KRYPTO-CD®

AUTENTICACIÓN FUERTE DE TRES FACTORES USANDO FIRMA ELECTRÓNICA CD CARD

1. DESCRIPCIÓN GENERAL

Hemos desarrollado un ingenioso sistema de autenticación de personas a distancia, con toda la potencia y seguridad brindada por un algoritmo criptográfico fuerte (CryptoFlash ® 1024-bits de FIRMAS DIGITALES SRL ®)
La solución es muy segura y atrayente por su sencillez de implementación.

La solución consiste en distribuir MINI CD o PEN DRIVES (llaves USB) personalizadas a los "clientes" de un centro de autenticación. El cliente coloca su dispositivo (no necesita instalar nada, puede operar desde cualquier cyber-café o locutorio desde cualquier punto del planeta conectado a Internet) o incluso desde su disco rígido, ingresa una contraseña secreta y genera en segundos un NÚMERO único (la firma electrónica), personal e irrepetible que varía cada minuto y que lo identifica sin lugar a dudas ante un centro de control de identidad.

2. DESCRIPCIÓN TÉCNICA

Técnicamente la solución consiste en asociar un número a una identidad (el cliente), usando un autenticador de tres factores (algo que el cliente *tiene* = la CD CARD o PENDRIVE, algo que el sistema genera = usando una función seudoaleatoria personal y algo que el cliente *sabe* = una contraseña)

Se usan soportes portátiles (caben en la billetera o llavero) o si se prefiere un soporte fijo (disco rígido de una PC) con un programa generador de passwords dinámicas, usando el algoritmo de alta seguridad CryptoFlash 1024-bits. . Con este sistema, cada miniCD o Pen Drive genera una única secuencia de números que varían cada minuto (utiliza datos de la fecha y la hora actual para calcular). Para poder generar el número, se requiere contar con una contraseña adecuada, la que debe ser conservada en reserva por el dueño del miniCD. Esa password dinámica es la ***firma electrónica*** del dueño, una vez incorporada a un documento y tiene respaldo legal en la Argentina por la Ley de Firma Digital vigente.

Técnicamente, el programa generador de passwords dinámicas se personaliza por medio de un PIN (16 bytes = 2^{128} combinaciones). Estos se generan al azar y se incorporan a cada dispositivo, encriptándose a su vez con un algoritmo simétrico fuerte (3DES 168-bits), cuya clave es función de una contraseña aleatoria. Esta contraseña aleatoria se distribuye junto al dispositivo como un único paquete (identificado por un número de serie). A su vez el sitio servidor de identidad, cuenta con una base de datos de clientes que en un campo encriptado con una clave maestra de administración conserva el valor del PIN y en otro campo el número de serie de ese

cliente. De esta forma, al conectarse un cliente, el sitio servidor puede recuperar el PIN y recalcular la password actual del minuto (la firma electrónica) y en caso de coincidir con la informada por el cliente, se prueba que el autor es quien dice serlo, dado que la combinación del dispositivo, el instante en el tiempo que es aleatorio y la contraseña sólo pueden estar en poder del firmante.

Cabe acotar tres observaciones:

a. Nombre histórico del sistema

   A pesar de llamarse Krypto-CD por razones históricas, se trata de un sistema que potencialmente puede operar desde cualquier clase de soporte activo o pasivo: CD CARD, PEN DRIVE, SMARTPHONE, TABLET, MEMORIA SD, DISCO RÍGIDO INTERNO o EXTERNO, etc.

b. Sincronización de fecha-hora entre el sitio cliente y el server.

