AF 推理服务器组合流程的安全性分析

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）; 5G System; Network Data Analytics Services; Stage 3 （辅助）
检查的性质	5 条：3 条成立，2 条不成立（2 个攻击）
发现	2；另在附录 B 复现已知结论： 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 B：复现的已知结论
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_Inference 服务让 NF 服务消费者在充当 VFL 服务器的 Application Function 上订阅，并接收推理结果的通知；Nnwdaf_VFLInference 服务让该 AF 以 VFL 服务器身份在充当 VFL 客户端的 Network Data Analytics Function 上订阅，并接收其 VFL 推理结果。在组合流程中，NWDAF 消费者在受信任的 AF 上创建推理订阅，AF 在 NWDAF VFL 客户端上为消费者指定的 UE 创建 VFL 推理订阅，在一轮客户端结果之后，AF 将推理结果回报给消费者。每个请求都是基于服务接口上的 HTTP 请求，由两个 NF 之间的 TLS 会话进行认证和加密，并由 NRF 为消费者签发的、覆盖该服务 scope 的 OAuth2 访问令牌授权。

各方：

- **AF**：充当 VFL 服务器的受信任 Application Function。持有：来自 NWDAF 的 inferAnaSubs；已训练的 VFL 模型及其 vflCorrId；用于 naf-inference 和 nnwdaf-vflinference 的 OAuth2 令牌。
- **NWDAF（消费者）**：Naf_Inference 的 NF 服务消费者。持有：分析订阅（inferAnaSubs、notifCorreId、notifUri）；用于 naf-inference 的 OAuth2 令牌。
- **NWDAF（VFL 客户端）**：充当 VFL 客户端的 NWDAF。持有：其本地训练数据；vflCorrId 对应的 VFL 模型；用于 nnwdaf-vflinference 的 OAuth2 令牌。

图 1 展示了文稿所规定的交换流程。

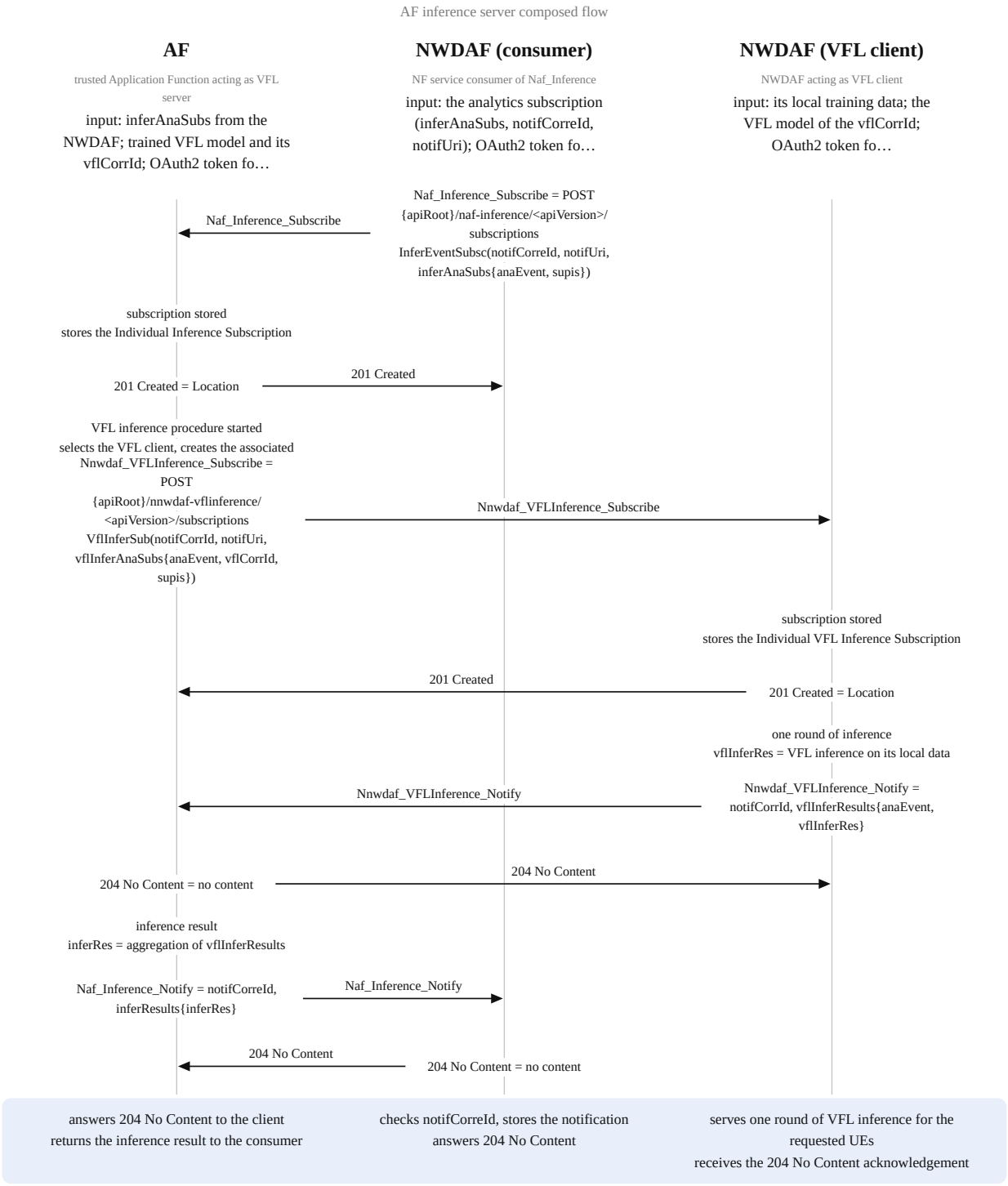


图 1. 文稿所规定的协议。

分析的范围见附录 D：分析了什么、省略了什么，以及依据文稿中的哪些章节。

2 发现

本次分析有 2 个发现：以下内容文稿中并未写明。其中 1 个发现，文稿是否写明不明确。文稿已写明的 1 个结果不计入其中，列于附录 B。

交换的对等认证和服务 scope 令牌检查在模型中成立，但组合流程没有把推理结果绑定到订阅的当前目标，VFL 客户端也没有把 VFL 订阅绑定到 VFL 过程的参与者。第一个是文稿未写明的弱点：在更新之前为消费者所请求的 UE 计算出的一轮推理，可以被报告为更新后订阅的结果。第二个针对的是持有服务级 scope 有效令牌的合法 NF。在五个目标中，两个由证明给出答案，一个由证明和攻击共同给出答案；两个由攻击给出答案，其中一个对其剩余主张给出了证明。所有证明都带有对照，且这些证明依赖于 TLS 会话和访问令牌的理想化，因此不覆盖令牌过期、撤销或端点被攻破的情况。

攻击图使用图 1 的列。红色表示攻击者的行为。黄色标记某方发送了规定交换在该时点本不应有的消息，以及该攻击所破坏的结果。

2.1 在途的 VFL 轮次被报告为更新后推理订阅的结果

类型	协议规范本身的弱点
是否新发现	是：文稿里没有写到
价值	高
涉及的性质	A08 （见第 3 节）
原文	s0055, s0059, s0086, s0593, s0599
依据	ProVerif attack query `a08`; Figure 2

发生了什么。 NWDAF 消费者为一个 UE 创建推理订阅，然后将同一个 Individual Inference Subscription 更新为另一个 UE。AF 在相同的 notifCorrId 下把更新传递给 NWDAF VFL 客户端，但客户端此前已为第一个 UE 集合计算完成的一轮仍在途中。通知只携带 notifCorrId 和 VFL 推理结果，结果中既没有 UE 标识，也没有订阅版本，因此 AF 无法区分这两轮，消费者将旧结果当作其更新后订阅的答案接受。

攻击者需要什么。 消费者在针对前一目标的一轮 VFL 推理仍在计算或传递时更新订阅；不需要任何凭证，也不需要网络攻击者的任何操作。

攻击者能得到什么。 NWDAF 消费者及其分析结果的下游，会把关于某个 UE 集合的 VFL 推理结果归因于更新后它所请求的 UE 集合。同一分析事件的多个订阅共享一个 VFL 关联 ID，使得这种混淆即便没有任何攻击者也能触发。

