DIVERSID AUTENTICACIÓN

PRESENTACIÓN
SISTEMA DE AUTENTICACIÓN DE DIVERSID

Premiado con medalla de plata en el Salón Internacional de Invenciones, Técnicas y Productos nuevos de GINEBRA-2003

Sistema registrado bajo Patente 02748876.6

Introducción

Todavía hay problemas en la autenticación necesaria en muchos de los diálogos que se realizan a distancia (Internet, pagos en comercios, uso de cajeros automáticos, atención telefónica, ...).

En el momento actual existen buenas soluciones que ya utilizan claves distintas para cada operación realizada, pero:

- en la mayoría de ellas solo se identifica el que inicia el diálogo dando por identificado al que ha sido llamado (sin eliminar el posible problema de suplantación de personalidad)

- es muy frecuente que utilicen claves cuyo tiempo de validez es limitado (a veces insuficiente si las líneas de comunicación son lentas o están cargadas)

DIVERSID AUTENTICACIÓN

¿ Qué aporta como novedad?

- Los participantes en una operación usan claves, sólo conocidas por ellos, que se encuentran a su disposición en un aparato de almacenamiento de claves

- Usa claves cuyo tiempo de validez es ilimitado (sus valores no se obtienen de ninguna variable temporal) pero que se usan una vez y no volverán a ser usadas

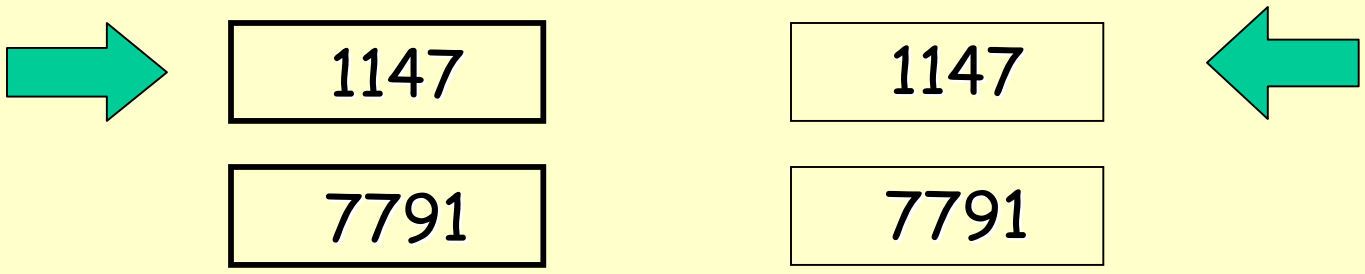
- Cada operación no presencial utiliza tres claves, o más, para la autenticación de los participantes. Para la siguiente operación a realizar las claves para la autenticación serán otras nuevas

- No considera identificado al que ha sido llamado hasta que se recibe de él una de las claves reservadas para ese fin en la operación en ejecución. Así se completa el proceso de autenticación y, al mismo tiempo, se genera confianza en el usuario del sistema que ve que el otro participante le envía la clave que espera de él

- Al disponer de varias claves para cada operación parte de ellas pueden ser utilizadas para la encriptación de la información

¿ En qué consiste ?

- En un procedimiento de intercambio de claves que han sido obtenidas previamente de forma aleatoria y almacenadas en un aparato agrupadas en paquetes.
- Cada aparato, con sus paquetes de claves, se pone a disposición de dos o más personas para que las claves que almacena sean compartidas e intercambiadas entre ellas en los diálogos que lleven a cabo, usando un paquete de claves para cada diálogo.
- Cuando un paquete ha sido utilizado se marca con el fin de que no pueda volver a ser utilizado.
- Lo normal será que una de las personas que interviene en el diálogo tenga el aparato y la otra disponga, en el soporte que sea más conveniente, de una copia de los paquetes de claves que están almacenados en el aparato. Así:



