

CyberSource 3DS 验证

使用 Simple Order API

2019 年 8 月



CyberSource 联系信息

有关我们的公司、产品和服务的概要信息，请访问 <http://www.cybersource.com>。

有关 CyberSource 服务的销售问题，请向 sales@cybersource.com 发送电子邮件或拨打 650-432-7350 或 888-330-2300（美国境内免费）。

有关任何 CyberSource 服务的支持信息，请访问支持中心，网址为 <http://www.cybersource.com/support>。

版权

© 2019 CyberSource Corporation。保留所有权利。CyberSource Corporation（简称“CyberSource”）根据本文档的读者（简称“您”）与 CyberSource 之间签订的适用协议（简称“协议”）提供本文档和本文档中所述的软件。您必须遵守协议中的条款来使用本文档和/或软件。除非协议有明确规定，否则本文档中包含的信息会在不事先通知的情况下发生变更，因此本文档中的信息在任何情况下均不应视为 CyberSource 作出的保证或担保。CyberSource 对本文档中可能出现的任何错误不承担任何责任。您必须严格遵照本协议来使用随本文档一起提供的受版权保护的软件。您在使用软件之前应认真阅读协议。除非协议允许，否则在未获得 CyberSource 事先书面同意的情况下，您不得复制本文档的任何内容、将本文档存储在检索系统中，或者以任何形式或任何方法（电子、机械、录制或其他方式）传输此文档。

受限权利标识

对于政府或国防部门：政府或国防部门的使用、复制或披露行为必须遵守 DFARS 252.227-7013 “技术数据和计算机软件中的权利”条款以及 FAR 和 NASA FAR 补充条款中类似条款的限制。

对于民间机构：使用、复制或披露必须遵守 52.227-19 “商用计算机软件受限权利”条款 (a) 到 (d) 项规定的限制，以及 CyberSource Corporation 关于此软件的标准商业协议中规定的限制。根据美国版权法的规定保留未公布的权利。

商标

Authorize.Net、eCheck.Net 和 The Power of Payment 是 CyberSource Corporation 的注册商标。

CyberSource、CyberSource Payment Manager、CyberSource Risk Manager、CyberSource Decision Manager 和 CyberSource Connect 是 CyberSource Corporation 的商标和/或服务标志。

所有其他品牌和产品名称都是其各自所有者的商标或注册商标。

As-Is Disclaimer

Case studies, comparisons, statistics, research and recommendations are provided 'AS IS' and intended for informational purposes only and should not be relied upon for operational, marketing, legal technical tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

免责声明

案例研究、对比数据、统计数据、研究和建议事项均依照“原样”呈现，仅供参考之用，不得用于经营、营销、法律、技术、税务、财务或其他领域。Visa 既不对本文件中信息的完整性或准确性作出任何保证或陈述，也不对因依赖此类信息而可能导致的任何后果承担任何责任。本文所含信息并非作为投资或法律建议，鼓励读者在需要此类建议时征求合格专业人士的意见。

目录

本文档的近期修订	7
关于本指南	9
受众和用途	9
内容范围	9
约定	10
备注、重要说明和警告声明	10
文本和命令约定	10
相关文档	11
客户支持	11

章节 1	3DS 验证简介	12
	拒付保护概述	12
	PSD2	13
	3D Secure 2.x	13
	实施 3DS 验证的前提条件	13
	将 3DS 验证集成到您的业务中	14
	实施 3D Secure 2.x	15
	场景 1: 新商户	15
	场景 2 目前在使用 CyberSource Simple Order API 和针对 3D Secure 1.0 的 3DS 验证服务	16
	场景 3: 使用针对手机应用的 SDK 进行集成	17
	使用 Secure Acceptance 进行 3DS 验证	18
	3DS 验证流程	18
	混合集成流程	18
	标准集成流程	19
	SDK 集成流程	20
	所需商户信息	21

章节 2	实施混合 3DS 验证	22
	流程概述	22
	开始之前	23
	凭据 /API 密钥	23

	创建 JWT	23
	添加 JavaScript	23
	BIN 检测	23
	实施混合 3DS 验证	24
	请求注册检查服务（混合）	24
	回复说明	25
	验证注册银行卡	26
	接收验证结果	27
	请求检验服务	27
	回复说明	28
	向消费者展示成功或失败消息页面	29
章节 3	实施标准 3DS 验证	30
	流程概述	30
	开始之前	31
	凭据 /API 密钥	31
	创建 JWT	31
	添加 JavaScript	31
	BIN 检测	31
	实施标准 3DS 验证	32
	开始验证	32
	向消费者展示成功或失败消息页面	33
	请求注册检查服务（标准）	34
章节 4	升级 3DS 验证服务	36
	升级至 3D Secure 2.x	36
	优势	36
	PSD2 影响	37
	强制性要求	37
	时间表	37
	建议集成方法	37
	配置要求	38
	混合集成调用 CyberSource API	39
	配置网站	41
	显示验证窗口	41
	使用 CardinalCommerce JavaScript	41
	测试	43
	迁移 FAQ	44
章节 5	测试 3DS 验证服务	46
	测试流程	46
	注册检查	46

验证检验	47
预期结果	48
3D Secure 1.0 的测试案例	50
Visa Secure	50
Mastercard Identity Check	59
Maestro	67
American Express SafeKey	71
JCB J/Secure	76
Diners Club ProtectBuy	81
Discover ProtectBuy	86
3D Secure 2.x 的测试案例	91
Visa Secure	91
Mastercard Identity Check	98
American Express SafeKey	105
Discover ProtectBuy	112

附录 A	API 字段	119
	格式限制	119
	数据类型定义	119
	编号元素	120
	请求字段	121
	响应字段	134

附录 B	原因代码	142
------	------	-----

附录 C	请求和回复示例	143
	标准集成示例	143
	注册检查请求示例	143
	注册检查回复示例	144
	混合集成示例	145
	注册检查请求示例	145
	注册检查回复示例	146
	验证检验请求示例	147
	验证检验回复示例	148

附录 D	网站修改参考	149
	网站修改步骤	149
	3D Secure 服务徽标	150
	通知消息示例	151

附录 E Business Center 中 3DS 验证交易的详细信息 152

搜索 3DS 验证详细信息	152
已注册的卡	152
注册检查	152
验证检验	155
卡未注册	155
3DS 验证详细信息	155
交易详细信息	157
3DS 验证搜索	157
存储 3DS 验证数据	158

附录 F 3DS 验证报告 159
3DS 验证汇总报告 159
下载报告 160
将报告与交易搜索结果匹配 162
解读报告 162
比较 3DS 验证和支付报告 163
3DS 验证明细报告 164
报告 164
<Result> 164
<PayerAuthDetail> 165
<ProofXML> 167
<VEReq> 168
<VERes> 169
<PAREq> 169
<PAREs> 171
<AuthInfo> 172
示例 174
失败的注册检查 174
验证成功 175

附录 G 基于规则的 3DS 验证 176
可用规则 176
API 回复 177
绕过验证的交易 177
基于风险的银行交易 178
 词汇表 179
 索引 185

本文档的近期修订

发布	变更
2019 年 8 月	为 SDK 集成添加了 3DS 验证高级流程说明。请参阅第 18 页， “3DS 验证流程” 。
2019 年 7 月	■ 添加了 Cardinal Cruise Direct Connection API 集成选项。请参阅“将 3DS 验证集成到您的业务中” ■ 将 <i>Mastercard SecureCode</i> 的名称改为 <i>Mastercard Identity Check</i>。
2019 年 5 月	■ 更新了指南内容，注明“如果分别请求 3DS 验证和银行卡授权服务，则必须在授权请求中包含 3D Secure 版本和目录服务器交易 ID 字段”。请参阅“3DS 验证流程”、第 2 章，实施混合 3DS 验证和第 3 章，实施标准 3DS 验证。 ■ 将 <i>Verified by Visa</i> 的名称改为 <i>Visa Secure</i>。 ■ 为新 Business Center 更新了附录 E，Business Center 中 3DS 验证交易的详细信息。
2019 年 4 月	■ 更新了简介章节，加入 PSD2 信息、不同场景的实施步骤以及使用 Secure Acceptance 进行 3DS 验证的详细信息。请参阅第 12 页，第 1 章，“3DS 验证简介”。 ■ 为 3D Secure 2.x 添加了必填字段列表。请参阅第 24 页，“请求注册检查服务（混合）”以及第 34 页，“请求注册检查服务（标准）”。 ■ 更新了第 91 页，“3D Secure 2.x 的测试案例”。 ■ 为 3D Secure 2.x 更新了必填和可选 API 字段。请参阅第 119 页，附录 A，“API 字段”。 ■ 更新了以下请求字段： • payerAuthEnrollService_challengeCode • payerAuthEnrollService_fraudActivity • payerAuthEnrollService_messageCategory • payerAuthEnrollService_preorder • payerAuthEnrollService_reorder ■ 添加了以下回复字段： • payerAuthEnrollReply_challengeRequired • payerAuthEnrollReply_directoryServer 交易 ID • payerAuthValidateReply_directoryServer 交易 ID

发布	变更
2019 年 3 月	■ 为测试案例 22: Mastercard Identity Check 注册卡: 验证不可用更新了电子商务交易指示符, 从 spa 变为 internet。 ■ 更新了测试案例 55: JCB J/Secure 未注册银行卡, 以移除责任转移部分。 ■ 更新了 2.x 测试案例的说明, 注明这些案例可用于混合集成或标准集成场景。请参阅第 91 页, 第 5 章, “3D Secure 2.x 的测试案例”。 ■ 移除了以下旧请求字段: • deviceFingerprintData_#_data • deviceFingerprintData_#_provider • payerAuthEnrollService_challengeRequired
2018 年 12 月	■ 为混合集成添加了 3DS 验证高级流程说明。请参阅第 18 页, “3DS 验证流程”。 ■ 将以前的集成章节分为混合集成和标准集成两部分。请参阅第 22 页, 第 2 章, “实施混合 3DS 验证”以及第 30 页, 第 3 章, “实施标准 3DS 验证”。 ■ 为目前使用 3DS 验证的商户添加了一个实施章节。请参阅第 36 页, 第 4 章, “升级 3DS 验证服务”。 ■ 更新了第 159 页, “3DS 验证汇总报告”, 为 New Business Center 提供报告下载的相关说明。

关于本指南

受众和用途

本指南面向想要使用 **CyberSource Simple Order API** 将 **3DS** 验证服务集成到订单管理系统中的应用程序开发人员。介绍完成此集成需要执行的任务。

实施 **CyberSource 3DS** 验证服务需要具备软件开发技能。您需要编写相应的程序，使用 **API** 请求和回复字段将 **3DS** 验证服务集成到您现有的订单管理系统中。

内容范围

本指南介绍如何使用 **Simple Order API** 将 **3DS** 验证服务与您的订单管理系统集成。不涉及 **Simple Order API** 的基本使用以及如何使用 **3DS** 验证以外的 **CyberSource** 服务。有关详细信息，请参阅[第 11 页](#)，“[相关文档](#)”。

约定

备注、重要说明和警告声明



备注 包含有用建议或本文档中未包含材料的参考信息。



重要说明 包含关于成功完成某项任务或学习某个概念的重要信息。



警告 包含如果不加以留意，可能导致安全风险、不可挽回的数据丢失，或者时间和/或收入巨大损失的信息或说明。

文本和命令约定

约定	用途
加粗	■ 文本中的字段和服务名称。例如： 包含 ics_applications 字段。 ■ 要求您执行的项目。例如： 单击保存。
斜体	■ 文件名和路径名。例如： 将筛选条件定义和映射添加至您的 <i>web.xml</i> 文件。 ■ 由您提供特定值的占位符变量。
屏幕文本	■ XML 元素。 ■ 代码示例。 ■ 在 API 环境中输入的文本。例如： ■ 将 davService_run 字段设置为 <code>true</code>。

相关文档

- *CyberSource Advanced for the Simple Order API 入门介绍* Simple Order API 的基本使用。(PDF | HTML)
- *使用 Simple Order API 的 Decision Manager 开发人员指南* 介绍如何将 Decision Manager（一种欺诈检测服务）与您的订单管理系统集成。(PDF | HTML)
- *使用 Simple Order API 的信用卡服务* 介绍如何将 CyberSource 支付处理服务集成到您的业务中。(PDF | HTML)
- *Secure Acceptance 托管结账工具集成指南* 介绍如何创建 Secure Acceptance 配置文件，将您的订单管理系统与 Secure Acceptance 网络/移动支付结账服务集成。(PDF | HTML)
- *Secure Acceptance 结账 API 集成指南* 介绍如何创建 Secure Acceptance 配置文件，将您的订单管理系统与网站集成来处理交易。(PDF | HTML)
- *报告开发人员指南* 介绍如何查看和配置 Business Center 报告。(PDF | HTML)
- [CyberSource API 版本页面](#) 提供有关 CyberSource API 版本的信息。

有关完整的 CyberSource 技术文档，请参阅支持中心：

http://www.cybersource.com/support_center/support_documentation

客户支持

有关任何 CyberSource 服务的支持信息，请访问支持中心：

<http://www.cybersource.com/support>

3DS 验证简介

CyberSource 3DS 验证服务使用 JavaScript 和 ICS 服务来提供验证。

借助 3DS 验证服务，您可为网店添加各种银行卡验证服务，包括 Visa SecureSM、Mastercard Identity Check[®]、Maestro[®] (UK Domestic and international)、American Express SafeKeySM、JCB J/SecureTM、Diners Club ProtectBuy 和 Discover ProtectBuy。

这些银行卡验证服务可防止卡的未授权使用，保护您避免被称为 *责任转移* 的欺诈性拒付活动。但是，CyberSource 3DS 验证并非欺诈管理服务，例如具备高级欺诈扫描功能的 Decision Manager。CyberSource 建议您在实施 3DS 验证服务外，还要制定全面的欺诈管理计划。

您可以对特定支付处理机构使用 3DS 验证服务。要了解支付处理机构是否支持此功能，请参阅 *使用 Simple Order API 的信用卡服务* ([PDF](#) | [HTML](#)) 中的“3DS 验证”部分。

拒付保护概述

如果商户加入 [3D Secure](#) 银行卡验证计划（例如 Visa Secure 或 Mastercard Identity Check），Visa、Mastercard、Maestro、American Express、JCB、Diners Club 和 Discover 会提供拒付保护。

拒付在交易处理后发生，拒付的处理方式取决于卡的发行地区。支付卡公司的规则可能随时间变化，并因地理区域而异。CyberSource 建议您联系商户账户提供商，了解拒付要求的准确解释以及提供哪些拒付保护。

PSD2

PSD2（支付服务指令 2）是欧洲新建的监管框架，用于控制支付处理以及消费者的安全和验证流程。PSD2 为欧洲经济区 (EEA) 打造了一个单一支付市场（包括英国，即使其不属于 EEA 的范畴），以提高支付服务的安全性和创新性。根据 PSD2 的强制性要求，所有电子支付交易均需实施强客户身份认证 (SCA)。这一要求将对商户收款和消费者验证身份的方式产生影响。PSD2 规定所有电子支付交易均需采用双因素验证技术。

3D Secure 2.x

3D Secure 2.x 是一种验证工具，由支持 SCA 的银行卡网络提供。为遵循 SCA 要求，商户必须在结账页面部署 3D Secure 2.x 或使用合规的托管结账方式。

升级至 3D Secure 2.x 之后，可传递附加数据并自动发送给发卡行。CyberSource 3DS 验证服务可向后兼容 3D Secure 1.0。

实施 3DS 验证的前提条件

要使用 3DS 验证服务，您和您的开发人员必须能够完成以下任务：

- 编写代码与发卡行建立连接。
- 在网站上添加验证服务所需的 JavaScript 工具。
- 将特定数据添加到发往 CyberSource 的 API 请求中。
- 检验必要数据。
- 为授权请求提供额外数据。
- 修改网站以帮助消费者理解流程。

将 3DS 验证集成到您的业务中

无论您现在是 3D Secure 1.0 用户，还是初次接触 3DS 验证，都可以在现有业务流程中集成 3DS 验证服务。

提供四类集成方式：

- 混合集成
- 标准集成
- 针对手机应用的 SDK 集成
- Cardinal Cruise Direct Connection API

有关 Cardinal Cruise Direct Connection API 的更多信息，请参阅 [JavaScript 文档](#)。如有任何疑问，请直接联系 CardinalCommerce 客户支持部门。



如果您使用了简码化功能，就必须采用混合集成方法。

SDK 集成仅适用于采用 3D Secure 2.x 技术的交易。

您也可以通过 Secure Acceptance 启动 3D Secure 2.x 来提供 3DS 验证服务。有关详细信息，请参阅“[使用 Secure Acceptance 进行 3DS 验证](#)”。

本手册的前几个章节分别概述了标准集成和混合集成的 3DS 验证流程。有关详细信息，请参阅：

- [第 22 页，第 2 章，“实施混合 3DS 验证”](#)
- [第 30 页，第 3 章，“实施标准 3DS 验证”](#)

对于目前使用 3D Secure 1.0 的商户，请参阅：

- [第 36 页，第 4 章，“升级 3DS 验证服务”](#)

实施 3D Secure 2.x

本节主要描述不同场景的实施步骤。

场景 1：新商户

-
- 步骤 1** 联系 CyberSource 业务经理或销售经理，了解有关 3D Secure 2.x 和 PSD2 的详细信息。
- 步骤 2** 设置 CyberSource 的商户 ID。
- a** 联系客户支持部门，根据需要为选定的银行卡类型、币种和收单行启用 3D Secure 2.x。有关详细信息，请参阅“[所需商户信息](#)”。
 - 如需处理使用 Secure Acceptance 的支付交易，您必须在此时提出请求；当然，您也可以请求令牌管理等其他服务。
 - b** 登入 Business Center，获取实施服务所需的 API 密钥。
- 步骤 3** 实施 3D Secure 2.x。
- 使用 CyberSource Simple Order API:
 - a** 在结账页面中添加 CardinalCommerce JavaScript 代码。
 - b** 为请求注册检查和验证检验服务，进行相应的系统配置。在请求中加入 API 必填字段，也可根据业务需求考虑添加可选字段。
 - 如需详细信息，请参阅“[3DS 验证流程](#)”、第 22 页，第 2 章，“[实施混合 3DS 验证](#)”或第 30 页，第 3 章，“[实施标准 3DS 验证](#)”。
 - 您可以对系统进行配置，请求通过 CyberSource 提供支付服务并借助 3D Secure 2.x 执行 3DS 验证（这不是强制性要求）。
- 步骤 4** 测试 3D Secure 2.x 服务。
- 此测试可帮助您熟悉可能出现的服务使用案例。
- 请参阅第 46 页，第 5 章，“[测试 3DS 验证服务](#)”，并运行“[3D Secure 2.x 的测试案例](#)”中的测试案例
- 步骤 5** 配置适用于生产环境的账户。
- a** 向客户支持部门索取一份涉及支付处理机构或收单行的上线表。
 - b** 在上线表中填入必要的信息，包括 CyberSource 商户 ID、收单行商户 ID 以及针对所有选定银行卡类型的 BIN 信息。有关详细信息，请参阅“[所需商户信息](#)”。
-

场景 2: 目前在使用 CyberSource Simple Order API 和针对 3D Secure 1.0 的 3DS 验证服务

-
- 步骤 1** 联系 CyberSource 业务经理、销售经理或技术客服，了解有关 3D Secure 2.x 和 PSD2 的详细信息。
- 步骤 2** 配置 CyberSource 的测试商户 ID。
- a** 联系客户支持部门进行必要的配置调整，根据需要为选定的银行卡类型和币种启用 3D Secure 2.x。
 - b** 登入 Business Center，获取实施服务所需的 API 密钥。
- 步骤 3** 迁移至混合集成平台，实施 3D Secure 2.x。
- a** 在结账页面中添加 CardinalCommerce JavaScript 代码。
 - b** 为请求注册检查和验证检验服务，进行相应的系统配置。在请求中加入 API 必填字段，也可根据业务需求考虑添加可选字段。
- 有关详细信息，请参阅第 36 页，第 4 章，“升级 3DS 验证服务”。
- 您可以对系统进行配置，请求通过 CyberSource 提供支付服务并借助 3D Secure 2.x 执行 3DS 验证（这不是强制性要求）。
- 步骤 4** 测试 3D Secure 2.x 服务。
- 此测试可帮助您熟悉可能出现的服务使用案例。
- 请参阅第 46 页，第 5 章，“测试 3DS 验证服务”，并运行“3D Secure 2.x 的测试案例”中的测试案例。
- 步骤 5** 配置适用于生产环境的账户。针对生产环境，重复第 2 步至第 4 步。
-

场景 3：使用针对手机应用的 SDK 进行集成

- 步骤 1** 联系 CyberSource 业务经理、销售经理或技术客服，了解有关 3D Secure 2.x 和 PSD2 的详细信息。
- 步骤 2** 配置 CyberSource 的测试商户 ID。
- a** 联系客户支持部门进行必要的配置调整，根据需要为选定的银行卡类型和币种启用 3D Secure 2.x。有关详细信息，请参阅“[所需商户信息](#)”。
 - b** 登入 Business Center，获取实施服务所需的 API 密钥。
- 步骤 3** 实施 3D Secure 2.x。
- 实施原生手机应用时，需要使用 CyberSource Simple Order API 以及 SDK。目前提供针对 iOS 或 Android 的 SDK。
- a** 实施 SDK 的目的是在原生应用中处理验证流程。这些 SDK 专门针对手机应用设计，作用相当于 CardinalCommerce JavaScript。
有关详细信息，请参阅：
 - [JavaScript 文档（针对 iOS SDK）](#)
 - [JavaScript 文档（针对 Android SDK）](#)
 - b** 为请求注册检查和验证检验服务，进行相应的系统配置。在请求中加入 API 必填字段，也可根据业务需求考虑添加可选字段。
如需详细信息，请参阅“[3DS 验证流程](#)”、第 22 页，第 2 章，“[实施混合 3DS 验证](#)”或第 30 页，第 3 章，“[实施标准 3DS 验证](#)”。
您可以对系统进行配置，请求通过 CyberSource 提供支付服务并借助 3D Secure 2.x 执行 3DS 验证（这不是强制性要求）。
- 步骤 4** 测试 3D Secure 2.x 服务。
- 此测试可帮助您熟悉可能出现的服务使用案例。
- 请参阅第 46 页，第 5 章，“[测试 3DS 验证服务](#)”，并运行“[3D Secure 2.x 的测试案例](#)”中的测试案例。
- 步骤 5** 配置适用于生产环境的账户。针对生产环境，重复第 2 步至第 4 步。
-

使用 Secure Acceptance 进行 3DS 验证

通过 Secure Acceptance 也可启动 3D Secure 2.x 来提供 3DS 验证服务。在 Business Center 的 Secure Acceptance 个人资料中选择相应的选项，即可升级。

如需进一步了解如何实施 Secure Acceptance 来进行 3DS 验证，请参阅 *Secure Acceptance 托管结账工具集成指南* 或 *Secure Acceptance 结账 API 集成指南*。

3DS 验证流程

本节主要描述适用于混合集成、标准集成和 SDK 集成的 3DS 验证流程。

混合集成流程

- 1 生成一个 JWT（JSON Web Token）。
- 2 在结账页面中添加 JavaScript 标签。
- 3 调用 *Cardinal.setup()*。
- 4 运行 BIN 检测。如果 BIN 符合 3D Secure 2.x 的要求，其将收集发卡行所需的 Method URL JavaScript 来采集其他设备数据。
- 5 请求注册检查服务，传递交易详细信息和 **payerAuthEnrollService_referenceID** 请求字段。
- 6 如果发卡行没有验证要求，注册检查回复将包含以下信息：
 - 电子商务交易指示符
 - CAVV（除 Mastercard 以外的所有银行卡类型）
 - AAV（仅限 Mastercard）
 - 交易 ID (XID)
 - 3D Secure 版本
 - 目录服务器交易 ID
- 7 如果发卡行有验证要求，回复将包含发卡行的 ACS URL、有效载荷以及调用 *Cardinal.continue* JavaScript 时加入的交易 ID。
- 8 JavaScript 显示验证窗口，消费者输入验证信息。
- 9 银行验证消费者的凭据并返回 JWT，要求商户在服务器端进行安全验证。
- 10 请求验证检验服务，从 JWT 中提取支付处理机构交易 ID 值，并将其放入 **payerAuthValidateService_authenticationTransactionID** 请求字段发送出去。回复中包含电子商务交易指示符、CAVV/AAV、交易 ID (XID)、3D Secure 版本以及目录服务器交易 ID。

确认验证成功之后，继续处理订单。

您必须在授权请求中传递银行卡类型和支付处理机构的所有相关数据。如需详细信息，请参阅第 27 页，“请求检验服务”。

标准集成流程

- 1 生成一个 JWT（JSON Web Token）。
- 2 在结账页面中添加 JavaScript 标签。
- 3 调用 *Cardinal.setup()*。
- 4 运行 BIN 检测。如果 BIN 符合 3D Secure 2.x 的要求，其将收集发卡行所需的 Method URL JavaScript 来采集其他设备数据。
- 5 当消费者在网站上下单时，调用 *cardinal.start* 函数来传递交易级数据，包括完整的 PAN 和订单明细。
- 6 JavaScript 通过服务器到服务器的调用向银行求证消费者的卡是否已在 3D Secure 银行卡验证计划中注册。
- 7 如果发卡行要求验证，JavaScript 将显示验证窗口。
- 8 如有必要，请消费者输入验证信息。
- 9 银行验证消费者的凭据并返回 JWT，要求商户在服务器端进行安全验证。
- 10 请求 ICS 注册检查服务，从 JWT 中提取支付处理机构交易 ID 值，并将其放入 **payerAuthEnrollService_authenticationTransactionID** 请求字段发送出去。回复包含以下信息：
 - 电子商务交易指示符
 - CAVV（除 Mastercard 以外的所有银行卡类型）
 - AAV（仅限 Mastercard）
 - 交易 ID (XID)
 - 3D Secure 版本
 - 目录服务器交易 ID

确认验证成功之后，继续处理订单。

您必须在授权请求中传递银行卡类型和支付处理机构的所有相关数据。如需详细信息，请参阅第 34 页，“请求注册检查服务（标准）”。

SDK 集成流程

- 1 生成一个 JWT（JSON Web Token）。
- 2 联系 CardinalCommerce 客户支持部门，了解注册获取 API 密钥的相关说明。
- 3 下载并导入针对 iOS 或 Android 的 Cardinal Mobile SDK。
- 4 设置构建环境。
- 5 配置 SDK。
- 6 调用 *Cardinal session.setup()*。
- 7 为商户服务器创建 API 调用以请求注册检查服务，传递交易详细信息和 **payerAuthEnrollService_referenceID** 请求字段。
- 8 如果发卡行没有验证要求，注册检查回复将包含以下信息：
 - 电子商务交易指示符
 - CAVV（除 Mastercard 以外的所有银行卡类型）
 - AAV（仅限 Mastercard）
 - 交易 ID (XID)
 - 3D Secure 版本
 - 目录服务器交易 ID
- 9 如果发卡行有验证要求，回复将包含有效载荷和从 SDK 调用 *Cardinal.continue* 时加入的交易 ID。
- 10 Cardinal Mobile SDK 显示验证窗口，消费者输入验证信息。
- 11 银行验证消费者的凭据并由 SDK 通过 *onValidated* 回调返回 JWT，要求商户在服务器端进行安全验证。
- 12 为商户服务器创建 API 调用以请求验证检验服务，从 JWT 中提取支付处理机构交易 ID 值，并将其放入 **payerAuthValidateService_authenticationTransactionID** 请求字段发送出去。回复中包含电子商务交易指示符、CAVV/AAV、交易 ID (XID)、3D Secure 版本以及目录服务器交易 ID。

确认验证成功之后，继续处理订单。

您必须在授权请求中传递银行卡类型和支付处理机构的所有相关数据。如需详细信息，请参阅第 27 页，“请求检验服务”。

所需商户信息

在生产中使用 CyberSource 3DS 验证之前，您必须与 CyberSource 客户支持部门联系，提供您公司和收单行的相关信息，以便 CyberSource 配置您的账户来实施这些服务。

您必须为 CyberSource 提供表 1 中列出的信息，然后才能启用 3DS 验证服务：

表 1 3DS 验证服务所需的商户信息

信息	说明
关于您的公司	■ 您的 CyberSource 商户 ID。 ■ 公司网站的 URL，例如： http://www.example.com ■ 您所在国家/地区的两字符 ISO 代码。 ■ 3D Secure 请求者 ID ■ 3D Secure 请求者名称 ■ 商户类别代码
银行信息	■ 收单行的名称。 ■ 银行联系人的全名和地址，包括电子邮箱地址。
Visa、Mastercard、Maestro、American Express、JCB、Diners Club 和 Discover 信息	收单行提供的您所配置的每个支付卡公司的相关信息： ■ 6 位 BIN 编号。
收单行商户 ID	■ 收单行商户 ID：收单行分配的商户 ID。 ■ 您能够处理的所有货币。

实施混合 3DS 验证

本章主要概述将混合 3DS 验证服务集成到现有业务流程中的过程。CyberSource 3DS 验证服务通过 CardinalCommerce JavaScript 来执行验证。访问本章包含的 JavaScript 文档链接可跳转至 Cardinal 网站。