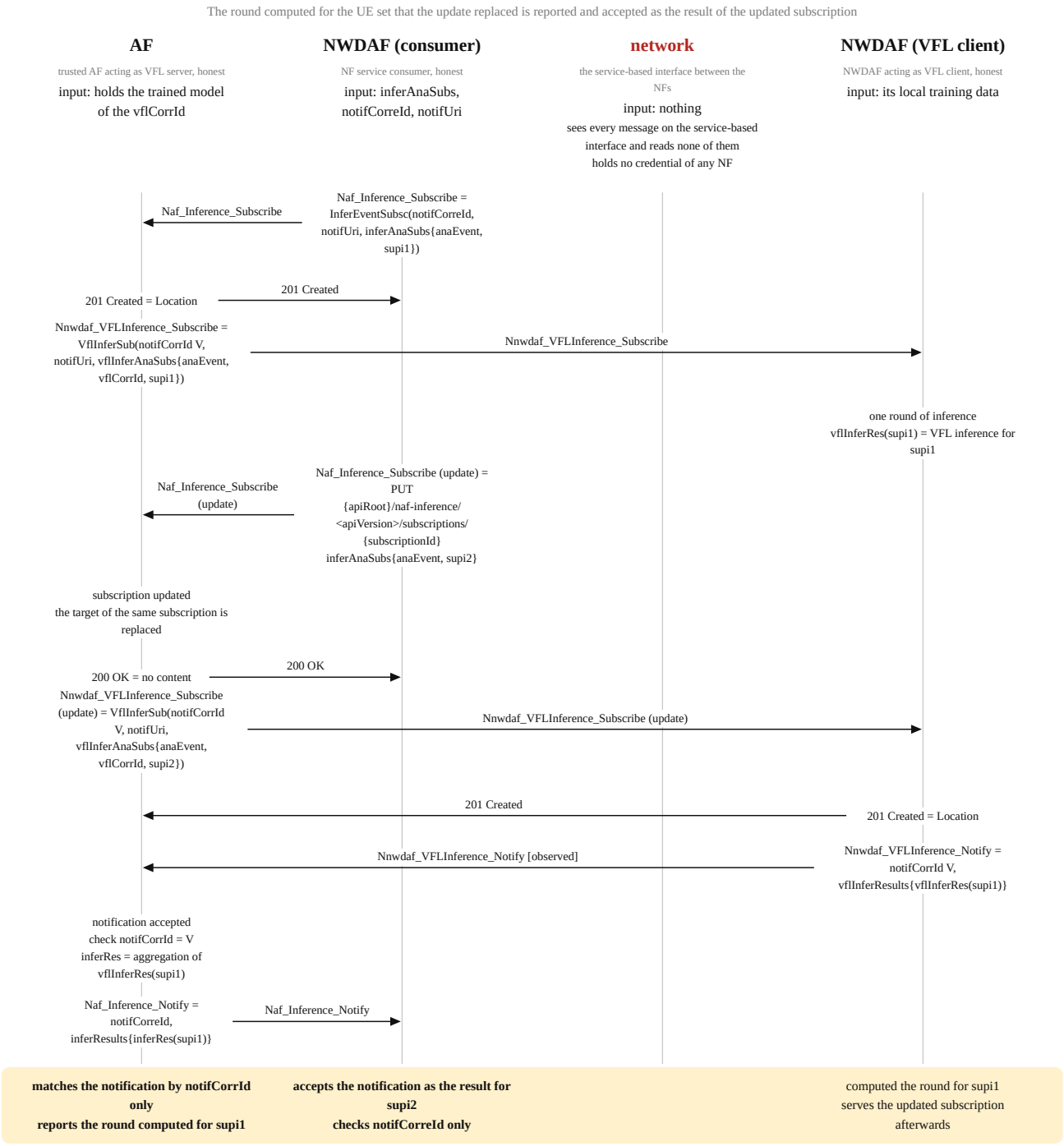


图 2. 为被更新替换的 UE 集合计算出的一轮被报告并接受为更新后订阅的结果。性质 A08；攻击查询 a08。

拟议修改。 在通知中携带轮次信息：在 VflInferNotif 和 InferNotif 中加入请求轮次的标识符（例如 vflCorrId 与该轮所计算的 UE 集合的组合，或随订阅维护的轮次计数器），并要求 AF 仅在该轮与更新后的订阅状态匹配时才报告，消费者仅在该轮匹配时才接受通知。两个通知中使用同一字段，便于编辑核对该规则。

用 ProVerif 复核。 未检查：该修改为两个数据结构增加一个字段，并在两方增加一次比较；在本次分析的时间内无法构建并在模型上运行。

2.2 仅持服务级 scope 的合法 NF 在 NWDAF 客户端加入另一个 VFL 过程

类型	协议规范本身的弱点
是否新发现	不确定：文稿只写了一部分，或没能检索
价值	中
涉及的性质	Z03 （见第 3 节）
原文	s0355, s0359, s0590, s0631, s0419
依据	ProVerif attack query `z03b`; Figure 3

发生了什么。 另一个 NWDAF 持有 naf-inference 和 nnwdaf-vflinference 服务的有效访问令牌，任何合法 NF 都是如此。它针对 AF 的 VFL 过程的 VFL 关联 ID 和相同的 UE，用自己的通知 URI 发送 Nnwdaf_VFLInference_Subscribe。NWDAF VFL 客户端接受该订阅并向它发送 VFL 推理结果，因为该服务为整个 API 定义了一个 scope，而客户端没有得到任何规则来把订阅绑定到该 VFL 关联的参与者。

攻击者需要什么。 同一信任域内一个合法 NF，拥有自己的 TLS 凭证和用于 nnwdaf-vflinference scope 的自己的访问令牌，以及 VFL 过程的 VFL 关联 ID，后者携带在其观察或猜测的订阅中。

攻击者能得到什么。 NWDAF VFL 客户端针对该 VFL 关联 ID 和 UE 集合运行 VFL 推理，并将中间 VFL 推理结果返回给它，因此一个并非该 VFL 过程参与者的 NF 获得了关于另一功能订阅的 UE 的推理输出。

