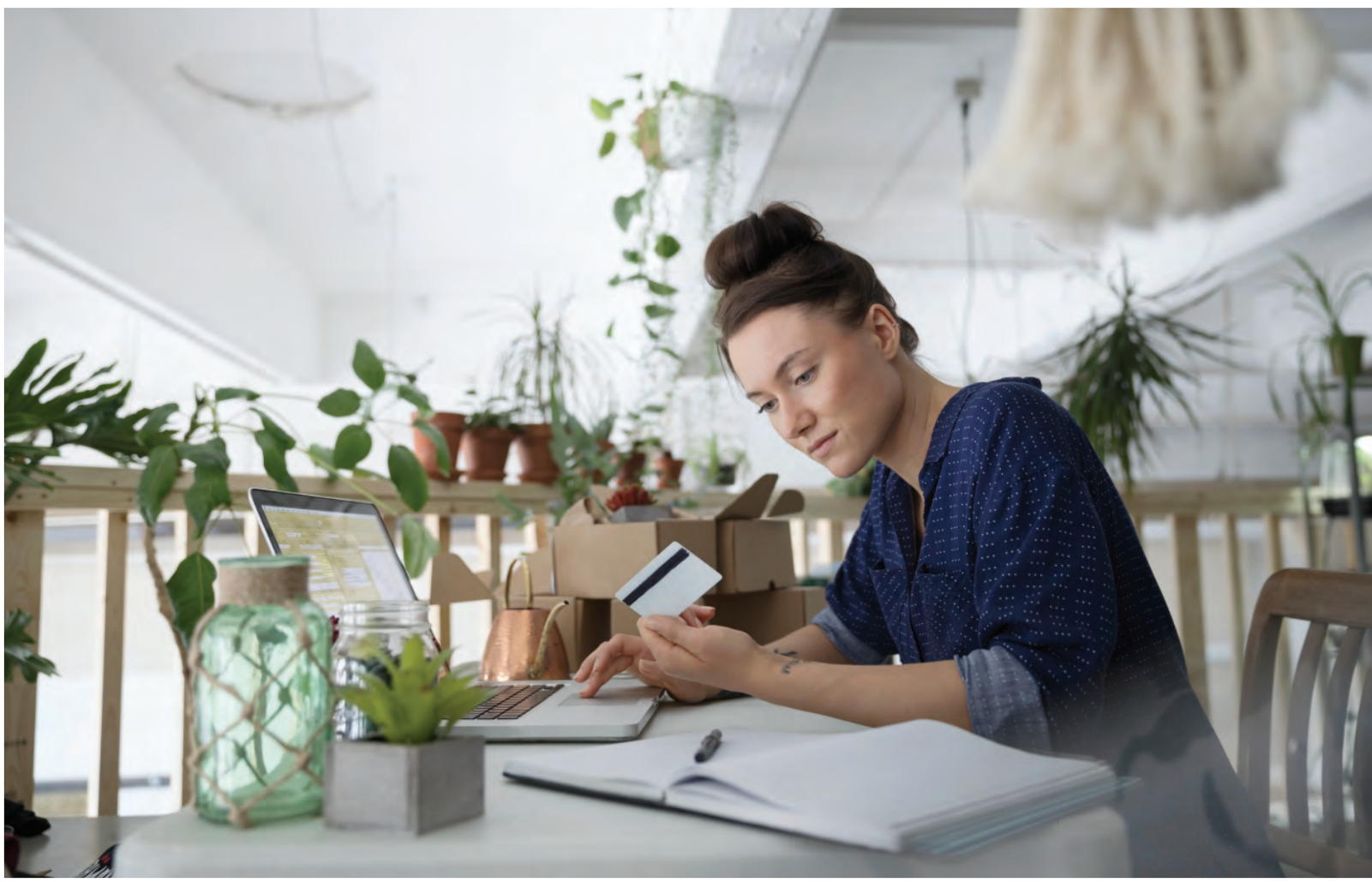
InterSystems IRIS数据平台，护航信用卡数据存储安全

解决方案指南



InterSystems™
IRIS Data Platform

简介

越来越多的购买和支付行为通过信用卡完成。虽然接受信用卡的商户和服务提供商有义务保护客户敏感信息，但他们使用的软件解决方案可能无法为信用卡信息提供最佳保护。为了解决这一问题，行业制定了信用卡信息安全标准，并广泛采纳。

支付卡行业（PCI）数据安全标准（DSS）是一组全面的指南，旨在确保持卡人信息安全，其中一个规定是建议将客户信息存储在数据库中。本文为软件供应商提供了指南，以阐明如何利用InterSystems IRIS数据平台来达到PCI DSS（支付卡行业数据安全标准）数据存储要求。

应用案例：保护信用卡信息

在数据库中保障信息安全的最好方式是绝对不要保留（或存储）它们。然而，企业在同信用卡数据打交道的过程中不得不收集很多信息，例如持卡人姓名、个人账号（PANs）、卡片失效日期和安全码。PCI DSS推荐只获取关于持卡人数据的最少量、最必要的信息。当不得不存储持卡人数据时，PCI DSS要求（至少）在数据库和所有日志中呈现的PANs信息应为不可读。

