CMS 密钥传输加 PSK 的安全性分析

本报告的其他语言版本：English。

rfc8696 · ProVerif+ Agent 报告

文稿	Using Pre-Shared Key (PSK) in the Cryptographic Message Syntax (CMS)（协议定义）
检查的性质	13 条：5 条成立，8 条不成立（9 个攻击）
发现	3

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

RFC 8696 让 CMS 以这样一种方式携带内容加密密钥：这种方式还需要一个预共享密钥，因此无论今天攻破经典的密钥传输，还是以后用量子计算机攻破它，都不足以读取内容。发送方生成一个内容加密密钥和一个密钥派生密钥，在 KeyTransPSKRecipientInfo 中用普通的 CMS 密钥传输把密钥派生密钥传给接收方，再通过 KDF 把它与 PSK 混合成密钥加密密钥，并用该密钥加密内容加密密钥。接收方持有 pskid 所指的 PSK 以及自己的密钥传输私钥。

交换结束时，发送方知道内容受到一个同时需要 PSK 的密钥保护。接收方知道内容加密密钥来自某个持有 PSK 且能把消息发往接收方公钥的一方，并且它就该密钥、算法和内容与这一方达成一致；它不知道这一方是谁。

参与方：

- **发送方**：发起方，持有 PSK。持有：PSK（按 pskid）、接收方公钥（证书）。
- **接收方**：一个接收方，持有 PSK。持有：PSK（按 pskid）、密钥传输私钥。

图 1 展示了文稿所规定的交换。

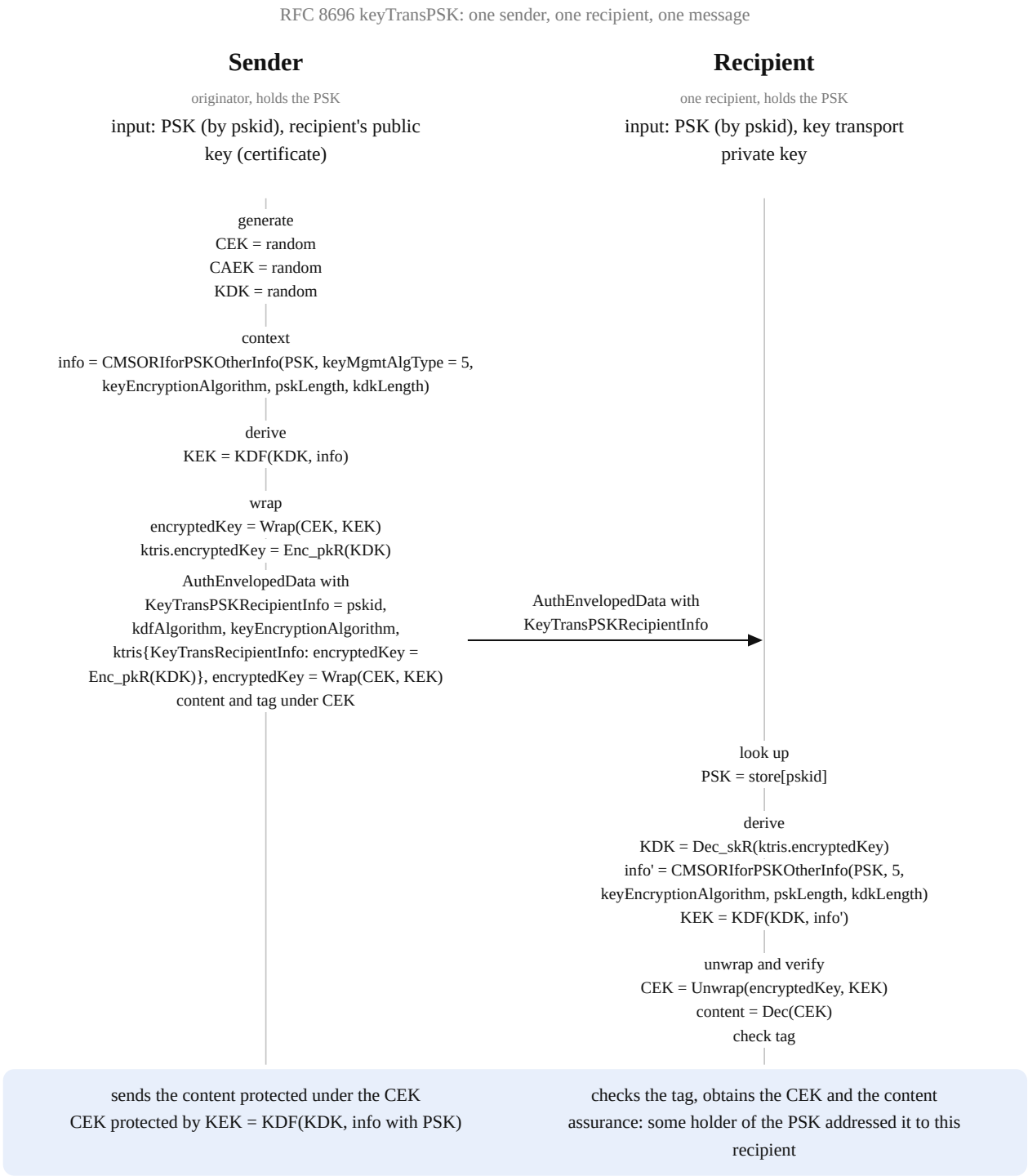


图 1. 文稿所规定的协议。

分析的范围见附录 D：分析了什么、遗漏了什么，以及它依据的是文稿的哪些章节。

2 发现

分析有 3 个发现：以下内容文稿中并未写明。其中 1 个是否写明尚不明确。

该机制实现了它的目的：攻击者即使拥有网络也无法触及内容加密密钥或内容，并且单独泄露密钥派生密钥或单独泄露 PSK 都不够，因此 PSK 确实带来了密钥传输无法提供的那种机密性。出现了三件文稿未写明的事。PSK 标识符不是派生密钥的一部分，因此一条消息可以被重新标记为另一个标识符，而接收方在该

标识符下持有同一个 PSK；任何持有 PSK 的人都能把内容发给接收方，因为流程没有指明发送方；并且一条消息可以被接受不止一次，因为其中没有任何新鲜的内容。在十三条性质中，十条得到证明，三条被攻击所回答，每个证明都配有一个失败的对照；PSK 标识符的隐私性正如文稿所述那样失败。这些证明依赖于理想的密钥传输、KDF 和密钥封装，依赖于单一接收方，并且依赖于长度被排除在模型之外。

攻击图使用图 1 的列。红色表示攻击者所做的操作。黄色标记某一方发送了指定交换在该处并不包含的消息，以及攻击所破坏的结果。

2.1 任何持有 PSK 的人都能以发送方的身份向接收方发送内容

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 (rfc5652:2864, rfc5652:2874, main:649)
价值	中
涉及的性质	A03, U03（见第 3 节）
原文	s0649, s0652
依据	ProVerif attack query `a03_forge`; Figures 2 and 3

发生了什么。 KeyTransPSKRecipientInfo 不指明发送方，也不携带签名。持有 PSK 的一方生成自己的密钥派生密钥，从 PSK 派生出密钥加密密钥，用接收方的公钥封装一个自选的内容加密密钥，然后发送一条完整的消息，接收方接受它的方式与接受真正发送方的消息完全相同。

攻击者需要什么。 攻击者是共享该 PSK 的群体中的一员，或者已经获取了该 PSK；它不需要其他秘密，因为接收方的公钥是公开的。文稿预想到了群体 PSK，但只讨论了窃听。

攻击者能得到什么。 接收方无法把发送方与任何其他持有 PSK 的人区分开，因此真实发送方从未产生的消息也会被接受。keyTransPSK 中的内容真实性仅依赖 PSK。

