DCCF 分析协调直连路径的安全分析

本报告的其他语言版本：English。

19.7.0 · ProVerif+ Agent 报告

文稿	5G System; Data Collection Coordination Services; Stage 3 （协议定义）; 5G System; Network Data Analytics Services; Stage 3 （辅助）
检查的性质	14 条：14 条成立，0 条不成立
发现	无

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

DCCF 为不直接寻址 NWDAF 的 NF 服务消费者协调分析。消费者在 DCCF 处订阅分析通知，DCCF 在一个 NWDAF 处订阅匹配的事件，DCCF 再以消费者订阅的关联标识符把 NWDAF 的通知转发给消费者。

消费者得到保证：其订阅会以它所请求的分析得到服务，通知会以其自己的关联标识符送达。DCCF 得到保证：请求来自其所声称的 NF。NWDAF 得到保证：上游订阅由 DCCF 在 NRF 授予的范围内发起。

各方：

- **NF 服务消费者**：订阅分析，接收通知。持有：其用于 ndccf-datamanagement 范围的 OAuth2 令牌；anaNotifUri。
- **DCCF**：把一个消费者订阅映射为一个 NWDAF 订阅。持有：其用于 Nnwdaf_EventsSubscription 范围的 OAuth2 令牌；自己的通知 URI。
- **NWDAF**：产生分析并发送通知。持有：事件订阅记录。

图 1 展示了文稿所规定的交换过程。

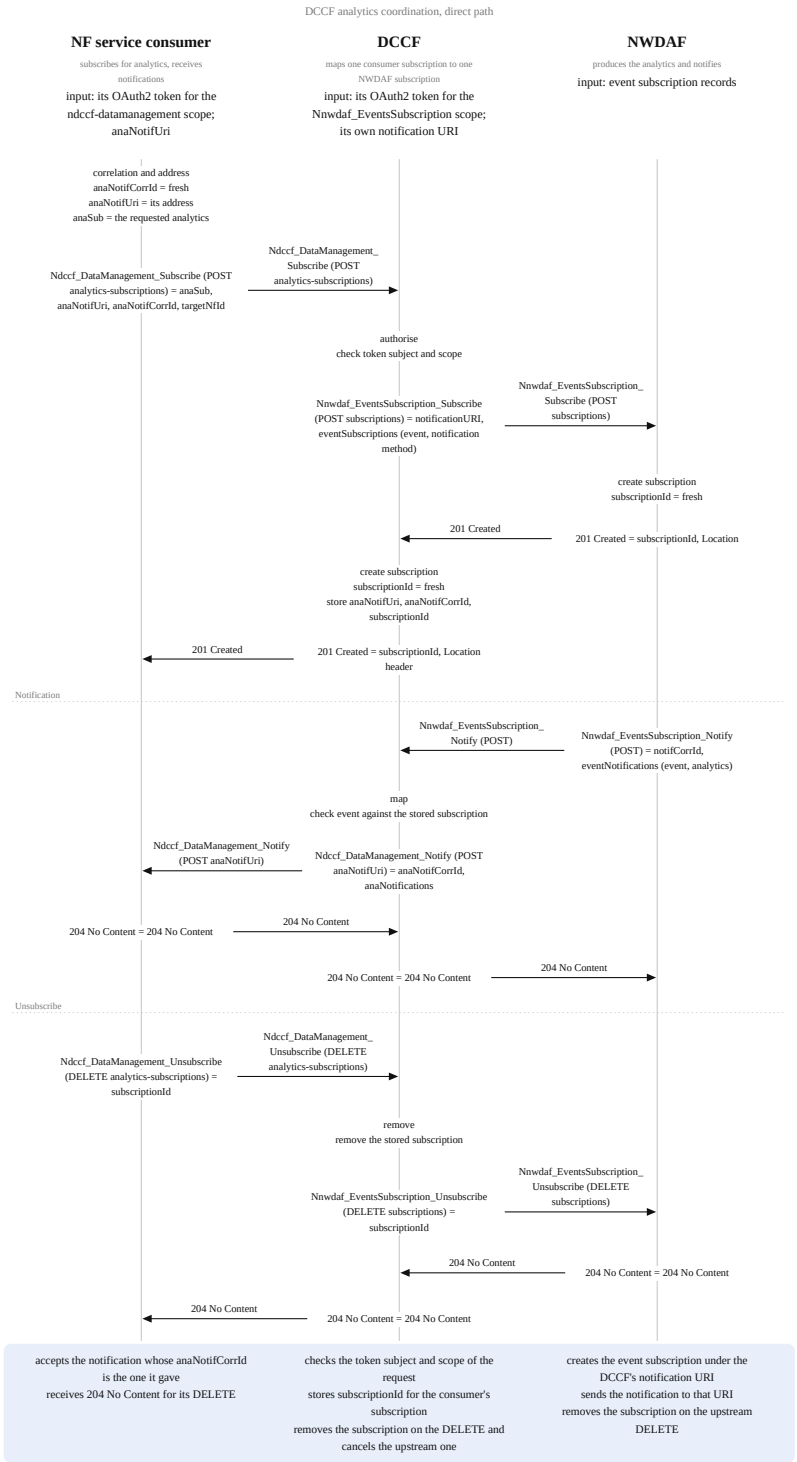


图 1. 文稿所规定的协议。

分析的范围见附录 D：分析了什么、省略了什么，以及它依据的文稿章节。

2 发现

没有发现。 分析没有发现文稿尚未说明或尚未排除的内容。第 3 节的表格给出了每条性质的结果。

无发现：所有检查过的性质在模型中均成立，分析也没有复现文稿所述的任何弱点。全部十四个目标都有答案：十个由证明回答，三个另由展开订阅生命周期的证明回答，取消类目标由终止路径的可达性回答。这些证明依赖原文未明确写出的两点：TLS 作为两个 NF 之间的私有通道，以及对令牌主体和范围的检查。

