AF VFL 客户端推理 API 的安全性分析

本报告的其他语言版本：English。

19.2.0 · ProVerif+ 智能体报告

文稿	5G System; Application Function Artificial Intelligence/Machine Learning (AI/ML) Services; Stage 3（协议定义）
检查的性质	15 条：12 条成立，3 条不成立（5 个攻击）
发现	2

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_VFLInference 服务将充当 VFL 客户端的可信应用功能（AF）暴露给网络数据分析功能（NWDAF）；当 AF 不可信时，则暴露给网络暴露功能（NEF）。AF 持有一个预训练模型，并针对消费者请求的分析事件生成 VFL 推理结果。参与方包括消费者、AF，以及作为 OAuth2 授权服务器的网络存储库功能（NRF）。消费者为 AF 及其 naf-vflinference 范围获取访问令牌，使用 notifUri、notifCorrId 和分析事件描述进行订阅，并收到带有新订阅 URI 的 201 Created；随后它可以更新该订阅，并用它取消订阅。AF 将每个已订阅的推理事件连同 notifCorrId 和 vflInferResults 通知到该订阅的 notifUri，消费者存储该通知并应答 204。交互结束后，消费者持有属于其自身订阅的结果，这些结果来自它所选择的 AF 实例；AF 则持有一个订阅，其所有者已经过 TLS 认证，并已通过令牌授权。除了令牌的范围之外，交互中没有任何内容将订阅与其所属的消费者绑定，也没有任何内容让任一方识别出重复的请求。

参与方：

- **NWDAF**：NF 服务消费者，VFL 服务器。持有：NF 身份、OAuth2 客户端凭据。
- **AF**：可信 AF，VFL 客户端。持有：NF 实例身份、预训练模型。
- **NRF**：OAuth2 授权服务器。持有：令牌签名密钥、NF 配置文件。

图 1 展示了文稿所规定的交互。

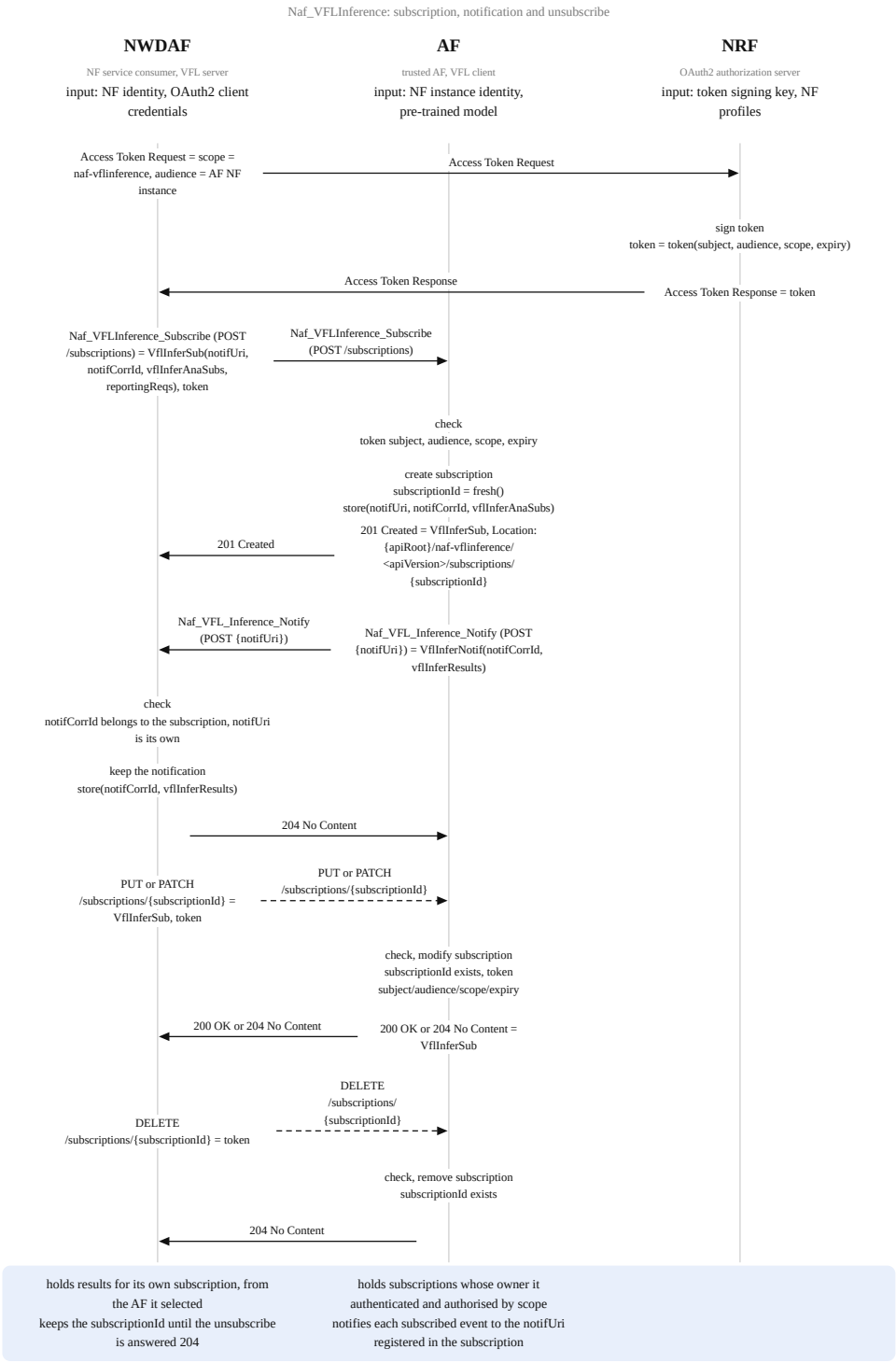


图 1. 所规定的协议。

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

本次分析有 2 项发现：以下内容并未在文稿中陈述。其中 2 项，文稿是否陈述了它们并不明确。

通知路径是健全的：消费者只接受来自其所选 AF 实例的、属于其自身订阅的结果，并且每条通知的 notifCorrId 和 notifUri 都来自同一个已存储的订阅；令牌机密性、其主体和受众绑定，以及用户标识符的机密性，在面对网络时均成立。资源路径则不然：该 API 只有一个服务级范围，且不要求检查请求者是否拥

有某个 subscriptionId，因此任何持有有效令牌且知道某个 subscriptionId 的 NF 都能替换或删除另一个消费者的订阅，而被替换的 notifUri 会把受害者的推理结果发送给攻击者。任何地方都没有重复检测：重放的通知会被接受并存储两次，重放的订阅请求会创建第二个订阅，重放的 DELETE 会再次被应答 204；在保留订阅状态的情况下，取消订阅只应用一次，之后不再接受任何通知。有两个结果依赖于一个界（一个订阅展开为三步），而所有结果都依赖于 TLS 端点认证和对称 OAuth2 令牌，因此这些保证的强度取决于这些假设，并且可信 AF 本身被假定为诚实的。

攻击图使用图 1 的列。红色表示攻击者的行为。黄色标记某一方发送的消息，尽管所规定的交互在该时间点并没有这条消息，以及攻击所破坏的结果。

2.1 任何具有服务范围的 NF 都能替换或删除另一个消费者的订阅

类型	协议规范本身的弱点
是否新发现	不明确：文稿只写了一部分，或没能检索
价值	高
涉及的性质	A08（见第 3 节）
依据	ProVerif 攻击查询 `a08_upd_own`、`a08_del_own`；图 2

发生了什么。 规范为整个服务定义了一个范围，没有资源级或操作级的范围，并且不要求检查 PUT、PATCH 或 DELETE 的请求者是否拥有该 subscriptionId。因此，任何持有 naf-vflinference 令牌且知道某个 subscriptionId 的 NF 都能替换或删除另一个消费者的订阅。模型中的 AF 会检查令牌的主体、受众、范围和有效期，但仍然接受该操作，因为原文中没有任何内容将 subscriptionId 与其所有者绑定。

攻击者需要什么。 攻击者是一个持有自身凭据和 naf-vflinference 范围令牌的合法 NF。它必须知道受害者的 subscriptionId，该值会在请求的资源 URI 和 Location 头中传递，因此中间节点或日志可以将其泄露。

攻击者能得到什么。 攻击者替换另一个消费者订阅的已注册 notifUri 和已订阅的分析，于是 AF 将该消费者的 vflInferResults 发送到攻击者的回调；或者它删除该订阅，消费者便不再收到结果，却仍然认为自己处于订阅状态。

