客户成功案例聚焦

全球十大银行之一

Bloombase® Spitfire SOA™
信息安全服务台

Bloombase® Spitfire StoreSafe™
存储信息安全服务台

Bloombase® Spitfire KeyCastle™
密钥管理服务台

Bloombase® Spitfire™ High Availability
高可用性模块

全球某十大银行之一，在全球拥有超过 12,000 间分行。其核心银行系统支持柜员及后台职员等众多用户，以提供各项重要服务，例如转账、票据结算、银行间电汇、自动付款、信用分析及客户服务等等。他们成功部署了 Bloombase Spitfire 信息安全服务器，从而确保了信息交换、数据仓库及灾难后复原基础设施的机密性、完整性及真实性都能符合各种严格的行业、国家及其内部的信息安全管制规范。

客户成功案例概况

关于客户

- 全球十大银行之一
- 分行数量：超过 12,000 间
- 员工人数：超过 250,000 人

概要

保护银行间交易数据，以避免这些基于 XML 的 SOA 传输中数据在经由互联网、通过虚拟专用网络传送时被盗取或篡改，以及在硬件或媒介被盗的情况下、保护数据库及已存储备份数据在免受非授权盗用。

主要挑战

- 为 SOA 信息安全、数据库加密、备份数据保护及全面的生命周期密钥管理提供单一而全面的解决方案
- 符合 OASIS ebXML 及 W3C XML 数字签名和加密标准
- 高吞吐量 XML 交易安全处理
- 数以 GB（千兆字节）数据量的 XML 交易报文安全批次处理
- 在线数据库传输中加密和解密
- 保护备份存档数据免遭盗用及篡改
- 不容许密钥交换及支持自动废止密钥
- 无需更改用户、管理员及操作员工作流程
- 关键性功能及容错能力
- 可与实时数据复制服务实现互操作能力，以支持存储同步

概况

某大全球性银行在全球 20 多个国家设有超过 12,000 间分行，并通过将分布于各间分行的分布式计算机基础设施互联起来、实现电子数据交换，支持各方面的业务运作，包括柜员服务、客户服务、转账、银行间转账、商户交易结算、自动付款及信用分析等等。该客户以往采用成本高昂的专用通信网络、即专用增值网络 (VAN)，以支持信息交换，当中包含了大量不能为外人知悉或篡改的高度敏感及机密数据。他们每间分行都拥有存储了机密客户数据的本地数据库，这样可避免因网络故障而影响业务运作及商业连续性。他们还设有用于批次交易的数据缓存区，当中包含仍未结算、并要在数小时后与总部中央结算系统进行同步处理的高度敏感金融信息。

为应付交易量的增加、提高服务可用性及减低总拥有成本 (TCO)，客户计划将网络载体由专用 VAN 转移到互联网。不过，互联网虽能带来多路由及节省成本等得益，但同时也增加了信息受到攻击的

BLOOMBASE®
博隆兴中

项目目标

- 保护以 XML 及/或专用平面文件 EDI 类数据形式进行的银行交易的机密性、真实性及完整性
- 确保存储于关系数据库系统的机密性客户数据的保密性
- 保护备份媒介和硬件，避免非授权盗取和篡改敏感存档数据
- 自动化、全面的生命周期密钥管理

解决方案及服务

- Spitfire SOA™ 安全服务器
- Spitfire StoreSafe™ 企业存储安全服务器
- Spitfire KeyCastle™ 密钥管理服务器
- Spitfire High Availability 高可用性模块

为什么选择 BLOOMBASE 的解决方案

- 高度安全、基于行业标准
- 高性能、高处理吞吐量及低等待时间
- 可处理庞大数据载荷及巨大的数据量
- 经过实践验证，并可应付关键性任务
- 硬件、平台及软件均具备互操作能力及可移植性
- 可配合硬件和平台资源进行扩充、以应付未来的增长需求
- 透明操作及管理
- 数据拥有及操作完全分离
- 高速自动加密、解密、生成签名及验证功能

可能性。传统的链接加密器及虚拟专用网 (VPN) 会考虑加强信息的保密性及完整性，以应付外来的攻击，但这些方法很容易被来自网络加密终点的核心攻击所击破。由于基于网络的防护并不足够，客户便转而采用深入的应用层数据保护方法，这些方法可有效保护经网络传送的交易信息的机密性、真实性及完整性，而永久性数据保护可避免敏感数据库及备份信息受到非授权盗用及篡改。