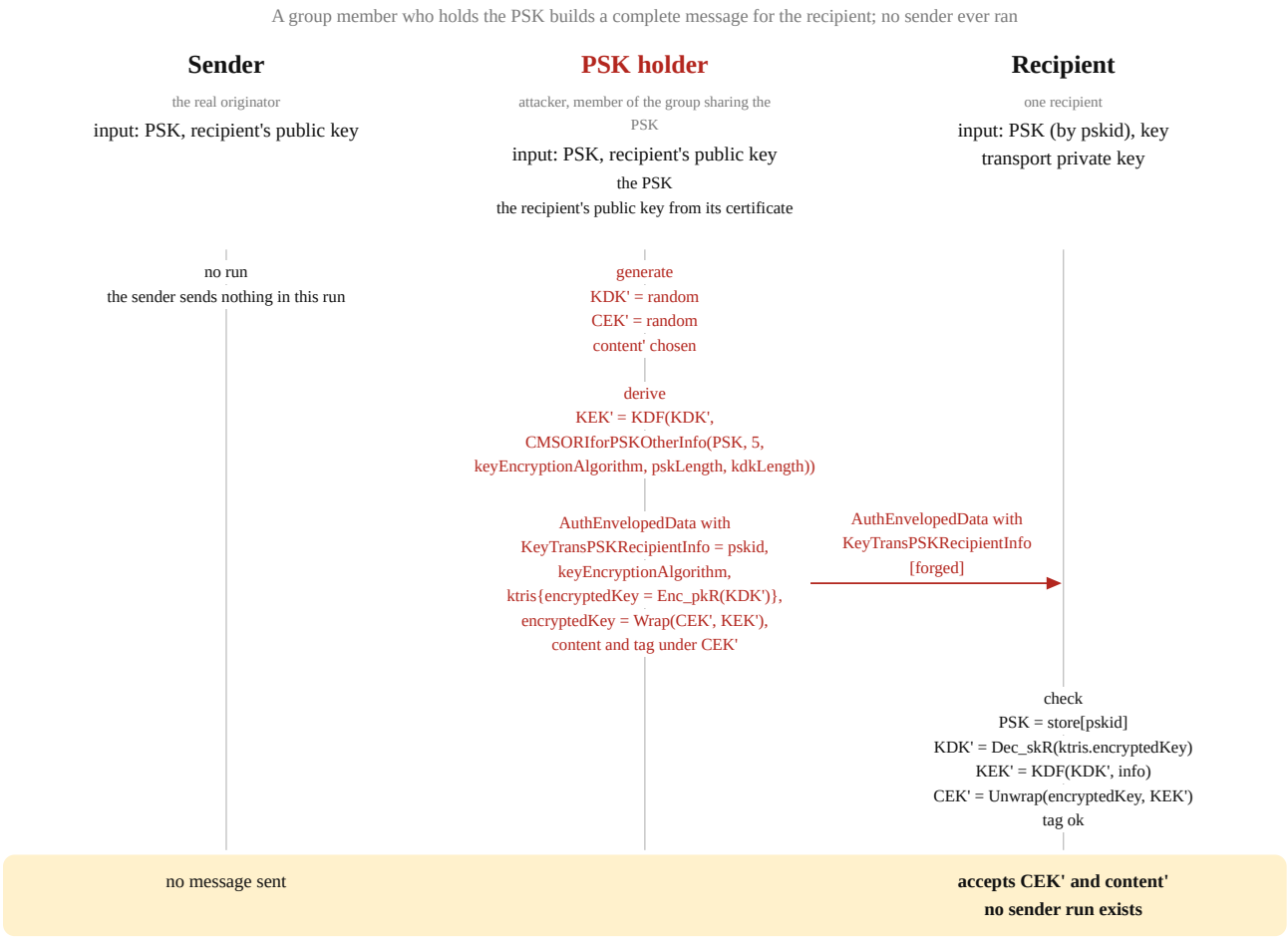


图 2. 持有 PSK 的群体成员为接收方构造了一条完整的消息；从未有发送方运行过。性质 A03；攻击查询 a03_forge。

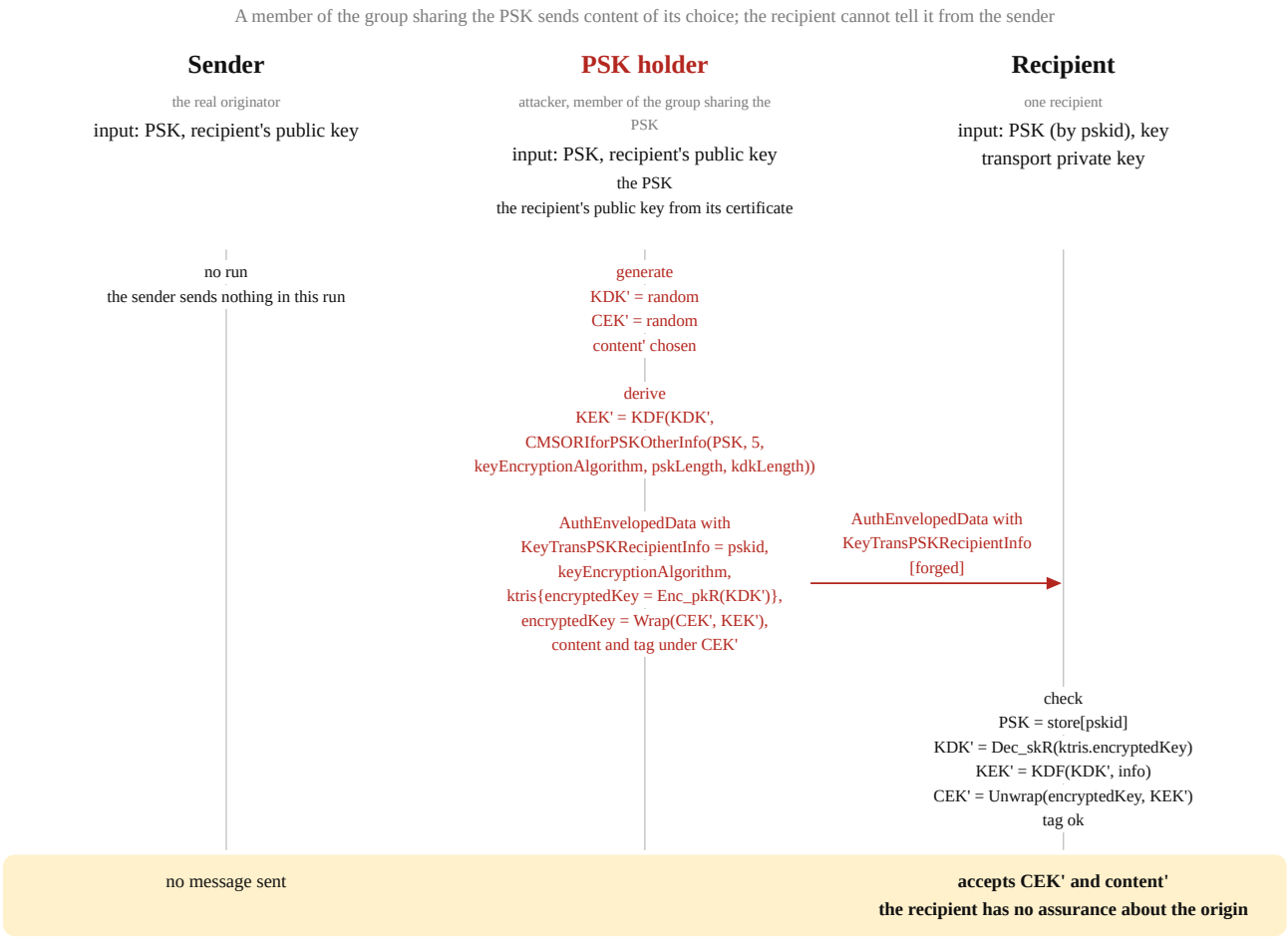


图 3. 共享 PSK 的群体中的一名成员发送了自选内容；接收方无法把它与发送方区分开。性质 U03；攻击查询 a03_forge。

拟议修改。 规范应写明，接收方对来源的保证仅限于持有 PSK 的一方，并且在来源重要的场合所使用的 PSK 必须是成对的，即每个发送方与接收方各一个，而不是由群体共享。

用 ProVerif 复核。 未检查：改用成对 PSK 恰好去掉了本发现中攻击者所具备的能力，因此被检查的模型会平凡地满足该性质，说明不了什么；既能保留群体 PSK 又能恢复来源保证的修改是签名，而任务把签名排除在范围之外，因此模型不包含它。

2.2 PSK 标识符在派生密钥之外，因此消息可以被重新标记

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	低
涉及的性质	A03, K04, D01, A07, U02（见第 3 节）
原文	s0012, s0038, s0039, s0193
依据	ProVerif attack query `a03_pskid`; Figures 4, 5, 6, 7 and 8

发生了什么。 KDF 的上下文是 CMSORIforPSKOtherInfo 的 DER 编码，它携带 PSK 值、密钥管理算法类型、密钥加密算法和两个长度，但不携带 pskid。接收方在自己的存储中解析收到的 pskid，因此它派生的密钥取决于它在那里找到的 PSK，而不是取决于该标识符。当同一个 PSK 在第二个标识符下也注册过时，攻击者把 pskid 改写为该标识符，接收方就派生出相同的密钥加密密钥并接受。

攻击者需要什么。 只需要网络：攻击者修改它观察到的一条消息的 pskid 字段。它需要接收方在第二个标识符下持有同一个 PSK，这一点原文既不要求也不禁止，因为原文只把唯一标识符称作最佳实践。

攻击者能得到什么。 实现或应用从已接受消息的 pskid 中读到的任何内容都是未经认证的：该标识符指向的是接收方持有的某个 PSK，而不是发送方所用的标识符。机密性没有损失，因为密钥仍取决于 PSK 值。