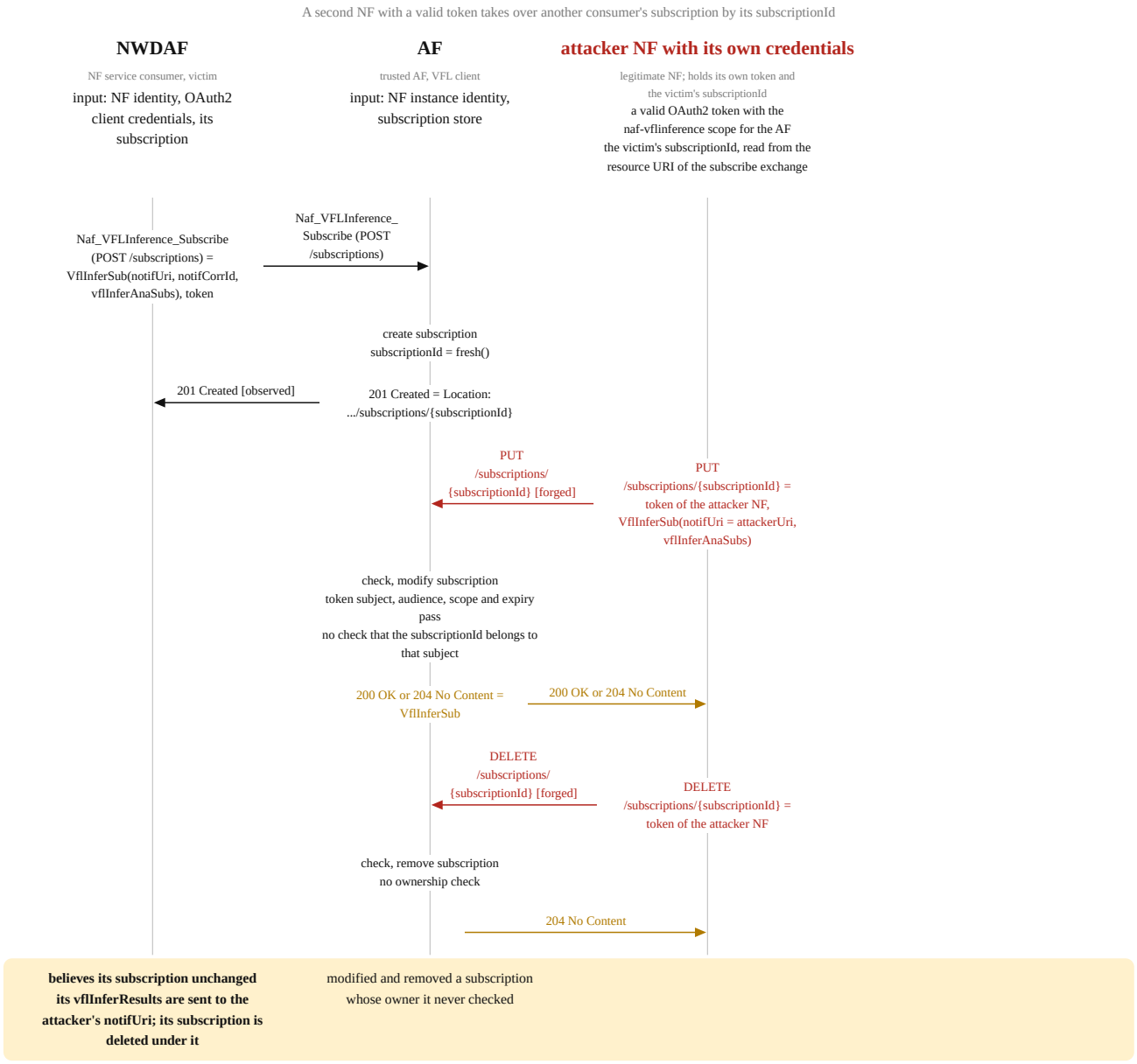


图 2. 第二个持有有效令牌的 NF 通过 subscriptionId 接管另一个消费者的订阅。性质 A08；攻击查询 a08_del_own、a08_upd_own。

拟议修改。 要求 AF 在 PUT、PATCH 和 DELETE 时检查 subscriptionId 是否属于所出示访问令牌的主体所对应的 NF 实例，否则应答 403；用于通知的 notifCorrId 和 notifUri 只从已存储的订阅中获取。

用 ProVerif 复核。 该修改被放入模型的一个副本中：在 PUT、PATCH 和 DELETE 时，AF 应检查 subscriptionId 是否属于所出示访问令牌的主体所对应的 NF 实例（已存储的订阅必须将请求者列为其消费者），否则应答 403（或 404）。在修改后的模型上，ProVerif 证明了 `a08_upd_own`、`a08_del_own`：该攻击在那里不再可能。协议的正常流程仍然能够被找到。其余 16 条已记录的答案保持不变。这是对模型的初步检查：它表明该修改在那里消除了此攻击，而不是表明它不会引入其他问题。修改后的模型：`records/fixes/0044-fix-owner.pv`。

2.2 重放的通知以及重放的订阅和删除请求会被再次接受

类型	协议规范本身的弱点
是否新发现	不明确：文稿只写了一部分，或没能检索
价值	中
涉及的性质	R02, R03（见第 3 节）
依据	ProVerif 攻击查询 `r02_once`、`r03_once_sub`、`r03_once_del`；图 3 和图 4

发生了什么。 被捕获的通知 POST 可以再次投递，消费者会第二次接受并存储它；被捕获的订阅 POST 会创建第二个订阅资源；被捕获的 DELETE 会被接受两次。无论是消息还是接收方所规定的行为，都不携带任何能区分重复请求与新请求的值，消费者也没有任何状态可以拒绝它已经消费过的通知。

攻击者需要什么。 只需要网络：攻击者保存并重新发送它已经见过的消息，而它重新发送的每条消息都是 AF 或消费者此前接受过的。

攻击者能得到什么。 重复的通知会被处理并存储两次，重复的订阅会留下一个带有自身 subscriptionId 的第二个订阅资源，于是消费者为同一个分析事件被计费两次，结果也被投递两次；重复的删除会为一个已不存在的资源再次得到 204。

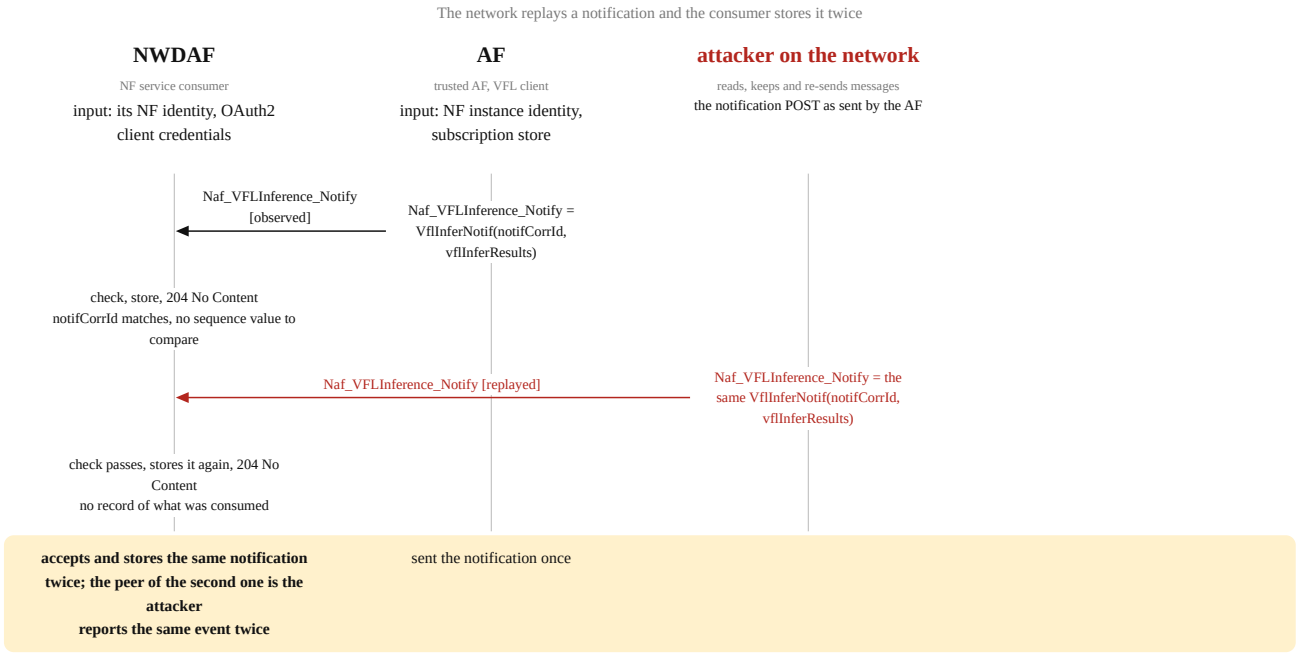


图 3. 网络重放一条通知，消费者将其存储两次。性质 R02；攻击查询 r02_once。

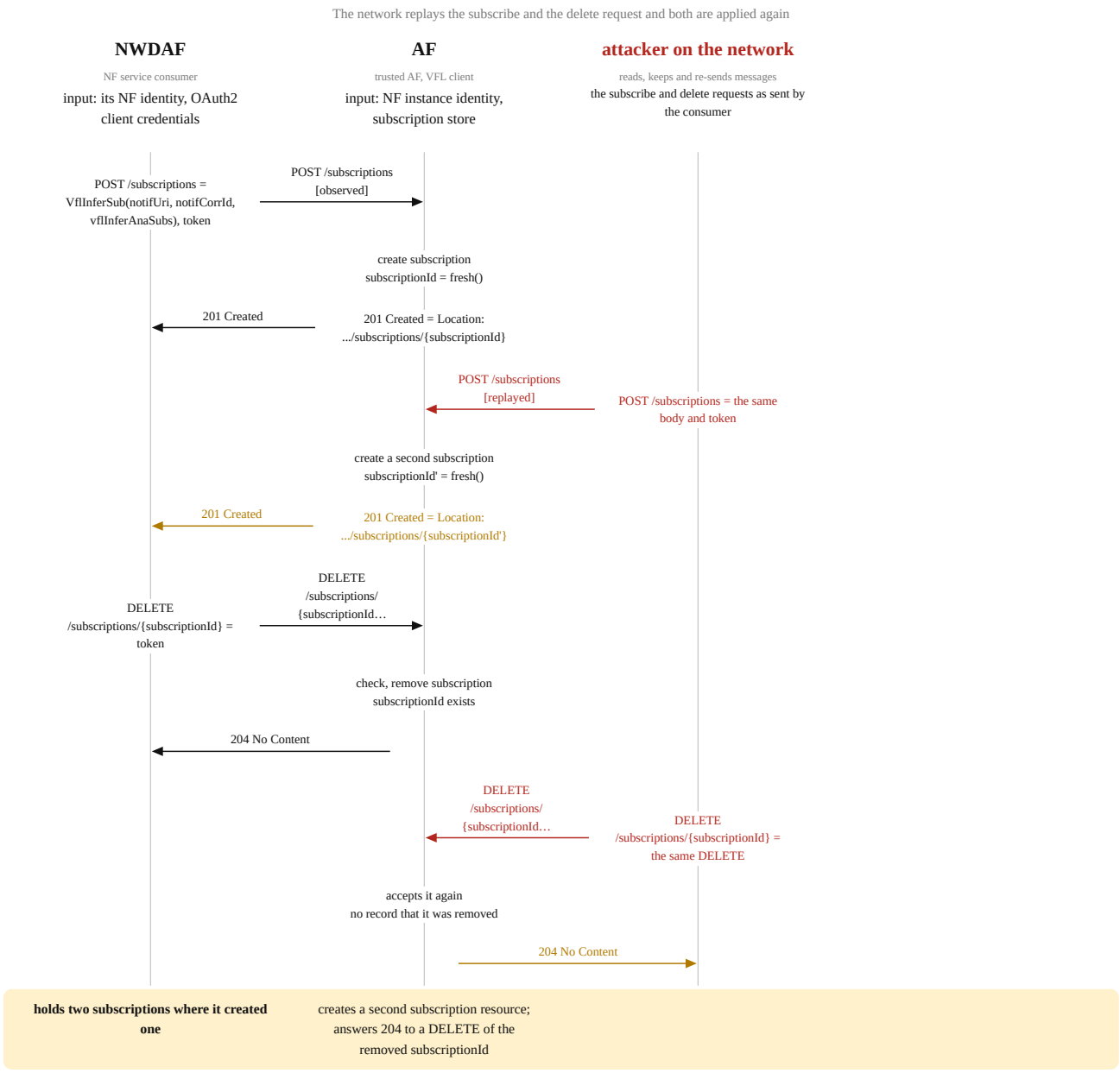


图 4. 网络重放订阅请求和删除请求，两者都被再次应用。性质 R03；攻击查询 r03_once_del、r03_once_sub。

拟议修改。 为通知 POST 提供一个值，使消费者能够识别重复，例如在 VflInferNotif 中为每个订阅设置一个通知计数器，由消费者与其最后接受的值进行比较；规定 AF 拒绝其 notifCorrId 已有订阅的订阅请求，并且对已移除的 subscriptionId 的 DELETE 应答 404。

