计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(3):273−278 [doi: 10.15888/j.cnki.csa.006270]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

# 虚拟现实的支付研究与设计①

周继恩, 吴文川, 汤之雄

(中国银联股份有限公司, 上海 201201)
通讯作者: 周继恩, E-mail: jezhou@unionpay.com

**摘　要**: 近几年来, 虚拟现实 (Virtual Reality, VR) 技术发展迅猛, 成为炙手可热的新兴行业. VR 硬件已达到基本成熟的阶段, VR 应用也应势成为新的掘金点, 在影视娱乐、游戏、教育等各个领域都得到了广泛的应用. 但在支付领域, 市场暂无优秀的 VR 支付解决方案. 本文基于虚拟现实的支付研究, 旨在利用 token 技术, 通过 VR 设备内安全模块加密保护银行卡数据和支付数据, 并利用 3D 建模技术构建沉浸式 VR 支付场景, 以寻求安全、便捷、开放的 VR 支付方案. 研究结果表明, 该设计解决了现今 VR 支付产品交互难、安全性低的问题, 并且有效提高了支付成功率.

**关键词**: 虚拟现实; 支付; token 技术; 安全模块; 3D 建模

引用格式: 周继恩,吴文川,汤之雄.虚拟现实的支付研究与设计.计算机系统应用,2018,27(3):273–278. http://www.c-s-a.org.cn/1003-3254/6270.html

## Payment Research and Design Based on Virtual Reality

ZHOU Ji-En, WU Wen-Chuan, TANG Zhi-Xiong

(China UnionPay, Shanghai 201201, China)

**Abstract**: With the rapid development in recent years, Virtual Reality (VR) has been one of the hottest new technologies in the world. VR hardware has become more mature, and VR apps has been widely used in various fields such as entertainment, gaming and education. But there is no good VR payment solution in current payment domain. Based on virtual reality payment research, this paper uses token technology to restore payment data into security module embedded in VR devices, and constructs immersive VR payment scene by using 3D modeling technology, to provide a safe, convenient and open VR payment solution. The results show that the design solves the problem of the bad interaction and low security in current VR payment, and it effectively increases the payment success rate.

**Key words**: virtual reality; payment; token technology; security module; 3D modeling

## 1　引言

虚拟现实是一种集成性的信息技术, 综合了计算机图形图像处理、互联网、传感器、多媒体、人机交互、仿真系统等多种技术[1], 可以为人们呈现一个具有较强沉浸感、模拟真实环境的虚拟世界. 通过多年的研究和改进, 虚拟现实技术已经在多个领域得到应用[2], 比如虚拟购物场景, 用户只要在家戴上 VR 设备即可身临其境般享受购物乐趣, 在虚拟现实中看到产品的真实大小并且全方位仔细查看商品, 从而大大提升了购物体验. 购物过程的重点在于体验, 而购物体验最终会落在支付.

目前的 VR 应用在支付时的交互方式主要分为以下两类: 一类产品在支付过程中, 需要用户取下 VR 设备, 通过传统互联网支付方式完成, 这一类产品的支付环节与 VR 场景脱离, 本质上并非虚拟现实支付. 而另一类产品, 如正处于实验阶段的蚂蚁金服的 VRPay, 通

① 收稿时间: 2017-07-03; 修改时间: 2017-07-17; 采用时间: 2017-07-24; csa 在线出版时间: 2018-02-09

过在 VR 环境中构建二维虚拟键盘的方式, 让用户通过凝视键盘来完成支付要素的填写, 这样做虽然支付过程延续了“虚拟现实”的场景, 但让用户在 VR 场景下输入支付信息会导致用户体验不佳, 并且存在着泄露支付要素的风险, 给用户带来了财产安全隐患. 这两类产品所遇到的共同问题即如何在保证安全的情况下给用户带来便捷、友好的交互体验, 这正是目前 VR 支付行业的痛点.