   Nuestro sistema permite la sincronización automática del programa cliente del dispositivo con la hora universal GMT de un pool de relojes atómicos de uso público, con lo cual este factor se soluciona incluso para un operador distante en cualquier punto del planeta. Alternativamente se puede sincronizar por evento, es decir asignando un número único a cada lanzamiento del programa.
   Idealmente, en la versión temporal y al estar ambos están sincronizados, generan el mismo número. En general no será así (puede haber un lag de segundos o demora por parte del usuario entre que calcula e informa), por lo cual el sitio servidor deberá calcular los valores para un **rango de minutos** antes y después del actual (la experiencia indica que +/- 3 minutos es suficiente) y verificar si el número recibido está incluido en ese rango. Si está, se dará por validada la identidad, en caso contrario se alertará al cliente (on-line) de la necesidad de reintentar la transacción (un máximo 3 intentos) antes de rechazar el servicio. En la versión de eventos, se puede sincronizar el número de evento en forma automática entre la memoria del servidor y la del cliente.

c. Vinculación entre el dispositivo, la contraseña de uso y la identidad del cliente.

   Estas tres entidades no pueden ser separadas. Si la contraseña dejara de ser de dominio exclusivo de su legítimo dueño y el cliente pierde simultáneamente el control sobre su dispositivo, se compromete el esquema de autenticación.
   Para que la responsabilidad de la autenticación repose exclusivamente del lado cliente, se debe asegurar el consentimiento expreso de la custodia de la tarjeta y su contraseña al instante de su adhesión y forzarlo a denunciar la pérdida de su dispositivo y/o la divulgación de su contraseña de uso si ello llegase a suceder. En ese caso, se procederá a renovar el juego anulando el actual.

El lado server del sistema cuenta con el programa administrador (biblioteca de funciones C++ o componente ActiveX según la plataforma) que le permitan calcular el número (firma electrónica) en función de un PIN y una fecha-hora actual. La

plataforma del servidor puede ser Win32/IIS o cualquier Unix/Web Server (Linux/Solaris/Apache etc.)

3. DIAGRAMAS TÉCNICOS

En un esquema simplificado y analizando sólo la sincronización temporal, el sistema opera de acuerdo a lo que muestra la **FIGURA 1:** el cliente coloca su dispositivo en la lectora de una PC estándar, no necesita instalar ningún software. Se lanza el ejecutable, el usuario ingresa su contraseña personal y cliquea el botón calcular. Aparece el número de identificación válido para ese minuto. El usuario comunica al servidor (centro de autorización) el número obtenido y el número serial impreso en su dispositivo. El Servidor recalcula el número de identificación y lo compara con el informado, si son iguales dá por válida la identidad del cliente.

En la **FIGURA 2** se detalla el contenido y la operatoria en el sitio cliente. El componente principal del dispositivo es el PIN encriptado (2.1). Este número único e irrepetible de 16 bytes caracteriza a cada algoritmo personal. El segundo componente personal es la password del usuario (2.2) con la cual se puede desencriptar al PIN. El usuario debe mantener cuidadosamente resguardada su contraseña, preferentemente memorizada y en caso contrario al menos lejos del dispositivo. Una vez desencriptado el PIN, este número de 16 bytes sirve para personalizar el algoritmo. En forma transparente, un reloj atómico (time server Internet) aporta la fecha-hora GMT/UTC universal con error de milisegundos (2.4) el que sumado al PIN permite al programa del algoritmo (2.5) calcular el número de identificación válido para ese intervalo de tiempo (2.6). En el siguiente paso, el usuario comunica (2.8) al server (centro de autenticación) tanto el número de identificación como el propio número serial del disco (2.7). Aquí se cierra la intervención del cliente y comienza a operar el lado servidor.

