_on_ambiguity); z0110_del (depends_on_ambiguity)	2 attack, 1 undecided

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给出的：

目标	主张	攻击者	回答	查询	对照
Z01	AF 仅在 NRF 为请求方消费者签发的访问令牌下才应用 Training Subscription 的更新。	`legal_nf`	proved	z01_upd	none
Z01	AF 仅在 NRF 为请求方消费者签发、以 AF 为受众且带有 naf-train scope 的访问令牌下才接受 Training Subscription 的创建。	`network`	proved	z01_create	none
Z01	AF 仅在 NRF 为请求方消费者签发的访问令牌下才应用 Training Subscription 的删除。	`legal_nf`	bounded（变化的值展开到 3 步）	z01_del	none
Z03	AF 为某个订阅发送的每条通知都发往该订阅所注册的 notifUri，并携带该订阅所注册的 notifCorreId。	`legal_nf`	proved	z03_reg	none
Z03	订阅的注册不能被转移到另一个消费者：任何其他持有自身有效 naf-train 令牌的 NF 都不能更改不属于自己的订阅的 notifUri。	`legal_nf`	attack（depends_on_ambiguity）	z0110_upd	
D01	消费者接受的每条通知都对应 AF 为该订阅发送的一条通知，notifCorreId 与报告内容均相同。	`network`	proved	d01	none
A03	消费者接受的每条通知都与 AF 为同一订阅、同一报告发送的一条不同通知相匹配；通知不能在同一关联标识符下被重放。	`network`	proved	a03	none
A08	AF 返回的 201 Created 表示与 Location URI 与消费者提交的 TrainEventsSubsc 相对应（notifCorreId 相同、notifUri 相同）。	`network`	proved	a08	none
A08	后续通知使用订阅中注册的 notifUri 与 notifCorreId。	`network`	proved	z03_reg	none
R03	创建请求到达 AF，并产生一个具有自身标识符的 Individual Training Subscription。	`legal_nf`	reachable	r03	

目标	主张	攻击者	回答	查询	对照
S05	DELETE 被应答为 204 No Content 之后，AF 不再为该订阅发送任何通知，且该标识符不能再次用于获取通知。	`legal_nf`	undecided	s05	
S05	删除被应答为 204 No Content，并且在展开后的 AF 中，此后指名该已删除订阅的请求既不产生通知也不产生回答。	`legal_nf`	reachable	s05	
Z03.8	AF 为某个订阅发送的每条通知都发往该订阅中注册的 notifUri，并携带该订阅的 notifCorreId，因此消费者能识别出自己各订阅的通知。	`legal_nf`	proved	z03_reg	none
U01	消费者接受的每份训练报告都对应 AF 为同一训练任务（事件、vflCorrId）发送的一条通知，且报告类别唯一。	`network`	proved	d01	none
Z01.10	另一个持有自身有效 naf-train 令牌的 NF 不能更新不属于自己的订阅，也不能把其通知转移到自己这里。	`legal_nf`	attack（depends_on_ambiguity）	z0110_upd	
Z01.10	另一个持有自身有效 naf-train 令牌的 NF 不能删除不属于自己的订阅。	`legal_nf`	undecided	z0110_del	
Z01.10	另一个持有自身有效 naf-train 令牌的 NF 不能删除不属于自己的订阅。	`legal_nf`	attack（depends_on_ambiguity）	z0110_del	

附录 D：分析是怎么跑的

一个 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给出的答案。

ProVerif+ Agent 会话 session-20261114T223818，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：71，证明器 289 s，实际耗时 20 min，费用 0.154 USD。

ProVerif：运行了 74 次证明，60 次有结论，14 次无答案，215 s，记录了 19 个答案。

分析了什么

协议	AF training server subscription
版本	19.2.0
分析范围	可信 AF 为 VFL server、NWDAF 为 NF consumer；固定既有训练任务的一次 TrainEventsSubsc 创建/更新/Notify/取消。具体 VFL client 计算已在边界内，不把事件 API 当完整训练算法；排除不可信 AF/NEF。
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	338 个编号原文单元（198526 字节），来自下列各章节。本报告中诸如 s0001 的引用就是其中之一