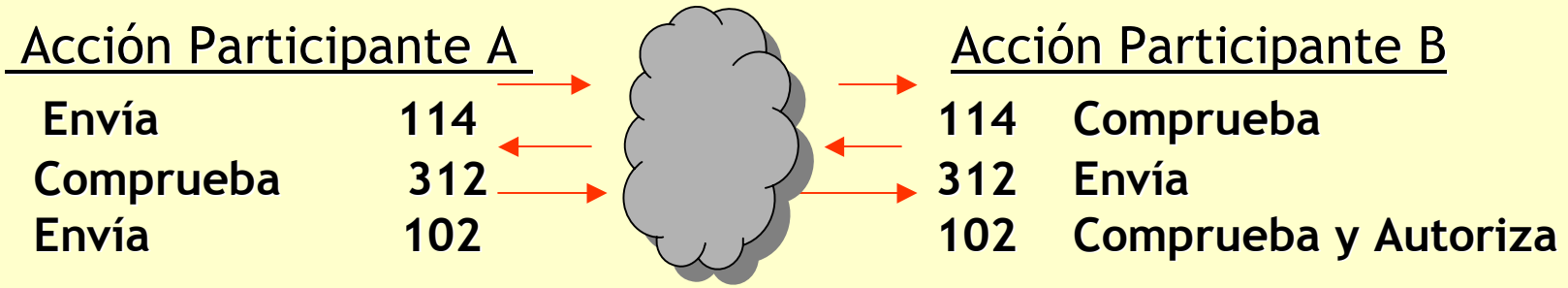
DIVERSID AUTENTICACIÓN

¿ Para qué sirve ?

Para la identificación de los participantes en diálogos a distancia asegurando que cada uno de los que interviene ES quien dice SER.
Al mismo tiempo protege la identidad e información sensible de sus usuarios en los diálogos.

Ejemplo de diálogo entre dos participantes A y B:

Paquete de claves compartidas por A y B {114,312,102}



Principales características del Sistema

- Las dimensiones del dispositivo en el que se almacenan las claves podrán ser similares a las que actualmente tiene una tarjeta de pago lo que le hace fácilmente transportable.

- Como dispositivo de almacenamiento y gestión de las claves también pueden ser utilizados otros ya existentes como, por ejemplo, un teléfono móvil.

- Para acceder a las claves almacenadas es necesario conocer la clave de entrada al dispositivo.

- Los paquetes de claves están formados por varias cifras obtenidas de forma aleatoria.

- Cada paquete de claves se usa en un único diálogo quedando en situación de no disponible una vez usado.

- Las cifras que componen las claves no se obtienen en función de ninguna variable temporal ni algoritmo lo que impide deducir nuevas claves partiendo de otras conocidas.

DIVERSID AUTENTICACIÓN

Principales características del Sistema

- Al no utilizar ninguna variable temporal no tiene un límite en cuanto al tiempo de validez de las claves y, por lo tanto, tampoco para el tiempo de respuesta a los mensajes que componen el diálogo.

- El sistema permite la escalabilidad y se adapta al nivel de seguridad del entorno en que se vaya a desarrollar el diálogo fijando tanto una longitud de claves como un número de cifras a intercambiar adecuadas.