En la **FIGURA 3** se muestra como procede el lado servidor con los datos remitidos por el cliente, se supone que ha recibido tanto el número de identificación (3.1) como el número serial impreso del dispositivo (3.2). El Servidor procede ahora a consultar su base de datos encriptada en la cual accede al PIN del cliente correspondiente al número serial del dispositivo informado (3.3), este PIN se desencripta con una clave maestra del administrador (3.4), recuperándose así el PIN en claro (3.5). A continuación, con el TimeStamp (fecha-hora) provisto por el reloj del sistema, sincronizado al minuto UTC/GMT(3.6) y el PIN se personaliza el algoritmo (3.7) con el cual se recalcula el valor del número de identificación (3.8). Luego se comparan (3.9) ambos números de identificación. En caso de coincidir, se da por válida la identidad del cliente. Para evitar el bloqueo de fraude por reingreso del número (replay), el servidor instalará un período de bloqueo temporal de cada usuario identificado. Durante ese período refractario, no se dará curso al número de identificación de ese usuario. En caso de cómputo de valores dentro de un rango de tiempo delta, basta bloquear al usuario por un tiempo delta/2.

FIG 1:

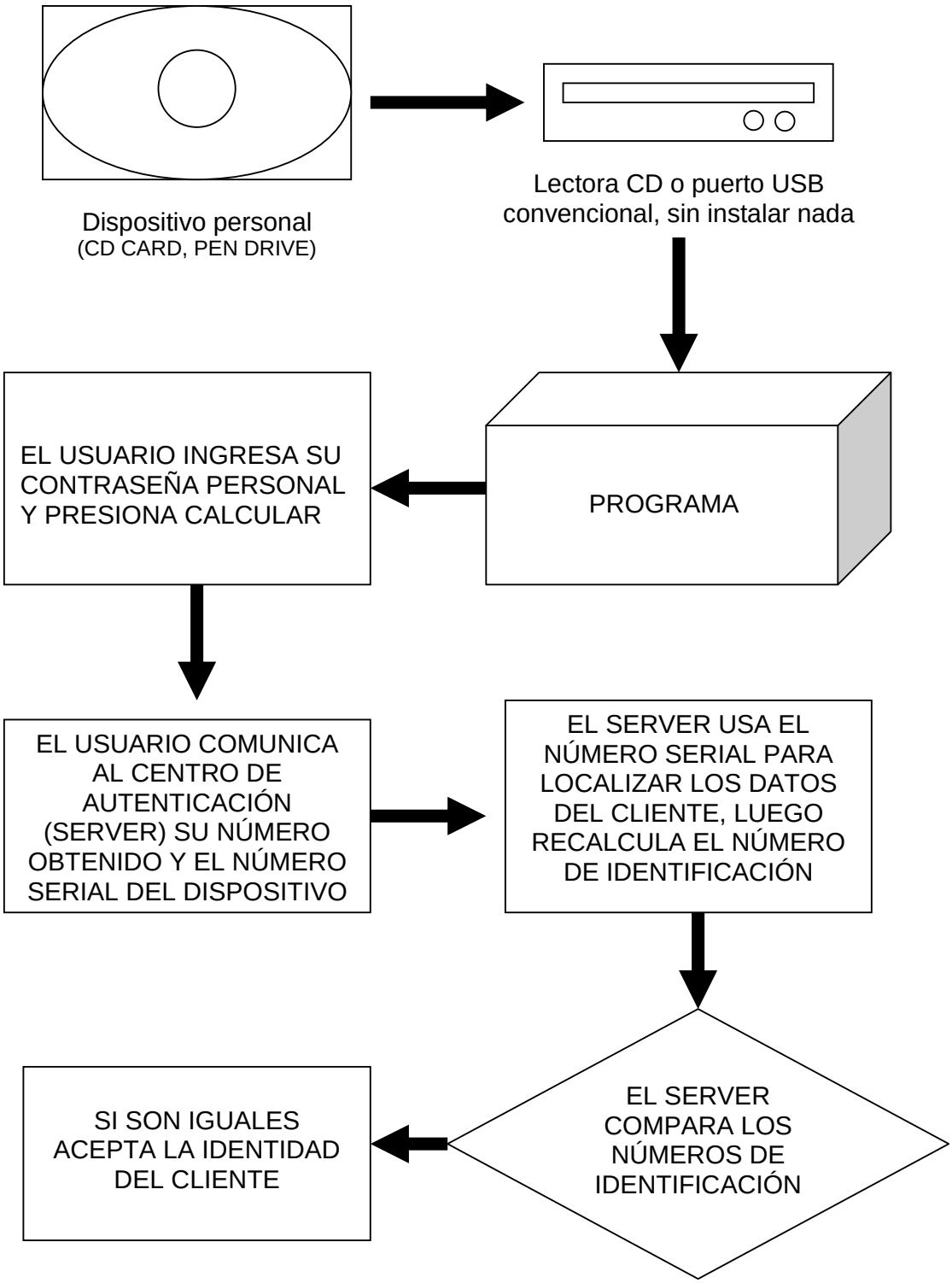
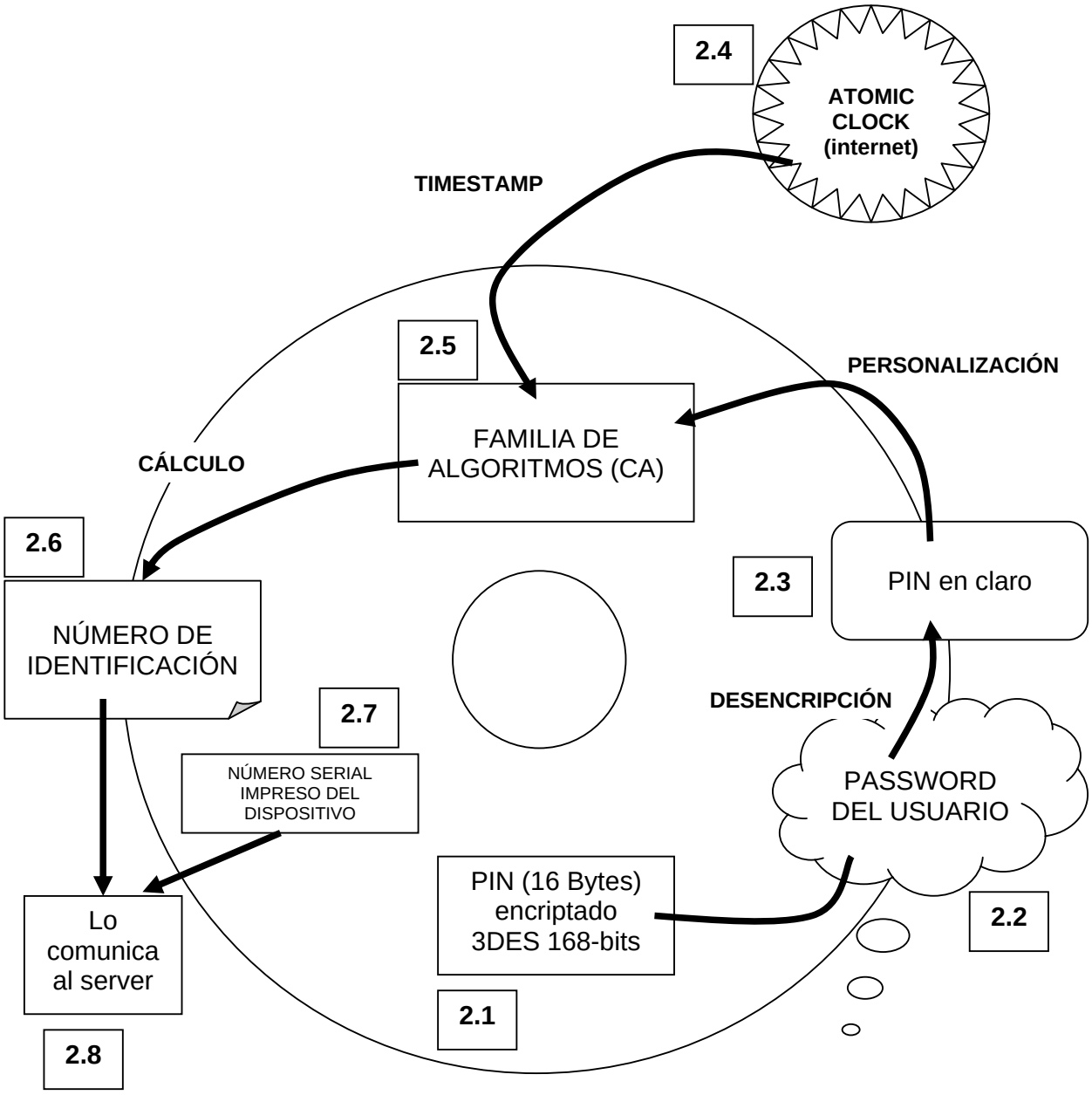
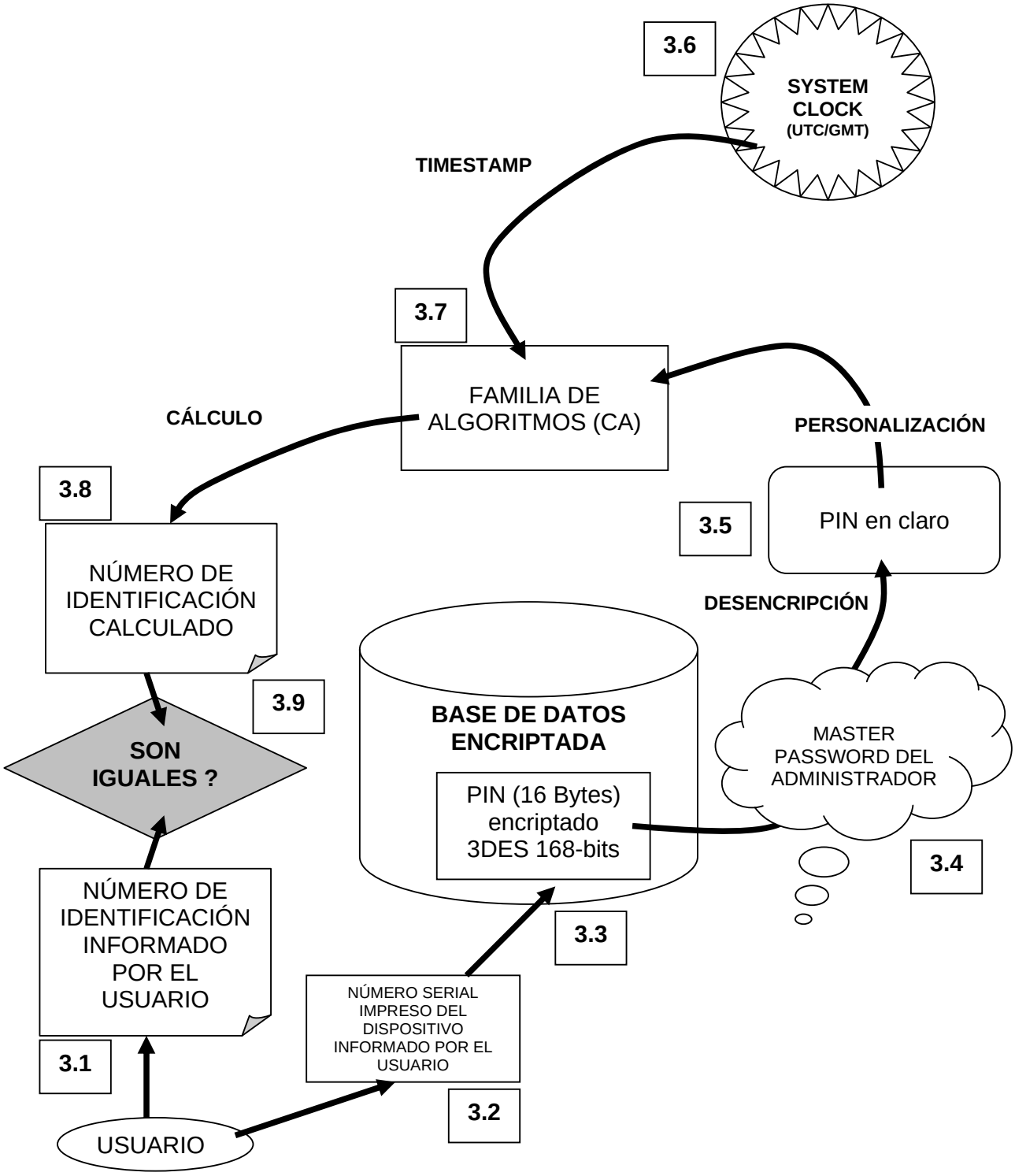


