# AccessMatrix™ UAS-E2EE

新一代通用认证服务器–端到端加密

## 端到端加密（E2EE）提供凭证和数据保护

### 关键优势

- 防止敏感信息的泄露，保持交易数据的机密性和完整性
- 避免来自内部和外部黑客的潜在的安全威胁
- 通过强身份认证方法和以用户为中心的活动跟踪来增强灵活身份认证和审计策略的安全性
- 具有强大的报告能力，报告用户活动和安全违规行为
- 提供100%的保证，除用于生成PIN码的可信硬件，没人知道用户的密码/PIN，包括中间层服务器（web服务器）

### 技术挑战

静态登录 ID/ PIN 是确认用户在线身份的一种常用的认证方法。

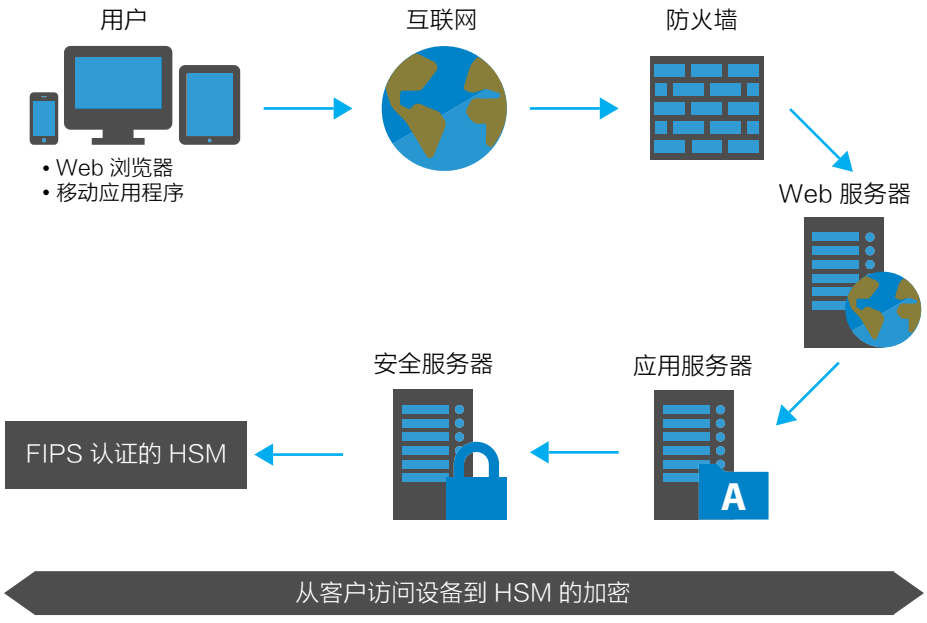
保护客户的 PIN 码信息，已经成为了服务提供商，如银行、SaaS 应用提供商和云提供商采取的顶级举措之一。由于企业在线业务越来越多，对安全的需求也在不断增加。尤其是随着互联网产品和服务范围的扩大，为组织提供了进入新市场的重大机遇。在线服务提供商必须确保进行交易的交付渠道是安全的，同时也要确保审计跟踪，数据隐私性的安全，以及符合法律法规要求。现在，互联网的应用程序采用简单的安全措施，如安全套接字层（SSL），来保护客户的 PIN 码和在 Web 浏览器和 Web 服务器之间传输的其他敏感数据。当数据到达 Web 服务器和应用服务器时，它会自动转换为原来的纯文本格式，这样就存在恶意攻击的可能。

据不完全统计，目前中国 SSL 滴血漏洞解决率不到 60%，多数企业的最终客户仍面临密码泄露的风险。安讯奔 E2EE 解决方案可完全解决上述风险问题，保障企业信息安全。

### HSM 集成

E2EE 在客户端设备与 HSM（硬件加密机）直接建立一条安全通道。 加密数据只能够通过放置在企业内部机房的硬件加密机物理模块进行解密处理，因此可以保障用户隐私信息在网络传输过程中的绝对安全；包括在企业内部应用及服务器上也是以密文形式存在。在整个流程中，AccessMatrix 应用服务器与 HSM 作为一套完整的企业级防篡改安全认证体系，为企业提供基于不同安全需求的数据保护解决方案。