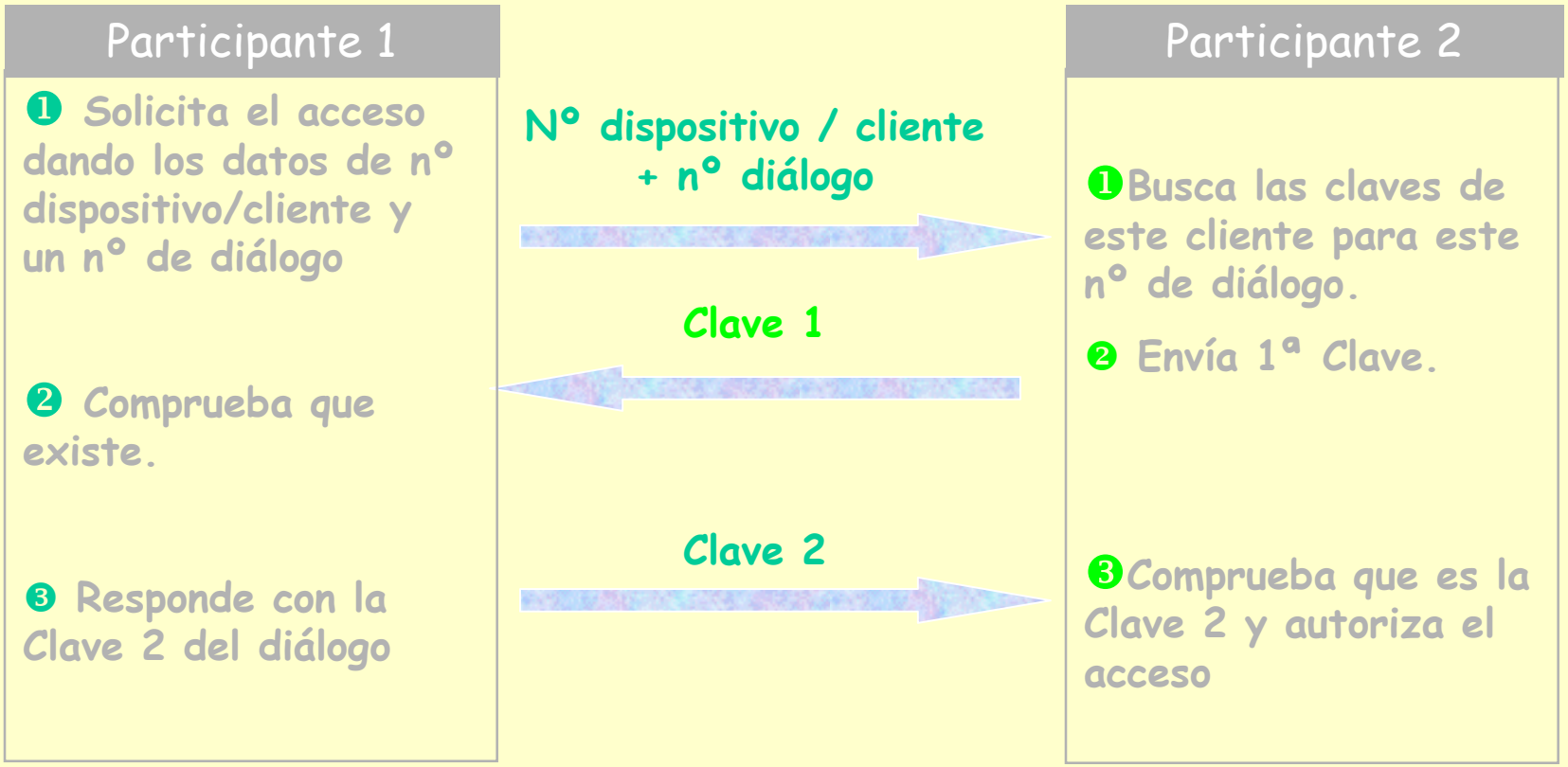
- La autenticación es completa ya que se identifican todos los participantes en el diálogo.

- El sistema permite la autenticación en diálogos en los que intervienen más de dos participantes con la peculiaridad de que ninguno de los intervinientes conoce todas las claves que se necesitan para poder terminar el diálogo.