该客户的信息技术安全小组在设计整体解决方案时发现了多项重大设计缺陷。他们手上的现有技术和产品很难克服这些问题，但若不妥善解决的话，更无异于完全没有安全防护措施。第一个重大问题是各个分行网点的大量密钥的管理、安全信托交换及废止操作；其次是所建议的专用限定平面文件（指无格式文件）数据加密格式的数据字段和信息难以扩展、以适合将来使用；其三是可用的企业级数据密码库都无法成功处理数百 MB（兆字节）至数以 GB（千兆字节）的批次交易量；最后也是最关键的，数据库及备份加密实用程序都要求对平台、软件及应用程序作出重大变更，这当然不会获得客户的接受。

客户最后选择了 Bloombase 的 Spitfire 信息安全服务器平台，以实现全透明、可无限扩充到点对点数据保护。Bloombase Spitfire SOA 安全服务器利用先进的加密及数字签名技术，保证了交换信息的机密性、完整性及真实性。采用 Bloombase Spitfire StoreSafe 存储安全服务器，无需更改应用程序便可实现数据库、文件及备份媒介的透明性加密。Spitfire KeyCastle 密钥管理服务器不但能保护加密密钥，而且提供了集中式的全面生命周期管理。

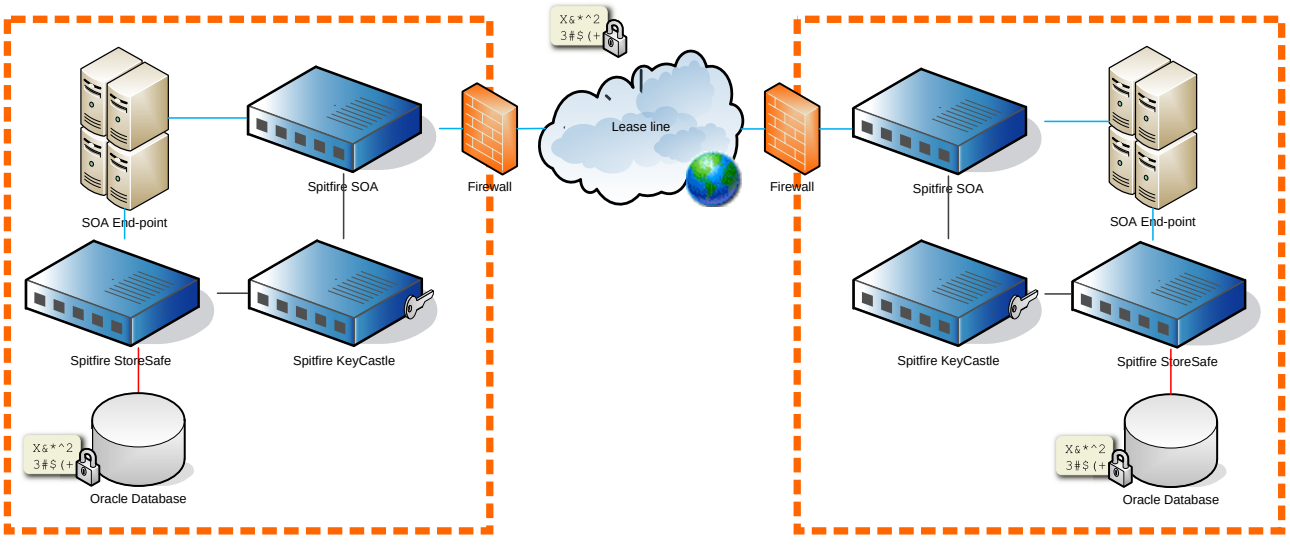
高度安全的银行间及银行内部信息交换

为配合客户在传输中数据保护方面的信息保密需求，Bloombase Spitfire SOA 安全服务器通过加密和数字签名，保护在 OASIS ebXML 相容信息包中封包的 XML 及平面文件信息载荷。Bloombase Spitfire SOA 安全服务器支持以幹路 (pass-through) 模式或旁路 (look-aside) 模式操作，前者以 SOA 终点代理形式出现，后者则应用于 SOA 终点远端调用。Spitfire SOA 安全服务器根据预定义的规则为 SOA 载荷提供透明的保护；而预定义规则则在其基于规则的安全处理引擎中配置。