用 ProVerif 复核。 未检查：该修改增加了一个由 AF 为每条通知递增、由消费者比较的值，因此其模型是一个在运行过程中会变化的值；ProVerif 只能将这样的值保存在 bounded.pv 的展开链中，该链覆盖一个订阅和三个步骤，因此检查只会对那一个订阅的前几条通知显示结果——这与两个有界结果已经携带的界相同。原文没有定义这样的字段，因此计数器、其范围（按订阅还是按消费者）以及拒绝规则都将由该建议发明，而对一条发明出来的规则建模并不能检查原文。

未给出针对一项发现的这些攻击的图：R02: r03_once_del, R02: r03_once_sub, R03: r02_once。

3 检查过的性质

每一行都是一条提交给 ProVerif 的性质。结果是 ProVerif 对分析者所建协议模型的回答；价值以及文稿是否已经写明该结果，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
A02	**请求与通知真实性。** 每当 AF 接受一个来自消费者 C 的订阅/更新/退订请求，或消费者接受一个来自 AF 的通知时，声称对端确实以本方身份运行过对应操作。	无	成立	低	否
A03	**通知匹配匹配运行。** 每当消费者接受一个通知，存在一个匹配的 AF 运行，其 notifCorrId、notifUri 与订阅内容一致；每当 AF 接受一个订阅/更新请求，存在匹配的消费者运行。	无	成立	中	否
A08	**操作绑定到自身 subscriptionId。** 每次对 Individual VFL Inference Subscription 的更新/部分更新/删除都作用于请求方自己创建的 subscriptionId，每次通知都发往该订阅登记的 notifUri 且携带对应 notifCorrId。	无	不成立（2 个攻击）	高	不明确
Z01	**需要有效作用域令牌。** 每次订阅创建、更新、部分更新、删除或通知提交，都必须有授权服务器签发的、覆盖 naf-vflinference scope 的有效令牌。	无	成立	中	否
Z03	**令牌绑定到主体和受众。** 一个为某消费者、某 AF 受众签发的令牌，不能被用来对另一消费者的订阅执行操作，也不能被用于另一 AF 实例。	无	成立	中	是
Z04	**删除订阅停止通知。** 一个订阅被删除之后，AF 不再针对该 subscriptionId 发出通知；一个订阅被更新之后，通知按更新后的内容发出。	无	在界内成立（变化的值展开到 3 步）	中	否
S05	**取消订阅后无通知。** 退订生效之后，旧的 subscriptionId 与 notifUri 组合不能再触发新的通知。	无	在界内成立（变化的值展开到 3 步）	中	否
S04	**通知字段来自同一订阅。** 每个通知所携带的 notifCorrId 与所发往的 notifUri，都来自同一订阅在其创建或更新阶段登记的值。	无	成立	低	否
R02	**通知最多接受一次。** 同一逻辑通知实例（同一 notifCorrId 与同一 vflInferResults）至多被消费者接受一次。	无	不成立（1 个攻击）	中	不明确
R03	**订阅和取消订阅仅应用一次。** 同一逻辑订阅创建请求至多产生一个订阅资源；同一逻辑退订请求至多删除一次。	无	不成立（2 个攻击）	中	不明确
K02	**结果与其他 NF 隔离。** vflInferResults 与订阅中的用户标识属性只对订阅的消费者与 AF 可见，其他 NF 或外部攻击者不能获得。	无	成立	中	是
K01	**访问令牌与其他 NF 隔离。** OAuth2 访问令牌只对签发它的授权服务器、持有它的消费者与校验它的 AF 可见，其他实体不能推导出它。	无	成立	中	是
U01	**结果匹配订阅请求。** 消费者接受的推理结果对应本次订阅所请求的输入样本与模型版本。	无	成立	低	否
U02	**通知来自选定 AF。** 消费者接受的通知来自所选 AF，且属于该消费者自己的订阅。	无	成立	中	否
Q3	**取消和更新后的订阅状态。** 取消与更新订阅后的有限状态行为及错误响应处理。	无	在界内成立（变化的值展开到 3 步）	中	否

提出的问题及分析者的回答：

问题	回答	依据
Q1: 输入样本/模型版本与推理结果的相关性	消费者接受的结果，恰好是 AF 为具有该 notifCorrId、notifUri 和分析描述的订阅所生成的那些结果；原文中没有结果里指明样本或模型版本的字段，因此问题的这一部分无法从这些原文单元回答，留给 TS 29.520 的 VflInferResult 结构处理。	U01, A03
Q2: 通知来自所选 AF 的认证与跨会话隔离	只有当通知由消费者所订阅的 AF 实例生成、且属于消费者自己创建的具有相同 notifCorrId、notifUri 和内容的订阅时，它才会被接受，因此一个会话不会与另一个会话混淆；第二个 AF 实例不能向未选择它的消费者发通知。	U02, A02, A03
Q3: 取消/更新的有限状态行为与错误响应处理	在保留订阅状态的情况下，订阅通过 PUT 修改、通过 DELETE 删除，重复的 DELETE 会被拒绝，退订返回 204 之后不再接受该订阅的通知；失败路径本身没有被建模，而且原文允许错误应答不带正文，因此对于错误响应会泄露什么，不作任何结论。	Q3, Z04, S05, R03

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和检查给出了或未能给出什么，其中密码学被视为理想的，而不涉及任何实现。

分析者指出，本分析不覆盖以下内容：

- TLS 被建模为每个端点一把密钥：模型不证明 TLS 握手、证书或密码套件的任何东西，并且假定每条消息都能到达其中指定的端点。
- OAuth2 被建模为 NRF 与 AF 之间共享的一把令牌签名密钥；TS 29.510 和 TS 33.501 中的令牌格式、内省和吊销没有被建模。
- 时间被冻结在某一瞬间，因此令牌的过期检查没有被测试：在这个模型中，过期的令牌无法与有效令牌区分开。
- PATCH 没有被单独建模；它走与 PUT 相同的接受路径，并且只有 bounded.pv 允许 PUT 改变已存储的订阅。
- model.pv 把订阅保存在一张单调表中，因此在那里观察不到删除；订阅生命周期的顺序性质在 bounded.pv 上回答，后者把一个订阅展开到三步。
- 用户标识（supis、gpsis、组标识）对每个 AF 都是一个不透明的值；TS 29.520 中 VflInferSub 与 VflInferResult 的结构，以及样本和数值算法，都在模型之外。
- 通知是通过 TLS 发往 notifUri 的一条消息；HTTP 事务、SCP 重定向以及 AF 中的任何存储转发都没有被建模。
- 控制 AF 或读取其所存内容的攻击者被假定不存在：任务固定了可信 AF，其诚实性是这里每一条结果的前提。

宿主记录的内容：

- Z04、S05、R02、R03、Q3 的答案依赖于模型简化的一个操作（附录 D）。
- 没带对照查询的证明（附录 C）：A02: a02_req, A02: a02_notif, A03: a03_bind, A08: s04_notif_uri, Z01: z01_sub, Z01: z01_upd, Z01: z01_del, Z03: z01_sub, Z04: b_notif_created, S04: s04_notif_uri, U01: a02_notif, U02: a03_bind, Q3: b_notif_created。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。

每条性质还有什么悬而未决，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，而不是证明器的回答：这些回答对协议意味着什么，解读依据什么，它能否按现状使用，以及它有多大价值。

A02: 请求与通知真实性

每当 AF 接受一个来自消费者 C 的订阅/更新/退订请求，或消费者接受一个来自 AF 的通知时，声称对端确实以本方身份运行过对应操作。

AF 只接受来自 TLS 会话和令牌所指明的 NF 实例的订阅，消费者只接受来自其所选 AF 实例的、针对其自己创建的订阅的通知。因此，只要 TLS 按模型假定的方式认证端点，每一方都知道自己在和谁通信。

- 结果：成立；回答了所问：是；可在有保留的情况下使用
- 价值低：它确认的是 SBI 基线已经要求、也没有读者怀疑的东西；它的价值在于其他结果都依赖于它。
- 文稿中已写明：否
- 依据：TLS 端点认证是被假定的，而非被证明的：模型给每个端点一把其对端也能推导出的私钥，并且不证明握手的任何东西。；令牌是由 NRF 用与 AF 共享的密钥签名的项；令牌内省和吊销在模型之外。

A03: 通知匹配匹配运行

每当消费者接受一个通知，存在一个匹配的 AF 运行，其 notifCorrId、notifUri 与订阅内容一致；每当 AF 接受一个订阅/更新请求，存在匹配的消费者运行。

消费者接受的通知总是对应于 AF 为该消费者创建的订阅，notifCorrId、notifUri 和分析描述都相同。这种对应关系成立，是因为 AF 从已存储的订阅中取这两个值，而消费者将其与自己的值进行比较。

- 结果：成立；回答了所问：是；可在有保留的情况下使用
- 价值中：它是整条通知路径所依赖的绑定，是被证明的而不是被假定的；它随模型的 TLS 抽象一同成立或失败。
- 文稿中已写明：否
- 依据：AF 从已存储的订阅中取 notifCorrId 和 notifUri；改变它们的 PUT 只在 bounded.pv 中生效。；TLS 端点认证是被假定的。

A08: 操作绑定到自身 subscriptionId

每次对 Individual VFL Inference Subscription 的更新/部分更新/删除都作用于请求方自己创建的 subscriptionId，每次通知都发往该订阅登记的 notifUri 且携带对应 notifCorrId。