具体如何保护PANs信息会因使用目的不同而有所差异。通常来说可以分为两类：信用卡纯粹被用于验证，或者被用于商品或服务的支付方式。

利用信用卡进行验证

当应用被设计为接受信用卡作为身份验证的形式时（例如，当某人使用信用卡检索其航空预订记录时），根本不需要存储明文PAN。根据PCI DSS规定，可以使用哈希算法（Hashing）或截断（Truncation）来存储账户（PAN）的某个片段，足以用于验证即可。

- **哈希算法**

  信息根据复杂的算法进行转换，只存储转换后的版本或散列后的版本。哈希算法是一种单向工作方式——即不可能从哈希版本获取关于原始信息的特定内容。出于验证目的时，可以将持卡人提供的PAN哈希版本与存储的哈希值进行比较。

- **截断**

  只存储部分信息。出于验证目的，持卡人提供的PAN以相同的方式被截断并与存储值进行比较。一般来说，截断提供的安全性比哈希算法弱。

利用信用卡进行支付

接受信用卡支付的应用必须能够访问一个可用的PAN来处理事务。根据PCI DSS，有三种处理PAN信息的方式可被接受。

- **完全不持久化（磁盘上存储）PAN**

  例如，当某人使用信用卡在线购物或以“客人”的身份退房时，可能会发生这种情况。持卡人每次购物都必须提供完整的PAN。应用程序将在内存中使用PAN，但不会持久化它（PCI DSS包含了在传输过程中保护PAN和其他敏感信息的指南，但这超出了本文范围）。

- **截断**

  只存储了PAN的一部分。持卡人必须提供缺失的信息，以便应用程序在内存中重组PAN。一个可用的PAN只会存在于内存中，而不在磁盘上。

- **加密**

  根据复杂的算法，使用加密密钥将PAN转换为密文或明文，但只存储密文。与哈希算法不同，加密允许双向转换。使用加密密钥，应用程序可以解码PAN并使用它（在内存中）处理信用卡事务。

  PCI DSS要求使用“强”加密，并定期对信息进行重新加密。此外，加密密钥不能存储或绑定到用户帐户中。

InterSystems IRIS护航数据存储

InterSystems IRIS数据平台为应用程序提供了一个稳健、一致、高性能的安全架构。

以下介绍了InterSystems产品是如何为诸如PANs这类存储数据保驾护航的：

- **哈希算法**

  InterSystems IRIS对哈希数据提供了几种安全哈希算法（例如SHA-1）的嵌入式访问。

- **截断**

  完全支持和满足运行在InterSystems IRIS数据平台上的应用程序。

- **数据加密**

  InterSystems IRIS采用高级加密标准（AES）算法。

  利用静态数据加密，整个数据库和前后图像日志都使用一个加密密钥加密。对密钥的访问由系统管理，因此用户帐户（例如，业务）不会拥有数据库加密密钥。

  被存储在加密数据库中的所有信息（包括索引）都会得到保护。

- **数据元素加密**

  通过提供加密套件，InterSystems IRIS能够使开发人员加密单个信息片段。数据元素加密通常被用于存储敏感信息，比如PANs，因为允许（在正确的配置下）对数据元素重新加密，而且不会中断数据库访问。

- **审计**

  InterSystems IRIS提供了健壮的、抗篡改的审计系统，可以对安全模型的所有更改进行审计。应用程序开发人员可以通过在代码中嵌入对审计系统的调用来使用相同的审计数据库。

InterSystems IRIS安全模型中的密钥管理

由于PCI DSS的广泛应用，InterSystems IRIS平台特意设计了一些功能，使构建符合标准的应用程序变得更容易。它们主要涉及数据元素加密所使用的密钥管理。

管理密钥

用于数据元素加密的加密密钥材料，系统将其存储在与数据库加密密钥相同的内存位置进行保护。应用程序可以使用唯一KeyID进行单个加密密钥，从而避免了对密钥材料本身的直接访问。

为了简化开发人员的工作，当使用这种新的数据元素加密方法时，KeyID被嵌入到生成的密文中。这样解密时能够自动识别用于加密数据的密钥。除了数据库加密密钥外，新的密钥管理系统还支持多个类似的密钥。这样应用开发人员可以很容易地满足实时重新加密的需求，而且几乎不会影响已部署的应用程序的性能。

结论

世界各地需要安全处理信用卡信息的商户和服务提供商都在采用PCI DSS，应用程序的提供者们也要确保其解决方案符合这一标准。

InterSystems IRIS为开发人员提供了构建符合PCI DSS的应用程序的能力，并将使这一任务变得更容易。

InterSystems是驱动世界上众多重量级行业应用的信息技术引擎。在医疗、金融、政府和诸多涉及国计民生的关键领域，InterSystems赋予了每一项重要成就以科技的原力。InterSystems创立于1978年，是一家总部位于美国马萨诸塞州剑桥市的私人控股公司，并在全球设立分支机构，其软件产品每天都在80多个国家服务于数百万用户。

更多详情，敬请登陆：https://www.intersystems.com/cn/products/intersystems-iris

InterSystems 中国

系联软件（北京）有限公司
北京市朝阳区建国门外大街乙 12 号
双子座大厦（东塔）1902 室
电话：+86 10-8524-9700
传真：+86 10-8524-9755

InterSystems.com/cn

为成就未来，赋予科技原力

InterSystems®
Health | Business | Government