流程概述

通知 CyberSource 客户代表您想要实施 3DS 验证 (3D Secure)。为其提供测试时需要使用的 CyberSource 商户 ID。如需详细信息，请参阅第 21 页，“所需商户信息”。

实施任务包括：

- 在结账页面中添加 JavaScript 代码。
- 针对每个购物请求
 - 构建验证请求
 - 调用 **payerAuthEnrollService**：3DS 验证注册检查服务
 - 调用验证
 - 处理拒绝事件
 - 调用以下服务：
 - **payerAuthValidateService**：3DS 验证检验（仅适用于混合集成）
 - **ccAuthService**：银行卡授权服务
- 使用第 46 页，第 5 章，“测试 3DS 验证服务”中的测试案例测试初始代码，并进行适当调整。在 JavaScript 代码中更改 URL 即可切换至测试环境。
- 确定账户已根据生产环境的要求进行配置。

开始之前

实施 3DS 验证服务之前，您的业务团队必须联系收单行和 CyberSource 设置服务。您的软件开发团队应熟悉此服务的 API 字段和技术详细信息。

凭据/API 密钥

实施时，需要 API 密钥来创建 JWT（JSON Web Token）。如需更多信息，请联系 CyberSource 客户支持部门。

创建 JWT

标准集成和混合集成都会使用 JWT（JSON Web Token）验证方法。要完成这一步骤，请参阅 [JavaScript 文档](#)。

添加 JavaScript

将 Songbird.js 添加至结账页面并完成其他步骤：

- 1 配置：**创建配置对象并将其传递至 `Cardinal.configure()`。
- 2 侦听事件：**订阅带有 `Cardinal.on()` 的事件并为以下事件设置回调函数：
 - `payments.setupComplete`：此可选事件在 JavaScript 完成初始化并调用 `Cardinal.setup()` 之后触发。
 - `payments.validated`：此事件在交易完成之后触发。
- 3 初始化：**针对每笔交易，调用 `Cardinal.setup()` 以触发并传递 JWT 至 JavaScript。

要完成这些步骤，请参阅 [JavaScript 文档](#)。

BIN 检测

BIN 检测作为必要功能，可帮助发卡行的 ACS 提供商收集更多设备数据；在结账页面打开之前收集此类数据有助于加速验证流程。这一步在验证之前发生，而且必须先于 `Cardinal.start` 事件（标准集成）或注册检查服务请求（混合集成）发生。如需详细信息，请参阅 [JavaScript 文档](#)。

实施混合 3DS 验证

本节主要描述混合 3DS 验证的实施步骤。

请求注册检查服务（混合）

使用注册检查服务检验消费者的卡是否已注册银行卡验证计划。请求针对混合集成的 ICS 注册检查服务时，必须填写 **payerAuthEnrollService_referenceID** 请求字段。以下字段也为必填项：

- billTo_city
- billTo_country
- billTo_email
- billTo_firstName
- billTo_lastName
- billTo_postalCode
- billTo_state
- billTo_street1
- card_accountNumber
- card_cardType
- card_expirationMonth
- card_expirationYear
- merchantID
- merchantReference 代码
- payerAuthEnrollService_mobilePhone
- payerAuthEnrollService_referenceID
- payerAuthEnrollService_run
- payerAuthEnrollService_transactionMode
- purchaseTotals_currency
- purchaseTotals_grandTotalAmount



备注

可发送附加请求数据来降低发卡行的加强验证率。最好是发送所有可用字段。

如需了解必填字段和可选字段的更多信息，请参阅第 121 页，“请求字段”。

您可在同一个请求或单独的请求中使用注册检查和卡授权服务：

- **同一个请求：**如果消费者未注册 3DS 验证计划，CyberSource 将尝试授权其银行卡。这种情况下，证明您曾尝试检查注册的必要字段值将自动传递给授权服务。如果必须进行验证，处理流程将自动中止。
- **单独请求：**您必须手动在授权服务请求（卡授权请求字段）中加入注册检查结果值（注册检查回复字段）。

表 2 列出了这些字段：

表 2 注册检查和回复字段

标识符	注册检查回复字段	银行卡授权请求字段
电子商务交易指示符	payerAuthEnrollReply_ commerceIndicator	ccAuthService_ commerceIndicator
采集指示符（仅限 Mastercard）	payerAuthEnrollReply_ ucafCollectionIndicator	ucaf_collectionIndicator
亚洲、中东和非洲支付接口 注册检查的结果	payerAuthEnrollReply_ veresEnrolled	ccAuthService_ veresEnrolled
3D Secure 版本	payerAuthEnrollReply_ specificationVersion	ccAuthService_ paSpecificationVersion
目录服务器交易 ID 备注 不是 3D Secure 1.0 的必填字段。	payerAuthEnrollReply_ directoryServer TransactionID	ccAuthService_ directoryServerTransacti onID

回复说明

所有类型卡的回复都是相似的。有关注册回复的示例，请参阅第 143 页，附录 C，“请求和回复示例”。

■ 注册银行卡

如果消费者的卡已注册 3DS 验证计划，反馈的原因代码为 475：如果收到此回复，接下来可对验证进行检验。

■ 未注册银行卡

在以下情况下，您将收到原因代码 100：

- 账号未注册 3DS 验证计划。请求中的其他服务正常处理。
- 卡类型不支持 3DS 验证。

如果收到此回复，接下来可进行卡授权。

验证注册银行卡

如果确认消费者的卡已在银行卡验证计划中注册，则必须将发卡行[访问控制器](#)的 URL (ACS URL)、有效载荷和 **payerAuthEnrollReply_authenticationTransactionID** 回复字段纳入 *Cardinal.continue* 函数，以供验证会话处理，参见[示例 1](#)。

示例 1 Cardinal.continue

```
Cardinal.continue('cca',

{

    "AcsUrl":"https://testcustomer34.cardinalcommerce.com/
merchantacsfrontend/pareq.jsp?vaa=b&gold=AAAAAAAA...AAAAA",

    "Payload":"eNpVUk1zgJAQvedXME7PJEFBVdKt1CECeDkVCk2PcfcnNjv8Kr+7tx4nlbGO
cz/se6GluMENPTPeeIz1G37WGEUth7YnpO21TfTvF3wDCBqspQ=="

},

{

    "OrderDetails":{

        "TransactionId" : "123456abc"

    }

}

);
```

Cardinal.continue 会在必要时显示验证窗口，并自动将消费者的会话重定向至 ACS URL 进行验证。消费者的浏览器显示验证窗口以及供其输入密码的选项。

接收验证结果

下一步，*Payments.validated* 启动并返回验证结果，连同回应 JWT 以及支付处理机构交易 ID，参见示例 2。

示例 2 解码后的回应 JWT

```
{
  "iss": "5a4504be6fe3d1127cdfd94e",
  "iat": 1555075930,
  "exp": 1555083130,
  "jti": "cc532159-636d-4fa8-931d-d4b0f4c83b99",
  "ConsumerSessionId": "0_9a16b7f5-8b94-480d-bf92-09cd302c9230",
  "aud": "d0cf3392-62c5-4107-bf6a-8fc3bb49922b",
  "Payload": {
    "Payment": {
      "Type": "CCA",
      "ProcessorTransactionId": "YGSaOBivyG0dzCFs2Zv0"
    },
    "ErrorNumber": 0,
    "ErrorDescription": "Success"
  }
}
```

请求检验服务

对于注册卡，下一步就是请求检验服务。提交检验请求时，必须：

- 发送 **payerAuthValidateService_authenticationTransactionID** 请求字段
- 发送信用卡信息，包括 PAN、币种和失效日期（年份和月份）。

收到的回复将包含检验结果。

CyberSource 建议您同时请求 3DS 验证和银行卡授权服务。如果同时请求，CyberSource 会自动将正确的信息发送给您的支付处理机构，还会将以下字段的值转换为支付处理机构要求的规范格式：

- **电子商务交易指示符**：payerAuthEnrollReply_commerceIndicator
- **CAVV**：payerAuthValidateReply_cavv
- **AAV**：payerAuthValidateReply_ucafAuthenticationData
- **XID**：payerAuthEnrollReply_xid 和 payerAuthValidateReply_xid

如果单独请求，您必须手动在授权服务请求（银行卡授权请求字段）中加入检验结果值（检验检查回复字段）。要获得责任转移保护，您必须在请求中传递银行卡类型和支付处理机构的所有相关数据。否则，可能无法进行交易的责任转移。在授权请求中加入电子商务交易指示符 (ECI)、交易 ID (XID)、3D Secure 版本、目录服务器交易 ID 及以下针对特定银行卡的信息：

- 对于 Visa、American Express、JCB、Diners Club 和 Discover，请加入 CAVV（持卡人验证检验值）。
- 对于 Mastercard，请加入 UCAF（通用持卡人验证字段）与采集指示符。

表 3 列出了这些字段。

表 3 检验检查和回复字段

标识符	检验检查回复字段	银行卡授权请求字段
电子商务交易指示符	payerAuthValidateReply_commerceIndicator	ccAuthService_commerceIndicator
CAVV（仅限 Visa 和 American Express）	payerAuthValidateReply_cavv	ccAuthService_cavv
AAV（仅限 Mastercard。称为 UCAF）	payerAuthValidateReply_ucafAuthenticationData	ucaf_authenticationData
XID	payerAuthValidateReply_xid	ccAuthService_xid
3D Secure 版本	payerAuthValidateReply_specificationVersion	ccAuthService_paSpecificationVersion
目录服务器交易 ID 备注 不是 3D Secure 1.0 的必填字段。	payerAuthValidateReply_directoryServer TransactionID	ccAuthService_directoryServerTransactionID

回复说明



重要说明

如果验证失败，Visa、American Express、JCB、Diners Club 和 Discover 会要求您拒绝接受该卡，而必须要求消费者使用其他支付方式。

根据收到的检验回应处理订单。所有类型卡的回复都是相似的：

- **成功:**

您将收到原因代码 100，其他服务请求（包括授权）将正常处理。
- **失败:**

您将收到原因代码 476（表示验证失败），请求中的其他服务不会被处理。
- **错误:**

如果收到支付卡公司发送的错误消息，请根据您的业务规则处理订单。如果错误频繁出现，请向**客户支持部门**报告。如果收到 **CyberSource** 系统错误消息，请确定原因，并仅在适当情况下对卡进行授权。

要检验注册和验证检查是否针对同一个交易，应确认注册检查和验证回复中的 XID 是否相同。

向消费者展示成功或失败消息页面

验证完成后，将消费者转到包含成功或失败消息的页面。您必须确保向消费者显示的所有消息均准确完整，并且确保它们可以描述已注册或未注册卡的所有可能情况。例如，如果验证失败，应向消费者显示以下消息：

```
Authentication Failed
```

```
Your card issuer cannot authenticate this card.Please select another card  
or form of payment to complete your purchase.
```

实施标准 3DS 验证

3

本章主要概述将标准 3DS 验证服务集成到现有业务流程中的过程。CyberSource 3DS 验证服务通过 CardinalCommerce JavaScript 来执行验证。访问本章包含的 JavaScript 文档链接可跳转至 Cardinal 网站。

流程概述

通知 CyberSource 客户代表您想要实施 3DS 验证 (3D Secure)。为其提供测试时需要使用的 CyberSource 商户 ID。如需详细信息，请参阅第 21 页，“所需商户信息”。

实施任务包括：

- 在结账页面中添加 JavaScript 代码。
- 针对每个购物请求
 - 构建验证请求
 - 调用验证
 - 处理拒绝事件
 - 调用以下服务：
 - **payerAuthEnrollService**: 3DS 验证注册检查
 - **ccAuthService**: 银行卡授权服务
- 使用第 46 页，第 5 章，“测试 3DS 验证服务”中的测试案例测试初始代码，并进行适当调整。在 JavaScript 代码中更改 URL 即可切换至测试环境。
- 确定账户已根据生产环境的要求进行配置。

开始之前

实施 3DS 验证服务之前，您的业务团队必须联系收单行和 CyberSource 设置服务。您的软件开发团队应熟悉此服务的 API 字段和技术详细信息。

凭据/API 密钥

实施时，需要 API 密钥来创建 JWT（JSON Web Token）。如需更多信息，请联系 CyberSource 客户支持部门。

创建 JWT

标准集成和混合集成都会使用 JWT（JSON Web Token）验证方法。要完成这一步骤，请参阅 [JavaScript 文档](#)。

添加 JavaScript

将 Songbird.js 添加至结账页面并完成其他步骤：

- 1 配置：**创建配置对象并将其传递至 `Cardinal.configure()`。
- 2 侦听事件：**订阅带有 `Cardinal.on()` 的事件并为以下事件设置回调函数：
 - `payments.setupComplete`：此可选事件在 JavaScript 完成初始化并调用 `Cardinal.setup()` 之后触发。
 - `payments.validated`：此事件在交易完成之后触发。
- 3 初始化：**针对每笔交易，调用 `Cardinal.setup()` 以触发并传递 JWT 至 JavaScript。

要完成这些步骤，请参阅 [JavaScript 文档](#)。

BIN 检测

BIN 检测作为必要功能，可帮助发卡行的 ACS 提供商收集更多设备数据；在结账页面打开之前收集此类数据有助于加速验证流程。这一步在验证之前发生，而且必须先于 `Cardinal.start` 事件（标准集成）或注册检查服务请求（混合集成）发生。如需详细信息，请参阅 [JavaScript 文档](#)。

实施标准 3DS 验证

下面这一节主要描述标准 3DS 验证的实施步骤。

开始验证

JavaScript 处理设备数据收集任务，发起验证交易、在必要时显示验证窗口，并返回验证结果。

商户（通常是在消费者点击“下单”或“提交订单”按钮的情况下）通过触发 **Cardinal.start()** 发起验证流程。**Cardinal.start()** 调用验证流程，对消费者实施验证。

创建订单对象并将其传递至 **Cardinal.start()** 事件。商户添加的字段越多，持卡人受到质询（要求其提供凭据）的可能性越低。请参阅 [JavaScript 文档](#)，了解 3D Secure 2.x 字段列表。

在授权之前启动 **Cardinal.start()**，参见 [示例 3](#)。数据的第二个参数是请求订单对象。商户可提前构建此对象或直接将其传递（参见示例）。

示例 3 Cardinal.start 带请求订单对象

```
Cardinal.start("cca", {
  OrderDetails: {
    OrderNumber: "1234567890"
  },
  Consumer: {
    Account: {
      AccountNumber: "40000000000001000",
      ExpirationMonth: "01",
      ExpirationYear: "2099"
      ...
      <Other 2.x required/optional fields>
    }
  }
  ...
});
```

Payments.validated 返回验证结果，连同回应 JWT 以及支付处理机构交易 ID，参见 [示例 4](#)。

示例 4 解码后的回应 JWT

```
{
  "iss": "5a4504be6fe3d1127cdfd94e",
  "iat": 1555075930,
  "exp": 1555083130,
  "jti": "cc532159-636d-4fa8-931d-d4b0f4c83b99",
  "ConsumerSessionId": "0_9a16b7f5-8b94-480d-bf92-09cd302c9230",
  "aud": "d0cf3392-62c5-4107-bf6a-8fc3bb49922b",
  "Payload": {
    "Payment": {
      "Type": "CCA",
      "ProcessorTransactionId": "YGSaOBivyG0dzCFs2Zv0"
    },
    "ErrorNumber": 0,
    "ErrorDescription": "Success"
  }
}
```

下一步，为 *payments.validated* 事件添加逻辑以处理特定的返回值。**ActionCode** 字段应作为主交易状态指示符使用。表 4 包含可用于 **ActionCode** 的值及其含义。

表 4 操作代码

值	说明
SUCCESS	验证完成。继续进行授权操作。
NOACTION	未实施验证，也没有出现服务级错误。这通常意味着商户可以继续进行授权操作，需要注意的是交易可能无法适用责任转移的规则。
FAILURE	验证失败；其中包括最终用户验证失败的情况。
ERROR	出错。

向消费者展示成功或失败消息页面

验证完成后，将消费者转到包含成功或失败消息的页面。您必须确保向消费者显示的所有消息均准确完整，并且确保它们可以描述已注册或未注册卡的所有可能情况。例如，如果验证失败，应向消费者显示以下消息：

```
Authentication Failed

Your card issuer cannot authenticate this card.Please select another card
or form of payment to complete your purchase.
```

请求注册检查服务（标准）

一旦完成检验，请使用注册检查服务来获取授权所需的值。

要请求注册检查服务，需从 JWT 中提取支付处理机构交易 ID 值，并将其放入 **payerAuthEnrollService_authenticationTransactionID** 请求字段发送出去。以下字段也为必填项：

- **billTo_city**
- **billTo_country**
- **billTo_email**
- **billTo_firstName**
- **billTo_lastName**
- **billTo_postalCode**
- **billTo_state**
- **billTo_street1**
- **card_accountNumber**
- **card_cardType**
- **card_expirationMonth**
- **card_expirationYear**
- **merchantID**
- **merchantReference** 代码
- **payerAuthEnrollService_mobilePhone**
- **payerAuthEnrollService_referenceID**
- **payerAuthEnrollService_run**
- **payerAuthEnrollService_transactionMode**
- **purchaseTotals_currency**
- **purchaseTotals_grandTotalAmount**



备注

可发送附加请求数据来降低发卡行的加强验证率。最好是发送所有可用字段。

如需了解必填字段和可选字段的更多信息，请参阅第 121 页，“请求字段”。

CyberSource 建议您同时请求 3DS 验证和银行卡授权服务。如果同时请求，CyberSource 会自动将正确的信息发送给您的支付处理机构，还会将以下字段的值转换为支付处理机构要求的规范格式：

- 电子商务交易指示符: `payerAuthEnrollReply_commerceIndicator`
- CAVV: `payerAuthValidateReply_cavv`
- AAV: `payerAuthValidateReply_ucafAuthenticationData`
- XID: `payerAuthEnrollReply_xid` 和 `payerAuthValidateReply_xid`

如果单独请求，您必须手动在授权服务请求（银行卡授权请求字段）中加入注册检查结果值（注册检查回复字段）。要获得责任转移保护，您必须在请求中传递银行卡类型和支付处理机构的所有相关数据。否则，可能无法进行交易的责任转移。在授权请求中加入电子商务交易指示符 (ECI)、交易 ID (XID)、3D Secure 版本、目录服务器交易 ID 及以下针对特定银行卡的信息：

- 对于 Visa、American Express、JCB、Diners Club 和 Discover，请加入 CAVV（持卡人验证检验值）。
- 对于 Mastercard，请加入 UCAF（通用持卡人验证字段）与采集指示符。

表 5 列出了这些字段。

表 5 注册检查和回复字段

标识符	注册检查回复字段	银行卡授权请求字段
电子商务交易指示符	<code>payerAuthEnrollReply_commerceIndicator</code>	<code>ccAuthService_commerceIndicator</code>
CAVV（仅限 Visa 和 American Express）	<code>PayerAuthEnrollReply_cavv</code>	<code>ccAuthService_cavv</code>
AAV（仅限 Mastercard。称为 UCAF）	<code>payerAuthEnrollReply_ucafAuthenticationData</code>	<code>ucaf_authenticationData</code>
XID	<code>payerAuthEnrollReply_xid</code>	<code>ccAuthService_xid</code>
3D Secure 版本	<code>payerAuthEnrollReply_specificationVersion</code>	<code>ccAuthService_paSpecificationVersion</code>
目录服务器交易 ID	<code>payerAuthEnrollReply_directoryServer TransactionID</code>	<code>ccAuthService_directoryServerTransactionID</code>
备注 不是 3D Secure 1.0 的必填字段。		

大部分情况下，一笔消费仅需请求一次卡授权。但是，如果原始授权在请款之前到期，则必须发送多个授权请求，当订单拆分履行或延迟履行时会出现这种情况。这种情况下，您必须在后续授权请求中加入与原始请求相同的 3DS 验证数据，以便收单行在出现争议时跟踪所有相关请求。验证数据仅可用于一次授权，不得多次重复使用或用于后续授权。

升级 3DS 验证服务

本章为目前使用 CyberSource 3DS 验证服务的商户提供升级至 3D Secure 2.x 的相关信息。

升级至 3D Secure 2.x

优势

3D Secure 2.x 有以下优势：

- 支持更多数据，让交易更安全。
- 3D Secure 2.x 可向后兼容。升级至 3D Secure 2.x 之后，将自动向发卡行发送更多数据。
- 为消费者提供简单易用的购物体验，实现无阻力验证并缩短交易时间。
- 兼容基于规则的 3DS 验证。
- 手机 SDK 即将发布。
- 可提高授权率。
- 发布后，将降低升级至 3D Secure 2.2 的难度。2.2 版本支持 PSD2 的相关豁免，以提供无阻力验证流程，其中包括收单行/发卡行交易风险评估、白名单、小额交易、单腿交易（交易的一方在欧洲经济区内）以及商户发起的交易。这些豁免功能将在上线时进行定义。

PSD2 影响

如果您受到 PSD2 的影响，就必须升级至 3D Secure 2.x。

PSD2 于 2018 年 1 月生效，依据监管技术标准 (RTS) 制定的附带安全措施于 2019 年 9 月生效。PSD2 对在线支付的身份检查要求更严格，尤其是大额交易。

根据 PSD2 的规定，欧洲的所有支付处理公司均需作出调整。其对商户的影响如下：

- 所有电子支付均需进行双因素验证；当然，为实现无阻力验证，也有一些豁免情形。
- 3-D Secure 电子商务商户必须集成动态验证工具（例如 3D Secure 2.x）。

如果您受到 PSD2 规则的影响，请务必升级至 3D Secure 2.x。

强制性要求

PSD2 针对强客户身份认证 (SCA)、豁免和质询设立了一系列强制性要求。有关强制性要求的详细信息，请参阅以下页面：

https://demos.cardinalcommerce.com/3DS_Info/Country_Mandates/index.html

时间表

如需 PSD2 的合规时间表，请参阅以下页面：

https://demos.cardinalcommerce.com/3DS_Info/Cardinal_Timelines/index.html

建议集成方法

适用于 3D Secure 2.x 的集成方法分为两类：

- 混合集成
- 标准集成

如果您在现有业务流程中使用 3DS 验证服务且需要升级至 3D Secure 2.x，CyberSource 建议您采用混合集成方法。

混合集成方法与目前的流程极为相似：首先请求注册检查服务验证消费者是否注册了银行卡验证计划，然后接收对方的回应。使用 3D Secure 2.x 时，回应中包含一个新值，即支付处理机构交易 ID。

对于注册卡，将 ACS URL、有效载荷和支付处理机构交易 ID 放入 *Cardinal.continue* 函数，并在验证会话中进行处理。

然后，向检验服务发送包含支付处理机构交易 ID 的请求，收到包含电子商务交易指示符和 CAVV/AAV 的回应。



备注

如果您使用了简码化功能，就必须采用混合集成方法。

在标准集成方法中，使用 JavaScript 来执行 3DS 验证的相关步骤。

JavaScript 通过服务器到服务器的调用完成以下操作：采集设备数据、与发卡行交互，并向银行求证消费者的卡是否已在 3D Secure 银行卡验证计划中注册。如果发卡行要求验证，JavaScript 将显示验证窗口。

银行验证消费者的凭据，并返回一个 JWT 由您在服务器端验证。您还需从 JWT 中提取支付处理机构交易 ID。

接下来，您向注册检查服务发送包含支付处理机构交易 ID 的请求。回应中包含电子商务交易指示符和 CAVV/AAV。

有关标准集成的详细信息，请参阅第 30 页，第 3 章，“实施标准 3DS 验证”。

配置要求

实施时，需要 API 密钥来创建 JWT（JSON Web Token）。如需更多支持，请联系 CyberSource 客户支持部门。

要升级现有的 3DS 验证服务，请通知 CyberSource 客户支持部门进行必要的配置调整，说明您使用的是 CyberSource 的现有商户 ID 还是新 ID。

混合集成调用 CyberSource API

类似于目前的流程，调用 **payerAuthEnrollService** 注册检查服务来验证消费者的卡是否已注册银行卡验证计划。不过，使用 3D Secure 2.x 时，可发送其他请求数据，这有助于降低发卡行的加强验证率。3D Secure 2.x 支持以下新字段：

- **billTo_customerAccountChangeDate**
- **billTo_customerAccountCreateDate**
- **billTo_customerAccountPasswordChangeDate**
- **billTo_passportCountry**
- **billTo_passportNumber**
- **item_#_productDescription**
- **payerAuthEnrollService_accountPurchases**
- **payerAuthEnrollService_addCardAttempts**
- **payerAuthEnrollService_alternateAuthentication** 数据
- **payerAuthEnrollService_alternateAuthentication** 日期
- **payerAuthEnrollService_alternateAuthentication** 方法
- **payerAuthEnrollService_authentication** 交易 ID
- **payerAuthEnrollService_challengeCode**
- **payerAuthEnrollService_customerCCAlias**
- **payerAuthEnrollService_defaultCard**
- **payerAuthEnrollService_fraudActivity**
- **payerAuthEnrollService_giftCardAmount**
- **payerAuthEnrollService_giftCardCount**
- **payerAuthEnrollService_giftCardCurrency**
- **payerAuthEnrollService_httpUserAccept**
- **payerAuthEnrollService_installmentTotalCount**
- **payerAuthEnrollService_marketingOptIn**
- **payerAuthEnrollService_marketingSource**
- **payerAuthEnrollService_merchantNewCustomer**
- **payerAuthEnrollService_merchantURL**
- **payerAuthEnrollService_messageCategory**
- **payerAuthEnrollService_npaCode**
- **payerAuthEnrollService_paymentAccountDate**
- **payerAuthEnrollService_preorder**
- **payerAuthEnrollService_preorderDate**
- **payerAuthEnrollService_recurringEndDate**
- **payerAuthEnrollService_recurringFrequency**

- `payerAuthEnrollService_recurringOriginalPurchaseDate`
- `payerAuthEnrollService_reorder`
- `payerAuthEnrollService_shipAddressUsageDate`
- `payerAuthEnrollService_transactionCountDay`
- `payerAuthEnrollService_transactionCountYear`
- `payerAuthEnrollService_transactionMode`
- `shipTo_destinationCode`

发送注册检查服务请求时，还应同时发送 `payerAuthEnrollService_referenceID` 请求字段。

如果确认消费者的卡已在银行卡验证计划中注册，则必须将发卡行访问控制器的 URL (ACS URL)、有效载荷和 `payerAuthEnrollReply_authenticationTransactionID` 回复字段纳入 *Cardinal.continue* 函数，以供验证会话处理。

Payments.validated 启动并返回验证结果，连同回应 JWT 以及支付处理机构交易 ID。

对于注册卡，下一步就是调用 `payerAuthValidateService` 检验服务。发送检验请求时，除了按照目前流程发送交易明细之外，还需在 `payerAuthEnrollService_authenticationTransactionID` 请求字段中加入支付处理机构交易 ID 值。收到的回复将包含检验结果。

3D Secure 2.x 与 3D Secure 1.0 3DS 验证集成服务的不同之处在于：

- 您不会收到 Proof XML 字段。
- 3D Secure 2.x 的附加字段不会显示在 3DS 验证报告中。未来发行版本将添加这些功能。
- 支付处理机构交易 ID 值作为新字段，其用途是在传递后连接注册检查服务并检验验证消息。

配置网站

本节提供设置结账页面和配置 CardinalCommerce JavaScript 组件的的详细说明。

显示验证窗口

如果发卡行要求验证，JavaScript 将向消费者显示验证窗口。

实施时，将 `JavaScript` 标签添加至结账页面，配置 `Cardinal.configure()` 组件，并调用 `Cardinal.setup()`，以便在处理每笔交易时触发 JWT 并将其传递至 JavaScript。

使用 CardinalCommerce JavaScript

为使用 **CardinalCommerce JavaScript**，必须按照本节所述配置并添加相关组件。

JWT (JSON Web Token)

JWT 是在后端服务器上生成的。JWT 的作用是协助 Cardinal 通过您的凭据来确认您的身份。JWT 包含 API 密钥、API 标识符和 Org Unit ID。

可使用任何第三方 JWT 库来生成 JWT。有关详细信息，请参阅 <https://jwt.io>。

对于每笔新交易，都应生成一个新的 JWT。通过 `Cardinal.setup (Init)` 调用来传递 JWT。

示例 5 JWT 示例

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiJiMDc5ZTU0C0ZnNWJlTRiZW
MtYmNmOC1lYWJmNTZmZDg0YyZiLCJpYXQiOiE1Mjk1OTU0NzIsImV4cCI6MTUyYTQyYwMjY3M
iwiaXNzIjo1ZGV2Y2VuOGVybmWVYyZhhbnQiLCJpcmdVmbl1SWQqiOiI1ODJiZTlkZWRhNTI5
MzJhOTQ2YzYzQ1YzQiLCJSZWZlcmlcmVuY2VJZCI6IkNydwWlZVRlc3Rlci0zMjI4NWZiIiwUGF
5bG9hZCI6eyJFcmlrclRldGFpbHMionSiT3KkZXXOdWl1ZXIiOiJDenVpc2VUZXR0ZXItM2
ZiIDVmc3R5fSwitTjZqWN0aWZ5UGF5bG9hZCI6dHJ1ZX0.JW00jfFilppIMI1Cwdl_
J1vlqGwN5Y82H6BxtliqdzF0
```

示例 6 通过 Cardinal.setup 发送解码后的 JWT(Init)