通知侧是健全的：AF 向订阅中登记的 notifUri 发送通知，并携带其 notifCorrId。资源侧则不健全：AF 只检查请求方持有具有服务级范围的令牌，因此任何知道某个 subscriptionId 的 NF 都能替换或删除另一消费者的订阅，而替换之后其结果会被发往别处。

- 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：它暴露了 Rel-19 API 资源模型中的一个缺口：令牌范围授权的是服务，而不是资源，一个 subscriptionId 就足以接管另一消费者的订阅。文稿没有说这是安全的。
- 文稿中已写明：不明确。所依据的原文：s0044, s0082, s0190, s0218, s0291

- 依据：AF 不执行所有权检查，因为原文没有规定这样的检查；唯一的证明是 s0291 为整个服务定义了单一范围。；攻击者拥有自己的凭据并知道一个 subscriptionId；模型不判定在部署中是否可能获知 subscriptionId。
- 悬而未决：subscriptionId 对消费者是否保密：原文从未说明，而这决定了该攻击在部署中是否可达。

Z01: 需要有效作用域令牌

每次订阅创建、更新、部分更新、删除或通知提交，都必须有授权服务器签发的、覆盖 naf-vflinference scope 的有效令牌。

AF 接受的每次订阅、更新和删除，都由 NRF 为该消费者、为该 AF 实例签发的令牌作为依据，该令牌带有 naf-vflinference scope 和当前有效期。检查的强度等同于令牌项与 NRF 所签内容相等，模型将这一点赋予 AF。

- 结果：Holds；所问是否得到回答：是；可用但有保留
- 价值 中：它表明，一旦 AF 校验令牌，API 的 OAuth2 访问控制对网络就是可靠的；而源文将令牌校验设为可选（may be authorised），因此该结果仅在部署了 OAuth2 的地方成立。
- 文稿中是否陈述：否
- 依据：NRF 用一个与 AF 共享的私名密钥签发令牌；模型只有一个时刻，因此有效期仅作为值来比较。；受众位于受保护的令牌请求内部；中间节点篡改的令牌请求不在考虑范围内。
- 待解决：令牌的有效期被冻结在一个时刻，因此使用过期令牌的操作未被测试。
- 下一步：用两种令牌变体对令牌有效期建模，由 AF 与当前时刻比较，以测试有效期检查。

Z03: 令牌绑定到主体和受众

一个为某消费者、某 AF 受众签发的令牌，不能被用来对另一消费者的订阅执行操作，也不能被用于另一 AF 实例。

令牌只在为其签发的 AF 实例处、为其签发的消费者被接受，因为 AF 将令牌与 NRF 为其自身身份和请求消费者所签的确切项进行比较。OAuth2 无法提供的是出示令牌的客户端与其被签发给的客户端之间的联系，模型通过 TLS 会话提供这一点。

- 结果：Holds；所问是否得到回答：部分；可用但有保留
- 价值 中：受众和主体绑定已为该 API 证明，而使它成为必要的限制由 RFC 6749 陈述，因此该结果是机械展示的已知边界。
- 文稿中是否陈述：是。文稿中何处陈述：rfc6749:2879, s0288, s0289, s0291
- 依据：主体和受众绑定依赖于标识消费者的 TLS 会话，而非仅依赖令牌，正如 RFC 6749 指出，它没有给资源服务器提供进行该检查的方法。；模型只有一个 NRF 密钥和一个时刻。
- 待解决：主张中关于另一消费者订阅的部分由对操作的攻击来回答，而非由令牌回答：见 A08。

Z04: 删除订阅停止通知

一个订阅被删除之后，AF 不再针对该 subscriptionId 发出通知；一个订阅被更新之后，通知按更新后的内容发出。

在保留订阅状态的情况下，AF 只对其持有的订阅发出通知，其在 PUT 之后的通知携带修改后的分析描述，而在 DELETE 的 204 之后，消费者不再接受该 subscriptionId 的任何内容。因此，得到应答的退订会停止通知，这正是模型展开的三步。

- 结果：在界内 Holds（变化值展开到 3 步）；所问是否得到回答：是；可用但有保留

- 价值 中：它以经过检查的模型回答了源文未确定的顺序问题，而对照查询表明该性质依赖于状态被保留。
- 文稿中是否陈述：否。所依据的源文：s0083, s0084, s0085
- 依据：bounded.pv 将一个订阅展开到三步：一次订阅、一次 PUT 和一次 DELETE；它不覆盖第二个订阅、PATCH 或失败应答。；假设消费者在收到 204 时丢弃其本地订阅；源文只说 AF 移除资源。
- 待解决：AF 是否可能在 204 之后、移除完成之前对其已移除的订阅发出通知：展开的模型没有这样的窗口。

S05: 取消订阅后无通知

退订生效之后，旧的 subscriptionId 与 notifUri 组合不能再触发新的通知。

在退订得到应答之后，一旦 AF 将订阅作为状态持有且消费者在 204 时丢弃它，旧的 subscriptionId 与 notifUri 组合不会产生消费者接受的任何通知。没有该状态时，同一通知会被再次接受，正如对照运行所示。

- 结果：在界内 Holds（变化值展开到 3 步）；所问是否得到回答：部分；可用但有保留
- 价值 中：它将源文的退订与消费者所需的状态区分开来，而源文并未规定该状态。
- 文稿中是否陈述：否。所依据的源文：s0083, s0084, s0085
- 依据：结果是有界的：三个展开步骤和一个订阅。；将通知重发给不保留状态的消费者的攻击者仍会被接受；那就是重放结果，并不是本目标的区别。
- 待解决：移除订阅但保留重试或缓存的 AF 是否会再通知一次；源文对此只字未提。

S04: 通知字段来自同一订阅

每个通知所携带的 notifCorrId 与所发往的 notifUri，都来自同一订阅在其创建或更新阶段登记的值。

AF 发送的每个通知都携带一个订阅的 notifCorrId，并发送到同一订阅中登记的 notifUri，因此同时检查两者的消费者不会被递送另一订阅的通知。该绑定是结构性的：两个值都从同一存储行读取。

- 结果：Holds；所问是否得到回答：是；可用
- 价值 低：它确认的是资源定义的结构性性质，而非协议的安全决策。
- 文稿中是否陈述：否
- 依据：订阅被存储为一行，通知由该行构建；模型没有缓存，也没有重试队列。；改变 notifUri 的 PUT 仅在 bounded.pv 中应用。
- 待解决：PATCH 之后 AF 从何处取得 notifUri：PATCH 未单独建模。

R02: 通知最多接受一次

同一逻辑通知实例（同一 notifCorrId 与同一 vflInferResults）至多被消费者接受一次。

该主张不成立：通知不携带任何能区分重复与新事件的值，消费者也不保留其所消费内容的记录，因此网络重放一个通知，消费者便接受并存储它两次。这是源文未定义的状态，而非模型缺少检查。

- 结果：Fails（1 个攻击）；所问是否得到回答：是；可用
- 价值 中：它机械地表明，一次性或周期性通知可被弄成到达两次，而正缺少序列值这一点正是编辑者必须修正的。
- 文稿中是否陈述：不明确。所依据的源文：s0095, s0096, s0097, s0098

- 依据：消费者接受 notifCorrId 和 notifUri 与其订阅匹配的通知，正如 s0096 和 s0098 的 204 所暗示，仅此而已。；该攻击只需要网络。
- 待解决：是否要求消费者实现检测重复；源文并未说它不要求。

R03: 订阅和取消订阅仅应用一次

同一逻辑订阅创建请求至多产生一个订阅资源；同一逻辑退订请求至多删除一次。

没有状态时两个主张都不成立：重放的订阅 POST 会创建带有自己 subscriptionId 的第二个订阅资源，重放的 DELETE 被接受并再次应答 204。在将订阅作为状态保留的情况下，AF 接受移除一次，这正是 bounded.pv 所示。

- 结果：Fails（2 个攻击）；所问是否得到回答：部分；可用但有保留
- 价值 中：它给出了 API 所容许的确切重复，并展示了订阅状态能带来什么，这正是编辑者制定幂等规则所需的。
- 文稿中是否陈述：不明确。所依据的源文：s0043, s0044, s0084, s0085
- 依据：bounded.pv 展开一个订阅；重复订阅在 model.pv 上展示，那里订阅从不被移除。；模型中的 AF 从不拒绝重复，这与未定义幂等键的源文一致。
- 待解决：AF 对已移除 subscriptionId 的 DELETE 应答什么：源文未说明，模型也不回答。

K02: 结果与其他 NF 隔离

vflInferResults 与订阅中的用户标识属性只对订阅的消费者与 AF 可见，其他 NF 或外部攻击者不能获得。

在交换过程中，网络和另一 NF 都不会得知用户标识或推理结果；结果只在消费者的 TLS 会话内传输，并由一个 AF 从不以明文发送的用户标识计算得出。妥协运行表明该性质并非空洞：当 AF 泄露其所持有的内容时，标识便会被得知。

- 结果：Holds；所问是否得到回答：是；可用但有保留
- 价值 中：用户标识和结果对网络的机密性是构建该 API 的承诺；文稿在 TLS 和 OAuth2 原则层面而非针对这些字段陈述它，因此机械结果补充了确切条件。
- 文稿中是否陈述：是。文稿中何处陈述：rfc6749:2859, s0045, s0097, s0115, s0262
- 依据：假设整个交换具有 TLS 机密性；未给任何攻击者另一端点的密钥。；用户标识是每个 AF 一个不透明值，而不是订阅的 supis 或组标识符列表。
- 待解决：获得消费者 TLS 密钥的恶意 NF，模型并未赋予它这一能力。

K01: 访问令牌与其他 NF 隔离

OAuth2 访问令牌只对签发它的授权服务器、持有它的消费者与校验它的 AF 可见，其他实体不能推导出它。

访问令牌只有 NRF、消费者以及它所指向的 AF 知道；网络攻击者和其他 NF 永远看不到它。对照查询表明，该性质依赖于令牌在 TLS 内传输：一旦签名密钥泄露，攻击者就能构造令牌，该性质随即不成立。

- 结果：成立；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：这是 RFC 6749 所要求的机密性，已针对本 API 面向网络证明，保留条件是令牌方案为对称方案。
- 文稿中有无陈述：有。文稿中的位置：rfc6749:2859, rfc6749:2870, s0288, s0289
- 依据：令牌由 NRF 与 AF 共享的对称密钥签名，因此 AF 能看到明文令牌；公钥方案或引用令牌方案未建模。；泄露场景的攻击者泄露的是签名密钥，而不是消费者存储的令牌。

- 未决：令牌从消费者存储中泄露的情形，模型未将其建模为攻击者。

U01: 结果匹配订阅请求

消费者接受的推理结果对应本次订阅所请求的输入样本与模型版本。

消费者接受的结果，恰好是 AF 针对具有该 correlation id、notifUri 和分析描述的订阅所计算出的结果，因此消费者不会拿到同一 AF 另一订阅的结果。结果是否与消费者请求的样本和模型版本绑定，无法向该原文单元提问，因为它不携带这类字段。

- 结果：成立；是否回答了所问：部分；可在有保留条件的情况下使用
- 价值低：它回答了所选原文单元能够承载的那部分问题，并准确指出了其余部分缺少什么。
- 文稿中有无陈述：无。所依据的原文：s0040, s0097, s0262
- 依据：AF 根据存储的分析描述计算结果；样本和模型版本是一个不透明的模型值。；假定 TLS 端点认证。
- 未决：结果是否标明其所依据的样本和模型版本：字段结构在 TS 29.520 中，不在所选原文单元范围内。

U02: 通知来自选定 AF

消费者接受的通知来自所选 AF，且属于该消费者自己的订阅。

消费者只接受来自其订阅所在 AF 实例的通知，且只接受针对其创建的订阅的通知；另一个获得相同请求的 AF 实例无法向该消费者发送通知。会话隔离来自按端点划分的 TLS 密钥以及通知中携带的 AF 身份。

- 结果：成立；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：它回答了消费者关于哪个 AF 在与自己通信的实际担忧，并隔离了会话；保留条件是 AF 身份是建模得到的，而非由规范字段携带。
- 文稿中有无陈述：无。所依据的原文：s0029, s0036, s0095
- 依据：通知在模型中携带 AF 身份；原文在通知体中未定义 AF 身份字段，因此模型补充了 TLS 和 URI 本应携带的内容。；假定 TLS 端点认证。

Q3: 取消和更新后的订阅状态

取消与更新订阅后的有限状态行为及错误响应处理。

在保留订阅状态的情况下，AF 在 PUT 时修改订阅、通知修改后的内容、在 DELETE 时删除订阅并作出应答，重复的 DELETE 会被拒绝；在 204 之后，消费者不再接受任何通知。因此，在展开运行中，有限状态在两侧之间保持一致，原文除此之外未作任何规定。

- 结果：在界内成立（变化值展开到 3 步）；是否回答了所问：部分；可在有保留条件的情况下使用
- 价值中：它给出了规范所隐含的状态机，并把有状态时成立的内容与原文未作要求的内容区分开来。
- 文稿中有无陈述：无。所依据的原文：s0192, s0205, s0218, s0275
- 依据：bounded.pv 展开了一个订阅的三步，且未建模 PATCH、重试或失败应答。；消费者在收到 204 后丢弃订阅，尽管原文并未要求它这样做。
- 未决：错误应答：403、404 和 29.500 的各类码未建模，因此对拒绝会泄露什么没有任何说明。

附录 C：主张和证明器的答案

证明器为每个目标记录的内容：达到的级别、达到该级别的查询、是否检查了对照，以及各次攻击及分析者对每次攻击的判定。

目标	级别	界	查询	对照	攻击	主张
A02	proved		a02_req			2 proved
A03	proved		a03_bind			1 proved
A08	proved		s04_notif_uri		a08_upd_own (holds_in_source); a08_del_own (holds_in_source)	1 proved, 2 attack
Z01	proved		z01_sub			3 proved
Z03	proved		z01_sub			1 proved
Z04	bounded	变化值展开到 3 步	b_notif_created	1 of 2		2 bounded
S05	bounded	变化值展开到 3 步	b_afterdel	checked		1 bounded
S04	proved		s04_notif_uri			1 proved
R02	none				r02_once (holds_in_source)	1 attack
R03	bounded	变化值展开到 3 步	b_del_once	checked	r03_once_sub (holds_in_source); r03_once_del (holds_in_source)	1 bounded, 2 attack
K02	proved		k02_secret	checked		1 proved
K01	proved		k01_secret	checked		1 proved
U01	proved		a02_notif			1 proved
U02	proved		a03_bind			1 proved
Q3	bounded	变化值展开到 3 步	b_notif_created			1 bounded

逐条主张，按分析者对每条主张的措辞给出；每条的答案即为证明器的答案：

目标	主张	攻击者	回答	查询	对照
A02	AF 只接受来自请求中所携带身份对应的 NF 服务消费者的订阅请求：AF 创建的每个订阅都对应一个该消费者实际发送过的订阅请求。	`network`	proved	a02_req	none
A02	消费者只接受由其选定的 AF 产生的通知，且 notifCorrId、notifUri 以及 results 与该 AF 为该订阅发送的内容一致。	`network`	proved	a02_notif	none
A03	消费者接受的每个通知都对应 AF 为该消费者创建的订阅，且 notifCorrId、notifUri 和 vflInferAnaSubs 一致。	`network`	proved	a03_bind	none
A08	AF 为某个订阅发送的每个通知都发送到该订阅中注册的 notifUri，并携带其 notifCorrId。	`network`	proved	s04_notif_uri	none
A08	对 Individual VFL Inference Subscription 的 PUT 只作用于请求者自己创建的 subscriptionId。攻击者除网络之外还拥有自己的有效 NF 凭据以及带有 naf-vflinference scope 的令牌，并且能从资源 URI 中得知其他消费者的 subscriptionId。	`uri_reader`	attack (holds_in_source)	a08_upd_own	

目标	主张	攻击者	回答	查询	对照
A08	DELETE 只作用于请求者自己创建的 subscriptionId。攻击者拥有自己的有效 NF 凭据和 scope 令牌，并且能从资源 URI 中得知其他消费者的 subscriptionId。	`uri_reader`	attack (holds_in_source)	a08_del_own	
Z01	只有请求携带了 NRF 为该消费者和该 AF 实例签发的、具有 naf-vflinference scope 且未过期的令牌时，才会创建订阅。	`network`	proved	z01_sub	none
Z01	只有请求携带了 NRF 为该消费者和该 AF 实例签发的、具有 naf-vflinference scope 且有效期有效的令牌时，才会接受 PUT。	`network`	proved	z01_upd	none
Z01	只有请求携带了 NRF 为该消费者和该 AF 实例签发的、具有 naf-vflinference scope 且有效期有效的令牌时，才会接受 DELETE。	`network`	proved	z01_del	none
Z03	令牌只会在为其签发的 AF 实例处、针对为其签发的消费者被接受：AF 接受某个操作意味着存在一个 NRF 签发的令牌，其 subject 为该消费者，其 audience 为该 AF 实例。	`network`	proved	z01_sub	none
Z04	只为 AF 仍然持有的订阅发送通知，且在接受的 PUT 之后，通知携带修改后的 vflInferAnaSubs。	`network`	bounded (the changing value unrolled to 3 steps)	b_notif_created	none
Z04	DELETE 应答 204 之后，消费者不再接受该 subscriptionId 的任何通知。	`network`	bounded (the changing value unrolled to 3 steps)	b_afterdel	checked
S05	退订被接受之后，旧的 subscriptionId 与 notifUri 组合不会触发任何消费者会接受的通知。	`network`	bounded (the changing value unrolled to 3 steps)	b_afterdel	checked
S04	AF 发送的每个通知都携带 notifCorrId，并发送到其创建的同一个订阅的 notifUri。	`network`	proved	s04_notif_uri	none
R02	同一个逻辑通知，即具有相同 notifCorrId 和相同 vflInferResults 的通知，至多被消费者接受一次。	`network`	attack (holds_in_source)	r02_once	
R03	重复的订阅请求至多创建一个订阅资源。	`network`	attack (holds_in_source)	r03_once_sub	
R03	重复的退订请求至多删除一次。	`network`	attack (holds_in_source)	r03_once_del	
R03	在保留订阅状态的情况下，重放的 DELETE 会被拒绝：持有该订阅的 AF 只接受一次，资源状态记录该移除。	`network`	bounded (the changing value unrolled to 3 steps)	b_del_once	checked
K02	订阅的 vflInferResults 和用户标识对网络和其他 NF 保密：在通知被接受的过程中，攻击者学不到任何用户标识。	`network`	proved	k02_secret	checked
K01	OAuth2 访问令牌只有 NRF、为其签发的消费者以及其指向的 AF 知道；交换过程中其他 NF 和网络攻击者都学不到它。	`network`	proved	k01_secret	checked
U01	消费者接受的结果恰好是 AF 为具有该 correlation id、notifUri 和分析描述的订阅计算出的结果，因此结果绑定到所订阅的请求，而不绑定到原文未携带的样本或模型版本。	`network`	proved	a02_notif	none
U02	消费者只接受来自其订阅所在 AF 实例的通知，且只接受为其自己创建的订阅的通知。	`network`	proved	a03_bind	none

目标	主张	攻击者	回答	查询	对照
Q3	PUT 和 DELETE 之后的有限状态：AF 先修改再移除订阅，其应答反映该状态，而第二个通知只有在内容被修改后才被接受。	network	bounded (the changing value unrolled to 3 steps)	b_notif_created	none

附录 D：分析是怎么跑的

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

ProVerif+ Agent 会话 session-20261114T232417，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：48，证明器 5 s，实际耗时 14 min，费用 0.136 USD。

ProVerif：运行 91 个证明，91 个已判定，0 个无答案，3 s，记录 23 个回答。

分析了什么

协议	AF VFL client inference API
版本	19.2.0
分析范围	可信 AF 作为 VFL client，NWDAF server 直接调用 Naf_VFLInference；模型预先训练，一个推理请求/报告有界会话；不含 NEF、训练、数值算法。
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	336 numbered passages (155963 bytes) from the sections listed below. A reference such as s0001 in this report is one of these passages

