Número 3
Abril 2006
ISSN: 1885-0103

REVISTA ITS

SISTEMAS INTELIGENTES DE TRANSPORTE

La revista de ITS España

ITS en el Transporte Público

Entrevista: José Manuel Pradillo Pombo
Director Gerente del Consorcio Regional de Transportes de Madrid

La seguridad en la billética inteligente

María del Amor León Fariña
Luis Criado Fernández
Área de Innovación Tecnológica
del Consorcio Regional de Transportes de Madrid

En la actualidad, está probada la idoneidad de las tarjetas inteligentes sin contactos (ISO 14443) en los sistemas de billetaje para los transportes, y prueba de ello es que en la mayoría de los países se está optando por soluciones de este tipo. La introducción de esta tecnología aporta considerables mejoras, máxime cuando se utilizan tarjetas que incorporan algoritmos de seguridad no propietarios, como es el triple-des. Las principales ventajas que añade esta tecnología al sistema de billetaje son:

- Cancelación más eficiente: más rápida, mejorando la accesibilidad y más cómodo para el usuario.
- Reducción del coste de mantenimiento de equipos, puesto que se eliminan gran parte de elementos mecánicos. Aumento de la fiabilidad de los equipos de cancelación.
- Lucha contra el fraude.
- Aumento de la flexibilidad del sistema tarifario.
- Facilita estudios de movilidad, explotación y otros.

De todas estas ventajas, de la que quizá menos se ha escrito es de la lucha contra el fraude. Este artículo pretende describir de forma general la robustez de estos sistemas, para luchar contra cualquier intento de estafa del usuario. Podemos clasificar el fraude en dos grandes grupos: a) el fraude visible, que se produce cuando un individuo accede sin título o con uno robado a un modo de transporte; y b) el fraude invisible, que resulta más difícil de detectar y en consecuencia de combatir, y que se produce cuando un individuo viaja en un

operador de transportes con un título falso. Las instituciones y organismos de transporte están más cada día concienciados en invertir esfuerzos por construir sistemas eficientes contra el fraude. Para evitarlo, la tecnología sin contacto se presenta como una herramienta sin precedentes.

> En caso de robo, el usuario deberá informar a la autoridad de transporte y, en dos días como máximo, la tarjeta estará bloqueada en todos los operadores

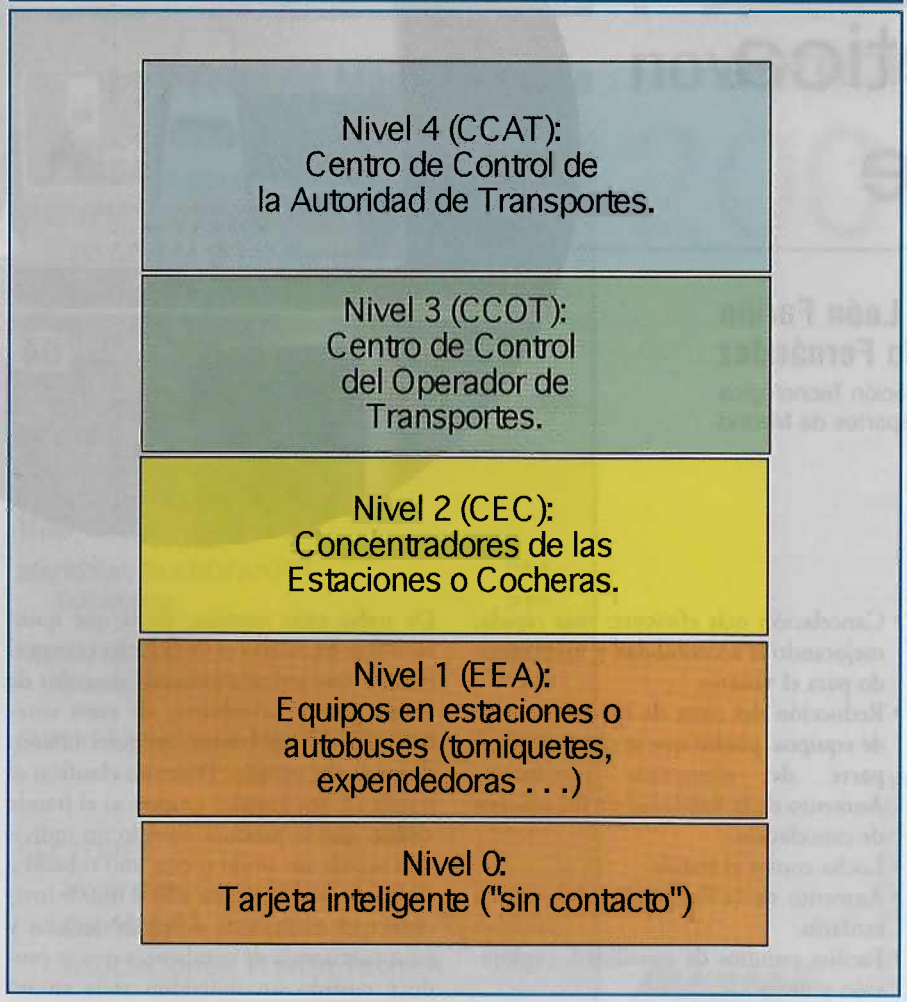
¿Por qué es tan robusta la tecnología de la tarjeta sin contactos contra el fraude invisible?. La respuesta es contundente, cada tarjeta incorpora una familia de claves únicas que le dan acceso exclusivo a su contenido. Es decir, no hay dos tarjetas con el mismo juego de claves. Además, la comunicación entre tarjeta y cualquier dispositivo del sistema (validadores/canceladores, terminal de carga o recarga, terminal de inspección, etc.), se establece mediante un canal seguro por radiofrecuencia; este canal seguro es negociado (con diferentes claves) con cada uso de la tarjeta.