```
{
  "jti": "b079e598-35bb-4bec-bcf8-eabf56fd84c6",
  "iat": 1529595472,
  "exp": 1529602672,
  "iss": "devcentermerchant",
  "OrgUnitId": "582be9deda52932a946c45c4",
  "ReferenceId": "CruiseTester-3fb85fb",
  "Payload": {
    "OrderDetails": {
      "OrderNumber": "CruiseTester-3fb85fb",
      {
        {,
      "ObjectifyPayload": true
    }
  }
}
```

Songbird.js 调用

除非另有说明，否则混合集成方法和标准集成方法均需使用以下组件：

- **Cardinal.configure** 用于在测试期间查看附加日志（设为 **Verbose**）。也可用来配置银行会话的打开方式：内联或模态窗口。
- 使用 **Cardinal.setup (Init)** 将 JWT 传递至 JavaScript。JavaScript 收到 Init 后，将验证您的商户身份并开始采集设备数据。
- 您可通过 **BIN 检测** 以极少量数据的形式传递 **BIN**，如有可能，也可传递完整的卡号。请参阅“**BIN 检测**”了解详情。
- **Cardinal.start**（仅适用于标准集成）是 JavaScript 函数，用于传递交易级详细信息，包括 PAN、币种和失效日期（年份和月份）。
- **Cardinal.continue**（仅适用于混合集成）是 JavaScript 函数，用于将银行重定向至事件。

BIN 检测

BIN 检测是标准集成或混合集成中的必要步骤。**BIN** 的发送顺序在交易级详细信息之前。对于标准集成，应在发送 **Cardinal.start** 以及请求注册检查服务之前发送 **BIN**。

借助 **BIN 检测**，可在消费者发起交易之前收集 **BIN**（如有可能，收集完整的卡号）并与 **Cardinal** 共享。由 **Cardinal** 确定 **BIN** 是否符合 3D Secure 1.0 或 3D Secure 2.x 的要求，然后开启正确的协议路由。

如果 **BIN** 符合 3D Secure 2.x 的要求，其将收集发卡行所需的 Method URL JavaScript 进行设备指纹采集和风险评估。

事件处理器/事件侦听器

除非另有说明，否则混合集成方法和标准集成方法均需使用以下组件：

- ***Payments.setupComplete*** 将在 *Init* 完成时向您发送通知，并确认设备数据是否采集完毕。您必须订阅此事件。
此事件还会提供一个会话 ID，您可将其作为注册检查服务的 ***payerAuthEnrollService_referenceID*** 请求字段。（对于混合集成，该字段为必填字段。）
- ***Payments.validated*** 可提供支付处理机构交易 ID 值，您必须在注册检查服务（适用于标准集成）或检验服务（适用于混合集成）中发送此值，以获取最终验证结果。
您必须订阅此事件。
如果 ***Cardinal.setup (Init)*** 函数出错，JavaScript 将提前调用 ***payments.validated***。如果 ***payments.validated*** 返回错误，您可以建立相关逻辑来继续下一步操作。
- ***Cardinal.start***（仅适用于标准集成）是 JavaScript 函数，用于传递交易级详细信息，包括 PAN、币种和失效日期（年份和月份）。
- ***Cardinal.continue***（仅适用于混合集成）是 JavaScript 函数，用于将银行重定向至事件。

测试

做好测试新服务的准备之后，请参阅“[3D Secure 2.x 的测试案例](#)”。在 JavaScript 代码中更改 URL 即可切换至测试环境。

迁移 FAQ

问：是不是要为每笔交易发送一个新的 JWT？

答：是的，虽然 JWT 的失效时间在两小时之后，但是您依然要为每笔交易发送一个新的 JWT。

问：*Cardinal.setup(Init)* 能否在请求注册检查服务之前运行？

答：不能，*Init* 的作用是采集设备信息，此操作必须在请求注册检查服务和发送交易级详细信息之前完成。

问：如果收到 *Init* 出错的消息，应该怎么做？

答：解码 JWT，确认凭据是否正确、时间戳是否为 Unix 格式、是否已添加所需的全部信息。如需更多支持，请联系 CyberSource 客户支持部门。

问：如何连接设备数据与交易级数据？

答：有两种方式：

可在原来的 JWT 中创建一个参考 ID，并为注册检查服务的 **payerAuthEnrollService_referenceID** 请求字段传递一个相同的值。

Payments.setupComplete 返回一个会话 ID，可将此值用于注册检查服务的 **payerAuthEnrollService_referenceID** 请求字段。

问：何时在 3DS 验证报告中加入 3D Secure 2.x 的新字段？

答：未来发行版本将添加这些功能。

问：在实施和测试新版本时，当前服务能继续正常运行吗？

答：是的，当前服务能继续正常运行。

问：如果 2.2 版本即将发布，还有必要实施 3D Secure 2.1 吗？

答：3D Secure 2.2 的相关规范尚未确定，PSD2 为其设定的交付期限为 2019 年 9 月，在此日期之前，这一版本不会发布。3D Secure 2.1 已经符合 PSD2 要求，2.2 版本的作用是使用豁免机制来减少 SCA。

问：混合集成方法与标准集成方法之间有何区别？

答：主要区别在于标准集成不包含 3DS 验证检验服务请求。有关详细信息，请参阅第 22 页，第 2 章，“实施混合 3DS 验证”和第 36 页，第 4 章，“升级 3DS 验证服务”。

问：为确保我的代码正常运行，应开展什么测试？

答：使用测试案例（第 91 页，“3D Secure 2.x 的测试案例”）测试初始代码，并进行适当调整。在 JavaScript 代码中更改 URL 即可切换至测试环境。

问：3D Secure 2.x 验证工具可从哪些方面改善消费者使用移动或平板设备购物的体验？

答：3D Secure 2.x 具有设备兼容性，您可以控制验证格式。3D Secure 2.x 还支持更新颖、更安全的验证工具，例如发送至消费者移动设备或电子邮箱的一次性密码 (OTP)。

测试 3DS 验证服务

完成对 Web 和 API 集成的必要更改后，执行所有适用于您所支持卡的测试，验证所有组件均正常工作。每项测试都包含特定输入数据和您在 API 回复中收到的最重要的结果字段。

测试流程

请在测试中使用指定卡号，并将卡的失效日期设置为当前年份加两年，月份设置为 12 月。例如，对于 2019 年，请使用 2022 年。另外，您还必须填写订单要求的必填字段。

注册检查

对于一些注册银行卡，完成注册检查后会出现验证窗口。



备注

要查看验证窗口，必须允许浏览器显示弹出窗口。

测试密码始终为 1234。

根据用户的操作，可能会产生两种结果：

- 如果用户提交已注册卡的密码，您将收到[访问控制服务器 \(ACS\)](#) 的 URL，可在其中对消费者进行验证。
- 如果用户点击“退出”链接并在验证窗口中点击“确定”，则不会进行验证。

表 6 列出了不同测试案例中使用的回复字段。

表 6 注册检查测试案例中使用的回复字段

测试案例中使用的名称	API 字段
ACS URL	payerAuthEnrollReply_acsURL
电子商务交易指示符	payerAuthEnrollReply_commerceIndicator
ECI	payerAuthEnrollReply_eci
PAReq	payerAuthEnrollReply_paReq
proofXML	payerAuthEnrollReply_proofXML
原因代码	payerAuthEnrollReply_reasonCode
已注册 VERes	payerAuthEnrollReply_veresEnrolled
XID	payerAuthEnrollReply_xid

验证检验

表 7 仅列出了不同测试案例中使用的回复字段。

表 7 验证检验测试案例中使用的回复字段

测试案例中使用的名称	API 字段
验证结果	payerAuthValidateReply_authenticationResult
电子商务交易指示符	payerAuthValidateReply_commerceIndicator
AAV（仅限 Mastercard）	payerAuthValidateReply_ucafAuthenticationData
CAVV（除 Mastercard 以外的所有银行卡类型）	payerAuthValidateReply_cavv
采集指示符	payerAuthValidateReply_ucafCollectionIndicator
ECI	payerAuthValidateReply_eci
PARes 状态	payerAuthValidateReply_authenticationStatusMessage
原因代码	payerAuthValidateReply_reasonCode
XID	payerAuthValidateReply_xid

预期结果

以下流程图根据卡的注册状态汇总了 3DS 验证流程，以及不同验证路径的后续消费者体验。

应将此信息与测试案例配合使用，来确定如何处理订单。

图 1 Visa、American Express、JCB、Diners Club 和 Discover 的验证路径

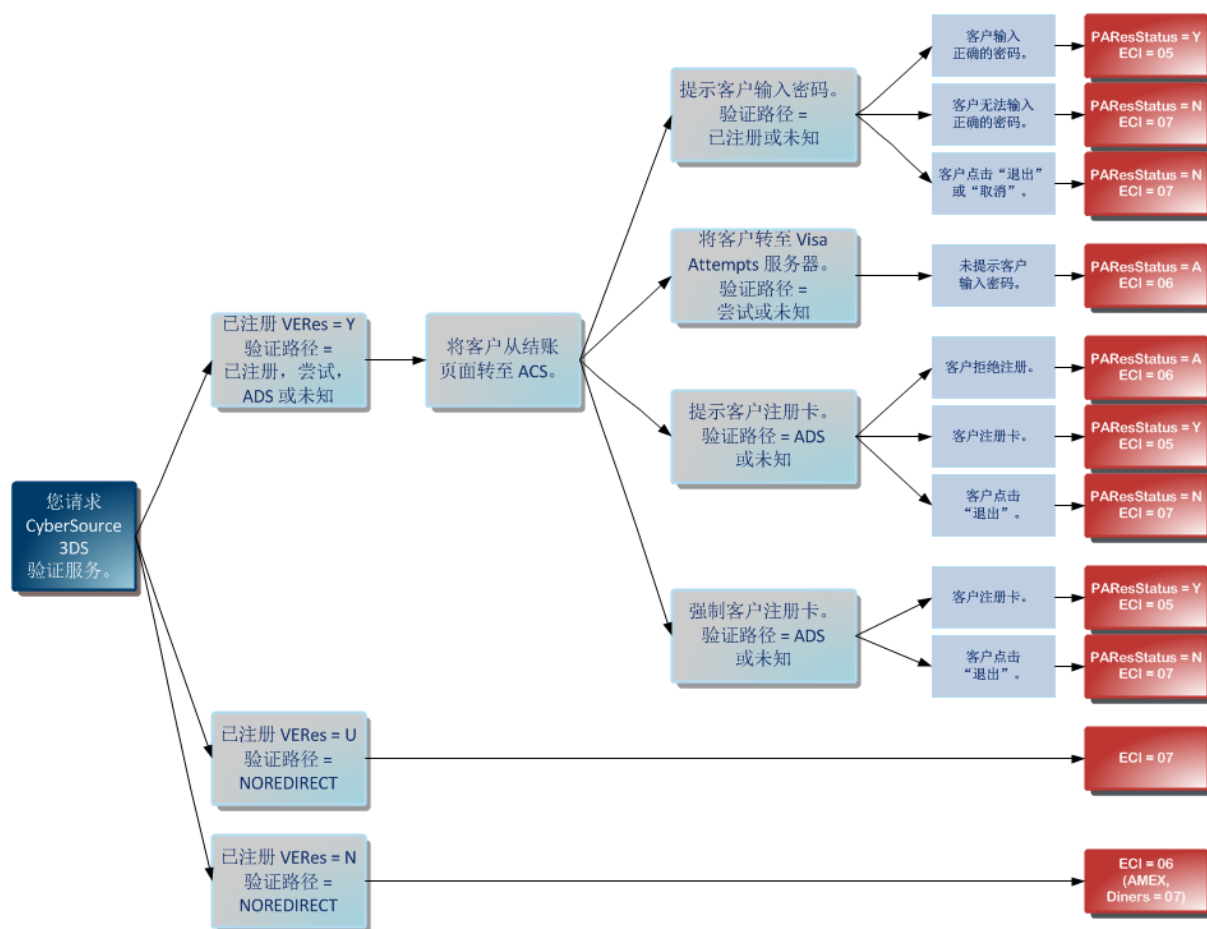
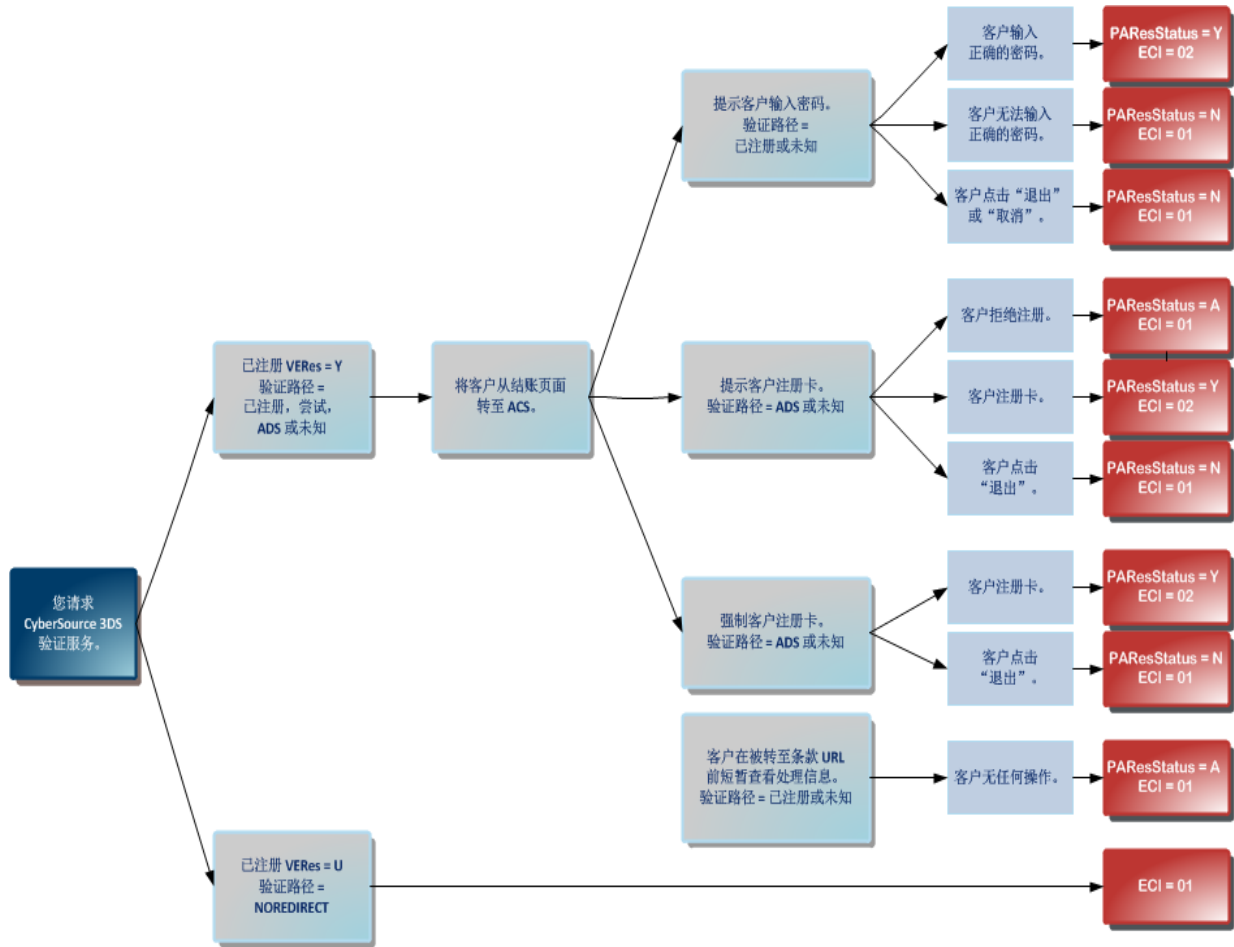


图 2 Mastercard 和 Maestro 的验证路径



3D Secure 1.0 的测试案例

Visa Secure

如果支付处理机构支持，可在 3DS 验证服务中使用 16 和 19 位的 Visa 卡。

表 8 Visa Secure 回复字段的可能值

结果及说明		验证检验回复			
		验证结果	ECI	商务交易指示符	原因代码
成功	验证成功。	0	05	vbv	100
	有尝试验证的记录。	1	06	vbv_ attempted	100
失败（非消费者责任）	阻止验证完成的系统错误：可继续验证，但是无责任转移。	6	1	— ²	100
	发卡行无法执行验证。	6	07	internet	100
	由于出现问题，目录服务器或发卡行无回应。		07	internet vbv_failure (支付处理机构： AIBMS、 Barclays、 Streamline 或 FDC Germany)	
	PAREs 无效。	-1	—	—	476
失败（消费者责任）	验证失败或持卡人未完成验证。 如果验证失败，Visa 会要求您不接受该卡。您必须要求消费者使用其他支付方式。	9	—	—	476

1 ECI 值因失败原因而异。
2 短划线 (—) 表示字段为空或不存在。

测试案例 1: Visa Secure 注册卡: 验证成功

卡号	4000000000000002 显示验证窗口	
	4000000000000000022	
	40000000000000119 不显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	ics_pa_validate 服务成功。	
	ACS URL URL	验证结果 0
	PAReq PAReq 值	CAVV CAVV 值
	proofXML proofXML 值	电子商务交易指示符 vbv
	已注册 VERes Y	ECI 05
	XID XID 值	PARes 状态 Y
		XID XID 值
操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。	

测试案例 2: Visa Secure 注册卡: 验证成功, 但 PARes 无效

卡号	4000000000000010 显示验证窗口	
	4000000000000000071	
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	我们遇到了一个 3DS 验证问题: PARes 签名摘要值不匹配。PARes 消息已被修改。	
	ACS URL URL 值	验证结果 -1
	PAReq PAReq 值	XID XID 值
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	请勿继续进行验证。而是应要求消费者使用其他支付方式。	

测试案例 3: Visa Secure 注册卡: 尝试处理

卡号	40000000000000101 不显示验证窗口 400000000000000063 显示验证窗口 40000000000000127 购物期间的银行卡注册选项	
验证类型	购物期间激活	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	ACS URL URL 值	验证结果 1
	PAReq PAReq 值	CAVV CAVV 值
	proofXML proofXML 值	电子商务交易指示符 vbv_attempted
	已注册 VERes Y	ECI 06
	XID XID 值	PARes 状态 A
		XID XID 值
操作	如果您单独请求验证检验和授权服务，请按以下步骤进行操作： 1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。 如果您同时请求验证检验和授权服务，上述流程将自动进行。借助测试卡 40000000000000127，您可以重现消费者在购买期间注册卡的流程。如果银行未注册银行卡，注册检查后，消费者的浏览器中会出现银行卡注册选项窗口。消费者可立即激活卡或稍后激活。在这两种情况下，都要对卡进行验证，并且验证要成功才会激活。	

测试案例 4: Visa Secure 注册卡: 未完成验证

卡号	4000000000000036 400000000000000055	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	■ 发卡行无法执行验证。 ■ ics_pa_validate 服务成功。
	ACS URL URL 值	验证结果 6
	PAReq PAReq 值	电子商务交易指示符 internet
	proofXML proofXML 值	ECI 07
	已注册 VERes Y	PARes 状态 U
	XID XID 值	XID XID 值
操作	要求消费者使用其他支付方式, 或提交交易。无责任转移。	

测试案例 5: Visa Secure 注册卡: 验证失败

卡号	4000000000000028 显示验证窗口 400000000000000048	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	■ 用户未通过验证。 ■ 无法对支付人进行验证。
	ACS URL URL 值	验证结果 9
	PAReq PAReq 值	PARes 状态 N
	proofXML proofXML 值	XID XID 值
	已注册 VERes Y	
	XID XID 值	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 6: Visa Secure 注册卡: 验证失败 (消费者退出)

卡号	4000008531947799	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	■ 消费者阻止验证。 ■ ics_pa_validate 服务成功。
	ACS URL URL 值	验证结果 9
	PAReq PAReq 值	PARes 状态 N
	proofXML proofXML 值	XID XID 值
	已注册 VERes Y	
	XID XID 值	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 7: Visa Secure 注册卡: 验证不可用

卡号	40000000000000069 4000000000000000014	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
详细信息	ics_pa_enroll 服务成功。	
	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	提交您的授权请求。无责任转移。	

测试案例 8: Visa Secure 注册卡: 验证错误

卡号	4000000000000093 40000000000000006	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	我们遇到了一个 3DS 验证问题: 处理 PAREs 时出错。
	ACS URL URL 值	电子商务交易指示符 internet
	PAReq PAReq 值	ECI 07
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 9: Visa Secure 未注册银行卡

卡号	4000000000000051 40000000000000030	
验证类型	非参与银行	
结果	注册检查	验证检验
汇总	原因代码 100	
详细信息	ics_pa_enroll 服务成功。	
	电子商务交易指示符 vbv_attempted	
	ECI 06	
	proofXML proofXML 值	
	已注册 VERes N	
操作	提交您的授权请求。责任转移。	

测试案例 10: Visa Secure 注册检查: 超时

卡号	4000000000000044	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 11: Visa Secure 注册检查错误

卡号	4000000000000085	错误响应
	4000000000000077	配置不正确: 无法进行验证
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	继续处理授权请求, 并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权, 则会自动处理授权。	

测试案例 12: Visa Secure 注册 RIBA_PASS

卡号	4000180000000002		
验证类型	被动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	详细信息	ACS URL URL	验证结果 0
		PAReq PAReq 值	CAVV CAVV 值
		proofXML proofXML 值	电子商务交易指示符 vbv
		已注册 VERes Y	ECI 05
		XID XID 值	PARes 状态 Y
			XID XID 值
操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。		

测试案例 13: Visa Secure 注册 RIBA_PASS: 验证失败

卡号	4000180000000028		
验证类型	被动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。		■ 用户未通过验证。 ■ 无法对支付人进行验证。
	详细信息	ACS URL URL 值	验证结果 9
		PAReq PAReq 值	PARes 状态 N
		proofXML proofXML 值	XID XID 值
		已注册 VERes Y	
		XID XID 值	
操作	您不可以提交此交易进行授权，而是应要求消费者使用其他支付方式。		

测试案例 14: Visa Secure 注册 RIBA

卡号	4000260000000002 显示验证窗口	
验证类型	基于风险的银行	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	ACS URL URL	验证结果 0
	PAReq PAReq 值	CAVV CAVV 值
	proofXML proofXML 值	电子商务交易指示符 vbv
	已注册 VERes Y	ECI 05
	XID XID 值	PARes 状态 Y
		XID XID 值
操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。	

测试案例 15: Visa Secure 注册 RIBA: 验证失败

卡号	40002600000000028 显示验证窗口	
验证类型	基于风险的银行	
结果	原因代码 475	原因代码 476
汇总	持卡人已注册 3DS 验证。请在授权之前进行验证。	■ 用户未通过验证。 ■ 无法对支付人进行验证。
详细信息	ACS URL URL 值	验证结果 9
	PAReq PAReq 值	PARes 状态 N
	proofXML proofXML 值	XID XID 值
	已注册 VERes Y	
	XID XID 值	
操作	您不可以提交此交易进行授权，而是应要求消费者使用其他支付方式。	

Mastercard Identity Check

表 9 Mastercard Identity Check 和 Maestro 回复字段的可能值

结果及说明		payerAuthValidateReply_			
		authentication Result	ucafCollection Indicator	commerce Indicator	reason Code
成功	验证成功。	0	2	spa	100
	有尝试验证的记录。	1	1	spa	100
	未完成验证。	1	0	spa	100
失败（非消费者责任）	系统错误（发卡行无法执行验证）：无法授权此卡；无责任转移。	6	0	internet	100
	PARes 无效。	-1	0		476
失败（消费者责任）	验证失败或持卡人未完成验证。	9	0	—	476

测试案例 16: Mastercard Identity Check 注册卡：验证成功

卡号	5200000000000007 显示验证窗口 52000000000000114 不显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	
	原因代码 475	原因代码 100
	银行卡已注册 3DS 验证。请在授权之前进行验证。	
	ics_pa_validate 服务成功。	
	详细信息	
	ACS URL URL	验证结果 0
	PAReq PAReq 值	AAV AAV 值
	proofXML proofXML 值	采集指示符 2
	已注册 VERes Y	电子商务交易指示符 spa
操作	XID XID 值	PARes 状态 Y
		XID XID 值
	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将所需的 3DS 验证值添加到授权请求。	

测试案例 17: Mastercard Identity Check 注册卡：验证成功，但 PAREs 无效

卡号	5200000000000015 显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	ACS URL URL	验证结果 -1
	PAReq PAReq 值	XID XID 值
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	请勿处理授权请求。而是应要求消费者使用其他支付方式。	

测试案例 18: Mastercard Identity Check 注册卡：尝试处理

卡号	5200000000000122 购物期间的银行卡注册选项 5200000000000106	
验证类型	购物期间激活	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	ACS URL URL	验证结果 1
	PAReq PAReq 值	AAV AAV 值
	proofXML proofXML 值	采集指示符 1
	已注册 VERes Y	电子商务交易指示符 spa
	XID XID 值	PARes 状态 A
		XID XID 值
操作	借助此测试卡，您可以重现消费者在购买期间注册卡的流程。如果银行未注册银行卡，注册检查后，消费者的浏览器中会出现银行卡注册选项窗口。消费者可立即激活卡或稍后激活。在这两种情况下，都要对卡进行验证，并且验证要成功才会激活。 1 将签名的 PAREs 添加到验证请求。 2 在回复中，确保注册检查中的 XID 与验证中的 XID 匹配。 3 将所需的 3DS 验证值添加到授权请求。	

测试案例 19: Mastercard Identity Check 注册卡: 未完成验证

卡号	5200000000000031 不显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	■ ics_pa_validate 服务成功。 ■ 发卡行无法执行验证。
	详细信息	ACS URL URL 值 验证结果 6
	PAReq PAReq 值	采集指示符 0
	proofXML proofXML 值	电子商务交易指示符 internet
	已注册 VERes Y	PARes 状态 U
	XID XID 值	XID XID 值
操作	要求消费者使用其他支付方式, 或提交交易。无责任转移。	

测试案例 20: Mastercard Identity Check 注册卡: 验证失败

卡号	5200000000000023 显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	■ 用户未通过验证 ■ 无法对支付人进行验证。
	详细信息	ACS URL URL 值 验证结果 9
	PAReq PAReq 值	PARes 状态 N
	proofXML proofXML 值	
	已注册 VERes Y	XID XID 值
	XID XID 值	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 21: Mastercard Identity Check 注册卡: 验证失败 (消费者退出)

卡号	5641821000010028	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	■ 消费者阻止验证。 ■ ics_pa_validate 服务成功。
	ACS URL URL 值	验证结果 9
	PAReq PAReq 值	PARes 状态 N
	proofXML proofXML 值	XID XID 值
	已注册 VERes Y	
	XID XID 值	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 22: Mastercard Identity Check 注册卡: 验证不可用

卡号	5200000000000064	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
详细信息	ics_pa_enroll 服务成功。	
	采集指示符 0	
	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	提交交易。无责任转移。	

测试案例 23: Mastercard Identity Check 注册卡: 验证错误

卡号	5200000000000098 不显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	我们遇到了一个 3DS 验证问题: 处理 PARES 时出错。
	ACS URL URL 值	采集指示符 0
	PAReq PAReq 值	电子商务交易指示符 internet
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 24: Mastercard Identity Check 注册检查超时

卡号	5200000000000049	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
详细信息	ics_pa_enroll 服务成功。	
	采集指示符 0	
	电子商务交易指示符 spa	
	proofXML proofXML 值	
操作	10-12 秒后继续处理授权消息。无责任转移。	

测试案例 25: Mastercard Identity Check 注册检查错误

卡号	5200000000000080	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
详细信息	ics_pa_enroll 服务成功。	
采集指示符	0	
电子商务交易指示符	internet	
proofXML	proofXML 值	
已注册 VERes	U	
操作	继续处理授权请求，并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权，则会自动处理授权。	

测试案例 26: Mastercard Identity Check RIBA_PASS

卡号	5200180000000007	
验证类型	被动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 100
详细信息	银行卡已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
ACS URL	URL	验证结果 0
PAREq	PAREq 值	AAV AAV 值
proofXML	proofXML 值	采集指示符 2
已注册 VERes	Y	电子商务交易指示符 spa
XID	XID 值	PARes 状态 Y
		XID XID 值
操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将所需的 3DS 验证值添加到授权请求。	

测试案例 27: Mastercard Identity Check RIBA_PASS: 验证失败

卡号	5200180000000023		
验证类型	被动验证		
结果	注册检查	验证检验	
汇总	原因代码	475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。		- 用户未通过验证 - 无法对支付人进行验证。
	ACS URL	URL 值	验证结果 9
	PAReq	PAReq 值	PARes 状态 N
	proofXML	proofXML 值	
	已注册 VERes	Y	XID XID 值
	XID	XID 值	
操作	您不可以提交此交易进行授权，而是应要求消费者使用其他支付方式。		

测试案例 28: Mastercard Identity Check RIBA

卡号	5200260000000007 显示验证窗口		
验证类型	基于风险的银行		
结果	注册检查	验证检验	
汇总	原因代码	475	原因代码 100
详细信息	银行卡已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	ACS URL	URL	验证结果 0
	PAReq	PAReq 值	AAV AAV 值
	proofXML	proofXML 值	采集指示符 2
	已注册 VERes	Y	电子商务交易指示符 spa
	XID	XID 值	PARes 状态 Y
		XID	XID 值
操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将所需的 3DS 验证值添加到授权请求。		

测试案例 29: Mastercard Identity Check RIBA: 验证失败

卡号	5200260000000023 显示验证窗口	
验证类型	基于风险的银行	
结果	注册检查	验证检验
	汇总	
	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	■ 用户未通过验证 ■ 无法对支付人进行验证。
	详细信息	
	ACS URL URL 值	验证结果 9
	PAReq PAReq 值	PARes 状态 N
	proofXML proofXML 值	
	已注册 VERes Y	XID XID 值
	XID XID 值	
操作	您不可以提交此交易进行授权，而是应要求消费者使用其他支付方式。	

Maestro

测试案例 30: Maestro 注册卡: 验证成功

卡号	6759411100000008	不显示验证窗口
	6759410000006404	显示验证窗口
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	原因代码 475
	原因代码	100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	ACS URL URL
	验证结果	0
	PAReq	PAReq 值
	AAV	AAV 值
	proofXML	proofXML 值
	采集指示符	2
操作	已注册 VERes	Y
	电子商务交易指示符	spa
	XID	XID 值
	PARes 状态	Y
	XID	XID 值
1 将签名的 PARes 添加到验证请求。 2 在回复中, 确保注册检查中的 XID 与验证中的 XID 匹配。 3 将所需的 3DS 验证值添加到授权请求。		

测试案例 31: Maestro 注册卡: 验证成功, 但 PARes 无效

卡号	6331101234567892	不显示验证窗口
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	原因代码 475
	原因代码	476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	3DS 验证问题: PARes 签名摘要值不匹配。PARes 消息已被修改。
	详细信息	ACS URL URL
	验证结果	-1
	PAReq	PAReq 值
	XID	XID 值
	proofXML	proofXML 值
	已注册 VERes	Y
操作	XID	XID 值
	请勿处理授权请求。而是应要求消费者使用其他支付方式。	

测试案例 32: Maestro 注册卡: 尝试处理

卡号	560000000000000193 购物期间的银行卡注册选项		
验证类型	购物期间激活		
结果	注册检查		验证检验
	汇总	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	详细信息	ACS URL URL	验证结果 1
		PAReq PAReq 值	AAV AAV 值
		proofXML proofXML 值	电子商务交易指示符 spa
		已注册 VERes Y	PARes 状态 A
		XID XID 值	XID XID 值
操作	借助此测试卡，您可以重现消费者在购买期间注册卡的流程。如果银行未注册银行卡，注册检查后，消费者的浏览器中会出现银行卡注册选项窗口。消费者可立即激活卡或稍后激活。在这两种情况下，都要对卡进行验证，并且验证要成功才会激活。 1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将所需的 3DS 验证值添加到授权请求。		

测试案例 33: Maestro 注册卡: 未完成验证

卡号	6331101250353227 不显示验证窗口		
验证类型	主动验证		
结果	注册检查		验证检验
	汇总	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。		发卡行无法执行验证。
	详细信息	ACS URL URL 值	验证结果 6
		PAReq PAReq 值	采集指示符 0
		proofXML proofXML 值	电子商务交易指示符 spa
		已注册 VERes Y	PARes 状态 U
		XID XID 值	XID XID 值
操作	要求消费者使用其他支付方式，或提交交易。无责任转移。		

测试案例 34: Maestro 注册卡: 验证失败

卡号	6331100610194313 不显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	用户未通过验证
	ACS URL URL 值	验证结果 9
	PAReq PAReq 值	PARes 状态 N
	proofXML proofXML 值	XID XID 值
	已注册 VERes Y	
	XID XID 值	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 35: Maestro 注册卡: 验证不可用

卡号	6331100266977839	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
详细信息	ics_pa_enroll 服务成功。	
	采集指示符 0	
	电子商务交易指示符 spa	
	proofXML proofXML 值	
操作	提交交易。无责任转移。	

测试案例 36: Maestro 注册卡: 验证错误

卡号	560000511607577094 不显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	我们遇到了一个 3DS 验证问题: 处理 PAREs 时出错。
	ACS URL URL 值	采集指示符 0
	PAREq PAREq 值	电子商务交易指示符 internet
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	请勿请求授权。而是应要求消费者使用其他支付方式。无责任转移。	

测试案例 37: Maestro 注册检查错误

卡号	560000841211092515	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
详细信息	ics_pa_enroll 服务成功。	
	采集指示符 0	
	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	继续处理授权请求, 并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权, 则会自动处理授权。	

American Express SafeKey

表 10 American Express SafeKey 回复字段的可能值

结果及说明		验证检验回复			
		验证结果	ECI	商务交易指示符	原因代码
成功	验证成功。	0	05	aesk	100
	有尝试验证的记录。	1	06	aesk_ attempted	100
失败（非消费者责任）	阻止验证完成的系统错误：可继续验证，但是无责任转移。	6	1	— ²	100
	发卡行无法执行验证。	6	07	internet	100
	验证未完成或不可用。		07	internet	
	PARes 无效。	-1	—	—	476
失败（消费者责任）	验证失败或持卡人未完成验证。 如果验证失败，Visa 会要求您不接受该卡。您必须要求消费者使用其他支付方式。	9	—	—	476

1 ECI 值因失败原因而异。
2 短划线 (—) 表示字段为空或不存在。

测试案例 38: American Express SafeKey 注册卡：验证成功

卡号	340000000003961	不显示验证窗口
	371449111020228	显示验证窗口
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	
	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	
	ACS URL URL 值	验证结果 0
	PAReq PAReq 值	CAVV CAVV 值
	proofXML proofXML 值	电子商务交易指示符 aesk
	已注册 VERes Y	ECI 05
	XID XID 值	PARes 状态 Y
		XID XID 值
操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。	

测试案例 39: American Express SafeKey 注册卡: 验证成功, 但 PAREs 无效

卡号	340000000006022		
验证类型	主动验证		
结果	注册检查	验证检验	
汇总	原因代码	475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。		我们遇到了一个 3DS 验证问题: PAREs 签名摘要值不匹配。PAREs 消息已被修改。
	ACS URL	URL 值	验证结果 -1
	PAReq	PAReq 值	XID XID 值
	proofXML	proofXML 值	
	已注册 VERes	Y	
	XID	XID 值	
操作	请勿继续进行验证。而是应要求消费者使用其他支付方式。		

测试案例 40: American Express SafeKey 注册卡: 尝试处理

卡号	340000000003391 不显示验证窗口	
	344400000000569 购物期间的银行卡注册选项	
验证类型	购物期间激活	
结果	注册检查	验证检验
	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	ACS URL URL 值	验证结果 1
	PAReq PAReq 值	CAVV CAVV 值
	proofXML proofXML 值	电子商务交易指示符 aesk_attempted
	已注册 VERes Y	ECI 06
	XID XID 值	PARes 状态 A
		XID XID 值
操作	如果您单独请求验证检验和授权服务，请按以下步骤进行操作： 1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。 如果您同时请求验证和授权服务，上述流程将自动进行。	

测试案例 41: American Express SafeKey 注册卡: 未完成验证

卡号	340000000002302 不显示验证窗口		
验证类型	主动验证		
结果	注册检查		验证检验
	汇总	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	详细信息	ACS URL URL 值	验证结果 6
		PAReq PAReq 值	电子商务交易指示符 internet
		proofXML proofXML 值	ECI 07
		已注册 VERes Y	PARes 状态 U
		XID XID 值	XID XID 值
	操作 要求消费者使用其他支付方式, 或提交交易。无责任转移。		

测试案例 42: American Express SafeKey 注册卡: 验证失败

卡号	340000000000033 不显示验证窗口		
验证类型	主动验证		
结果	注册检查		验证检验
	汇总	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。		- 用户未通过验证。 - 无法对支付人进行验证。
	详细信息	ACS URL URL 值	验证结果 9
		PAReq PAReq 值	PARes 状态 N
		proofXML proofXML 值	ECI 07
		已注册 VERes Y	XID XID 值
		XID XID 值	
	操作 您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。		

测试案例 43: American Express SafeKey 注册卡: 验证不可用

卡号	340000000007780	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	提交您的授权请求。无责任转移。	

测试案例 44: American Express SafeKey 注册卡: 验证错误

卡号	340000000009299	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	我们遇到了一个 3DS 验证问题: 处理 PAREs 时出错。
详细信息	ACS URL URL 值	ECI 07
	PARReq PARReq 值	电子商务交易指示符 internet
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 45: American Express SafeKey 未注册银行卡

卡号	340000000008135	
验证类型	非参与银行	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	ECI 07	
	proofXML proofXML 值	
	已注册 VERes N	
操作	提交交易。	

测试案例 46: American Express SafeKey 注册检查: 超时

卡号	340000000008309	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	ECI 07	
	proofXML proofXML 值	
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 47: American Express SafeKey 注册检查错误

卡号	340000000007244	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	继续处理授权请求，并联系支持代表解决问题。如果同时请求了 3DS 验证和授权，则会自动处理授权。无责任转移。	

JCB J/Secure

表 11 JCB J/Secure 回复字段的可能值

结果及说明		payerAuthValidateReply_			
		authentication Result	eci	commerceIndicator	reasonCode
成功	验证成功。	0	05	js	100
	有尝试验证的记录	1	06	js_attempted	100
失败（非消费者责任）	阻止验证完成的系统错误：可继续验证，但是无责任转移。	6	1	— ²	
	发卡行无法执行验证	6	07	internet	100
	验证未完成或不可用。		07	internet js_failure	
	PARes 无效。	-1	00		476
失败（消费者责任）	验证失败或持卡人未完成验证。 如果验证失败，Visa 会要求您不接受该卡。您必须要求消费者使用其他支付方式。	9	—	—	476

1 ECI 值因失败原因而异。

2 短划线 (—) 表示字段为空或不存在。

测试案例 48：JCB J/Secure 注册卡：验证成功

卡号	3569990010083722 不显示验证窗口	
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	
	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	
	ACS URL URL	验证结果 0
	PAReq PAReq 值	CAVV CAVV 值
	proofXML proofXML 值	电子商务交易指示符 js
	已注册 VERes Y	ECI 05
	XID XID 值	PARes 状态 Y
		XID XID 值
操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。	

测试案例 49: JCB J/Secure 注册卡: 验证成功, 但 PAREs 无效 (签名失败)

卡号	3569990010083748	
验证类型	主动验证	
结果	注册检查	验证检验
	汇总	原因代码 475
	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	验证结果	-1
	详细消息	XID 值
操作		

测试案例 50: JCB J/Secure 注册卡: 尝试验证

卡号	3569960010083758	
验证类型	购物期间激活	
结果	注册检查	验证检验
	汇总	原因代码 475
	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	验证结果	1
	详细消息	ics_pa_validate 服务成功。
	ACS URL	URL 值
	PAREq	PAREq 值
	proofXML	proofXML 值
	已注册 VERes	Y
	XID	XID 值
操作		

测试案例 51: JCB J/Secure 注册卡: 未完成验证 (不可用)

卡号	3541599998103643 不显示验证窗口		
验证类型	主动验证		
结果	注册检查		验证检验
	汇总	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。		■ 发卡行无法执行验证。 ■ ics_pa_validate 服务成功。
详细信息	ACS URL	URL 值	验证结果 6
	PAReq	PAReq 值	电子商务交易指示符 internet
	proofXML	proofXML 值	ECI 07
	已注册 VERes	Y	PARes 状态 U
	XID	XID 值	XID XID 值
操作	要求消费者使用其他支付方式, 或提交交易。无责任转移。		

测试案例 52: JCB J/Secure 注册卡: 验证失败

卡号	3569990110083721 不显示验证窗口		
验证类型	主动验证		
结果	注册检查		验证检验
	汇总	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。		■ 用户未通过验证。 ■ 无法对支付人进行验证。
详细信息	ACS URL	URL 值	验证结果 9
	PAReq	PAReq 值	PARes 状态 N
	proofXML	proofXML 值	XID XID 值
	已注册 VERes	Y	
	XID	XID 值	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。		

测试案例 53: JCB J/Secure 注册卡: 验证不可用

卡号	3541599999103865	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	提交您的授权请求。无责任转移。	

测试案例 54: JCB J/Secure 注册卡: 处理 PAREs 时发生验证错误

卡号	3541599999103881	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	我们遇到了一个 3DS 验证问题: 处理 PAREs 时出错。
详细信息	ACS URL URL 值	ECI 07
	PARReq PARReq 值	电子商务交易指示符 internet
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 55: JCB J/Secure 未注册银行卡

卡号	3569970010083724	
验证类型	非参与银行	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 js_attempted	
	ECI 06	
	proofXML proofXML 值	
	已注册 VERes N	
操作	提交您的授权请求。	

测试案例 56: JCB J/Secure 注册检查: 超时

卡号	3569980010083723	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 57: JCB J/Secure 注册检查: 处理消息请求时发生查询错误

卡号	3541599969103614	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	继续处理授权请求，并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权，则会自动处理授权。	

Diners Club ProtectBuy

表 12 Diners Club ProtectBuy 回复字段的可能值

结果及说明		验证检验回复			
		验证结果	ECI	商务交易指示符	原因代码
成功	验证成功。	0	05	pb	100
	有尝试验证的记录。	1	06	pb_ attempted	100
失败（非消费者责任）	阻止验证完成的系统错误：可继续验证，但是无责任转移。	6	1	— ²	100
	发卡行无法执行验证。	6	07	internet	100
	验证未完成或不可用。		07	internet	
	PARes 无效。	-1	—	—	476
失败（消费者责任）	验证失败或持卡人未完成验证。 如果验证失败，Visa 会要求您不接受该卡。您必须要求消费者使用其他支付方式。	9	—	—	476

1 ECI 值因失败原因而异。
2 短划线 (—) 表示字段为空或不存在。

测试案例 58: Diners Club ProtectBuy 注册卡：验证成功

卡号	3005000000006246		
验证类型	主动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。	
	详细信息	ACS URL URL	验证结果 0
		PAReq PAReq 值	CAVV CAVV 值
		proofXML proofXML 值	电子商务交易指示符 pb
		已注册 VERes Y	ECI 05
		XID XID 值	PARes 状态 Y
			XID XID 值
	操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。	

测试案例 59: Diners Club ProtectBuy 注册卡: 验证成功, 但 PAREs 无效

卡号	3005000000004373		
验证类型	主动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 476
	详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
		我们遇到了一个 3DS 验证问题: PAREs 签名摘要值不匹配。PAREs 消息已被修改。	
		ACS URL URL 值	验证结果 -1
		PAReq PAReq 值	XID XID 值