分析所依据的文稿章节：

文稿	章节	标题
main	5.3	Naf_VFLInference 服务
main	5.3.1	服务描述
main	5.3.1.1	概述
main	5.3.1.2	服务架构
main	5.3.1.3	网络功能
main	5.3.1.3.1	应用功能 (AF)
main	5.3.1.3.2	NF 服务消费者
main	5.3.2	服务操作
main	5.3.2.1	引言
main	5.3.2.2	Naf_VFLInference_Subscribe 服务操作
main	5.3.2.2.1	概述
main	5.3.2.2.2	订阅 VFL 推理事件通知
main	5.3.2.2.3	更新事件通知订阅
main	5.3.2.2.4	部分更新事件通知订阅
main	5.3.2.3	Naf_VFLInference_Unsubscribe 服务操作

文稿	章节	标题
main	5.3.2.3.1	概述
main	5.3.2.3.2	取消订阅 VFL 推理通知
main	5.3.2.4	Naf_VFLInference_Notify 服务操作
main	5.3.2.4.1	概述
main	5.3.2.4.2	关于已订阅事件的通知
main	6.2	Naf_VFLInference 服务 API
main	6.2.1	引言
main	6.2.2	HTTP 的使用
main	6.2.2.1	概述
main	6.2.2.2	HTTP 标准头
main	6.2.2.2.1	概述
main	6.2.2.2.2	内容类型
main	6.2.2.3	HTTP 自定义头
main	6.2.3	资源
main	6.2.3.1	资源结构
main	6.2.3.2	资源：VFL 推理订阅
main	6.2.3.2.1	描述
main	6.2.3.2.2	资源定义
main	6.2.3.2.3	资源标准方法
main	6.2.3.2.3.1	POST
main	6.2.3.2.4	资源自定义操作
main	6.2.3.3	资源：单个 VFL 推理订阅
main	6.2.3.3.1	描述
main	6.2.3.3.2	资源定义
main	6.2.3.3.3	资源标准方法
main	6.2.3.3.3.1	GET
main	6.2.3.3.3.2	PUT
main	6.2.3.3.3.3	PATCH
main	6.2.3.3.3.4	DELETE
main	6.2.3.3.4	资源自定义操作
main	6.2.4	无关联资源的自定义操作
main	6.2.5	通知
main	6.2.5.1	概述
main	6.2.5.2	VFL 推理事件通知
main	6.2.5.2.1	描述
main	6.2.5.2.2	操作定义

文稿	章节	标题
main	6.2.6	数据模型
main	6.2.6.1	概述
main	6.2.6.2	结构化数据类型
main	6.2.6.2.1	引言
main	6.2.6.2.2	类型 VflInferSub
main	6.2.6.2.3	类型 VflInferSubPatch
main	6.2.6.3	简单数据类型与枚举
main	6.2.6.3.1	引言
main	6.2.6.3.2	简单数据类型
main	6.2.7	错误处理
main	6.2.7.1	概述
main	6.2.7.2	协议错误
main	6.2.7.3	应用错误
main	6.2.8	特性协商
main	6.2.9	安全
main	6.2.10	HTTP 重定向

协议的目的，按原文单元在文稿中的定位：可信 AF 作为 VFL client，NWDAF server 直接调用 Naf_VFLInference；模型预先训练，一个推理请求/报告有界会话；不含 NEF、训练、数值算法。

对照文稿定性质

在编写查询之前，分析者将起草的性质清单与文稿本身对协议目的的说明进行了对照。名称、性质所涉及的内容以及文稿的说法均属分析者的解读；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
A02	请求与通知真实性	AF 确信 subscribe/update/delete 请求来自它所声称的 NF 服务消费者；NF 服务消费者确信通知来自它选定的 AF。	该服务仅由 NWDAF（可信 AF）或 NEF（不可信 AF）消费，访问可能由 OAuth2 授权；SBI 基线要求消费者与生产者双向认证，并对每条传入消息进行校验；原文指出，除 TLS 和 OAuth2 之外没有消息级认证。	ts-33-501:2871, ts-33-501:2875, s0004, s0011, s0013, s0014, s0031, s0090, s0288, s0289
A03	通知匹配匹配运行	消费者接受的每条通知都对应消费者创建的一个订阅，notifCorrId、notifUri 和订阅内容均相同；AF 创建的每个订阅都对应一个消费者请求。	VflInferSub 消息体携带 notifUri、notifCorrId 和 vflInferAnaSubs（s0037-s0040）；通知携带 notifCorrId 和 vflInferResults，发往 {notifUri}（s0095-s0097）。原文没有用文字提出对应关系要求；它由资源描述隐含。	s0037, s0038, s0039, s0040, s0095, s0096, s0097
A08	操作绑定到自身 subscriptionId	对 Individual VFL Inference Subscription 的 PUT、PATCH 和 DELETE，以及为其发送的通知，都代表拥有该 subscriptionId 的消费者并面向该消费者执行。	资源 URI 携带 {subscriptionId}（s0044, s0082），且只存在服务级范围 naf-vflinference，资源级和操作级都没有范围（s0291）；原文不要求对 PUT/PATCH/DELETE 做所有权检查。	ts-33-501:2875, s0044, s0045, s0082, s0190, s0218, s0291

ID	简称	对象	文稿怎么说	出处
Z01	需要有效作用域令牌	AF 上的每次 subscribe、update、partial update、delete 和通知处理，都由 NRF 签发的令牌授权，该令牌具有 naf-vflinference 范围且尚未过期。	访问可使用 OAuth2 客户端凭据授权，由 NRF 作为授权服务器；消费者应在消费服务前获取令牌；该 API 只定义单一范围 naf-vflinference（s0288-s0291）。	rfc6749:2859, ts-33-501:2883, s0288, s0289, s0290, s0291
Z03	令牌绑定到主体和受众	为某个 NF 服务消费者和某个 AF 实例签发的令牌，不能被用来在另一个 AF 实例上操作，也不能操作另一个消费者的订阅。	令牌在消费服务前从 NRF 获取（s0288-s0290）；RFC 6749 指出，OAuth2 本身无法让资源服务器检查客户端出示的令牌确实是签发给该客户端的，这正是 SBI 基线必须通过受众和主体检查来弥补的缺口。	rfc6749:2879, ts-33-501:2885, s0288, s0289, s0291
Z04	删除订阅停止通知	某个 subscriptionId 的 DELETE 被接受后，AF 不再为其发送通知；PUT 或 PATCH 之后，通知遵循修改后的订阅。	DELETE 时 AF 删除订阅并返回 204（s0083-s0085）；PUT 和 PATCH 时它修改资源（s0190, s0197-s0209）。原文没有说明被删除的订阅何时停止产生通知。	s0083, s0084, s0085, s0190, s0200, s0201
S05	取消订阅后无通知	取消订阅被接受后，旧的 subscriptionId 与 notifUri 组合不能再触发新通知。	DELETE 时 AF 删除订阅并返回 204（s0083-s0085）；没有规定保留或缓存规则。	s0082, s0083, s0084, s0085
S04	通知字段来自同一订阅	通知携带的 notifCorrId 与通知发往的 notifUri 均来自同一订阅，即创建或更新时登记的内容。	notifUri 和 notifCorrId 在订阅中登记（s0038, s0039），通知发往 {notifUri} 并携带该 notifCorrId（s0095, s0096）。	s0038, s0039, s0044, s0095, s0096
R02	通知最多接受一次	同一逻辑通知，即相同 notifCorrId 和相同 vflInferResults，最多被消费者接受一次。	AF 通知已订阅的 VFL 推理事件，可为一次性或周期性（s0022, s0095），消费者存储通知并返回 204（s0098）；没有规定通知序列号或重复检测。	ts-33-501:2865, s0022, s0095, s0096, s0097, s0098
R03	订阅和取消订阅仅应用一次	重复的 subscribe 请求最多创建一个订阅资源，重复的 unsubscribe 最多删除一次。	POST 创建新的 Individual VFL Inference Subscription 并返回 201 和新 subscriptionId（s0043, s0044）；DELETE 在匹配 subscriptionId 的资源被删除后返回 204（s0084, s0085, s0218）。没有规定幂等键或重传规则。	ts-33-501:2865, ts-33-501:2875, s0043, s0044, s0084, s0085, s0218
K02	结果与其他 NF 隔离	订阅的 vflInferResults 和用户标识符（supis、gpsis、intGroupIds、exterGroupIds）仅对订阅的消费者和 AF 可见。	订阅携带用户标识符，通知携带 vflInferResults（s0045, s0097, s0262）；传输保护按 TS 33.501 使用 TLS（s0115），消费者被要求存储通知（s0098）。	rfc6749:2859, ts-33-501:2865, s0045, s0097, s0115, s0262
K01	访问令牌与其他 NF 隔离	消费者的 OAuth2 访问令牌只有 NRF、该消费者及其所面向的 AF 知道。	访问令牌是凭据，在传输和存储中必须保密，且只能在授权服务器、资源服务器和客户端之间共享（RFC 6749）；令牌在消费服务前从 NRF 获取（s0288, s0289）。	rfc6749:2859, rfc6749:2870, s0288, s0289
U01	结果匹配订阅请求	消费者接受的 vflInferResults 是 AF 为该消费者订阅产生的结果，即针对该订阅的分析描述和预训练模型版本产生的结果。	订阅在 vflInferAnaSubs 中描述所订阅的分析事件（s0040），通知携带其结果（s0097）；结果的结构定义在 TS 29.520 中，不在所选原文单元内，因此原文没有规定将结果与样本或模型版本关联的字段。	s0040, s0045, s0097, s0262

ID	简称	对象	文稿怎么说	出处
U02	通知来自选定 AF	消费者接受的通知来自消费者选定的 AF 实例，且属于该消费者的某个订阅。	消费者在其发现的 AF 处订阅（s0029, s0036），AF 向该订阅的 {notifUri} 发送通知（s0095）；通知消息体没有定义 AF 身份字段。	ts-33-501:2871, s0029, s0036, s0095, s0096
Q3	取消和更新后的订阅状态	PUT、PATCH 和 DELETE 之后订阅的有限状态，以及这些方法的错误响应，特别是已删除的订阅是否仍产生通知，以及能否让消费者保持与 AF 不同的状态。	PUT 返回 200 或 204，PATCH 返回 200 或 204，DELETE 返回 204，并带有 403 和 29.500 错误码（s0192, s0205, s0218, s0274-s0282）；除删除和修改资源外，原文没有定义状态机。	s0192, s0205, s0218, s0275, s0282