分析所依据的文稿章节：

文稿	章节	标题
main	5.4	Naf_Training Service
main	5.4.1	Service Description
main	5.4.1.1	Overview
main	5.4.1.2	Service Architecture
main	5.4.1.3	Network Functions
main	5.4.1.3.1	Application Function (AF)
main	5.4.1.3.2	NF Service Consumers
main	5.4.2	Service Operations
main	5.4.2.1	Introduction
main	5.4.2.2	Naf_Training_Subscribe
main	5.4.2.2.1	General
main	5.4.2.2.2	Training Subscription Creation
main	5.4.2.2.3	Training Subscription Update
main	5.4.2.3	Naf_Training_Unsubscribe
main	5.4.2.3.1	General

文稿	章节	标题
main	5.4.2.3.2	Training Subscription Deletion
main	5.4.2.4	Naf_Training_Notify
main	5.4.2.4.1	General
main	5.4.2.4.2	Training Notification
main	6.3	Naf_Training Service API
main	6.3.1	Introduction
main	6.3.2	Usage of HTTP
main	6.3.2.1	General
main	6.3.2.2	HTTP standard headers
main	6.3.2.2.1	General
main	6.3.2.2.2	Content type
main	6.3.2.3	HTTP custom headers
main	6.3.3	Resources
main	6.3.3.1	Overview
main	6.3.3.2	Resource: Training Subscriptions
main	6.3.3.2.1	Description
main	6.3.3.2.2	Resource Definition
main	6.3.3.2.3	Resource Standard Methods
main	6.3.3.2.3.1	POST
main	6.3.3.2.4	Resource Custom Operations
main	6.3.3.3	Resource: Individual Training Subscription
main	6.3.3.3.1	Description
main	6.3.3.3.2	Resource Definition
main	6.3.3.3.3	Resource Standard Methods
main	6.3.3.3.3.1	GET
main	6.3.3.3.3.2	PUT
main	6.3.3.3.3.3	PATCH
main	6.3.3.3.3.4	DELETE
main	6.3.4	Custom Operations without associated resources
main	6.3.5	Notifications
main	6.3.5.1	General
main	6.3.5.2	Training Notification
main	6.3.5.2.1	Description
main	6.3.5.2.2	Target URI
main	6.3.5.2.3	Standard Methods
main	6.3.5.2.3.1	POST

文稿	章节	标题
main	6.3.6	Data Model
main	6.3.6.1	General
main	6.3.6.2	Structured data types
main	6.3.6.2.1	Introduction
main	6.3.6.2.2	Type: TrainEventsSubsc
main	6.3.6.2.3	Type: TrainEventsSubscPatch
main	6.3.6.2.4	Type: EventSubsc
main	6.3.6.2.5	Type: MlModelMonitorInfo
main	6.3.6.2.6	Type: TrainEventsNotif
main	6.3.6.2.7	Type: EventNotif
main	6.3.6.3	Simple data types and enumerations
main	6.3.6.3.1	Introduction
main	6.3.6.3.2	Simple data types
main	6.3.6.4	Data types describing alternative data types or combinations of data types
main	6.3.6.5	Binary data
main	6.3.6.5.1	Binary Data Types
main	6.3.7	Error Handling
main	6.3.7.1	General
main	6.3.7.2	Protocol Errors
main	6.3.7.3	Application Errors
main	6.3.8	Feature negotiation
main	6.3.9	Security
main	6.3.10	HTTP redirection

原文步骤在文稿中定位到的协议目的：可信 AF 为 VFL server、NWDAF 为 NF consumer；固定既有训练任务的一次 TrainEventsSubsc 创建/更新/Notify/取消。具体 VFL client 计算已在边界内，不把事件 API 当完整训练算法；排除不可信 AF/NEF。

对照文稿定性质

在写出查询之前，分析者把起草的性质清单与文稿自身对协议用途的陈述做了对照。性质的名称、性质所涉及的内容以及文稿的陈述都是分析者的解读；所提到的位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
Z01	对每个订阅操作的授权	AF（VFL 服务器）得到保证：只有当 NF 服务消费者出示由 NRF 签发的、受众为 AF、范围包含 naf-train 的有效访问令牌时，它才接受该消费者创建、更新和删除训练订阅。	访问可通过 OAuth2 客户端凭据授权，NRF 为授权服务器；消费者在使用服务前应先获取令牌；该 API 只定义了一个范围 naf-train。TS 29.500 要求生产者在允许访问所请求的资源之前，校验令牌、其有效期及其访问范围。	main:5849, main:5851, main:5855, ts-29-500:4994, s0285, s0286, s0288
Z03	通知与其订阅绑定	订阅的 NF 消费者得到保证：每条通知都按其订阅注册的 notifUri 投递，并携带该订阅的 notifCorreId；且该注册不能被转移到另一个消费者。	AF 应将通知 POST 到 {notifUri}，该值在创建/更新相应订阅时收到；notifCorreId 在 TrainEventsSubsc 和 TrainEventsNotif 中均为必选。	main:1425, main:5124, s0074, s0213, s0241, s0253
D01	仅在真实发送后发送通知	订阅的 NF 消费者得到保证：它接受的每条通知都对应 AF 为其订阅实际发送的通知，具有相同的 notifCorreId 和相同的报告内容。	AF 将 TrainEventsNotif 发送到 {notifUri}，消费者以 204 No Content 确认；该路径的保护交由端点之间的 TLS 负责。	main:1425, main:5124, s0074, s0075, s0253
A03	匹配通知投递，无重放	订阅的 NF 消费者得到保证：它接受的每条通知都对应 AF 为同一订阅和报告发送的不同通知。	TrainEventsNotif 携带相应订阅的 notifCorreId，并以 204 No Content 应答；未定义任何重放或去重规则。	main:1425, main:5124, s0074, s0075, s0253
A08	创建的资源与请求匹配	订阅的 NF 消费者得到保证：201 Created 表示和 Location URI 与其提交的 TrainEventsSubsc 一致，且后续通知使用其注册的 notifUri 和 notifCorreId。	AF 以 TrainEventsSubsc 表示和 Location 头 {apiRoot}/naf-train/<apiVersion>/subscriptions/{subscriptionId} 应答 201 Created；notifUri 和 notifCorreId 在 TrainEventsSubsc 中均为必选。	main:1065, main:1067, s0038, s0039, s0134, s0241
R03	每个操作一个副作用	AF 的训练订阅存储：一个逻辑上的创建、更新或删除请求在 AF 处至多产生一个副作用。	这些操作按一次请求、一次成功响应来描述；未定义任何幂等键、请求标识符或重试规则。	main:1065, s0027, s0030, s0054, s0062
S05	删除后无任何内容	订阅的 NF 消费者得到保证：在其 DELETE 被应答 204 No Content 之后，AF 不再为该订阅发送任何通知，且该标识符不能再次用于获取通知。	删除：对 Individual Training Subscription URI 的 DELETE 以 204 No Content 应答；未提及删除时正在传输中的通知。	main:1148, s0054, s0061, s0062, s0074

ID	简称	对象	文稿怎么说	出处
Z03.8	notifUri和notifCorreId绑定（Q1）	订阅者（Q1）：每条通知都发送到该订阅中注册的 notifUri，并携带该订阅的 notifCorreId，因此消费者能识别自己各订阅的通知。	如通知流程所述：{notifUri} 是创建/更新相应订阅时得到的值，notifCorreId 在 TrainEventsNotif 中被回显。	main:1425, main:5124, s0074, s0213, s0241, s0253
U01	报告与其训练任务绑定（Q2）	订阅者（Q2）：它接受的每份训练报告都对应 AF 为同一训练任务（event、vflCorrId）发送的、具有一个报告类别的通知。	EventNotif 携带订阅的事件、vflCorrId 以及训练指示或终止原因；TrainEventsNotif 携带 notifCorreId；未定义任何关于 vflCorrId 的规则。	main:5124, s0253, s0256
Z01.10	无跨消费者订阅控制（Q3）	订阅的 NF 消费者（Q3）：持有自己有效 naf-train 令牌的另一个 NF 服务消费者，若没有针对该订阅的专门授权，就不能更新或删除其订阅，也不能将其通知转移到别处。	更新和删除发往 Individual Training Subscription URI，且仅由令牌授权；该 API 定义了一个服务级范围，没有资源级或操作级范围，而 TS 29.500 允许在需要专门授权时使用操作级和资源级范围。	main:5855, ts-29-500:4996, s0045, s0061, s0288