Pero, ¿podría un hacker clonar o generar una de esas tarjetas únicas? Un hacker es un experto en una o varias técnicas relacionadas con las tecnologías de la información y las telecomunicaciones. Sin embargo, en este caso se exige un conocimiento profundo de elementos particulares del sistema, como circuitos electrónicos, teoría de antenas, procesos pormenorizados que realizan las distintas aplicaciones, experiencia en Módulos de Acceso Seguro (SAM), manejar y conocer las estructuras de datos, etc. Esta tecnología posee un elevado grado de innovación y se alimenta de numerosas áreas de conocimiento, lo que minimiza en extremo la posibilidad de vulnerar el sistema.

Partamos de la posibilidad remota de que el hacker conozca la tecnología y tenga el equipamiento necesario para fabricar la tarjeta. La primera vez podría utilizarla pero, cuando la información identificativa de ésta llegase a la autoridad de transportes, se comprobaría que la tarjeta es falsa. Esto desencadenaría la activación del mecanismo de bloqueo de la tarjeta en todos los operadores de transporte.

Para conocer el mecanismo que sigue el operador de transporte para realizar la comprobación de la legitimidad de la tarjeta, es necesario conocer a grandes rasgos la arquitectura, es decir, conocer cómo envía la información el operador de transportes a la autoridad de transportes y cómo se procesa todo para determinar las acciones efectivas.