		proofXML proofXML 值	
		已注册 VERes Y	
		XID XID 值	
操作	请勿继续进行验证。而是应要求消费者使用其他支付方式。		

测试案例 60: Diners Club ProtectBuy 注册卡: 尝试处理

卡号	3005000000005271 购物期间的银行卡注册选项		
验证类型	购物期间激活		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 100
	详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
		ics_pa_validate 服务成功。	
		ACS URL URL 值	验证结果 1
		PAReq PAReq 值	CAVV CAVV 值
		proofXML proofXML 值	电子商务交易指示符 pb_attempted
		已注册 VERes Y	ECI 06
		XID XID 值	PAREs 状态 A
操作	如果您单独请求验证检验和授权服务, 请按以下步骤进行操作:		
	1 将签名的 PAREs 添加到验证请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。 如果您同时请求验证检验和授权服务, 上述流程将自动进行。		

测试案例 61: Diners Club ProtectBuy 注册卡: 未完成验证

卡号	3005000000007376		
验证类型	主动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 100
	详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
		■ 发卡行无法执行验证。 ■ ics_pa_validate 服务成功。	
		ACS URL URL 值	验证结果 6
		PAReq PAReq 值	电子商务交易指示符 internet
		proofXML proofXML 值	ECI 07
		已注册 VERes Y	PARes 状态 U
操作	XID XID 值		
	要求消费者使用其他支付方式, 或提交交易。无责任转移。		

测试案例 62: Diners Club ProtectBuy 注册卡: 验证失败

卡号	3005000000005925		
验证类型	主动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 476
	详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
		■ 用户未通过验证。 ■ 无法对支付人进行验证。	
		ACS URL URL 值	验证结果 9
		PAReq PAReq 值	PARes 状态 N
		proofXML proofXML 值	XID XID 值
		已注册 VERes Y	
操作	XID XID 值		
	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。		

测试案例 63: Diners Club ProtectBuy 注册卡: 验证不可用

卡号	3005000000006030	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	提交您的授权请求。无责任转移。	

测试案例 64: Diners Club ProtectBuy 注册卡: 验证错误

卡号	3005000000005602	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	我们遇到了一个 3DS 验证问题: 处理 PAREs 时出错。
详细信息	ACS URL URL 值	电子商务交易指示符 internet
	PARReq PARReq 值	ECI 07
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 65: Diners Club ProtectBuy 未注册银行卡

卡号	3005000000007269	
验证类型	非参与银行	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	ECI 07	
	proofXML proofXML 值	
	已注册 VERes N	
操作	提交交易。	

测试案例 66: Diners Club ProtectBuy 注册检查: 超时

卡号	3005000000001890	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 67: Diners Club ProtectBuy 注册检查错误

卡号	3005000000009877 错误响应	
	3005000000004837 配置不正确: 无法进行验证	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	继续处理授权请求, 并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权, 则会自动处理授权。	

Discover ProtectBuy

表 13 Discover ProtectBuy 回复字段的可能值

结果及说明		验证检验回复			
		验证结果	ECI	商务交易指示符	原因代码
成功	验证成功。	0	05	dipb	100
	有尝试验证的记录。	1	06	dipb_ attempted	100
失败（非消费者责任）	阻止验证完成的系统错误：可继续验证，但是无责任转移。	6	1	— ²	100
	发卡行无法执行验证。	6	07	internet	100
	验证未完成或不可用。		07	internet	
	PARes 无效。	-1	—	—	476
失败（消费者责任）	验证失败或持卡人未完成验证。 如果验证失败，Visa 会要求您不接受该卡。您必须要求消费者使用其他支付方式。	9	—	—	476

1 ECI 值因失败原因而异。
2 短划线 (—) 表示字段为空或不存在。

测试案例 68：Discover ProtectBuy 注册卡：验证成功

卡号	6011000000000004		
验证类型	主动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	详细信息	ACS URL URL	验证结果 0
		PAReq PAReq 值	CAVV CAVV 值
		proofXML proofXML 值	电子商务交易指示符 dipb
		已注册 VERes Y	ECI 05
		XID XID 值	PARes 状态 Y
			XID XID 值
	操作	1 将签名的 PARes 添加到验证检验请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。	

测试案例 69: Discover ProtectBuy 注册卡: 验证成功, 但 PAREs 无效

卡号	6011000000000012	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	我们遇到了一个 3DS 验证问题: PAREs 签名摘要值不匹配。PAREs 消息已被修改。
	ACS URL URL 值	验证结果 -1
	PAReq PAReq 值	XID XID 值
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	请勿继续进行验证。而是应要求消费者使用其他支付方式。	

测试案例 70: Discover ProtectBuy 注册卡: 尝试处理

卡号	6011000000000038 购物期间的银行卡注册选项	
验证类型	购物期间激活	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	ACS URL URL 值	验证结果 1
	PAReq PAReq 值	CAVV CAVV 值
	proofXML proofXML 值	电子商务交易指示符 dipb_attempted
	已注册 VERes Y	ECI 06
	XID XID 值	PAREs 状态 A
		XID XID 值
操作	如果您单独请求验证检验和授权服务, 请按以下步骤进行操作: 1 将签名的 PAREs 添加到验证请求。 2 确保注册检查中的 XID 与验证检验中的 XID 匹配。 3 将 CAVV 和 ECI 值添加到授权请求。 如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 71: Discover ProtectBuy 注册卡: 未完成验证

卡号	6011000000000103		
验证类型	主动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 100
	详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
		■ 发卡行无法执行验证。 ■ ics_pa_validate 服务成功。	
		ACS URL URL 值	验证结果 6
		PAReq PAReq 值	电子商务交易指示符 internet
		proofXML proofXML 值	ECI 07
		已注册 VERes Y	PARes 状态 U
操作	XID XID 值		
	要求消费者使用其他支付方式, 或提交交易。无责任转移。		

测试案例 72: Discover ProtectBuy 注册卡: 验证失败

卡号	6011000000000020		
验证类型	主动验证		
结果	注册检查	验证检验	
	汇总	原因代码 475	原因代码 476
	详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
		■ 用户未通过验证。 ■ 无法对支付人进行验证。	
		ACS URL URL 值	验证结果 9
		PAReq PAReq 值	PARes 状态 N
		proofXML proofXML 值	XID XID 值
		已注册 VERes Y	
操作	XID XID 值		
	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。		

测试案例 73: Discover ProtectBuy 注册卡: 验证不可用

卡号	6011000000000061	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	提交您的授权请求。无责任转移。	

测试案例 74: Discover ProtectBuy 注册卡: 验证错误

卡号	6011000000000095	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	我们遇到了一个 3DS 验证问题: 处理 PAREs 时出错。
详细信息	ACS URL URL 值	电子商务交易指示符 internet
	PARReq PARReq 值	ECI 07
	proofXML proofXML 值	
	已注册 VERes Y	
	XID XID 值	
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 75: Discover ProtectBuy 未注册银行卡

卡号	6011000000000053	
验证类型	非参与银行	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	ECI 07	
	proofXML proofXML 值	
	已注册 VERes N	
操作	提交交易。	

测试案例 76: Discover ProtectBuy 注册检查: 超时

卡号	6011000000000046	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 77: Discover ProtectBuy 注册检查错误

卡号	6011000000000087 错误响应	
	6011000000000079 配置不正确: 无法进行验证	
验证类型	主动验证	
结果	注册检查	验证检验
汇总	原因代码 100	
	ics_pa_enroll 服务成功。	
详细信息	电子商务交易指示符 internet	
	proofXML proofXML 值	
	已注册 VERes U	
操作	继续处理授权请求, 并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权, 则会自动处理授权。	

3D Secure 2.x 的测试案例

本节包含 Cardinal Cruise 混合集成或标准集成的测试案例。

请在测试中使用指定卡号，并将卡的失效日期设置为当前年份加三年，月份设置为 1 月。例如，对于 2019 年，请使用 2022 年。另外，您还必须填写订单要求的必填字段。



备注

基于遗留原因，3D Secure 2.x 的测试案例中也包含 XID 值。

Visa Secure

测试案例 2.1: Visa Secure 注册卡：无阻力验证成功

卡号	4000000000001000	
结果	注册检查	验证检验
	汇总	
	原因代码 100	NA
	ics_pa_enroll 服务成功。	
	详细信息	
	已注册 VERes Y	
	PARes 状态 Y	
	CAVV CAVV 值	
	电子商务交易指示符 vbv	
	ECI 05	
	XID XID 值	
操作	如果您分别请求验证检验和授权服务，请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务，上述流程将自动进行。	

测试案例 2.2: Visa Secure 注册卡: 无阻力验证不成功

卡号	4000000000001018	
结果	注册检查	验证检验
	汇总	
	原因代码 476	NA
	■ 用户未通过验证。 ■ 无法对支付人进行验证。	
	详细信息	
	已注册 VERes Y	
	PARes 状态 N	
	ECI 07	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.3: Visa Secure 注册卡: 尝试处理无阻力验证

卡号	4000000000001026	
结果	注册检查	验证检验
	汇总	
	原因代码 100	NA
	ics_pa_enroll 服务成功。	
	详细信息	
	已注册 VERes Y	
	PARes 状态 A	
	CAVV CAVV 值	
	电子商务交易指示符 vbv_attempted	
	ECI 06	
	XID XID 值	
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.4: Visa Secure 注册卡: 无阻力验证不可用

卡号	4000000000001034	
结果	注册检查	验证检验
	汇总	
	原因代码 100	NA
	ics_pa_enroll 服务成功。	
	详细信息	
	已注册 VERes Y	
	PARes 状态 U	
	电子商务交易指示符 internet	
	ECI 07	
操作	提交您的授权请求。无责任转移。	

测试案例 2.5: Visa Secure 注册卡: 无阻力验证被拒绝

卡号	4000000000001042	
结果	注册检查	验证检验
	汇总	原因代码 476 NA
	详细信息	■ 用户未通过验证。 ■ 无法对支付人进行验证。
		已注册 VERes Y
		PARes 状态 R
		ECI 07
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.6: Visa Secure 注册卡: 查询时验证不可用

卡号	4000000000001059	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	详细信息	ics_pa_enroll 服务成功。
		已注册 VERes U
		电子商务交易指示符 internet
		ECI 07
操作	提交您的授权请求。无责任转移。	

测试案例 2.7: Visa Secure 注册检查错误

卡号	4000000000001067	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	详细信息	ics_pa_enroll 服务成功。
		已注册 VERes U
		电子商务交易指示符 internet
操作	继续处理授权请求, 并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权, 则会自动处理授权。	

测试案例 2.8: Visa Secure 注册检查: 超时

卡号	4000000000001075	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	PARes 状态 U
	电子商务交易指示符	internet
	ECI	07
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 2.9: Visa Secure 绕过验证

卡号	4000000000001083	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes B
	电子商务交易指示符	internet
	操作	提交您的授权请求。无责任转移。

测试案例 2.10a: Visa Secure 注册卡: 加强验证成功 (混合)

卡号	4000000000001091	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	ics_pa_validate 服务成功。	
	详细信息	已注册 VERes Y
	PAReq	PAReq 值 PARes 状态 Y
	ACS URL	URL 值 CAVV CAVV 值
	XID	XID 值 电子商务交易指示符 vbv
		ECI 05
		XID XID 值
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.10b: Visa Secure 注册卡: 加强验证成功 (标准)

卡号	4000000000001091	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	Y
	CAVV	CAVV 值
	电子商务交易指示符	vbv
	ECI	05
	XID	XID 值
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.11a: Visa Secure 注册卡: 加强验证不成功 (混合)

卡号	4000000000001109	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	详细信息	- 用户未通过验证。 - 无法对支付人进行验证。
	已注册 VERes	Y
	PAReq	PAReq 值
	ACS URL	URL 值
	PARes 状态	N
	ECI	07
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.11b: Visa Secure 注册卡: 加强验证不成功 (标准)

卡号	4000000000001109	
结果	注册检查	验证检验
	汇总	原因代码 476 NA
	- 用户未通过验证。 - 无法对支付人进行验证。	
	详细信息	已注册 VERes Y
	PARes 状态	N
	ECI	07
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.12a: Visa Secure 注册卡: 加强验证不可用 (混合)

卡号	4000000000001117	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	已注册 VERes Y
	PAReq PAReq 值	PARes 状态 U
	ACS URL URL 值	电子商务交易指示符 internet
		ECI 07
操作	重新尝试验证, 或在无责任转移的情况下处理交易。	

测试案例 2.12b: Visa Secure 注册卡: 加强验证不可用 (标准)

卡号	4000000000001117	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态 U	
	电子商务交易指示符 internet	
	ECI 07	
操作	重新尝试验证, 或在无责任转移的情况下处理交易。	

测试案例 2.13a: Visa Secure 注册卡: 未完成验证 (混合)

卡号	4000000000001125	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	已注册 VERes Y
	PAReq PAReq 值	PARes 状态 U
	ACS URL URL 值	电子商务交易指示符 internet
		ECI 07
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 2.13b: Visa Secure 注册卡: 未完成验证 (标准)

卡号	4000000000001125	
结果	注册检查	验证检验
	汇总	
	原因代码 100	NA
	ics_pa_enroll 服务成功。	
	详细信息	
	已注册 VERes Y	
	PARes 状态 U	
操作	电子商务交易指示符 internet	
	ECI 07	
	要求消费者使用其他支付方式。无责任转移。	

测试案例 2.14a: Visa Secure 注册卡: 加强验证绕过商户 (混合)

卡号	4000000000001133	
结果	注册检查	验证检验
	汇总	
	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	
	已注册 VERes Y	
	PAReq PAReq 值	PARes 状态 B
操作	ACS URL URL 值	电子商务交易指示符 internet
		ECI 07
	提交您的授权请求。无责任转移。	

测试案例 2.14b: Visa Secure 注册卡: 加强验证绕过商户 (标准)

卡号	4000000000001133	
结果	注册检查	验证检验
	汇总	
	原因代码 100	NA
	ics_pa_enroll 服务成功。	
	详细信息	
	已注册 VERes Y	
	PARes 状态 B	
操作	电子商务交易指示符 internet	
	ECI 07	
	提交您的授权请求。无责任转移。	

Mastercard Identity Check



备注

注册检查和验证检验服务的回复中包含 3D Secure 版本和目录服务器交易 ID，但本节的 Mastercard 测试案例未将其列入。测试案例即将更新，新版案例会列入这些字段。

测试案例 2.15: Mastercard Identity Check 注册卡：无阻力验证成功

卡号	5200000000001005	
结果	注册检查	验证检验
	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	已注册 VERes	Y
	PARes 状态	Y
	AAV	AAV 值
	电子商务交易指示符	spa
	采集指示符	2
	XID	XID 值
操作	如果您分别请求验证检验和授权服务，请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务，上述流程将自动进行。	

测试案例 2.16: Mastercard Identity Check 注册卡：无阻力验证不成功

卡号	5200000000001013	
结果	注册检查	验证检验
	原因代码 476	NA
详细信息	- 用户未通过验证。 - 无法对支付人进行验证。	
	已注册 VERes	Y
	PARes 状态	N
	采集指示符	0
操作	您不可以提交此交易进行授权，而是应要求消费者使用其他支付方式。	

测试案例 2.17: Mastercard Identity Check 注册卡：尝试处理无阻力验证

卡号	5200000000001021	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	A
	AAV	AAV 值
	电子商务交易指示符	spa
	采集指示符	1
	XID	XID 值
操作	如果您分别请求验证检验和授权服务，请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务，上述流程将自动进行。	

测试案例 2.18: Mastercard Identity Check 注册卡：无阻力验证不可用

卡号	5200000000001039	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	U
	电子商务交易指示符	internet
	采集指示符	0
操作	提交您的授权请求。无责任转移。	

测试案例 2.19: Mastercard Identity Check 注册卡：无阻力验证被拒绝

卡号	5200000000001047	
结果	注册检查	验证检验
	汇总	原因代码 476 NA
	- 用户未通过验证。 - 无法对支付人进行验证。	
	详细信息	已注册 VERes Y
	PARes 状态	R
	采集指示符	0
操作	您不可以提交此交易进行授权，而是应要求消费者使用其他支付方式。	

测试案例 2.20: Mastercard Identity Check 注册卡：查询时验证不可用

卡号	5200000000001054	
结果	注册检查	验证检验
汇总	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	已注册 VERes U	
	电子商务交易指示符 internet	
	采集指示符 0	
操作	提交您的授权请求。无责任转移。	

测试案例 2.21: Mastercard Identity Check 注册检查错误

卡号	5200000000001062	
结果	注册检查	验证检验
汇总	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	已注册 VERes U	
	电子商务交易指示符 internet	
	采集指示符 0	
操作	继续处理授权请求，并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权，则会自动处理授权。	

测试案例 2.22: Mastercard Identity Check 注册检查：超时

卡号	5200000000001070	
结果	注册检查	验证检验
汇总	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	PARes 状态 U	
	电子商务交易指示符 internet	
	采集指示符 0	
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 2.23: Mastercard Identity Check 绕过验证

卡号	5200000000001088	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes B
	电子商务交易指示符	internet
	采集指示符	0
操作	提交您的授权请求。无责任转移。	

测试案例 2.24a: Mastercard Identity Check 注册卡: 加强验证成功 (混合)

卡号	5200000000001096	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	ics_pa_validate 服务成功。	
	详细信息	已注册 VERes Y
	PAReq	PAReq 值 PARes 状态 Y
	ACS URL	URL 值 AAV AAV 值
	XID	XID 值 电子商务交易指示符 spa
		采集指示符 2
		XID XID 值
操作	如果您分别请求验证检验和授权服务，请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务，上述流程将自动进行。	

测试案例 2.24b: Mastercard Identity Check 注册卡: 加强验证成功 (标准)

卡号	5200000000001096	
结果	注册检查	验证检验
	汇总	
	原因代码 100	NA
	ics_pa_enroll 服务成功。	
	已注册 VERes Y	
	PARes 状态 Y	
	AAV AAV 值	
	电子商务交易指示符 spa	
	采集指示符 2	
操作	XID XID 值	
	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.25a: Mastercard Identity Check 注册卡: 加强验证不成功 (混合)

卡号	5200000000001104	
结果	注册检查	验证检验
	汇总	
	原因代码 475	原因代码 476
	持卡人已注册 3DS 验证。请在授权之前进行验证。	- 用户未通过验证。 - 无法对支付人进行验证。
	已注册 VERes Y	
	PAReq PAReq 值	PARes 状态 N
	ACS URL URL 值	采集指示符 0
	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.25b: Mastercard Identity Check 注册卡: 加强验证不成功 (标准)

卡号	5200000000001104	
结果	注册检查	验证检验
	汇总	
	原因代码 476	NA
	- 用户未通过验证。 - 无法对支付人进行验证。	
	已注册 VERes Y	
	PARes 状态 N	
	采集指示符 0	
	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.26a: Mastercard Identity Check 注册卡：加强验证不可用（混合）

卡号	5200000000001112	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	已注册 VERes Y
	PAReq PAReq 值	PARes 状态 U
	ACS URL URL 值	电子商务交易指示符 internet
		采集指示符 0
操作	重新尝试验证，或在无责任转移的情况下处理交易。	

测试案例 2.26b: Mastercard Identity Check 注册卡：加强验证不可用（标准）

卡号	5200000000001112	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态 U	
	电子商务交易指示符 internet	
	采集指示符 0	
操作	重新尝试验证，或在无责任转移的情况下处理交易。	

测试案例 2.27a: Mastercard Identity Check 注册卡：未完成验证（混合）

卡号	5200000000001120	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	已注册 VERes Y
	PAReq PAReq 值	PARes 状态 U
	ACS URL URL 值	电子商务交易指示符 internet
		采集指示符 0
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 2.27b: Mastercard Identity Check 注册卡: 未完成验证 (标准)

卡号	5200000000001120	
结果	注册检查	验证检验
汇总	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	已注册 VERes Y	
	PARes 状态 U	
	电子商务交易指示符 internet	
	采集指示符 0	
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 2.28a: Mastercard Identity Check 注册卡: 加强验证绕过商户 (混合)

卡号	5200000000001138	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	已注册 VERes Y	
	PAReq PAReq 值	PARes 状态 B
	ACS URL URL 值	电子商务交易指示符 internet
		采集指示符 0
操作	提交您的授权请求。无责任转移。	

测试案例 2.28b: Mastercard Identity Check 注册卡: 加强验证绕过商户 (标准)

卡号	5200000000001138	
结果	注册检查	验证检验
汇总	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	已注册 VERes Y	
	PARes 状态 B	
	电子商务交易指示符 internet	
	采集指示符 0	
操作	提交您的授权请求。无责任转移。	

American Express SafeKey

测试案例 2.29: American Express SafeKey 注册卡: 无阻力验证成功

卡号	340000000001007	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	Y
	CAVV	CAVV 值
	电子商务交易指示符	aesk
	ECI	05
	XID	XID 值
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.30: American Express SafeKey 注册卡: 无阻力验证不成功

卡号	340000000001015	
结果	注册检查	验证检验
	汇总	原因代码 476 NA
	- 用户未通过验证。 - 无法对支付人进行验证。	
	详细信息	已注册 VERes Y
	PARes 状态	N
	ECI	07
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.31: American Express SafeKey 注册卡: 尝试处理无阻力验证

卡号	340000000001023	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	A
	CAVV	CAVV 值
	电子商务交易指示符	aesk_attempted
	ECI	06
	XID	XID 值
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.32: American Express SafeKey 注册卡: 无阻力验证不可用

卡号	340000000001031	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	U
	电子商务交易指示符	internet
	ECI	07
操作	提交您的授权请求。无责任转移。	

测试案例 2.33: American Express SafeKey 注册卡: 无阻力验证被拒绝

卡号	340000000001049	
结果	注册检查	验证检验
	汇总	原因代码 476 NA
	- 用户未通过验证。 - 无法对支付人进行验证。	
	详细信息	已注册 VERes Y
	PARes 状态	R
	ECI	07
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.34: American Express SafeKey 注册卡: 查询时验证不可用

卡号	340000000001056	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes U
	电子商务交易指示符	internet
	ECI	07
操作	提交您的授权请求。无责任转移。	

测试案例 2.35: American Express SafeKey 注册检查错误

卡号	340000000001064	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes U
	电子商务交易指示符	internet
	ECI	07
操作	继续处理授权请求，并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权，则会自动处理授权。	

测试案例 2.36: American Express SafeKey 注册检查: 超时

卡号	340000000001072	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes U
	电子商务交易指示符	internet
	ECI	07
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 2.37: American Express SafeKey 绕过验证

卡号	340000000001080	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes B
	电子商务交易指示符	internet
	ECI	07
操作	提交您的授权请求。无责任转移。	

测试案例 2.38a: American Express SafeKey 注册卡: 加强验证成功 (混合)

卡号	340000000001098	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	ics_pa_validate 服务成功。	
	详细信息	已注册 VERes Y
	PAReq	PAReq 值 PARes 状态 Y
	ACS URL	URL 值 CAVV CAVV 值
	XID	XID 值 电子商务交易指示符 aesk
		ECI 05
		XID XID 值
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.38b: American Express SafeKey 注册卡: 加强验证成功 (标准)

卡号	340000000001098	
结果	注册检查	验证检验
汇总	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	已注册 VERes Y	
	PARes 状态 Y	
	CAVV CAVV 值	
	电子商务交易指示符 aesk	
	ECI 05	
	XID XID 值	
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.39a: American Express SafeKey 注册卡: 加强验证不成功 (混合)

卡号	340000000001106	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	- 用户未通过验证。 - 无法对支付人进行验证。
	已注册 VERes Y	
	PAReq PAReq 值	PARes 状态 N
	ACS URL URL 值	ECI 07
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.39b: American Express SafeKey 注册卡: 加强验证不成功 (标准)

卡号	340000000001106	
结果	注册检查	验证检验
汇总	原因代码 476	NA
详细信息	- 用户未通过验证。 - 无法对支付人进行验证。	
	已注册 VERes Y	
	PARes 状态 N	
	ECI 07	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.40a: American Express SafeKey 注册卡: 加强验证不可用 (混合)

卡号	340000000001114		
结果	注册检查		验证检验
	原因代码	475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	已注册 VERes	Y	
	PAReq	PAReq 值	PARes 状态 U
	ACS URL	URL 值	电子商务交易指示符 internet
			ECI 07
操作	重新尝试验证, 或在无责任转移的情况下处理交易。		

测试案例 2.40b: American Express SafeKey 注册卡: 加强验证不可用 (标准)

卡号	340000000001114		
结果	注册检查		验证检验
	原因代码	100	NA
详细信息	ics_pa_enroll 服务成功。		
	已注册 VERes	Y	
	PARes 状态	U	
	电子商务交易指示符	internet	
	ECI	07	
操作	重新尝试验证, 或在无责任转移的情况下处理交易。		

测试案例 2.41a: American Express SafeKey 注册卡: 未完成验证 (混合)

卡号	340000000001122		
结果	注册检查		验证检验
	原因代码	475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	已注册 VERes	Y	
	PAReq	PAReq 值	PARes 状态 U
	ACS URL	URL 值	电子商务交易指示符 internet
			ECI 07
操作	要求消费者使用其他支付方式。无责任转移。		

测试案例 2.41b: American Express SafeKey 注册卡: 未完成验证 (标准)

卡号	340000000001122	
结果	注册检查	验证检验
	汇总	
	原因代码 100	NA
	ics_pa_enroll 服务成功。	
	详细信息	
	已注册 VERes Y	
	PARes 状态 U	
操作	电子商务交易指示符 internet	
	ECI 07	
	要求消费者使用其他支付方式。无责任转移。	

测试案例 2.42a: American Express SafeKey 注册卡: 加强验证绕过商户 (混合)

卡号	3400000000001130	
结果	注册检查	验证检验
	汇总	
	原因代码 475	原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	ics_pa_validate 服务成功。
	详细信息	
	已注册 VERes Y	
	PAReq PAReq 值	PARes 状态 B
操作	ACS URL URL 值	电子商务交易指示符 internet
		ECI 07
	提交您的授权请求。无责任转移。	

测试案例 2.42b: American Express SafeKey 注册卡: 加强验证绕过商户 (标准)

卡号	3400000000001130	
结果	注册检查	验证检验
	汇总	
	原因代码 100	NA
	ics_pa_enroll 服务成功。	
	详细信息	
	已注册 VERes Y	
	PARes 状态 B	
操作	电子商务交易指示符 internet	
	ECI 07	
	提交您的授权请求。无责任转移。	

Discover ProtectBuy

测试案例 2.43: Discover ProtectBuy 注册卡: 无阻力验证成功

卡号	6011000000001002	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	Y
	CAVV	CAVV 值
	电子商务交易指示符	dipb
	ECI	05
	XID	XID 值
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.44: Discover ProtectBuy 注册卡: 无阻力验证不成功

卡号	6011000000001010	
结果	注册检查	验证检验
	汇总	原因代码 476 NA
	- 用户未通过验证。 - 无法对支付人进行验证。	
	详细信息	已注册 VERes Y
	PARes 状态	N
	ECI	07
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.45: Discover ProtectBuy 注册卡: 尝试处理无阻力验证

卡号	6011000000001028	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	A
	CAVV	CAVV 值
	电子商务交易指示符	dipb_attempted
	ECI	06
	XID	XID 值
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.46: Discover ProtectBuy 注册卡: 无阻力验证不可用

卡号	6011000000001036	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes Y
	PARes 状态	U
	电子商务交易指示符	internet
	ECI	07
操作	提交您的授权请求。无责任转移。	

测试案例 2.47: Discover ProtectBuy 注册卡：无阻力验证被拒绝

卡号	6011000000001044	
结果	注册检查	验证检验
	汇总	原因代码 476 NA
	■ 用户未通过验证。 ■ 无法对支付人进行验证。	
	详细信息	已注册 VERes Y
	PARes 状态	R
	ECI	07
操作	您不可以提交此交易进行授权，而是应要求消费者使用其他支付方式。	

测试案例 2.48: Discover ProtectBuy 注册卡：查询时验证不可用

卡号	6011000000001051	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes U
	电子商务交易指示符	internet
	ECI	07
操作	提交您的授权请求。无责任转移。	

测试案例 2.49: Discover ProtectBuy 注册检查错误

卡号	6011000000001069	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes U
	电子商务交易指示符	internet
	ECI	07
操作	继续处理授权请求，并联系支持代表解决问题。无责任转移。如果同时请求了 3DS 验证和授权，则会自动处理授权。	

测试案例 2.50: Discover ProtectBuy 注册检查: 超时

卡号	6011000000001077	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes U
	电子商务交易指示符	internet
	ECI	07
操作	10-12 秒后继续处理授权请求。无责任转移。	

测试案例 2.51: Discover ProtectBuy 绕过验证

卡号	6011000000001085	
结果	注册检查	验证检验
	汇总	原因代码 100 NA
	ics_pa_enroll 服务成功。	
	详细信息	已注册 VERes B
	电子商务交易指示符	internet
	ECI	07
操作	提交您的授权请求。无责任转移。	

测试案例 2.52a: Discover ProtectBuy 注册卡: 加强验证成功 (混合)

卡号	6011000000001093	
结果	注册检查	验证检验
	汇总	原因代码 475 原因代码 100
	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	ics_pa_validate 服务成功。	
	详细信息	已注册 VERes Y
	PAReq	PAReq 值 PARes 状态 Y
	ACS URL	URL 值 CAVV CAVV 值
	XID	XID 值 电子商务交易指示符 dipb
		ECI 05
		XID XID 值
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.52b: Discover ProtectBuy 注册卡: 加强验证成功 (标准)

卡号	6011000000001093	
结果	注册检查	验证检验
	原因代码 100	NA
汇总	ics_pa_enroll 服务成功。	
详细信息	已注册 VERes Y	
	PARes 状态 Y	
	CAVV CAVV 值	
	电子商务交易指示符 dipb	
	ECI 05	
	XID XID 值	
操作	如果您分别请求验证检验和授权服务, 请在授权请求中添加所需的 3DS 验证值。如果您同时请求验证检验和授权服务, 上述流程将自动进行。	

测试案例 2.53a: Discover ProtectBuy 注册卡: 加强验证不成功 (混合)

卡号	6011000000001101	
结果	注册检查	验证检验
	原因代码 475	原因代码 476
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	- 用户未通过验证。 - 无法对支付人进行验证。	
	已注册 VERes Y	
	PAReq PAReq 值	PARes 状态 N
	ACS URL URL 值	ECI 07
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.53b: Discover ProtectBuy 注册卡: 加强验证不成功 (标准)

卡号	6011000000001101	
结果	注册检查	验证检验
	原因代码 476	NA
详细信息	- 用户未通过验证。 - 无法对支付人进行验证。	
	已注册 VERes Y	
	PAReq 状态 N	
	ECI 07	
操作	您不可以提交此交易进行授权, 而是应要求消费者使用其他支付方式。	

测试案例 2.54a: Discover ProtectBuy 注册卡: 加强验证不可用 (混合)

卡号	6011000000001119		
结果	注册检查		验证检验
	原因代码	475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	已注册 VERes	Y	
	PAReq	PAReq 值	PARes 状态 U
	ACS URL	URL 值	电子商务交易指示符 internet
			ECI 07
操作	重新尝试验证, 或在无责任转移的情况下处理交易。		

测试案例 2.54b: Discover ProtectBuy 注册卡: 加强验证不可用 (标准)

卡号	6011000000001119		
结果	注册检查		验证检验
	原因代码	100	NA
详细信息	ics_pa_enroll 服务成功。		
	已注册 VERes	Y	
	PARes 状态	U	
	电子商务交易指示符	internet	
	ECI	07	
操作	重新尝试验证, 或在无责任转移的情况下处理交易。		

测试案例 2.55a: Discover ProtectBuy 注册卡: 未完成验证 (混合)

卡号	6011000000001127		
结果	注册检查		验证检验
	原因代码	475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。		ics_pa_validate 服务成功。
	已注册 VERes	Y	
	PAReq	PAReq 值	PARes 状态 U
	ACS URL	URL 值	电子商务交易指示符 internet
			ECI 07
操作	要求消费者使用其他支付方式。无责任转移。		

测试案例 2.55b: Discover ProtectBuy 注册卡: 未完成验证 (标准)

卡号	6011000000001127	
结果	注册检查	验证检验
汇总	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	已注册 VERes Y	
	PARes 状态 U	
	电子商务交易指示符 internet	
	ECI 07	
操作	要求消费者使用其他支付方式。无责任转移。	

测试案例 2.56a: Discover ProtectBuy 注册卡: 加强验证绕过商户 (混合)

卡号	6011000000001135	
结果	注册检查	验证检验
汇总	原因代码 475	原因代码 100
详细信息	持卡人已注册 3DS 验证。请在授权之前进行验证。	
	已注册 VERes Y	ics_pa_validate 服务成功。
	PAReq PAReq 值	PARes 状态 B
	ACS URL URL 值	电子商务交易指示符 internet
		ECI 07
操作	提交您的授权请求。无责任转移。	

测试案例 2.56b: Discover ProtectBuy 注册卡: 加强验证绕过商户 (标准)

卡号	6011000000001135	
结果	注册检查	验证检验
汇总	原因代码 100	NA
详细信息	ics_pa_enroll 服务成功。	
	已注册 VERes Y	
	PARes 状态 B	
	电子商务交易指示符 internet	
	ECI 07	
操作	提交您的授权请求。无责任转移。	

API 字段

此附录介绍可用于访问 CyberSource 3DS 验证服务的 Simple Order API 字段。API 和客户工具包可从 CyberSource 网站下载，网址如下：

http://www.cybersource.com/developers/develop/integration_methods/simple_order_and_soap_toolkit_api/

格式限制

除非另有说明，所有字段名称均区分大小写，所有字段均接受特殊字符，例如 @、# 和 %。



备注

item_# 字段的值不得包含脱字符 (^) 或冒号 (:)，因为这些字符为 CyberSource 服务专用字符。

对于 Atos，**billTo** 字段不得包含冒号 (:)。

所有请求字段的值均不得包含新行或回车符。但是，可包含嵌入空格和任何其他可打印字符。将删除所有前导和后缀空格。

数据类型定义

有关数据类型的详细信息，请参阅“万维网联盟 (W3C) XML 模式第 2 部分：数据类型说明”：

<http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>

数据类型	说明
Integer	整数 {..., -3, -2, -1, 0, 1, 2, 3, ...}。
String	由字母、数字、空格和特殊字符（例如 @ 和 #）组成的序列。

编号元素

CyberSource XML 架构包含多个计数元素。您可在请求中多次加入这些复杂元素。例如，当消费者的订单包含多种商品时，就必须在请求中加入多个 `<item>` 元素。每个商品都会编号，从 0 开始。XML 架构在商品的开始标记中使用 `id` 属性表示该编号。例如：

```
<item id="0">
```

作为名称-值对字段名称，此标记将显示为 **item_0**。在字段名称的这个部分，编号前的下划线不表示 XML 架构中的层次结构。商品字段在文档中一般指的是 **item_#_<element name>**。

以下是一个编号 `<item>` 元素和对应名称-值对字段名称的示例。如果使用 Simple Object Access Protocol (SOAP)，客户将包含对应的 `Item` 类。

示例 7 编号 XML 架构元素名称和名称-值对字段名称

XML 架构元素名称	对应的名称-值对字段名称
<code><item id="0"></code> <code><unitPrice></code> <code><quantity></code> <code></item></code>	item_0_unitPrice item_0_quantity
<code><item id="1"></code> <code><unitPrice></code> <code><quantity></code> <code></item></code>	item_1_unitPrice item_1_quantity



重要说明

当请求为 XML 格式并包含 `<item>` 元素时，该元素必包含 `id` 属性。例如：
`<item id="0">`。

请求字段

有关通过 Simple Order API 访问使用名称-值对或 XML 的 CyberSource 服务的详细信息，请参阅 [使用 Simple Order API 的信用卡服务 \(PDF | HTML\)](#) 和 [CyberSource Advanced 入门 \(PDF | HTML\)](#)。



备注

下表中的字段仅针对注册和检验服务。有关验证字段的详细信息，请参阅 [使用 Simple Order API 的信用卡服务 \(PDF | HTML\)](#)。

表 14 请求字段

字段名称	说明	必填/可选	类型和长度
airlineData_leg_#_carrierCode	这个航段航空公司的国际航空运输协会 (IATA) 代码。 对于每个航段均为必填字段。 对于旅行相关请求的 American Express SafeKey 为必填字段。	注册 (O)	String (2)
airlineData_leg_#_departureDate	旅程第一个航段的出发日期。格式：YYYYMMDD。 对于旅行相关请求的 American Express SafeKey 为必填字段。 备注 编号元素名称应包含 0，不包含 #。 3DS 验证服务仅使用旅程第一个航段。请参阅第 120 页，“编号元素”。	注册 (O)	Integer (8)
airlineData_leg_#_destination	这个航段目的机场的国际航空运输协会 (IATA) 代码。 对于每个航段均为必填字段。 对于旅行相关请求的 American Express SafeKey 为必填字段。	注册 (O)	String (5)
airlineData_leg_#_originatingAirportCode	第一航段出发机场的国际航空运输协会 (IATA) 代码。 对于旅行相关请求的 American Express SafeKey 为必填字段。	注册 (O)	String (5)
airlineData_numberOfPassengers	收票旅客数量。如果未在请求中包含此字段，CyberSource 将使用默认值 1。 对于旅行相关请求的 American Express SafeKey 为必填字段。	注册 (O)	Integer (3)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
airlineData_passenger_#_firstName	收票旅客的名字。如果有多位旅客，请加入机票上列出的所有旅客。 请勿使用逗号、连字符或撇号等特殊字符。仅支持 ASCII 字符。 对于旅行相关请求的 American Express SafeKey 为必填字段。	注册 (O)	String (60)
airlineData_passenger_#_lastName	收票旅客的姓氏。如果有多位旅客，请加入机票上列出的所有旅客。 请勿使用逗号、连字符或撇号等特殊字符。仅支持 ASCII 字符。 对于旅行相关请求的 American Express SafeKey 为必填字段。	注册 (O)	String (60)
billTo_city	账单地址所在的城市。	注册 (R)	String (50)
billTo_country	账户的账单地址所在的国家/地区。应使用 两字符国家/地区代码 。	注册 (R)	String (2)
billTo_customerAccountChangeDate	持卡人账户的最后变更日期。变更包括账单或送货地址变更、新增支付账户或新增用户。 此字段可包含以下其中一个值： ■ -1：来宾账户 ■ 0：本次交易期间发生变更 如果两个选项均不适用，请按 YYYYMMDD 格式输入日期。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (8)
billTo_customerAccountCreateDate	持卡人开立账户的日期。 此字段可包含以下其中一个值： ■ -1：来宾账户 ■ 0：本次交易期间开立 如果两个选项均不适用，请按 YYYYMMDD 格式输入日期。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (8)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
billTo_customerAccountPasswordChangeDate	持卡人最后更改或重置账户密码的日期。 此字段可包含以下其中一个值： ■ -1：来宾账户 ■ 0：本次交易期间发生变更 如果两个选项均不适用，请按 YYYYMMDD 格式输入日期。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (8)
billTo_email	消费者的电子邮箱地址，包括完整的域名。使用以下格式：name@host.domain（例如 jdoe@example.com）。	注册 (R)	String (255)
billTo_firstName	消费者的名字。此值应与卡上所示的名字相同。	注册 (R)	String (60)
billTo_ipAddress	网络服务器通过套接字信息报告的消费者 IP 地址，例如 10.1.27.63。	注册 (O)	String (45)
billTo_lastName	消费者的姓氏。此值应与卡上所示的姓氏相同。	注册 (R)	String (60)
billTo_passportCountry	持卡人护照的签发国家/地区。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (3)
billTo_passportNumber	持卡人的护照号码。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	String (40)
billTo_phoneNumber	消费者的电话号码。 对于美国或加拿大以外的国家/地区，如果可以，请在电话号码开头添加国家/地区代码。否则，将使用账单地址所在国家/地区确定国家/地区代码。	注册 (O)	String (15)
billTo_postalCode	账单地址的邮政编码。邮政编码必须由 5 到 9 位数字组成。 当账单国家/地区为美国时，9 位邮政编码必须采用以下格式： [5 位数字][短划线][4 位数字] 示例 12345-6789 当账单国家/地区为加拿大时，6 位邮政编码必须采用以下格式： [字母][数字][字母][空格] [数字][字母][数字] 示例 A1B 2C3 仅在 billTo_country 字段为 US 或 CA 时为必填。	注册 (R)	String (10)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
billTo_state	消费者所在州或省。对于美国和加拿大为必填字段。应使用 两字符州、省或领地代码 。	注册 (R)	String (2)
billTo_street1	信用卡发卡机构记录上的账单地址的第一行。	注册 (R)	String (60)
billTo_street2	其他地址信息，例如： <i>收件人：应付账款</i>	注册 (O)	String (60)
card_accountNumber	消费者的卡号。	注册 (R) 检验 (O)	Integer (20)
card_cardType	卡类型。有关详细信息，请参阅 使用 Simple Order API 的信用卡服务 (PDF HTML) 。此字段包含以下其中一个值： ■ 001: Visa ■ 002: Mastercard ■ 003: American Express ■ 004: Discover ■ 005: Diners Club ■ 007: JCB ■ 024: Maestro (UK Domestic) ■ 042: Maestro (International)	注册 (R) 检验 (R)	String (3)
card_expirationMonth	信用卡到期月份 (MM)。如果包含 card_accountNumber ，则对检验服务为必填字段。	注册 (R) 检验 (O)	String (2)
card_expirationYear	信用卡到期年份 (YYYY)。如果包含 card_accountNumber ，则对检验服务为必填字段。	注册 (R) 检验 (O)	String (4)
item_#_passengerFirstName	旅客的名字。 请参阅 第 120 页 ，“编号元素”。	注册 (O)	String (60)
item_#_passengerLastName	旅客的姓氏。 请参阅 第 120 页 ，“编号元素”。	注册 (O)	String (60)
item_#_productDescription	商品的简要说明。	注册 (O)	String (256)
item_#_productName	产品的名称。 请参阅 第 120 页 ，“编号元素”。	注册 (O)	String (255)
item_#_productSKU	商户产品标识码。 请参阅 第 120 页 ，“编号元素”。	注册 (O)	String (255)
item_#_quantity	所购买产品的数量。默认值为 1。 请参阅 第 120 页 ，“编号元素”。	注册 (O)	非负 Integer (10)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
item_#_unitPrice	产品单价。该值不能为负。该金额将会截断为正确的小数位数。可在此字段中包含小数点 (.)，但是不得包含任何其他特殊字符。 备注 如果使用 <code>purchaseTotals_grandTotalAmount</code> 字段，则 <code>item_#_unitPrice</code> 字段为可选字段。 请参阅第 120 页，“编号元素”。	注册 (R) 检验 (R)	String (15)
merchantDefinedData_ mddField_1 至 merchantDefinedData_ mddField_5	可用于存储信息的字段。值显示在 Business Center 的“案例管理详细信息”窗口中。前四个字段与“安全数据”服务使用的字段相同。这些字段仅可在参考目标 API 1.75 版或更高版本时使用。 重要说明 这些字段将覆盖旧的商户定义字段。例如，如果在同一个请求中使用旧字段 <code>merchantDefinedData_field15</code> 和新字段 <code>merchantDefinedData_mddField_15</code>，新字段的值将覆盖旧字段中指定的值。 警告 商户定义字段不能且不得用于获取个人识别信息。因此，商户不得在商户定义字段中或通过商户定义字段采集、获取和/或传输任何个人识别信息。个人识别信息包括（但不限于）：地址、信用卡卡号、社会保障号码、驾驶执照编号、公民身份证号码、护照号码和信用卡验证码 (CVV、CVC2、CVV2、CID、CVN)。如果 CyberSource 发现商户通过商户定义字段获取和/或传输个人识别信息，无论商户是否有意为之，CyberSource 都会立即暂停其账户，这会导致该商户之后提交的交易请求全部遭到拒绝。	注册 (O)	String (255)
merchantID	您的 CyberSource 商户 ID。	注册 (R) 检验 (R)	String (30)
merchantReference 代码	商户生成的订单参考号或跟踪编号。	注册 (R) 检验 (R)	String (50)
payerAuthEnrollService_ accountPurchases	过去六个月内使用此持卡人账户购买商品的次数。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (4)
payerAuthEnrollService_ addCardAttempts	过去 24 小时内尝试添加卡的次数。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (3)
payerAuthEnrollService_ alternateAuthentication 数据	记录和支持特定验证流程的数据。	注册 (O)	String (2048)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
payerAuthEnrollService_ alternateAuthentication 日期	持卡人验证的日期和时间 (UTC)。 格式： YYYYMMDDHHMM	注册 (O)	Integer (12)
payerAuthEnrollService_ alternateAuthentication 方法	持卡人针对 3D Secure 请求者的验证机制。 可能的值： ■ 01：未进行验证 ■ 02：使用商户系统凭据登录 ■ 03：使用 Federated ID 登录 ■ 04：使用 FIDO Authenticator 登录	注册 (O)	Integer (2)
payerAuthEnrollService_ authentication 交易 ID	传递的 3DS 验证交易标识符，用于连接注册检查服务并检验验证消息。 备注 标准集成的必填字段。	注册 (O)	String (20)
payerAuthEnrollService_ challengeCode	可能的值： ■ 01：无首选项 ■ 02：无质询请求 ■ 03：请求质询（3D Secure 请求者首选项） ■ 04：请求质询（授权） ■ 05-79：为 EMVCo 预留（未经 EMVCo 定义的值均无效） ■ 80-99：为 DS 预留	注册 (O)	String (2)
payerAuthEnrollService_ customerCCAlias	别名，可作为消费者账户和存档信用卡的唯一标识 备注 如果商户个人资料设置中启用了简码化功能，则此字段为必填字段。	注册 (O)	String (128)
payerAuthEnrollService_ defaultCard	表示使用的卡被指定为购物主支付卡。此字段可包含以下其中一个值： ■ true ■ false 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	String (5)
payerAuthEnrollService_ fraudActivity	表示商户是否发现过账户的可疑活动（包括以往欺诈）。此字段可包含以下其中一个值： ■ 01：无可疑活动 ■ 02：发现可疑活动 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	String (2)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
payerAuthEnrollService_giftCardAmount	所购买预付代金卡的总计金额（主要货币单位） 例如： 123.45 USD= 123	注册 (O)	Integer (15)
payerAuthEnrollService_giftCardCount	所购买预付代金卡的总计数。	注册 (O)	Integer (2)
payerAuthEnrollService_giftCardCurrency	购买代金卡所用的货币。使用 支持中心 中的标准 ISO 代码。	注册 (O)	Integer (3)
payerAuthEnrollService_httpAccept	消费者的 Web 浏览器发送的 Accept 字头的值。 备注 如果消费者的浏览器提供了值，则必须在请求中包含该值。	注册 (O)	String (255)
payerAuthEnrollService_httpUserAccept	HTTP 字头接受字段的确切内容。	注册 (O)	String (256)
payerAuthEnrollService_httpUserAgent	消费者的 Web 浏览器发送的 User-Agent 字头的值。 备注 如果消费者的浏览器提供了值，则必须在请求中包含该值。	注册 (O)	String (255)
payerAuthEnrollService_installmentTotalCount	大于 1 的整数值，表示分期付款授权的允许尝试次数上限。 备注 如果商户和持卡人已约定分期付款，则此值为必填字段。	注册 (O)	Integer (4)
payerAuthEnrollService_marketingOptIn	表示消费者是否选择参加营销优惠。此字段可包含以下其中一个值： ■ true ■ false 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	String (5)
payerAuthEnrollService_marketingSource	表示营销优惠的来源。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	String (40)
payerAuthEnrollService_MCC	商户类别代码。 重要说明 仅对巴西的 Visa Secure 交易为必填。请勿将此请求字段用于任何其他交易类型。	注册 (O)	Integer (4)
payerAuthEnrollService_merchantName	希望消费者在发卡行验证表格中看到的公司名称。此值将覆盖收单行指定的值。 对 Visa Secure 旅行交易为必填。	注册 (O)	String (25)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
payerAuthEnrollService_merchantNewCustomer	说明消费者是商户的新客户还是老客户。 此字段可包含以下其中一个值： ■ true ■ false	注册 (O)	String (5)
payerAuthEnrollService_merchantURL	公司网站的 URL，例如： http://www.example.com 。 此值将覆盖收单行指定的值。	注册 (O)	String (100)
payerAuthEnrollService_messageCategory	特定使用案例的消息类别。 可能的值： ■ 01: PA- 支付验证 ■ 02: NPA- 非支付验证 ■ 03–79: 为 EMVCo 预留（未经 EMVCo 定义的值均无效） ■ 80–99: 为 DS 预留	注册 (O)	String (2)
payerAuthEnrollService_mobilePhone	持卡人的手机号码。 适用于巴西的 Visa Secure 交易。	注册 (R)	Integer (25)
payerAuthEnrollService_npaCode	非 3DS 验证标识符。 可能的值： ■ 01: 添加卡 ■ 02: 维护卡片信息 ■ 03: 针对 EMV 令牌的持卡人验证 ■ 04–80: 为 EMVCo 预留 ■ 80–90: 预留的 DS	注册 (O)	Integer (2)
payerAuthEnrollService_overridePaymentMethod	指定用于交易的巴西支付账户类型。此字段将覆盖请求中可能指定的其他支付类型。 对于此字段，请使用以下其中一个值： ■ NA: 不适用。不覆盖请求中指定的其他支付类型。 ■ CR: 信用卡。 ■ DB: 借记卡。 ■ VSAVR: Visa Vale Refeicao ■ VSAVA: Visa Vale Alimentacao 重要说明 仅对巴西的 Visa Secure 交易为必填。请勿将此请求字段用于任何其他交易类型。	注册 (O)	String (10)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
payerAuthEnrollService_ paymentAccountDate	支付账户添加到持卡人账户的日期。 此字段可包含以下其中一个值： ■ -1：来宾账户 ■ 0：本次交易期间添加 如果两个选项均不适用，请按 YYYYMMDD 格式输入日期。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (8)
payerAuthEnrollService_ preorder	表示持卡人的订单是否包含未来到货或上市日期。 此字段可包含以下其中一个值： ■ 01：商品到货 ■ 02：未来到货	注册 (O)	String (2)
payerAuthEnrollService_ preorderDate	预售货品的预期到货日期。 格式： YYYYMMDD	注册 (O)	Integer (8)
payerAuthEnrollService_ productCode	指定产品代码，用于确定交易类型。对于此字段，请指定以下其中一个值： ■ AIR：购买航空公司服务 重要说明 对于 American Express SafeKey 为必填字段。 ■ ACC：租房 ■ ACF：账户付款 ■ CHA：承兑支票 ■ DIG：数字商品 ■ DSP：现金出纳 ■ GAS：燃料 ■ GEN：一般零售 ■ LUX：奢侈品零售 ■ PAL：预付激活和加载 ■ PHY：购买商品或服务 ■ QCT：准现金交易 ■ REN：汽车租赁 ■ RES：餐厅 ■ SVC：服务 ■ TBD：其他 ■ TRA：旅行 重要说明 对巴西的 Visa Secure 交易为必填。请勿将此请求字段用于任何其他交易类型。	注册 (O)	String (3)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
payerAuthEnrollService_recurringEndDate	此日期之后不再执行任何定期支付授权。格式：YYYYMMDD。 备注 对于定期支付交易，该字段为必填字段。	注册 (O)	Integer (8)
payerAuthEnrollService_recurringFrequency	整数值，表示定期支付授权之间的间隔天数下限。按月支付交易的对应值为 28。间隔多个月的对应值为若干个 28 天。 例如： 6 个月 = 168 备注 对于定期支付交易，该字段为必填字段。	注册 (O)	Integer (3)
payerAuthEnrollService_recurringOriginalPurchaseDate	原始购物日期。定期支付交易的必填字段。 格式： YYYYMMDD:HH:MM:SS 备注 如果此字段为空，则使用当前日期。	注册 (O)	String (17)
payerAuthEnrollService_referenceID	与之前收集的指纹数据对应的参考 ID。 备注 混合集成的必填字段。	注册 (R)	String (50)
payerAuthEnrollService_reorder	表示持卡人是否再度购买以前购入的商品。 此字段可包含以下其中一个值： 01：首次购买 02：再度购买	注册 (O)	String (2)
payerAuthEnrollService_run	是否在请求中包含 payerAuthEnrollService 。 该字段包含以下其中一个值： - true：在请求中包含该服务。 - false（默认）：不在请求中包含该服务。	注册 (R)	String (5)
payerAuthEnrollService_shipAddressUsageDate	此交易的送货地址首次使用的日期。 此字段可包含以下其中一个值： -1：来宾账户 0：本次交易期间首次使用 如果两个选项均不适用，请按 YYYYMMDD 格式输入日期。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (8)
payerAuthEnrollService_transactionCountDay	此持卡人账户在过去 24 小时内进行的交易次数（成功或放弃）。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (3)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
payerAuthEnrollService_transactionCountYear	此持卡人账户去年进行的交易次数（成功和放弃）。 如果使用 Discover ProtectBuy，建议包含此字段。	注册 (O)	Integer (3)
payerAuthEnrollService_transactionMode	交易模式标识符。表示交易发起的渠道。 可能的值： ■ M: MOTO（邮件订单电话订单） ■ R: 零售 ■ S: 电子商务 ■ P: 移动设备 ■ T: 平板电脑	注册 (R)	String (1)
payerAuthValidateService_authentication 交易 ID	传递的 3DS 验证交易标识符，用于连接注册检查服务并检验验证消息。 备注 混合集成的必填字段。	检验 (O)	String (20)
payerAuthValidateService_signedPARES	发卡行返回的 3DS 验证结果 (PARES) 消息。如果需要提供注册检查的证据，可能需要解析字符串来获得支付卡公司所要求的信息。如需详细信息，请参阅第 158 页，“存储 3DS 验证数据”。 备注 字段格式为 base64。将 PARES 添加到请求之前，必须删除所有回车符和换行符。	检验 (O)	String（无限制，可能很大）
payerAuthValidateService_run	是否在请求中包含 payerAuthValidateService 。该字段可包含以下其中一个值： ■ true: 在请求中包含该服务。 ■ false（默认）：不在请求中包含该服务。	检验 (R)	String (5)
purchaseTotals_currency	订单使用的货币。使用 支持中心 中的标准 ISO 代码。	注册 (R) 检验 (R)	String (5)
purchaseTotals_grandTotalAmount	订单总计。您的请求必须包含此字段或 item_#_unitPrice 。有关详细信息，请参阅 使用 Simple Order API 的信用卡服务 (PDF HTML) 。 备注 如果使用 item_#_unitPrice 字段，则 purchaseTotals_grandTotalAmount 字段为可选字段。	注册 (R) 检验 (R)	String (15)
shipTo_city	送货地址所在的城市。 如果包含任何送货地址信息，则为必填字段。 对于 American Express SafeKey 为必填字段。	注册 (O)	String (50)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
shipTo_country	送货地址所在的国家/地区。使用两字符 ISO 标准国家/地区代码 。 对于 American Express SafeKey 为必填字段。	注册 (O)	String (2)
shipTo_destinationCode	表示为交易选择的目的地。 可能的值： ■ 01：装运至持卡人账单地址 ■ 02：装运至商户存档的其他验证地址 ■ 03：装运至账单地址以外的其他地址 ■ 04：装运至店面（店面地址应按请求填充） ■ 05：数字商品 ■ 06：旅行和活动门票，不装运 ■ 07：其他	注册 (O)	Integer (2)
shipTo_firstName	收件人的名字。	注册 (O)	String (60)
shipTo_lastName	收件人的姓氏。	注册 (O)	String (60)
shipTo_phoneNumber	送货地址的电话号码。 有关格式的信息，请参阅 billTo_phoneNumber 。	注册 (O)	String (15)
shipTo_postalCode	送货地址的邮政编码。邮政编码必须由 5 到 9 位数字组成。 当送货国家/地区为美国时，9 位邮政编码必须遵循以下格式： [5 位数字][短划线][4 位数字] 示例 12345-6789 当送货国家/地区为加拿大时，6 位邮政编码必须遵循以下格式： [字母][数字][字母][空格] [数字][字母][数字] 示例 A1B 2C3 仅在 shipTo_country 字段为 US 或 CA 时为必填字段。 对于 American Express SafeKey 为必填字段。	注册 (O)	String (10)

表 14 请求字段（续）

字段名称	说明	必填/可选	类型和长度
shipTo_shippingMethod	产品的送货方式。可能的值： ■ lowcost: 最低成本服务 ■ sameday: 快递或当天送达服务 ■ oneday: 次日或隔天送达服务 ■ twoday: 两天送达服务 ■ threeday: 三天送达服务 ■ pickup: 商店提货 ■ other: 其他送货方式 ■ none: 无送货方式，因为产品为服务或订阅 对于 American Express SafeKey 为必填字段。	注册 (O)	String (10)
shipTo_state	送货地址所在的州/省。使用美国与加拿大的州/省及领地代码。 如果 shipTo_country 为 CA 或 US，则为必填字段。 对于 American Express SafeKey 为必填字段。	注册 (O)	String (2)
shipTo_street1	送货地址的第一行。 如果包含任何送货地址信息，则为必填字段。 对于 American Express SafeKey 为必填字段。	注册 (O)	String (60)
shipTo_street2	送货地址的第二行。 对于 American Express SafeKey 为必填字段。	注册 (O)	String (60)

响应字段

表 15 回复字段

字段名称	说明	返回方式	类型和长度
decision	汇总请求的全部结果。该字段可包含以下其中一个值： ■ ACCEPT ■ ERROR ■ REJECT	注册 检验	String (255)
invalidField_0 through invalidField_N	请求中包含无效数据的字段。	注册 检验	String (255)
merchantReferenceCode	订单参考号或跟踪编号。	注册 检验	String (255)
missingField_0 through missingField_N	请求中缺少的必填字段。	注册 检验	String (255)
payerAuthEnrollReply_acsURL	注册卡时收到的发卡行验证表格的 URL。此字段可能很长。	注册	String（无长度限制）
payerAuthEnrollReply_authenticationPath	表示验证过程中向消费者显示的内容。此字段可包含以下其中一个值： ■ ADS:（卡未注册）在结账过程中提示消费者激活卡。 ■ ATTEMPTS:（尝试处理）结账完成之前短暂显示 <i>正在处理...</i>。 ■ ENROLLED:（卡已注册）显示发卡行的验证窗口。 ■ UNKNOWN: 无法确定卡注册状态。 ■ NOREDIRECT:（卡未注册，验证不可用或出错）不向消费者显示任何内容。 如果使用基于规则的 3DS 验证，将返回以下值。请参阅第 176 页，“基于规则的 3DS 验证”： ■ RIBA: 发卡行支持基于风险的验证，但是无法确定持卡人是否会遭到质询。 ■ RIBA_PASS: 发卡行支持基于风险的验证，并且持卡人很可能不会被要求提供凭证，也称为<i>无声验证</i>。	注册	String (255)

表 15 回复字段（续）

字段名称	说明	返回方式	类型和长度
payerAuthEnrollReply_authenticationResult	来自发卡行的原始验证数据。表示验证是否成功以及是否发生责任转移的主验证字段。您应首先检查此字段的结果。此字段包含以下其中一个值： ■ -1: PAREs 无效。 ■ 0: 检验成功。 ■ 1: 持卡人未参与，但有尝试验证的记录。 ■ 6: 发卡行无法执行验证。 ■ 9: 持卡人未完成验证。	注册	仅包含数字的 String (255)
payerAuthEnrollReply_authenticationStatus Message	解释 payerAuthEnrollReply_authenticationResult 内容的消息。	注册	String (255)
payerAuthEnrollReply_authentication 交易 ID	传递的 3DS 验证交易标识符，用于连接注册检查服务并检验验证消息。	注册	String (20)
payerAuthEnrollReply_cavv	在对消费者进行验证后由发卡行生成的唯一标识符。值的格式为 base64 。请求卡授权服务时，CyberSource 会自动将值（而非字段名称）转换为支付处理机构要求的格式。 备注 此字段仅针对 Visa Secure、American Express SafeKey、JCB、Diners Club 和 Discover 交易生成。	注册	String (255)
payerAuthEnrollReply_cavvAlgorithm	payerAuthEnrollReply_paresStatus 包含值 Y（验证成功）或 A（尝试验证）时返回的字段。此字段包含以下其中一个值： ■ 2: Visa、American Express、JCB、Diners Club 和 Discover ■ 3: Mastercard 和 Maestro 备注 此字段仅在您使用 Atos 支付处理机构时适用。如果使用 Atos，请在授权服务的 ccAuthService_cavvAlgorithm 请求字段中发送此字段的值。	注册	Integer (1)
payerAuthEnrollReply_challengeRequired	表示验证时是否需要填写质询字段。 可能的值： ■ Y: 质询必填 ■ N: 质询非必填 备注 适用于混合集成。	ics_pa_enroll	String (1)

表 15 回复字段（续）

字段名称	说明	返回方式	类型和长度
payerAuthEnrollReply_commerceIndicator	未注册卡的商务交易指示符。此字段包含以下其中一个值： ■ internet: 卡未注册，或 3DS 验证不支持卡类型。无责任转移。 ■ js_attempted: JCB 卡未注册，但有尝试验证的记录。责任转移。 ■ js_failure: 如果 JCB 的目录服务不可用，则会收到此结果。无责任转移。 ■ spa: Mastercard 未注册。无责任转移。 ■ vbv_attempted: Visa 卡未注册，但有尝试验证的记录。责任转移。 ■ vbv_failure: 对于支付处理机构 Barclays、Streamline、AIBMS 或 FDC Germany，如果 Visa 的目录服务不可用，您将收到此结果。无责任转移。	注册	String (255)
payerAuthEnrollReply_directoryServer 交易 ID	目录服务器交易 ID 由目录服务器在验证期间生成，返回时包含验证结果。持卡人的品牌商可能要求持卡人在授权服务请求中发送此字段。	ics_pa_enroll	String (36)
payerAuthEnrollReply_eci	备注 此字段仅适用于非美国发行的卡。 仅针对未注册的 Visa、American Express、JCB、Diners Club 和 Discover 卡的交易返回的数字电子商务交易指示符 (ECI)。 如果不使用 CyberSource 支付服务，则必须在后续卡授权请求中将此值发送给支付处理机构。此字段包含以下其中一个值： ■ 06: 卡可注册。责任转移。 ■ 07: 卡无法注册。无责任转移。	注册	String (255)
payerAuthEnrollReply_eciRaw	可针对 Visa、Mastercard、American Express、JCB、Diners Club 和 Discover 返回的 ECI 值。当验证失败时，此字段不存在。如果支付处理机构是 Streamline，则必须发送此字段的值，而非 payerAuthEnrollReply_eci 或 payerAuthEnrollReply_ucafCollectionIndicator 的值。 此字段可包含以下其中一个值： ■ 01: 尝试验证 (Mastercard) ■ 02: 验证成功 (Mastercard) ■ 05: 验证成功 (Visa、American Express、JCB、Diners Club 和 Discover) ■ 06: 尝试验证 (Visa、American Express、JCB、Diners Club 和 Discover)	注册	String (255)

表 15 回复字段（续）

字段名称	说明	返回方式	类型和长度
payerAuthEnrollReply_paReq	需要转发给 ACS 的 3DS 验证请求 (PAREq) 消息。此字段可能很长。值的格式为 base64 。	注册	String (无长度限制)
payerAuthEnrollReply_paresStatus	验证检查的原始结果。此字段可包含以下其中一个值： ■ A: 生成了验证尝试的证据。 ■ B: 绕过验证。 ■ N: 消费者未通过验证或者取消了验证。交易被拒绝。 ■ R: 验证被拒绝（仅适用于 3D Secure 2.x 交易） ■ U: 验证出于任何原因未完成。 ■ Y: 消费者成功通过验证。 备注 此字段仅适用于亚洲、中东和非洲支付接口。如果您配置的是此支付处理机构，则必须在授权请求中发送此字段的值。	注册	String (255)
payerAuthEnrollReply_proofXML	注册检查的日期和时间以及 VEReq 和 VERes 元素。如果需要提供注册检查的证据，将需要分析字符串来获得支付卡公司所要求的信息。如需详细信息，请参阅第 158 页，“存储 3DS 验证数据”。此值可能很大。 ■ 对于在美国或加拿大发行的卡，Visa 可能需要此数据来了解特定商户类别代码。 ■ 对于在美国或加拿大境外发行的卡，您的银行可能会要求此数据，作为您由于拒付而重新提交的任何 3DS 验证交易的注册检查的证据。	注册	String (无长度限制)
payerAuthEnrollReply_proxyPAN	3DS 验证请求消息中使用的加密版卡号。	注册	String (255)
payerAuthEnrollReply_reasonCode	与“注册检查”服务请求的结果对应的数值。有关可能的值，请参阅第 142 页，附录 B，“原因代码”。	注册	Integer (5)
payerAuthEnrollReply_specificationVersion	此字段包含用于处理交易的 3D Secure 版本。例如，1.0.2 或 2.0.0。	注册	String (20)
payerAuthEnrollReply_ucafAuthenticationData	AAV 是在对消费者进行验证后由发卡行生成的唯一标识符。值的格式为 base64。在卡授权请求中包含此数据。 备注 此字段仅对 Mastercard Identity Check 交易返回。	注册	String (255)

表 15 回复字段（续）

字段名称	说明	返回方式	类型和长度
payerAuthEnrollReply_ucafCollectionIndicator	表示由于消费者未注册而不需要验证。将此字段的值添加到授权字段 ucaf_collectionIndicator。此字段可包含以下值：0、1。 备注 此字段仅对 Mastercard Identity Check 交易返回。	注册	String (255)
payerAuthEnrollReply_veresEnrolled	注册检查的结果。此字段可包含以下其中一个值： ■ Y：卡已注册；必须进行验证。责任转移。 ■ N：卡未注册，继续进行授权。责任转移。 ■ U：出于任何原因无法进行验证。无责任转移。 备注 此字段仅适用于亚洲、中东和非洲支付接口。如果您配置的是此支付处理机构，则必须在授权请求中发送此字段的值。 如果使用基于规则的 3DS 验证，将返回以下值。请参阅第 176 页，“基于规则的 3DS 验证”： ■ B：表示绕过了验证。	注册	String (255)
payerAuthEnrollReply_xid	CyberSource 为成功注册检查生成的交易标识符。使用此值匹配传出 PAReq 与传入 PARes。如果您的支付处理机构是 Barclays，CyberSource 将转发 XID 与您的卡授权服务请求。值的格式为 base64。	注册	String (255)
payerAuthValidateReply_authenticationResult	来自发卡行的原始验证数据。表示验证是否成功以及是否发生责任转移的主验证字段。您应首先检查此字段的结果。此字段包含以下其中一个值： ■ -1：PARes 无效。 ■ 0：检验成功。 ■ 1：持卡人未参与，但有尝试验证的记录。 ■ 6：发卡行无法执行验证。 ■ 9：持卡人未完成验证。	检验	仅包含数字的 String (255)
payerAuthValidateReply_authenticationStatus Message	解释 payerAuthValidateReply_authenticationResult 内容的消息。	检验	String (255)
payerAuthValidateReply_cavv	在对消费者进行验证后由发卡行生成的唯一标识符。值的格式为 base64。请求卡授权服务时，CyberSource 会自动将值（而非字段名称）转换为支付处理机构要求的格式。 备注 此字段仅针对 Visa Secure、American Express SafeKey、JCB、Diners Club 和 Discover 交易生成。	检验	String (255)

表 15 回复字段（续）

字段名称	说明	返回方式	类型和长度
payerAuthValidateReply_cavvAlgorithm	payerAuthValidateReply_paresStatus 包含值 Y（验证成功）或 A（尝试验证）时返回的字段。此字段包含以下其中一个值： ■ 2: Visa、American Express、JCB、Diners Club 和 Discover ■ 3: Mastercard 和 Maestro 备注 此字段仅在您使用 Atos 支付处理机构时适用。如果使用 Atos，请在授权服务的 ccAuthService_cavvAlgorithm 请求字段中发送此字段的值。	检验	Integer (1)
payerAuthValidateReply_commerceIndicator	用于区分不同交易类型的指示符。如果不返回此字段，验证则失败。如果同时请求授权服务，此字段的值将自动传递给该服务。此字段包含以下其中一个值： ■ aesk: 成功通过 American Express SafeKey 验证。 ■ aesk_attempted: 卡未注册 American Express SafeKey，但有尝试验证的记录。 ■ dipb: 成功通过 Discover ProtectBuy 验证。 ■ dipb_attempted: 卡未注册 Discover ProtectBuy，但有尝试验证的记录。 ■ internet: 验证失败。 ■ js: 成功通过 J/Secure 验证。 ■ js_attempted: 卡未注册 J/Secure，但有尝试验证的记录。 ■ moto: 邮购或电话订购。 ■ pb_attempted: 卡未注册 Diners Club ProtectBuy，但有尝试验证的记录。 ■ recurring: 循环交易。 ■ spa: 成功通过 Mastercard Identity Check 验证。 ■ spa_failure: Mastercard Identity Check 验证失败。 ■ vbv: 成功通过 Visa Secure 验证。 ■ vbv_attempted: 卡未注册 Visa Secure，但有尝试验证的记录。 ■ vbv_failure: Visa Secure 验证服务不可用。 备注 对于 Visa，如果支付处理机构为 Streamline、Barclays、AIBMS 或 FDC Germany，当 payerAuthValidateReply_eci 为 07 时，将收到 vbv_failure 而非 internet。	检验	String (255)

表 15 回复字段（续）

字段名称	说明	返回方式	类型和长度
payerAuthValidateReply_directoryServer 交易 ID	目录服务器交易 ID 由目录服务器在验证期间生成，返回时包含验证结果。持卡人的品牌商可能要求持卡人在授权服务请求中发送此字段。	ics_pa_validate	String (36)
payerAuthValidateReply_eci	仅针对 Visa、American Express、JCB、Diners Club 和 Discover 交易返回的数字电子商务交易指示符 (ECI)。必须在后续卡授权请求中将此值发送给支付处理机构。此字段包含以下其中一个值： 05：验证成功 06：尝试验证 07：验证失败（由于出现问题，商户无回应。）	检验	String (255)
payerAuthValidateReply_eciRaw	可针对 Visa、Mastercard、American Express、JCB、Diners Club 和 Discover 返回的 ECI 值。当验证失败时，此字段不存在。如果支付处理机构是 Streamline，则必须发送此字段的值，而非 payerAuthValidateReply_eci 或 payerAuthValidateReply_ucafCollectionIndicator 的值。 此字段可包含以下其中一个值： 01：尝试验证 (Mastercard) 02：验证成功 (Mastercard) 05：验证成功 (Visa、American Express、JCB、Diners Club 和 Discover) 06：尝试验证 (Visa、American Express、JCB、Diners Club 和 Discover)	检验	String (255)
payerAuthValidateReply_paresStatus	验证检查的原始结果。此字段可包含以下其中一个值： - A：生成了验证尝试的证据。 - B：绕过验证 - N：消费者未通过验证或者取消了验证。交易被拒绝。 - R：验证被拒绝（仅适用于 3D Secure 2.x 交易） - U：验证出于任何原因未完成。 - Y：消费者成功通过验证。 备注 此字段仅适用于亚洲、中东和非洲支付接口。如果系统配置的是此支付处理机构，则必须在授权请求中发送此字段的值。	检验	String (255)
payerAuthValidateReply_reasonCode	与检验请求的结果对应的数值。有关可能的值，请参阅第 142 页，附录 B，“原因代码”。	检验	Integer (5)

表 15 回复字段（续）

字段名称	说明	返回方式	类型和长度
payerAuthValidateReply_specificationVersion	此字段包含用于处理交易的 3D Secure 版本。例如，1.0.2 或 2.0.0。	检验	String (20)
payerAuthValidateReply_ucafAuthenticationData	AAV 是在对消费者进行验证后由发卡行生成的唯一标识符。值的格式为 base64。在卡授权请求中包含此数据。 备注 此字段仅对 Mastercard Identity Check 交易返回。	检验	String (255)
payerAuthValidateReply_ucafCollectionIndicator	数字电子商务交易指示符 (ECI)。当验证失败时，此字段不存在。必须在卡授权请求中将此值发送给支付处理机构。此字段包含以下其中一个值： 0：您的网站不支持 UCAF 采集。消费者验证未完成。 1：您的网站支持 UCAF 采集，但是 UCAF 未填充。消费者验证未完成。 2：您的网站支持 UCAF 采集，且 UCAF 已填充。消费者完成验证。 备注 此字段仅对 Mastercard Identity Check 交易返回。	检验	String (255)
payerAuthValidateReply_xid	CyberSource 生成的用于检验检查的交易标识符。使用此值（格式为 base64）匹配 PAREq 与 PAREs。CyberSource 会将 XID 及卡授权服务转发给以下支付处理机构： - Barclays - Streamline（当商务交易指示符为 spa 时）	检验	String (255)
purchaseTotals_currency	订单使用的货币。使用 支持中心 中的标准 ISO 代码。	注册 检验	String (255)
reasonCode	与整个请求的结果对应的数值。有关可能的值，请参阅第 142 页，附录 B，“原因代码”。	注册 检验	Integer (5)
requestID	请求的标识符。	注册 检验	String (255)
requestToken	CyberSource 所生成请求的标识符。 CyberSource 为每次响应创建的请求令牌数据。此字段是一个编码字符串，不包含账号或信用卡验证码等机密信息。该字符串最多可包含 256 个字符。	注册 检验	String (256)

原因代码

下表列出了与回复一同返回的原因代码。CyberSource 保留随时添加新原因代码的权利。如果错误处理程序收到了无法识别的原因代码，则应使用 **decision** 字段来确定结果。

表 16 原因代码

原因代码	说明
100	交易成功。
101	请求中缺少一个或多个必填字段。 可行的解决方法：查看回复字段 missingField_0 至 missingField_N ，确定缺少的字段。填写缺少的信息，并重新发送请求。
102	请求中的一个或多个字段包含无效数据。 可行的解决方法：查看回复字段 invalidField_0 至 invalidField_N ，确定无效字段。使用正确的信息重新发送请求。
150	错误：一般系统故障。 可行的解决方法：稍候几分钟，然后重新发送请求。
151	错误：收到了请求，但出现服务器超时。此错误不包括客户端与服务器之间的超时。 可行的解决方法：稍候几分钟，然后重新发送请求。
152	错误：收到了请求，但出现服务超时。 可行的解决方法：稍候几分钟，然后重新发送请求。
234	CyberSource 商户配置存在问题。 可行的解决方法：不要重新发送请求。请与客户支持部门联系以更正配置问题。
475	消费者注册了 3DS 验证。请先对持卡人进行验证，然后再继续交易。
476	无法对消费者进行验证。 可行的解决方法：审核消费者的订单。

请求和回复示例

本附录提供了注册检查服务和验证检验服务的示例。所有示例均采用名称-值对格式。



这些示例中仅包含一些必要字段，供演示之用。请勿按照这些示例中所示的字段进行操作。这些示例仅供参考。

标准集成示例

以下是注册检查服务请求的示例：

注册检查请求示例

示例 8 注册检查