还有两个状态候选尚未确认：DCCF 在上游删除得到确认之前就删除了自己的订阅记录；上游删除失败会使两侧失去同步。

3 检查过的性质

每一行是一条提交给 ProVerif 的性质。结果就是 ProVerif 对分析者所建协议模型的回答；价值以及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	**操作对端身份一致性。** 每当 DCCF 接受一个 analytics 订阅请求（201 Created），或 consumer 接受一条 analytics 通知（204/200），或 NWDAF 接受 DCCF 的上游订阅请求时，声称的对端必须确实以本方身份运行过对应服务操作。	无	成立	中	是
A03	**通知关联与会话绑定。** consumer 接受的每条通知，其 anaNotifCorrId 与 anaNotifUri 必须与 consumer 此前为该订阅提供的值一致，且对应 DCCF 确实为该 consumer 创建过该订阅；DCCF 接受的上游订阅与 consumer 请求的 analytics 事件一致。	无	成立	中	是
A04	**不重复接受通知。** consumer 接受的每条 analytics 通知对应 DCCF 一次不同的通知运行（以 anaNotifCorrId 与通知内容区分），同一通知实例不被重复接受为新的通知。	无	成立	低	不明确
K01	**访问令牌与TLS密钥保密。** 攻击者不能获得任一合法 NF 的 OAuth2 访问令牌或 TLS 会话密钥；每个令牌只对其合法持有者可用。	无	成立	低	是
D01	**通知地址绑定至订阅者。** consumer 接受的每条通知，其 anaNotifUri 与 anaNotifCorrId 必须来自该 consumer 的真实订阅请求，且发送方为 DCCF；恶意合法 NF 不能使通知被投递到其控制的地址。	无	成立	中	不明确
A08	**上游订阅与请求匹配。** DCCF 创建的上游订阅所指向的 NWDAF 与 analytics 事件必须与 consumer 请求中的 targetNfId/targetNfSetId 与 anaSub 一致；consumer 接受的通知的 anaNotifCorrId 必须与订阅值一致。	无	成立	中	是
Z01	**每个受保护操作的授权。** DCCF 或 NWDAF 提交的每个受保护操作（创建/删除订阅、发送通知）必须有来自 NRF 的有效授权许可，且许可的 scope 覆盖该操作。	无	成立	中	是
Z03	**令牌主体受众范围绑定。** 每个授权许可的 subject、audience、scope 与使用上下文必须与提交该操作的 NF 及操作一致；令牌不能被移植到其他 NF 或其他操作。	无	成立	中	是
Z04	**退订后不再通知。** 取消（DELETE 成功）或终止（terminationReq=true）生效之后，DCCF 不再为该订阅发送新通知；在途通知按明确界定的有限状态处理。	无	在界内成立（变化值展开到 2 步）	中	不明确
S05	**已终止订阅标识符失效。** 订阅终止（取消或 terminationReq）生效点之后，旧 subscriptionId 或旧订阅状态不能触发新的通知发送。	无	在界内成立（变化值展开到 2 步）	中	不明确

ID	性质	假定的泄露	结果	价值	文稿是否已写
U01	**上下游订阅对应。** DCCF 为 consumer 创建的下游订阅与它向 NWDAF 创建的上游订阅一一对应，通知的 anaNotifCorrId 在两层之间不错配。	无	成立	中	是
U02	**通知地址来自订阅者自身。** DCCF 记录的 anaNotifUri 必须来自发起该订阅请求的 consumer 本身，恶意合法 NF 不能替换其他 consumer 的通知接收地址。	无	成立	中	不明确
U03	**退订传播至上游。** consumer 取消订阅后 DCCF 取消对应上游订阅；取消生效点之后在途通知不再被接受；生命周期用有限状态界定。	无	在界内成立（变化值展开到 2 步）	中	不明确
X01	**分析载荷对其他NF保密。** 除订阅的 consumer 外，任何一方都不得获知该订阅通知的分析内容，网络攻击者和持有自己令牌的其他合法 NF 都不行。	持有 ndccf-datamanagement 范围令牌的合法 NF；它可以调用 DCCF API 并选择 anaNotifUri、事件和目标 NWDAF	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.

提出的问题，以及分析者的回答：

问题	回答	依据
Q1: DCCF 内外订阅和 notification correlation ID 的映射	DCCF 在同一进程内为每个上游订阅保留下游订阅：它转发的每条通知都来自该订阅的上游通知，并携带消费者的 anaNotifCorrId，消费者不接受其他任何内容。	U01, A03, A08
Q2: 合法 NF 无法替换别人的通知接收地址	合法 NF 只能记录自己的身份和自己的地址，因为 DCCF 把请求绑定到令牌主体，所以它无法替换其他消费者的地址。DCCF 不检查该地址是否属于请求者，因此这一保证依赖上述身份绑定，以及按请求会话路由通知。	U02, D01, Z03
Q3: 取消传播与在途通知用有限状态明确限定	退订到达 DCCF 并传播到 NWDAF，在展开模型中，到达终止点之后才到的在途通知不会被投递。原文没有规定两次删除的先后顺序，而 DCCF 先删除自己的记录，因此上游删除失败会使两侧失去同步；该候选被报告为未确认。	U03, Z04, S05

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什么、没能给出什么，其中密码学按理想情况处理，与任何实现无关。

按分析者的陈述，本次分析不覆盖以下内容：

- TLS 被建模为每对端点之间的一个私有通道，因此网络攻击者既不能读取也不能更改已建立的会话；原文把 TLS 交给基线处理。
- 令牌检查（主体和范围）按基线要求建模；所选文本只说明可以使用 OAuth2 并给出各范围名称。
- DCCF 和 NWDAF 没有复制：模型每条通道只有一个会话，因此这些答案谈论的是写明的会话，而不是任意数量的会话。
- 没有对访问令牌的泄露建模；持有者令牌一旦泄露，冒用按定义随之而来，文稿转而要求令牌保密。
- 经 UDM 的用户同意、静音标志、特性协商和重定向均未建模。
- 通知按请求者的 TLS 会话路由，因此一个不属于任何人的已注册地址在模型中没有投递效果。
- 在第二个模型中订阅生命周期展开到两个通知步；关于迟到的通知永远不会被接受的直接查询返回不确定。

- 这条路径上没有密码学原语起实质作用：令牌是一个私有构造子，载荷是一个新鲜值。

宿主记录的内容：

- Z04、S05、U03 的答案依赖模型所做的一处简化（附录 D）。
- 没带对照查询的证明（附录 C）：A02: a02a, A02: a02b, A02: a02c, A03: a03, A04: a04, K01: k01, D01: a03, D01: a02b, A08: a08, Z01: a02b, Z03: a02b, U01: u01, U02: a02b, X01: x01。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未解决、怎样才能解决，见附录 A。

附录 A：逐条性质的解读

以下是分析者本人对证明器回答的解读，不是证明器的回答：这些回答对协议意味着什么，解读依赖什么，解读能否照原样使用，以及它有多大价值。

A02: 操作对端身份一致性

每当 DCCF 接受一个 analytics 订阅请求（201 Created），或 consumer 接受一条 analytics 通知（204/200），或 NWDAF 接受 DCCF 的上游订阅请求时，声称的对端必须确实以本方身份运行过对应服务操作。

DCCF 只为其所携带令牌指明的身份接受订阅，NWDAF 只接受来自 DCCF 的上游订阅，持有自己令牌的合法 NF 无法以其他 NF 的名义行事。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 中：在被假定的检查下，它确认了文稿所述的授权目标。
- 文稿中有述：是。文稿所述之处：s0412、s0413、s0415
- 依据：每对端点之间的私有通道代表 TLS；主体与范围检查按基线要求被假定；每个通道一个会话
- 下一步：此路径无需下一步。

A03: 通知关联与会话绑定

consumer 接受的每条通知，其 anaNotifCorrId 与 anaNotifUri 必须与 consumer 此前为该订阅提供的值一致，且对应 DCCF 确实为该 consumer 创建过该订阅；DCCF 接受的上游订阅与 consumer 请求的 analytics 事件一致。

consumer 接受的通知，其关联标识符总是 DCCF 为该 consumer 记录的某个订阅的标识符，地址也是该 consumer 提供的地址。不能使 consumer 接受另一订阅的通知。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 中：这是协调功能的核心绑定，且按规范成立。
- 文稿中有述：是。文稿所述之处：s0060、s0061
- 依据：consumer 检查关联标识符与 DCCF 的令牌；原文只要求回显该标识符；每对端点之间的私有通道代表 TLS
- 下一步：此路径无需下一步。