> “除了安全套接字层（SSL），金融机构应该在应用层实现端到端加密安全，这样客户的PIN码和口令在这里进行验证时，就不会在浏览器和主机之间的任何中间节点泄露。”
>
> –新加坡金融管理局
> 科技风险管理指导中心
> 2013.7



## 系统要求

- 服务器OS：MS Windows Server 2008、IBM AIX、Oracle Linux、Oracle Solaris
- 应用服务器：Oracle WebLogic、 IBM WebSphere 和 Apache Tomcat
- Java 运行环境：JRE 1.6 及以上
- 数据库存储：MS SQL Server、Oracle RDBMS、IBM DB2 和 Oracle MySQL
- 外部用户存储：AD目录，LDAP v3 兼容目录 and JDBC 兼容数据库
- FIP 认证的 HSM
- 支持的移动平台：iOS、Android、黑莓 和 Windows Mobile

> “香港金融管理局要求敏感数据在网络服务器和金融机构的内部系统之间的传输过程也需要加密。金融机构应该考虑采用端到端加密这种强加密功能来传输高度敏感的数据（如用户密码），从而保证这类数据在客户端和企业的内部系统之间传输时都得到加密。即使在网络或内部系统已被攻破的情况下，这些敏感数据也不会被泄露。”
>
> –香港金融管理局

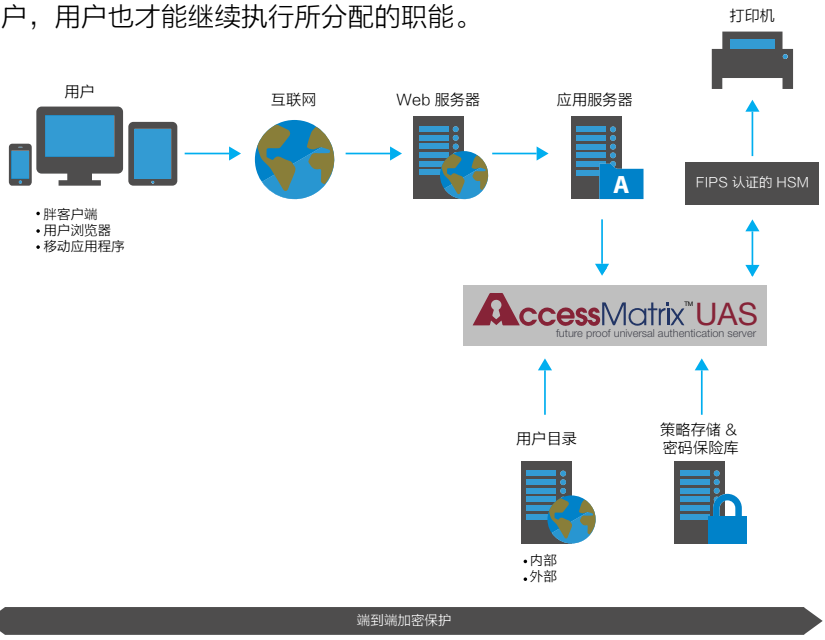
## 产品特性

E2EE 经过完善集成和测试的解决方案，由 AccessMatrix™ UAS 和通过 FIPS 认证的 HSM 设备组成，有效降低集成的复杂性，缩短安全敏感程序的端到端密码保护的部署时间。此解决方案提供以下功能，来满足端到端保护要求：

- 便于使用的安全服务 API，简化 HSM 集成的复杂度。易于部署在用户浏览器上。
- 灵活的管理模块，便于细粒度的管理授权和用户管理。
- 全面的审计和报告模块，提供以用户为中心的报告功能，可报告访问活动和安全违规信息。
- ATM 的 E2EE 模块，在网络信道传输的 ATM PIN 码是基于 ISO9564 格式的 ATM PIN 码传输，与现有基础设施集成相兼容。
- 加密库可用于常见的移动平台，如 iOS、安卓、黑莓和 Windows 等移动设备。
- HSM 与流行品牌 HSM 设备可以进行交互， E2EE 在客户端和硬件安全模块（HSM）之间创建一个安全通道，AccessMatrix™ 安全服务器和 HSM 集成解决方案，可以提供经过认证的防伪认证库。
- 可定制的 PIN Mailer 邮件程序，可进行邮件整合和 PIN 邮件的安全打印，细粒度密码策略。
- 可扩展的身份验证模块，包括像证书、硬件的 OTP 令牌、智能卡、生物识别设备等其他验证机制，并且无需对代码进行大的改动。
- 已验证的可扩展性和可靠性功能，满足最严格的服务级别和大规模部署运营要求。

## E2EE 工作原理

- 安讯奔 UAS E2EE 模块为 Web 应用、胖客户端应用及移动应用程序提供终端加密库来保障数据安全。当用户访问一个应用服务时（例如：访问网上银行）， UAS E2EE 加密库会通过公钥加密保护机制自动下载到请求发起端。
- 在用户输入用户 ID 和密码信息后，E2EE 数据库将使用公共密钥加密信息，并提交给服务器进行处理。一旦来自用户端和来自对应的安全服务器数据库的加密 PIN 信息到达服务器，服务器将会把加密 PIN 信息传递到 HSM 来进行验证。加密过程和 PIN 验证只会发生在 HSM 设备的安全防篡改保护的环境里。因此，在用户输入信息后，认证信息在整个链路中是一直处于加密状态的。
- 如果 HSM 的反馈信息正确则通过验证，直到此时系统才会成功认证用户，用户也才能继续执行所分配的职能。



## 简介

i-Sprint Innovations（i-Sprint），专注于为全球金融机构和高安全敏感环境提供身份、凭证和访问管理解决方案。i-Sprint凭借其优秀的产品和服务，在其客户之间获得极高的评价，并成为金融界公认的最优秀的品牌之一。

i-Sprint于2000年在新加坡设立了第一家公司。新加坡是亚洲高科技城市之一，它稳定、清廉、高效率的政府支持多媒体与通信基础建设和安全策略，这为 i-Sprint的成长提供了无限的良机。

i-Sprint的总部设在新加坡，并且在亚太地区迅速发展壮大。如今，我们在中国（珠海、北京、深圳、成都）、香港、台湾、马来西亚、泰国、越南、日本和美国都已有了直接授权并稳定可靠的合作伙伴。

i-Sprint独有品牌的安全产品、知识产权和专利，都是经过专门设计，以令这些产品超越全球金融服务法规要求。为了把握快速增长的身份、凭证和访问管理（ICAM）市场， i-Sprint不断创新产品功能，积极通过自有安全产品提供身份保护、云保护、移动保护和数据保护。

i-Sprint独特的顶级安全解决方案包括，安全成熟的点到点加密（E2EE）身份验证和数据保护，以对网上银行应用程序进行便捷（单点登录）、安全的访问。我们的解决方案符合多个国家监管机构规定的网上银行安全准则；并能克服大多数互联网和手机银行解决方案的安全挑战。基于通用安全平台，我们提供强大的银行级、通用强身份验证（生物识别，多因素认证等）和令牌管理平台，以确保多个应用交付环境（网络、移动设备和云端）的安全。

通过专业的解决方案和服务，我们为全球企业客户把先进的技术转化为价值。我们的客户包括领先的全球和地区性的金融机构、跨国公司及政府机构。

**Global Headquarters**
Blk 750D Chai Chee Road
#08-01 Viva Business Park
Singapore 469004
Global: +65 6244 3900
enquiry@i-sprint.com
www.i-sprint.com

**For a complete list of our offices in**
United States, Malaysia, Thailand, China, Hong Kong & Japan, please visit
**www.i-sprint.com/contactus**