FIG 2:



CONTENIDO DEL KRYPTO-CD® Y OPERACIÓN DEL SITIO CLIENTE

FIG 3:



OPERACIÓN DEL SITIO SERVIDOR

4. DESCRIPCIÓN ADMINISTRATIVA DE UN CASO TESTIGO (Ej: Clientes de un Sitio de e-Commerce)

a. Contrato de adherencia del servicio e-Commerce con firma electrónica

El Sitio decide si los trámites serán con concurrencia del interesado a su Local o a domicilio del cliente, lo cual no altera nuestro sistema.
El cliente completa una planilla (original y duplicado) con sus datos personales (con las condiciones preimpresas del servicio) y firma su conformidad. Previa identificación fehaciente con su DNI (y eventualmente abonar un arancel) recibe un pack (personalmente o por correo) consistente en un dispositivo y una tarjeta (tipo raspadita) con el campo contraseña oculto y que contiene al dorso instrucciones de uso del servicio, ambas identificadas con un mismo número serial. En el caso de querer operar independientemente todo el circuito de generación de dispositivos, el adquirente deberá contar con el programa generador de PINES, contraseñas y números seriales, o alternativamente capturar previamente las contraseñas que elijan los mismos usuarios finales. Más adelante se describe en detalle este escenario.

b. Activación del servicio e-Commerce con firma electrónica

El Sitio almacenará en una base de datos los datos del cliente y su número serial. El Sitio dispondrá además de una tabla de números seriales y correspondientes PIN encriptados con una clave maestra. A partir de una hora preconvenida (P.Ej: 24 Horas) el cliente podrá acceder al servicio en la página web del Sitio. La Base de Datos (cualquiera, Oracle, Informix, SQL Server, etc.) contendrá para cada registro un FLAG de activación que le permite dar de alta (o baja) a cada dispositivo.

c. Uso del servicio e-Commerce con firma electrónica

El cliente raspa su tarjeta y toma nota por separado (o memoriza) su contraseña. El dispositivo es portable (billetera, portadocumento, llavero) **SIN la tarjeta**. La contraseña está diseñada para facilitar su memorización (palabra del diccionario mas tres dígitos). Si no puede memorizar la contraseña la deberá anotar en su agenda, prestándole el mismo cuidado que al PIN de su tarjeta de Red Bancaria. Cuando se conecte al servicio de e-Commerce deberá hacerlo desde una PC Windows95/98/NT/ME/2000 con Lectora CD o puerta USB (domicilio, locutorio, cyber-café, etc). Al colocar dispositivo en la lectora, se abre el programa de generación de firma, ingresa su contraseña y obtiene con un clic su *firma electrónica*. Ese número lo incorpora en la página donde completa el formulario e-Commerce (supongamos una autorización de pago). Al recibir el servidor ese formulario, recalcula la firma del cliente para un rango de tiempo adecuado (P.Ej: tres minutos antes a tres minutos después de la hora oficial argentina). En caso de no verificar la firma le informa al cliente que reintente la operación. Al tercer intento fallido lo saca del sistema y se le pide que concurra a la sede del Sitio (se presume intento de fraude). Si la firma es aceptada, se almacenan los datos y se da curso a la transacción.