分析者没有补充性质：起草的清单已覆盖文稿写明的目标。

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 33 段，没选 365 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	OAuth2 威胁的引言列表；后续各段另行处理。
P003 至 P006	rfc6749:2790-2823	Z01, `legal_nf`	
P007 至 P010	rfc6749:2827-2850	Z01.10, `legal_nf`	
P011 至 P015	rfc6749:2859-2881	Z01, Z01.10, `legal_nf`	
P016 至 P033	rfc6749:2885-3003	没有陈述目标	刷新令牌、授权码、重定向 URI、资源所有者口令凭据：该 API 仅使用客户端凭据授权。
P034 至 P035	rfc6749:3013-3019	Z03, D01	
P036	rfc6749:3023-3028	Z01, D01	
P037 至 P039	rfc6749:3032-3041	Z01	

段落	出处	定为	不选的原因
P040 至 P052	rfc6749:3045-3150	不在范围内	钓鱼、CSRF、点击劫持和代码注入属于浏览器和用户代理的问题；SBI 没有用户代理。
P053 至 P054	rfc6749:3154-3167	不在范围内	开放重定向涉及授权请求的重定向 URI；该 API 的重定向不在所建模的流程范围内。
P055 至 P062	rfc6749:3170-3210	没有陈述目标	隐式授权中的令牌误用；未使用隐式授权，也不存在资源所有者。
P063	ts-33-501:2491-2491	不在范围内	加密和完整性算法的降级；算法原语的强度不在范围内。
P064 至 P072	ts-33-501:2495-2511	不在范围内	5GS 接入中的 UE 与网络认证和授权，与本 API 流程无关。
P073 至 P078	ts-33-501:2515-2529	不在范围内	5G 接入层的密钥和一般接入网安全要求。
P079 至 P125	ts-33-501:2533-2631	不在范围内	空口信令保护、订阅凭据的安全存储和用户隐私；均不属于 SBI 服务流程。
P126 至 P198	ts-33-501:2637-2811	不在范围内	gNB、ng-eNB、F1/E1 和 SEAF 要求：RAN 侧安全。
P199 至 P213	ts-33-501:2819-2853	不在范围内	对 UDM、AUSF、UDR 和 SIDF 的要求；此处 NRF 是授权服务器。
P214	ts-33-501:2859-2859	Z01.10	
P215 至 P220	ts-33-501:2865-2875	Z01, `legal_nf`	
P221 至 P227	ts-33-501:2879-2891	Z01	
P228 至 P234	ts-33-501:2895-2907	不在范围内	NEF 对其暴露功能的安全要求；NEF 在此仅作为消费者出现。
P235 至 P241	ts-33-501:2911-2923	不在范围内	SCP 要求：SCP 部署变体不在所建模的流程范围内。
P242 至 P254	ts-33-501:2929-2953	不在范围内	SEPP 和互联安全：漫游不在范围内。
P255 至 P303	ts-33-501:2957-3055	不在范围内	SEPP 要求、N32-f 保护和漫游中间节点：互联。
P304 至 P312	ts-33-501:3059-3075	不在范围内	N32-f 上的属性保护，包括授权令牌：互联。
P313 至 P314	ts-33-501:3079-3081	不在范围内	GTP-U 的 IPUPS 转发规则。
P315 至 P318	ts-33-501:3085-3091	没有陈述目标	始发 PLMN 头的处理，属于部署相关；未陈述该 API 的任何性质。
P319 至 P327	ts-33-501:3097-3115	不在范围内	信令监控的配置和流式传输。
P328 至 P337	ts-33-501:3121-3141	不在范围内	对运营商的安全可见性和可配置性要求。
P338 至 P369	ts-33-501:3149-3215	不在范围内	算法标识符和选择：算法原语的强度不在范围内。
P370 至 P375	ts-33-501:3219-3231	不在范围内	对 5G-RG 和 NSSAAF 的要求。

