

# EMVCO 支付标记化规范

v1.0

TSP 产品研发小组

科蓝公司

# 目录

---

<b>第 1 章 介绍</b>	<b>4</b>
1.1 概述	4
1.2 使用者	5
1.3 规范性参考文献	5
1.4 条款	6
1.5 缩写	6
1.6 定义	6
1.7 更多信息	12
<b>第 2 章 制约</b>	<b>13</b>
2.1 生态系统的制约	13
<b>第 3 章 标记化的生态环境</b>	<b>13</b>
3.1 支付标记生态环境	13
3.2 标记服务提供方	14
3.3 持卡人	14
3.4 发卡方	14
3.5 商户	15
3.6 收单方	15
3.7 支付网络	15
3.8 标记请求者	15
<b>第 4 章 支付标记的数据元素</b>	<b>16</b>
4.1 数据元素	16
<b>第 5 章 对 TSP 的要求</b>	<b>20</b>
5.1 介绍	20
5.2 标记保险库要求	21
支付标记生成	21
支付标记发布和配置	21
安全和控制	22
标记请求者注册	22
标记保证	23
标记域限制控制	23
报告和原始数据	24
5.3 收单方要求	25
5.4 支付网络要求	25
<b>第 6 章 身份识别和验证 (ID&amp;V) 的方法</b>	<b>25</b>

6.1 介绍 .....	25
6.2 ID&V 发卡行的识别认证 .....	25
6.2.1 不执行 ID&V .....	27
6.2.2 账户验证 .....	27
6.2.3 TSP 保证 .....	27
6.2.4 标记服务提供商保证请求数据 .....	27
6.2.5 发卡行对持卡人信息验证 .....	28
<b>第 7 章 TSP 的 API .....</b>	<b>28</b>
7.1 总览 .....	28
7.2 标记服务参与端点 .....	28
7.2 接口类别 .....	29
7.3.1 标记请求和发放 .....	29
7.3.2 标记安全级别更新 .....	34
7.3.3 去标记化查询 .....	36
7.3.4 去标记化验证 .....	38
7.3.5 标记生命周期管理 .....	40
<b>第 8 章 支付标记过程 .....</b>	<b>41</b>
8.1 概述 .....	41
8.2 路由和帐户范围表 .....	42
8.3 交易授权 .....	42
8.4 交易期间标记域限制控制 .....	42
8.5 采集加工 .....	43
8.6 结算 .....	43
8.7 异常处理 .....	43
<b>第 9 章 标记化支付的交易流程 .....</b>	<b>43</b>
9.1 通用 .....	43
9.2 使用场景 1: 商户的移动 NFC .....	44
9.3 使用场景 2: 移动数字钱包 .....	47
9.4 使用场景 3: 虚拟文件卡 .....	49
9.5 使用场景 4: 扫码 .....	51
9.6 日终和清算流程 .....	53
9.7 异常处理流程 .....	54

# 第 1 章 介绍

---

本文档的目的是为行业协调和互操作的支付标记化（标记）解决方案提供详细的技术规范，这将有利于收购方，商家，发卡机构和持卡人。

本规范描述了支付标记化场景，定义支持支付标记所需的实体的关键角色，识别此规范的影响，指定与标记请求、标记发放和供应、事务处理相关联的必需和可选数据字段，并识别必要的应用编程接口（API）。

本规范还旨在提供对生态系统中每个实体特定的支付标记化生态，术语定义，关键职责和控制的详细描述。此外，本文档提供了潜在的用例，相关的交易流程，以及跨传统支付功能（如授权，捕获，清算和异常处理）的 these 事务流中的必需和可选字段的标准化。

## 1.1 概述

支付行业正在发展，以支持支付多形式因素，提供增加防止假冒，帐户滥用和其他形式的欺诈。虽然 EMV 芯片卡可以为卡存在事务提供实质性保护，但是存在类似的需求，以最小化持卡人帐户数据的未授权使用，并且减少将不存在卡和新出现的交易环境的交叉信道欺诈，其结合了卡存在和卡的元素 不存在交易。支付标记化系统具有满足这些需求的实质性前景。

支付标记是代替付款生态系统中主账号（PAN）的代替值。支付标记可以用于发起支付交易，而非支付标记可以用于辅助处理，例如忠诚度跟踪。本规范描述了创建和使用支付标记的最低要求。虽然本规范不涉及非支付标记，但并不排除它们的使用。

支付标记可与所有持卡人验证方法（CVM）一起使用，包括签名，在线和离线 PIN 以及无 CVM。如果在线 PIN 与支付标记一起使用，根据 ISO 9564-1 PIN 块格式 0 或格式 3，PIN 块将包括代替 PAN 的支付标记。标记服务提供商（参见第 3.2 节标记服务提供商）负责确保发卡行接收带有 PAN 或支付标记的 PIN 块，以便进行验证。

为了使支付标记提供更好的保护，防止滥用，支付标记被限制在特定域中使用，例如特定商家或频道。这些底层使用控制是支付标记的主要优点，并且本说明书描述了他们的方法 实施。

此外，在发出支付标记时，可以采取步骤来确保支付标记正在替换被标记请求者合法使用的 PAN。该过程称为识别和验证（ID&V），并且在每次请求支付标记时执行。可以执行不同类型的 ID&V，导致相应级别的标记担保。例如，没有或最小 ID 和 V 执行应导致低保证支付标记，而高水平的 ID&V 可能导致高保证支付标记。

支付生态系统中的所有利益相关者都有好处，有助于鼓励采用支付标记：

- 发卡行和持卡人可以受益于新的和更安全的支付方式，改进的交易批准水平，并且在数据泄露的情况下降低随后的欺诈的风险，在该数据泄露中暴露付费标记而不是 PAN。。
- 获得者和商家可以体验到减少的在线攻击和数据泄露的威胁，因为支付标记数据库将是不太吸引力的目标，由于它们限于特定域。收购方和商家也可能受益于支付标记提供的更高的担保级别。
- 支付处理网络将能够采用开放规范，这有利于互操作性并有助于减少对支付网络及其参与者的数据保护要求。

## 1.2 使用者

本文档旨在供支付行业生态系统中的所有参与者使用，如卡发行商，商家，收单，支付网络，付款处理器和第三方服务提供商。

## 1.3 规范性参考文献

表 1-1 列出了本文档中提到的可用于实现标记支付处理的参考。除非明确说明发布日期，否则适用最新版本。

表 1-1：规范性参考

参考	文档标题
ISO 7812	身份证-发行人的识别
ISO 8583	金融交易卡发起的消息-交换消息规范

ISO 9564-1	金融服务 - 个人识别号码 (PIN) 管理和安全 - 第 1 部分：基于卡的系统中的 PIN 的基本原则和要求
ISO 13491	银行 - 安全加密设备，所有部分
ISO 27001	信息技术 - 安全技术 - 信息安全管理系统
PCI DSS	支付卡行业数据安全标准

## 1.4 条款

术语“SHALL”和“SHALL”不表示规范的强制性要求。术语 SHOULD 和 不应该表示本规范推荐的指南

## 1.5 缩写

表 1-2：缩写

缩写	定义
API	应用程序接口
AVS	地址验证服务
ICC	集成电路卡
NFC	近场通信
TEE	可信执行环境

## 1.6 定义

表 1-3：定义

条款	定义
----	----

3-D 安全	电子商务中的持卡人验证协议
代理	由发卡人委托的代表卡发行商执行特定功能的实体。这些功能的一些示例包括卡处理，使用 3-D 安全协议的持卡人验证和标记服务。
银行识别码 (BIN)	BIN 由付款网络分配给发卡行。BIN 符合 ISO 7812 要求，以根据 BIN 和关联的帐户范围识别付款网络。
BIN 控制器/管理器	控制 ISO BIN 发行和分配的实体，根据本规范将用于发放支付标记。
卡	任何持卡人设备或形状因素，如移动电话，可用于启动金融交易。
持卡人	任何已发行由发卡银行提供给银行卡的金融帐户的个人
卡接受者	发起支付交易并向交易商提供交易数据的实体，通常为商人
卡接受者 ID	卡接受者的标识值。
信用卡发行商	金融机构或其代理人向持卡人发卡。
发卡机构访问控制服务器 (ACS)	为 ID&V 提供 3-D 安全服务的发卡行代理。
去标记化	根据存储在标记保险库中的 PAN 映射的支付标记兑换与其相关联的 PAN 值的支付标记的过程。检索 PAN 以换取其相关联的支付标记的能力应限于特定的授权实体，个人，应用或系统。
识别和验证 (ID&V)	一个有效的方法，通过它，实体可以成功验证持卡人和持卡人的账户，以建立支付标记到 PAN /持卡人绑定的置信水平。ID&V 方法的示例是：

	<ul style="list-style-type: none"> <li>● 帐户验证邮件</li> <li>● 基于 PAN 评估的风险评分</li> <li>● 卡发行商或其代理使用一次性密码验证持卡人</li> </ul>
付款网络	电子支付系统，用于接受，传输或处理 由货币、商品或服务的支付卡进行的交易，以及在发行方、收购方、支付处理商、商户和持卡人之间转移信息和资金。
付款处理器	为收购方和/或发行方提供支付处理服务的实体。除了处理之外，付款处理者可以为收单方或发卡方提供操作，报告和其他服务
支付标记	支付标记可以在支付行业采用各种格式。对于本说明书，术语支付标记是指必须通过帐号的基本验证规则（包括 Luhn 校验位）的 13 到 19 位数字值的 PAN 的代理值。在被指定为标记 BIN 范围的 BIN 范围内生成支付标记，并且在所有适当的 BIN 表中相应地标记。支付标记不能与真实的 PAN 具有相同的值或冲突。
主帐号 (PAN)	在卡发行商与 BIN 相关联的帐户范围内生成的可变长度 13 到 19 位数的 ISO 7812 兼容帐号。
请求/分配的标记担保级别	请求标记担保级别由标记请求者从标记服务提供商请求。请求的标记担保级别是包括在标记请求中的字段。分配的标记担保级别是标记服务提供商作为 ID&V 过程的结果而分配的实际值，并且响应于标记请求而被提供回标记请求者。
标记担保级别	允许标记服务提供商向 PAN /持卡人绑定指示支付标记的置信度的值。它是作为执行的识别和验证（ID & V）类型和执行它的实体的结果确定的。它也可能受到额外因素的影响，例如标记位置。



	标记担保级别在发出支付标记时设置，并且如果执行额外的 ID&V，则可以更新。标记担保级别值由标记服务提供商定义。
标记 BIN	BIN 中的特定 BIN 或范围，其仅被指定用于发布支付标记，并且在 BIN 表中被相应地标记。
标记 BIN 范围	由标记 BIN 的前 6 至 12 位组成的唯一标识符。标记 BIN 范围可以被设计为承载与相关的卡发行方卡范围相同的属性，并且将被包括在分布给参与的获取方和商家以支持路由决策的 BIN 路由表中。
标记密码	使用支付标记和其他交易数据生成的密码，以创建交易唯一值。计算和格式可能因用例而异。
标记域	可以使用支付标记的交易类型。标记域可以是信道特定的（例如仅 NFC），商家特定的，数字钱包特定的或任何上述的组合。
标记域限制控制	<p>由标记服务提供商建立的作为支付标记发行的一部分的一组参数，其将允许在支付交易中强制适当地使用支付标记。控制的一些示例是：</p> <ul style="list-style-type: none"> <li>● 使用特定演示模式的支付标记，例如非接触式或电子商务</li> <li>● 在可以唯一标识的特定商家处使用支付标记</li> <li>● 验证每个事务特有的标记密码的存在</li> </ul>
标记到期日期	由标记保险库生成并维护的支付标记的到期日期，并在事务处理期间在 PAN 到期日期字段中传递，以确保互操作性并最小化标记化实施的影响。标记到期日期是一个 4 位数字值，与 ISO 8583 格式一致。
标记互操作性	当使用具有在本说明书中定义的新字段和字段值的付费标记时，确保通过现有的可互操作能力来处理和交换各方之间的交易的过程被保留。