d. Litigios

Si hubiese litigio ulterior, la responsabilidad del Sitio queda cubierta por los siguientes argumentos:

- La firma electrónica fue generada por el titular del pack identificado con número serial, recibido por el dueño bajo firma y previa identificación de identidad (DNI).
- En ese acto, el cliente se hizo responsable del buen uso del servicio y custodia de su dispositivo y contraseña.
- Nadie que no esté en posesión de ese dispositivo y conozca su contraseña (exclusiva, personal y única) podría haber generado **ese número en ese instante**, o sea su firma electrónica. Esto puede ser probado por una pericia técnica ante cualquier juzgado.
- El cliente no puede alegar sustracción o pérdida de su dispositivo (o eventual violación del secreto de su contraseña) porque una de las condiciones por él firmadas exige la inmediata denuncia ante el centro de revocación del servicio e-Commerce.
- La asesoría legal del Sitio incorporará además en el contrato de adhesión las cláusulas necesarias y suficientes para forzar la responsabilidad exclusiva del cliente del servicio (salvo error u omisión por parte del Sitio).

5. Soluciones alternativas

Se pueden concretar esquemas operativos alternativos, la solución es personalizable a las necesidades del usuario, por ejemplo podemos implementar instalaciones con contraseñas que varíen por evento (cada vez que un usuario acceda) y no por tiempo. Cualquiera sea la solución, un Hacker que logre interceptar una contraseña no podrá reusarla ni anticipar cuál será el valor siguiente.

En el caso que se opte por la generación integral de los miniCD por parte de Firmas Digitales SRL, las contraseñas personales estarán formadas por una palabra de un diccionario (a coordinar con el adquirente) y tres o más dígitos (mínimo total de 8 caracteres), facilitando su memorización nemotécnica, sin pérdida de seguridad.

Alternativamente, las contraseñas podrán ser elegidas por cada usuario final (a través de un canal seguro via web – sesión SSL v3) y almacenadas (encriptadas) del lado server por parte del adquirente. Ulteriormente, con un aplicativo provisto por nosotros, el adquirente genera en base a esas passwords, los archivos de PINes encriptados (encripción fuerte 3DES 168-bits modo CBC) que se nos entregan para la grabación de los dispositivos. Una vez grabados, entregamos los dispositivos al adquirente para que puedan ser distribuidos a los respectivos usuarios finales.

Otra modalidad de venta consiste en la entrega de la tecnología al adquirente para que él mismo pueda generar todos los dispositivos por su cuenta.

Cualquiera sea la modalidad adoptada, se recomienda dotar al web site del adquirente con un certificado digital (tipo Global-ID© VeriSign©) que fuerce la generación de sesiones SSL v3 con 128-bits de encripción simétrica, para que las transacciones con el KRYPTO-CD® sean absolutamente confidenciales y controlada por integridad.

6. Business Case exitoso:

La solución KRYPTO-CD® no es una posibilidad teórica, se encuentra 100% operativa en OCA (Organización Coordinadora Argentina SA), para su servicio e-commerce de comunicaciones fehacientes con ocho mil clientes on-line y desde el año 2000, sin haberse registrado un solo incidente técnico y/o legal.

Puede consultarse en el site https://www.oca.com.ar/ocaprin/etelegramahome.asp?l=1
y cliquear en el ícono “DEMO INTERACTIVA” para conocer detalles del sistema. Como se podrá observar nuestra empresa fue distinguida como SOCIO TECNOLÓGICO de OCA por los excelentes resultados obtenidos con este sistema. Puede consultarse al gerente de la división e-commerce de dicha empresa para obtener una ratificación de lo expresado.

7. Registro de Marcas y Propiedad Intelectual: