



El lento declinar de la contraseña prolífica

Desde la presentación en Securmática 2000 del proyecto **ATICO** (Autenticación por Tarjeta Inteligente **CO**rporativa), promovido por profesionales de seguridad de Telefónica de España y concebido para unificar, mediante el uso de tarjetas inteligentes y certificados digitales, el control de acceso físico al centro de trabajo del personal y su acceso al entorno de trabajo informático y de red, se ha ido conformando en nuestro país una tendencia a emprender iniciativas de modernización parecidas para simplificar la vida a los usuarios en su interacción con las TIC empresariales, marcadas por una heterogeneidad de aplicaciones y sistemas que convierten en engorrosos y poco eficientes los procesos de identificación y autenticación mediante ejércitos de contraseñas débiles.

Tras ATICO, el siguiente proyecto conocido pionero en España en la materia fue **TITAN** (Tarjeta Inteligente con Tecnología Avanzada para Negocio), de Caja Madrid, presentado en Securmática 2003 y distinguido con un galardón en la primera edición de los premios SIC, en 2004. En dicha iniciativa, dirigida por el departamento de Seguridad Informática de la institución financiera de referencia, se utilizó la tarjeta de empleado –EMV– para realizar autenticación robusta y entrada única de empleados a su entorno de trabajo en el sistema de información.

Existen, por supuesto, otras acciones trascendentes en este camino hacia la modernización real de las TIC. Pueden citarse, entre otras, las llevadas a efecto por el Ministerio de Defensa y por la Gerencia de Informática de la Seguridad Social. Y hay más en ciernes.

Pero por ahora, quizás el último gran paso haya que reconocérselo al Banco de España, cuya Unidad de Seguridad Informática, dependiente de la Dirección de Sistemas de Información, ha encabezado el despliegue de una PKI que, entre otras finalidades, se orienta a proveer a los empleados de certificados electrónicos en tarjeta inteligente para el control de acceso, firma y cifrado electrónicos. En este proyecto, denominado **PKIBDE**, del que se publica un interesante artículo en esta edición de SIC (páginas 42, 43 y 44), se ha adaptado una herramienta de fabricante para solucionar los problemas del archivo de claves en el contexto de la gestión de los certificados de cifrado.

Parece, pues, que la implantación correcta de la criptografía en el escenario interno de las entidades es hoy una línea de trabajo poco discutida, que tiende a reducir los riesgos asociados a la confidencialidad, la integridad y la autenticación. El siguiente paso debe ser hacer lo propio en escenarios más amplios (banca desde Internet, por ejemplo).

Y aquí aparece el DNI electrónico (del que, dicho sea de paso, se esperan noticias a mediados de este mes). Es posible que bancos y cajas estén expectantes ante su instauración para modernizarse y, al tiempo, solucionar algunos de los problemas de inseguridad que padecen sus servicios en la interacción con los clientes. Claro está, si se fían del DNI electrónico. ●