Infraestructura de Clave Pública en la Industria de Pagos con Tarjetas de Crédito

Edgar González Fernández[1], Guillermo Morales-Luna[1], and Feliú Sagols Troncoso[2]

[1]Departamento de Computación, Cinvestav-IPN
[2]Departamento de Matemáticas, Cinvestav-IPN

Existe una alta demanda de servicios electrónicos en el ámbito bancario y comercial, tales como transferencias electrónicas, consultas y movimientos bancarios mediante portales "web", transacciones comerciales en red y mediante terminales de punto de venta. Es de gran importancia crear esquemas de comunicación que provean confidencialidad, integridad y disponibilidad. Cada una de las entidades que participan en una transacción debe tener la capacidad de proveer estos servicios, lo que es difícil debido a la gran diversidad de sectores que están involucrados: instituciones bancarias y gubernamentales, comerciantes, tarjetas de crédito, procesadores de pago, etc. En los servicios básicos en la industria hoy en día conviven en diversos niveles la Criptografía e Infraestructura de Clave Pública y los Esquemas de Clave Privada o simétricos. Instituciones y agencias internacionales, como son ANSI (American National Standards Institue), NIST (National Institute of Standards and Technology), ECC (European Payments Council), ISO, y otras han hecho esfuerzos para estandarizar algoritmos de cifrado, gestión de claves, componentes electrónicos y protocolos de comunicación. Para esta plática revisaremos protocolos basados en PKI utilizados para transacciones con tarjeta de crédito, mencionados en los estándares ANSI X9 y PKCS entre otros. Haremos un somero repaso de la serie modular FIPS PUB 140-X , de los criterios ISO/IEC 15408, ISO 13491, ISO/CD 21188, de los estándares X9.68 y X9.79 de ANSI y TS 101 862, TS 101 903 y TR 102 040 de la Unión Europea. Comentaremos brevemente el Capítulo X de la "Circular Única de Bancos" de la CNBV y de la Circular 34/2010 del Banco de México para el caso mexicano.