

## 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。

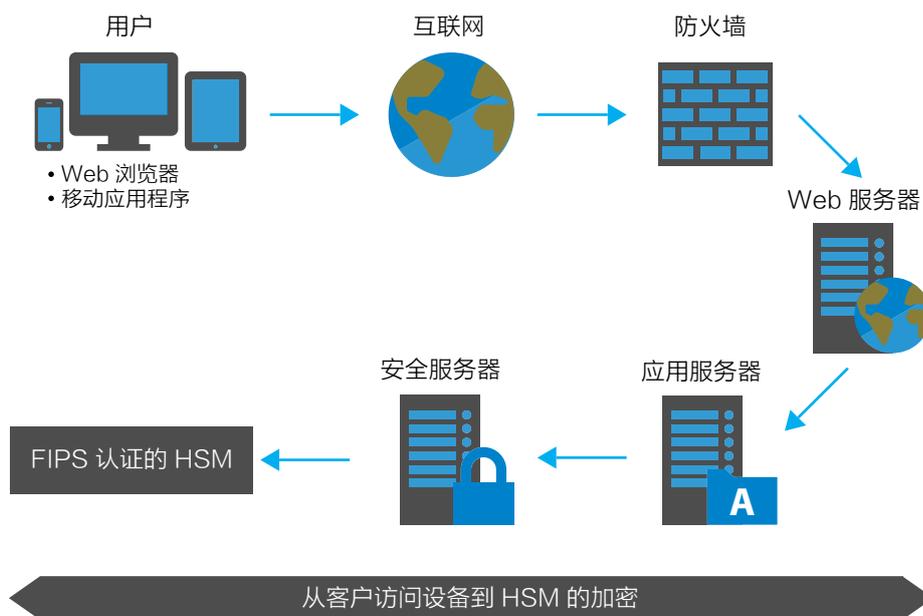
据不完全统计，目前中国 SSL 滴血漏洞解决率不到 60%，多数企业的最终客户仍面临密码泄露的风险。安讯奔 E2EE 解决方案可完全解决上述风险问题，保障企业信息安全。

### 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 2012/ 2016 及 Red Hat Enterprise Linux 7
- 应用服务器: Oracle WebLogic, IBM WebSphere, Apache Tomcat 及 JBoss Web Server
- Java 运行环境: JRE 1.8 及 JRE 11 LTS
- 数据库支持: MS SQL Server、Oracle RDBMS 和 Oracle MySQL
- 外部用户存储: AD目录、LDAP v3 兼容目录 和 JDBC 兼容数据库
- FIPS 认证的 HSM
- 支持的移动平台: iOS、Android 和 Windows Mobile

## 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。

“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