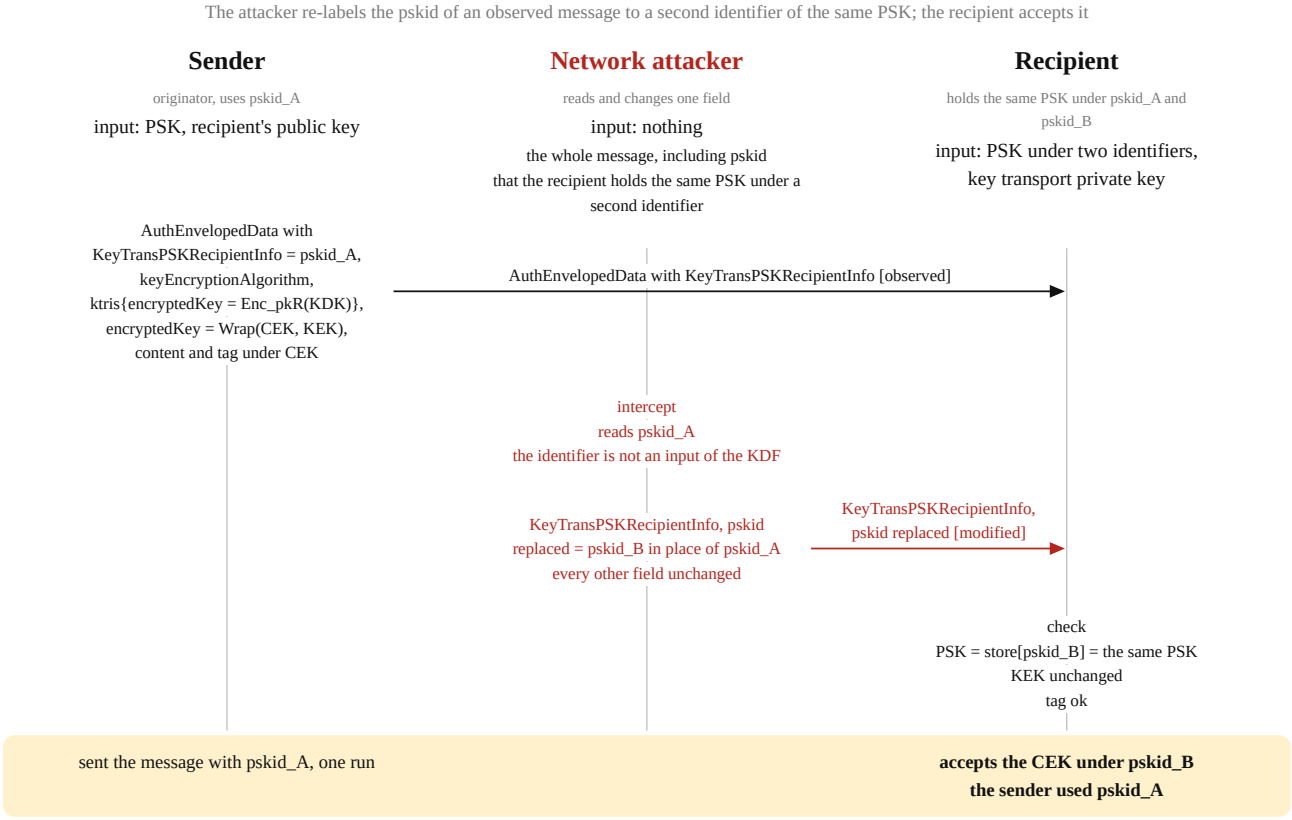


图 4. 攻击者把观察到的一条消息的 pskid 重新标记为同一 PSK 的第二个标识符；接收方接受了它。性质 A03；攻击查询 a03_pskid。

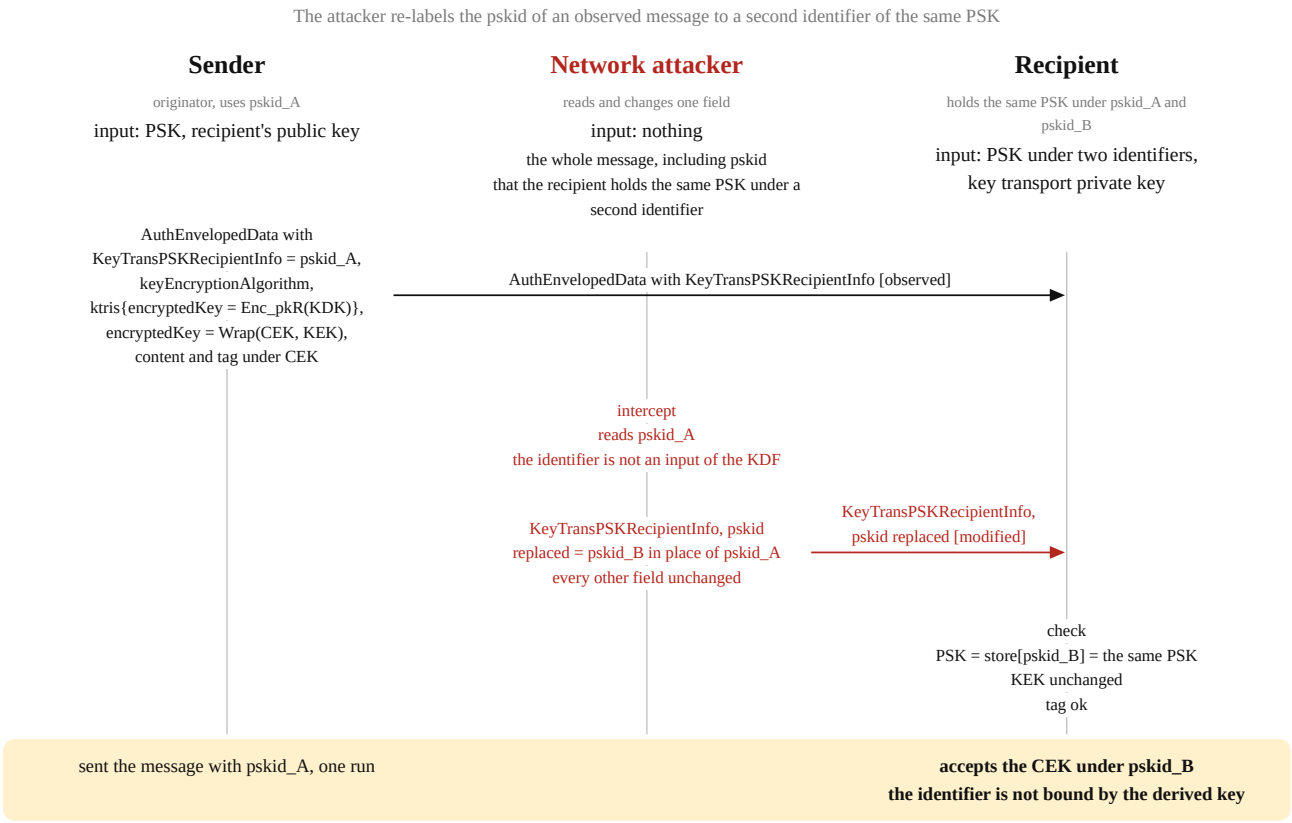


图 5. 攻击者把观察到的一条消息的 pskid 重新标记为同一 PSK 的第二个标识符。性质 K04；攻击查询 a03_pskid。

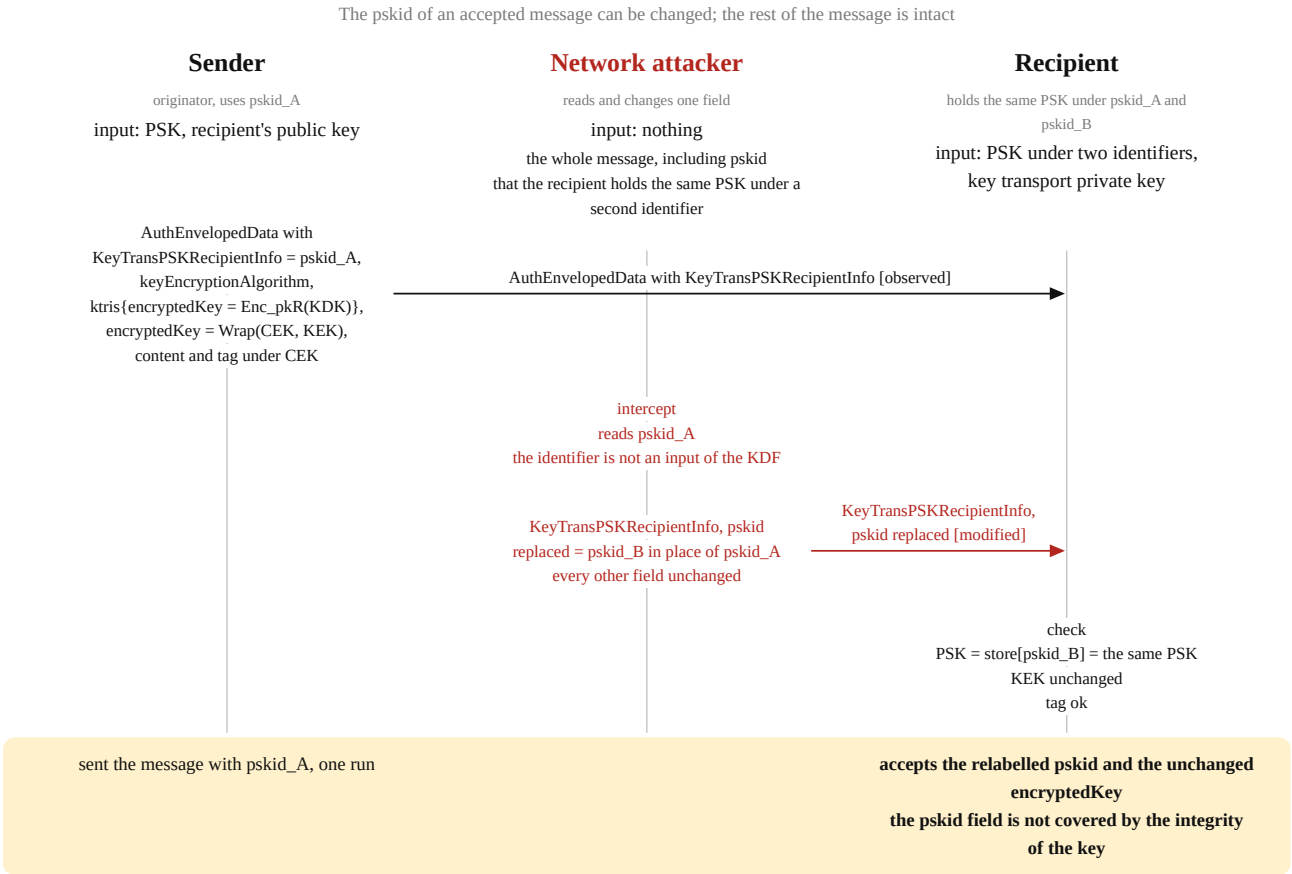


图 6. 已接受消息的 pskid 可以被修改；消息的其余部分保持完整。性质 D01；攻击查询 a03_pskid。

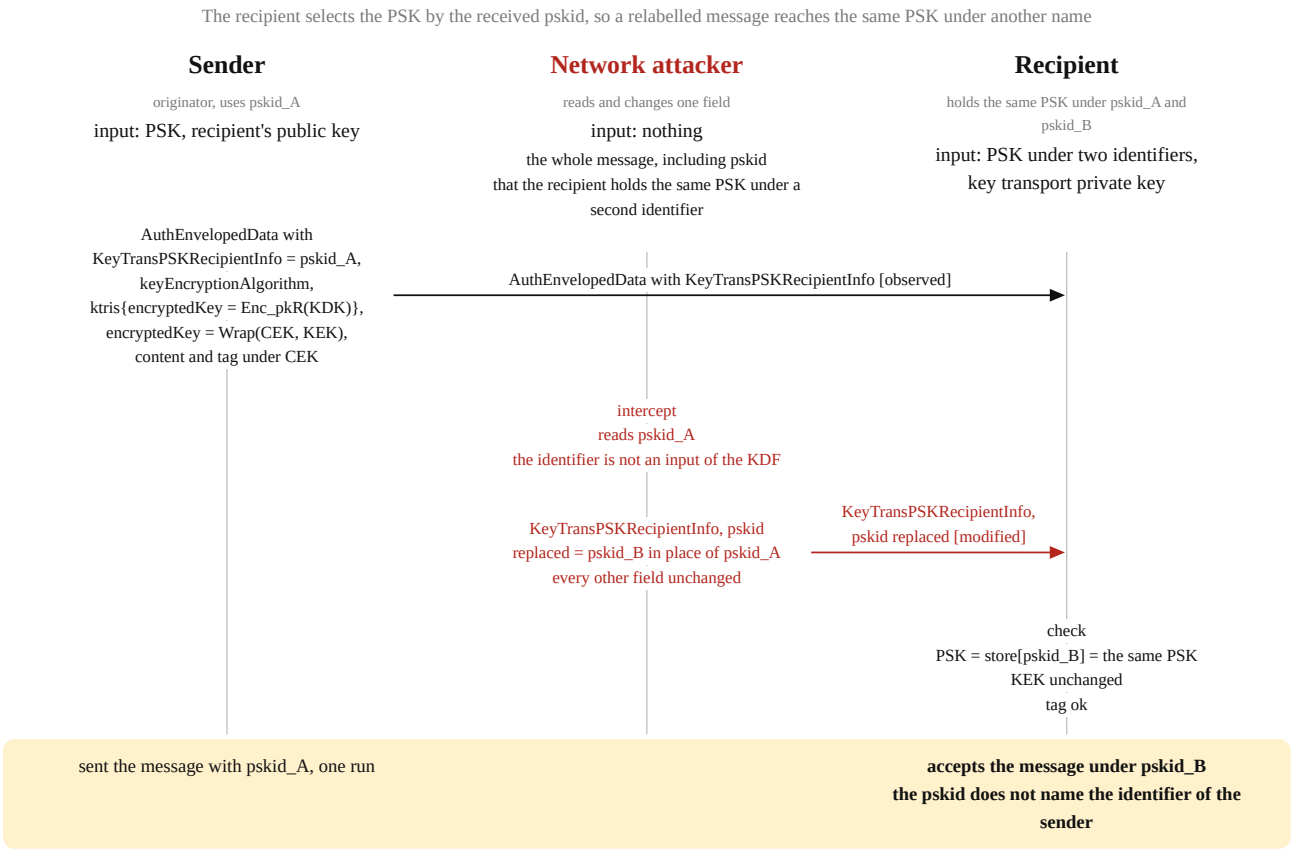


图 7. 接收方按收到的 pskid 选择 PSK，因此被重新标记的消息以另一个名字到达同一个 PSK。性质 A07；攻击查询 a03_pskid。

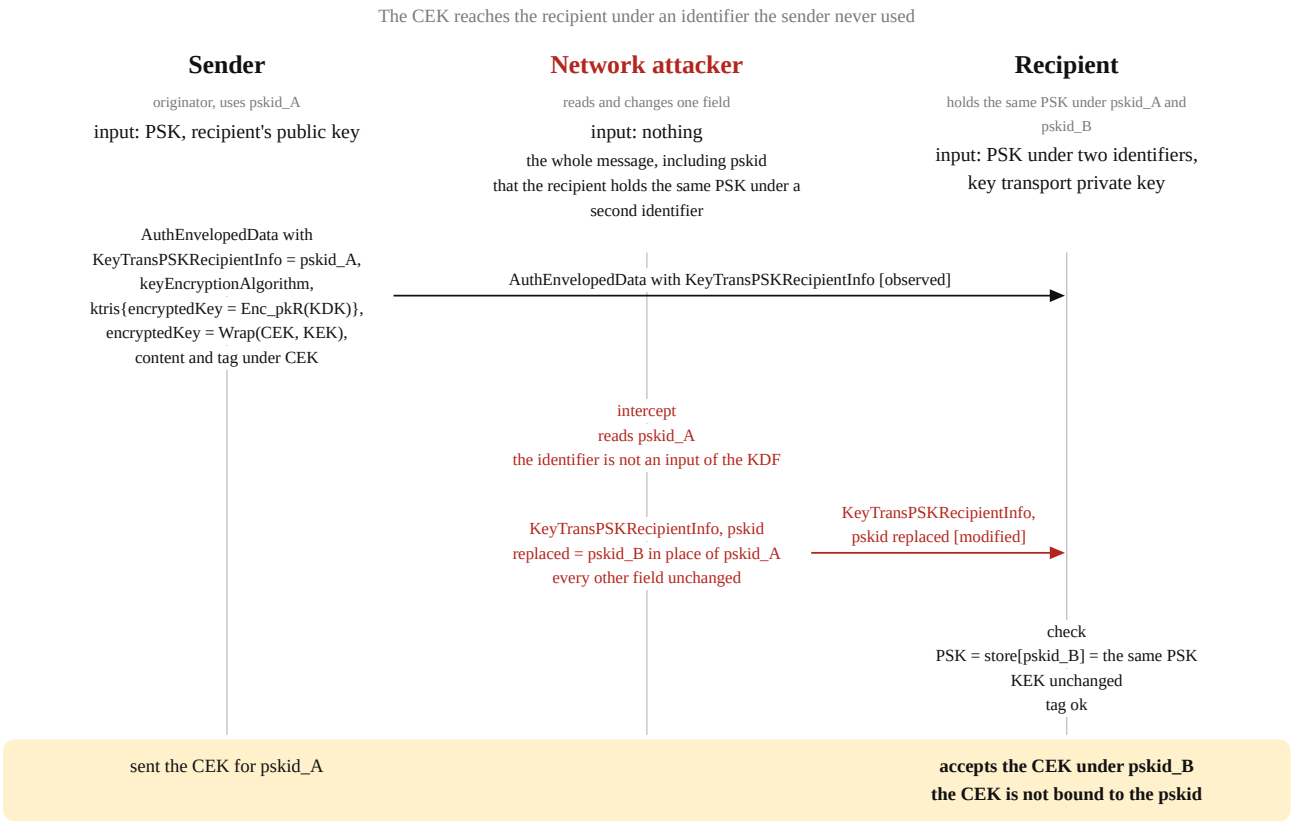


图 8. CEK 以发送方从未使用过的标识符到达接收方。性质 U02；攻击查询 a03_pskid。

拟议修改。 把 pskid 加入 CMSORIforPSKOtherInfo，使该标识符成为 KDF 的输入，从而密钥加密密钥同时取决于它和 PSK 值。

用 ProVerif 复核。 该修改被放入模型的一个副本：把 pskid 加入 KDF 上下文：KDF 的 CMSORIforPSKOtherInfo 输入携带 PSK 标识符，因此派生出的 KEK 同时取决于 pskid 和 PSK 值。在修改后的模型上，ProVerif 证明了 `a03_pskid`：该攻击在那里不再可能。协议的正常流程仍然能被找到。在其他已记录的答案中，21 条仍然成立，1 条发生变化：`x01_privacy`（X01，原为攻击）现在为无结论。这是对模型的初步检查：它表明该修改在该模型中消除了这个攻击，而不是表明它不会引入其他问题。修改后的模型：`records/fixes/0034-fix-pskid.pv`。

2.3 一条消息实例可以被接受不止一次

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	低
涉及的性质	A04（见第 3 节）
原文	s0002, s0015
依据	ProVerif attack query `a04_once`; Figure 9

发生了什么。 这条消息不携带任何对该消息而言新鲜的值：没有 nonce，没有计数器，没有实例标识符，密钥管理结构也不添加任何此类值。网络上的攻击者将同一条 AuthEnvelopedData 消息投递两次，接收者就两次接受它，且两次都基于来自发送者的同一把密钥派生密钥和同一把内容加密密钥。

攻击者需要什么。 只需要网络：攻击者记录一条消息，再投递一次。

攻击者能得到什么。 若接收者把已接受的内容加密密钥视为一次性事件，或对接受次数计数，就会被误导。对于普通的封装内容，重复投递只是重新投递接收者已经拥有的内容。

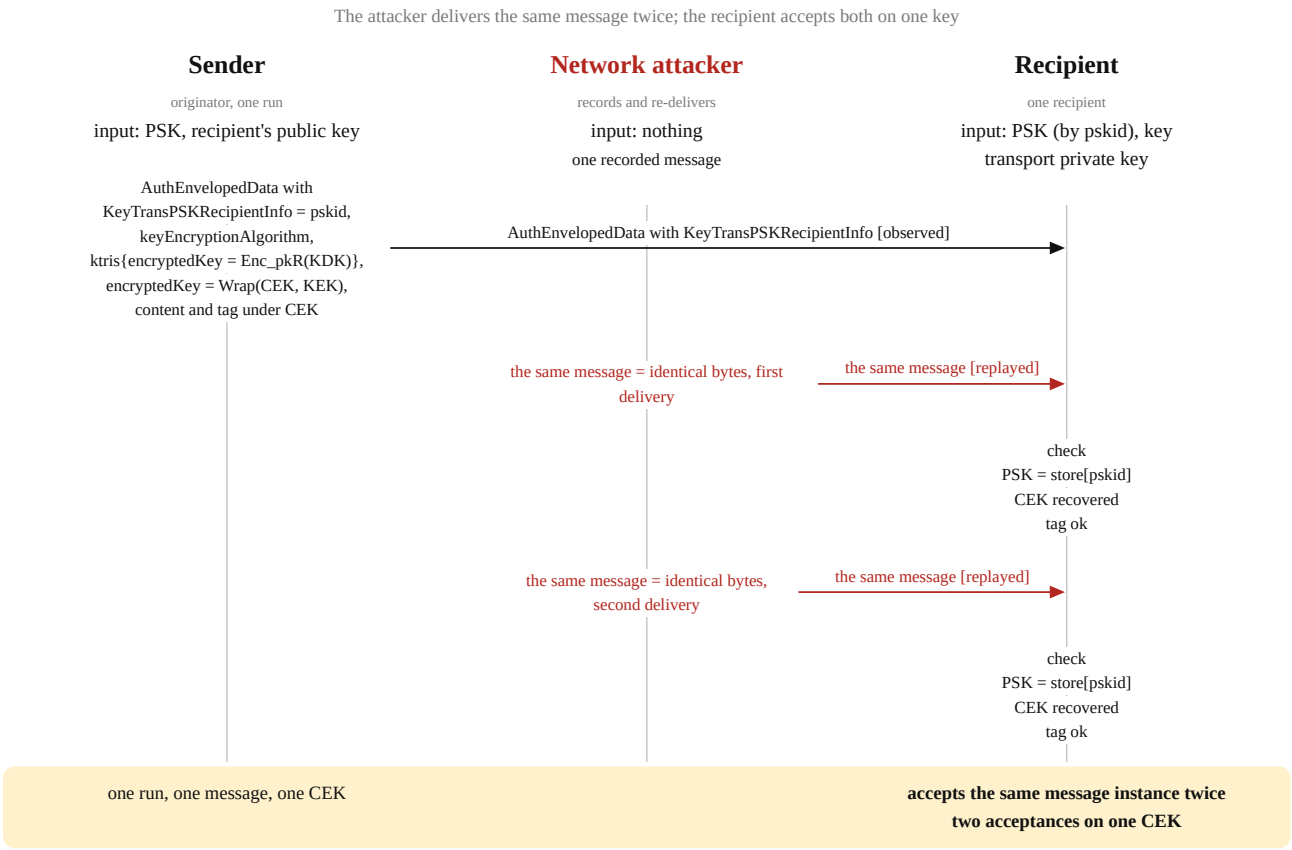


图 9. 攻击者将同一条消息投递两次；接收者在同一把密钥上接受了两次。性质 A04；攻击查询 a04_once。

拟议修改。 规范应说明已接受的内容加密密钥是否只能使用一次。若只能使用一次，发送者必须把新鲜值放入 KDF context，接收者必须拒绝已见过的值，这要求接收者保存状态。

用 ProVerif 复核。 未检查：拒绝重复需要接收者记住早前的消息，而单消息流程的模型没有这种状态；检查需要一个带重放存储的有界模型，本模型无法表达。

3 检查过的性质

每一行是一条交给 ProVerif 检查的性质。结果是证明器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由分析者判断，理由见附录 A。

ID	性质	假定的泄露	结果	价值	文稿是否已写
K01	**CEK、KEK、KDK 和 PSK 的保密性。** 对 CEK/CAEK、KEK、key-derivation key 与 PSK 分别检查不可推导性，合法知悉者为发送者与持有该 PSK 的接收者。	无	成立	中	是
K02	**受保护内容的机密性。** CEK/CAEK 及由其保护的内容只对发送者与持有同一 PSK 的接收者可见。	无	成立	中	是
A03	**CEK、pskid 和算法的协商一致性。** 接收者每次接受 CEK 都有发送者匹配运行，双方在身份、pskid、keyEncryptionAlgorithm 与 CEK 上一致。	无	不成立（2 个攻击）	中	不确定

ID	性质	假定的泄露	结果	价值	文稿是否已写
A04	**每个消息实例仅接受一次。** 接收者每次接受 CEK 对应不同的发送者运行，同一消息实例至多接受一次。	无	不成立（1 个攻击）	低	否
K04	**派生 KEK 的域分离。** 不同 pskid、keyMgmtAlgType、keyEncryptionAlgorithm 或长度下派生的 KEK 必须不同。	无	不成立（1 个攻击）	低	否
D01	**encryptedKey 与上下文的完整性。** 接收者接受的 encryptedKey 与 pskid、kdfAlgorithm、keyEncryptionAlgorithm 对应发送者的真实发送且未被篡改。	无	不成立（1 个攻击）	低	不确定
A07	**pskid 选择接收方自己的 PSK。** 接收者接受的 pskid 与实际持有该 PSK 的接收者身份一致，不会把其他接收者的凭据误认。	无	不成立（1 个攻击）	低	否
C03	**KDK 或 PSK 泄露时的会话隔离。** 泄露一个会话的 key-derivation key 或 PSK 时，其他会话的 CEK 仍保密。	key-derivation key 或 PSK (会话完成后)	成立	中	是
U01	**KDK 泄露时 CEK 保持保密。** key-derivation key 泄露、PSK 未泄露时，CEK/CAEK 不可推导。	key-derivation key (会话完成后)	成立	中	是
U02	**CEK 与其上下文的绑定。** 接收者接受的 CEK 与发送者的 pskid、接收者身份、KDF context 和 key wrap 算法一致。	无	不成立（1 个攻击）	低	否
U03	**单方泄露与发送方身份。** 分别检查只有 PSK 泄露、只有 key-derivation key 泄露时 CEK 保密，以及发送者认证边界。	PSK 或 key-derivation key (会话完成后)	不成立（1 个攻击）	中	不确定
X01	**PSK 标识符隐私。** 消息的观察者无法判断发送者使用了哪个 PSK 标识符，即 PSK 标识符不会告诉观察者哪些参与方共享同一 PSK。	无	攻击成立（文稿已写明）	低	是
X02	**密钥传输被破坏时的 CEK 交付。** 持有某会话 key-derivation key 的攻击者，无法让接收者接受一个没有任何发送者产生过的 content-encryption key，也无法让它接受由攻击者自选的 CEK。	某会话的 key-derivation key，通过用大规模量子计算机破解密钥传输获得，或通过读取接收者的密钥传输私钥获得；网络	成立	中	是

“攻击成立（文稿已写明）”：证明器找到了这个攻击，而文稿自己已经写明它存在。这条性质不成立；这是已知结果，不算发现（附录 B）。

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

提出的问题及分析者的回答：

问题	回答	依据
Q1: 传统 key transport 密钥泄露而 PSK 未泄露时 CEK 保密	是：会话的 key-derivation key 已知、PSK 保密时，content-encryption key 仍未知，这一点已被证明，也正是该机制的要点。	U01, K01
Q2: PSK ID、接收者、KDF context 和 key wrap 绑定	接收者、密钥加密算法与内容都被绑定，但 PSK 标识符没有：一条消息可以在一选取同一 PSK 的另一个标识符下被接受，因此实现不得从已接受消息的 pskid 中读出任何东西。	U02, A03, K04, D01, A07

问题	回答	依据
Q3: 只有 PSK/只有传统密钥泄露的控制与发送者认证边界	每个密钥单独泄露时 content-encryption key 仍然保密，两者同时泄露则暴露该密钥，与文稿所述一致；但不存在发送者认证，因为任何持有该 PSK 的人都能向接收者投递消息。	U03, C03, A03

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在密码学被视为理想的前提下给出或不给出什么，而不涉及任何实现。

据分析者所述，本次分析不覆盖以下内容：

- 一个接收者和一条消息流程：多个接收者、由一组 PSK 持有者共享的消息以及 keyAgreePSK 都在分析范围之外。
- 密钥传输、KDF、密钥封装与认证加密被理想化为黑盒：不建模长度、不比较算法强度、不建模分组密码或计数器模式的行为、不作计算性假设。
- KDF context 的 pskLength 和 kdkLength 输入在模型中没有对应物，因此它们提供的域分离未被检查。
- pskid 重新标注这一发现假设同一 PSK 以两个标识符注册；原文对此未作定论。
- 未建模发送者签名、证书与接收者标识符处理、AuthAttributes 和内容类型。
- 持有某会话 content-encryption key 或 key-encryption key 的攻击者按定义可以读取该内容；这些情形不属于性质，也未作为问题提出。
- 不对可用性、时序、随机数生成、算法强度或抗量子计算机能力作任何主张：模型只说明，单独一个被破坏的密钥传输不会泄露密钥。

每条性质还有哪些未决之处，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、解读依据是什么、能否直接使用、价值如何。

K01: CEK、KEK、KDK 和 PSK 的保密性

对 CEK/CAEK、KEK、key-derivation key 与 PSK 分别检查不可推导性，合法知悉者为发送者与持有该 PSK 的接收者。

仅有网络时，攻击者无法获知 content-encryption key、key-encryption key、key-derivation key 或 PSK：key-derivation key 只在密钥传输内部传递，key-encryption key 从不发送。破解密钥传输的攻击者会获知 key-derivation key，这正是该机制所假设的。

- 结果：成立；回答了所问：是；有保留地可用
- 价值中：这四个值的保密性是该机制声明的目的（main:581-600，特别是只有 PSK 与 key-derivation key 同时具备才暴露内容）。
- 文稿是否已写：是。文稿中所在位置：main:581, main:592
- 依据：密钥传输、KDF 和密钥封装被理想化：不建模算法强度、长度、相关密钥行为。；一个接收者和一条消息流程；组 PSK 和 keyAgreePSK 在范围之外。；KDF context 的 pskLength 和 kdkLength 输入未建模。
- 未决：实现所选的 KDF 和封装算法在实践中是否保持这一区分，是一个计算性问题。
- 下一步：此处无需进一步工作；KDF 和封装的计算强度超出 ProVerif 能说明的范围。

K02: 受保护内容的机密性

CEK/CAEK 及由其保护的内容只对发送者与持有同一 PSK 的接收者可见。

无论内容还是 content-encryption key 都不会到达网络上的攻击者：内容在一把密钥下加密并认证，而这把密钥本身又被封装在一把由 PSK 和新鲜的 key-derivation key 派生出的密钥之下。这与文稿中的陈述一致：ProVerif 证明表明 content-encryption key 无法从交换中获知。

- 结果：成立；回答了所问：是；有保留地可用
- 价值中：main:692-698 正是为该机制陈述了这一结果，main:576-579 沿用了 CMS enveloped-data 的相关考虑。
- 文稿是否已写：是。文稿中所在位置：main:576, main:692
- 依据：认证加密被建模为同一密钥下的理想加密加 MAC。；内容是一个值；AuthAttributes 和内容类型在模型之外。；一个接收者；由多个接收者共享的消息在范围之外。
- 下一步：此处无需进一步工作。

A03: CEK、pskid 和算法的协商一致性

接收者每次接受 CEK 都有发送者匹配运行，双方在身份、pskid、keyEncryptionAlgorithm 与 CEK 上一致。

针对网络，接收者的接受总能与一次发送者运行相匹配，二者在密钥、算法和内容上一致，但 pskid 不在覆盖范围内：一条消息可以在同一 PSK 的另一个标识符下被接受。针对属于共享该 PSK 的组的攻击者，则根本没有匹配的发送者，因为任何持有该 PSK 的人都能构造一条接收者会接受的消息，而流程中没有任何内容说明是谁发送的。

- 结果：不成立（2 次攻击）；是否回答了所问：部分；可带保留使用
- 价值中：文稿给出了通用规则，即密钥管理技术本身必须提供数据源认证，而 RSA 密钥传输不提供（rfc5652:2864-2872）；由两方以上共享的密钥不提供源认证（rfc5652:2874-2877）；main:649-659 仅针对窃听讨论组 PSK。没有任何文稿说明 PSK 持有者可以冒充发送者向接收者放置内容。
- 文稿中是否陈述：不明确。所依据的原文：rfc5652:2864、rfc5652:2874、main:649、s0649、s0652
- 依据：pskid 攻击假设接收者在第二个标识符下注册了同一 PSK，而原文对此未作限定。；pskid 在模型中被有意排除在 KDF 上下文之外，与原文一致：上下文携带 PSK 值（s0038-s0045）。；仅一个接收者；接收者标识符不是单独字段，因为密钥传输将消息绑定到接收者的公钥。
- 未决：是否本就打算从 keyTransPSK 消息推断发送者身份。
- 下一步：在规范中说明接收者可以就来源推断什么，即可确定这一解读。

A04: 每个消息实例仅接受一次

接收者每次接受 CEK 对应不同的发送者运行，同一消息实例至多接受一次。

同一消息可以被投递两次并被接受两次：流程中没有消息标识符、nonce 或计数器，因此把已接受的密钥视为一次性事件的接收者得不到保护。对于普通封装内容，重复只会重新投递相同内容。

- 结果：不成立（1 次攻击）；是否回答了所问：是；可带保留使用
- 价值低：我在全部五份文稿中搜索了 replay、replay protection、nonce 和 freshness；replay 一词从未出现，也没有任何消息携带可用于拒绝重复的值。
- 文稿中是否陈述：否
- 依据：接收者被复制，这才使重放得以显现；协议没有早先消息的接收者状态，因此未建模该状态。；重复是否有害是协议不回答的应用问题。
- 未决：规范是否意图让已接受的密钥仅可使用一次。
- 下一步：编辑者应说明应用是否可以依赖每条消息仅被接受一次。

K04: 派生 KEK 的域分离

不同 pskid、keyMgmtAlgType、keyEncryptionAlgorithm 或长度下派生的 KEK 必须不同。

密钥加密密钥绑定到 PSK、密钥管理算法类型和密钥加密算法，因此消息不能在另一算法下被接受。它不绑定到 pskid：标识符在接收者处选择 PSK，不进入派生，因此选择同一 PSK 的两个标识符给出相同的密钥。

- 结果：不成立（1 次攻击）；是否回答了所问：部分；可带保留使用
- 价值低：原文要求所有 KDF 输入影响输出（s0048）并列出上下文（s0039），但没有任何文稿注意到 pskid 在上下文之外，因此上下文之间的分离仅依赖 PSK 值。
- 文稿中是否陈述：否
- 依据：keyMgmtAlgType 在模型中为常量 5，结构如此固定；未建模 keyAgreePSK 上下文（值 10），因此跨协议分离只能在同时具有两者的模型中检查。；pskLength 和 kdkLength 在原文中是上下文的输入，但在符号模型中没有对应物。；pskid 攻击假设一个 PSK 注册在两个标识符下。
- 未决：分离两种密钥管理类型（5 对 10）超出本模型范围。；两个长度输入给出的分离未被建模。
- 下一步：在一个模型中建模两种 recipient-info 类型，或在携带长度的模型上检查长度输入。

D01: encryptedKey 与上下文的完整性

接收者接受的 encryptedKey 与 pskid、kdfAlgorithm、keyEncryptionAlgorithm 对应发送者的真实发送且未被篡改。

被修改的 encryptedKey、内容或密钥加密算法会被拒绝：接收者的接受与具有相同值的发送者运行相匹配。pskid 字段不在该完整性覆盖范围内，因此可以将其改为同一 PSK 的另一个标识符，消息仍会被接受。