A04: 不重复接受通知

consumer 接受的每条 analytics 通知对应 DCCF 一次不同的通知运行（以 anaNotifCorrId 与通知内容区分），同一通知实例不被重复接受为新的通知。

consumer 接受的每条通知对应 DCCF 一次不同的转发运行，因此重复投递不会被当作新通知接受。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 低：原文未规定防重放规则，该结果来自新的关联标识符。
- 文稿中有述：不明确。所依据的原文：s0061
- 依据：consumer 每个订阅会话接受一条通知；未建模重传或失败路径
- 下一步：无。

K01: 访问令牌与TLS密钥保密

攻击者不能获得任一合法 NF 的 OAuth2 访问令牌或 TLS 会话密钥；每个令牌只对其合法持有者可用。

任何一方都无法获知另一 NF 的访问令牌：每个令牌只留在其持有者处。对照查询表明，放到开放网络上的令牌会被获知，因此该查询并非空。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 低：它直接来自基线给出的传输假定。
- 文稿中有述：是。文稿所述之处：s0412
- 依据：每对端点之间的私有通道代表 TLS；令牌从不在开放网络上发送
- 下一步：无。

D01: 通知地址绑定至订阅者

consumer 接受的每条通知，其 anaNotifUri 与 anaNotifCorrId 必须来自该 consumer 的真实订阅请求，且发送方为 DCCF；恶意合法 NF 不能使通知被投递到其控制的地址。

到达 consumer 通知地址的内容属于 DCCF 为该 consumer 存储的某个订阅。合法 NF 只能登记自己的身份和自己的地址，因此无法让另一 consumer 的通知被投递给自己。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 中：它表明该绑定之所以成立，是因为身份与令牌绑定，而不是因为检查了地址。
- 文稿中有述：不明确。所依据的原文：s0007、s0060
- 依据：通知按请求 NF 的 TLS 会话路由；DCCF 不检查地址是否属于请求者；原文未规定此类检查
- 待解：NF 登记一个并非自己的地址能获得什么
- 下一步：建立一个模型，使通知路由按登记的地址而不是按会话进行。

A08: 上游订阅与请求匹配

DCCF 创建的上游订阅所指向的 NWDAF 与 analytics 事件必须与 consumer 请求中的 targetNfId/targetNfSetId 与 anaSub 一致；consumer 接受的通知的 anaNotifCorrId 必须与订阅值一致。

consumer 请求的事件就是上游订阅的事件，其他事件的通知不会转给 consumer。不诚实的 NWDAF 无法通过 DCCF 传递未被请求的事件。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 中：它表明了使两层保持一致的检查。
- 文稿中有述：是。文稿所述之处：s0021、s0061
- 依据：DCCF 原样转发 consumer 的事件；NWDAF 被建模为可以选择其通知的事件，DCCF 对此进行过滤
- 下一步：无。

Z01: 每个受保护操作的授权

DCCF 或 NWDAF 提交的每个受保护操作（创建/删除订阅、发送通知）必须有来自 NRF 的有效授权许可，且许可的 scope 覆盖该操作。

DCCF 只接受其令牌指明请求 NF 并带有服务范围的请求，NWDAF 对 DCCF 的上游请求也如此。API 为整个服务定义一个范围，因此该范围无法区分一个操作与另一个操作、一个订阅与另一个订阅。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 中：它确认了所述框架，同时表明授权是按服务而非按资源进行的。
- 文稿中有述：是。文稿所述之处：s0412、s0415
- 依据：令牌检查被假定；API 级范围被建模为覆盖所有操作的一个字符串
- 下一步：无。

Z03: 令牌主体受众范围绑定

每个授权许可的 subject、audience、scope 与使用上下文必须与提交该操作的 NF 及操作一致；令牌不能被移植到其他 NF 或其他操作。

令牌只能由签发对象 NF 使用：DCCF 只接受其令牌主体所对应的请求。受众与有效期未被建模，因此对其不作任何主张。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 中：它回答了模型能够表达的绑定部分，并标明其余部分待解。
- 文稿中有述：是。文稿所述之处：s0415、s1227
- 依据：只建模了主体与范围；每对端点之间的私有通道代表 TLS
- 待解：受众与有效期绑定
- 下一步：阅读基线中关于受众与有效期的规则，并扩展令牌。

Z04: 退订后不再通知

取消（DELETE 成功）或终止（terminationReq=true）生效之后，DCCF 不再为该订阅发送新通知；在途通知按明确界定的有限状态处理。

在 DELETE 被接受后，DCCF 没有路径再投递通知，并且在展开模型中，该时点之后到达的通知会被丢弃，不会到达 consumer。

- 结果：在界内成立（变化值展开到 2 步）；所问是否得到回答：是；可用但有保留
- 值 中：它表明终止行为在展开模型中成立，但需注意该检查本身不在原文中。
- 文稿中有述：不明确。所依据的原文：s0040、s0041
- 依据：生命周期展开为两个通知步；终止点之后的丢弃是建模选择；原文未规定此类检查；关于迟到的通知永不被接受的直接查询无结论
- 待解：终止时点在途通知的确切处理
- 下一步：由编辑就在途通知作出说明，然后建立遵循该说明的模型。

S05: 已终止订阅标识符失效

订阅终止（取消或 terminationReq）生效点之后，旧 subscriptionId 或旧订阅状态不能触发新的通知发送。

在展开模型中，携带已终止订阅的关联标识符的消息不会向 consumer 产生新的投递。

- 结果：在界内成立（变化值展开到 2 步）；所问是否得到回答：是；可用但有保留
- 值 中：这是目标提出的标识符重用问题，在展开模型上得到了回答。
- 文稿中有述：不明确。所依据的原文：s0041、s0069
- 依据：生命周期展开为两步；已终止状态通过丢弃后续通知来建模
- 下一步：无。

U01: 上下游订阅对应

DCCF 为 consumer 创建的下游订阅与它向 NWDAF 创建的上游订阅一一对应，通知的 anaNotifCorrId 在两层之间不错配。

DCCF 为某个订阅转发的每条通知都来自该订阅的上游通知，并携带其内容，因此 consumer 的订阅与 DCCF 的上游订阅一一对应。

- 结果：成立；所问是否得到回答：是；可用但有保留
- 值 中：它针对直接路径回答了用户提出的映射问题。
- 文稿中有述：是。文稿所述之处：s0021、s0026
- 依据：DCCF 在一个进程中保存该映射，每个上游订阅对应一个下游订阅；未建模该映射的并发删除或修改
- 下一步：无。

U02: 通知地址来自订阅者自身

DCCF 记录的 anaNotifUri 必须来自发起该订阅请求的 consumer 本身，恶意合法 NF 不能替换其他 consumer 的通知接收地址。

为订阅记录的地址就是令牌所指 NF 的请求中的地址，因此合法 NF 无法以自己身份记录另一 consumer 的地址。DCCF 不检查地址是否属于请求者，模型按请求者的会话路由通知，因此外来地址不会产生投递效果。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值中：它以明确陈述模型无法展示的内容回答了地址问题。
- 文稿中是否说明：不明确。所依据的原文：s0007、s0021
- 依据：按请求者的 TLS 会话进行通知路由；原文中未对地址做所有权检查
- 待解决：按注册地址路由的 DCCF
- 下一步：建立基于地址路由的模型，测试外部地址是否可被滥用。

U03: 退订传播至上游

consumer 取消订阅后 DCCF 取消对应上游订阅；取消生效点之后在途通知不再被接受；生命周期用有限状态界定。

消费者的退订会传播至 NWDAF，在该点之后到达的在途通知不会被传递给消费者。DCCF 在上游删除确认之前就移除了自己的记录，这就是单独报告的状态候选。

- 结果：在界内成立（变化值展开到2步）；是否回答了所问：是；可用但有保留
- 价值中：它回答了传播问题，并标出了仍然存在的顺序缺口。
- 文稿中是否说明：不明确。所依据的原文：s0039、s0041、s0981
- 依据：展开两个通知步骤；未对上游删除失败建模
- 待解决：如果上游删除失败会发生什么
- 下一步：关于重试或回滚的原文陈述，或失败路径的模型。

X01: 分析载荷对其他NF保密

除订阅消费者外，任何一方都不会获知该订阅通知的分析内容，网络攻击者和持有自己令牌的另一合法 NF 都不例外。

传递给消费者的分析内容只留在该消费者处：网络攻击者和另一合法 NF 都不会获知。合法 NF 确实会收到自己的分析，因此该主张针对的是另一消费者通知的内容。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值中：这是通知路径本应提供的机密性目标，已对写明的会话证明。
- 文稿中是否说明：是。文稿中的位置：s0060、s0061
- 依据：内容是派生自上游订阅的值；每对端点之间的私有通道代表 TLS
- 下一步：此路径无需下一步。

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，以及攻击和每个攻击的分析者判定。

目标	级别	界	查询	对照	攻击	主张
A02	proved		a02a			4 proved
A03	proved		a03			2 proved
A04	proved		a04			1 proved
K01	proved		k01	1 of 2		2 proved
D01	proved		a03			2 proved
A08	proved		a08			2 proved
Z01	proved		a02b			2 proved
Z03	proved		a02b			2 proved
Z04	bounded	变化值展开到2步	once	checked		1 bounded, 1 reachable
S05	bounded	变化值展开到2步	once	checked		1 bounded, 1 reachable
U01	proved		u01			1 proved
U02	proved		a02b			2 proved
U03	bounded	变化值展开到2步	once	checked		1 bounded, 1 reachable
X01	proved		x01			2 proved

逐条主张，用分析者对每条主张的表述；每条的回答来自证明器：

目标	主张	攻击者	回答	查询	对照
A02	当消费者接受其订阅的 201 Created 时，该创建携带消费者自己发起的订阅请求的 anaNotifCorrId 和 anaNotifUri	`network`	proved	a02a	none
A02	当 DCCF 接受订阅请求并存储订阅时，该请求是在其所声明的身份下、以该请求的地址和相关标识符发出的	`network`	proved	a02b	none
A02	当 NWDAF 接受上游订阅时，DCCF 已针对该相关标识符和事件执行了对应的上游订阅操作	`network`	proved	a02c	none
A02	持有自己令牌的合法 NF 无法让 DCCF 以另一消费者的身份存储订阅（令牌主体必须等于请求中的身份）	`malicious_nf`	proved	a02b	none
A03	消费者接受的通知携带 DCCF 为该消费者存储的订阅的 anaNotifCorrId，因此与该订阅绑定	`network`	proved	a03	none
A03	另一合法 NF 无法让消费者把通知作为该消费者的订阅接受：相关标识符是 DCCF 为该消费者存储的那个	`malicious_nf`	proved	a03	none
A04	消费者接受的每条通知对应该 DCCF 的一次不同转发运行；没有通知被接受两次	`network`	proved	a04	none
K01	任何其他方都不会获知合法 NF 的 OAuth2 访问令牌：令牌留在持有者处	`network`	proved	k01	checked
K01	持有自己令牌的合法 NF 除自己的令牌外不会获知任何令牌	`malicious_nf`	proved	k01	none

目标	主张	攻击者	回答	查询	对照
D01	到达消费者 anaNotifUri 的内容与 DCCF 为该消费者存储的订阅匹配，并带有该订阅的相关标识符	`network`	proved	a03	none
D01	合法 NF 无法让 DCCF 为以其自己名义发出的订阅记录另一消费者的地址，也无法让 DCCF 把另一消费者的通知投递给它	`malicious_nf`	proved	a02b	none
A08	到达 NWDAF 的上游订阅携带消费者所请求的分析事件，通知相关性在两层之间一致	`network`	proved	a08	none
A08	不诚实的 NWDAF 无法让没有消费者订阅的事件进入上游：DCCF 只传递已订阅的事件，针对另一事件的通知不会被转发	`nwdaf_dishonest`	proved	a08	none
Z01	DCCF 仅对携带有效令牌的请求存储订阅，该令牌的主体是请求所声明的 NF，且其范围覆盖 ndccf-datamanagement	`network`	proved	a02b	none
Z01	持有自己令牌的合法 NF 无法以另一 NF 的身份存储订阅，因此仅凭范围并不能授权代表另一 NF 行事	`malicious_nf`	proved	a02b	none
Z03	令牌只用于其签发对象 NF：DCCF 仅接受针对其携带令牌主体的请求	`network`	proved	a02b	none
Z03	合法 NF 无法移植自己的令牌以代表另一 NF 行事，或将其移入请求中的另一身份	`malicious_nf`	proved	a02b	none
Z04	终止路径存在：被接受的退订到达 DCCF，上游 NWDAF 订阅被移除	`network`	reachable	z04r	
Z04	在终止点之后，该订阅的进一步通知不会被投递：它被 DCCF 丢弃，消费者对每条通知至多接受一次	`network`	bounded（变化值展开到2步）	once	checked
S05	DCCF 在接受 DELETE 时移除自己的订阅记录	`network`	reachable	s05r	
S05	在终止之后携带已终止订阅相关标识符的消息无法触发对消费者的新投递	`network`	bounded（变化值展开到2步）	once	checked
U01	DCCF 为某订阅转发的每条通知都来自它为该书阅收到的上游通知，因此两层对应	`network`	proved	u01	none
U02	DCCF 把其所声明 NF 的请求中携带的地址记录为 anaNotifUri，该订阅的每条通知都携带该订阅的相关标识符	`network`	proved	a02b	none
U02	合法 NF 无法替换另一消费者的通知地址：它只能以自己的身份记录自己的地址	`malicious_nf`	proved	a02b	none
U03	被接受的退订会被传播：DCCF 为被删除的消费者订阅移除上游 NWDAF 订阅	`network`	reachable	z04r	
U03	退订传播到上游订阅，在该点之后到达的在途通知不会被传递给消费者	`network`	bounded（变化值展开到2步）	once	checked
X01	除订阅消费者外，任何一方都不会获知其通知的分析内容	`network`	proved	x01	none
X01	合法 NF 不会获知传递给另一消费者的分析内容，即使它可以订阅并收到自己的分析	`malicious_nf`	proved	x01	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，并把每条性质交给 ProVerif；第 3 节的每个结果都是证明器的回答。

ProVerif+ Agent 会话 session-20261115T094237，2026-11-15。状态：已完成。模型：deepseek-v4-1-flash-261017。步骤：47，证明器 3 s，实际耗时 13 min，成本 0.110 USD。

ProVerif：运行 48 次证明，45 次判定，3 次无答案，1 s，记录 28 个回答。

分析了什么

协议	DCCF analytics coordination direct path
版本	19.7.0
分析范围	单 NF consumer→DCCF→单 NWDAF，非 UE 聚合 analytics 直接通知路径；创建一个上游订阅与一个下游订阅映射，通知和取消；排除 MFAF、ADRF、缓存复用和多 NWDAF 聚合。必须建模上游服务，不能把 DCCF 数据凭空生成。
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	1266 个编号原文单元（927204 字节），来自下列章节。本报告中如 s0001 这样的引用即其中之一

分析所依据的文稿章节：

文稿	章节	标题
main	4.2.2.2.2	分析通知的订阅
main	4.2.2.3.2	取消分析通知订阅
main	4.2.2.4.2	关于已订阅分析的通知
main	5.1	Ndccf_DataManagement 服务 API
main	5.1.1	引言
main	5.1.2	HTTP 的使用
main	5.1.2.1	概述
main	5.1.2.2	HTTP 标准头部
main	5.1.2.2.1	概述
main	5.1.2.2.2	内容类型
main	5.1.2.3	HTTP 自定义头部
main	5.1.3	资源
main	5.1.3.1	概览
main	5.1.3.2	资源：DCCF Analytics Subscriptions
main	5.1.3.2.1	描述
main	5.1.3.2.2	资源定义

文稿	章节	标题
main	5.1.3.2.3	资源标准方法
main	5.1.3.2.3.1	POST
main	5.1.3.2.4	资源自定义操作
main	5.1.3.3	资源：Individual DCCF Analytics Subscription
main	5.1.3.3.1	描述
main	5.1.3.3.2	资源定义
main	5.1.3.3.3	资源标准方法
main	5.1.3.3.3.1	PUT
main	5.1.3.3.3.2	DELETE
main	5.1.3.3.4	资源自定义操作
main	5.1.3.4	资源：DCCF Data Subscriptions
main	5.1.3.4.1	描述
main	5.1.3.4.2	资源定义
main	5.1.3.4.3	资源标准方法
main	5.1.3.4.3.1	POST
main	5.1.3.4.4	资源自定义操作
main	5.1.3.5	资源：Individual DCCF Data Subscription
main	5.1.3.5.1	描述
main	5.1.3.5.2	资源定义
main	5.1.3.5.3	资源标准方法
main	5.1.3.5.3.1	PUT
main	5.1.3.5.3.2	DELETE
main	5.1.3.5.4	资源自定义操作
main	5.1.3.6	空白
main	5.1.3.7	空白
main	5.1.4	无关联资源的自定义操作
main	5.1.4.1	概览
main	5.1.4.2	操作：transfer-data-sub
main	5.1.4.2.1	描述
main	5.1.4.2.2	操作定义
main	5.1.5	通知
main	5.1.5.1	概述
main	5.1.5.2	分析通知
main	5.1.5.2.1	描述
main	5.1.5.2.2	目标 URI
main	5.1.5.2.3	标准方法

文稿	章节	标题
main	5.1.5.2.3.1	POST
main	5.1.5.3	数据通知
main	5.1.5.3.1	描述
main	5.1.5.3.2	目标 URI
main	5.1.5.3.3	标准方法
main	5.1.5.3.3.1	POST
main	5.1.5.4	获取通知
main	5.1.5.4.1	描述
main	5.1.5.4.2	目标 URI
main	5.1.5.4.3	标准方法
main	5.1.5.4.3.1	POST
main	5.1.6	数据模型
main	5.1.6.1	概述
main	5.1.6.2	结构化数据类型
main	5.1.6.2.1	引言
main	5.1.6.2.2	类型 NdccfAnalyticsSubscription
main	5.1.6.2.3	类型 NdccfDataSubscription
main	5.1.6.2.4	类型 NdccfAnalyticsSubscriptionNotification
main	5.1.6.2.5	类型 NdccfDataSubscriptionNotification
main	5.1.6.2.6	类型 FormattingInstruction
main	5.1.6.2.7	类型 ProcessingInstruction
main	5.1.6.2.8	类型 ParameterProcessingInstruction
main	5.1.6.2.9	类型 NotifSummaryReport
main	5.1.6.2.10	类型 EventParamReport
main	5.1.6.2.11	类型 ReportingOptions
main	5.1.6.2.12	空白
main	5.1.6.2.13	类型 DccfEvent
main	5.1.6.2.14	类型 NotifyEndpoint
main	5.1.6.2.15	类型：StorageHandlingInformation
main	5.1.6.2.16	类型：DeletionAlert
main	5.1.6.2.17	类型：NotifResponse
main	5.1.6.2.18	空白
main	5.1.6.2.19	类型：DataTransferResp
main	5.1.6.3	简单数据类型与枚举
main	5.1.6.3.1	引言
main	5.1.6.3.2	简单数据类型

文稿	章节	标题
main	5.1.6.3.3	枚举：SummarizationAttribute
main	5.1.6.3.4	枚举：AggregationLevel
main	5.1.6.3.5	枚举：DataCollectionPurpose
main	5.1.6.3.6	枚举：TermCause
main	5.1.6.4	描述备选数据类型或数据类型组合的数据类型
main	5.1.6.5	二进制数据
main	5.1.7	错误处理
main	5.1.7.1	概述
main	5.1.7.2	协议错误
main	5.1.7.3	应用错误
main	5.1.8	特性协商
main	5.1.9	安全
ts-29-520	4.2.1	服务描述
ts-29-520	4.2.1.1	概览
ts-29-520	4.2.1.2	服务架构
ts-29-520	4.2.1.3	网络功能
ts-29-520	4.2.1.3.1	网络数据分析功能（NWDAF）
ts-29-520	4.2.1.3.2	NF 服务消费者
ts-29-520	4.2.2.2	Nnwdaf_EventsSubscription_Subscribe 服务操作
ts-29-520	4.2.2.2.1	概述
ts-29-520	4.2.2.2.2	事件通知的订阅
ts-29-520	4.2.2.2.3	更新事件通知订阅
ts-29-520	4.2.2.3	Nnwdaf_EventsSubscription_Unsubscribe 服务操作
ts-29-520	4.2.2.3.1	概述
ts-29-520	4.2.2.3.2	取消事件通知订阅
ts-29-520	4.2.2.4	Nnwdaf_EventsSubscription_Notify 服务操作
ts-29-520	4.2.2.4.1	概述
ts-29-520	4.2.2.4.2	关于已订阅事件的通知
ts-29-520	5.1.1	引言
ts-29-520	5.1.2	HTTP 的使用
ts-29-520	5.1.2.1	概述
ts-29-520	5.1.2.2	HTTP 标准头部
ts-29-520	5.1.2.2.1	概述
ts-29-520	5.1.2.2.2	内容类型
ts-29-520	5.1.2.3	HTTP 自定义头部
ts-29-520	5.1.3.1	资源结构

文稿	章节	标题
ts-29-520	5.1.3.2	资源：NWDAF Events Subscriptions
ts-29-520	5.1.3.2.1	描述
ts-29-520	5.1.3.2.2	资源定义
ts-29-520	5.1.3.2.3	资源标准方法
ts-29-520	5.1.3.2.3.1	POST
ts-29-520	5.1.3.2.4	资源自定义操作
ts-29-520	5.1.3.3	资源：Individual NWDAF Event Subscription
ts-29-520	5.1.3.3.1	描述
ts-29-520	5.1.3.3.2	资源定义
ts-29-520	5.1.3.3.3	资源标准方法
ts-29-520	5.1.3.3.3.1	DELETE
ts-29-520	5.1.3.3.3.2	PUT
ts-29-520	5.1.3.3.4	资源自定义操作
ts-29-520	5.1.5	通知
ts-29-520	5.1.5.1	概述
ts-29-520	5.1.5.2	事件通知
ts-29-520	5.1.5.2.1	描述
ts-29-520	5.1.5.2.2	操作定义
ts-29-520	5.1.6.2.2	类型 NnwdafEventsSubscription
ts-29-520	5.1.6.2.3	类型 EventSubscription
ts-29-520	5.1.6.2.4	类型 NnwdafEventsSubscriptionNotification
ts-29-520	5.1.6.2.5	类型 EventNotification
ts-29-520	5.1.6.2.7	类型 EventReportingRequirement
ts-29-520	5.1.6.2.22	类型 NetworkPerfRequirement
ts-29-520	5.1.6.2.23	类型 NetworkPerfInfo
ts-29-520	5.1.6.2.30	类型 ThresholdLevel
ts-29-520	5.1.6.2.49	类型 ConsumerNfInformation
ts-29-520	5.1.6.3.3	枚举：NotificationMethod
ts-29-520	5.1.6.3.4	枚举：NwdafEvent
ts-29-520	5.1.6.3.10	枚举：NetworkPerfType
ts-29-520	5.1.6.3.26	枚举：TermCause
ts-29-520	5.1.7	错误处理
ts-29-520	5.1.7.1	概述
ts-29-520	5.1.7.2	协议错误
ts-29-520	5.1.7.3	应用错误
ts-29-520	5.1.8	特性协商

文稿	章节	标题
ts-29-520	5.1.9	安全

源文步骤在文稿中定位到的协议用途：单 NF consumer→DCCF→单 NWDAF，非 UE 聚合 analytics 直接通知路径；创建一个上游订阅与一个下游订阅映射，通知和取消；排除 MFAF、ADRF、缓存复用和多 NWDAF 聚合。必须建模上游服务，不能把 DCCF 数据凭空生成。

对照文稿定性质

在编写任何查询之前，分析者把草拟的性质清单与文稿本身对协议用途的说明逐一对照。名称、性质所涉内容以及文稿的说法均属分析者的解读；所列位置确实存在于文稿中。

ID	简称	对象	文稿怎么说	出处
A02	操作对端身份一致性	consumer 得到保证：DCCF 以及接受上游订阅的 NWDAF 就是它们自称的对端；DCCF 得到保证：请求来自它所指名的 consumer	身份携带在请求中，并由来自 NRF 的 OAuth2 令牌授权 (s0005, s0412, s0413)	s0005, s0412
A03	通知关联与会话绑定	consumer 得到保证：通知携带它给出的 anaNotifCorrId 和目的地，并且属于 DCCF 为它创建的订阅；上游携带它请求的事件	请求中必须包含 anaSub、anaNotifUri、anaNotifCorrId (s0006, s0007, s0008)，并在通知中返回 (s0060, s0061)	s0061
A04	不重复接受通知	consumer：每个被接受的通知都是 DCCF 为该订阅执行的一次不同通知运行	通知携带用于关联的 anaNotifCorrId (s0061)；未说明任何防重放规则	s0061
K01	访问令牌与TLS密钥保密	每个 NF：其 OAuth2 令牌和 TLS 会话密钥仅由其自身持有	在客户端凭据授予下从 NRF 获取 OAuth2 令牌 (s0412, s0413)	s0412
D01	通知地址绑定至订阅者	consumer：到达其 anaNotifUri 的内容属于其自身订阅并来自 DCCF；恶意 NF 无法让通知投递到它不拥有的地址	consumer 提供 anaNotifUri (s0007)，DCCF 向其发布 (s0060)；未说明所有权检查	s0007, s0060
A08	上游订阅与请求匹配	上游订阅指明 NWDAF 和 consumer 请求的事件，关联在两层之间保持一致	targetNfId 选择 NWDAF (s0014)；DCCF 创建 Nnwdaf 订阅以服务该请求 (s0021)	s0014, s0021
Z01	每个受保护操作的授权	DCCF 和 NWDAF：每个受保护操作都由持有有效 NRF 授权且其范围覆盖该操作的参与方提交	以 NRF 为授权服务器的 OAuth2 (s0412, s0413)；一个服务级范围 (s0415)	s0412, s0415
Z03	令牌主体受众范围绑定	DCCF 和 NWDAF：令牌只能由签发对象 NF 使用，且仅用于其范围覆盖的操作	范围定义 (s0415, s1227)；绑定交由基线	s0415, s1227
Z04	退订后不再通知	consumer：成功 DELETE 后，DCCF 不再为该订阅发送新通知	DCCF 移除订阅并应答 204 (s0040, s0041, s0042)	s0041
S05	已终止订阅标识符失效	consumer：终止后，旧的 subscriptionId 和旧状态不能触发新通知	DCCF 在 DELETE 时移除订阅 (s0041)，并可在通知中请求终止 (s0069)	s0041, s0069
U01	上下游订阅对应	DCCF：每个 consumer 订阅恰好映射到一个上游 NWDAF 订阅，且关联标识符不被交换	DCCF 创建 Nnwdaf 订阅，然后创建、编号并存储自己的订阅 (s0021, s0026, s0028)	s0021
U02	通知地址来自订阅者自身	DCCF 仅将发起请求的 NF 给出的地址记录为 anaNotifUri；其他 NF 不能替换另一个 consumer 的通知地址	请求应包含通知目标地址 (s0007)，DCCF 向其发布 (s0060)	s0007, s0060
U03	退订传播至上游	consumer 退订时，DCCF 取消对应的上游订阅，且在生效点之后不再接受在途通知	consumer 删除订阅 (s0039)，DCCF 移除并应答 204 (s0041)	s0039, s0041

ID	简称	对象	文稿怎么说	出处
X01	分析载荷对其他NF保密	为 consumer 自身订阅投递给它的通知内容	通知发布到 consumer 的 anaNotifUri 并携带分析内容 (s0060, s0061)；原文未对载荷本身陈述保密目标	s0060

分析者依据文稿补充的性质：X01.

文稿里的安全表述，逐段去向

宿主把文稿里说明协议保护什么、防什么的章节逐段列出，共 398 段；分析者对每一段说明了去向：定为性质、定为攻击者条件，或者为什么都不选。选了 53 段，没选 345 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	总体介绍
P003 至 P006	rfc6749:2790-2823	Z01, K01, `malicious_nf`	
P007 至 P010	rfc6749:2827-2850	A02, Z03, `malicious_nf`	
P011 至 P015	rfc6749:2859-2881	没有陈述目标	泄露的持有者令牌可被其持有者使用；文稿要求令牌保密，这由 K01 陈述
P016 至 P025	rfc6749:2885-2943	没有陈述目标	此授予中无刷新令牌或授权码
P026 至 P029	rfc6749:2947-2980	D01, U02, `malicious_nf`	
P030 至 P033	rfc6749:2984-3003	没有陈述目标	未使用口令授予
P034 至 P035	rfc6749:3013-3019	K01, `network`, `malicious_nf`	
P036	rfc6749:3023-3028	A02, D01, `network`	
P037 至 P039	rfc6749:3032-3041	K01, `network`	
P040 至 P042	rfc6749:3045-3066	不在范围内	无资源所有者
P043 至 P052	rfc6749:3070-3150	没有陈述目标	无浏览器或用户代理参与
P053 至 P054	rfc6749:3154-3167	D01, U02, `malicious_nf`	
P055 至 P062	rfc6749:3170-3210	没有陈述目标	未使用隐式授予
P063	ts-33-501:2491-2491	不在范围内	算法协商
P064 至 P072	ts-33-501:2495-2511	Z01, Z03, A02, `network`, `malicious_nf`	
P073 至 P213	ts-33-501:2515-2853	不在范围内	此 API 路径之外的 RAN、UE 和 UDM 要求

段落	出处	定为	不选的原因
P214	ts-33-501:2859-2859	network, malicious_nf	
P215 至 P220	ts-33-501:2865-2875	Z01, Z03, A02, malicious_nf	
P221 至 P241	ts-33-501:2879-2923	不在范围内	NRF、NEF 和 SCP 内部
P242 至 P254	ts-33-501:2929-2953	K01, A02, network	
P255 至 P314	ts-33-501:2957-3081	不在范围内	漫游、SEPP 和 IPUPS
P315 至 P318	ts-33-501:3085-3091	Z01, A02, network, malicious_nf	
P319 至 P327	ts-33-501:3097-3115	不在范围内	信令监控
P328 至 P337	ts-33-501:3121-3141	没有陈述目标	运营可见性
P338 至 P369	ts-33-501:3149-3215	证明器问不了	算法强度与选择
P370 至 P398	ts-33-501:3219-11901	不在范围内	5G-RG、NSSAAF、N3、EAP-TLS、IAB、MBSF、NEF

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 25 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 13 项，没设的 12 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	malicious_nf	
S02	DCCF	参与方	按定义全部失守	不诚实的 DCCF 会中介此路径的每个操作
S03	NWDAF	参与方	nwdaf_dishonest	
S04	NRF	参与方	按定义全部失守	不诚实的 NRF 可签发任意令牌；文稿改为要求 NRF 安全
S05	恶意合法 NF	参与方	malicious_nf	
S06	订阅请求中的 consumer 身份	值	malicious_nf	
S07	通知中的 DCCF 身份	值	按定义全部失守	伪造 DCCF 身份需要 DCCF 自身的密钥，视为安全
S08	上游订阅中的 DCCF 身份	值	按定义全部失守	与通知中的 DCCF 身份相同
S09	anaNotifUri	值	malicious_nf	
S10	anaNotifCorrId	值	malicious_nf	
S11	subscriptionId	值	malicious_nf	
S12	anaSub 中的 analytics 事件	值	攻击者得不到更多	事件标识符是公开的
S13	通知内容	值	malicious_nf	
S14	OAuth2 访问令牌	值	malicious_nf	

ID	参与方或值	类别	攻击者条件	不设的原因
S15	TLS 会话密钥	值	攻击者得不到更多	TLS 密钥是私有通道内部的
S16	通知载荷	值	`malicious_nf`	
S17	targetNfId/targetNfSetId	值	攻击者得不到更多	NF 标识符由发现服务发布
S18	anaSub	值	攻击者得不到更多	订阅内容是 consumer 自身的数据
S19	scope	值	攻击者得不到更多	subject、audience 和 scope 是公开的令牌字段
S20	subject	值	攻击者得不到更多	subject、audience 和 scope 是公开的令牌字段
S21	audience	值	攻击者得不到更多	subject、audience 和 scope 是公开的令牌字段
S22	订阅状态	值	`malicious_nf`	
S23	上下游订阅映射	值	`malicious_nf`	
S24	订阅请求	值	攻击者得不到更多	请求就是 consumer 自己发送的内容
S25	在途通知	值	`malicious_nf`	

每条性质在各攻击者条件下的答案

攻击者由分析者在编写查询之前设定；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”是为该性质设定的攻击者，在该攻击者下证明器让某条主张未决，或未记录任何内容；空单元格是分析者未为该性质设定的攻击者。

攻击者	持有什么	依据	出处
`network`	仅有网络：它读取、丢弃、更改和发送消息，不持有任何一方的秘密		
`malicious_nf`	一个合法的 NF，持有其自身用于 ndccf-datamanagement 范围的 token；它可以调用 DCCF API，并选择 anaNotifUri、事件和目标 NWDAF	来自 NRF 的 OAuth2 token（s0412、s0413）和一个服务级范围（s0415）：任何持有该范围的 NF 都可以调用所有操作。	s0412, s0415
`token_leak`	一个签发给合法 NF 的有效访问 token，带有其 subject、audience 和 scope，在操作之前获得	RFC 6749 10.3：访问 token 是持有者凭证；泄露的 token 可被其持有者使用。	rfc6749:2859
`nwdaf_dishonest`	为上游订阅提供服务的 NWDAF 是不诚实的：它通知未订阅的事件，内容由其自行选择	NWDAF 生成分析并发送 Nnwdaf_EventsSubscription_Notify（s0997）；没有任何要求它必须诚实。	s0997

ID	`network`	`malicious_nf`	`token_leak`	`nwdaf_dishonest`
A02	成立	成立		
A03	成立	成立		
A04	成立			
K01	成立	成立		
D01	成立	成立		
A08	成立			成立
Z01	成立	成立		
Z03	成立	成立		
Z04	成立			

ID	network	malicious_nf	token_leak	nwdaf_dishonest
S05	成立			
U01	成立			
U02	成立	成立		
U03	成立			
X01	成立	成立		

原文和目标

来源：1266 个原文单元，927204 字节，冻结于 source-delivery-01.json。 目标：13 个已批准（A02、A03、A04、K01、D01、A08、Z01、Z03、Z04、S05、U01、U02、U03）；提出的问题：3 个。 目标清单按草稿事先经 --approve-targets 批准。