段落	出处	定为	不选的原因
P376 至 P380	ts-33-501:6540-6548	不在范围内	N3 上的安全要求和流程。
P381 至 P398	ts-33-501:9656-11901	不在范围内	EAP-TLS 订阅标识符隐私、IAB、MBS 和 NEF 附录：均与本 API 无关。

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 19 项，没设的 1 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	不在范围内	任务将 AF 固定为可信的 VFL 服务器；不诚实的 AF 按定义就掌握每一个订阅和每一份训练报告，而范围排除了不受信任的 AF。
S02	NWDAF	参与方	`legal_nf`	
S03	NEF	参与方	`legal_nf`	
S04	NRF	参与方	`legal_nf`	
S05	NWDAF/NEF	参与方	`legal_nf`	
S06	OAuth2 访问令牌	值	`legal_nf`	
S07	训练订阅资源	值	`legal_nf`	
S08	notifUri	值	`legal_nf`	
S09	notifCorreId	值	`legal_nf`	
S10	subscriptionId	值	`legal_nf`	
S11	训练事件报告	值	`legal_nf`	
S12	TrainEventsNotif 内容	值	`legal_nf`	
S13	eventNotifs	值	`legal_nf`	
S14	TrainEventsSubsc 参数	值	`legal_nf`	
S15	Location URI	值	`legal_nf`	
S16	event	值	`legal_nf`	
S17	vflCorrId	值	`legal_nf`	
S18	termCause	值	`legal_nf`	
S19	vflNotOnTimeInd	值	`legal_nf`	
S20	训练报告内容	值	`legal_nf`	

每条性质在各攻击者条件下的答案

攻击者是分析者设定的，在写查询之前就已确定；每个答案都是在其中某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”是指分析者为该性质设定的某个攻击者条件下，证明器未对某条主张作出结论，或没有记录任何内容；空单元格是指分析者没有为该性质设定该攻击者。

攻击者	持有什么	依据	出处
`network`	仅网络：它能读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`legal_nf`	合法的 NF 服务消费者（NWDAF 或 NEF），持有自己有效的、由 NRF 签发的、用于 naf-train 范围的访问令牌，从自己的 TLS 端点发起请求，并知道公开的资源结构 {apiRoot}/naf-train/v1/subscriptions/{subscriptionId}，因此能够访问另一个消费者的 Individual Training Subscription 资源。它无法读取另一个 NF 的 TLS 会话，也无法为另一个消费者伪造令牌。	NWDAF 和 NEF 是已知的消费者 NF，持有各自的凭据；该 API 只定义一个服务级范围，因此任何消费者的令牌都携带相同的权限；Individual Training Subscription 的 Location URI 结构是公开的，没有任何要求规定 subscriptionId 必须保密。	main:5849, main:5855, ts-29-500:4996, s0010, s0011, s0012, s0134, s0288

ID	`network`	`legal_nf`
Z01	成立	成立
Z03		不成立
D01	成立	
A03	成立	
A08	成立	
R03		无答案
S05		无答案
Z03.8	成立	成立
U01	成立	
Z01.10		不成立

原文和目标

原文：338 个原文单元，198526 字节，冻结于 source-delivery-01.json。 目标：8 个已批准（Z01、Z03、D01、A03、A08、R03、S05、U01）；提出的问题：3 个。 目标清单一如草稿，事前已用 --approve-targets 批准。