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 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	安全考虑的引言、对实现者的建议以及对 OAuth 威胁模型的引用；未陈述此 API 的任何性质。
P003 至 P006	rfc6749:2790-2823	Z01, K01	
P007 至 P010	rfc6749:2827-2850	A02, Z03, `malicious_nf`	
P011 至 P014	rfc6749:2859-2877	K01, Z01	
P015	rfc6749:2879-2881	Z03	
P016 至 P021	rfc6749:2885-2917	不在范围内	刷新令牌不属于此 API 使用的客户端凭据授予（s0288-s0289）。
P022 至 P025	rfc6749:2921-2943	不在范围内	未使用授权码授予；NRF 通过客户端凭据授予向 NF 服务消费者签发令牌。
P026 至 P029	rfc6749:2947-2980	不在范围内	此授予中没有授权码流程，因此也没有授权响应重定向 URI。
P030 至 P033	rfc6749:2984-3003	没有陈述目标	关于资源所有者口令凭据的警告；此 API 不使用该授予，也未就其陈述任何性质。
P034 至 P035	rfc6749:3013-3019	K01, K02	
P036	rfc6749:3023-3028	A02, U02	
P037 至 P039	rfc6749:3032-3041	证明器问不了	客户端凭据的强度以及所需的猜测次数超出了符号证明器所能回答的范围。
P040 至 P042	rfc6749:3045-3066	没有陈述目标	针对资源所有者的钓鱼攻击；此 API 没有最终用户或用户代理，因此在此未陈述任何性质。
P043 至 P048	rfc6749:3070-3110	没有陈述目标	跨站请求伪造需要带 cookie 的浏览器会话；NF 服务消费者通过 TLS 使用客户端凭据，因此未陈述此 API 的任何性质。

段落	出处	定为	不选的原因
P049 至 P050	rfc6749:3119-3138	没有陈述目标	点击劫持需要用户代理和可嵌入的内容；此 API 中不存在。
P051 至 P052	rfc6749:3142-3150	Z01, A08	
P053 至 P054	rfc6749:3154-3167	没有陈述目标	授权端点上的开放重定向；此 API 的重定向由 SCP 执行，不在所选原文单元内。
P055 至 P062	rfc6749:3170-3210	没有陈述目标	在隐式授予中滥用访问令牌冒充资源所有者；未使用隐式授予，也不存在资源所有者。
P063	ts-33-501:2491-2491	证明器问不了	安全特性的降级协商涉及算法协商的强度，符号证明器无法判断。
P064 至 P072	ts-33-501:2495-2511	不在范围内	5G 接入网中的订阅认证、服务网络认证和 UE 授权；任务固定为 Naf_VFLInference API 子过程。
P073 至 P074	ts-33-501:2515-2517	不在范围内	无线接口和 N3 接口上 AS/NAS/UP 保护的密钥长度。
P075 至 P078	ts-33-501:2523-2529	不在范围内	对 UE 和 ng-eNB 的要求。
P079 至 P089	ts-33-501:2533-2553	不在范围内	UE 与网络之间的用户数据和信令机密性。
P090 至 P103	ts-33-501:2557-2583	不在范围内	UE 与网络之间的用户数据和信令完整性。
P104 至 P110	ts-33-501:2587-2599	不在范围内	订阅凭据在 UE 和 UICC 中的安全存储。
P111 至 P125	ts-33-501:2603-2631	不在范围内	空口上 SUPI 的订户隐私；VFL 订阅中携带的用户标识改由 K02 覆盖。
P126	ts-33-501:2637-2637	不在范围内	对 gNB 的一般要求。
P127 至 P136	ts-33-501:2641-2659	不在范围内	gNB 用户数据和信令机密性。
P137 至 P147	ts-33-501:2663-2683	不在范围内	gNB 用户数据和信令完整性。
P148 至 P156	ts-33-501:2687-2703	不在范围内	gNB 的建立和配置。
P157 至 P158	ts-33-501:2707-2709	不在范围内	gNB 内部的密钥管理。
P159 至 P160	ts-33-501:2713-2715	不在范围内	gNB 中用户面数据的处理。
P161 至 P162	ts-33-501:2719-2721	不在范围内	gNB 中控制面数据的处理。
P163 至 P168	ts-33-501:2725-2735	不在范围内	gNB 的安全环境。
P169 至 P174	ts-33-501:2739-2749	不在范围内	gNB F1 接口要求。
P175 至 P176	ts-33-501:2753-2755	不在范围内	gNB E1 接口要求。
P177 至 P178	ts-33-501:2759-2761	不在范围内	对 ng-eNB 的要求。

段落	出处	定为	不选的原因
P179 至 P185	ts-33-501:2767-2779	不在范围内	NG 接口上的信令数据机密性。
P186 至 P192	ts-33-501:2783-2795	不在范围内	NG 接口上的信令数据完整性。
P193 至 P196	ts-33-501:2799-2805	不在范围内	NG 接口上的订户隐私。
P197 至 P198	ts-33-501:2809-2811	不在范围内	对 SEAF 的要求。
P199 至 P201	ts-33-501:2819-2823	不在范围内	对 UDM/UDR 订阅数据处理的通用要求。
P202 至 P207	ts-33-501:2827-2837	不在范围内	对 UDM 和 SIDF 的订户隐私要求。
P208 至 P210	ts-33-501:2841-2845	不在范围内	对 AUSF 的要求。
P211 至 P213	ts-33-501:2849-2853	不在范围内	对 UDR 的要求。
P214	ts-33-501:2859-2859	`network`	
P215 至 P220	ts-33-501:2865-2875	A02, Z01, R02, R03, `network`	
P221 至 P227	ts-33-501:2879-2891	Z01, Z03, K01, `malicious_nrf`	
P228 至 P234	ts-33-501:2895-2907	不在范围内	任务排除了 NEF 对不可信 AF 的暴露，固定为可信 AF 直接调用。
P235 至 P241	ts-33-501:2911-2923	`uri_reader`	
P242 至 P254	ts-33-501:2929-2953	不在范围内	漫游和跨 PLMN 安全，包括 SEPP；所建模的路径是单一信任域。
P255 至 P292	ts-33-501:2957-3031	不在范围内	对安全边缘保护代理的要求；所选路径中没有漫游。
P293 至 P303	ts-33-501:3035-3055	不在范围内	由漫游中间节点生成的消息；没有漫游。
P304 至 P312	ts-33-501:3059-3075	不在范围内	跨漫游接口的属性保护。
P313 至 P314	ts-33-501:3079-3081	不在范围内	跨 PLMN 边界处的 IPUPS 功能。
P315 至 P318	ts-33-501:3085-3091	没有陈述目标	始发网络头携带 PLMN 标识；它未陈述此 API 的任何性质，且所建模的路径为单一 PLMN。
P319 至 P323	ts-33-501:3097-3105	不在范围内	信令监控的配置。
P324 至 P327	ts-33-501:3109-3115	不在范围内	信令监控数据的流式传输。
P328 至 P334	ts-33-501:3121-3133	不在范围内	安全可见性，属于部署能力。
P335 至 P337	ts-33-501:3137-3141	不在范围内	运营商的安全可配置性。

段落	出处	定为	不选的原因
P338 至 P347	ts-33-501:3149-3167	不在范围内	无线接口上的加密算法标识符。
P348 至 P357	ts-33-501:3171-3189	不在范围内	无线接口上的完整性算法标识符。
P358 至 P369	ts-33-501:3193-3215	证明器问不了	关于算法选择和强度的要求，符号证明器无法判断。
P370 至 P371	ts-33-501:3219-3221	不在范围内	对 5G-RG 的要求。
P372 至 P375	ts-33-501:3225-3231	不在范围内	对 NSSAAF 的要求。
P376 至 P380	ts-33-501:6540-6548	不在范围内	N3 上的安全要求和过程。
P381 至 P388	ts-33-501:9656-10897	不在范围内	订阅标识隐私的 EAP-TLS 示例以及 IAB 节点要求。
P389 至 P394	ts-33-501:10901-10917	不在范围内	IAB 宿主和 IAB F1 要求。
P395 至 P396	ts-33-501:11439-11443	不在范围内	MBSF 和 MBSTF 的要求。
P397 至 P398	ts-33-501:11899-11901	不在范围内	NEF 对不可信 AF 暴露的安全要求，任务已排除。

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 18 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 11 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 是任务固定的受信 VFL 客户端（s0004、s0013）。攻击者取代它后会自行产生结果和通知，因此结果正确性、通知内容和令牌校验按定义全部失去，原文对不诚实的 AF 也不提出任何性质要求。
S02	NF service consumer	参与方	`malicious_nf`	
S03	NRF	参与方	`malicious_nrf`	
S04	订阅资源	值	`uri_reader`	
S05	通知	值	攻击者得不到更多	通知在 AF 与消费者之间受 TLS 保护。拿到副本只能重放，而这正是 R02 的攻击者。
S06	notifCorrId	值	攻击者得不到更多	notifCorrId 是消费者选择的不透明标识符，本身不认证任何东西。
S07	notifUri	值	攻击者得不到更多	notifUri 是消费者自己的回调地址。知道它并不能让另一方读取发往该地址的流量。
S08	vflInferAnaSubs	值	攻击者得不到更多	这是所订阅分析事件的描述。知道它并不能获得对订阅资源的访问权。
S09	vflInferResults	值	`malicious_nf`	
S10	subscriptionId	值	`uri_reader`	

ID	参与方或值	类别	攻击者条件	不设的原因
S11	OAuth2 访问令牌	值	`malicious_nf`	
S12	naf-vflinference scope	值	攻击者得不到更多	作用域字符串 naf-vflinference 是公开的，由规范定义（s0291）。
S13	AF 实例身份	值	攻击者得不到更多	AF 的 NF 实例身份是公开的，通过 NRF 发现。
S14	通知消息	值	攻击者得不到更多	通知消息受 TLS 保护。网络手中持有的副本就是 R02 的攻击者。
S15	supis/gpsis/intGroupIds/exterGroupIds	值	`malicious_nf`	
S16	输入样本	值	不在范围内	输入样本和数值算法被任务排除在外，API 只承载它们的结果。
S17	模型版本	值	不在范围内	模型版本不是所选原文单元中消息的字段（VflInferResult 定义于 TS 29.520）。
S18	错误响应	值	攻击者得不到更多	ProblemDetails 和 HTTP 错误码不携带受保护的值，原文甚至允许不带响应体的 403。