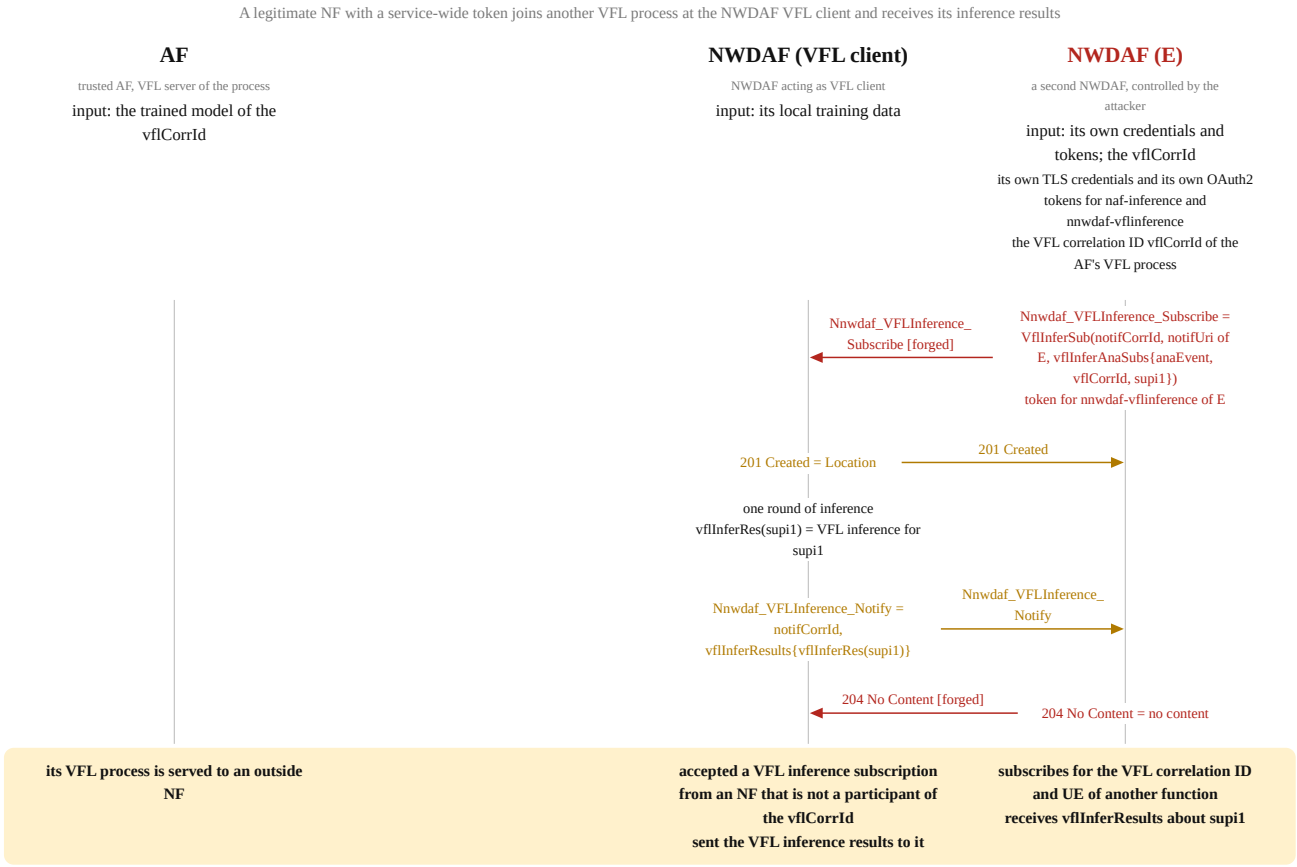


图 3. 持有服务级令牌的合法 NF 在 NWDAF VFL 客户端加入另一个 VFL 过程并接收其推理结果。性质 Z03；攻击查询 z03b。

拟议修改。 要求 NWDAF VFL 客户端在接受 Nnwdaf_VFLInference_Subscribe 之前检查请求的消费者是该 vflCorrId 的 VFL 参与者之一，且请求的 UE 集合在该 VFL 过程建立时所允许的范围内，否则以 403 拒绝。

用 ProVerif 复核。 未检查：模型需要把 VFL 过程的参与者列表作为客户端比对所用的输入，而该列表定义在 TS 29.552 中，不在原文单元内。

3 检查过的性质

每一行是提交给 ProVerif 的一条性质。结果是 ProVerif 对分析者所建协议模型的回答；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
A02	**交换的对等认证。** 每当 AF 接受一个来自 NWDAF 的推理订阅请求（或 NWDAF 接受 AF 的 VFL 推理订阅请求）时，该对端此前确实以本方为通信对象运行过对应流程。	无	成立	中	是
A03	**关联与字段一致性。** AF 与 NWDAF 对同一订阅的 notifCorreId、vflCorrId、anaEvent 及通知目标 URI 达成一致：每次接受都有一个匹配的对端运行，且这些字段一致。	无	成立	中	是
A08	**通知与当前订阅匹配。** AF 发出的通知所携带的 notifCorreId、vflCorrId 与通知目标 URI，对应 NWDAF 当前有效的订阅（含更新后的订阅），而不是已被替换或删除的旧订阅。	无	不成立（1 个攻击）	高	否
Z01	**受保护操作需要有效令牌。** 每次订阅创建/更新/删除与通知提交，都对应授权服务器签发的、覆盖该服务 scope 的有效令牌；无有效令牌的请求不产生受保护操作。	无	成立	低	是
Z03	**令牌绑定到其使用者与上下文。** 一个令牌只能用于其被授予的消费者身份与订阅上下文；不能把某消费者的令牌用于另一消费者的订阅或通知目标。	无	不成立（1 个攻击）	中	不确定

所提出的问题及分析者的回答：

问题	回答	依据
Q1: 外层 inference 订阅与内层 VFL 结果相关性	内层 VFL 通知只携带 notifCorrId 和 VFL 推理结果，结果中带有分析事件，但既没有 UE 集合也没有轮次标识符，因此 AF 只能通过 notifCorrId 把一轮与外部订阅关联起来；外部订阅更新后，同一个 notifCorrId 会允许为旧 UE 集合计算的那一轮被接受，随后被当作更新后订阅的答案上报。	A08, A03
Q2: 客户端/AF/最终消费者三方角色绑定	消费者与 AF 相互认证，AF 与 VFL 客户端也相互认证，因此一方不能冒用另一 NF 的身份行事；但 VFL 客户端没有把请求方绑定到 VFL 过程，所以持有有效令牌的第三方 NF 可以订阅同一个 VFL 关联 ID 并收到结果。	A02, Z03
Q3: 旧内层结果不会错误绑定到更新后的外层订阅	否：客户端的结果没有标记其所属的轮次或 UE 集合，因此为已被更新替换的目标产生的结果会被接受，并在更新后的订阅下上报；消费者无法将其与新鲜结果区分开。	A08

4 本次分析的局限

这里的结论是关于协议模型的结论：它说明所规定的消息和检查在密码学被视为理想的情况下能提供或不能提供什么，而不涉及任何实现。

分析者指出本分析未覆盖的内容如下：

- 两个 NF 之间的 TLS 会话被建模为使用固定密钥的成对认证加密信封；TLS 1.3 的记录级重放保护、连接建立和证书处理未建模，因此在模型中，会话内重放消息是可能的，而 TLS 会拒绝这种重放。
- OAuth2 访问令牌被建模为绑定到主体、受众和范围且不可伪造的值；其签名、过期、撤销和 NRF 令牌请求未建模，因此 Z01 对过期或已撤销的令牌不作任何说明。

- 每个角色只建模一个会话（一个消费者、一个 AF、一个 VFL 客户端、一个其他 NWDAF）；同一消费者有多个并发订阅，或消费者同时也是 VFL 客户端时的行为未覆盖。
- 按任务要求，不信任的 AF 和 5.5.2.2.2 条的 NEF 路径被排除在外；VFL 训练分支和未选择客户端的 AF（s0043、s0048）同样被排除。
- 订阅的删除未建模，因为证明器的表只会增长；更新后仍在途的轮次代表删除情形，删除后的旧通知未被询问。
- vflInferRes 的内容是厂商特定的且未标准化（s0599）；模型把结果视为客户端的不透明值，因此无法对推理本身的正确性作任何说明。
- 可用性、时序、vflNotOnTimeInd 指示的最大响应时间以及密码算法的强度，都超出证明器所能回答的范围。
- 一致性性质的单射解读（每个对端运行对应一次接受）未被单独询问；重复的订阅请求未被区分。

宿主记录的内容：

- A08 的答案依赖于模型简化的一项操作（附录 D）。

每条性质仍悬而未决之处以及何种证据可解决它，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答案的解读，而非证明器的答案：这些答案对协议意味着什么、解读依据是什么、能否按原样使用，以及它有多大价值。

A02: 交换的对等认证

每当 AF 接受一个来自 NWDAF 的推理订阅请求（或 NWDAF 接受 AF 的 VFL 推理订阅请求）时，该对端此前确实以本方为通信对象运行过对应流程。

AF 仅在所指定的 NWDAF 确实向其发送了该订阅请求时才处理该请求，NWDAF 的 VFL 客户端对 VFL 订阅也如此。消费者仅接受来自 AF 的通知。该保证正是 SBI 基线所要求的，且完全依赖于 TLS 会话的存在。

- 结果：Holds；回答了所问：是；可在有保留的情况下使用
- 价值 中：这是对基线所要求的双向认证的证明，是在组合流程上重现的结果，而非新结果。
- 文稿中有述：是。文稿中的位置：ts-33-501:2871, s0040, s0086, s0419
- 依据：SBI 跳是使用固定密钥的成对认证加密信封；TLS 连接建立、证书和记录重放保护未建模。；每个角色一个对端：模型只有一个消费者、一个 AF 和一个 VFL 客户端。；每个证明所给的对照查询显示接受事件在结论不成立的情况下也会发生，因此该蕴含并非空洞。
- 下一步：对不带 SBI 信封的跳建模，以表明该一致性正是 TLS 会话所提供的内容。

A03: 关联与字段一致性

AF 与 NWDAF 对同一订阅的 notifCorreId、vflCorrId、anaEvent 及通知目标 URI 达成一致：每次接受都有一个匹配的对端运行，且这些字段一致。

内层 VFL 订阅的 notifCorreId、更新所针对的资源与分析目标，以及外层订阅的 notifCorreId，均被携带并比较，因此每次接受都属于对端以这些字段发送的请求。未携带的字段，即该轮的 UE 集合和订阅的任何版本，正是通知绑定所缺少的内容。

- 结果：Holds；回答了所问：是；可在有保留的情况下使用
- 价值 中：确认了两个 API 的关联标识符按数据结构的意图进行了绑定，并界定了通知无法绑定的内容。
- 文稿中有述：是。文稿中的位置：ts-33-501:2875, s0237, s0243, s0584, s0590, s0593
- 依据：字段一致性仅对数据结构所携带的字段得到证明；消息不携带的字段无法证明任何检查。；每个角色一个会话，因此一致性仅针对一个订阅生命周期。
- 下一步：在数据模型中增加轮次标识符，并检查此后能否强制执行 A08 所要求的通知绑定。