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

- approve_package: 批准源文包 protocol-eae0246ed96fbe0bdc5d0a5395bb

这一步自报的情况：1 次请求（1 次失败），0.000 USD，输入 99457 个 token，输出 4220 个，257 秒。

关于证明器和模型的说明

- Z01：在 ProVerif 中作答，分析者为此目标标注了 changing_state
- R03：在 ProVerif 中作答，分析者为此目标标注了 changing_state
- S05：在 ProVerif 中作答，分析者为此目标标注了 changing_state
- Z01.10：在 ProVerif 中作答，分析者为此目标标注了 changing_state

简化代数（xor、dh_algebra、other_algebra）的 ProVerif 模型赋予攻击者的能力少于真实运算：这样的模型中的证明是针对更弱的攻击者的证明，这样的模型中的攻击则是一次攻击。遗漏对会变化的值（changing_state）的检查的 ProVerif 模型，会让参与方接受更多：这样的模型中的证明成立，而这样的模型中的攻击可能只是缺少了该检查。Tamarin+ Agent 按原样对这些进行建模。

分析者的状态审查

这一部分是分析者自己根据原文所作出的解读，不是证明器的答案。ProVerif 显示下的“是”表示 ProVerif 在展开的模型中找到了包含这些步骤的迹，因此这些步骤是可能的；它们是否破坏了某个目标，只由答案表中的攻击说明，它们还付出了什么代价则是分析者的解读。“未发现”说明检查了哪些模式，并不证明任何东西。

值	持有者	变化时机	检查时机	参考
训练订阅记录：subscriptionId、notifUri、notifCorreId 以及所订阅的事件	AF（VFL 服务器），每个订阅一条记录（bounded.pv 将其展开为三步：创建、更新、删除）	由 POST 创建（AF 分配 subscriptionId），其 notifUri 和 notifCorreId 被针对该资源的 PUT 或 PATCH 替换，并由 DELETE 移除。	在每个指定 Individual Training Subscription URI 的请求上：AF 查找该资源并检查请求的令牌；令牌检查是唯一的比较，请求者与创建该记录的消费者之间没有任何比较。	s0038, s0039, s0045, s0061, s0288
回调 URI notifUri	AF，按订阅持有	被针对该订阅的 PUT 或 PATCH 的 notifUri 替换。	被使用，不被比较：AF 把每条通知发往记录中持有的 notifUri，规范不要求检查该 URI 属于该消费者。	s0045, s0074, s0213
通知关联标识符 notifCorreId	AF 按订阅持有，消费者也按订阅持有	被 PUT 或 PATCH 的 notifCorreId 替换（在 TrainEventsSubscPatch 中是可选的）。	由消费者在其接受的每条通知中与其注册的值进行比较。	s0241, s0244, s0253

模式	结果	目标	ProVerif 显示	步骤
race_between_sessions	候选	Z01.10	是：ProVerif 在 bounded.pv 上否证了 `z0110_del`	NWDAF 创建一个订阅，AF 存储其记录（s0038、s0039）。/ 在该记录仍被持有期间，第二个持有自己有效令牌的 NF 对同一资源发送 PUT，AF 替换其中存储的 notifUri 和 notifCorreId（s0045、s0048）——ProVerif 在 bounded.pv 和 model.pv 上都发现了这一点。/ AF 随后在第二个 NF 的端点处发送通知（s0074），于是 NWDAF 订阅的报告离开了它（这是 model.pv 和 bounded.pv 上 z0110_upd 的已确认迹）。/ 更新之后，第二个 NF 对同一资源发送 DELETE，AF 删除该记录（s0061、s0062），ProVerif 在 bounded.pv 上的 z0110_del 迹中确认了这一点。
desynchronisation	候选	Z01.10	是：ProVerif 在 bounded.pv 上否证了 `z0110_upd`	NWDAF 注册 notifUri_A 和 notifCorreId_A；AF 存储它们（s0038、s0039）。/ 第二个 NF 通过对同一资源的 PUT 将它们替换为自己的值（s0045、s0048）。/ AF 持有 notifUri_B/notifCorreId_B，而 NWDAF 仍期望自己的值，报告被发往第二个 NF（s0074）。/ 流程中没有任何东西告诉 NWDAF 其注册已改变：没有订阅变更的通知，消费者也不会回读该资源（GET 存在于条款 6.3.3.3.3.1 中，但不属于本流程），因此双方保持分离。
replay	候选		否：未用 ProVerif 尝试	NF 服务消费者发送带有 TrainEventsSubsc(notifUri, notifCorreId) 的 POST（s0038），但没有收到 201 Created，例如因为响应丢失。/ 消费者再次发送相同的 POST，正如 HTTP 客户端在超时后所做的那样。/ AF 没有任何东西可以用来识别第二个请求：它创建第二个 Individual Training Subscription，新的 subscriptionId、相同的 notifCorreId 和相同的 notifUri，并再次回答 201（s0039，条款 6.3.3.2.3.1）。/ 消费者持有一个逻辑订阅，而 AF 持有两个，两者都把相同的训练报告投递到同一个端点。
repeat_one_time_action	未发现	S05		
update_before_check	未发现			
no_rollback_on_failure	未发现			
distinguishable_failure	未发现			
wrap_or_window	未发现			