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之下。单元格是证明器在该攻击者下对相应性质给出的答案；“无答案”表示该攻击者下证明器对某条主张未作判定或没有记录任何内容；空单元格表示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`	只持有网络：读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`malicious_nf`	一个合法的 NF，从一开始就持有自己的 NF 身份、自己的 TLS 凭据以及带有 naf-vflinference 作用域的有效 OAuth2 访问令牌。	NF service consumer 可能是不诚实的 NWDAF 或 NEF。任务把持有自身凭据的恶意合法 NF 与外部网络攻击者区分开，TS 33.501 则区分信任域。	ts-33-501:2859, ts-33-501:2865
`uri_reader`	另一消费者订阅的 subscriptionId 及其他资源 URI 部分，如中间节点在通知发出前所见（s0044 的 Location 响应头、s0082 的请求 URI、s0293/s0295 的重定向）。	请求在资源 URI 中携带 {subscriptionId}，并可能经由 SCP 重定向，而 SCP 会处理该 URI。原文没有说明 subscriptionId 对其所有者是保密的。	ts-33-501:2911, s0044, s0082, s0293, s0295
`malicious_nrf`	授权服务器角色：可以为任意主体、受众和作用域签发令牌，并持有令牌签名密钥。	NRF 是授权服务器，签发 AF 所校验的令牌（s0288-s0290）。授权服务器一旦失守，所有基于令牌的校验都会失效。	ts-33-501:2885, s0288, s0289, s0290

ID	`network`	`malicious_nf`	`uri_reader`	`malicious_nrf`
A02	成立			
A03	成立			
A08	成立		不成立	
Z01	成立			
Z03	成立			
Z04	成立			
S05	成立			
S04	成立			

ID	network	malicious_nf	uri_reader	malicious_nrf
R02	不成立			
R03	不成立			
K02	成立			
K01	成立			
U01	成立			
U02	成立			
Q3	成立			

原文和目标

原文：336 个原文单元，155963 字节，冻结于 source-delivery-01.json。 目标：已批准 14 个（A02、A03、A08、Z01、Z03、Z04、S05、S04、R02、R03、K02、K01、U01、U02）；提出了 3 个问题。 目标清单在事先按草稿形式以 --approve-targets 批准。

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

- approve_package: 批准源文包 protocol-1ebf059b4d1aa0ece99bbb214373

本步骤的自述：1 次请求（1 次失败），0.000 USD，输入 82562 tokens，输出 5293，耗时 260 s。

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
- R02：在 ProVerif 中作答，分析者为该目标指定了 changing_state
- R03：在 ProVerif 中作答，分析者为该目标指定了 changing_state
- Q3：在 ProVerif 中作答，分析者为该目标指定了 changing_state

对代数做了简化（xor、dh_algebra、other_algebra）的 ProVerif 模型给攻击者的能力弱于真实运算：其中的证明是针对更弱攻击者的证明，其中的攻击仍是攻击。省略了对会变化的值（changing_state）的校验的 ProVerif 模型会让参与方接受更多内容：其中的证明成立，其中的攻击可能只是缺少了该校验。Tamarin+Agent 按原样对这些建模。

以步数表示的界是 bounded.pv 上的答案：这是分析者的第二个 ProVerif 模型，其中持有会变化的值的一方连同其校验展开到该步数。该模型做的少于协议本身，因此性质只对这些步成立，再往后就不成立了；在其中发现的攻击仍是攻击。步数由分析者陈述。

分析者的状态审查

这部分是分析者自己对原文的解读，不是证明器的答案。ProVerif 显示下的“是”表示 ProVerif 在展开模型中找到了包含这些步骤的轨迹，因此这些步骤是可能的；它们是否破坏某个目标只由答案表中的攻击来断定，它们还付出了什么代价则是分析者的解读。“未发现”只说明检查了哪些模式，并不证明任何东西。

值	持有方	何时变化	何时校验	refs
订阅资源（subscriptionId、notifUri、notifCorrId、vflInferAnaSubs）	AF（VFL 客户端），作为 Individual VFL Inference Subscription 资源	由对 subscriptions 资源的 POST 创建（s0043、s0044）；由 PUT（s0190）和 PATCH 修改；由 DELETE 删除（s0083、s0084）。	每次 PUT/PATCH/DELETE 时，AF 在行动前先查找 subscriptionId；每次发送通知时，都读取它所通知的订阅（s0095）。	s0043, s0044, s0083, s0084, s0085, s0190, s0218
订阅的通知状态（notifCorrId、已消费的结果）	NF service consumer（NWDAF 或 NEF）	每当 AF 通知该订阅的事件时（s0095）；消费者存储该通知并应答 204（s0098）。	每次收到通知 POST 时，对照本地登记的 notifCorrId 和 notifUri 进行校验（s0096）。	s0095, s0096, s0098, s0100
subscriptionId	AF 和 NF service consumer	订阅创建时由 AF 一次性分配（s0044）。	在 PUT、PATCH、DELETE 的资源 URI 以及重定向的 Location（s0082、s0193、s0219）中比较，并由消费者在使用所获 Location 时比较。	s0044, s0082, s0193, s0219

模式	结果	目标	ProVerif 显示的结果	步骤
replay	candidate	R02	是：ProVerif 在 bounded.pv 上否证了 `b_afterdel_ctl`	AF 向 {notifUri} 发送某订阅的通知 POST，其中包含 notifCorrId 和 vflInferResults（s0095-s0097）。/ 攻击者保留该 POST 的副本，而不是丢弃它。/ 消费者接受该 POST 并返回 204，存储该通知（s0098）。/ 攻击者再次投递同一个 POST；消费者再次接受并存储，因为消息本身和消费者的任何状态都不携带序列号或重复标记。
repeat_one_time_action	candidate	R03	是：ProVerif 在 bounded.pv 上否证了 `b_del_once_ctl`	消费者向 {apiRoot}/naf-vflinference/<apiVersion>/subscriptions/{subscriptionId} 发送 DELETE；AF 删除该订阅并返回 204（s0082-s0085）。/ 攻击者重新发送同一个 DELETE。/ AF 再次接受并第二次返回 204：原文中没有任何记录表明该资源已被删除，而对于一个已被删除的 subscriptionId 也不要求返回 404。
repeat_one_time_action	candidate	R03	否：ProVerif 在 bounded.pv 上对 `b_del_once` 显示已验证	如果 AF 将订阅作为状态保留直到被删除，那么重复的 DELETE 找不到订阅并被拒绝；b_del_once 在一个未展开的订阅上展示了这一点。
desynchronisation	candidate		否：未用 ProVerif 尝试	另一个持有有效令牌和 naf-vflinference 范围的 NF 获知受害者的 subscriptionId（s0044、s0082），并用自己的 notifUri 和自己的 vflInferAnaSubs 发送 PUT（s0190）。/ AF 接受该 PUT 并修改订阅；受害者消费者保留自己的 notifCorrId 和 notifUri，认为订阅未变。/ 随后 AF 将修改后的订阅通知到攻击者的 notifUri，于是受害者的推理结果到达攻击者，而受害者毫无察觉；如果攻击者改为删除该订阅，受害者则等待永远不会到来的通知。
no_rollback_on_failure	candidate		否：未用 ProVerif 尝试	消费者发送 DELETE；AF 删除订阅并返回 204（s0083-s0085）。/ 攻击者丢弃该 204，于是消费者保留订阅及其 notifCorrId，认为退订没有发生。/ 消费者重试或等待；无论哪种方式，双方都保持不同的状态，而原文没有定义消费者获知资源已不存在的任何方式。
update_before_check	nothing found			在两个 AF 角色中，令牌都在查找订阅之前检查，因此没有任何接受发生在状态改变之后，也无需查询即可看出顺序。
race_between_sessions	nothing found			每个 AF 角色都在行动之前查找订阅；对未知 subscriptionId 的请求不会改变已存储的内容。

模式	结果	目标	ProVerif 显示的结果	步骤
distinguishable_failure	nothing found			原文允许 AF 返回不带响应体的 403（s0155），并将失败指向 29.500（s0275、s0276）；模型不给出失败应答，因此该模式超出其能展示的范围。
wrap_or_window	nothing found			该 API 没有计数器、序列号或接受窗口；其标识符是不透明字符串。

分析者为目标命名的内容：

步骤	目标	特征	原因
22	R02、R03、Z04、S05、Q3	changing_state	这些目标依赖于跨步骤变化的值：AF 的订阅资源（由 POST 创建，由 PUT/PATCH 修改，由 DELETE 删除）以及消费者对已消费通知的认知。在 model.pv 中，存储是一张单调表，删除完全没有建模，因此关于顺序的问题（“删除之后不再有通知”、“重复请求只改变资源一次”）只能在 bounded.pv 上回答，其中 AF 和消费者被展开到固定步数。

分析者的结束注记

全部十五个目标都有答案。在 model.pv 上证明：请求和通知的真实性、通知与订阅的绑定、notifCorrId/notifUri 的配对、subscribe、update 和 delete 的令牌要求及其主体和受众绑定，以及访问令牌和结果中用户标识符的机密性，两者各有一个不成立的对照。在 bounded.pv 上证明，一个订阅展开到三步：只有当 AF 持有某个订阅时才为其发送通知，并且在 PUT 之后携带修改后的内容；退订只应用一次；在 204 之后消费者不再接受该 subscriptionId 的任何通知；最后两项有不成立的对照。两项发现。第一项也最重要：该 API 只有一个服务范围的 OAuth2 范围，且未规定检查 PUT、PATCH 或 DELETE 的请求者是否拥有该 subscriptionId，因此任何持有有效令牌并知道某个 subscriptionId 的 NF 都能替换或删除另一个消费者的订阅，而被替换的 notifUri 会转移该消费者的 vflInferResults；该补救措施已用 check_fix 检查——将存储的订阅绑定到令牌主体后，两个攻击查询均验证通过，正常流程得以保留，其余十六个已记录的答案全部不变。第二项：任何地方都没有重复检测，因此重放的通知被存储两次，重放的 subscribe 创建第二个订阅，重放的 DELETE 再次被接受；该建议未经检查，因为一个随每条通知变化的计数器只能在三步展开链中建模，而计数器本身将由该建议虚构。一切都依赖于 TLS 端点认证、对称 OAuth2 令牌、一个冻结的时间概念（使到期检查未经测试），以及 AF 作为任务所固定的可信方；PATCH、错误应答和 TS 29.520 的结果结构不在模型范围内。报告风格中的对照无法在单个文件内为对应性证明构建，报告指明了哪些证明没有对照。