A08: 通知与当前订阅匹配

AF 发出的通知所携带的 notifCorreId、vflCorrId 与通知目标 URI，对应 NWDAF 当前有效的订阅（含更新后的订阅），而不是已被替换或删除的旧订阅。

消费者所接受的通知可能报告为已被其更新替换的 UE 集合计算的那一轮，因为两种通知都不携带 UE 集合或轮次标识符；AF 没有字段可检查，消费者也没有字段可检查。不需要任何凭据：该轮是更新时仍在途的 VFL 客户端的真实消息。

- 结果：Fails（1 次攻击）；回答了所问：是；可用

- 价值 高：组合流程本应提供的一项保护缺失，且文稿未陈述该弱点。
- 文稿中有述：否。所依据的原文：s0055, s0059, s0086, s0593, s0599
- 依据：消费者在一轮仍在途时更新其订阅；此顺序是模型所允许的，也是原文未排除的。；删除未建模；更新代表订阅状态的变更。；结果值是不透明项，因此模型对其内容的说明仅限于它是为某个 UE 集合计算的。
- 开放：删除后是否出现同样的混淆，或共享同一 VFL 关联 ID 的两个订阅之间是否出现，均未建模。
- 下一步：也对取消订阅建模，并检查消费者删除订阅后旧通知是否会被接受。

Z01: 受保护操作需要有效令牌

每次订阅创建/更新/删除与通知提交，都对应授权服务器签发的、覆盖该服务 scope 的有效令牌；无有效令牌的请求不产生受保护操作。

AF 和 NWDAF 的 VFL 客户端都不会为不持有向其签发的、对应服务范围的令牌的消费者执行订阅操作；没有此类令牌的请求根本不会到达受保护操作。这是基线所规定的 OAuth2 授权，对照查询表明该性质正是令牌检查，而非其他内容。

- 结果：Holds；回答了所问：是；可在有保留的情况下使用
- 价值 低：该性质源自文稿所要求的 OAuth2 授权；分析确认该检查有效，并为其提供了对照查询。
- 文稿中有述：是。文稿中的位置：rfc6749:2870, ts-33-501:2867, s0272, s0273, s0628, s0629
- 依据：令牌是绑定到主体、受众和范围且不可伪造的值；其签名、过期和撤销未建模。；无任何令牌的 NF 请求由 AF 的未检查副本建模，即对照查询；真实 AF 会拒绝它。
- 开放：过期、撤销和令牌请求未建模，因此答案仅覆盖不可伪造且未过期的令牌。
- 下一步：对 NRF 令牌请求和令牌过期建模，以便对过期令牌询问同一性质。

Z03: 令牌绑定到其使用者与上下文

一个令牌只能用于其被授予的消费者身份与订阅上下文；不能把某消费者的令牌用于另一消费者的订阅或通知目标。

一个令牌不能冒充另一个消费者出示，网络攻击者也读不到推理结果。不成立的是订阅上下文：一个合法 NF 用自己有效的令牌，在 NWDAF VFL client 上订阅另一个功能 VFL 进程的 VFL correlation ID 和 UE，并收到结果。原因是一个 scope 覆盖整个服务，客户端没有任何参与者检查。

- 结果：不成立（1 个攻击）；是否回答了所问：部分；可谨慎使用
- 价值：中：一个合法 NF 获得关于另一个订阅的 UE 的 VFL 推理结果；文稿写明了服务级 scope，但没有写明这一后果。
- 文稿中是否写明：不明确。依据的原文：s0275, s0631, s0590, s0355, s0419
- 依据：s0631 的服务级 scope 被建模为单个 scope 值；按资源的授权（如果运营商标配了的话）不在模型中。；假定 VFL correlation ID 可被另一个 NF 知晓或猜测；模型直接把它交给第二个 NWDAF。；TS 29.552 中 VFL 信令流程的参与者规则未建模。
- 待定：VFL client 是否必须检查 VFL 参与关系由 TS 29.552 定义，而该规范不在原文单元中。；令牌过期和吊销不在模型范围内。
- 下一步：阅读 TS 29.552 的 VFL 参与者规则，判断是否已经要求客户端检查这些规则；如果没有，客户端需要增加参与者检查。

附录 B：复现的已知结论

文稿已经写明、或已被文稿搁置的性质不成立，不算发现。以下属于这一类：分析在模型上复现了它，并给出了确切条件。

B.1 组合流程每一跳的对端认证和令牌检查都成立

类型	已确认的保证
文稿出处	ts-33-501:2871, main:10528
价值	中
涉及的性质	A02, A03, Z01 （见第 3 节）
原文	s0040, s0086, s0419

发生了什么。 在 SBI TLS 会话以及绑定到其 subject、audience 和 scope 的令牌就位的情况下，AF 和 NWDAF VFL client 只对它们所指名对端的请求采取行动，AF 只接受它向其订阅的客户端的通知，消费者只接受 AF 发给自己 notifCorreId 的通知。

攻击者能得到什么。 实现者或编辑者可以知道，在 SBI 基线规定的传输上哪些性质成立，以及其中哪些不依赖于该传输。

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、是否检查了对照查询，以及分析者对每个攻击的判定。

目标	级别	界	查询	对照	攻击	主张
A02	proved		a02	checked		2 proved
A03	proved		a03a	checked		3 proved
A08	none				a08 (holds_in_source)	1 attack
Z01	proved		z01a	checked		6 proved
Z03	proved		z01a	checked	z03b (depends_on_ambiguity)	3 proved, 1 attack

逐条主张，按分析者对每条主张的措辞；每条的回答来自证明器：

目标	主张	攻击者	回答	查询	对照
A02	AF 只有在被命名为消费者的 NWDAF 执行了订阅流程并将该请求发送给 AF 时，才接受 Naf_Inference 订阅请求（带有该 notifCorreId 和 notifUri）；攻击者是网络上的攻击者，不持有任何 NF 凭据。	`network`	proved	a02	checked
A02	NWDAF VFL client 只有在被命名为消费者的 NF 发送了该请求本身（相同的 notifCorrId、notifUri 和 UE 目标）时，才接受 Nnwdaf_VFLInference 订阅请求；攻击者是网络上的攻击者。	`network`	proved	a02b	checked
A03	AF 只对它登记在 VFL client 的 notifCorrId 接受 Nnwdaf_VFLInference 通知，且只接受该客户端发送的结果载荷；攻击者是网络上的攻击者。	`network`	proved	a03a	checked
A03	AF 只对消费者创建的 Individual Inference Subscription 资源接受推理订阅的更新，且只接受消费者所请求的分析目标（UE），从而 notifCorreId 和目标在消费者与 AF 之间一致；攻击者是网络上的攻击者。	`network`	proved	a03b	checked
A03	消费者只接受携带自己 notifCorreId 且由 AF 为该订阅生成的通知；攻击者是网络上的攻击者。	`network`	proved	a03c	checked
A08	消费者接受的通知所报告的结果是为订阅当前的分析目标（更新后的 UE）计算的，而不是更新所替换的目标仍在途的那一轮；攻击者是网络上的攻击者。	`network`	attack (holds_in_source)	a08	
Z01	AF 只为持有向其签发的 naf-inference 服务 scope 访问令牌的消费者创建、更新或应答推理订阅；攻击者是网络上的攻击者，不持有令牌，也不持有 NF 凭据。	`network`	proved	z01a	checked
Z01	NWDAF VFL client 只接受持有向其签发的 nnwdaf-vflinference 服务 scope 访问令牌的消费者的 VFL 推理订阅；攻击者是网络上的攻击者。	`network`	proved	z01b	checked
Z01	AF 只为持有向其本身签发、用于 naf-inference scope 的令牌的消费者创建、更新或应答推理订阅，因此一个持有自己有效令牌的合法 NF 不能使 AF 以另一个身份为它行动；攻击者是一个持有自身凭据和令牌的合法 NF。	`dishonest_nf`	proved	z01a	checked
Z01	NWDAF VFL client 只接受持有向其本身签发、用于 nnwdaf-vflinference scope 的令牌的消费者的 VFL 推理订阅；攻击者是一个持有自身凭据和令牌的合法 NF。	`dishonest_nf`	proved	z01b	checked

目标	主张	攻击者	回答	查询	对照
Z01	签发给另一个消费者的令牌不能在 AF 上使用，因为 AF 要求令牌是签发给出示该令牌的身份的那个令牌；攻击者已从存储中读取了另一个 NF 的令牌。	`stolen_token`	proved	z01a	checked
Z01	签发给另一个消费者的令牌不能在 NWDAF VFL client 上使用，因为客户端要求令牌是签发给出示该令牌的身份的那个令牌；攻击者已从存储中读取了另一个 NF 的令牌。	`stolen_token`	proved	z01b	checked
Z03	令牌只能由签发对象消费者使用：AF 和 NWDAF VFL client 只对令牌签发对象身份接受操作，因此合法 NF 不能把自己的令牌冒充为另一个消费者的；攻击者是一个持有自身凭据和令牌的合法 NF。	`dishonest_nf`	proved	z01a	checked
Z03	从存储中读取的令牌不能冒充另一个消费者出示：接收方要求令牌签发给出示它的身份；攻击者已读取了另一个 NF 的令牌。	`stolen_token`	proved	z01a	checked
Z03	消费者只能将其令牌用于它拥有的订阅上下文：另一个 NF 持有同一服务级 scope 的有效令牌时，不得获得其并非参与者的 VFL correlation ID 和 UE 的 VFL 推理结果；攻击者是一个持有自身凭据和令牌的合法 NF。	`dishonest_nf`	attack (depends_on_ambiguity)	z03b	
Z03	关于 UE 的 VFL 推理结果不能被网络上的攻击者从基于服务的接口消息中获得；它只通过消费者与生产者之间的 TLS 会话到达该消费者。	`network`	proved	z03net	checked

附录 D：分析是怎么跑的

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

ProVerif+ Agent session session-20261114T224019，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：60，证明器 3 秒，实际耗时 14 分钟，成本 0.132 USD。

ProVerif：运行 69 次证明，67 次有结论，2 次无答案，2 秒，记录 23 个回答。

分析了什么

协议	AF 推理服务器组合流程
版本	19.2.0
分析范围	可信 AF 为 VFL server、NWDAF consumer 加一个 NWDAF VFL client；模型预先训练，AF 收到订阅后可发 Nnwdaf_VFLInference_Subscribe，收一轮 client 结果后报告。完整保留内外两组 ID 映射；排除 NEF 和缺模型触发训练分支。
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 677 个编号原文单元（377484 字节）。本报告中的 s0001 这样的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	5.5	Naf_Inference Service
main	5.5.1	服务描述
main	5.5.1.1	概述
main	5.5.1.2	服务架构
main	5.5.1.3	网络功能
main	5.5.1.3.1	应用功能（AF）
main	5.5.1.3.2	NF 服务消费者
main	5.5.2	服务操作
main	5.5.2.1	引言
main	5.5.2.2	Naf_Inference_Subscribe
main	5.5.2.2.1	概述
main	5.5.2.2.2	推理订阅创建
main	5.5.2.2.3	推理订阅更新
main	5.5.2.3	Naf_Inference_Unsubscribe
main	5.5.2.3.1	概述
main	5.5.2.3.2	推理订阅删除

文稿	章节	标题
main	5.5.2.4	Naf_Inference_Notify
main	5.5.2.4.1	概述
main	5.5.2.4.2	推理通知
main	6.4	Naf_Inference Service API
main	6.4.1	引言
main	6.4.2	HTTP 的使用
main	6.4.2.1	概述
main	6.4.2.2	HTTP 标准头
main	6.4.2.2.1	概述
main	6.4.2.2.2	内容类型
main	6.4.2.3	HTTP 自定义头
main	6.4.3	资源
main	6.4.3.1	概述
main	6.4.3.2	资源：推理订阅
main	6.4.3.2.1	描述
main	6.4.3.2.2	资源定义
main	6.4.3.2.3	资源标准方法
main	6.4.3.2.3.1	POST
main	6.4.3.2.4	资源自定义操作
main	6.4.3.3	资源：单个推理订阅
main	6.4.3.3.1	描述
main	6.4.3.3.2	资源定义
main	6.4.3.3.3	资源标准方法
main	6.4.3.3.3.1	PUT
main	6.4.3.3.3.2	PATCH
main	6.4.3.3.3.3	DELETE
main	6.4.3.2.4_2	资源自定义操作
main	6.4.4	无关联资源的自定义操作
main	6.4.5	通知
main	6.4.5.1	概述
main	6.4.5.5	推理通知
main	6.4.5.5.1	描述
main	6.4.5.5.2	目标 URI
main	6.4.5.5.3	标准方法
main	6.4.5.5.3.1	POST
main	6.4.6	数据模型

文稿	章节	标题
main	6.4.6.1	概述
main	6.4.6.2	结构化数据类型
main	6.4.6.2.1	引言
main	6.4.6.2.2	类型 InferEventSubsc
main	6.4.6.2.3	类型 InferEventSubscPatch
main	6.4.6.2.4	类型 InferAnaSub
main	6.4.6.2.5	类型 InferNotif
main	6.4.6.2.6	类型 InferResult
main	6.4.6.3	简单数据类型与枚举
main	6.4.6.3.1	引言
main	6.4.6.3.2	简单数据类型
main	6.4.7	错误处理
main	6.4.7.1	概述
main	6.4.7.2	协议错误
main	6.4.7.3	应用错误
main	6.4.8	特性协商
main	6.4.9	安全
main	6.4.10	HTTP 重定向
ts-29-520	4.11	Nnwdaf_VFLInference Service
ts-29-520	4.11.1	服务描述
ts-29-520	4.11.1.1	概述
ts-29-520	4.11.1.2	服务架构
ts-29-520	4.11.1.3	网络功能
ts-29-520	4.11.1.3.1	网络数据分析功能（NWDAF）
ts-29-520	4.11.1.3.2	NF 服务消费者
ts-29-520	4.11.2	服务操作
ts-29-520	4.11.2.1	引言
ts-29-520	4.11.2.2	Nnwdaf_VFLInference_Subscribe 服务操作
ts-29-520	4.11.2.2.1	概述
ts-29-520	4.11.2.2.2	订阅 VFL 推理事件通知
ts-29-520	4.11.2.2.3	更新事件通知订阅
ts-29-520	4.11.2.2.4	部分更新事件通知订阅
ts-29-520	4.11.2.3	Nnwdaf_VFLInference_Unsubscribe 服务操作
ts-29-520	4.11.2.3.1	概述
ts-29-520	4.11.2.3.2	取消订阅 VFL 推理通知
ts-29-520	4.11.2.4	Nnwdaf_VFLInference_Notify 服务操作

文稿	章节	标题
ts-29-520	4.11.2.4.1	概述
ts-29-520	4.11.2.4.2	关于已订阅事件的通知
ts-29-520	5.10	Nnwdaf_VFLInference Service API
ts-29-520	5.10.1	引言
ts-29-520	5.10.2	HTTP 的使用
ts-29-520	5.10.2.1	概述
ts-29-520	5.10.2.2	HTTP 标准头
ts-29-520	5.10.2.2.1	概述
ts-29-520	5.10.2.2.2	内容类型
ts-29-520	5.10.2.3	HTTP 自定义头
ts-29-520	5.10.3	资源
ts-29-520	5.10.3.1	资源结构
ts-29-520	5.10.3.2	资源：NWDAF VFL 推理订阅
ts-29-520	5.10.3.2.1	描述
ts-29-520	5.10.3.2.2	资源定义
ts-29-520	5.10.3.2.3	资源标准方法
ts-29-520	5.10.3.2.3.1	POST
ts-29-520	5.10.3.2.4	资源自定义操作
ts-29-520	5.10.3.3	资源：单个 VFL 推理订阅
ts-29-520	5.10.3.3.1	描述
ts-29-520	5.10.3.3.2	资源定义
ts-29-520	5.10.3.3.3	资源标准方法
ts-29-520	5.10.3.3.3.1	PUT
ts-29-520	5.10.3.3.3.2	PATCH
ts-29-520	5.10.3.3.3.3	DELETE
ts-29-520	5.10.3.3.3.4	GET
ts-29-520	5.10.3.3.4	资源自定义操作
ts-29-520	5.10.4	无关联资源的自定义操作
ts-29-520	5.10.5	通知
ts-29-520	5.10.5.1	概述
ts-29-520	5.10.5.2	VFL 推理事件通知
ts-29-520	5.10.5.2.1	描述
ts-29-520	5.10.5.2.2	操作定义
ts-29-520	5.10.6	数据模型
ts-29-520	5.10.6.1	概述
ts-29-520	5.10.6.2	结构化数据类型