```
payerAuthEnrollService_run=true  
merchantID=patest  
merchantReferenceCode=23AEE8CB6B62EE2AF07  
item_0_unitPrice=19.99  
purchaseTotals_currency=USD  
card_expirationMonth=01  
card_expirationYear=2020  
card_accountNumber=xxxxxxxxxxxxxxxxxx  
card_cardType=001  
payerAuthEnrollService_authenticationTransactionID=F18d1UW9VwTyawKTdex0
```

注册检查回复示例

示例 9 Visa 卡 Visa Secure 的交易回复

```
requestID=0340290070000167905080
merchantReferenceCode=23AEE8CB6B62EE2AF07
purchaseTotals_currency=USD
decision=ACCEPT
reasonCode=100
payerAuthEnrollReply_reasonCode=100
payerAuthEnrollReply_authenticationResult=0
payerAuthEnrollReply_authenticationStatusMessage=Success
payerAuthEnrollReply_authenticationTransactionID=F18d1UW9VwTyawKTdex0
payerAuthEnrollReply_cavv=Y2FyZGluYWxjb21tZXJjZWFlbGg=
payerAuthEnrollReply_commerceIndicator=vbv
payerAuthEnrollReply_eci=5
payerAuthEnrollReply_eciRaw=05
payerAuthEnrollReply_paresStatus=Y
payerAuthEnrollReply_reasonCode=100
payerAuthEnrollReply_specificationVersion=2.0.1
payerAuthEnrollReply_veresEnrolled=Y
```

混合集成示例

注册检查请求示例

示例 10 注册检查