分析者为各目标标注的内容：

步骤	目标	特性	原因
47	Z01, Z03, D01, A03, A08, Z03.8, U01, Z01.10	plain_primitives, many_sessions	访问令牌是在 NRF 与 AF 共享的密钥下，对（subject、audience、scope）计算的 MAC；通知路径是每个端点各自的私有通道；没有使用其他代数。所询问的性质要求覆盖消费者和 AF 的任意数量会话，ProVerif 能够覆盖这一点；但 AF 是一条每个进程实例对应一个订阅的链，而不是一张表，因此模型无法在任意后续请求之间保留订阅记录。
47	R03, S05	changing_state	两个目标都依赖于 AF 的 Training Subscription 记录：该记录由 POST 创建，其 notifUri 和 notifCorreId 由 PUT/PATCH 替换，并由 DELETE 删除。ProVerif 对此类值的存储只会增长（一张表）或以不确定结束（私有通道上的单元格），因此无法为任意数量的请求建模删除和替换；这两个目标记录的答案仅基于 model.pv，且为 undecided，因为本次会话中未产出 AF 的有界展开和状态审查。
65	Z01, Z01.10	changing_state	Z01 的删除主张和 Z01.10 的两个主张都依赖于 AF 的 Training Subscription 记录，该记录会被创建、替换和删除；这些主张在 bounded.pv 上得到回答，其中该记录被展开为三步（创建、更新、删除），而持有它的 AF 是一串进程宏。该界遗漏的是对同一记录的第四次或更晚的请求，以及两个订阅的任何交错。

分析者的结语

两个授权性质不成立，通知性质成立。已证明：AF 仅凭 NRF 为发起请求的消费者签发的令牌才执行创建和更新，并且在展开模型上，删除也是如此；每条通知都发往其订阅中登记的 notifUri 并使用其中登记的 notifCorreId，适用于任意数量的会话；消费者只接受 AF 发送的通知，每条都对应一次不同的发送；201 Created 会回显其提交的 TrainEventsSubsc。已攻击：第二个合法的 NF 消费者仅凭自己的 naf-train 令牌和另一个消费者的 Individual Training Subscription URI，对该订阅发送 PUT，AF 因仅依据服务级 scope 进行授权而执行了该请求，随后受害者的培训报告被投递给第二个 NF；用同一令牌，它删除了该订阅。这就是发现：一个弱点，两条攻击轨迹；新颖性不明确（文稿陈述了单一服务 scope，但从未说明其后果），并且 depends_on_ambiguity 针对订阅 URI 可知这一假设。未决：重试的创建是否会产生第二个订阅（仅在 reachability 层面得到回答），以及删除被应用时在途通知会发生什么。局限：关于订阅记录的一切仅针对三个展开步骤得到回答，没有任何证明带有对照变体，推荐的修复——将订阅绑定到其创建者的令牌 subject，并在 PUT、PATCH 和 DELETE 上检查——未在模型上验证。Tamarin+ Agent 按记录和代数的原样建模，将解决重试、删除后顺序问题并检查该修复。