文稿	章节	标题
ts-29-520	5.10.6.2.1	引言
ts-29-520	5.10.6.2.2	类型 VflInferSub
ts-29-520	5.10.6.2.3	类型 VflInferSubPatch
ts-29-520	5.10.6.2.4	类型 VflInferAnaSub
ts-29-520	5.10.6.2.5	类型 VflInferNotif
ts-29-520	5.10.6.2.6	类型 VflInferReq
ts-29-520	5.10.6.2.7	类型 VflInferResult
ts-29-520	5.10.6.3	简单数据类型与枚举
ts-29-520	5.10.6.3.1	引言
ts-29-520	5.10.6.3.2	简单数据类型
ts-29-520	5.10.6.3.3	枚举：VflTermCause
ts-29-520	5.10.7	错误处理
ts-29-520	5.10.7.1	概述
ts-29-520	5.10.7.2	协议错误
ts-29-520	5.10.7.3	应用错误
ts-29-520	5.10.8	特性协商
ts-29-520	5.10.9	安全

源文步骤在文稿中定位到的协议用途如下：可信 AF 充当 VFL server，NWDAF consumer 则新增一个 NWDAF VFL client。模型事先已训练好，AF 收到订阅后可发出 Nnwdaf_VFLInference_Subscribe，收齐一轮 client 结果后再上报。内、外两组 ID 映射均完整保留；排除 NEF，也排除“缺模型触发训练”这一分支。

对照文稿确定性质

在编写任何查询之前，分析者先把草拟的性质清单与文稿本身对协议用途的说明做了对照。性质的名称、所涉及的方面以及文稿的说法均属分析者的解读；所列位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
A02	交换的对等认证	AF 确信某个 Naf_Inference 订阅请求来自它所指名为消费者的 NWDAF；NWDAF VFL 客户端确信某个 Nnwdaf_VFLInference 订阅请求来自运行组合流程的 AF；消费者确信通知来自 AF。	文稿将这些操作定义为 NF 服务消费者与作为 NF 服务生产者的 AF 之间的 HTTP 请求（s0004、s0032、s0350、s0411），并将认证交给 SBI 基线，该基线要求消费者与生产者之间进行双向认证（TS 33.501 5.9.2.1），并对每条传入消息进行验证（TS 33.501 5.9.2.1）。	ts-33-501:2871, s0004, s0021, s0079, s0086, s0322, s0350, s0411, s0419
A03	关联与字段一致性	对于同一个订阅，AF 与 NWDAF 对 notifCorreId、vflCorrId、分析事件和通知目标 URI 达成一致；每次接受都对应一个恰好发送了这些字段的对端运行。	数据结构将 notifCorreId、notifUri、vflInferAnaSubs（含 vflCorrId 和 anaEvent）设为请求中的必填项，并要求通知中携带相同的 notifCorrId（s0237、s0243、s0584、s0590、s0593、s0419）；TS 33.501 要求每个 NF 依据协议规范和网络状态验证传入消息。	ts-33-501:2875, s0237, s0243, s0246, s0584, s0590, s0593, s0364, s0419

ID	简称	对象	文稿怎么说	出处
A08	通知与当前订阅匹配	AF 发给消费者的通知携带 NWDAF 当前有效订阅的 notifCorreId、vflCorrId 和目标 URI，并报告针对该订阅当前分析目标计算出的结果，而不是针对已被更新替换的订阅。	当消费者更新其订阅时，AF 应更新相关联的 Nnwdaf_VFLInference 订阅（s0059），并应通过对应 Individual Inference Subscription 资源的 notifUri 发送通知（s0086）；通知本身只携带 notifCorreId 和结果（s0246、s0593），因此这种绑定必须来自 AF 所持有的订阅。	main:10677, s0032, s0055, s0059, s0061, s0086, s0243, s0419, s0590, s0593
Z01	受保护操作需要有效令牌	除非请求携带授权服务器为该消费者针对相应服务范围签发的 OAuth2 访问令牌，否则 AF 不为消费者执行任何推理订阅的创建、更新或通知，NWDAF VFL 客户端也不接受任何 VFL 推理订阅。	两个 API 的访问均可通过 OAuth2 客户端凭据授予方式授权，NRF 为授权服务器，消费者应在使用服务前获取令牌（s0272、s0273、s0628、s0629）；TS 33.501 要求对服务请求进行授权（5.9.2.1），并要求令牌不可伪造（RFC 6749 10.3）。	rfc6749:2870, ts-33-501:2867, s0272, s0273, s0275, s0628, s0629, s0631
Z03	令牌绑定到其使用者与上下文	令牌只能由签发对象消费者使用，且只能用于该消费者拥有的订阅和通知目标；持有同一服务级范围令牌的另一个 NF 不能代表它行事，也不能收到它的推理结果。	两个 API 都为整个服务定义单一范围，没有资源级或操作级范围（s0275、s0631），因此令牌不携带订阅级权利；RFC 6749 指出，OAuth2 本身无法让资源服务器检查令牌是否签发给了出示它的客户端（10.3）。	rfc6749:2879, main:10528, s0275, s0631, s0237, s0246, s0584, s0593

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 24 段，没选 374 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 安全考虑的引言；未陈述关于本协议的任何要求。
P003 至 P006	rfc6749:2790-2823	Z01, `stolen_token`, `dishonest_nf`	
P007 至 P010	rfc6749:2827-2850	Z03, Z01, `stolen_token`, `dishonest_nf`	
P011 至 P013	rfc6749:2859-2872	Z01, `stolen_token`	
P014	rfc6749:2874-2877	Z03	
P015	rfc6749:2879-2881	Z03	
P016 至 P021	rfc6749:2885-2917	不在范围内	刷新令牌；5GC 使用的客户端凭据授予方式没有刷新令牌。

段落	出处	定为	不选的原因
P022 至 P025	rfc6749:2921-2943	不在范围内	授权码；不与客户端凭据授予方式一起使用。
P026 至 P029	rfc6749:2947-2980	不在范围内	重定向 URI 操纵；客户端凭据授予方式及这些 API 中均无重定向。
P030 至 P033	rfc6749:2984-3003	不在范围内	资源所有者口令凭据；未使用。
P034 至 P036	rfc6749:3013-3028	A02, `network`	
P037 至 P039	rfc6749:3032-3041	证明器问不了	客户端凭据猜测；NF 持有的是机器凭据和 TLS 密钥，而非用户选择的秘密，且此类凭据是否可猜测属于秘密强度问题，无法向证明器提问。
P040 至 P042	rfc6749:3045-3066	不在范围内	终端用户钓鱼；无终端用户参与。
P043 至 P048	rfc6749:3070-3110	不在范围内	跨站请求伪造；无基于浏览器的流程。
P049 至 P050	rfc6749:3119-3138	不在范围内	点击劫持；无基于浏览器的流程。
P051	rfc6749:3142-3146	A03	
P052	rfc6749:3148-3150	没有陈述目标	关于输入验证的一般性建议；除 A03 外未陈述本协议的任何性质。
P053 至 P054	rfc6749:3154-3167	不在范围内	开放重定向；本流程中无重定向。
P055 至 P062	rfc6749:3170-3210	不在范围内	隐式授予；5GC 配置未使用。
P063	ts-33-501:2491-2491	不在范围内	算法降级；所选条款中的两个 API 未定义任何特性或算法协商（空特性表，s0270、s0626）。
P064 至 P072	ts-33-501:2495-2511	不在范围内	UE 认证、服务网络认证和 UE 授权；涉及接入网，而非 AF 推理订阅。
P073 至 P074	ts-33-501:2515-2517	不在范围内	接入网密钥。
P075 至 P213	ts-33-501:2523-2853	不在范围内	无线和接入层的用户数据与信令保护、订阅凭据的安全存储，以及对 gNB、AMF、SEAF、AUSF、UDM 和 UDR 的要求；这些参与方均不参与所建模的 AF 流程。
P214	ts-33-501:2859-2859	`dishonest_nf`	