```
payerAuthEnrollService_run=true
merchantID=patest
merchantReferenceCode=23AEE8CB6B62EE2AF07
item_0_unitPrice=19.99
purchaseTotals_currency=USD
card_expirationMonth=01
card_expirationYear=2020
card_accountNumber=xxxxxxxxxxxxxxxxxx
card_cardType=001
...
<Other 2.0 optional fields>
referenceID=CybsTester-778d0f67
```

注册检查回复示例

示例 11 Mastercard Identity Check 的交易回复

```
requestID=0340290070000167905080
merchantReferenceCode=23AEE8CB6B62EE2AF07
purchaseTotals_currency=USD
decision=REJECT
reasonCode=475
payerAuthEnrollReply_reasonCode=475
payerAuthEnrollReply_acsURL=https://www.example.com
payerAuthEnrollReply_authenticationTransactionID=x0Jpbq2uIT7o0tQqwd60
payerAuthEnrollReply_paReq=value in base64:
eJxVUuFyggjAMfhXPw9Tkv9g6...
payerAuthEnrollReply_specificationVersion=2.0.1
payerAuthEnrollReply_veresEnrolled=Y
request_
token=AhjzbwSTHCfKtXsaE6eleEQJP+BFNcZtIHTiD9au3tjijj5Uar+AuAAAAkAY5
```

验证检验请求示例

示例 12 验证检验请求

```
payerAuthValidateService_run=true
merchantID=patest
merchantReferenceCode=23AEE8CB6B62EE2AF07
item_0_unitPrice=19.99
purchaseTotals_currency=USD
card_expirationMonth=01
card_expirationYear=2020
card_accountNumber=xxxxxxxxxxxxxxxx
card_cardType=001
payerAuthValidateService_authenticationTransactionID=
UhGFMw6IPZbgt9diHK0
referenceID=CybsTester-cc719e84
```

验证检验回复示例

示例 13 Mastercard Identity Check 的交易回复

```
requestID=0340290070000167905080
merchantReferenceCode=23AEE8CB6B62EE2AF07
purchaseTotals_currency=USD
decision=ACCEPT
reasonCode=100
payerAuthValidateReply_reasonCode=100
payerAuthValidateReply_authenticationResult=0
payerAuthValidateReply_authenticationStatusMessage=Success
payerAuthValidateReply_cavv=Y2FyZGluYWxjb21tZXJjZWFlZGg=
payerAuthValidateReply_commerceIndicator=vbv
payerAuthValidateReply_eci=5
payerAuthValidateReply_eciRaw=05
payerAuthValidateReply_paresStatus=Y
payerAuthValidateReply_reasonCode=100
payerAuthValidateReply_specificationVersion=2.0.1
request_
token=AhjzbwSTHCfKtXsaE6e1EQJP+BFNcZtIHTiD9au3tjijj5Uar+AuAAAAkAY5
```

网站修改参考

本附录介绍如何修改网站来将 CyberSource 3DS 验证服务集成到您的结账流程中。另外还提供了一些支付卡公司网站的链接，您可从中下载适用的徽标。

网站修改步骤

1 修改网页按钮：

- 订单提交按钮：在消费者完成所有支付和验证要求之前，禁用最终“购买”按钮。
- 浏览器后退按钮：考虑意外的消费者行为。在验证过程中使用会话检查来避免对交易进行重复验证。避免会令人产生迷惑的消息，例如关于到期页面的警告。

2 添加适用徽标：

- 确保下载所支持卡的适用徽标，并将这些徽标放置在结账页面的卡信息输入字段旁。有关获取和使用徽标的详细信息，请参阅第 150 页，“3D Secure 服务徽标”。

3 添加通知消息：

- 在最终“购买”按钮和卡的徽标旁添加一条消息，告知消费者可能会收到提示，要求他们提供验证密码或注册针对其所用卡的验证计划。有关可用消息的示例，请参阅第 151 页，“通知消息示例”。

3D Secure 服务徽标

下表中包含支付卡公司网站的链接，您可从中下载徽标以及如何将其集成到在线结账流程中的相关信息。

表 17 3D Secure 服务徽标下载位置

3D Secure 服务	下载位置
Visa Secure	http://usa.visa.com/merchants/grow-your-business/payment-technologies/verified-by-visa.jsp 此网站包含 Visa Secure 的相关信息和可下载徽标的链接。另外还包含一些 Visa Secure 最佳实施方式的链接和一个商户工具包的链接。要下载这些文件，请查看网页右边缘的链接列表。
Mastercard Identity Check 和 Maestro	http://www.mastercard.us/merchants/securecode.html 此网站包含 Identity Check 的相关信息、可下载徽标的链接，以及将 Identity Check 信息集成到网站结账页面中的相关信息。 有关 Maestro 徽标的信息，请访问： http://www.mastercardbrandcenter.com/us/howtouse/bms_mae.shtml
American Express SafeKey	https://network.americanexpress.com/uk/en/safekey/ 此网站包含 SafeKey 的相关信息和可下载徽标的链接。
JCB J/Secure	http://partner.jcbcard.com/security/jsecure/logo.html 此网站包含 J/Secure 的相关信息和可下载徽标的链接。
Diners Club ProtectBuy	http://www.dinersclubprotect-buy.net/Public/MerchantTools.aspx 此网站包含 Diners Club ProtectBuy 的相关信息和可下载徽标的链接。
Discover ProtectBuy	https://www.discovernetwork.com/en-us/business-resources/free-signage-logos 此网站包含 Discover ProtectBuy 的相关信息和可下载徽标的链接。

通知消息示例

在结账界面的最终“购买”按钮旁添加一条简要消息，告知消费者可能会收到提示，要求他们提供验证密码或注册针对其所用卡的验证计划。

可参考以下示例，但应咨询具体的卡验证计划，以确保符合其消息传送要求。

示例 14

为帮助避免 `<card_type>` 卡在未经授权的情况下被在线使用，`<your_business_name>` 加入 `<card_authentication_program>`。

提交订单后，您可能会收到来自 `<card_type>` 发卡行的 `<card_authentication_program>` 消息。如果您的卡或发卡行未参加计划，将返回我们的安全结账页面完成订单。交易处理过程中请耐心等待。请勿点击“后退”按钮或关闭浏览器窗口。

示例 15

您的卡有资格注册或已经注册 Visa Secure、Mastercard、Maestro、American Express SafeKey、JCB J/Secure、Diners Club ProtectBuy 或 Discover ProtectBuy 计划。提交订单后，您的发卡行可能会提示您提供密码，之后才能完成购买。

Business Center 中 3DS 验证交易的详细信息

本附录介绍如何在 Business Center 中搜索 CyberSource 3DS 验证所扫描交易的详细信息。交易数据存储 12 个月，您可视需要将其发送给支付卡公司。

搜索 3DS 验证详细信息

可使用 Business Center 中的“交易搜索”功能搜索 API 回复字段中返回的 3DS 验证数据。

对于其他服务，绿色表示服务请求成功，红色表示失败，黑色表示服务请求并未运行。但是，对于注册检查结果，表示的含义有所不同：

- 如果卡已注册，申请结果将显示为红色，表示您需要先对用户进行验证，然后才能请求卡授权。
- 如果卡未注册，申请结果将显示为绿色，表示您不需要对用户进行验证。可立即为卡授权。

已注册的卡

如果卡已注册，则需要执行两步操作：检查注册，然后对消费者进行验证。

注册检查

对于注册卡的注册检查，可从以下部分的“交易搜索详细信息”窗口查找 3DS 验证数据：

- “请求信息”部分：注册检查服务显示为红色，因为卡已注册。您将收到对应的回复信息。如果同时请求了卡授权服务，该服务不会运行并将显示为灰色。

您可通过点击右侧链接（事件搜索和详细信息）获取关于相关订单的其他信息。

- “订单信息”部分：如果需要验证，请保存 XID 以供以后使用。由于验证尚未完成，因此不会向您发送 ECI 或 AAV_CAVV。

您需要通过请求检验服务来验证用户。

与 3DS 验证相关的事件

当 XID 值可用时，您也可选择使用“相似搜索”链接下的“按 3DS 验证历史记录”搜索交易的其他部分。

您可以使用该链接查找显示相关卡验证和授权结果的详细信息页面。在结果页面：

- 最新事件为成功验证。如果点击请求 ID，将打开验证详细信息页面。如果此事件还返回了 XID 值，则会出现“按 3DS 验证历史记录”链接。点击该链接可返回结果页面。
- 前一个事件是注册检查。

如果在 3DS 验证的同时请求了卡授权服务，则授权不会与注册检查一同运行，而是与验证检验请求一同运行。在结果页面：

- 最新事件是成功完成消费者验证和卡授权。如果点击请求 ID，将打开详细信息页面。
- 前一个事件是注册检查，显示为红色，因为卡已注册。

3DS 验证详细信息

您还可通过“扩展视图”下的“查看 3DS 验证详细信息”链接搜索 3DS 验证数据。如果点击“导出至 XML 文件”，将返回 XML 代码，如示例 16 所示。CyberSource 在交易后会将 3DS 验证信息存储 12 个月。有关此 XML 报告的详细信息，请参阅第 164 页，“3DS 验证明细报告”。

示例 16 导出的 XML 格式的交易详细信息

```

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Result SYSTEM "https://ebc.cybersource.com/ebc/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    <RequestID>1889453160000167904548</RequestID>
    <MerchantID>example</MerchantID>
    <TransactionDate>Sep 04 2007 03:35:16 PM</TransactionDate>
    <TransactionType>ics_pa_enroll</TransactionType>
    <ProofXML>
      <Date>20070904 15:30:21</Date>
      <DSURL>https:123.456.789.01:234</DSURL>
      <PAN>XXXXXXXXXXXX1007</PAN>
      <AcqBIN>1234567</AcqBIN>
      <MerID>00032805455400000</MerID>
      <Password>XXXXXXXX</Password>
      <Enrolled>Y</Enrolled>
    </ProofXML>
    <VReq>
      <PAN>XXXXXXXXXXXX1007</PAN>
      <AcqBIN>1234567</AcqBIN>
      <MerID>special_id</MerID>
    </VReq>
    <VRes>
      <Enrolled>Y</Enrolled>
      <AcctID>G7XnvRUvB6jKH5/KxVBwYnx6cyw=</AcctID>
      <URL>https://www.example_url.com</URL>
    </VRes>
    <PReq>
      <AcqBIN>1234567</AcqBIN>
      <MerID>00032805455400000</MerID>
      <Name>Example_Merchant</Name>
      <Country>US</Country>
      <URL>http://www.example_merchant.com</URL>
      <XID>a/Q7zFs2EdyKlZjve2/X4gEAAAc=</XID>
      <Date>Sep 04 2007 03:30:21 PM</Date>
      <PurchaseAmount>1.00 USD</PurchaseAmount>
      <AcctID>G7XnvRUvB6jKH5/KxVBwYnx6cyw=</AcctID>
      <Expiry>0905</Expiry>
    </PReq>
  </PayerAuthDetail>
</Result>

```

验证检验

对于顺利完成检验和卡授权服务的交易，可从以下部分的“交易搜索详细信息”窗口查找 3DS 验证数据：

- “请求信息”部分：检验成功。收到原因代码 100 及对应的回复消息。必要的 3DS 验证信息被传送到卡授权服务（已成功完成）。两项服务都显示为绿色。
- “订单信息”部分：由于检验成功，收到所有三个参数返回的值。如果系统错误阻止发卡行执行检验或持卡人未完成该流程，则不会收到 ECI 值。

卡未注册

如果卡未注册，注册检查服务结果将显示为绿色，卡授权请求（如果同时请求）将正常进行。

3DS 验证详细信息

您还可通过“扩展视图”下的“查看 3DS 验证详细信息”链接搜索 3DS 验证数据。如果点击“导出至 XML 文件”，将返回 XML 代码，如示例 17 所示。CyberSource 在交易后会将 3DS 验证信息存储 12 个月。有关此 XML 报告的详细信息，请参阅第 164 页，“3DS 验证明细报告”。

示例 17 导出的 XML 格式的交易详细信息

```

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Result SYSTEM "https://ebc.cybersource.com/ebc/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    <RequestID>1897243130000167904548</RequestID>
    <MerchantID>example</MerchantID>
    <TransactionDate>Sep 13 2007 03:58:36 PM</TransactionDate>
    <TransactionType>ics_pa_enroll</TransactionType>
    <ProofXML>
      <Date>20070913 15:53:37</Date>
      <DSURL>https:123.456.789.01:234</DSURL>
      <PAN>XXXXXXXXXXXX0008</PAN>
      <AcqBIN>123456</AcqBIN>
      <MerID>special_id</MerID>
      <Password />
      <Enrolled>N</Enrolled>
    </ProofXML>
    <VEReq>
      <PAN>XXXXXXXXXXXX0008</PAN>
      <AcqBIN>123456</AcqBIN>
      <MerID>special_id</MerID>
    </VEReq>
    <VERes>
      <Enrolled>N</Enrolled>
      <AcctID />
      <URL />
    </VERes>
  </PayerAuthDetail>
</Result>

```

交易详细信息

对于未注册卡的交易，可从以下部分的“交易搜索详细信息”窗口查找 3DS 验证数据：

- “请求信息”部分：服务显示为绿色。您可通过点击右侧链接获取相关订单的其他信息。
- “订单信息”部分：授权服务的详细信息：
 - ECI 值为 1：不需要验证，因为消费者的 Mastercard 未注册。
 - AAV/CAVV 区域为空，因为仅会在消费者经过验证后您才会收到相应的值。
 - XID 区域为空，因为卡未注册。

3DS 验证搜索

搜索使用了 3DS 验证和卡授权服务的交易。搜索交易时，请注意：

- 搜索选项：
 - 可使用 XID 作为搜索参数查找通过已注册的卡所处理交易的这两个环节。使用 XID 作为搜索选项时，请确保 = 符号位于字符串末尾。
 - 申请列表进行了简化，以便于搜索相关服务请求。
 - 3DS 验证信息会在交易日期之后保留 12 个月。
- 搜索结果：结果选项包含 XID 和消费者账号 (PAN)。可使用 XID 查找交易的所有环节。
- 3DS 验证详细信息：所有交易详细信息都在第 152 页，“搜索 3DS 验证详细信息”中进行了介绍。

存储 3DS 验证数据

支付卡公司允许 3DS 验证和授权请求间隔一定天数。如果您结算早于预定义天数的交易，支付卡公司可能要求您向其发送 AAV、CAVV 或 XID（如果发生拒付）。具体要求取决于卡类型和所在区域。有关详细信息，请参阅您与支付卡公司的协议。结算交易后，您还可使用此数据更新业务统计信息。

您可能需要在 PAREs、XML 证据与 PAREq 字段中提供收到的值，作为对您由于拒付而重新提交的任何 3DS 验证交易进行了注册检查的证明。您的账户提供商可能要求您以可读的格式提供所有数据，因此请确保您能够解码 PAREq 和 PAREs。有关注册回复示例，请参阅第 143 页，附录 C，“请求和回复示例”。所有类型卡的回复都是相似的。

各大支付卡公司已在世界各地通过不同方式实施了 3D Secure 协议。CyberSource 建议您联系您的商户账户提供商了解相关要求。有关解密和提供 PAREs 的详细信息，请联系您的业务经理。

3DS 验证报告

本章介绍可从 **Business Center** 下载的报告。生产服务器中的所有报告都将保留 **16** 个月，但是数据库中的交易历史记录仅保留 **6** 个月。测试服务器中的所有报告都会在两周后删除。仅会报告处理过的交易。不会报告导致系统错误或超时的交易。有关 **API** 回复及其含义的详细信息，请参阅第 **119** 页，附录 **A**，“**API 字段**”。



备注

要获取报告，必须在支持中心提交支持票证。

3DS 验证汇总报告

这种每日、每周和每月汇总报告用交易数量和交易总金额来表示注册和检验服务的功效。报告针对您支持的每种货币和卡类型提供这些信息。您可以使用这些信息评估 **3DS** 验证对交易的扫描情况：成功、尝试和未完成验证。报告的卡包括 **Visa**、**Mastercard**、**Maestro**、**American Express**、**JCB**、**Diners Club** 和 **Discover**。每日报告通常在 **EST** 早 **7:00** 发布。该报告中的数据保留 **6** 个月时间。

下载报告

要查看 **Classic Business Center** 中的报告，请遵循下列步骤：

步骤 1 在导航窗格中选择**报告 > 报告搜索**。

图 3 报告搜索窗口

报告搜索

[我需要有此页面的帮助。](#)

如要查看或下载报告，请选择报告和期间。如要查看您已不再订阅的报告，请选择“全部”。

报告搜索条件

报告

3DS 验证报告

频率

每日

日报表搜索

日期

4 月

9 日

2006 年

提交

2006 年 4 月 9 日的报告

没有可用的报告

2006 年 4 月 9 日的可下载报告

没有可用的报告

步骤 2 选择报告和频率。
您选择的报告类型（每日、每周或每月）决定了下面显示的日期或时间范围。

步骤 3 选择适合的日期或时间范围，然后提交搜索请求。
■ 如果有报告，则会显示一个列表。

图 4 报告搜索结果

报告搜索结果

搜索参数：报告 = 全部，频率 = 每日，日期 = 2006 年 3 月 30 日

报告

报告名称

3DS 验证报告

可下载报告

没有可用的报告

■ 如果无可用报告，**Business Center** 会显示消息*没有可用的报告*。

步骤 4 点击 **3DS 验证报告**。
报告打开。

图 5 3DS 验证报告



此报告显示三个成功通过验证的 **Visa** 交易。

可切换页面来在线查看报告，但要存储内容，请将报告导出为 **PDF** 文件或图中所示的电子表格。

要查看 **New Business Center** 中的报告，请遵循下列步骤：

- 步骤 1** 点击左侧导航栏的**报告**图标。
- 步骤 2** 在交易报告下方，点击 **3DS 验证摘要**。显示“3DS 验证摘要报告”页面。
- 步骤 3** 在搜索工具栏中，选择报告中包含的**日期范围**。账户级用户必须同时选择一个商户。
- 步骤 4** 根据选定的“日期范围”，选择需要审查的特定天、特定周或特定月。
- 月份列表仅显示当年已经度过的月份 – 要查看以前年份的所有月份，请依次选择相应的年份和所需月份。
- 要查看选定时期的前一期或后一期，请点击搜索工具栏下方的**上一步**或**下一步**。

将报告与交易搜索结果匹配

下图显示了包含上述报告中所示交易的搜索结果。有关搜索结果的详细信息，请参阅第 152 页，“搜索 3DS 验证详细信息”。

图 6 3DS 验证报告详细信息

2006 年 3 月 30 日 12:00 AM				
ubcvp1_2 Mar 30 2006 03:42:16 PM	1437540121000167904064 1143754012100	PATRICK MCMAHON null@cybersource.com	1.00 USD 0771	信用卡授权 3DS 验证检验
ubcvp1_2 Mar 30 2006 03:41:17 PM	1437543646410167904065 1143754364636	P MAN null@cybersource.com	101.00 USD 0771	信用卡授权 3DS 验证检验
ubcvp1_2 Mar 30 2006 03:40:09 PM	1437538846880167904064 1143753884687	PATRICK MCMAHON null@cybersource.com	16.00 USD 0771	信用卡授权 3DS 验证检验

解读报告

报告标题中显示标题、下载报告的用户 ID、商户 ID 以及报告的日期或日期范围。报告按卡类型编排。每个部分的货币均按字母顺序排列。您会收到每一种货币的 3DS 验证检验结果，显示为交易总金额和交易数量。

表 18 3DS 验证报告解读

卡类型	解读	受保护?	报告	
			商务交易指示符	ECI
Visa、American Express 和 JCB	无验证	否	Internet	7
	有尝试验证的记录	是	尝试 VbV、Aesk 或 JS	6
	验证成功	是	VbV、JS 或 Aesk	5
Mastercard 和 Maestro	无验证	否	Internet ²	7 ¹
	有尝试验证的记录	是	SPA	1
	验证成功	是	SPA	2
Diners Club 和 Discover	无验证	否	Internet	7
	有尝试验证的记录	是	已尝试 PB 或 DIPB	6
	验证成功	是	PB 或 DIPB	5

1 即使报告标题为 7，您也会收到采集指示值 1，或该回复字段为空。

2 即使报告标题为 Internet，您也会在商务交易指示符回复字段中收到 spa_failure。

交易被分为两组：您受保护的交易和您不受保护的交易：

- 对于 Visa、American Express、JCB、Diners Club 和 Discover：责任转移适用于 VbV 和 VbV 尝试
- 对于 Mastercard 和 Maestro：责任转移仅适用于 SPA
- 对于所有其他结果：无责任转移

比较 3DS 验证和支付报告

由于经过验证的交易可能未获得授权，因此 3DS 验证报告和支付报告之间可能存在差异。

3DS 验证报告中的值（金额和计数）可能与其他对比资料无法完全匹配，这是因为此报告显示的是经过 3DS 验证的交易，但这些交易未必获得授权。如果在 CyberSource 外处理授权，出现差异的可能性会更高。

示例 18 3DS 验证报告与支付报告比较

假设有 10,000 个订单，您可能会收到以下结果：

- 9900 次成功的注册检查（3DS 验证报告）
- 9800 次成功的验证检查（3DS 验证报告）
- 9500 次成功的授权检查（支付报告）

3DS 验证报告中的金额和数量可能高于支付报告。本例显示了 3DS 验证报告中的前两个数字与支付报告中的最后一个数字。

为了在使用 3DS 验证时更轻松地对报告，我们建议您要验证的金额最好与您要授权的金额相同。

3DS 验证明细报告

本部分介绍点击 Business Center “3DS 验证” 详细信息页面中的 “导出至 XML” 功能下载的 XML 报告。此报告中的数据将保留 12 个月。您可在 Business Center 的 **报告 > DTD** 部分获得 DTD。

文件名

您下载的文件将按以下格式命名：

`<MerchantID>-<RequestID>-<TransactionType>.xml`

示例 19

`example_merchant-1884340770000167904548-ics_pa_enroll.xml`

日期和时间

在报告中，日期和时间的显示格式如下：

`YYYY-MM-DDTHH:MM:SS[+ | -]HH:MM:`

- `YYYY-MM-DD` 为年、月、日。
- `THH:MM:SS` 为时间（时、分、秒）。T 用于分隔日期和时间。
- `[+ | -]HH:MM` 是所在时区与格林威治标准时间 (GMT) 之间的时差，其中 HH 表示小时，MM 表示分钟。数字可以使用加号 (+) 或减号 (-) 作为前缀，表示时差为正还是为负。例如，太平洋夏令时 (PDT) 的时差为 -07:00。

示例 20

`2016-07-31T16:31:18-07:00` 相当于 2016 年 7 月 31 日 16:31:18 (PDT 下午 4:31:18)

报告

<Result>

<Result> 元素是报告的根元素。

```
<Result>
  (PayerAuthDetail+)
</Result>
```

表 19 <Report> 的子元素

元素名称	说明
<PayerAuthDetail>	包含报告中的交易。有关子元素的列表，请参阅<PayerAuthDetail>。

示例 <Report> 元素

<pre><?xml version="1.0" encoding="utf-8"?> <!DOCTYPE Report SYSTEM "https://ebctest.cybersource.com/ebctest/reports/dtd/ payerauthdetails.dtd"> <Result> <PayerAuthDetail> ... </PayerAuthDetail> </Result></pre>
--

<PayerAuthDetail>

<PayerAuthDetail> 元素包含关于单个交易的信息。

<PayerAuthDetail>
(RequestID)
(MerchantID)
(TransactionDate)
(TransactionType)
(ProofXML) ?
(VEReq) ?
(VERes) ?
(PAReq) ?
(PARes) ?
(AuthInfo) ?
</PayerAuthDetail>

表 20 <PayerAuthDetail> 的子元素

元素名称	说明	类型和长度
<RequestID>	CyberSource 为交易生成的唯一标识符。此字段与 requestID API 字段对应。	Numeric (26)
<MerchantID>	用于交易的 CyberSource 商户 ID。	String (30)
<TransactionDate>	交易的处理日期。	DateTime (25)
<TransactionType>	以 SCMP 格式请求的 CyberSource 服务。此字段可包含以下其中一个值： ■ ics_auth: 银行卡授权服务 ■ ics_pa_enroll: 3DS 验证注册检查 ■ ics_pa_validate: 3DS 验证检验	String (20)

表 20 <PayerAuthDetail> 的子元素（续）

元素名称	说明	类型和长度
<ProofXML>	包含注册检查的日期和时间以及 VEReq 和 VERes 元素的数据。此字段与 payerAuthEnrollReply_proofXML API 字段对应。	String (1024)
<VEReq>	由商户服务器发送给目录服务器，并由目录服务器发送给 ACS 的注册检验请求 (VEReq)，用于确定消费者的卡号能否进行验证。有关子元素的列表，请参阅第 168 页，“<VEReq>”。	
<VERes>	目录服务器发送的注册检验请求 (VERes)。有关子元素的列表，请参阅第 169 页，“<VERes>”。	
<PAREq>	通过支付卡公司发送给 ACS 的 3DS 验证请求消息。与 payerAuthEnrollReply_paReq API 字段对应。有关子元素的列表，请参阅第 169 页，“<PAREq>”。	
<PAREs>	ACS 发送的 3DS 验证回应消息。有关子元素的列表，请参阅第 171 页，“<PAREs>”。	
<AuthInfo>	地址和卡验证数据。有关子元素的列表，请参阅第 172 页，“<AuthInfo>”。	

示例 <PayerAuthDetail> 元素

```
<PayerAuthDetail>
  <RequestID>0004223530000167905139</RequestID>
  <MerchantID>example_merchant</MerchantID>
  <TransactionDate>2007-07-25T18:23:22-07:00</TransactionDate>
  <TransactionType>ics_pa_enroll</TransactionType>
  <ProofXML>
    ...
  </ProofXML>
  <VEReq>
    ...
  </VEReq>
  <VERes>
    ...
  </VERes>
  <PAREq>
    ...
  </PAREq>
  <PAREs>
    ...
  </PAREs>
</PayerAuthDetail>
```

<ProofXML>

<ProofXML> 元素包含注册检查的日期和时间以及 VEReq 和 VERes 元素数据。此元素与 **payerAuthEnrollReply_proofXML** API 字段对应。