不同于以上两类 VR 支付产品, 本文设计的 VR 支付方案旨在利用支付标记化 (token) 技术保证持卡人支付安全与便捷, 通过安全模块加密保护终端存储的银行卡数据和支付数据, 利用生物特征验证用户身份, 避免支付数据输入, 利用 3D 建模技术构建沉浸式支付场景, 从而设计出一种既能提升用户体验, 同时又保证安全性的解决行业痛点的标准支付方案.

## 2 VR 支付的技术研究

### 2.1 支付标记化

支付标记 (Payment Token) 指符合主账号 PAN 的基本验证规则 (如 LUHN 算法校验) 的一个替代值. 在本文的支付方案中, 利用 token 代替银行卡号, 用 token 的有效期代替银行卡号的有效期, 确保了敏感信息在交易时的安全.

在支付标化系统中有两个重要角色, 即标记请求方 (Token Requestor, TR) 和标记服务提供方 (Token Service Provider, TSP). 其中 TR 作为标记请求的实体需遵循 TSP 的注册流程、技术规范与管理标准[3]. 在 TSP 成功注册后, TR 将被分配一个 TR ID, 同一实体在不同 TSP 注册 TR, 或同一实体在同一 TSP 注册不同交易渠道的服务将被分配不同的 TR ID.

在支付标记化系统中, TR 向 TSP 申请 token, 并同步管理需要应用 token 的实体 (商户、持卡人等). TSP 负责对 token 进行分配管理、去标记化等, 是支付标记化系统的核心, 它根据不同的业务场景、受理渠道以及标记的应用域控, 制定与之配套的个性化参数和控制措施, 最终达到标记交易控制和风险监控. 其架构如图 1 所示 (其中实线箭头代表已有系统的数据交互, 虚线箭头代表标记服务相关应用接口).

### 2.2 安全模块

安全模块用于提供金融信息的安全存储以及安全访问控制, 包括对称、非对称加解密算法和数字证书的下发与更新、银行金融数据的动态下发、删除和更新、金融数据的安全隔离、提供安全交易的 API.

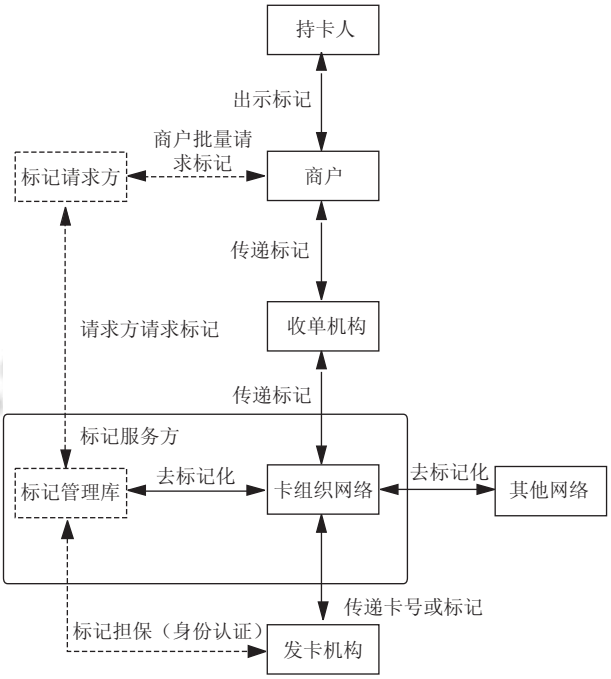


图 1 支付标记化结构图

安全模块分为硬件和软件两类. 硬件的安全模块主要是 eSE 安全芯片或 swp-SIM 卡[4]; 软件的安全模块主要是基于白盒密码技术的程序[5]. 目前, 市场上 VR 设备主要是手机, 而主流手机设备大多具有安全芯片或支持插入 swp-SIM 卡, 因此 VR 设备大多支持基于硬件的安全模块方案. 对于不支持硬件安全模块的手机, 可以选择采用白盒密码技术实现的软件安全模块来保护金融数据.

在 VR 支付方案中, 首先通过安全模块与平台间建立端到端的安全通道, 在线下发银行卡信息及算法密钥, 并存储在安全模块内; 接着, 安全模块的访问权限控制机制将杜绝其他应用对安全模块内金融数据的访问, 只有白名单应用才具有对安全域内数据读取和更新的权限; 最后, 应用通过安全交易 API 访问数据, 使用非对称密钥加密及签名保护, 防止支付信息的泄露和篡改.