Niveles funcionales de la arquitectura general del sistema



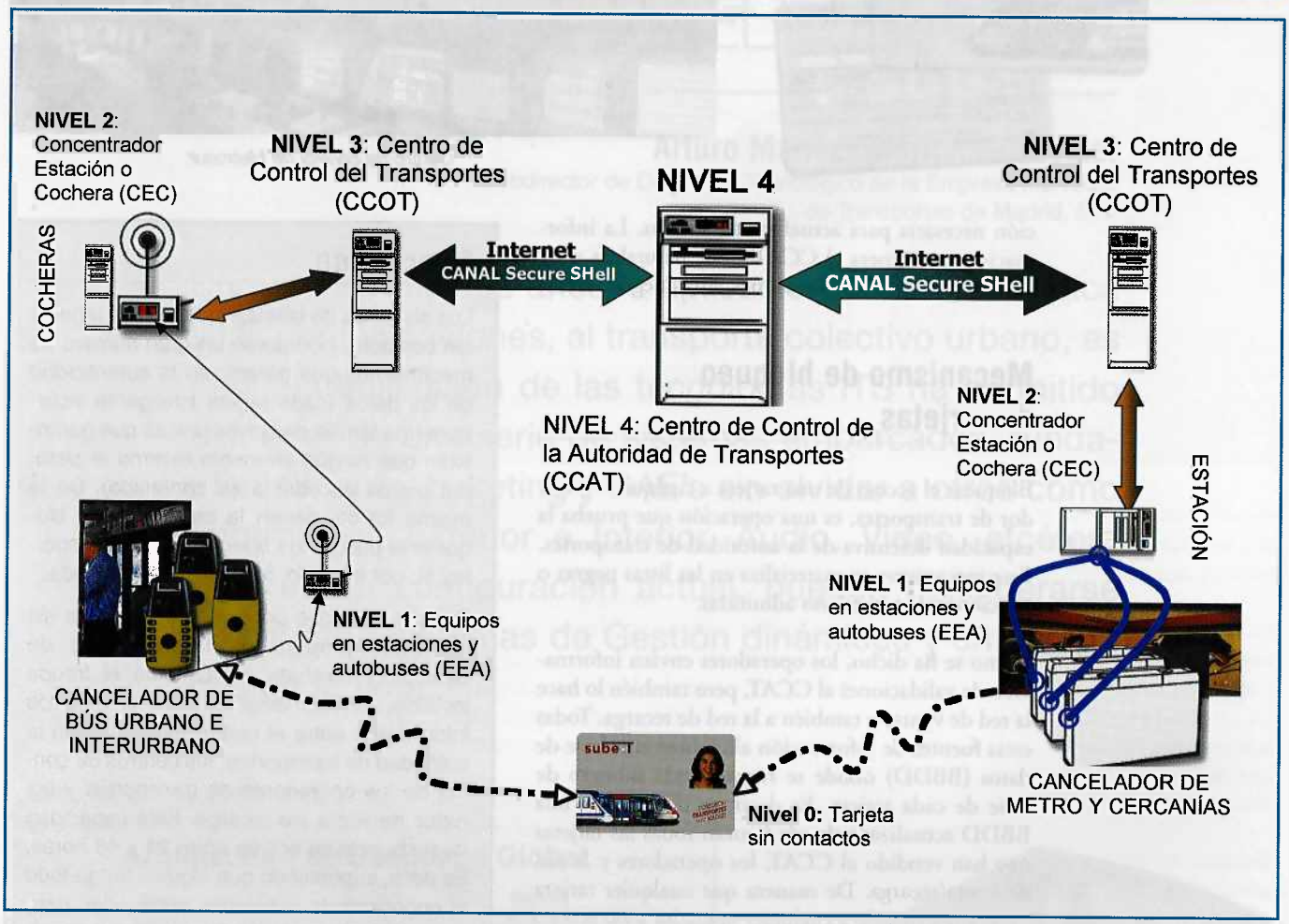
Arquitectura de un sistema de billetaje sin contacto

Los trabajos actuales en este tipo de sistemas coinciden en establecer cinco niveles funcionales como arquitectura general del sistema:

- Nivel 0: Tarjeta inteligente ("sin contacto")
- Nivel 1 (EEA): Equipos en Estaciones o Autobuses (validadotes, torniquetes, expendedoras, ...)
- Nivel 2 (CEC): Concentradores de las Estaciones o Cocheras.
- Nivel 3 (CCOT): Centro de Control del Operador de Transportes.
- Nivel 4 (CCAT): Centro de Control de la Autoridad de Transportes.

Estos niveles representan las diferentes capas funcionales del sistema de billetaje inteligente. El nivel 4 es donde se realiza todo el procesado de datos de los diferentes operadores y redes de venta y/o recar-

Comunicación de CCAT con el Operador de Transportes



ga. Los niveles 3, 2 y 1 representan la jerarquía funcional del operador de transportes, y el nivel 0 hace referencia a la tarjeta sin contacto.

El flujo de información

Comenzaremos explicando cómo circula la información desde que se detecta la tarjeta en los validadores hasta que llega a la autoridad de transportes (CCAT).

El usuario entra en el transporte público y sitúa la tarjeta sin contactos (ISO 14443) sobre la antena del validador en una operación muy rápida, del orden de milisegundos. En este instante se activa el proceso que consiste en la comprobación de que al menos uno de todos los títulos que residen en la tarjeta sin contactos es válido en dicho instante. Este proceso se realiza enviando tramas de información por radiofrecuencia, cifrando los paquetes de datos que se envían entre tarjeta y validador para evitar el fraude. Los datos personales de la tarjeta no se envían para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos (LOPD).