- 结果：不成立（1 次攻击）；是否回答了所问：部分；可带保留使用
- 价值低：main:576-579 沿用了 authenticated-enveloped-data 的考虑，覆盖加密内容；原文未说明 pskid 在派生密钥的完整性之外。
- 文稿中是否陈述：不明确
- 依据：密钥包装和认证加密是理想的：未建模分组密码模式的任何部分修改。；仅检查模型携带的字段：pskid、密钥加密算法、密钥传输值、被包装的密钥、内容及其标签。
- 下一步：无需进一步；pskid 部分由绑定结果回答。

A07: pskid 选择接收方自己的 PSK

接收者接受的 pskid 与实际持有该 PSK 的接收者身份一致，不会把其他接收者的凭据误认。

接收者使用其自身存储中由收到的 pskid 所选择的 PSK，因此用另一 PSK 保护的消息不会被接受。标识符本身未被认证：在第二个标识符下持有同一 PSK 的接收者会在该标识符下接受消息，因此不能依赖 pskid 作为所用 PSK 的名称。

- 结果：不成立（1 次攻击）；是否回答了所问：部分；可带保留使用
- 价值低：main:189-196 要求使用标识符，并称唯一标识符最佳，且接收者可以在一个标识符下持有多个 PSK；它未说明接收者可以从已接受消息的标识符推断什么。
- 文稿中是否陈述：否。所依据的原文：main:189
- 依据：一个接收者一个存储；共享 PSK 的接收者组不在模型范围内。；标识符到 PSK 的映射被建模为接收者的配置，与原文一致。
- 下一步：关于如何将标识符分配给 PSK 的规则可确定此问题。

C03: KDK 或 PSK 泄露时的会话隔离

泄露一个会话的 key-derivation key 或 PSK 时，其他会话的 CEK 仍保密。

泄露的密钥派生密钥只损害其自身会话，因为每个会话都有自己的密钥派生密钥；仅泄露 PSK 不会泄露任何内容加密密钥，因为密钥传输仍需被破解。只有 PSK 连同某会话的密钥派生密钥才能给出该会话的密钥，这正是文稿所述。

- 结果：成立；是否回答了所问：是；可带保留使用
- 价值中：main:581-600 指出，密钥加密密钥的泄露，或 PSK 与密钥派生密钥组合的泄露，会泄露受该密钥材料保护的内容，而仅 PSK 不会。
- 文稿中是否陈述：是。文稿中的位置：main:581、main:592
- 依据：泄露按会话建模，如文稿所述量子攻击者发现一个密钥派生密钥。；每个会话都是发送者的一次全新运行，具有自己的密钥派生密钥和内容加密密钥。
- 下一步：此处无需进一步。

U01: KDK 泄露时 CEK 保持保密

key-derivation key 泄露、PSK 未泄露时，CEK/CAEK 不可推导。

拥有某会话密钥派生密钥的攻击者仍然不知道该会话的内容加密密钥，因为密钥加密密钥还需要 PSK。这是该机制的承诺：破解密钥传输，无论现在还是将来用量子计算机，都不足以读取内容。

- 结果：成立；是否回答了所问：是；可带保留使用
- 价值中：main:602-605 称大规模量子计算机可以发现密钥派生密钥，main:592-600 称只有 PSK 连同密钥派生密钥才泄露内容。
- 文稿中是否陈述：是。文稿中的位置：main:592、main:602
- 依据：KDF 是其输入的单向函数，没有代数结构；PSK 作为独立参数进入。；密钥传输是理想的，攻击者被直接给予密钥派生密钥，这是密钥传输被破解的最强形式。；未建模长度和算法强度。
- 下一步：KDF 对知道密钥派生密钥的攻击者的计算安全性超出 ProVerif 所能说明的范围。

U02: CEK 与其上下文的绑定

接收者接受的 CEK 与发送者的 pskid、接收者身份、KDF context 和 key wrap 算法一致。

内容加密密钥绑定到接收者、密钥加密算法和内容，因此被篡改或误投的消息会被拒绝。它不绑定到 pskid，因此消息可以在选择同一 PSK 的另一个标识符下被接受。

- 结果：不成立（1 条攻击）；回答了所问：部分；可用但有注意事项
- 价值低：s0039 中的上下文列表不包含 pskid，且没有文稿说明这留下了什么未绑定。
- 文稿中已说明：否
- 依据：接收方身份仅通过密钥传输绑定到其公钥；RecipientIdentifier 字段未单独建模。；只有一个接收方，因此未考察接收方之间的重定向。
- 未决：两个共享同一 PSK 的接收方之间的误导未建模。
- 下一步：一个包含两个共享同一 PSK 的接收方的模型将确定绑定中与接收方有关的部分。

U03: 单方泄露与发送方身份

分别检查只有 PSK 泄露、只有 key-derivation key 泄露时 CEK 保密，以及发送者认证边界。

任一方机密单独泄露都不会使内容加密密钥泄露：PSK 泄露而 key-derivation key 不泄露，以及 key-derivation key 泄露而 PSK 不泄露，均如此。PSK 不能提供的是关于内容由谁发送的任何保证：每个持有 PSK 的人都能向接收方发送消息，因此接收方唯一能得出的结论是某个持有 PSK 的人发送了它。

- 结果：不成立（1 条攻击）；回答了所问：是；可用但有注意事项
- 价值中：main:649-659 指出知道 PSK 本身并不能实现窃听，也没有说明谁可以发送；rfc5652:2864-2877 给出了通则：密钥传输不提供数据源认证，由多方共享的密钥也不提供。
- 文稿中已说明：不明确。所依据的源文：rfc5652:2864, main:649, s0649, s0652
- 依据：组 PSK 是攻击者已知的值，文稿正是这样描述由组共享的 PSK。；伪造的消息用接收方的公钥构造，模型将该公钥作为证书发布。；发送方签名不在模型范围内，任务也将其置于范围之外。
- 下一步：在规范中加一句关于接收方可推断来源的说明，即可确定这一点。

X01: PSK 标识符隐私

消息的观察者无法分辨发送方使用了哪个 PSK 标识符，也就是说，PSK 标识符不会告诉观察者哪些参与方共享一个 PSK。

PSK 标识符以明文传输，因此观察者能得知消息用哪个 PSK 保护，并据此对消息分组。文稿说明了这一点，并论证接收方标识符本来就已经可见，因此隐私状况不会变差。

- 结果：攻击成立（文稿中已说明）；回答了所问：是；可用
- 价值低：main:702-709 明确说明了这一点。
- 文稿中已说明：是。文稿说明的位置：main:702
- 依据：隐私问题仅针对标识符提出，且使用两个选择同一 PSK 的标识符，使两次运行都能完成；未考察其他区分器。
- 下一步：无需进一步处理；文稿已经说明。

X02: 密钥传输被破坏时的 CEK 交付

持有某会话 key-derivation key 的攻击者，无法使接收方接受一个没有发送方产生的 content-encryption key，也无法使其接受攻击者自行选择的 CEK。

攻破了密钥传输并持有某会话 key-derivation key 的攻击者，无法使接收方接受其自行选择的密钥：没有 PSK 就无法生成密钥加密密钥，因此内容加密密钥的交付在该攻击者面前仍然完好。

- 结果：成立；回答了所问：是；可用但有注意事项
- 价值中：main:692-698 指出，ProVerif 证明显示量子攻击者无法破坏内容加密密钥的交付。
- 文稿中已说明：是。文稿说明的位置：main:692
- 依据：攻击者被直接给予 key-derivation key，而不是进行一次密钥传输破坏，这是最强形式。；密钥传输是理想的，因此接收方总能恢复发送给它的 key-derivation key。
- 下一步：此处无需进一步处理。

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，以及各项攻击及其分析者的判定。

目标	级别 界	查询	对照	攻击	主张
K01	proved	k01_cek	checked		4 proved
K02	proved	k02_content	checked		2 proved
A03	proved	a03_agree	checked	a03_pskid (depends_on_ambiguity); a03_forge (holds_in_source)	1 proved, 2 attack
A04	none			a04_once (holds_in_source)	1 attack
K04	proved	k04_alg	checked	a03_pskid (depends_on_ambiguity)	1 proved, 1 attack
D01	proved	a03_agree	checked	a03_pskid (depends_on_ambiguity)	1 proved, 1 attack
A07	proved	a03_agree	checked	a03_pskid (depends_on_ambiguity)	1 proved, 1 attack
C03	proved	u03_psk	checked		2 proved
U01	proved	u01_kdk	checked		1 proved
U02	proved	k04_alg	checked	a03_pskid (depends_on_ambiguity)	2 proved, 1 attack
U03	proved	u03_psk	checked	a03_forge (holds_in_source)	2 proved, 1 attack
X01	none			x01_privacy (holds_in_source)	1 attack
X02	proved	x02_delivery	checked		1 proved

逐条主张，按分析者对每条主张的措辞；每条主张的答案来自证明器：

目标	主张	攻击者	回答	查询	对照
K01	仅拥有网络的攻击者无法推导出会话的内容加密密钥（CEK/CAEK）；此查询无泄露。	network	proved	k01_cek	checked
K01	仅拥有网络的攻击者无法推导出密钥加密密钥（KEK）；它从不离开双方。	network	proved	k01_kek	checked
K01	仅拥有网络的攻击者无法推导出密钥派生密钥（KDK）：只有在会话的 KDK 泄露之处它才会被知晓。	network	proved	k01_kdk	checked
K01	仅拥有网络的攻击者无法推导出 PSK。	network	proved	k01_psk	checked
K02	仅拥有网络的攻击者无法推导出受 CEK 保护的内容。	network	proved	k02_content	checked
K02	保护内容的内容加密密钥（CEK/CAEK）仅对发送方和持有 PSK 的接收方可见。	network	proved	k01_cek	checked
A03	接收方对 CEK 的每次接受都对应一次发送方运行，且发送方与接收方在 CEK、内容以及 KDF 上下文中的密钥加密算法上达成一致。	network	proved	a03_agree	checked
A03	接收方接受的 pskid 就是发送方使用的 pskid：接收方不会接受一个标有其他标识符的消息，即使它在那个标识符下持有相同的 PSK。	network	attack (depends_on_ambiguity)	a03_pskid	