### 2.3 VR 建模

为了构建一个沉浸感强的支付环境, 采用全景图进行环境建模是一种高效的方式. 全景图一般通过照片、视频、3D 模型等表现形式, 构建出大于双眼正常

有效视角的环境, 它是一种新的图像信息组织模式, 可以表达完整的周围环境信息, 相对于对于观察者而言, 是建立在图像上立体的多角度的图形环境[6].

采用全景图进行环境建模, 不仅比基于几何的 VR 建模真实感更强, 而且其细节复杂性对运行速度几乎无任何影响. 另外, 当今出货量最多、普及率最广的 VR 设备是基于手机的, 由于手机在刷新率、CPU 性能等硬件条件上亚于基于 PC 的 VR 设备, 所以全景图的高效性在手机 VR 应用上将会得到更大发挥.

本文在设计中采用了球面全景图来构建支付环境, 利用 3D 建模等技术构建支付页面、选卡页面等, 整个虚拟场景是按以下步骤生成的:

(1) 利用采集的离散图像或连续的视频作为基础数据, 经过处理形成全景图像;

(2) 通过合适的空间模型 (如球面、六面体、柱面等, 本文选取了球面) 把全景图像组织成虚拟全景空间.

(3) 在全景空间里建立物体, 即 3D 模型、2D 模型等 (如 3D 商品、2D 银行卡等).

(4) 通过一些脚本为物体做控制处理, 让这些物体为用户带来友好的交互体验.

基于以上的 VR 建模, 用户便可在构建出的虚拟场景中进行前进、后退、360 度环视等一系列真实环境下的行为操作, 沉浸感强、交互友好.

## 3 VR 支付的设计

### 3.1 架构设计

为了在高频交易下兼顾用户体验与安全, VR 支付方案需满足 4 点要求: 1) 高可用性: 保证用户联网情况下顺畅支付; 2) 可伸缩性: 保证架构设计强内聚、松耦合; 3) 高性能: 保证终端用户便捷访问; 4) 安全性: 保证金融数据与交易过程安全. VR 支付方案的技术架构设计如图 2 所示.

VR 支付系统主要包括 5 部分: VR 支付控件、安全模块、在线支付平台、可信服务、TSP 等.

(1) VR 支付控件: 在 VR 场景中为用户提供支付入口, 让用户选择支付卡和优惠, 利用生物识别认证用户身份, 动态生成支付数据密文, 并通过线上支付平台验证支付数据和承兑交易.

(2) 安全模块: 基于设备 eSE 的安全域或基于白盒码的软件安全模块, 用于存储银行卡信息及加密密钥, 并提供安全访问接口.

(3) 线上支付平台: 提供线上支付接入、验证支付数据并承兑交易.

(4) 可信服务: 与运营商、终端厂商等可信服务系统互联, 为银行提供空中发卡、安全模块生命周期管理等服务.

(5) TSP: 提供支付标记化服务.

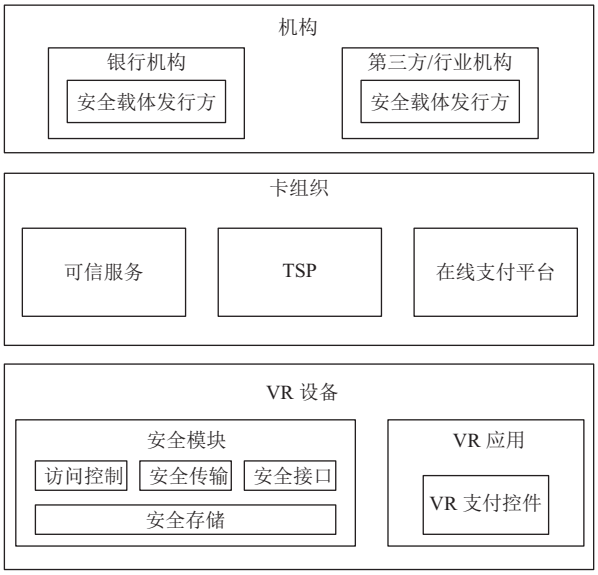


图 2 技术架构图

### 3.2 流程设计

虚拟现实中的支付行为需要兼顾用户的体验、安全等多方面因素. 所以本文在支付流程的设计上尽可能优化交互流程, 让支付的数据流程更加便捷安全.