Independientemente del resultado, se debe generar un registro de la operación al que llamaremos registro de validación. Este registro de validación debe incluir como mínimo el número de serie de la tarjeta, el resultado de validación, la fecha y hora. El proceso descrito forma parte del nivel 0/1. Cuando el validador o el subconcentrador (concentrador de validadores de una batería o vestíbulo) puede comunicar con el concentrador (nivel 2), le envía todos los registros de validación. Todos los concentradores de estación o cocheras envían sus registros al centro de control del correspondiente operador de transportes (CCOT, nivel 3).

Para la transmisión de la información de validación entre el nivel 3 (CCOT) y el nivel 4 (CCAT), se elegirá una ventana de tiempo que garantice la velocidad de transmisión de los procesos, normalmente en modo nocturno, aunque pueden darse comunicaciones diurnas.

> "El flujo de información entre el operador y la autoridad del transporte se realiza en ambos sentidos"

Para que la transmisión sea segura, el canal debe ser seguro, utilizando por ejemplo el protocolo SSH.

Por este canal, se transmitirán desde de el nivel 3 al nivel 4 toda la información correspondiente a los registros de validación generados en los operadores de transporte a lo largo del día. Por otro lado, el CCOT descargará del CCAT la informa-

Centro de control de Metrosur

ción necesaria para actualizar su sistema. La información que genera el CCAT es de naturaleza muy diversa; tarifas, configuraciones, listas negras, etc.

Mecanismo de bloqueo de tarjetas

Bloquear el acceso de una tarjeta a cualquier operador de transportes, es una operación que prueba la capacidad defensiva de la autoridad de transportes. Este mecanismo se materializa en las listas negras o relaciones de tarjetas no admitidas.

Como se ha dicho, los operadores envían información de validaciones al CCAT, pero también lo hace la red de ventas y también a la red de recarga. Todas estas fuentes de información alimentan una base de datos (BBDD) donde se registra cada número de serie de cada tarjeta. Es decir, se dispone de una BBDD actualizada donde figuran todas las tarjetas que han vendido el CCAT, los operadores y la red de venta/recarga. De manera que cualquier tarjeta que haya accedido a cualquier operador y no esté en la BBDD, no habrá sido vendida por ningún operador de trasportes ni por la red de venta. Por lo tanto, será falsa y se pondrá en lista negra.

Cuando el operador, en conexión con la autoridad, comprueba que hay una nueva lista negra, procederá a descargarla; una vez recibida en su sistema, verificará la firma electrónica de la lista negra para autentificarla, informando al CCAT que la ha recibido correctamente; inmediatamente, el operador distribuirá la lista negra por su red, es decir, enviará cada fichero desde el nivel 3 al 1, llegando por tanto hasta cada validador del operador. Así, por ejemplo, si el CCAT genera una lista negra en la que una nueva tarjeta sin contactos ha sido incluida, el operador detectará el cambio y actualizará su lista negra a nivel 3, para después transmitirla al nivel 2. Cada concentrador de estación (nivel 2) enviará la nueva lista a los distintos subconcentradores, transmitiendo esta información a todos los posibles equipos intermedios hasta que la reciban todos los validadores (nivel 1). De manera que al día siguiente, cuando la tarjeta afectada intente entrar a cualquier dependencia del operador de transportes, se le denegará el acceso, ya que el validador comprobará que la tarjeta está en lista negra, informando de esta situación y bloqueando el paso. ■

Conclusión

Los sistemas de billetaje que utilizan tarjetas sin contacto, incorporan un gran número de mecanismos que garantizan la autenticidad de los datos (cada tarjeta inteligente incorpora una familia de claves únicas que garantizan que ningún elemento externo al sistema pueda acceder a su contenido). De la misma forma, tienen la capacidad de bloquear el paso a los operadores de transportes si, por ejemplo, la tarjeta fuese robada.

Por si esto fuese poco, la propia tarjeta sin contactos proporciona la capacidad de detectar y combatir eficazmente el fraude invisible, en combinación con el flujo de información entre el centro de control de la autoridad de transportes, los centros de control de los operadores de transportes y las redes de venta y/o recarga. Esta capacidad de respuesta se estima entre 24 y 48 horas. Es decir, suponiendo que alguien tenga todo el conocimiento y equipos necesarios para generar tarjetas compatibles con el sistema, la vida de dichas tarjetas no superará en ningún caso los dos días.

torniquete con tecnologías sin contacto y magnética