段落	出处	定为	不选的原因
P215 至 P219	ts-33-501:2865-2873	A02, `network`	
P220	ts-33-501:2875-2875	A03	
P221 至 P227	ts-33-501:2879-2891	不在范围内	NRF 发现与注册；NRF 是令牌签发者，但其自身流程未被建模或选取。
P228 至 P234	ts-33-501:2895-2907	不在范围内	NEF 要求；任务排除了面向不可信 AF 的 NEF 路径。
P235 至 P241	ts-33-501:2911-2923	不在范围内	SCP 与间接通信；该流程被建模为直接的 SBI 跳转。
P242 至 P254	ts-33-501:2929-2953	不在范围内	PLMN 间互联与 SEPP；本流程不涉及漫游。
P255 至 P314	ts-33-501:2957-3081	不在范围内	SEPP、漫游中间节点与 IPUPS；不属于所建模的流程。
P315 至 P318	ts-33-501:3085-3091	不在范围内	始发 PLMN ID 头；所建模流程之外的漫游元数据。
P319 至 P337	ts-33-501:3097-3141	没有陈述目标	信令监控、安全可见性与可配置性；属于运行措施，而非协议消息的性质。
P338 至 P369	ts-33-501:3149-3215	证明器问不了	加密与完整性算法标识符及算法选择；原语的强度超出符号证明器所能回答的范围。
P370 至 P398	ts-33-501:3219-11901	不在范围内	对 5G-RG、NSSAAF、N3、EAP-TLS 接入、IAB、MBSF 和 NEF 的要求；这些参与方或接口均不参与所建模的流程。

性质目录，逐条去向

性质是从一份安全和隐私性质目录起草的。起草时有 37 条没选，分析者把它们逐条过了一遍：作为性质在这里检查，或者写明原因不检查。检查了 18 条，没检查 19 条。“文稿没有提到”不能作为不检查的原因。

条目	目录里的性质	作为哪条性质检查　不检查的原因
K01	密钥／凭据保密性	Z01
K02	载荷与端到端保密性	Z03
K03	强保密／秘密值不可区分性	Z03
K04	密钥用途、方向与会话分离	A02
D01	消息完整性与数据来源真实性	A02
A01	对端曾参与性（Aliveness）	A02
A04	单射一致性认证	A02

条目	目录里的性质	作为哪条性质检查	不检查的原因
A05	隐式密钥认证	不适用	这两个 API 都没有定义密钥建立；SBI 的 TLS 基线按给定条件建模。
A06	显式密钥确认	不适用	本流程中不发生任何密钥确认。
A07	身份—凭据—密钥绑定	Z03	
R01	认证／挑战新鲜性	A08	
R02	消息级抗重放	A08	
R03	业务操作至多一次	A08	
R04	消息接受顺序／窗口安全	A08	
R05	抗降级／安全策略保持	不在范围内	所选条款中无法协商版本、套件或安全级别；两张特性表都是空的。
C01	前向保密性（FS）	不适用	这些 API 不建立任何会话密钥。
C02	抗密钥泄露冒充（KCI）	不适用	不存在长期密钥可能被攻破的密钥协商。
C03	已知密钥安全／泄露隔离	不适用	本流程不属于任何密钥层级。
C04	临时秘密／部分状态泄露韧性	不在范围内	读取一方的内存超出建模的攻击者范围；只考虑了 S01–S03 这几项参与方暴露。
C05	泄露后安全恢复（PCS）	不适用	本流程中没有任何棘轮或密钥更新。
C06	注册凭据泄露后的增强认证	不适用	没有注册记录，也没有 PAKE。
C07	抗离线字典攻击	不适用	NF 不使用口令或其他可猜测的秘密。
C08	指定原语失效下的目标保持	证明器问不了	对原语被攻破的抵抗能力超出符号模型能支持的范围。
Z02	委托权限不扩张	A08	
Z04	撤销与过期生效	Z01	
Z05	跨租户／跨服务安全隔离	Z03	
S01	加密 nonce 唯一性	不适用	本流程不包含任何基于 nonce 的加密。
S02	重传／密钥重安装安全	不适用	没有密钥安装，也没有密钥材料重传。
S03	抗回滚与状态单调性	A08	
S04	跨阶段安全上下文一致性	A08	
S05	终止与旧状态失效	A08	
P01	身份匿名性	不适用	NF 身份在 SBI 上并不隐藏；两个 API 也都不要求匿名性。
P02	会话不可关联性	不适用	对 NF 订阅没有不可关联性要求。
P03	用户／凭据存在性隐藏	不适用	这些 API 中不隐藏用户或凭据的存在性。
V01	条件性进展／错误恢复	证明器问不了	条件性进展与恢复属于活性性质，超出 ProVerif 能回答的范围。
V02	无非预期死锁	证明器问不了	无死锁属于活性性质，超出 ProVerif 能回答的范围。
V03	受限资源滥用／抗放大	证明器问不了	资源耗尽与放大超出 ProVerif 能回答的范围。

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 16 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 5 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	整个组合流程的诚实性都依赖 AF；一旦它被攻击者控制，就会伪造或重定向每一个推理结果，而文稿并不要求在受信任的 AF 被攻破的情况下满足这些性质中的任何一条。
S02	NWDAF	参与方	`dishonest_nf`	
S03	NRF	参与方	按定义全部失守	NRF 签发访问令牌；攻击者掌握授权服务器就能为任意消费者签发令牌，因此这里要求的每一条授权性质都按定义失效，而文稿并不要求在授权服务器被攻破的情况下满足其中任何一条。
S04	订阅请求中的消费者身份	值	攻击者得不到更多	消费者身份在请求中携带，接收方也知道；在 TLS 之下，它无法被用来冒充该消费者。
S05	通知中的生产者身份	值	攻击者得不到更多	生产者身份就是 TLS 对端的身份；知道它并不会给网络攻击者带来它所缺少的东西。
S06	notifCorreId	值	攻击者得不到更多	通知关联标识由消费者选定；持有它并不能让网络攻击者通过 AF 的 TLS 会话发送通知。
S07	vflCorrId	值	`dishonest_nf`	
S08	anaEvent	值	攻击者得不到更多	分析事件类型是公开的枚举值。
S09	notifUri	值	攻击者得不到更多	通知 URI 是公开的，并在请求中携带。
S10	订阅上下文	值	攻击者得不到更多	订阅上下文由 AF 和消费者持有；由于通知绑定到 AF 的 TLS 会话，网络攻击者无法使用它。
S11	通知目标	值	攻击者得不到更多	通知目标 URI 是公开的；要投递到它需要生产者的 TLS 会话。
S12	OAuth2 访问令牌	值	`stolen_token`	
S13	naf-inference / nnwdaf-vflinference scope	值	`stolen_token`	
S14	访问令牌	值	`stolen_token`	
S15	订阅标识 notifCorreId	值	攻击者得不到更多	与 S06 相同：持有该关联标识并不能代为应答生产者。
S16	通知目标 notifUri	值	攻击者得不到更多	与 S11 相同：目标 URI 是公开的。

每条性质在各攻击者条件下的答案

这些攻击者由分析者设定，且在编写任何查询之前就已确定；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该性质给出的答案；“无答案”表示在该攻击者下，证明器对某条主张未作判定，或没有记录任何结果；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`	仅网络：它读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`dishonest_nf`	一个合法的 NF，拥有自己的 TLS 凭据，以及用于 naf-inference 和 nnwdaf-vflinference 范围的自己的 OAuth2 访问令牌；它面向 AF 或 NWDAF VFL 客户端扮演任一 API 的消费者角色，并在自己的请求中选择各值。	TS 33.501 5.9.1 把网络划分为信任区，5.9.2.1 要求每个 NF 对服务请求进行授权；同一信任域内的合法 NF 持有有效凭据，因此当组合流程要针对与其毫无关系的 UE 请求推理时，它正是必须能够抵御的攻击者。任务还要求把外部攻击者与恶意的合法 NF 区分开。	ts-33-501:2859, ts-33-501:2867
`stolen_token`	授权服务器签发给另一个 NF 的、用于该服务范围的 OAuth2 访问令牌，从存储中或从它能观察到的传输中读取得到。	RFC 6749 10.3 要求访问令牌凭据在传输和存储中保持机密，并指出如果令牌未被保密，恶意客户端可以冒充另一个客户端（10.2）。	rfc6749:2859, rfc6749:2827

ID	network	dishonest_nf	stolen_token
A02	成立		
A03	成立		
A08	不成立		
Z01	成立	成立	成立
Z03	成立	不成立	成立

原文和目标

来源：677 个原文单元，377484 字节，冻结在 source-delivery-01.json 中。 目标：5 个已批准（A02、A03、A08、Z01、Z03）；所提问题：3 个。 目标清单按草稿原样、事先经 --approve-targets 批准。