#### 3.2.1 交互流程

在 VR 购物场景中, 用户首先进入商品选择流程, 选择要购买的商品. 为了让用户获得沉浸式的体验, VR 购物应用会构建出虚拟货架、商品、标签等在现实世界中真实存在的对象, 仿造出一个真实的购物环境. 用户选择商品后, 商品选择页面上呈现选中商品的 3D 模型、商品详情和价格等信息, 为用户进一步展示商品细节, 帮助用户选择心仪的商品. 在用户选定某一商品后, 进入 VR 支付流程. 支付页面以浮动屏幕的形态展现在商品的旁边, 支付页面中包含可选银行卡、优惠信息、分期信息等. 实现的 VR 支付页面图如图 3 所示.

当用户选择一张银行卡作为支付卡时, 只需要凝视该卡一定时间, 系统就会自动读取卡信息并生成支付数据, 同时用户可以通过凝视等操作选择银行卡对

应的优惠信息, 确认支付便可发起支付请求、完成支付. 支付结果如图 4 所示.


图 3 VR 支付页面图


图 4 VR 支付结果图

整个交互流程可走免密支付, 这样就避开了 VR 场景下输入信息难的问题, 支付过程简单、便捷.

3.2.2 数据流程

当用户凝视选择确认支付时, VR 支付控件根据在线支付平台所创建的订单号, 将 token 等支付信息上送至在线支付平台进行处理, 数据流程如图 5 所示.

总体步骤如下:

(1) 客户端通过交易流水号 (TN) 调用 VR 支付控件.

(2) VR 支付控件向银联在线支付平台发送 (TN) 请求订单信息.

(3) 银联在线支付平台根据 TN 下发商户订单信息.

(4) 用户通过 VR 支付控件确认支付后, 由向银联后台发起支付请求.

(5) 银联在线支付平台上传 ARQC 到银联 TSP 平台做校验, 并拿到授权应答.

(6) 银联在线支付平台将去标记的卡 Pan 上送至银行进行验证, 并拿到授权结果.

(7) 银联在线支付平台处理支付.

(8) 银联在线支付平台将支付结果返回给 VR 支付控件与商家后台.

(9) VR 支付控件根据支付结果进行虚拟场景下的支付结果展示.

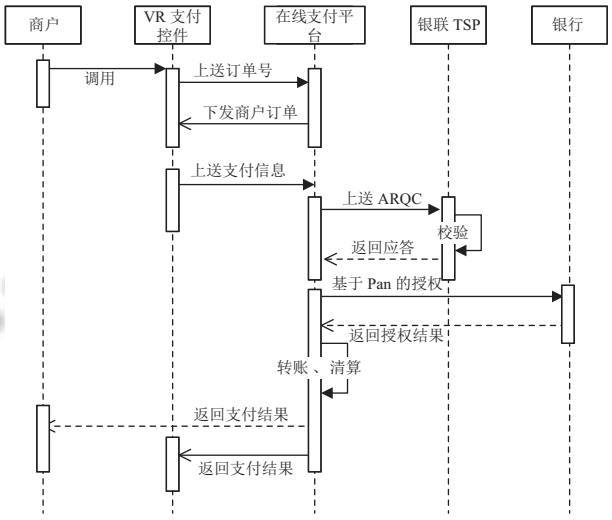


图 5 VR 支付时序图

### 3.3 安全设计

VR 支付场景中, 由于信息输入导致交互体验不佳, 因此在方案设计时, 为避免让用户输入信息做交易验证, 而采用通过生物识别验证用户身份, 然后动态生成支付数据作交易验证的方式. 在此方案中, 保证支付安全成为整个方案的核心关键. 而支付安全性需要分别从业务安全性和技术安全性两方面着手.

3.3.1 业务安全

在业务安全性上, 主要从业务流程上降低用户银行卡信息泄露危害以及防止冒用他人身份在 VR 场景中完成支付. 业务流程分别从银行卡信息安全和用户身份认证两个维度来保证安全性.

(1) 银行卡信息安全

为降低银行卡信息泄露带来的危害, 将下发的 token 与特定银行卡、设备及 VR 支付渠道绑定, 因此存储在安全域中的金融数据只能用于该银行卡在当前设备上完成 VR 支付, 即使 token 号等金融数据泄露也不能在其他场景或设备上支付, 使银行卡信息得到保护, 防范了风险.

(2) 身份认证

为防范身份冒用, 在用户使用设备或开启应用前, 要求用户通过指纹解锁设备和开启应用, 借助生物特

征技术, 保证了只有已录入指纹的用户才具有该设备和应用的操作权限, 并获得 VR 支付授权; 其次, 在商户应用需要支付时调起 VR 支付控件, 此时用户无需再次验证身份, 通过之前验证身份获得的授权, 访问当前设备上存储的金融数据, 并使用支付密钥对金融数据进行加密和生成签名, 这样就保证了只有该设备和在该设备上完成验证的用户才能发起支付.

因此, 本方案利用 token 与生物特征识别技术, 建立用户与特定设备的绑定关系, 并根据用户身份验证结果授权该用户使用当前设备存储的金融数据进行支付, 来保证非密码验证情况下的支付安全性.

3.3.2 技术安全

技术方案上, 分别从金融数据下发、金融数据存储、和金融数据支付三个过程来保证支付的安全性.

(1) 金融数据下发

安全模块内预置通讯密钥, 包括敏感信息密钥 DEK、报文密钥 S_ENC、验签密钥 S_MAC, 每次金融数据下发前, 客户端与服务端分别生成随机数, 利用随机数和序列数作为随机因子对预置密钥做分散产生会话密钥, 之后通讯数据均使用会话密钥加密. 由于序列数动态更新, 因此会话密钥一次一密, 保证通讯过程中金融数据安全性. 下发的金融数据包括银行卡 token、卡交易数据以及支付密钥等, 用于支付过程中生成动态支付数据密文. 安全模块的架构如图 6 所示.

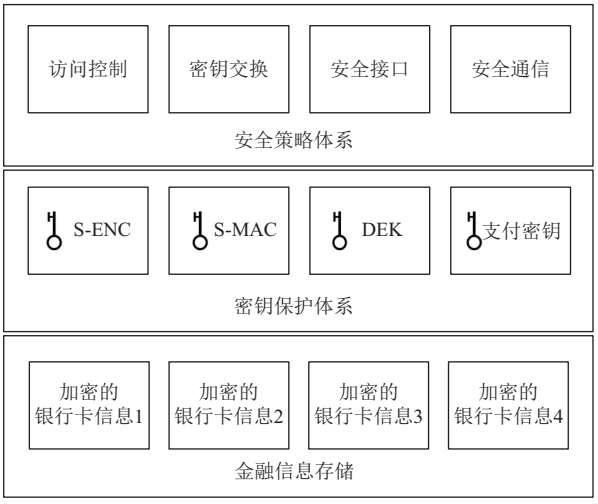


图 6 安全模块架构图

(2) 金融数据存储

可信服务下发的金融信息和支付密钥加密存储在安全模块内. 对于基于 eSE 实现的安全模块, GP 规范限制卡内其它应用直接读取金融安全域内的数据; 对于基于白盒实现的安全模块, 在金融数据和密钥下发后, 采用白盒转加密完成通讯密钥解密和存储密钥加密过程. 存储密钥由根密钥加上终端设备信息分散得到, 一设备一密, 保证了存储数据的安全性. 同时, VR 支付使用动态生成的支付密文做交易验证, 保证了金融数据密文即使被获取也无法用于支付.