目标	主张	攻击者	回答	查询	对照
A03	对 CEK 的每次接受都对应一次发送方运行，即使攻击者是共享该 PSK 的群组成员也是如此。超出网络的攻击者能力：PSK 值本身。	psk_holder	attack (holds_in_source)	a03_forge (the control of x02_delivery)	
A04	接收方对某一次发送方运行的某个消息实例至多接受一次，因此每次接受都对应不同的发送方运行。	network	attack (holds_in_source)	a04_once	
K04	在不同 pskid 下派生出的 KEK 是不同的密钥：KEK 绝不会在标有其他 pskid 的上下文中使用。	network	attack (depends_on_ambiguity)	a03_pskid	
K04	在不同 keyEncryptionAlgorithm 下派生出的 KEK 是不同的密钥：接收方只会在发送方放入 KDF 上下文的算法下接受 CEK。	network	proved	k04_alg	checked
D01	接收方接受的 encryptedKey 以及接受它时所用的密钥加密算法均来自发送方的真实发送，途中未被修改。	network	proved	a03_agree	checked
D01	随被接受的 encryptedKey 携带的 pskid 就是发送方使用的那个，且未被修改。	network	attack (depends_on_ambiguity)	a03_pskid	
A07	接收方使用自己存储中为所收到 pskid 保存的 PSK 进行解密：每次接受都对应一次使用了该存储中某个 PSK 的发送方运行，因此不会使用其他方的 PSK。	network	proved	a03_agree	checked
A07	接收方接受的 pskid 指明的就是发送方使用的标识符，因此接收方不会在其存储中的另一个标识符下接受该消息。	network	attack (depends_on_ambiguity)	a03_pskid	
C03	仅泄露 PSK 不会泄露任何会话的 CEK；只有同时知晓该会话的密钥派生密钥时，该会话的 CEK 才会泄露。超出网络的攻击者能力：PSK 值。	psk_holder	proved	u03_psk	checked
C03	泄露的密钥派生密钥只危及它所属的会话：只有当某个会话自身的密钥派生密钥泄露时，该会话的 CEK 才会被知晓，因此其他所有会话都保持其 CEK。超出网络的攻击者能力：一个会话的密钥派生密钥。	kdk_leak	proved	u01_kdk	checked
U01	只要 PSK 未知，持有某会话密钥派生密钥的攻击者仍然无法知晓该会话的 CEK。超出网络的攻击者能力：该会话的密钥派生密钥。	kdk_leak	proved	u01_kdk	checked
U02	CEK 与接收方绑定：密钥派生密钥被传输到接收方自己的公钥，且每次接受都对应一次在该接收方 PSK 下的发送方运行。	network	proved	a03_agree	checked
U02	CEK 与发送方使用的 pskid 绑定：接收方绝不会在发送方未发送的 pskid 下接受 CEK。	network	attack (depends_on_ambiguity)	a03_pskid	
U02	CEK 与 KDF 上下文以及密钥加密算法绑定：接收方只在发送方放入派生过程的算法下接受它。	network	proved	k04_alg	checked
U03	仅泄露 PSK 时 CEK 仍然保密；只有 PSK 与密钥派生密钥同时泄露才会暴露它。超出网络的攻击者能力：PSK 值。	psk_holder	proved	u03_psk	checked
U03	仅泄露密钥派生密钥时 CEK 仍然保密。超出网络的攻击者能力：该会话的密钥派生密钥。	kdk_leak	proved	u01_kdk	checked

目标	主张	攻击者	回答	查询	对照
U03	接收方无法确知消息由哪个发送方产生：只有当攻击者不是共享该 PSK 的群组成员时，每次对 CEK 的接受才对应一次发送方运行。超出网络的攻击者能力：PSK 值。	`psk_holder`	attack (holds_in_source)	a03_forge (the control of x02_delivery)	
X01	观察者无法分辨发送方使用了哪个 PSK 标识符：pskid 不会告诉观察者哪些方共享一个 PSK。	`network`	attack (holds_in_source)	x01_privacy	
X02	持有某会话密钥派生密钥的攻击者无法使接收方接受一个没有发送方产生的 CEK，也无法使它接受自己选定的 CEK。超出网络的攻击者能力：该会话的密钥派生密钥。	`kdk_leak`	proved	x02_delivery	checked

“攻击者分不清用的是两个值里的哪一个”这类性质，证明器从不直接判为不成立。它没有证出来，并给出了一条攻击者能把两个值分开的轨迹，攻击按这条轨迹记录：x01_privacy.

附录 D：分析是怎么跑的

分析者由 LLM 担任，从文稿构建协议模型，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 会话 session-20261114T231408，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：46，证明器用时 8 秒，实际耗时 12 分钟，成本 0.105 美元。

ProVerif：运行 123 次证明，117 次有结论，6 次无答案，用时 4 秒，记录 30 个答案。

分析了什么

协议	CMS key transport plus PSK
版本	rfc8696
分析范围	固定 RFC8696 KeyTransPSKRecipientInfo 的单接收者单消息流程；KEK 结合高熵对端独立预配置 PSK 与传统 key transport 随机秘密。使用规范 KDF/context 和 AuthEnvelopedData；PSK 传输、群组共享和发送者签名不在范围。
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/正例对照。
原文	48 个编号原文单元（10358 字节），来自下列章节。本报告中诸如 s0001 的引用即为其中一个原文单元

分析所依据的文稿章节：

文稿	章节	标题
main	3	keyTransPSK
main	4	keyAgreePSK
main	5	Key Derivation

原文步骤在文稿中定位到的协议目的：固定 RFC8696 KeyTransPSKRecipientInfo 的单接收者单消息流程；KEK 结合高熵对端独立预配置 PSK 与传统 key transport 随机秘密。使用规范 KDF/context 和 AuthEnvelopedData；PSK 传输、群组共享和发送者签名不在范围。

对照文稿定性质

在撰写查询之前，分析者把起草的性质清单对照文稿本身所说明的协议目的。性质名称、性质所涉及的内容以及文稿所述内容均为分析者的解读；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
K01	CEK、KEK、KDK 和 PSK 的保密性	The content-encryption key (CEK/CAEK), the key-encryption key (KEK), the key-derivation key (KDK) and the PSK are known only to the sender and the recipient that holds that PSK; no one else learns them from the exchange.	KEK 由 PSK 和 KDK 派生，必须受到保护（main:581-590）；KDK 只出现在 KeyTransRecipientInfo 的 encryptedKey 中（s0015），CEK 只出现在 KEK 下的 encryptedKey 中（s0016）。	main:581, main:592, s0002, s0013, s0015, s0016, s0035, s0038, s0047

ID	简称	对象	文稿怎么说	出处
K02	受保护内容的机密性	The content carried in AuthEnvelopedData under the CEK is readable only by the sender and the recipients that hold the PSK; an attacker on the network learns neither the CEK nor the content.	CEK 按内容随机生成，用于保护内容；CMS enveloped-data 和 authenticated-enveloped-data 的安全考虑仍然适用（main:576-579, s0016）。	main:576, main:692, s0002, s0016
A03	CEK、pskid 和算法的协商一致性	Each acceptance of a CEK by the recipient is matched by a sender run, and sender and recipient agree on the PSK identifier, the key-encryption algorithm and the CEK.	文稿没有声明明确的认证目标；rfc5652:2864-2872 指出，密钥管理技术本身必须提供数据源认证，而 RSA 密钥传输不提供；rfc5652:2874-2877 指出，共享密钥的各方无法获得数据源认证。	main:576, rfc5652:2864, rfc5652:2874, s0002, s0015, s0016, s0038
A04	每个消息实例仅接受一次	A recipient accepts a given message instance of a sender run at most once; every acceptance corresponds to a different sender run.	没有任何文稿声明重放保护：这个词在五份文稿中都没有出现。目标要求单消息流程应具备该性质，而文稿对此没有说明。	s0002, s0015
K04	派生 KEK 的域分离	A KEK derived under a different pskid, keyMgmtAlgType, keyEncryptionAlgorithm or length is a different key, so a KEK of one context is never used in another.	KDF 的输入为 psk、keyMgmtAlgType（keyTrans 时为 5）、keyEncryptionAlgorithm、pskLength 和 kdkLength，所有输入 MUST 影响输出（s0038-s0048）。	main:627, s0013, s0038, s0039, s0042, s0044, s0045, s0048
D01	encryptedKey 与上下文的完整性	The encryptedKey the recipient accepts, and the pskid, kdfAlgorithm and keyEncryptionAlgorithm fields it is accepted with, belong to a genuine send and have not been modified.	encryptedKey 是用 KEK 加密的 CEK（s0016），上下文字段参与派生（s0013, s0038）；authenticated-enveloped-data 的相关考虑适用（main:576-579）。	main:576, s0002, s0013, s0016
A07	pskid 选择接收方自己的 PSK	The recipient decrypts with the PSK its own store holds for the received pskid; it never accepts a message under another party's PSK and a pskid it accepts names the PSK that was really used.	pskid 是发送方所用 PSK 的标识符（s0012）；该标识符 MUST 被分配，SHOULD 唯一，接收方可以在同一标识符下持有多个 PSK 并逐一尝试（main:189-196）。	main:189, s0012, s0015
C03	KDK 或 PSK 泄露时的会话隔离	A leaked key-derivation key compromises only its own session; a leaked PSK alone discloses no CEK of any session; earlier and other sessions keep their CEK.	KEK 或密钥管理私钥泄露可能暴露用该密钥材料保护的内容，而仅有 PSK 不会（main:581-600）。	main:581, main:592, s0013, s0015, s0016, s0035, s0038
U01	KDK 泄露时 CEK 保持保密	The CEK/CAEK of a session stays unknown to an attacker that holds that session's key-derivation key, as long as the PSK is not known; the PSK is what carries the confidentiality.	大规模量子计算机能够求出密钥派生密钥（main:602-605），PSK 才是保护内容的关键；只有 PSK 与 KDK 同时泄露才会暴露内容（main:592-600）。	main:592, main:602, s0013, s0015, s0016, s0035, s0038
U02	CEK 与其上下文的绑定	The CEK the recipient accepts is the one the sender produced for that pskid, that recipient, that KDF context and that key-encryption algorithm.	pskid 标识 PSK（s0012），KDF 上下文是 CMSORIforPSKOtherInfo 的 DER 编码（s0038-s0045），算法随消息携带（s0013）；除这一构造之外，文稿没有声明明确的绑定目标。	s0012, s0013, s0015, s0016, s0038, s0039
U03	单方泄露与发送方身份	A leaked PSK alone, or a leaked key-derivation key alone, leaves the CEK secret; and the recipient has no assurance of which sender produced a message, since any holder of the PSK can produce one.	PSK 可能为一个群体所知，知道它本身并不使人能够窃听（main:649-659）；rfc5652:2864-2877 指出，使用 RSA 的密钥传输不提供数据源认证。	main:649, rfc5652:2864, s0012, s0013, s0015, s0016, s0035, s0038

ID	简称	对象	文稿怎么说	出处
X01	PSK 标识符隐私	The pskid field of KeyTransPSKRecipientInfo and the privacy of the parties that share a PSK, against an observer on the network.	main:702 指出，观察者只要观察 PSK 密钥标识符，就能看出哪些方在使用哪个 PSK；文稿声明不提供这种隐私。	main:702
X02	密钥传输被破坏时的 CEK 交付	The delivery of the CEK to the recipient, against an attacker who has broken the key transport (a large-scale quantum computer, or the recipient's transport private key).	main:692-698 指出，一项 ProVerif 证明表明，拥有大规模量子计算机的攻击者既无法破坏内容加密密钥向接收方的交付，也无法获知该密钥。	main:692

分析者依据文稿补充的性质：X01, X02.