标记发行	创建支付标记并将其传递给标记请求者的过程。支付标记可以发行多次使用或单次使用。
标记位置	<p>标记请求者在从标记服务提供商请求支付标记时提供的支付标记和任何相关数据的预期存储模式的指示。</p> <p>此位置的安全性可能会影响可分配给支付标记的标记担保级别。标记请求者提供的安全性的尽职调查是每个标记服务提供商的责任，并且每个标记申请者分配位置类型将由每个标记服务提供商自行决定。</p> <p>当前识别的位置类型是：</p> <ul style="list-style-type: none"> <li>● 远程存储：一个示例是 card-onfile 数据库</li> <li>● EMVCo /支付网络类型的安全元件/ ICC</li> <li>● 本地设备存储：一个示例是使用消费者控制设备的标准数据存储机制存储的支付标记数据</li> <li>● 本地硬件安全存储：一个示例是使用 TEE 来确保对数据的适当限制访问</li> <li>● 远程硬件安全存储：一个例子是符合 ISO 13491 的存储</li> </ul> <p>可以随时间增加更多类别的存储位置</p>
标记呈现模式	<p>支付标记用于付款的模式。此信息将解析到一个现有的字段，称为销售点（POS）入口模式，如 ISO 8583 消息中定义，并且将被增强以包括作为本规范一部分的新的潜在值。每个支付网络将定义和发布任何新的 POS 入口模式值作为其现有消息规范和客户通知过程的一部分。除了支持非接触式的现有值，可以通过参与以下的支付网络来定义新值（如果尚未存在）：</p>

	<ul style="list-style-type: none"> <li>● 服务器启动（Card-on-file 用例）</li> <li>● 扫描（光学）</li> </ul>
标记处理	交易处理，其中代替 PAN 存在支付标记，并且从交互点到付款网络和标记服务提供商的用于 DeTokenisation 的库处理，以便允许交易完成。标记处理可以跨越包括授权，捕获，清算和异常处理的支付过程。
标记配置	将支付标记和相关值（可能包括用于密码生成的一个或多个秘密密钥）递送到标记位置的动作。
标记引用 ID	用作支付标记的替代品的值，不会显示有关支付标记或支付标记替换的 PAN 的信息。
标记请求	标记请求器从标记服务提供商请求支付标记的过程。作为该动作的结果，可以使用标记请求指示符来执行 ID&V，以示出正在使用的 ID&V 机制是用于标记请求的目的，而不是用于一些其它目的。
标记请求指示符	用于指示认证/验证消息与标记请求相关的值。它可选地作为识别和验证（ID&V）API 的一部分传递给卡发行方，以通知卡发行方正在执行帐户状态检查的原因。
标记请求者	寻求根据本说明书实现标记化并通过向标记服务提供商提交标记请求来发起对 PAN 进行标记的请求的实体。每个标记请求者将被标记化服务提供商在标记化系统内唯一地注册和标识。
标记请求者注册	正式处理标记请求，标记服务提供商可以收集关于请求者的性质和相关使用支付标记的信息，以验证和正式批准标记请求者并建立适当的标记域限制控制。成功注册的标记请求者将被分配一个标记请求者 ID，该 ID 也将在标记保险库中输入和维护。

标记服务	由标记 BIN 促成生成和发放支付标记的关键功能组成的系统，并且当标记请求者请求时，维持所建立的支付标记到 PAN 的映射。 它还包括建立标记担保级别以指示支付标记对 PAN /持卡人绑定的置信度的能力。 该服务还提供了支持标记处理的能力，该支付处理使用付费标记通过对支付标记进行解码来获得实际的 PAN 来提交。
标记服务提供商	提供由标记保险库和相关处理组成的标记服务的实体。 标记服务提供商将能够将许可的 ISO BINS 作为标记 BIN 来发出根据本规范提交的 PAN 的支付标记
标记库	由 Tokenisation 系统实现的仓库，其将建立的支付标记维持到 PAN 映射。 此存储库称为标记保险库。 标记保险库还可以维护在注册时确定的标记请求者的其他属性，并且可以由标记服务提供者用来在事务处理期间应用域限制或其他控制。
标记化	主帐户（PAN）被替换为称为支付标记的代理值的过程。 可以进行标记以增强交易效率，改进交易安全性，增加服务透明度或提供用于第三方支持的方法。

## 1.7 更多信息

有关其他支付标记实施信息，请访问 [www.emvco.com](http://www.emvco.com)。

## 第 2 章 制约

---

### 2.1 生态系统的制约

本规范旨在支付生态系统多个制约下展开，包括已经存在的实体，交易流程，相关规定和案例，这些制约包括以下：

- 本规范不是要取代或干扰任何国际，国家，区域或地方法律法规；那些法律法规高于任何行业标准。
- 本规范并不排除现有的收款方或其他第三方实施了支付标记化解决方案，这些实体在其平台中已经存在的支付标记和主账号(PAN)的映射。
- 基于不同支付环境的政策和要求，可以向收购方或商户提供额外的数据（主账号 pan 的全部或者部分），需要注意的是提供全部的主账号（pan）给商户风险要高于提供标记给商户。
- 保留产品属性，如产品类型（借记卡或信用卡），被标记过的交易可以保证现有业务不受影响，产品属性对于支付方参与者保持透明。
- 这些标记 BIN 的范围必须能被各方接受，并能依此让他们自己选择交易路由。
- 正在使用的主账号（PAN）的支付标记要有生命周期，如标记服务在处理 PAN 更新、丢失或被盗以及失效的标记将按此规范来进行
- 标记服务提供方必须了解支付环境，确保将改标记服务提供到改支付环境中，提供者不能改变现有流程，包括卡发行方，商户以及交易路由。

## 第 3 章 标记化的生态环境

---

### 3.1 支付标记生态环境

本规范所概述的是按本规范来进行支付标记化解决方案的实施并涉及到生态环境的相关角色（一些在传统的支付行业中存在的角色，和其他人是新的角色），

下图提供了支付标记生态系统中各种角色的概述，在后续章节中会更加详细介绍这些角色和功能。

图 1，支付标记服务概述

### 3.2 标记服务提供方

标记服务提供者在标记化生态系统中为授权的实体提供标记请求的标记。标记服务提供者作为支付标记授权方负责提供多个不同功能的标记容器。这些责任包括但不限于：

1. 持续的操作和维护标记库
2. 支付标记生成和发布
3. 管理并安全的应用
4. 支付标记供应
5. 标记请求登记功能

标记服务提供者负责建立并管理自己的标记请求 API，标记容器，标记供应平台和标记记录。这个规范本省并没有详细描述具体功能需求和这些所属的平台和系统，然而，标记服务提供则必须保证标记 BINS 或标记 BIN 范围区别于传统的 BINS 或 BIN 范围，是为了避免主账户和支付标记重复而产生意外。

### 3.3 持卡人

本规范不改变持卡人的角色。持卡人将继续使用发卡行发行的卡和卡账户。在大多数情况下，持卡人不期望知道一个支付标记已产生来代表他们的帐户。标记请求者可以要求持卡人进行到标记保证的身份审核，或让持卡人自行选择。

### 3.4 发卡方

发卡机构继续保持与持卡人所持卡现有这种关系，以及在支付标记系统中的授权和进行中的风险管理。任何发卡行实施的标记服务应参考这个规范以保持一致性。

### 3.5 商户

商户将继续保持现有的角色，但取决于具体的案例，可能是一个代替主账户（PAN）的支付标记的容器，例如在交易中使用 NFC 的例子。商户也可能是一个标记请求者，例如卡片管理档案使用案例会在后续的章节中具体介绍。商户继续以现有的方式处理交易，包括授权的和已有的，并将按照此规范和任何商户的收款方或支付处理者所需的要求来用任何必须或可选的数据要素作为**标记**，在使用的情况下，商家也是一个标记请求方，商家需要适应实现标记服务，在本规范中，随后通过一个标记服务提供商作为其解决方案的参考 API。更多信息，参见第 9 节支付标记交易流程。

### 3.6 收单方

收单方将按现有的方式处理所有的交易，包括包括授权、捕获、结算、和异常处理。可能需要额外的字段来支持规范。

### 3.7 支付网络

在此规范内支付网络继续在他们目前的角色，并可能额外执行标记服务提供功能，包括为标记服务提供者定义各方的角色。

支付网络作为标记服务提供商负责建设和管理自己的专有标记请求的 API，标记库，标记供应平台，和标记登记为 3.2 节标记服务提供商概述。支付网络也负责定义和制定授权、清算、和异常处理消息的影响他们的标记服务。

不是标记服务提供商的支付网络应该支持处理此功能的实现，该处理功能允许与标记服务提供商交换消息以用于去标记化，以确保付款标记互操作性。

### 3.8 标记请求者

支付标记请求者可以是支付行业中的传统参与者或新兴参与者。潜在标记请求者包括但不限于：

1. Card-on-file 商户
2. 收单方，收单方和代表商家的付款网关
3. 支付设备，如原始设备制造商（OEM）设备制造商

#### 4. 数字钱包供应商

#### 5. 发卡机构

标记请求者将被要求与标记服务提供商登记并遵守他们专有的注册表要求，系统和流程。在一个标记提供商注册成功后，标记请求会返回一个标记 ID

标记请求者，在注册了一个指定的标记服务提供商并分配了标记 ID，会执行指定的标记 API，在标记请求者在生产上安装了标记 API 后，标记请求者将能够按照 API 指定流程和技术发起支付标记请求。

当标记请求者发起的支付标记请求被标记服务提供商处理后，支付标记将被发布。

## 第 4 章 支付标记的数据元素

### 4.1 数据元素

作为本说明书的一部分，以下数据元素可能用于在支付标记发起的交易中。这些数据元素的映射和流动将通过现有的付款消息传递。

尽管每个数据元素在特定消息或 API 调用的上下文中有可能是必需的，有条件的或可选的，，以确保支付的交互性，所有参与的应支持这些所有的数据元素。

表 4-1：支付标记规范数据元素

字段名称	8583 域	长度	类型	备注
支付标记	2	13-19	数字	支付标记是指主账号(PAN) 的一个替代值，一般由 13 至 19 位的数字组成，该数值必须符合主账号的基本验证规则，其中包括 LUHN 算法校验。在银行卡支付交易中用支付标记替换卡号，用