在 SOA 终点产生的外传银行交易信息会在 Spitfire SOA 安全服务器中被截住，其中机密性载荷会首先由接收者的密钥加密，其后再由发送者的私人钥匙签名。受保护的 ebXML 封包穿过 VPN，而当中，盗取信息者无法在 Spitfire SOA 加密前取得私人信息。在信息抵达接收者时，Spitfire SOA 安全服务器会充当接收者终点代理，并通过验证数字签名的真实性、核实信息发送者的身份及完整性。若证实这些信息有效，Spitfire SOA 安全服务器即会在将无格式原始电子交易信息呈交给实际接收 SOA 服务终点前，自动将经加密的载荷内容解密，然后才展开实际的商业应用处理操作。这样便保障了分行间数据交换的信息保密性、内容的完整性及信息来源身份。

与传统的数据密码库不同，Spitfire SOA 安全服务器是针对性设计的高度链式服务器，它能处理数以 GB 计、甚至更庞大的载荷数据，也能同时处理大量同时发生的信息请求，从而支持客户的实时网上业务运作及资源密集的离线批次处理需求。

Bloombase Spitfire KeyCastle 密钥管理服务器则可让客户集中管理密码钥匙。Spitfire KeyCastle 以公钥基础设施 (PKI) 技术设计和制造、避免了令人头痛的不安全密钥交换。由于无需共享秘密，因此不但为密钥提供了真正的保密性，而且在各个个别网点建立了信任和钥匙有效性，从而让客户简化了管理、同时加强了密钥管理的安全性。



BLOOMBASE®
博隆兴中

永久性存储数据 – 保护及安全

在永久性数据保护方面，客户采用 Bloombase Spitfire StoreSafe 存储安全服务器保护其 Oracle 数据库、文件系统及备份存档。Bloombase Spitfire StoreSafe 存储安全服务器配备存储块设备及磁盘代理，可为数据库服务器虚拟化实际数据库存储及备份磁带设备，以及象无格式永久性数据般备份代理、以作存取之用。Spitfire StoreSafe 将加密技术应用于企业存储通信基础设施，为机密信息加密的写操作提供虚拟磁盘，另一方面又在存储读取操作方面对加密敏感数据自动进行解密。

“Bloombase Spitfire™ 企业信息安全平台将传输中数据保护、存储数据加密及密钥管理结合于同一套解决方案，不但带来了很高的投资回报 (ROI)，而且还能提供无限的扩充能力和扩展性。”

机密性银行交易和客户数据经加密后存放于物理磁盘、磁带及虚拟磁带库 (VTL) 中，无论管理员、操作员或入侵者都无法存取纯秘密信息。即使在最糟糕的情况下、存储媒介被取走或硬件被盗，机密信息也能保持其秘密性，从而满足了客户的行业和内部信息安全需求。

Spitfire StoreSafe 虚拟存储配置简易、操作透明，并且无需改动数据库系统和备份基础设施。由于不必改动应用程序，因此不但为客户节省了再次配置所费的人力，而且将对现有计算机系统服务的影响减到最低，从而为客户带来既高效、又更为安全的银行系统。

总而言之，由于传输中和已存储信息更加可靠，因此既加强了信息保密及完整性，又不会影响用户的满意度及运作效率，从而帮助客户进一步实现各项目标，包括节省成本、加强服务、增加顾客信心、提供有效的风险管理，以及为下一个层次的商业部署做好准备等。

了解更多详情

如需进一步了解有关银行及金融机构方面的 Bloombase 信息安全解决方案，请联系 Bloombase 营业代表，或浏览我们的网站：

www.bloombase.com

实行要点

真正“点对点”安全及具备卓越扩充能力、并完全依据 Bloombase Spitfire 安全平台设计的信息交换及数据仓库系统

主要优点

- 为传输中及已存储数据提供完全透明的信息保密性、完整性及真实性
- 真正安全及全面的密钥管理
- 高度可用性及容错能力
- 卓越加密性能

硬件

- IBM p-Series 服务器
- Egenera BladeFrame 系统

操作系统

- IBM AIX 5.3
- Sun Solaris 10
- Red Hat Enterprise Linux
- Microsoft Windows Server 2003

软件

- Oracle 数据库
- BEA WebLogic 网络服务台

12/2007

BLOOMBASE® 博隆兴中