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 34 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 12 段，没选 22 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
P01	main:576-579	K02, D01	
P02	main:581-590	K01, C03, `psk_holder`, `kdk_leak`	
P03	main:592-600	K01, U01, U03, C03, `psk_holder`, `kdk_leak`	
P04	main:602-613	U01, K01, `kdk_leak`	
P05	main:615-625	证明器问不了	它把有效强度限定为两种算法中较弱的一方；符号证明器无法比较算法强度。
P06	main:627-632	证明器问不了	它用所选 KDF 的强度限定 KEK 的强度。
P07	main:634-640	不在范围内	它讲的是用传统技术和 PSK 混合技术同时保护同一内容；本任务固定了单接收者的 keyTransPSK 流程，没有对第二种密钥管理技术建模。
P08	main:642-647	不在范围内	它讲的是把两条携带同一内容的不同消息关联起来；模型每次运行只有一条消息流，没有跨消息关联。
P09	main:649-659	U03, C03, A03, `psk_holder`	
P10	main:661-670	K01, K02	
P11	main:672-682	证明器问不了	它讲的是随机数生成器的质量，符号证明器假定这是完美的。
P12	main:684-690	证明器问不了	它讲的是算法随时间变弱，超出符号证明器能说明的范围。
P13	main:692-698	K01, K02, A03, X02, `kdk_leak`	
P14	main:702-709	X01, `network`	
P15	rfc5083:308-310	没有陈述目标	它说适用 CMS 的安全考虑；目标在 CMS 的段落 P22-P31。
P16	rfc5083:312-317	证明器问不了	它比较计数器模式和 CBC 模式的隐私保证，这是分组密码模式的性质。
P17	rfc5083:325-328	证明器问不了	它讲的是用新密钥和每次加密的 nonce 使用计数器模式的建议，这是认证加密算法的性质。

段落	出处	定为	不选的原因
P18	rfc5083:330-337	K02	
P19	rfc5083:339-348	证明器问不了	它讲的是随机数生成器的质量。
P20	rfc5083:350-355	不在范围内	它讲的是 AuthAttributes 的消息摘要属性可支持内容追踪；AuthAttributes 和签名属性都在建模流程之外。
P21	rfc5083:357-369	证明器问不了	它讲的是处理不需要的消息流量，是部署和过滤策略，不是交换的性质。
P22	rfc5652:2837-2839	没有陈述目标	它只说 CMS 提供签名、摘要、加密和认证；对本流程没有要求。
P23	rfc5652:2841-2842	不在范围内	它讲的是签名者的私钥和通过签名冒充，发送者签名在本任务之外。
P24	rfc5652:2844-2849	C03, K01, U01, `kdk_leak`	
P25	rfc5652:2851-2855	不在范围内	它讲的是认证数据内容类型的消息认证密钥，在建模流程之外。
P26 至 P27	rfc5652:2864-2877	A03, `psk_holder`	
P28	rfc5652:2879-2889	证明器问不了	它讲的是随机数生成器的质量。
P29	rfc5652:2891-2903	证明器问不了	它比较密钥加密算法和内容加密算法的强度。
P30	rfc5652:2905-2911	证明器问不了	它说算法随时间变弱；符号证明器无法表达这一点。
P31	rfc5652:2917-2927	不在范围内	它讲的是副签和副签属性，在建模流程之外。
P32	rfc5869:355-360	没有陈述目标	它把分析交给 HKDF 论文；对本协议没有要求。
P33	rfc5869:362-371	没有陈述目标	它讲的是 HKDF 的密码学分析及其对哈希函数的依赖；这是 KDF 原语的性质。
P34	rfc8619:195-199	没有陈述目标	它引用 HKDF 设计分析；对本协议没有要求。

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 6 项，没设的 10 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	发送者	参与方	`psk_holder`	
S02	接收者	参与方	`psk_holder`, `kdk_leak`	
S03	CEK/CAEK	值	按定义全部失守	持有某个会话的内容认证加密密钥的一方按定义就能读取该内容；没有目标对攻击者已持有其 CEK 的会话提出性质。
S04	KEK	值	按定义全部失守	KEK 的存在就是为了保护该会话的 CEK；有了它，CEK 按定义就失守了（main:584-590）。
S05	key-derivation key	值	`kdk_leak`	

ID	参与方或值	类别	攻击者条件	不设的原因
S06	PSK	值	`psk_holder`	
S07	受保护内容	值	按定义全部失守	受保护内容本身就是机密性目标所保护的值；持有它按定义就回答了这些目标。
S08	pskid	值	攻击者得不到更多	pskid 在每条消息中都明文传输（main:702-709），所以网络上的攻击者已经拥有它。
S09	keyEncryptionAlgorithm	值	攻击者得不到更多	keyEncryptionAlgorithm 是消息中的一个字段，是公开的。
S10	encryptedKey	值	攻击者得不到更多	encryptedKey 是消息中的一个字段，是公开的。
S11	KDF context	值	`psk_holder`	
S12	上下文字段	值	攻击者得不到更多	消息中携带的上下文字段（pskid、keyEncryptionAlgorithm、算法标识、长度）都是公开的。
S13	接收者身份	值	攻击者得不到更多	接收者由 RecipientIdentifier 和 pskid 明文标识（main:702-709）。
S14	CEK	值	按定义全部失守	CEK 就是机密性目标所保护的值；持有它的一方按定义就能读取内容。
S15	key wrap 算法	值	攻击者得不到更多	keyEncryptionAlgorithm 在消息中携带，是公开的。
S16	发送者身份	值	`psk_holder`	

每条性质在各攻击者条件下的答案

攻击者条件是分析者在写查询之前设定的；每个答案都在其中一个条件之下记录。单元格是证明器在该攻击者条件下对相应性质给出的答案；“无答案”是指证明器对某项主张未作出判定、或没有记录任何答案的攻击者条件；空单元格是分析者没有为该性质设定的攻击者条件。

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		
`psk_holder`	PSK 值本身（与 PSK 共享的群组成员，或 PSK 泄露）；网络	main:649-656 说 PSK 可能为一个群组所知，且知道它本身并不当然就能窃听；main:592-600 说 PSK 必须受到保护，且仅有 PSK 不够，PSK 加上传输私钥或 KDK 才行	main:649, main:592
`kdk_leak`	某个会话的 key-derivation key，通过大规模量子计算机攻破密钥传输获得，或通过读取接收者的密钥传输私钥获得；网络	main:602-605（大规模量子计算机可以发现 key-derivation key）和 main:592-600（密钥传输私钥失守）	main:602, main:592

ID	`network`	`psk_holder`	`kdk_leak`
K01	成立		
K02	成立		
A03	不成立	不成立	
A04	不成立		
K04	不成立		
D01	不成立		
A07	不成立		
C03		成立	成立

ID	network	psk_holder	kdk_leak
U01			成立
U02	不成立		
U03		不成立	成立
X01	不成立		
X02			成立

原文和目标

原文：48 个原文单元，10358 字节，冻结在 source-delivery-01.json 中。 目标：11 个已批准（K01, K02, A03, A04, K04, D01, A07, C03, U01, U02, U03）；提出的问题：3 个。 目标清单事先按草稿批准，使用 --approve-targets。

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

- approve_package: 批准源文包 protocol-6d92b1ad9595b57db364c5cf5fb1

这一步的自报：1 次请求（1 次失败），0.000 USD，输入 17857 tokens，输出 4318 tokens，用时 22 s。

关于证明器和模型的说明

分析者为目标指定的内容：

step	targets	features	reason
32	K01, K02, A03, A04, K04, D01, A07, C03, U01, U02, U03, X01, X02	plain_primitives, many_sessions	所有目标都在一个模型上回答，该模型只使用理想化的对称原语（KEK 派生作为没有代数律的单向函数，认证加密作为理想加密加 MAC）和理想化的公钥密钥传输（aenc/adec 作为完美加密），并对任意数量的发送者和接收者会话做量化。没有使用异或、Diffie-Hellman 或其他代数，也没有在任何步骤之间保留并修改值，所以没有目标依赖被修改的值；密钥传输、KDF 和算法的密码学强度完全没有建模。

分析者的结束说明

RFC 8696 keyTransPSK，单接收者和单消息，在 ProVerif 中建模，使用理想的密钥传输、KDF、key wrap 和认证加密，无界会话，KDF context 按原文所列构造：PSK 值、keyMgmtAlgType = 5 和密钥加密算法，故意不含 pskid。

已确立的内容。十三条性质中有十条得到证明，每条都配有一个不成立的对照查询。内容加密密钥、密钥加密密钥、密钥派生密钥和 PSK 均处于网络攻击者的触及范围之外，内容同样如此。核心承诺成立：即使攻击者掌握了会话的密钥派生密钥（攻破密钥传输或拥有量子计算机即可得到），仍然无法获知内容加密密钥，因为密钥加密密钥还需要 PSK；仅泄露 PSK 也一无所获；只有两者同时泄露才会暴露会话密钥。一个会话的密钥派生密钥只危害该会话。接收方与密钥、密钥加密算法及内容相绑定，被改动的值会被拒绝。文稿自身关于量子攻击者无法破坏内容加密密钥交付的主张得到了复现。

不成立的内容。PSK 标识符不是 KDF 的输入，因此不在派生密钥的覆盖范围内：当接收方以第二个标识符持有同一 PSK 时，攻击者改标 pskid，消息便会在错误标识符下被接受。任何持有 PSK 的人都能为接收方构造完整消息，因为流程中没有指明发送方，所以内容真实性仅依赖 PSK。消息不携带任何新鲜数据，因此同一条消息可被接受两次。pskid 的隐私性如文稿第 8 节所述，确实不成立。

阻碍其余部分的问题。这些证明依赖于理想化原语、单一接收方，以及长度不在模型之内；密钥管理类型的区分（5 对 10）和上下文的两个长度输入无法被查询。pskid 修复在第二个模型上得到检验——将 pskid 加入 CMSORIforPSKOtherInfo 可消除该攻击，同时保持正常流程和所有其他已记录的答案——而重放修复需要接收方状态，单消息模型无法容纳；发送方认证缺口只能通过成对 PSK 或签名来弥补，超出分析范围。没有任何值在步骤之间被保留和更改，因此没有适用有界模型，也没有进行状态审查；计算性问题以及多接收方和多机制情形需要 Tamarin+ Agent。