宿主按其记录的默认值（任务 `decisions: auto`）做出的决定，供你核查：

- approve_package：批准源文包 protocol-097945ce877ab933708785b53954

本步骤的自报情况：1 次请求（1 次失败），0.000 美元，输入 388619 个 token，输出 5952 个，282 秒。

关于证明器和模型的说明

- Z04：在 ProVerif 中作答，分析者为该目标指定了 changing_state
- S05：在 ProVerif 中作答，分析者为该目标指定了 changing_state
- U03：在 ProVerif 中作答，分析者为该目标指定了 changing_state

一个简化代数（xor、dh_algebra、other_algebra）的 ProVerif 模型给攻击者的能力少于真实操作：在那里得到的证明是针对更弱攻击者的证明，在那里得到的攻击就是攻击。一个省略了对变化值（changing_state）检查的 ProVerif 模型让各方接受更多：在那里得到的证明成立，在那里得到的攻击可能只是缺失了检查。Tamarin+ Agent 按原样对这些建模。

步数上的界是对 bounded.pv 的答案：这是分析者的第二个 ProVerif 模型，其中保存变化值的一方被展开到该步数，其检查保持不变。该模型所做的少于协议所做的，因此该性质对这些步成立，不能更进一步，在那里发现的攻击就是攻击。步数由分析者说明。

分析者的状态审查

这部分是分析者自己对原文的解读，不是证明器的答案。ProVerif 显示下为“是”表示 ProVerif 在展开模型中找到了包含这些步的迹，因此这些步是可能的；它们是否破坏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是分析者的解读。“未发现”说明查看了哪些模式，并不证明任何事。

值	由谁保存	何时变化	何时检查	参考
消费者的订阅记录（subscriptionId、anaNotifUri、anaNotifCorrId、上游 subscriptionId）	DCCF	在 DCCF 接受分析订阅请求时创建（s0026-s0029），在被接受的 DELETE 时移除（s0040、s0041）	当来自 NWDAF 的该订阅通知到达并映射到消费者的 anaNotifUri 和 anaNotifCorrId 时（s0060、s0061）	s0026, s0027, s0028, s0029, s0040, s0041, s0060, s0061

值	由谁保存	何时变化	何时检查	参考
上游 NWDAF 事件订阅（由 NWDAF 签发的 subscriptionId）	DCCF 和 NWDAF	由 DCCF 在处理请求时创建（s0021），由 Nnwdaf_EventsSubscription_Unsubscribe 移除（s0981-s0984）	在 NWDAF 发送通知（s0997）之前，未规定对其状态进行检查	s0021, s0981, s0982, s0983, s0984, s0985
DCCF 的通知路径所见的订阅阶段（open / terminated）	DCCF	在被接受的 DELETE 时（s0041）	原文未说明 DCCF 在通知到达时检查订阅状态	s0040, s0041, s0060

模式	结果	目标	ProVerif 显示	步数
replay	未发现			在 bounded.pv 中，已终止订阅的通知在终止点之后到达并被丢弃（事件 DroppedAfterTerm），而消费者是否曾再次接受它的直接查询（late）无定论：ProVerif 的推导复用了先前的通知，而任何迹都无法投递两次。单射查询 once 已验证，因此消费者对每次 DCCF 转发至多接受一次。
repeat_one_time_action	未发现			在 bounded.pv 中，DELETE 对每个订阅只处理一次；第二次 DELETE 在模型中没有路径。
update_before_check	候选		否：未用 ProVerif 尝试	消费者订阅分析通知（s0005）；DCCF 创建上游 NWDAF 订阅（s0021、s0026）。/ 消费者为其订阅发送 DELETE；DCCF 移除自己的订阅记录并应答 204（s0040、s0041、s0042）。/ 只有在应答之后，DCCF 才为上游订阅调用 Nnwdaf_EventsSubscription_Unsubscribe（s0981）。/ 如果该上游 DELETE 失败或其 204 始终不到来，原文不要求重试也不要求回滚（s0985），于是 NWDAF 保留其订阅，而 DCCF 没有它的记录：两侧保留不同的状态。
desynchronisation	候选		否：未用 ProVerif 尝试	DCCF 将消费者的 DELETE 视为订阅的结束并应答 204（s0041、s0042）。/ 上游删除是对 NWDAF 的单独请求（s0981）；原文未规定两者之间的顺序或重试。/ 上游删除失败会使 NWDAF 保持订阅并持续通知，而 DCCF 丢弃这些通知：分析继续为无人计算。
no_rollback_on_failure	未发现			未对 DCCF 的失败路径建模；原文只规定错误按第 5.1.7 条应答（s0043）。
race_between_sessions	未发现			model.pv 为每个消费者分配自己的 TLS 会话，为每个订阅分配自己的应答和通知通道，因此两个会话不会读取同一个值；原文未描述消费者之间共享的订阅状态。
distinguishable_failure	未发现			规定了失败响应（400 SUBSCRIPTION_CANNOT_BE_SERVED、403 USER_CONSENT_NOT_GRANTED），但未对失败路径建模，因此这里无法区分任何东西。
wrap_or_window	未发现			订阅标识符和关联标识符是不透明的新鲜值，在此路径中没有计数器，也没有接受窗口。

分析者为目标指定的内容：

步骤	目标	特征	原因
32	Z04, S05, U03	changing_state, plain_primitives	Z04、S05 和 U03 都建立在订阅生命周期之上：订阅被创建、被通知、在 DELETE 时被移除，而这些目标询问在终止点及之后会发生什么。model.pv 的答案只表明终止路径可达，因此这些在 bounded.pv 中展开。其余目标只使用无哈希的 token 构造、私有通道和新鲜名，即简单原语。

分析者的结束说明

模型针对 DCCF 直接协调路径（消费者 → DCCF → 一个 NWDAF）构建：在 DCCF 处订阅，DCCF 以其自己的通知 URI 建立 Nnwdaf_EventsSubscription 订阅，201 Created 并返回 subscriptionId，上游通知，在 anaNotifCorrId 下转发的 Ndccf_DataManagement_Notify，以及向上游传播的 DELETE。TLS 是每对端点之间的私有通道；每个 NF 持有一个 OAuth2 token（带有 subject 和 scope 的私有构造子），接收方检查其 subject 和 scope；由攻击者驱动的一个恶意合法 NF 用其自行选择的地址和事件请求自己的订阅。

全部 14 个目标都有答案：A02、A03、A04、K01、D01、A08、Z01、Z03、U01、U02 和 X01 通过在 model.pv 上证明；Z04、S05 和 U03 通过终止路径的可达性，加上在 bounded.pv 中对展开生命周期的证明（两个通知步骤，已检查对照）。K01 有一个对照查询不成立，因此保密性查询并非空泛。没有目标失败，所以没有发现，报告也如此说明。这些证明依赖于传输采用 TLS（每对之间一条私有信道）以及令牌的主体/范围检查，而所选原文并未明确说明这两点。

未确认的状态候选：DCCF 在上游删除确认之前就移除了自己的订阅记录（s0041 对 s0981），并且上游删除失败会使双方失去同步；其步骤记录在状态审查中，但没有查询能显示它们。未建模的内容：通过 UDM 的用户同意、静音标志、特性协商、重定向，以及泄露的令牌——有了泄露的令牌，冒充按定义随之而来，而文稿要求令牌保密性（K01）。