(3) 金融数据使用安全

首先, 支付控件和安全模块分别对调用方做权限验证, 通过 APP 包名签名校验且在白名单内的应用方可调用接口; 其次, 支付过程不使用静态的金融数据作验证, VR 支付应用在验证用户身份通过后, 基于安全模块中的金融数据及支付密钥动态生成支付密文, 支付密文与其他支付信息一起上送服务端完成验证和支付. 支付密文中包含银行卡 token、卡数据等静态信息以及操作序列数、时间等动态信息, 保证了支付密文无法被窃取, 且其密文无法被重放.

因此在安全模块的保护下, 当用户在使用自己的 VR 设备进行购物、消费时, 黑客无法通过软件层面的攻击来获取隐私信息, 整个支付过程都是安全的, 并且高于蚂蚁金服 VRPay 的安全等级.

## 4 结果分析

为验证 VR 支付方案的可用性和可靠性, 在三星 Galaxy S6 edge+上对 VR 支付场景与过程进行了模拟. 金融数据存储方案分别采用基于 eSE 和白盒实现的安全模块, VR 头戴设备为三星 Gear VR, 支付链路为银联在线支付平台系统. 经模拟测试:

VR 支付与传统移动支付各步骤平均耗时对比如表 1 所示, VR 支付成功率如表 2 所示.

表 1 VR 支付与传统移动支付各环节平均耗时对照 (单位: s)

| | VR支付 | | 传统移动支付 |
|---|---|---|---|
| | ese模式 | 白盒模式 | 快捷支付 |
| 选卡耗时 | 1.5 | 1.5 | 1.2 |
| 支付耗时 | 2.3 | 1.6 | 2.1 |
| 总计 | 3.8 | 3.1 | 3.3 |

表 2 VR 支付与传统移动支付成功率对照

| | VR支付 | | 传统移动支付 |
|---|---|---|---|
| | ese模式 | 白盒模式 | 快捷支付 |
| 总笔数 | 200 | 200 | 200 |
| 成功笔数 | 171 | 195 | 192 |
| 成功率(%) | 85.5 | 97.5 | 96.0 |

由表 1 和表 2 可知: 在 VR 支付方案中, 基于 eSE 安全模块的支付耗时比白盒模式高, 原因在于 eSE 模式读取金融安全域时有更多的指令交互. 在支付成功率上, VR 支付比传统移动支付的成功率更高, 原因在于 VR 支付省去了密码输入过程, 避免了密码错误导致的交易失败; 同时, VR 支付交互设计较为简易、直观, 没有用户因为不熟悉支付操作而交易失败.

## 5 结论与展望

本文利用支付标记化技术, 通过 VR 设备内嵌的安全模块加密保护银行卡数据和支付数据, 设计出一种标准的支付方案, 利用 3D 建模技术构建出沉浸式的支付场景, 解决了 VR 市场上支付产品交互难、安全性低的问题, 填补 VR 支付产品的空白, 促进 VR 产业的健康发展. 期望通过本项目的研究, 促进 VR 支付产业的规范化, 为进一步为形成 VR 支付的行业标准奠定基础. 另外, 在进行大额消费时, 增强验证是一个必不可少的环节, 如何在 VR 环境中更方便快捷地认证用户身份, 是一个难点, 也是一个具有应用价值的研究方向.

## 参考文献

1 斯凯·奈特. 虚拟现实: 下一个产业浪潮之巅. 2 版. 北京: 中国人民大学出版社, 2016: 11–13.
2 王寒. 虚拟现实: 引领未来的人机交互革命. 北京: 机械工业出版社, 2016: 20–21.
3 EMVCo. Payment tokenization. https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2.0.pdf. [2017-09].
4 GlobalPlatform. 可信执行环境：以更低的成本实现更安全的移动市场. https://www.globalplatform.org/documents/whitepapers/GP_WhitePaper_TEE_2015_chinese.pdf. [2015-06].
5 林婷婷, 来学嘉. 白盒密码研究. 密码学报, 2015, 2(3): 258–267.
6 周晓成, 张煜鑫, 冷荣亮. 虚拟现实交互设计. 北京: 化学工业出版社, 2016: 132–139.