宿主按其文档化的默认值（任务 `decisions: auto`）做出的决定，请你核对：

- approve_package：批准源文包 protocol-e60fcf52f8ed63a9b30641206c35

本步骤自报：2 个请求（2 个失败），0.000 USD，输入 356920 个 token，输出 3708 个，262 s。

关于证明器和模型的说明

- A08：在 ProVerif 中作答，分析者为此目标指定了 changing_state

简化代数的 ProVerif 模型（xor、dh_algebra、other_algebra）给攻击者的能力比真实运算更少：在该模型中得到证明，就是对更弱攻击者的证明；在该模型中发现攻击，那就是真实的攻击。省略了对变化值检查（changing_state）的 ProVerif 模型会让参与方接受更多：在该模型中得到证明可能成立，但发现的攻击可能不过是因为缺少了这项检查。Tamarin+ Agent 按原样对它们建模。

分析者的状态复核

这部分是分析者自己对原文的解读，不是证明器的答案。“由 ProVerif 展示”下的“是”表示 ProVerif 在展开的模型中找到了包含这些步骤的轨迹，因此这些步骤是可能发生的；说它们会破坏某个目标，只以答案表中的一次攻击为依据，而它们还付出了什么代价，则是分析者的解读。“未发现”只说明查看了哪些模式，并不证明任何东西。

值	由谁保存	何时变化	何时检查	引用
notifCorreId、notifUri 以及外部订阅的分析目标（UE），连同内部 VFL 订阅的 notifCorrId	AF（VFL 服务器），针对外部 Naf_Inference 订阅以及关联的 Nnwdaf_VFLInference 订阅	在创建 Individual Inference Subscription 的 POST 上（s0040）以及在更新它的 PUT/PATCH 上（s0055）；随后 AF 以相同的 notifCorrId 更新关联的 Nnwdaf_VFLInference 订阅（s0059）。	当 VflInferNotif 到达时：AF 只匹配 notifCorrId（s0419、s0593）；请求该轮次时生效的分析目标不与通知中的任何内容进行比较。	s0040、s0055、s0059、s0419、s0593
notifCorreId 及其订阅的当前分析目标	NWDAF 消费者	在创建时以及在其发送的每个 PUT/PATCH 上（s0055）。	在每个 InferNotif 上：只比较 notifCorreId（s0086、s0246）。	s0055、s0086、s0246、s0088
notifCorrId、notifUri、UE 目标以及 VFL 推理订阅的 VFL 关联 ID	NWDAF VFL 客户端	在其收到的每个 Nnwdaf_VFLInference_Subscribe 上，即同一订阅的创建或更新（s0355）；VFL 关联 ID 是 VFL 过程的唯一句柄（s0590）。	当它发送 VflInferNotif 时，只填充 notifCorrId 和 vflInferResults（s0419、s0593）。	s0355、s0419、s0590、s0593、s0631

模式	结果	目标	由 ProVerif 显示	步骤
replay	candidate	A08	是：ProVerif 在 bounded.pv 上证伪 `a08`	NWDAF 为 supi1 创建 Individual Inference Subscription，带有 notifCorreId 和 notifUri（s0040）。/ AF 为 supi1 创建关联的 Nnwdaf_VFLInference 订阅，带有自己的 notifCorrId（s0355）。/ NWDAF 将同一订阅更新为 supi2（s0055）；AF 更新内部订阅，保持相同的 notifCorrId（s0059）。/ VFL 客户端为 supi1 计算的轮次仍在进行中，并到达 AF。/ AF 按 notifCorrId 匹配它，报告给 NWDAF，NWDAF 将其作为 supi2 的结果接受（s0086）。
update_before_check	candidate	A08	是：ProVerif 在 bounded.pv 上证伪 `a08`	AF 在 notifCorrId V 下持有 supi1 的 VFL 订阅。/ NWDAF 将外部订阅更新为 supi2（s0055）。/ AF 立即将 VFL 订阅的目标替换为 supi2，并将更新发送给客户端（s0059）。/ 随后 AF 接受下一个携带 notifCorrId V 的 VflInferNotif，而不检查它是否属于新请求（s0419）。
race_between_sessions	candidate	A08	是：ProVerif 在 bounded.pv 上证伪 `a08`	NWDAF 的创建和更新是对同一 Individual Inference Subscription 的两个请求（s0055）。/ AF 的两个 Nnwdaf_VFLInference_Subscribe 请求（创建和更新）以相同顺序到达 VFL 客户端，但客户端对第一个请求的轮次已经在途。（s0059）/ AF 将进行中的轮次作为更新后订阅的答案并报告它（s0086）。
repeat_one_time_action	nothing found			被拒绝的更新返回错误并使订阅保持原状（s0064）；这些操作不安装任何密钥、计数器或一次性资源。
desynchronisation	nothing found			文稿没有说 AF 和消费者保持不同的目标：两者最终都在 supi2 上；分歧在于结果内容，而不在于所存储的订阅。
no_rollback_on_failure	nothing found			失败的创建或更新返回 HTTP 错误（s0050、s0064）且不改变所存储的订阅；不会留下后续消息可以利用的状态。
distinguishable_failure	nothing found			这些操作中唯一的失败应答是带有 ProblemDetails 主体的 HTTP 状态码（s0050、s0088、s0367）；建模流程中没有任何内容依据它们进行分支，因此没有失败应答能区分某一方或某个存储值。
wrap_or_window	nothing found			订阅状态没有计数器、序列号或接受窗口；唯一的标识符是 notifCorrId，它从不回绕。

分析者为目标命名的内容：

步骤	目标	特征	原因
47	A08	changing_state	A08 依赖推理订阅作为变化的值：消费者替换同一 Individual Inference Subscription 的分析目标，AF 用相同的 notifCorrId 替换关联的 Nnwdaf_VFLInference 订阅的目标，而该性质关乎该上下文接受哪一轮结果。模型在 bounded.pv 中把该生命周期展开为固定的三步（创建、更新、通知）。
47	A02、A03、Z01、Z03	plain_primitives、other	A02、A03、Z01 和 Z03 仅依赖建模为成对认证加密信封（TLS 会话）的 SBI 传输，以及建模为绑定到主体、受众和范围且不可伪造的值的 OAuth2 访问令牌；不需要代数定律。“other”特征就是访问令牌，模型将其理想化为不可伪造的项，而不是带有效期的签名 JWT，因此令牌过期和撤销未被建模。

分析者的结束语

组合流程的模型（在受信任的 AF 上创建/更新/通知 Naf_Inference 订阅，连同 Nnwdaf_VFLInference 订阅以及向 NWDAF VFL 客户端的通知）运行一个完整会话（model.pv，到达 EndRun），而 bounded.pv 将同一生命周期表述为固定的三步展开。

答案均经宿主重新运行：两个订阅跳的对等认证 A02 针对网络攻击者得到证明（2 条主张，带有被证伪的对照）。字段与关联一致性 A03（内部 notifCorrId、资源与分析目标的更新、消费者自己的 notifCorreId）得到证明（3 条主张，带有对照）。Z01，即 AF 和 VFL 客户端处的令牌检查，针对网络攻击者、持有自己令牌的合法 NF 以及被盗令牌均得到证明，并带有一个对照：AF 接受一个令牌属于另一范围的请求。Z03 被拆分：令牌不能为另一消费者出示，且网络攻击者无法读取推理结果（已证明），但仅持有服务级范围的合法 NF 在 NWDAF VFL 客户端为另一功能的 VFL 关联 ID 和 UE 进行订阅并收到结果（被证伪；结论为 depends_on_ambiguity，因为参与者规则位于 TS 29.552，在原文单元之外）。A08 在 model.pv 和 bounded.pv 上均被证伪：在消费者将其订阅从一个 UE 更新为另一个之后，AF 报告了为第一个 UE 计算且仍在进行中的 VFL 轮次，消费者将其作为更新后订阅的答案接受，因为两个通知都不携带 UE 集合或轮次标识符，唯一的比较是未改变的 notifCorrId。这就是主要发现（新颖性：文稿中未记录）。

状态审查记录了某一方保留和改变的三个值，并将 replay、update_before_check 和 race_between_sessions 标记为已确认的候选（均由 a08 查询显示），其余五种模式标记为 nothing found。

进一步推进的障碍：TLS 会话和 OAuth2 令牌被理想化（没有过期、撤销、记录重放保护或 NRF），删除和多会话状态未被建模，且两项建议（两个通知中的轮次标识符；VFL 客户端中的参与者检查）在预算内均未用 check_fix 检查。令牌过期和 TS 29.552 的参与者规则需要 Tamarin+Agent 或缺失的规范才能确定。