				支付标记的有效期替换卡号有效期，不影响交易处理，增强了交易安全
标记到期日	14	4	数字	<p>由标记保险库生成并维护的标记的过期日期。 标记到期日期字段是与 ISO 8583 格式一致的 4 位数字值。。</p> <p><b>交易信息</b></p> <ul style="list-style-type: none"> <li>● 标记到期日以代替 PAN 到期日期。</li> <li>● 该值由带有 PAN 到期日的标记服务提供商替换，然后作为授权请求的一部分传递给卡发行商。。</li> </ul>
PAN 的最后 4 位数	支付特定	4	数字	<p>主帐号的最后四位数字可通过收单方提供商用于客户服务使用，</p> <p>例如印刷在消费者上收据。</p>
产品 ID	支付特定	3	字符串	<p>PAN 产品 ID 是用于确定标记化的卡产品类型的可选标识符。它可能在一些对交易透明度有要求的情况下。</p> <p><b>交易信息</b></p> <ul style="list-style-type: none"> <li>● PAN 产品 ID 是可选地作为从标记服务提供商传递到获取方授权响应的一部分。</li> </ul>
POS 输入模式	22	2	数字	<p>使用 POS 输入模式字段来指示支付标记在支付的时候被呈现的模式</p>

				<p>式。卡组织将定义和发布任何新的 POS 入口模式值作为其现有消息规范和客户通知过程的一部分。</p> <p><b>交易信息</b></p> <ul style="list-style-type: none"> <li>● POS 输入模式是将通过授权，捕获，清算和异常消息传递的现有字段。</li> </ul>
标记请求者 ID	支付特定	11	数字	<p>该值唯一地标识标记请求者与标记域的配对。因此，如果给定标记请求者需要用于多个域的标记，则它将具有多个标记请求者 ID，每个域一个。它是由标记服务提供商分配的 11 位数字值，在标记保险库中是唯一的：</p> <ul style="list-style-type: none"> <li>● 位置 1-3：标记服务提供商代码，对于每个标记服务提供商是唯一的</li> <li>● 位置 4-11：由标记服务提供商为每个请求实体和标记域分配</li> </ul> <p><b>交易信息</b></p> <ul style="list-style-type: none"> <li>● 标记请求者 ID 可以可选地通过授权，捕获，清除和异常消息传递。</li> </ul>
标记担保级别	支付特定	2	数字	<p>担保级别用于表示所申请的支付标记和其绑定的主账号 PAN 的可信程度，该值受很多因素的影响，包括账户验证的结果、身</p>

				<p>份认证的结果、风险监控系统的评分等等，它也会受到标记存储位置 等其它因素的影响。</p> <p>担保级别在标记产生时由标记服务 提供方根据一系列控制要素和验证结果综合判定；在标记产生之后，如果对该标 记进行额外的 ID&amp;V 操作，标记的担保级别也可进行更新</p> <p><b>交易信息</b></p> <ul style="list-style-type: none"> <li>● 标记担保级别将由标记服务提供商提供。</li> <li>● 该值可以可选地作为授权请求的一部分传递给卡发行方。</li> <li>● 该值可以可选地在授权响应，捕获，清除和异常处理消息中传递给 Acquirer / Merchant。</li> </ul>
标记担保数据	支付特定	可变	二进制	<p>由标记服务提供商提供的该数据包包含标记担保级别的支持信息。</p> <p><b>交易信息</b></p> <ul style="list-style-type: none"> <li>● 该数据可以可选地作为授权请求的一部分传递给卡发行方。</li> </ul>
标记密码	支付特定	可变	二进制	<p>该密码由标记请求器唯一地生成以验证授权使用标记。 密文将基于事务类型和关联的用例在事务</p>

				<p>消息中的不同字段中携带：</p> <ul style="list-style-type: none"> <li>● NFC 非接触式交易将在现有芯片数据字段中携带标记密码。</li> <li>● 其他事务，例如源自数字钱包的事务，可以在现有字段中携带标记密码。</li> </ul> <p><b>交易信息</b></p> <ul style="list-style-type: none"> <li>● 标记密码将在授权请求中传递并由标记服务提供商和/或卡发行商验证。</li> </ul>
以下数据元素仅用作标记服务提供商和颁发者之间的 ID&V 期间的可选字段				
标记请求指示符	付款网络特定 / ID & V 过程具体	可变	付款网络特定 / ID & V 过程具体	用于在支付标记请求期间认证持卡人的指示符。

## 第 5 章 对 TSP 的要求

### 5.1 介绍

本节描述标记服务提供商实现符合本规范的标记服务的要求。使用 ID&V(识别和验证)方法，标记服务 API，标记处理功能和标记生命周期管理将

多个责任分配给标记服务提供商，包括标记保险库，标记发行，标记担保。

尽管说明书描述了标记请求器和标记服务提供商之间的直接关系，但是它不排除充当聚合器或网关的中间实体，向多个标记服务提供商提供该标记请求者的表示，只要标记域限制控制保持。

## 5.2 标记保险库要求

标记服务提供商应开发和操作标记保险库，该标记保险库将提供生成和发放支付标记的能力，建立和维护支付标记到 **PAN** 卡的映射，并提供底层安全性和相关处理控制，例如事务处理期间的域限制。标记保险库提供支付标记到 **PAN** 映射的机制，使其在事务处理（例如授权，捕获，清算和异常处理）期间可用。标记保险库需要在其整个生命周期中维护映射到给定 **PAN** 的所有关联的支付标记。

### 支付标记生成

标记服务提供商生成支付标记以响应支付标记请求。支付标记生成应仅使用分配的标记 **BIN** 或 **BIN** 内的范围来执行生成过程，以确保不存在生成与 **PAN** 冲突的可能性。在支付标记生成时，标记服务提供商应该识别和存储支付标记到 **PAN** 映射，以用于标记保险库中的后续事务处理。标记保险库还应将每个生成的支付标记和发起请求的请求者 **ID** 相关联：

包括授权，清算和异常处理的业务功能的传统处理将需要与适当的支付网络和相关标记保险库解决方案集成，以确保标记服务以保持这些交易过程的互操作性和持续完整性的方式执行。任何发卡行实施的标记服务应该考虑遵循此规范，以便与使用此规范部署的解决方案的互操作性和一致性。生成的支付标记应包括标记到期日期。标记到期日应满足 **PAN** 到期日的格式要求。

### 支付标记发布和配置

支付标记应通过对已经注册的标记请求者请求进行响应，通过有效的标记请求者 **ID**。支付标记请求应根据标记请求方和标记服务提供商所同意的请求担保级别采用指定的 **ID&V** 认证方法。

支付标记发行还可以包括向标记请求者提供支付标记。支付标记配置在支付标记生成并且保证步骤完成之后进行。与之相关联的方法是每个标记服务提供商专有的，并且在本说明书的范围之外。

通过标记请求器和标记服务提供商之间的接口来执行付费标记。

标记服务提供商还可以选择通过使用特定的基于 ISO 8583 的授权请求消息来执行支付标记发放和提供，以执行支付标记请求并且将 ID&V 信息传送到标记服务提供商用于后续处理。在这种情况下，基于 ISO 8583 的授权响应消息可以用于将支付标记和相关联的标记到期日返回给标记请求者。

### 安全和控制

由于存储和管理的数据映射的敏感，标记保险库应通过根据行业标准的强物理和逻辑安全措施来保护

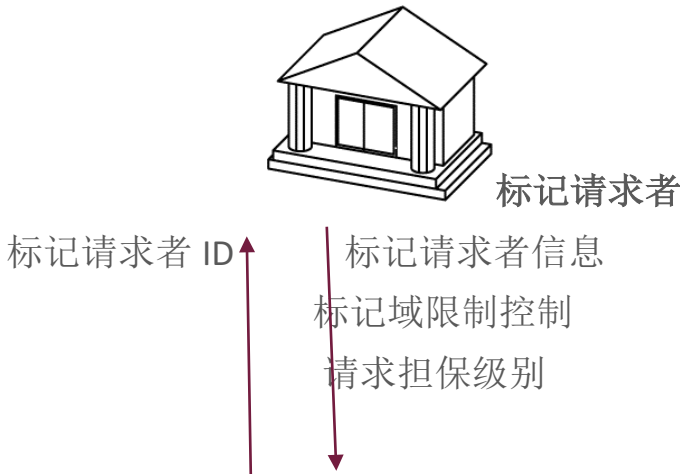
标记服务提供商结合支付交易处理，应负责将基于标记的交易限制到与在标记请求者注册时确定的给定标记请求者相关联的适当域

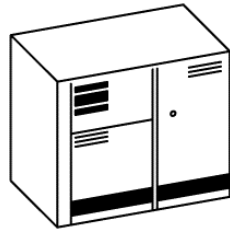
标记请求者通过注册，批准和注册实体作为标记请求者来确保标记服务的完整性。标记服务提供者应当向给定的标记请求者分配至少一个唯一的标记请求者 ID，并且负责标记请求者及其相关联的标记请求者 ID 的生命周期管理。作为注册的一部分，标记服务提供者还应捕获与给定标记请求者相关联的所请求的标记担保级别和标记域限制控制，并确保这些域限制可用于标记保险库以在支付标记交易期间应用这些限制 处理。

### 标记请求者注册

标记服务提供商应建立一个过程来注册请求指定为标记请求者的实体。可以使用多个标记服务提供商的标记请求器的实体、根据每个标记服务提供商建立的专有过程，与每个标记服务提供商分开注册。

图 3：标记请求器注册过程





标记服务提供商

每个标记服务提供商确定从标记请求者收集的信息，并建立其自己的专有过程用于收集，审查和批准。收集的信息可能包括典型的了解您的客户（KYC）信息以及注册标记请求者将支持的支付标记使用场景，包括任何适当的域名限制和其他交易控制。

注册功能的结果是对预期标记请求者的注册申请的批准或拒绝决定。批准的标记请求者被分配唯一的标记请求者 ID。域限制和其他事务控制应传送到标记保险库并与其协调以便实施。

### 标记保证

标记服务提供商应确定与每个批准的标记请求者相关联的期望的担保级别，并且基于用例来定义在支付标记请求和批准过程期间应用的 ID 和 V 的类型。初始标记保证等级是在支付标记请求时基于 ID&V 过程的类型和结果确定。在支付标记发行之时，可以更新标记担保级别。

### 标记域限制控制

为了确保标记请求者意图使用付费标记，需要额外的控制来管理和验证付费标记的基本使用。这些控制应由标记服务提供商基于条件（包括用例）来定义和实现，标记域，例如在标记请求者注册过程期间识别的商家标识符和 POS 输入模式。这些标记域限制控制旨在确保支付标记的任何暴露不会导致后续欺诈的显著水平。给定标记请求者的允许的标记域限制控制部分地由在标记请求者注册时指定并且由标记服务提供商批准的支付标记使用情况驱动。这些标记域限制控制应存储在标记保险库中或具有同等安全保护的位置。实际的标记域限制控制由标记服务提供商及其专有标记保险库应用和执行。

## 标记请求者 ID

由标记服务提供商分配的每个标记请求者 ID 应是唯一的，并且不与来自同一标记服务提供商或另一标记服务提供商的其他分配的标记请求者 ID 冲突。

每个标记请求者将被分配一个标记请求者 ID，每个域一个。它是标记服务提供商分配的 11 位数字值，具有以下约定：

- 位置 1-3：标记服务提供商代码，每个标记服务提供商都是唯一的
- 位置 4-11：由标记服务提供商为每个请求实体和标记域分配

标记服务提供商代码被分配给每个标记服务提供商并由 EMVCo 维护。有关更多信息，请访问 EMVCo 网站：[www.emvco.com](http://www.emvco.com)。

标记请求者 ID 是应当在事务中存在的底层控制数据元素。在将标记请求者 ID 传递给商家的使用情况下，如果交易中存在的标记请求者 ID 与存储在标记保险库中的该支付标记的标记请求者 ID 不匹配，则这些交易不应被允许成功处理。

## POS 输入模式

被设计为限制与特定标记请求者相关联的交易的其他控制包括使用 POS 输入模式代码字段中携带的 POS 输入模式值，以将标记的使用限制为仅仅在标记请求者注册期间同意的那些 POS 输入模式。

## 商户信息

在商家可以是标记请求者的使用情况下，商家相关数据元素，例如卡接受者 ID 与获取者识别数据元素的组合，应当用于通过比较 事务处理消息和标记申请者在注册期间确定的信息后并在标记库中建立控制。一个这样的使用情况将是由文件卡商人持有的 PAN 的标记化。

## 报告和原始数据

令牌服务提供商应该能够向报告工具提供关于已批准，待决或被拒绝的令牌请求（包括任何分配的令牌请求者 ID）的报告或数据输出。

标记服务提供商还应该能够向报告工具和应用提供与基于标记的事务相关的数据输出，并且在报告输出中适当地呈现支付标记和/或 PAN。如果标记请求者被撤销或分配了新的标记请求者 ID，则此信息还应当进行报告和审计，并与标记保险库容。



## 5.3 收单方要求

收单方应实施本规范中引用的任何必需或可选数据元素，并由支持的支付网络的消息规范进一步定义。

## 5.4 支付网络要求

付款网络应在其专有消息规范的上下文中实现所有字段，包括本规范中定义的必需字段和可选字段，并通过现有通信通道传达这些更改。

# 第 6 章 身份识别和验证（ID&V）的方法

---

## 6.1 介绍

ID&V 方法提供了一组功能和服务，支付标记与持卡人信息联系在一起，用于验证持卡人及其账户的有效性的方法，ID&V 作为支付标记申请时的一个重要环节，其结果直接决定了所申请的支付标记和原始主账号 PAN 之间的可信程度。

标记发行/配置时所采取 ID&V 步骤，以及使用支付标记，标记级别的基本要素，可以由 TSP 建立特别计划、交易分类或其他专有业务划定。用于通信支付标记级别和 ID 和 V 步骤进行支付标记，TSP 标记服务提供商应保持下面执行步骤

1. 标记级别确定

2. 标记数据确定

TSP 标记服务提供商应通过相应方法和过程来进行确认标记级别和数据，级别和数据需要和主账户、持卡人相结合。

## 6.2 ID&V 发卡行的识别认证

ID&V 方法可单独使用或组合，以提供特定的支付级别。这些级别的范围从没有保证到高保证取决于 ID&V 方法和 TSP 标记服务提供商评估确认结果。以下是 ID&V 的方法：实例标记的方法，可单独使用或组合使用

1. 帐户验证

2. 标记服务提供商风险评分
3. 标记服务提供商对标记请求数据风险评分
4. 发卡行对卡的信息校验

附加的方法可以在标记服务提供者的酌情权下实现。标记服务提供者应实现一个或多个 ID&V 方法。此外，该标记服务提供商应确保与标记相应的 ID&V 方法。发行标记时总是执行保证级别。

ID&V 的步骤可以由标记服务提供商进行，在由标记以外的实体执行 id&v 步骤的情况下提供服务的，应当提供可验证的流程，以证明步骤是执行和所得到的结果提供。可核实的证据可以包括：

标记提供给标记服务提供者的值。服务提供商可能会验证。什么是可核查的结果的细节外，本规范的范围，但包括密码或授权码。这些要求适用于所有的 ID&V 方法，除了其中的条件不执行 ID&V。标记服务提供者应将标记保证级别设置为适当的值的基础上进行的 ID&V（00 = 没有 ID&V，99 = 最高保证），和标记存储提供的标记请求信息和使用标记请求注册时间。下表提供了基于 id&v 步骤执行的派生标记保证级别。额外的 ID&V 方法可以定义在未来的补充或修订本规范。

ID&V 保证方法	执行保证	用途
不执行 ID&V	无	账号替换支付标记
账号验证（0 金额授权、是否有 AVS、卡校验位）	标 记 请 求 者 服务提供商	账号替换支付标记
标记服务提供商风险评估	服务提供商	认证数据标记
支付标记评估风险，通过用户数据和支付数据	发卡行、代理商	通过特定信道或域，确保高保证级别与标记验证数据

### 6.2.1 不执行 ID&V

当支付时，标记保证级别应设置为不保证值。标记已发出没有任何 ID 和 V 步骤执行标记。根据标记使用情况和标记服务提供商规则，支付标记仍可以用于发起支付交易，但不进行任何标记保证。

### 6.2.2 账户验证

这个 ID&V 保证方法提供了一个基本的帐户验证检查，以验证主账号 PAN 在发卡行是否有效。验证方法可以包括，但不限于：

- 0 美元的授权
- 卡校验位验证
- 邮政编码和地址验证

帐户验证方法可以由标记请求通过标记服务提供商提供的 API 发起，或由标记服务提供商在标记时间发起。

### 6.2.3 TSP 保证

标记服务提供商应建立和维护评估技术和工具支持以风险为基础的评估。标记服务提供商定义了将保证级别与适用方包括发卡机构。

### 6.2.4 标记服务提供商保证请求数据

此 ID 和 V 保证方法涉及使用由标记请求者提供的数据元素，可以预测诈骗。数据元素的例子包括，但不是限于：

- 帐户年龄和历史
- 地址和联系信息
- IP 地址
- 设备标识和设备信息
- 地理位置地址
- 交易速度

标记服务提供商应该有适当的评估技术和工具地方实施此 ID&V 方法，并结合所得的 ID&V 数据与标记服务提供商的风险和验证数据相关的主账号 PAN 来确定分配的标记保证级别。发卡机构可能参与这一过程。标记服务提供商定义了用于通信保证级别和 ID&V 的方法。适用各方的步骤，包括发卡人。

### 6.2.5 发卡行对持卡人信息验证

此 ID&v 方法涉及与发卡行或其代理交互执行对持卡人验证，以满足必要的保证完成绑定主账户通过支付标记。用于验证的方法应设计提供基于设备类型的可接受的用户体验，例如移动电话或计算机；持卡人可在认证过程中使用。设备指引应创建和遵循，以确保一致的用户体验。发卡机构的认证设计应利用输入数据和分数，标记请求者通过信用卡发行机构提供最准确的数据验证。使用这些数据，在许多情况下，允许发卡机构和授权的持卡人，进行支付标记不必在添加额外的步骤。

## 第 7 章 TSP 的 API

---

### 7.1 总览

本节建立了每个 TSP 服务接口的通用数据元素，每个 TSP 服务的 APIs 都应支持外部另一个可用的 TSP 服务。

TSP 必须实现接口，并提供给所有与 TSP 交互的实体来使用。

本规范不提供每一个 TSP 接口在技术层面的实施细节的或详细说明。

TSP 必须与每一个交互的实体实现安全的交互方法。

本节不设计标记处理流程。更多信息，参见第 9 节支付标记交易流程

### 7.2 标记服务参与端点

TSP 必须有为那些授权通过安全方法验证的实体提供建立和使用标准接口或 APIs 的能力, 以下是可能发生这些交互的认证方法的示例：

- Web services
- 复合 ISO 8583 规范通过现有的支付网络接口进行消息交换
- 批量文件

以下是可以参与和使用标记服务接口的实体的示例：

- 标记请求者
- 收单方

- 支付系统
- 第三方系统
- 商户
- 需求方和发卡处理方
- 发卡机构
- 发卡机构 3D 安全 ACS

## 7.2 接口类别

本节描述 TSP 将实现的接口和消息，以提供标记服务。这些接口分为以下类别：

- 标记请求和发放
- 标记保证 (ID&V)
- 去标记化
- 标记路由
- 标记生命周期管理

每种类别应具有一个或多个定义的接口或消息以执行特定的标记相关操作

### 7.3.1 标记请求和发放

TSP 应提供一种标准方法，可以使用该方法通过标准接口提交注册标记请求，通过输入原始支付凭证来获得响应的付款标记。

TSP 必须实现适当的控制和处理通过输入主账号(PAN)来生成标记。另外，必须保证该请求的安全。当这种保证步骤涉及也用于其他目的的机制（例如 3-D Secure）的情况下，标记请求指示符应当用于指示该机制正被用作标记请求的一部分。

标记请求接口可支持实时请求，并安全的返回支付标记。或是通过批量文件接口批量返回支付标记。

#### 7.3.1.1 输入元素

此请求最小必须包含以下数据元素：

- Token Requestor ID（标记请求者 ID）
- PAN（主账号）
- PAN Expiry Date（主账号到期日）

如果请求了特定的安全级别，则存在请求安全级别。

标记位置提供有关标记数据存储位置的信息。该位置的安全性可能影响可以分配给标记的安全级别。标记请求者提供的安全性的尽职调查是每个标记服务提供商的职责，并且每个标记申请者分配位置类型将由每个标记服务提供商自行决定。标记地址在付款标记的生命周期内不会更改

当前指定的存储为:

- 远程存储：例如 一个 **card-on-file** 数据库
- **EMVCo** /支付网络类型的安全元件/ **ICC**
- 本地设备存储：例如 使用消费者受控设备的标准数据存储机制来存储标记数据
- 本地硬件安全存储：例如 使用 **TEE** 来确保适当地限制对数据的访问
- 远程硬件安全存储：符合 **ISO 13491** 标准的存储

协议提供了标记请求者如何与持卡人通信的信息。所使用的通信信道的安全性可以影响可以分配给支付标记的安全级别。

帐户验证结果包含先前执行的帐户验证交易的结果，例如具有或不具有地址验证的\$0验证。





可选的持卡人数据元素可以包括附加数据，例如但不限于票据/运送地址和邮政编码以执行标记保证 **ID&V** 方法。这不是一个详尽的列表，并可能在未来增长。

设备信息用于标识存储付款标记的特定设备。示例包括安全元件 **ID** 和/或设备的特性，例如 **MAC** 地址，操作系统版本，语言等。

**Table 7-1 标记申请请求元素**

字段名	长度	格式	R/C/O	描述
版本号	3	N.N	<b>R</b>	该消息版本号
标记请求者 ID	11	Numeric	<b>R</b>	引用自 Table 4-1：支付标记规范数据元素的详细描述。
主账号长度	2	Numeric	<b>R</b>	主账号长度
主账号	13-19	Numeric	<b>R</b>	主账号
主账号到期日	4	Numeric	<b>R</b>	主账号到期日
要求的标记保证级别	2	Numeric	<b>O</b>	如果要求保证级别，请参见表 1-3：定义以了解详细描述

标记位置	2	Numeric	C	<p>除非在标记请求程序 API 中固有，否则必需。表示付款标记的存储位置：</p> <ul style="list-style-type: none"> <li>• 01 –远程存储</li> <li>• 02 –EMVCo /支付网络类型的安全元件/ ICC</li> <li>• 03 –本地设备存储</li> <li>• 04 –本地硬件安全存储</li> <li>• 05 –远程硬件安全存储</li> <li>• 06 –预备以后使用</li> </ul>
协议	2	Numeric	C	<p>除非在标记请求程序 API 中固有，否则必需。描述标记请求者使用什么协议与持卡人通信。值是标记服务提供程序特定的，可以包括的值：</p> <ul style="list-style-type: none"> <li>• 移动 App</li> <li>• 浏览器</li> </ul>
账户验证结果	2	Numeric	O	表示帐户验证的结果（如果执行），例如 通过，失败（值将是付款网络特定）
账户验证参考长度	2	Numeric	R	帐户验证参考的长度，如果不存在，将包含零（0）
账户验证参考	Variable	Alphanumeric	O	<p>标记请求者执行的帐户验证事务的引用。</p> <p>注意：如果需要，引用应包含足够的信息以确定执行的认证类型。</p>
标记请求风险	4	Numeric	O	欺诈风险评分，由标记请求



评分				者提供
地址不匹配指示器	2	Numeric	<b>O</b>	如果运费和帐单地址不同，则填入
持卡人数据长度	4	Numeric	<b>R</b>	持卡人数据的长度，如果不存在，将包含零（0）
持卡人数据	Variable	Alphanumeric	<b>C</b>	支持请求安全级别所需的数据。包括但不限于：  帐单地址  装运地址  邮政编码  CAV2 / CVC2 / CVV2 / CID 有关 ID 和 V 方法的详细信息，请参阅第 6 节标记保证 ID&V 方法。
设备信息长度	2	Numeric	<b>R</b>	设备信息长度，如果不存在，将包含零（0）
设备信息	Variable	Alphanumeric	<b>O</b>	可用于标识设备的设备属性

R-必需的，C-有条件的，O-可选的



字段格式的实现由每个标记服务提供者 API 定义

### 7.3.1.2 输出元素

接口应提供在响应中包含以下数据元素的响应消息：

-  请求的状态 - 成功或失败
-  原因代码 - 指示故障类型的代码

对于成功的请求，应在响应中返回以下附加数据元素：

-  支付标记
-  支付标记到期日



当在标记请求时已经执行标记保证方法时，接口可以可选地提供为该付款标记计算的指派的标记保证等级

**Table 7-2 标记请求响应元素**

字段名	长度	格式	R/C/O	描述
版本号	3	N.N	<b>R</b>	该消息版本号
请求状态	1	Numeric	<b>R</b>	表示请求的成功或失败
原因代码长度	2	Numeric	<b>R</b>	原因代码长度，如果不存在，将包含零（0）
原因代码	Variable	Alphanumeric	<b>C</b>	如果请求状态不成功，则显示
标记长度	2	Numeric	<b>R</b>	付款标记的长度，如果不存在，将包含零（0）
支付标记	Variable (from 13 to 19 digits)	Numeric	<b>C</b>	如果请求状态成功，则表示支付标记由 TSP 生成
标记参考 ID 长度	2	Numeric	<b>R</b>	标记长度参考 ID，如果不存在，将包含零（0）
标记参考 ID	Variable	Numeric	<b>O</b>	支付标记的参考标识符
标记到期日	4	Numeric	<b>C</b>	如果请求状态成功，则表示标记到期日期，由 TSP 生成
标记分配保 证级别	2	Numeric	<b>C</b>	如果请求状态成功并且请求了 ID&V，则存在，参见表 4-1：付费标记规范数据元素的详细描述

## 7.3.2 标记安全级别更新

### 7.3.2.1 输入元素

此请求的输入最低限度包含以下数据元素：





- 付款标记
- 标记到期日期
- 标记请求者 ID

如果请求了特定的安全级别，则存在请求安全级别。

可选的持卡人数据元素可以包括附加数据，例如但不限于票据/运送地址和邮政编码以执行标记保证 ID&V 方法。这不是一个详尽的列表，可能会在未来扩大。

**Table 7-3 标记安全级别更新请求元素**

字段名	长度	格式	R/C/O	描述
版本号	3	N.N	R	该消息版本号
标记长度	2	Numeric	R	支付标记长度
支付标记/ 标记参考 ID	Variable (from 13 to 19 digits)	Numeric	R	支付标记参号
标记请求 者 ID	11	Numeric	R	分配给请求支付标记的注册企业实体的唯一值
要求的标记保 证级别	2	Numeric	C	表示标记请求者希望执行的验证级别。如果标记请求者正在请求特定的标记安全级别（而不是仅仅一个，安全级重新评估）
账户验证 结果	2	Numeric	O	表示帐户验证的结果（如果执行），例如 通过，失败（值将是支付网络指定）
账户验证	2	Numeric	R	帐户验证参考的长度，如

参考长度				果不存在，将包含零（0）
账户验证 参考	Variable	Alphanumeric	O	标记请求者执行的帐户验证事务的引用。  注意：如果需要，引用应包含足够的信息以确定执行的认证类型。
标记请求 风险评分	4	Numeric	O	欺诈风险评分，由标记请求者提供
地址不匹 配指示器	1	Boolean	O	指示出货地址和帐单地址是否不同
持卡人数据 长度	4	Numeric	R	持卡人数据的长度，如果不存在，将包含零（0）
持卡人数据	Variable	Alphanumeric	C	支持请求安全级别所需的数据。包括但不限于：  <div>  帐单地址 </div> <div>  装运地址 </div> <div>  邮政编码 </div> <div>  CAV2 / CVC2 / CVV2 / CID </div> 有关 ID 和 V 方法的详细信息，请参阅第 6 节标记保证 ID&V 方法。
设备信息长度	2	Numeric	R	设备信息长度，如果不存在，将包含零（0）
设备信息	Variable	Alphanumeric	O	可用于标识设备的设备属性

### 7.3.2.2 输出元素

**Table 7-4 标记安全级别更新响应元素**

字段名	长度	格式	R/C/O	描述
版本号	3	N.N	<b>R</b>	该消息版本号
请求状态	1	Numeric	<b>R</b>	表示请求的成功或失败
原因代码长度	2	Numeric	<b>R</b>	原因代码长度，如果不存在，将包含零（0）
原因代码	Variable	Alphanumeric	<b>C</b>	如果请求状态不成功，则显示
标记长度	2	Numeric	<b>R</b>	付款标记的长度，如果不存在，将包含零（0）
支付标记	Variable (from 13 to 19 digits)	Numeric	<b>C</b>	如果请求状态成功，则表示支付标记由 TSP 生成
分配的标记 保证级别	2	Alphanumeric	<b>R</b>	标记安全级别，请求状态成功并且已请求 ID&V 时显示

### 7.3.3 去标记化查询

去标记化查询接口通过将映射的原始 PAN 和 PAN 到期日期凭证返回给经认证的实体，是交换支付标记的必要机制。

对此请求不执行事务特定验证：其目的是使原始卡详细信息可用于可信方，并且不在事务处理中使用。

TSP 应实现适当的访问安全控制，特别是 TSP 应确保从已识别，授权和验证的源接收请求。

#### 7.3.3.1 输入元素

**Table 7-5 去标记化查询请求元素**

字段名	长度	格式	R/C/O	描述
-----	----	----	-------	----

版本号	3	N.N	<b>R</b>	该消息版本号
标记请求者 ID	11	Numeric	<b>C</b>	当可用于去标记化请求 Token Length 时存在。 有关 详细说明，请参阅表 4-1： 付款标记规范数据元素。
标记长度	2	Numeric	<b>R</b>	支付标记长度
支付标记	Variable (from 13 to 19 digits)	Numeric	<b>R</b>	已发放的支付标记
标记到期日	4	Numeric	<b>R</b>	已发放的支付标记到期日期

### 7.3.3.2 输出元素

接口应提供包含以下数据元素的响应消息：

- 请求的状态 - 成功或失败
- 原因代码 - 解释故障类型的代码

对于成功的请求，响应中返回以下附加数据元素：

- AN
- AN 到期日期

**Table 7-6 去标记化查询响应元素**

字段名	长度	格式	R/C/O	描述
版本号	3	N.N	<b>R</b>	该消息版本号
请求状态	1	Numeric	<b>R</b>	表示请求的成功或失败
原因代码长度	2	Numeric	<b>R</b>	原因代码长度，如果不存在，将包含零（0）
原因代码	Variable	Alphanumeric	<b>C</b>	如果请求状态不成功，则显示
主账号长度	2	Numeric	<b>C</b>	如果请求状态成功，显示主账号长度

主账号	Variable (from 13 to 19 digits)	Numeric	C	如果请求状态成功，显示主 账号
主账号到期 日	4	Numeric	C	如果请求状态成功，显示 PAN 到期日期

### 7.3.4 去标记化验证

去标记化查询接口通过将映射的原始 PAN 和 PAN 到期日期凭证返回给经认证的实体，是交换支付标记的必要机制。同时执行对支付标记的任何所需验证并且实施与标记域相关联的标记域限制。

#### 7.3.4.1 输入元素

**Table 7-7 去标记化验证请求元素**

字段名	长度	格式	R/C/O	描述
版本号	3	N.N	R	该消息版本号
标记请求 者 ID	11	Numeric	C	当可用于去标记化请求 Token Length 时存在。 有关详细说明，请参阅 表 4-1：付款标记规范数 据元素。
标记长度	2	Numeric	R	支付标记长度
支付标记	Variable (from 13 to 19 digits)	Numeric	R	已发放的支付标记
标记到期 日	4	Numeric	R	已发放的支付标记到期 日期
交易数据 长度	3	Numeric	R	事务数据元素字段长 度，如果不存在，将包

				含零（0）
交易数据	Variable	Implementation Dependent	O	其它的 TSP 执行请求所必要的交易数据元素，内容为 TSP 所私有

#### 7.3.4.2 输出元素

**Table 7-8 去标记化验证响应元素**

字段名	长度	格式	R/C/O	描述
版本号	3	N.N	R	该消息版本号
请求状态	1	Numeric	R	表示请求的成功或失败
原因代码长度	2	Numeric	R	原因代码长度，如果不存在，将包含零（0）
原因代码	Variable	Alphanumeric	C	如果请求状态不成功，则显示
主账号长度	2	Numeric	C	如果请求状态成功，显示主账号长度
主账号	Variable (from 13 to 19 digits)	Numeric	C	如果请求状态成功，显示主账号
主账号到期日	4	Numeric	C	如果请求状态成功，显示 PAN 到期日期
交易数据长度	3	Numeric	R	事务数据元素字段长度，如果不存在，将包含零（0）
交易数据	Variable	Implementation Dependent	O	其他事务数据元素为 TSP 执行请求所必需，内容是 TSP 所专有的

### 7.3.5 标记生命周期管理

支付标记可能需要由于 PAN 和 PAN 到期日期的更改，以及可能需要停用映射的事件

而进行的持续管理和更新。

TSP 应通过接口提供生命周期更新，以管理影响已发出的支付标记的更改。这些接口可以由多方使用，包括标记请求方，卡发行方和支付网络。生命周期管理可能需要支持现有的常规商业流程，例如发卡行组合转换。下表提供了应该由令 TSP 作为接口提供的生命周期事件的示例集合。注意，TSP 不执行针对每个事件描述的动作，这并不是必需的：针对每个事件执行的动作将由 TSP 自行决定。

前面章节中定义的数据元素也适用于这些接口。

**Table 7-9 生命周期时间**

序号	Interface	示例事件/描述	发起者	执行的操作
1	取消标记	1) 设备丢失或被盗 2) 原始凭据不再有效 3) 标记请求程序不再携带卡上文件 4) PAN 丢失或被盗 5) PAN 上的欺诈警报 6) 付款标记上的欺诈警报	标记请求者 卡发行商 支付网络	支付标记与 PAN 断开连接，并且禁用映射以供进一步使用。
2	暂停标记	由于设备丢失或被盗，暂时停用	标记请求者 卡发行商	支付标记到 PAN 映射被暂时挂起，并且将停止



			支付网络	进一步使用。
3	激活标记	首次激活或恢复已暂停的支付标记到 PAN 映射	标记请求者 卡发行商 支付网络	支付标记到 PAN 映射被激活。
4	更新标记保证	持续管理付款标记上的标记安全级别	标记请求者 卡发行商 支付网络 TSP	基于所执行的 ID & V 方法或作为内部操作的结果，针对支付标记到 PAN 映射更新标记保证级别
5	更新主账号属性	更新原始凭证，例如 PAN 到期日	卡发行商 TSP	更新主账号属性，例如主账号到期日，用于延长支付标记到主账号的映射的使用

## 第 8 章 支付标记过程

---

### 8.1 概述

本规范包括使用现有数据字段，包含支付标记相关的当前字段中的数据，以及新字段，其中有些是必需的，以便在整个支付系统中提供一致性和互操作性。作为本规范的一部分引入的其他新字段是可选的。与支付交易处理相关领域内 tokenisation 的存在类型将因用例在第 9 节支付标记事务流中的突出而变化。

## 8.2 路由和帐户范围表

路由和帐户范围表需要清楚区分标记 bins 和标记 bin 范围从传统的 bins 和 bin 范围，以确保潜在的完整性支付标记事务处理。这需要标记服务提供商分配 bins 和标记 bin 范围是独特的，不同于传统的 bins 范围标记相应的所有路由和帐户范围表。

## 8.3 交易授权

交易授权信息，特殊的请求信息来自需求的商户，需要的支付网络，和卡发行的支付网络，and 全部相应的响应消息，收到本规范的影响。影响的程度不同的使用案例，将授权信息规范定义通过参与支付网络沟通作为其执行的一部分基于这一规范标记的解决方案。

以下是支付象征性的事务处理关键要求：

1. 标记服务提供商应验证传入中的支付标记.授权信息对数据元素，包括 Requestor ID（如果标记可用，并向支付网络提供支付有效性的结果标记域限制控件中的标记。
2. 支付网络应该使用标记服务提供商映射支付.在发送消息之前标记进入授权信息发到发卡行，并应始终映射主账号 PAN 支付标记在任何响应消息返回（除非卡发行人作为标记服务提供商）。
3. 当已被视为丢失的支付标记/被盗和/或已被标记为暂停，标记服务提供商应向支付网络通知更改支付标记状态。

## 8.4 交易期间标记域限制控制

标记服务提供商和参与支付网络提供的应用能力特定的标记域限制控制对于一个给定的标记请求和使用定义案例。标记域限制控制依赖于特定控件的可用性，事物处理消息和基础数据完整性中的相关数据元素，如这些数据元素将是至关重要的，以确保控制使用支付标记。域可以包含一个或多个通道，只要标记域限制控制可以全面执行防止交叉渠道欺诈。

## 8.5 采集加工

本规范对捕获处理的影响是通过这样的实体定义或基于与参与支付相关的结算要求的支付处理器网络。本规范定义的结算要求，并在由支付网络操作的结算系统的上下文，确定任何影响支付处理器处理和相关商家。

## 8.6 结算

从需要方的支付结算信息流网络，发卡行支付网络，受本规范影响的影响程度不同的用例和将被定义在结算消息规范通过参与支付网络沟通作为他们的支付解决方案，是基于 **tokenisation** 部分实现本规范。这些结算相关规格确定的变化需求方和支付处理器捕获处理消息规范。

## 8.7 异常处理

发卡行支付网络和需求方的支付网络，可以通过退款信息发送，通过本规范的影响。影响的程度因使用而变化案件将在扣款信息规范所定义的参与支付网络作为其支付 **tokenisation** 实现部分基于此规范的解决方案。

# 第 9 章 标记化支付的交易流程

---

## 9.1 通用

基于该规范的标记服务实现目前正在推进，但它并没有想改变传统的使用 **PAN** 支付交易的方法和流程。然而，支付标记的引入需要在一些新的数据元素中传递数据，在现有数据元素内携带一些标记相关数据，并且确保支付网络可以识别支付标记交易，以便确保支付标记被替换，在交易处理中由适当的标记服务提供者标记。为了解基本要求，本规范对付款标记交易流的影响必须对每个潜在用例单独检查。

每个标记服务提供商有责任通知持卡人对授权（和其他）消息的任何更改，特别是哪些字段的用法已更改，哪些字段是新的。每个标记服务提供商也有责任确保发卡行在处理付款标记交易时了解责任分离，例如在 **NFC** 销售点使用情况下，标记服务提供商可以认证支付标记的有效性，但是卡发行商仍然检查是否需要卡持有人验证。

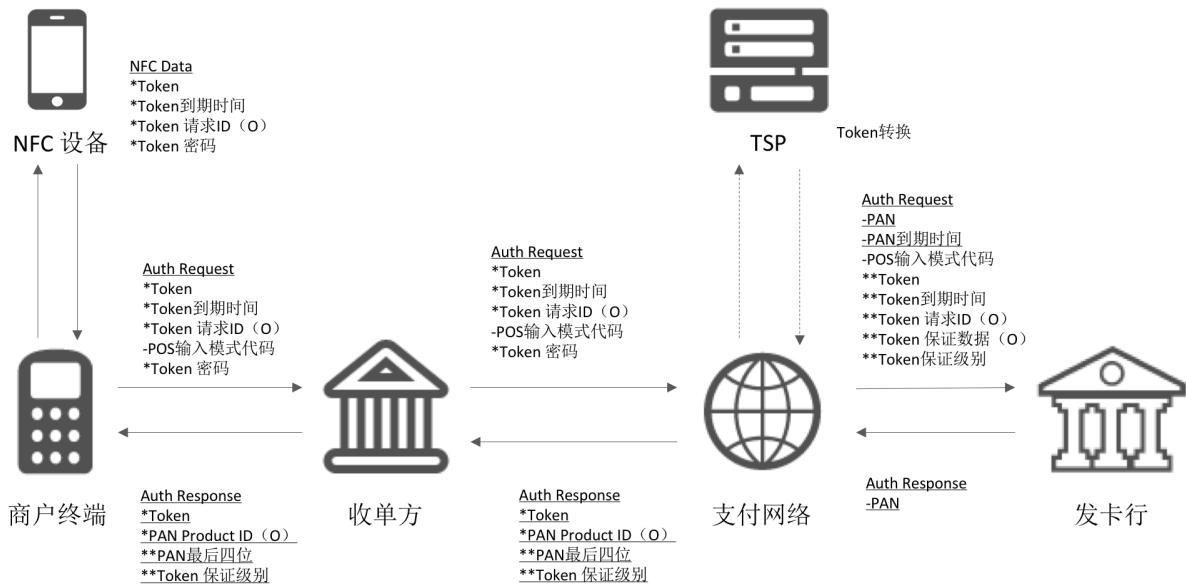
在本规范中定义的样例用例包括在 **POS** 上的、移动/数字钱包电子商务、基于文件卡的电子商务和销售点扫描的移动 **NFC**。根据用例，对授权、提交和退款事务处理、基本消息请求有不同级别的影响。这些用例中的每一个关于现有字段的使用，当前字段中的支付标记数据的存在以及新的数据字段（必需的和可选的）来检查，包括用于支持标记域限制控制的支付标记控制字段标记服务提供商与付款网络相结合。下图标示了授权、捕获、清除和异常处理事务中可能存在或可能不存在的一些关键数据元素，这取决于用例以及数据元素是否被认为是必需的或可选的。对于每个消息，将根据用例，支付品牌等存在附加的数据字段。这些附图不试图提供在每个消息中使用的数据元素的完整列表。

所提供的用例仅是示例，不需要被支持，也不打算是可能的用例的详尽列表。除了这里介绍的内容之外，这个规范可以用于服务更多的用例。

## 9.2 使用场景 1：商户的移动 **NFC**

在这种使用情况下，支付标记存储在支持 **NFC** 的移动设备中，或者在远程服务器中并且即时地传送到设备。标记提供可以由标记请求器与标记服务提供商接口来完成。当发起交易时，移动设备和/或远程服务器将生成非接触交易包括支付标记，标记到期日期，标记密码和其他芯片数据元素，并且经由 **NFC** 接口将事务传递到商家的终端。

具体流程如下图：



以下步骤描述了当移动设备在具有 NFC 功能的销售点终端处使用时授权消息中的标准支付标记数据字段的流程：

1. 移动设备将通过支付应用与 NFC 终端交互，并将以下关键的支付标记数据元素传递到商家终端：
  - a. 付款标记放在现有 PAN 字段域中传递
  - b. 标记到期日将在 PAN 到期日字段中传递
  - c. 标记密码将基于标记数据元素生成，并将在密码密码字段中传递。  
(密码可以是全芯片密码，或缩写的 Track 2 等效密码。)
  - d. 标记请求者 ID 将作为可选字段传递。
  - e. 所有其他非接触式数据元素将按照非接触式数据标准创建和传递

#### 【注】

从移动设备生成的标记密码以及 POS 输入模式将用作域限制控制字段，标记服务提供商使用该字段限制字段来验证使用该付款标记的交易的完整性。

2. 商家终端将把非接触授权请求传递给收单方，其携带所有标准的支付标记数据字段和非接触式数据元素；POS 入口模式将被设置为指示非接触式交易
3. 收单方将执行常规处理检查并将标记数据字段和非接触数据传递到支付网络
4. 支付网络将与标记服务提供商对接，标记服务提供商提供如下功能：
  - a. 检索 PAN。

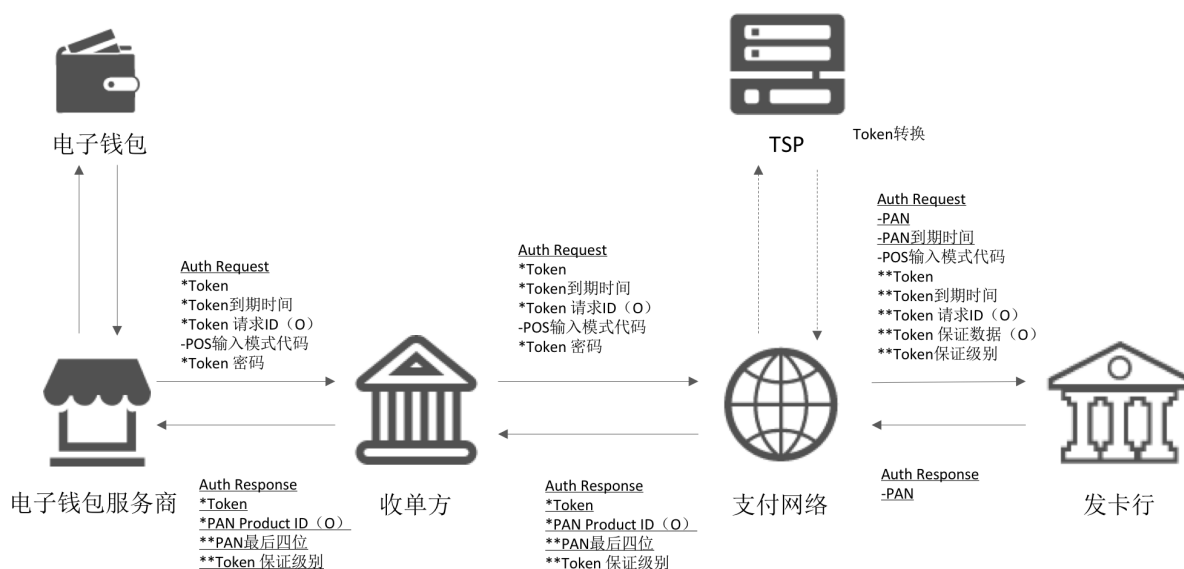
- b. 针对有效的付款标记和为该付款标记定义的其他控制，验证标记保险库中付款标记到 PAN 映射的状态
  - c. 验证标记密码并验证该付款标记的标记域限制控制（或者卡发行可以验证密文，如果它具有必要的密钥）。
  - d. 如果授权消息中未提供，检索标记请求者 ID。
5. 支付网络将授权请求发送到卡发行方，对授权请求消息进行以下改变：
- a. 将标记替换为付款 PAN
  - b. 将标记到期日替换为 PAN 到期日
  - c. 添加一个已验证标志，向发卡行传达验证已由标记服务提供商完成
  - d. 以下标记相关字段在授权请求中传递给发卡行：
    - a) 付款标记
    - b) 标记到期日期（可选）
    - c) 标记保证数据（可选）
    - d) 标记保证级别
    - e) 标记请求者 ID
    - f) POS 输入模式代码
6. 发卡行完成帐户级验证和授权检查，并将 PAN 的授权响应发送回支付网络
7. 支付网络（可能与标记服务提供商通信）可以生成响应密文，并且将基于映射关系，将 PAN 替换为标记，并且除了将授权响应的收单方要求的部分其他标准数据元素：
- a. 付款标记
  - b. 标记保证级别
  - c. PAN 的最后 4 位数
  - d. PAN 产品 ID（可选）
8. 收单方将授权响应传递给商家
9. 将通知消费者交易的成功或失败。

**【注】**

这个场景同样适用于使用标记加载联系人或使用非接触式芯片。这种付款标记将不同于在磁条卡上编码的 PAN

## 9.3 使用场景 2：移动数字钱包

此使用场景是指持卡人使用移动/数字钱包向电子商务网站支付以完成支付订单信息的情况。钱包可以由发卡银行，支付网络或第三方操作；数字钱包运营商将可能是标记请求者。在这种使用情况下，钱包操作者使用支付标记化，以便不再需要为了安全或其他商业理由而将 **PAN** 存储在钱包平台中。当持卡人在电子商务商家支付时，钱包将通过钱包 **API** 向商家传递代替 **PAN** 的支付标记以及附加的支付标记相关字段。商家将使用在 **PAN** 和 **PAN** 到期日期的现有字段内携带的付款标记和随附的标记到期日期启动授权。尽管需要执行去标记化和标记域限制控制，但还是可以使用支付网络的现有流程支持分期付款和定期付款，具体流程如下图：



以下步骤描述了当消费者使用移动设备中的商家应用或数字钱包发起电子商务交易以进行购买时授权消息中的标准支付标记数据字段的流程：

1. 移动设备中的商家应用/数字钱包将与支付应用交互并将以下关键的支付标记数据元素传递到商家平台
  - a. 付款标记将在现有 **PAN** 字段中传递。
  - b. 标记到期日将在 **PAN** 到期日字段中传递
  - c. 标记密码将基于付款标记数据元素生成，并将在标记密码字段中传递

- d. 标记请求者 ID 将作为可选字段传递。
- e. 所有其他必需的数据元素将被创建和传递。
- 2. 商户平台将授权请求传递给收单方，其携带所有标准的支付标记字段；POS 入口模式将被设置为指示电子商务交易
- 3. 收单方将对数据元素执行处理检查，并将付款标记数据字段传递到支付网络
- 4. 支付网络将与标记服务提供商对接，标记服务提供商提供如下功能：
  - a. 检索 PAN。
  - b. 针对有效的付款标记和为该付款标记定义的其他控制，验证标记保险库中付款标记到 PAN 映射的状态
  - c. 验证标记密码并验证该付款标记的标记域限制控制（或者卡发行可以验证密文，如果它具有必要的密钥）。
  - d. 如果授权消息中未提供，检索标记请求者 ID。
- 5. 支付网络将授权请求发送到卡发行方，对授权请求消息进行以下改变：
  - a. 将标记替换为付款 PAN
  - b. 将标记到期日替换为 PAN 到期日
  - c. 添加一个已验证标志，向发卡行传达验证已由标记服务提供商完成
  - d. 以下标记相关字段在授权请求中传递给发卡行：
    - a) 付款标记
    - b) 标记到期日期（可选）
    - c) 标记保证数据（可选）
    - d) 标记保证级别
    - e) 标记请求者 ID
    - f) POS 输入模式代码
- 6. 发卡行完成帐户级验证和授权检查，并将 PAN 的授权响应发送回支付网络
- 7. 支付网络（可能与标记服务提供商通信）可以生成响应密文，并且将基于映射关系，将 PAN 替换为标记，并且除了将授权响应发给收单方还包括其他标准数据元素：
  - a. 付款标记

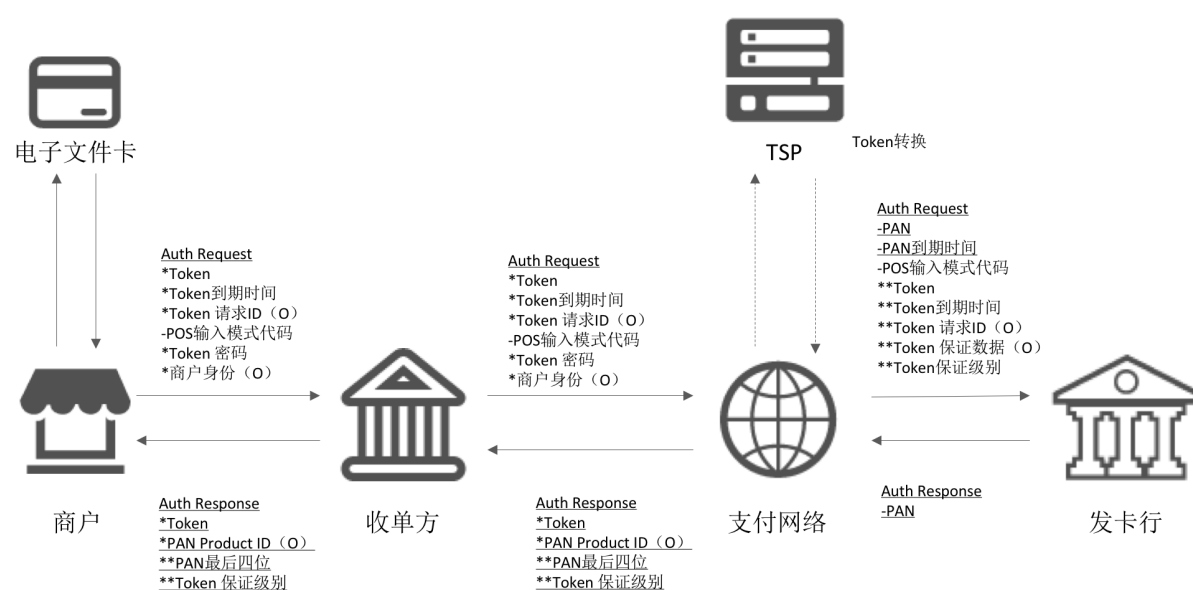


- b. 标记保证级别
  - c. PAN 的最后 4 位数
  - d. PAN 产品 ID（可选）
8. 收单方将授权响应传递给商家
  9. 将通知消费者交易的成功或失败。

## 9.4 使用场景 3：虚拟文件卡

他的使用案例指的是电子商务商户具有在数据库中存储的支付卡数据的情况，其试图通过用付款标记替换 PAN 来移除存储卡数据的潜在安全风险。在这种情况下，这些商家很可能是标记请求者。一旦付款标记返回到这些卡上文件商家，所有处理的后续电子商务交易将使用付款标记和标记到期日代替 PAN 和 PAN 到期日期字段。

具体流程如下图：



以下步骤解释当消费者使用文件卡发起电子商务购买时授权消息中的标准支付标记数据字段的流程。

1. 持卡人与文件中的商家进行电子商务购买。商户网站将以下关键付款标记数据元素传递到商户平台
  - a. 付款标记将在现有 PAN 字段中传递。
  - b. 标记到期日将在 PAN 到期日字段中传递

- c. 标记请求者 ID 将作为可选字段传递
- d. 标记密码将根据付款标记数据字段生成并传递（可选）
- e. 将创建并传递所有其他商户认证数据（可选）

**【注】**

标记请求者 ID 和相关的商家标识符将作为域限制控制字段，用于验证交易的完整性。

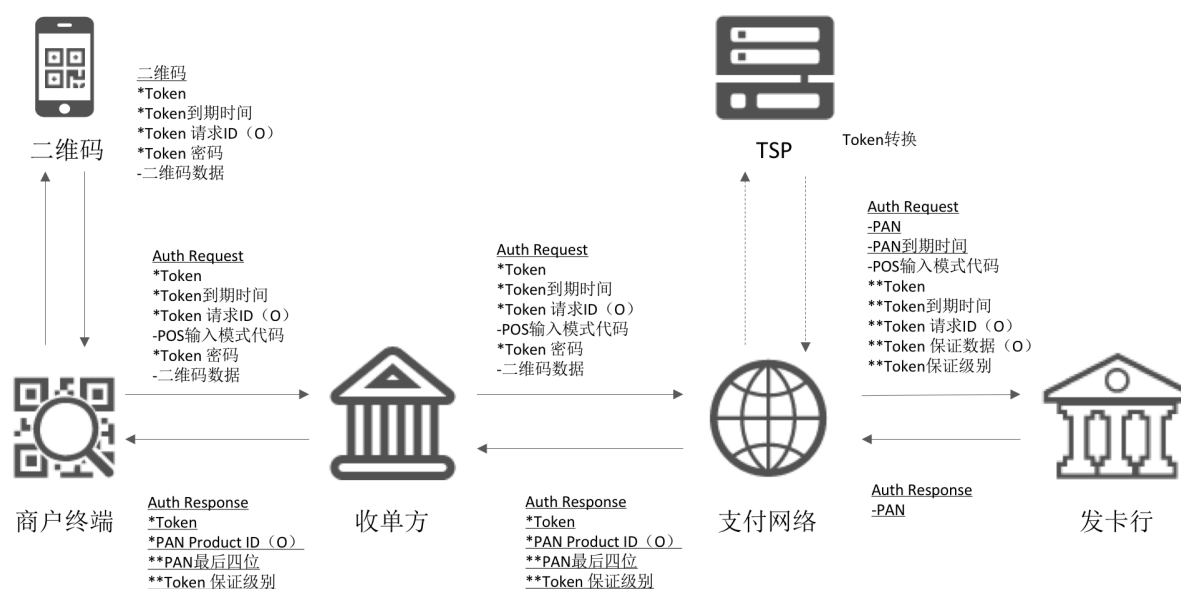
2. 商家平台将授权请求传递给收单方，其中包含所有标准的付款标记数据字段和任何所需的商家特定标识符
3. 收单方将对数据元素执行处理检查，并将包括标记密码的付款标记数据字段传递到支付网络。
4. 支付网络将与标记服务提供商对接，标记服务提供商提供如下功能：
  - a. 检索 PAN
  - b. 针对有效的付款标记和为该付款标记定义的其他控制，验证标记保险库中付款标记到 PAN 映射的状态
  - c. 验证标记密码，并验证该付款标记的标记域限制控制（或者卡发行商可以验证密钥具有必要的密钥）。
  - d. 如果授权消息中未提供，检索标记请求者 ID。
5. 付款网络将授权请求发送到发卡行，对授权请求消息进行以下改变：
  - a. 将标记替换为付款 PAN
  - b. 将标记到期日替换为 PAN 到期日
  - c. 添加一个已验证标志，向发卡行传达验证已由标记服务提供商完成
6. 以下标记相关字段在授权请求中传递给发卡行：
  - a. 付款标记
  - b. 标记到期日期（可选）
  - c. 标记保证数据（可选）
  - d. 标记保证级别
  - e. 标记请求者 ID
  - f. POS 输入模式代码
  - g. 发卡行完成帐户级验证和授权检查，并向支付网络发送授权响应。
7. 付款网络将基于映射用付款标记替换 PAN，并且除了其他标准数据元素之外，将以下字段传递到授权响应的收单行

8. 收单行将授权响应传递给商家
9. 将通知消费者交易的成功或失败

## 9.5 使用场景 4：扫码

这种场景是指使得移动设备能够在商家地点发起基于 QR 二维码的支付，其可以在销售点接受这种形式的支付。在该使用情况下，每当以安全方式发起支付时，移动设备中的应用生成动态 QR 码。当发起交易时，移动设备将生成包括支付标记，标记到期日期和标记密码元素以及来自 QR 码的任何其它数据的事务，并将其传递到商家的点对点终端。

具体流程如下图所示：



以下步骤描述当在销售点使用移动设备使用二维码来呈现付款标记时授权消息中的标准支付标记数据字段的流程

1. 移动设备将与能够读取 QR 码的商家终端交互，并将以下关键的支付标记数据元素传递到商家终端
  - a. 付款标记将在现有 PAN 字段中传递
  - b. 标记到期日将在 PAN 到期日字段中传递。
  - c. 可以基于支付标记数据元素生成标记密码。
  - d. 标记请求者 ID 将作为可选字段传递
  - e. 所有其他 QR 数据元素将被创建并传递到相应的事务数据字段中

## 【注】

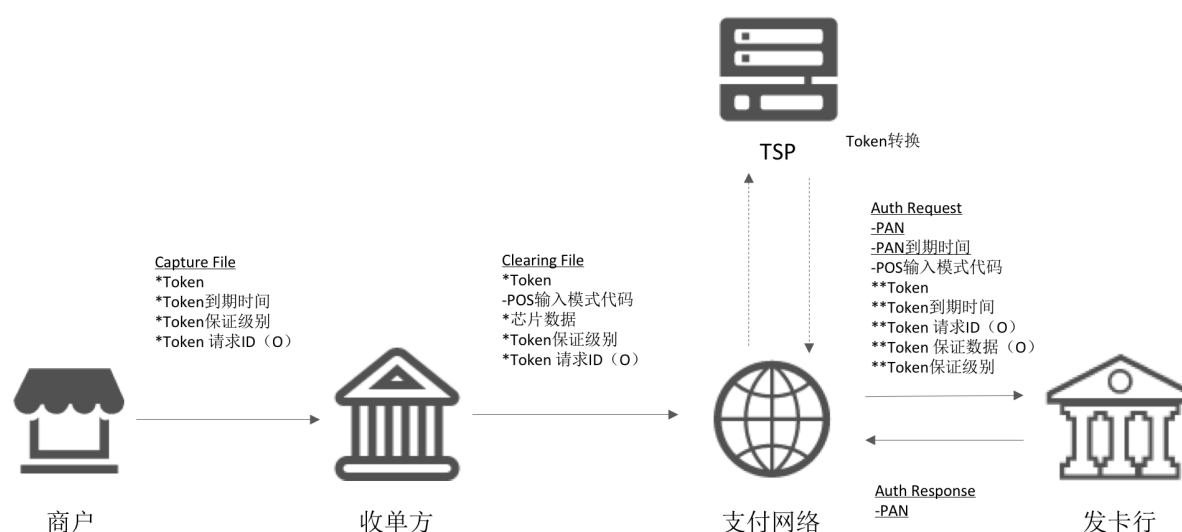
生成标记密码，并且在存在时将作为域限制控制字段使用，标记服务提供商程序将使用该字段来验证使用标记交易的完整性

2. 商家终端将授权请求传递给收单方，携带如上图所示的所有标准的支付标记字段; POS 入口模式将被设置为指示基于 QR 码的交易。
3. 收单方将执行标准处理检查，并将付款标记数据字段传递到支付网络。
4. 支付网络将与标记服务提供商对接，标记服务提供商提供如下功能：
  - a. 检索 PAN
  - b. 针对有效的付款标记和为该付款标记定义的其他控制，验证标记保险库中的付款标记到 PAN 映射的状态。
  - c. 验证标记密码并验证该付款标记的标记域限制控制（或者卡发行商可以验证密文，如果它具有必要的密钥）
  - d. 如果授权消息中未提供，请检索标记请求者 ID。
5. 支付网络将授权请求发送到卡发行方，对授权请求消息进行以下改变：  
支付网络将授权请求发送到卡发行方，对授权请求消息进行以下改变：
  - a. 将标记替换为付款 PAN
  - b. 将标记到期日替换为 PAN 到期日
  - c. 添加一个已验证标志，向发卡行传达验证已由标记服务提供商完成
  - d. 以下标记相关字段在授权请求中传递给发卡行：
    - a) 付款标记
    - b) 标记到期日期（可选）
    - c) 标记保证数据（可选）
    - d) 标记保证级别
    - e) 标记请求者 ID
    - f) POS 输入模式代码
6. 发卡行完成帐户级验证和授权检查，并将 PAN 的授权响应发送回支付网络
7. 支付网络（可能与标记服务提供商通信）可以生成响应密文，并且将基于映射关系，将 PAN 替换为标记，并且除了将授权响应的收单方其他标准数据元素：

- a. 付款标记
  - b. 标记保证级别
  - c. PAN 的最后 4 位数
  - d. PAN 产品 ID（可选）
8. Acquirer 将授权响应传递给商家
  9. 将通知消费者交易的成功或失败。

## 9.6 日终和清算流程

下图显示了付款标记交易的日终和清算过程。



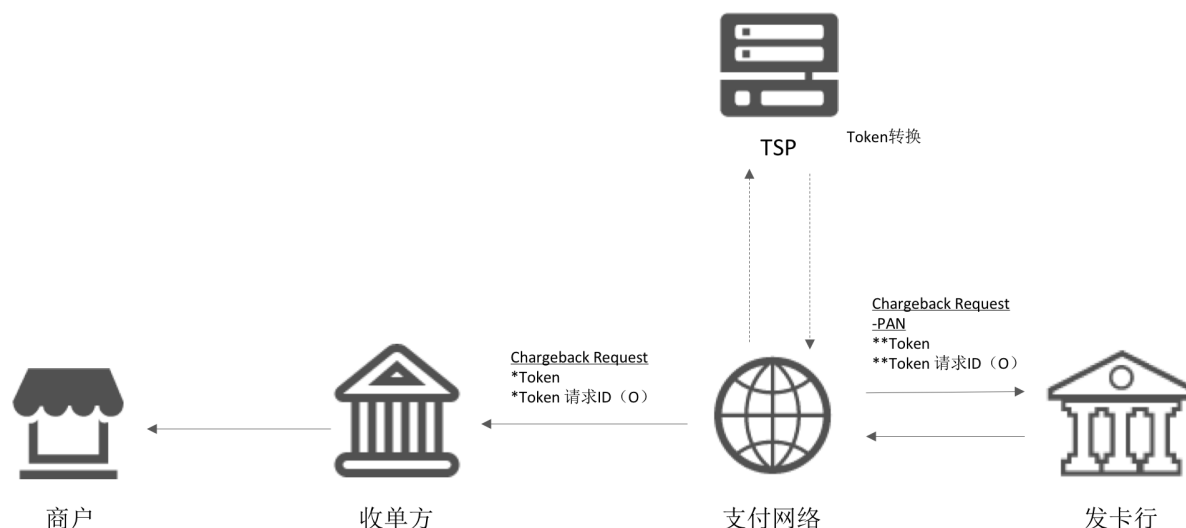
以下步骤描述作为交易生命周期一部分的日终和清算过程中的标准支付标记数据字段的流程

1. 用于日终文件处理的信息由获取者基于消费者在事务启动期间提供的信息创建，付款标记将在日终文件的现有 **PAN** 字段中传递，以及其他标准的付款标记数据元素，并发送给收单方。
2. 收单方将对数据元素执行处理检查，并将使用以下付款标记数据字段创建要发送到支付网络的清算文件：
  - a. 付款标记将在现有 **PAN** 字段中传递
  - b. POS 输入模式将被设置为通道特定交易的标准 POS 输入模式，并包括在清算文件中

- c. 标记保证级别将包括在结算文件中，并且将是用于支付标记交易的新数据字段
  - d. 标记请求 ID 将作为清算文件中的可选字段传递
- 3. 支付网络将与标记服务提供商对接，并提供如下服务：
  - a. 检索 PAN
  - b. 针对有效的付款标记和为该付款标记定义的其他控制，验证标记保险库中付款标记到 PAN 映射的状态
  - c. 验证付款标记的标记域限制控制
- 4. 支付网络将清算文件发送给发卡银行，并提供以下信息：
  - a. 用 PAN 替换付款标记
  - b. 添加一个指示符，向发卡行传达代表验证已由付款标记的标记服务提供商完成
  - c. 在清算文件中传递以下与付款标记相关的字段。这些是可选地发送到清算文件中的发卡行的新字段：
    - a) 付款标记
    - b) 标记 Exp。日期（可选）
    - c) 标记请求 ID
    - d) 标记保证级别
- 5. 发卡行对清算文件执行验证并完成清算过程

## 9.7 异常处理流程

下图显示退款请求标记处理流程



如下的步骤描述了在交易生命周期的异常处理过程中标准支付标记数据字段的处理流程。

1. 发卡行通常在确认原始交易是有效的退款，并且发卡机构具有适当的退款权利之后提出退款申请
2. 发卡行生成用于退款的文件，并提供以下付款标记数据字段，以创建要发送到付款网络的退款记录
  - a) 在原始购买交易中使用的 **PAN**
  - b) 付款标记将是提供的退款记录中引入的新数据元素
  - c) 标记请求者 ID 将可选地由卡发行方传递
3. 支付网络将与标记服务提供商对接，并提供如下服务：
  - a) 检索 **PAN**
  - b) 针对有效的付款标记和为该付款标记定义的其他控制，验证标记保险库中付款标记到 **PAN** 映射的状态
  - c) 如果付款标记不是发卡行发出，检索有争议的交易付款标记发送给收单方
4. 将退款记录发送给收单方，包含以下信息：
  - a. 使用付款标记替换 **PAN**
  - b. 标记请求者 ID 将作为可选字段传递
5. 收单方对退款记录执行验证，并根据实际情况进行调查，转到争议处理的另一个阶段或解决退款