```
<ProofXML>
  (Date)
  (DSURL)
  (PAN)
  (AcqBIN)
  (MerID)
  (Password)
  (Enrolled)
</ProofXML>
```

表 21 <ProofXML> 的子元素

元素名称	说明	类型和长度
<Date>	XML 证据生成的日期。 备注 尽管在处理订单的所有阶段日期和时间都应按顺序显示，但由于服务器之间的时区和同步存在差异，因此可能无法按顺序显示。	DateTime (25)
<DSURL>	XML 证据来源目录服务器的 URL。	String (50)
<PAN>	消费者的掩码账号。此元素与 payerAuthEnrollReply_proxyPAN API 字段对应。	String (19)
<AcqBIN>	收单行标识号的前六位。	Numeric (6)
<MerID>	收单行提供的标识符；用于登录 ACS URL。	String (24)
<Password>	商户登录 ACS 的掩码验证密码；由收单行提供。仅适用于在美国以外地区发行的卡。	String (8)
<Enrolled>	注册检查的结果。此字段可包含以下其中一个值： ■ Y：可以进行验证。 ■ N：持卡人未参与。 ■ U：出于任何原因无法进行验证。	String (1)

示例 <ProofXML> 元素

```
<ProofXML>
  <Date>20070725 11:18:51</Date>
  <DSURL>https:123.456.789.01:234/DSMsgServlet</DSURL>
  <PAN>XXXXXXXXXXXX0771</PAN>
  <AcqBIN>123456</AcqBIN>
  <MerID>44444444</MerID>
  <Password />
  <Enrolled>Y</Enrolled>
</ProofXML>
```

<VEReq>

<VEReq> 元素包含注册检查请求数据。

```
<VEReq>
  (PAN)
  (AcqBIN)
  (MerID)
</VEReq>
```

表 22 <VEReq> 的子元素

元素名称	说明	类型和长度
<PAN>	消费者的掩码账号。此元素与 payerAuthEnrollReply_proxyPAN API 字段对应。	String (19)
<AcqBIN>	收单行标识号的前六位。	Numeric (6)
<MerID>	收单行提供的标识符；用于登录 ACS URL。	String (24)

示例 <VEReq> 元素

```
<VEReq>
  <PAN>XXXXXXXXXXXX0771</PAN>
  <AcqBIN>123456</AcqBIN>
  <MerID>example</MerID>
</VEReq>
```

<VERes>

<VERes> 元素包含注册检查回复数据。

```
<VERes>
  (Enrolled)
  (AcctID)
  (URL)
</VERes>
```

表 23 <VERes> 的子元素

元素名称	说明	类型和长度
<Enrolled>	注册检查的结果。此字段可包含以下其中一个值： ■ Y： 可以进行验证。 ■ N： 持卡人未参与。 ■ U： 出于任何原因无法进行验证。	String (1)
<AcctID>	ACS 使用的掩码字符串。	String (28)
<URL>	发送 PAREq 的访问控制服务器 URL。此元素与 payerAuthEnrollReply_acsURL API 字段对应。	String (1000)

示例 <VERes> 元素

```
<VERes>
  <Enrolled>Y</Enrolled>
  <AcctID>NDAXMjAwMTAxMTAwMDc3MQ==</AcctID>
  <URL>https://www.example_url.com</URL>
</VERes>
```

<PAREq>

<PAREq> 元素包含 3DS 验证请求消息。此元素与 payerAuthEnrollReply_paReq API 字段对应。

```
<PAREq>
  (AcqBIN)
  (MerID)
  (Name)
  (Country)
  (URL)
  (XID)
  (Date)
  (PurchaseAmount)
  (AcctID)
  (Expiry)
</PAREq>
```

表 24 <PAREq> 的子元素

元素名称	说明	类型和长度
<AcqBIN>	收单行标识号的前六位。	Numeric (6)
<MerID>	收单行提供的标识符；用于登录 ACS URL。	String (24)
<Name>	商户的公司名称。	String (25)
<Country>	商户运营所在国家/地区的两字符代码。	String (2)
<URL>	商户的商业网站。	String
<XID>	CyberSource 为每个支付验证请求 (PAREq) 消息生成的唯一交易标识符。发卡行发回的 PAREs 包含 PAREq 的 XID。为确保两个 XID 相同，请将其与回复中的 XID 进行比较。要查找与交易相关的所有请求，可以搜索特定 XID 对应的交易。	String (28)
<Date>	请求的日期和时间。 备注 尽管在处理订单的所有阶段日期和时间都应按顺序显示，但由于服务器之间的时区和同步存在差异，因此可能无法按顺序显示。	DateTime (25)
<Purchase Amount>	交易的授权金额和货币。此元素与出售行或以下字段的总额对应。 ■ ccAuthReply_amount （请参阅 <i>使用 Simple Order API 的信用卡服务</i> [PDF HTML]）或外部数据中的 purchaseTotals_grandTotalAmount 。	Amount (15)
<AcctID>	ACS 使用的掩码字符串。	String (28)
<Expiry>	消费者所持卡的到期月份和年份。	Numeric (4)

示例 <PAREq> 元素

```

<PAREq>
  <AcqBIN>123456</AcqBIN>
  <MerID>444444</MerID>
  <Name>example</Name>
  <Country>US</Country>
  <URL>http://www.example.com</URL>
  <XID>fr2VCDrbEdyC37MOPfIzMwAHBwE=</XID>
  <Date>2007-07-25T18:18:51-07:00</Date>
  <PurchaseAmount>1.00 USD</PurchaseAmount>
  <AcctID>NDAXMjAwMTAxMTAwMDc3MQ==</AcctID>
  <Expiry>0811</Expiry>
</PAREq>

```

<PAREs>

<PAREs> 元素包含 3DS 验证回复消息。

```
<PAREs>
  (AcqBIN)
  (MerID)
  (XID)
  (Date)
  (PurchaseAmount)
  (PAN)
  (AuthDate)
  (Status)
  (CAVV)
  (ECI)
</PAREs>
```

表 25 <PAREs> 的子元素

元素名称	说明	类型和长度
<AcqBIN>	收单行标识号的前六位。	Numeric (6)
<MerID>	收单行提供的标识符；用于登录 ACS URL。	String (24)
<XID>	消费者验证回复中返回的 XID 值。此元素与 payerAuthEnrollReply_xid 和 payerAuthValidateReply_xid API 字段对应。	String (28)
<Date>	请求的日期和时间。 备注 尽管在处理订单的所有阶段日期和时间都应按顺序显示，但由于服务器之间的时区和同步存在差异，因此可能无法按顺序显示。	DateTime (25)
<PurchaseAmount>	交易的授权金额和货币。此元素与出售行或以下字段的总额对应。 ■ ccAuthReply_amount （请参阅使用 <i>Simple Order API</i> 的信用卡服务 [PDF HTML] ）或外部数据中的 purchaseTotals_grandTotalAmount	Amount (15)
<PAN>	消费者的掩码账号。此元素与 payerAuthEnrollReply_proxyPAN API 字段对应。	String (19)
<AuthDate>	请求的日期和时间。 备注 尽管在处理订单的所有阶段日期和时间都应按顺序显示，但由于服务器之间的时区和同步存在差异，因此可能无法按顺序显示。	DateTime (25)
<Status>	验证检查的结果。此字段可包含以下其中一个值： ■ Y：消费者成功通过验证。 ■ N：消费者未通过验证或者取消了验证。交易被拒绝。 ■ U：验证出于任何原因未完成。 ■ A：生成了验证尝试的证据。	String (1)

表 25 <PAREs> 的子元素 （续）

元素名称	说明	类型和长度
<CAVV>	消费者验证回复中返回的 CAVV（Visa、American Express、JCB、Diners Club 和 Discover 卡 = 下方的 *）或 AAV（Mastercard 和 Maestro 卡 = 下方的 **）。此元素与 payerAuthValidateReply_cavv (*) 和 payerAuthValidateReply_ucafAuthenticationData (**) API 字段对应。	String (50)
<ECI>	消费者验证回复中返回的电子商务交易指示符。此元素与 payerAuthValidateReply_eci (*) 和 payerAuthValidateReply_ucafCollectionIndicator (**) API 字段对应。	Numeric (1)

示例 <Card> 元素

```
<PAREs>
  <AcqBIN>123456</AcqBIN>
  <MerID>44444444</MerID>
  <XID>Xe5DcjrqEdyC37MOPfIzMwAHBwE=</XID>
  <Date>2007-07-25T20:05:18-07:00</Date>
  <PurchaseAmount>1002.00 USD</PurchaseAmount>
  <PAN>0000000000000771</PAN>
  <AuthDate>2007-07-25T20:05:18-07:00</AuthDate>
  <Status>Y</Status>
  <CAVV>AAAAAAAAAAAAAAAAAAAAAAAAAAAA=</CAVV>
  <ECI>5</ECI>
</PAREs>
```

<AuthInfo>

<AuthInfo> 元素包含地址和卡验证信息。

```
<AuthInfo>
  (AVSResult)
  (CVVResult)
</AuthInfo>
```

表 26 <AuthInfo> 的子元素

元素名称	说明	类型和长度
<AVSResult>	地址验证测试的可选结果。 请参阅 <i>使用 Simple Order API 的信用卡服务</i> (PDF HTML) 中的 ccAuthReply_avsCode 或 afsService_avsCode （如果为外部数据）。	String (1)
<CVVResult>	卡验证码测试的可选结果。 请参阅 <i>使用 Simple Order API 的信用卡服务</i> (PDF HTML) 中的 ccAuthReply_cvvCode 或 afsService_cvCode （如果为外部数据）。	String (1)

示例 <AuthInfo> 元素

```
<AuthInfo>
  <AVSResult>Y</AVSResult>
  <CVVResult/>
</AuthInfo>
```

示例

以下示例显示了一项完整交易：失败的注册检查（已注册卡）以及后续的成功验证。

失败的注册检查

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Result SYSTEM "https://ebc.cybersource.com/ebc/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    <RequestID>1895549430000167904548</RequestID>
    <MerchantID>sample_merchant_id</MerchantID>
    <TransactionDate>Sep 11 2007 04:55:44 PM</TransactionDate>
    <TransactionType>ics_pa_enroll</TransactionType>
    <ProofXML>
      <Date>20070911 16:51:00</Date>
      <DSURL>https:123.456.789.01:234/DSMsgServlet</DSURL>
      <PAN>XXXXXXXXXXXX0771</PAN>
      <AcqBIN>123456</AcqBIN>
      <MerID>4444444</MerID>
      <Password />
      <Enrolled>Y</Enrolled>
    </ProofXML>
    <VEReq>
      <PAN>XXXXXXXXXXXX0771</PAN>
      <AcqBIN>123456</AcqBIN>
      <MerID>example</MerID>
    </VEReq>
    <VERes>
      <Enrolled>Y</Enrolled>
      <AcctID>NDAXMjAwMTAxMTAwMDc3MQ==</AcctID>
      <URL>https://www.sample_url.com</URL>
    </VERes>
    <PAREq>
      <AcqBIN>123456</AcqBIN>
      <MerID>example</MerID>
      <Name>Merchant Name</Name>
      <Country>US</Country>
      <URL>http://www.merchant_url.com</URL>
      <XID>2YNAGDBEdydJ6WI6aFJWAAHBwE=</XID>
      <Date>Sep 11 2007 04:51:00 PM</Date>
      <PurchaseAmount>1.00 USD</PurchaseAmount>
      <AcctID>NDAXMjAwMTAxMTAwMDc3MQ==</AcctID>
      <Expiry>0811</Expiry>
    </PAREq>
  </PayerAuthDetail>
</Result>
```

验证成功

```

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Result SYSTEM "https://ebc.cybersource.com/ebc/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    <RequestID>1895549900000167904548</RequestID>
    <MerchantID>ics2test</MerchantID>
    <TransactionDate>Sep 11 2007 04:56:31 PM</TransactionDate>
    <TransactionType>ics_pa_validate</TransactionType>
    <PRes>
      <AcqBIN>469216</AcqBIN>
      <MerID>6678516</MerID>
      <XID>2YNanGDBEdydJ6WI6aFJWAAHBwE=</XID>
      <Date>Sep 11 2007 04:51:00 PM</Date>
      <PurchaseAmount>1.00 USD</PurchaseAmount>
      <PAN>0000000000000771</PAN>
      <AuthDate>Sep 11 2007 04:51:00 PM</AuthDate>
      <Status>Y</Status>
      <CAVV>AAAAAAAAAAAAAAAAAAAAAAAAAAAA=</CAVV>
      <ECI>5</ECI>
    </PRes>
  </PayerAuthDetail>
</Result>

```

基于规则的 3DS 验证

基于规则的 3DS 验证使您可以指定 3D Secure 卡验证计划的交易验证规则。例如，您可以关闭需要消费者互动的主动交易验证，以避免影响客户体验。而通过发卡行基于风险的验证方式对消费者验证，因为这种验证不需要消费者互动。

要为您的账户启用基于规则的 3DS 验证，请联系您的 CyberSource 销售代表。



备注

对于某些卡类型和国家/地区，主动授权将取代基于规则的 3DS 验证，恢复为传统 3D Secure。

可用规则

如果您的账户启用 3DS 验证，默认会对所有交易进行验证。

对于未绕过的交易类型，可能会要求您完成验证。

您可启用以下一种或几种验证交易类型。任何设置为绕过验证的交易类型都会返回原因代码 100。如果注册检查返回原因代码 475，即使消费者无需参与，也必须完成验证。

表 27 基于规则的 3DS 验证类型

验证类型	说明	测试案例示例
主动验证	提示消费者进行验证。	测试案例 1: Visa Secure 注册卡: 验证成功
尝试处理	提示消费者注册 3D Secure 卡验证计划。此交易类型提供 3D Secure 的所有功能。	测试案例 3: Visa Secure 注册卡: 尝试处理
非参与银行	发卡行未参与 3D Secure 计划。检查注册后, 此交易类型提供 3D Secure 的所有功能, 包含消费者“非本人”交易的欺诈拒付责任转移和 5-59 个基点的交换减免。	测试案例 9: Visa Secure 未注册银行卡
被动验证	不提示消费者进行验证。完成被动验证后, 此交易类型提供 3D Secure 的所有功能。	测试案例 12: Visa Secure 注册 RIBA_PASS
基于风险的银行	发卡行采用基于风险的验证。可能的结果是不要求消费者输入凭证。大部分验证无需消费者互动。此交易类型提供 3D Secure 的所有功能。	测试案例 14: Visa Secure 注册 RIBA

API 回复



备注

默认关闭与基于规则的 3DS 验证明确相关的 API 回复。请联系 CyberSource 客户支持部门在触发规则时启用这些 API 回复。

绕过验证的交易

当借助基于风险的 3DS 验证配置绕过卡验证时, 您会收到以下注册检查值:

- **payerAuthEnrollReply_veresEnrolled = B** (表示已绕过验证)

基于风险的银行交易

当交易涉及的发卡行支持基于风险的验证时，您可能收到以下验证路径回复（具体取决于发卡行是否认为交易有风险）：

■ payerAuthEnrollReply_authenticationPath

- = RIBA

发卡行支持基于风险的验证，但是无法确定持卡人是否会遭到质询。

- = RIBA_PASS

发卡行支持基于风险的验证，并且持卡人很可能不会被要求提供凭证，也称为*无声验证*。

词汇表

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

数字

3D Secure Visa Secure、Mastercard Identity Check、American Express SafeKey、JCB JSecure、Diners Club ProtectBuy 和 Discover ProtectBuy 用于在线信用卡和借记卡交易的安全协议。

A

AAV 账户验证值。用于 3D Secure 交易的唯一 32 字符交易令牌。对于 Mastercard Identity Check，AAV 的名称为 [UCAF](#)。对于 Visa Secure，AAV 的名称为 [CAVV](#)。

ACS 访问控制服务器。发卡行用于存储 3DS 验证数据的主机。

ACS URL 在注册检查请求的回复中返回的发卡行访问控制服务器 URL。必须向其发送 [PAREq](#) 才能对消费者进行验证。

ADS 购物期间激活。发卡行在商户向 [ACS URL](#) 发送数据时要求持卡人注册卡验证服务的功能。

American Express 以 3 开头，CyberSource 的卡类型标识符为 003 的一种全球发行的信用卡。这些卡参与 [3D Secure](#) 提供的卡验证服务 ([SafeKey](#))。

API 应用程序编程接口。软件组件之间相互通信所以使用的一种规格。

B

base64 通过互联网传输数据的标准编码方式。

BIN 银行识别码。用于标识发卡行的前 6 位卡号。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

C

CAVV 持卡人验证检验值。针对已注册 [Visa Secure](#) 的卡返回的 base64 编码字符串，专门标识发卡行和 [Visa](#) 交易。[Visa Secure](#) 交易采集和发送 AAV 数据的标准。请参阅 [AAV](#)。

CAVV 算法 [PAREs](#) 状态为 Y 或 A 时返回的 1 位数回复。如果您的支付处理机构是 ATOS，则必须将此回复传送给授权（如适用）。

CVV 卡验证值信用卡和借记卡的安全功能。此功能由两个值或代码组成：其中一个位于磁条中，另一个印在卡上。CVV 通常是卡背面的 3 位数字。[American Express](#) 卡的 CVV 是卡正面的 4 位数字。发卡行将 CVV 用于额外检验。

D

Diners Club 以 3 或 5 开头的一种全球发行的信用卡。[Diners Club](#) 在 [CyberSource](#) 中的卡类型标识符为 005。这些卡参与 [3D Secure](#) 提供的卡验证服务 ([ProtectBuy](#))。

Discover 一种以 6 开头的美国信用卡。[Discover](#) 在 [CyberSource](#) 中的卡类型标识符为 004。这些卡参与 [3D Secure](#) 提供的卡验证服务 ([ProtectBuy](#))。

电子商务交易指示符 表示交易类型的字母字符值，例如 MOTO 或 INTERNET。

E

ECI (ECI Raw) 为银行提供的表示 3DS 验证处理期间实现的责任转移程度的数字商务交易指示符。

F

发卡行 发行信用卡的银行。

H

HTTP 超文本传输协议。用于互联网数据传输的应用程序协议。

HTTP POST 请求 POST 是 HTTP 协议支持的一种请求方式。当客户需要在请求中将数据发送到服务器时，例如上传文件或提交已完成的表格，使用 POST 请求方式。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

H（续）

HTTPS 与 SSL/TLS（安全套接字层/传输层安全）结合使用，为通过互联网数据传输提供安全加密的超文本传输协议。

I

Identity Check Mastercard 验证服务的商标名称。

J

J/Secure JCB 的 3D Secure 计划。

JCB 日本信用卡株式会社。以 3 开头的一种全球发行的信用卡。JCB 卡在 CyberSource 中的卡类型标识符为 007。这些卡参与 3D Secure 提供的卡验证服务 (J/Secure)。

基于风险的验证 基于风险的验证由发卡行提供。发卡行收集持卡人的交易数据或利用现有数据，根据其感知的交易风险程度对持卡人进行无声验证。他们根据持卡人的消费习惯、订单或产品交易频率、设备 IP 地址、订单金额等因素评估风险。

检验 用于解码和解密 PARES 来确定验证是否成功的 CyberSource 服务。检验服务会返回授权所需的值。

M

Maestro Mastercard 旗下的一个品牌，包含多种英国和欧洲境内的借记卡 BIN，之前称为 Switch。在线接受 Maestro 卡的商户需要使用 SecureCode——Mastercard 的一项卡验证服务。Maestro 卡在 CyberSource 中的卡类型标识符为 024 和 042。请注意，许多国际 Maestro 卡并未设置在线受理，即使其参与 SecureCode 卡验证计划也不能使用。

Mastercard 一种全球发行的卡，包含信用卡和借记卡。这些卡以 5 开头。这些信用卡和借记卡在 CyberSource 中的卡类型标识符为 002。这些卡参与 3D Secure 提供的卡验证服务 (Identity Check)。

MD 作为隐藏字段发布到 ACS URL 的商户定义数据。您可使用此数据标识返回的交易。此数据用于将发卡行的回应与消费者的特定订单进行匹配。虽然支付卡公司建议您使用 XID，您仍可使用订单号等数据。此字段为必要字段，但可选择是否包含值。值对于银行没有任何意义，将按原样返回给商户。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

M（续）

MPI 商户插件。用于连接[目录服务器](#)和解密 [PAREs](#) 的软件。

目录服务器 用于检验卡验证服务注册的 Visa 和 Mastercard 服务器。

P

PAN 主账号。表示信用卡卡号的另外一个术语。

PAReq 3DS 验证请求。经过数字签名的 [base64](#) 编码 3DS 验证请求消息，包含商户发送给发卡行的唯一交易 ID。发送此数据时，请勿更改或解码。请注意，字段名称中的“a”为小写 (PaReq)，但消息名称中的“A”为大写 (PAReq)。

PAREs 3DS 验证回应。发卡行提供的经过压缩的 [base64](#) 编码回应。将此数据传送到 CyberSource 进行检验。

PAREs 状态 3DS 验证回应状态。Visa 和 Mastercard 返回的单字符状态，对于亚洲、中东和非洲支付接口授权为必需数据。

ProofXML 包含 [VEReq](#) 和 [VERes](#) 的 CyberSource 字段，供商户存储。商户可将此数据用于拒绝未来的拒付。

ProtectBuy Diners Club 和 Discover 卡验证服务的商标名称。

Q

请求 ID 标识发送给 CyberSource 的每个交易的唯一 22 或 23 位编号。商户应存储此编号，以供未来参考。

S

SafeKey American Express 卡验证服务的商标名称。

SCMP API CyberSource 之前的名称-值对 API，现已被 [Simple Order API](#) 取代。

Simple Order API CyberSource 最新的 API，提供三种访问 CyberSource 服务的方式：名称-值对 (NVP)、XML 和 SOAP。

Solo Maestro 之前所有的一种借记卡。2011 年 3 月 31 日永久停用。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

S（续）

Switch	请参阅 Maestro 。
商户 ID	每个参与商户的 Mastercard 和 Visa 卡验证过程中必须上传的数据。商户 ID 通常为银行账号或包含银行账号。 注册 检查期间，此数据存储在 目录服务器 中，用于标识商户。
收单处理机构	为商户银行提供信用卡处理、结算和服务的支付处理机构。
收单行	代表商户接受产品或服务付款的金融机构。也称为“收单行”。该银行接收使用其他银行发行的信用卡进行的交易。
收单行 BIN	一个标识收单行的唯一 6 位数字编号。对于每个参与的收单行， Mastercard （以 5 开头）和 Visa （以 4 开头）都有不同的收单行 BIN。
授权	向发卡行发送的，用于确保持卡人的信用卡中有充足的资金进行特定购买的请求。肯定授权将生成授权代码并冻结资金。在 3DS 验证请求的后面，授权必须具有包含支卡注册详细信息的付人验证字段。如果这些字段未正确发送到银行，卡验证提供的责任转移将失效。这种系统性的故障会导致对支付卡公司进行罚款。

T

TermURL	商户网站上的终端 URL，发卡行在其中发布 3DS 验证回应 (PAREs) 消息。
---------	---

U

UCAF	通用持卡人验证字段。针对已注册 Mastercard Identity Check 的卡返回的 base64 编码字符串，专门标识发卡行和 Mastercard 交易。 Mastercard Identity Check 交易采集和发送 AAV 数据的标准。请参阅 AAV 。
UCAF 采集指示符	表示 Mastercard 持卡人是否已经过验证的值：1 或 2。

V

VEReq	检验注册请求。发送到 目录服务器 检验卡是否注册卡验证服务的请求。
VERes	检验注册回应。 目录服务器 对 VEReq 的回应。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

V（续）

Visa 一种全球发行的卡，包含信用卡和借记卡。这些卡以 4 开头。这些信用卡和借记卡在 **CyberSource** 中的卡类型标识符为 001。这些卡参与 **3D Secure** 提供的卡验证服务 (**Visa Secure**)。

Visa Secure (VbV) Visa 卡验证服务的商标名称。

X

XID Visa 和 Mastercard 用于在 **目录服务器** 中标识特定交易的字符串。此字符串值应在整个交易历史中保持一致。

Y

验证结果 发卡行发送的表示验证状态的原始数据。不需要将此数据传送给授权。

已注册 VERes 已注册检验注册回应。Visa 和 Mastercard 返回的单字符状态，对于亚洲、中东和非洲支付接口授权为必需数据。

Z

支付处理机构 处理支付的金融实体。另请参阅 **收单处理机构**。

注册 用于检验卡是否已注册 **Identity Check** 或 **Visa Secure** 服务的 CyberSource 交易。

索引

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

数字

16 和 19 位 Visa 卡 [50](#)

3DS 验证报告

 报告的交易 [159](#)

 解读 [162](#)

 频率 [159](#)

 与支付报告比较 [163](#)

3DS 验证搜索选项 [157](#)

3DS 验证详细信息

 存储期限 [153](#)

 未注册的卡 [155](#)

 已注册的卡 [153](#)

A

AAV

 payerAuthValidateReply_

 ucafAuthenticationData 字段 [137, 141](#)

aesk_attempted [71](#)

AIBMS

 商务交易指示符, 检验 [139](#)

 商务交易指示符, 注册 [136](#)

American Express

 SafeKey [12](#)

 卡测试 [71](#)

 验证结果 [71, 105](#)

B

Barclays

 商务交易指示符, 检验 [139](#)

 商务交易指示符, 注册 [136](#)

Barclays, 检验 XID [141](#)

Barclays, 注册 XID [138](#)

base64 格式, 转换 [27](#)

Business Center 中的申请结果 [152](#)

巴西交易 (Visa Secure)

 payerAuthEnrollService_MCC field [127](#)

 payerAuthEnrollService_mobilePhone
 field [128](#)

 payerAuthEnrollService_
 overridePaymentMethod field [128](#)

 payerAuthEnrollService_productCode
 field [129](#)

报告

 保留时间限制 [159](#)

 汇总 [159](#)

 明细 [164](#)

 明细, XML 格式 [164](#)

 下载汇总报告 [160](#)

C

CAVV [135, 138](#)

测试 [46](#)

 American Express [71](#)

 Diners Club 卡 [81](#)

 Discover 卡 [86, 112](#)

 JCB J/Secure [76](#)

 Maestro 卡 [67](#)

 Mastercard [59, 98](#)

 Visa 卡 [50, 91](#)

存储 3DS 验证数据 [153](#)

D

Diners Club

 ProtectBuy [12](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Diners Club ProtectBuy

验证结果 [81](#)

Diners Club 卡测试 [81](#)

dipb_attempted [86](#)

Discover ProtectBuy

验证结果 [86](#)

Discover 卡测试 [86, 112](#)

电子商务交易指示符 (ECI) [140](#)

F

FDC Germany

商务交易指示符, 检验 [139](#)

商务交易指示符, 注册 [136](#)

发卡行

CAVV [135, 138](#)

验证表格, URL [134](#)

注册检查 [19, 38](#)

H

汇总报告 [159](#)

J

J/Secure [12](#)

J/Secure, 验证结果 [76](#)

JCB

J/Secure [12](#)

测试 [76](#)

基于风险的验证 [177](#)

交易历史记录, 保留时间限制 [159](#)

交易搜索

经过验证的卡 [155](#)

使用 [152](#)

未注册的卡 [155](#)

已注册的卡 [152](#)

交易详细信息

注册检查信息 [152](#)

接受的信用卡类型 [124](#)

结算交易, 时间限制 [158](#)

M

Maestro

(U.K. domestic) 测试 [59](#)

测试 [67](#)

Maestro 卡 [12](#)

Mastercard

Identity Check [12](#)

Mastercard 测试 [59, 98](#)

Mastercard Identity Check

检验结果 [59](#)

密码, 已注册的卡 [18, 19, 20](#)

明细报告 [164](#)

P

PAReq 和 PAREs 存储 [158](#)

PAREs [183](#)

payerAuthEnrollService

示例代码 [143, 144, 145, 146](#)

pb_attempted [81](#)

proofXML 存储 [158](#)

S

SafeKey [12](#)

Streamline

ECI Raw [136, 140](#)

商务交易指示符, 检验 [139](#)

商务交易指示符, 注册 [136](#)

身份检查 [12](#)

示例代码

payerAuthEnrollService [143, 144, 145, 146](#)

使用 3DS 验证的卡授权 [27, 35](#)

授权, 到期或多个 [35](#)

数据存储 [158](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**V**

vbv_attempted [50](#)

Verified by Visa

验证结果 [71](#)

Visa

Visa Secure [12](#)

Visa 卡测试 [50, 91](#)

Visa Secure

巴西交易要求, 产品代码 [129](#)

巴西交易要求, 商户类别代码 [127](#)

巴西交易要求, 手机号 [128](#)

巴西交易要求, 账户类型 [128](#)

检验结果 [50](#)

Visa Vale Alimentacao (VSAVA) [128](#)

Visa Vale Refeicao (VSAVR) [128](#)

Visa, 16 和 19 位卡 [50](#)

W

未注册的卡, 3DS 验证详细信息 [155](#)

X

XID

API 字段 [138](#)

在回复中检验 [141](#)

XML 报告示例 [174](#)

Y

亚洲、中东和非洲支付接口

payerAuthEnrollReply_veresEnrolled

字段 [138](#)

payerAuthValidateReply_paresStatus

字段 [137, 140](#)

验证表格

URL [134](#)

原因代码

检验 [140](#)

Z

注册检查服务

请求 [19](#)

说明 [18](#)

注册数据存储 [158](#)