Cómo funciona.-

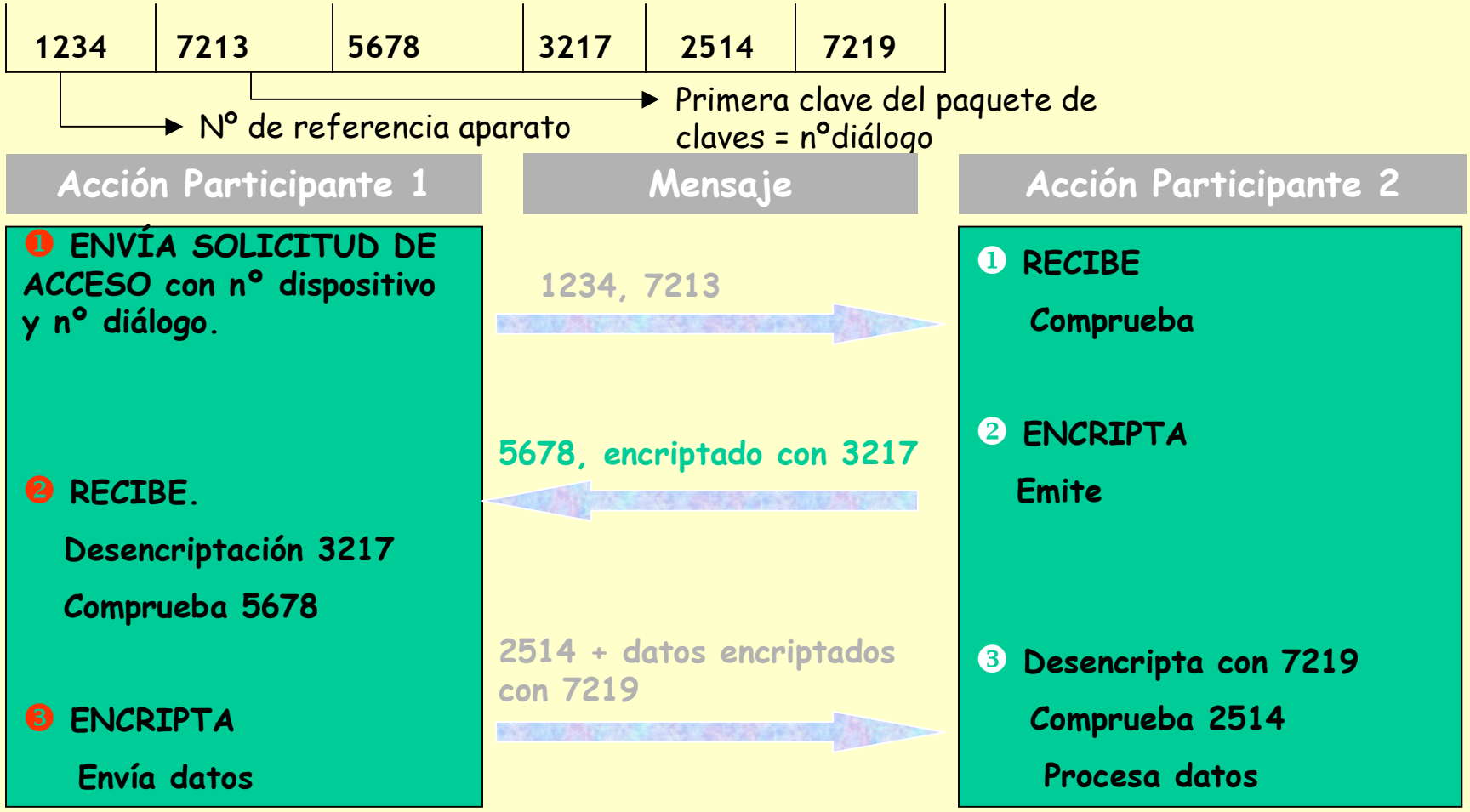
1. Ejemplo de Diálogo con intercambio de claves con posible aplicación en todo tipo de operaciones no presenciales.

Nota: el nº de diálogo citado en el ejemplo es la 1ª clave del paquete de claves



2. Ejemplo de Diálogo con encriptación en operaciones por Internet.

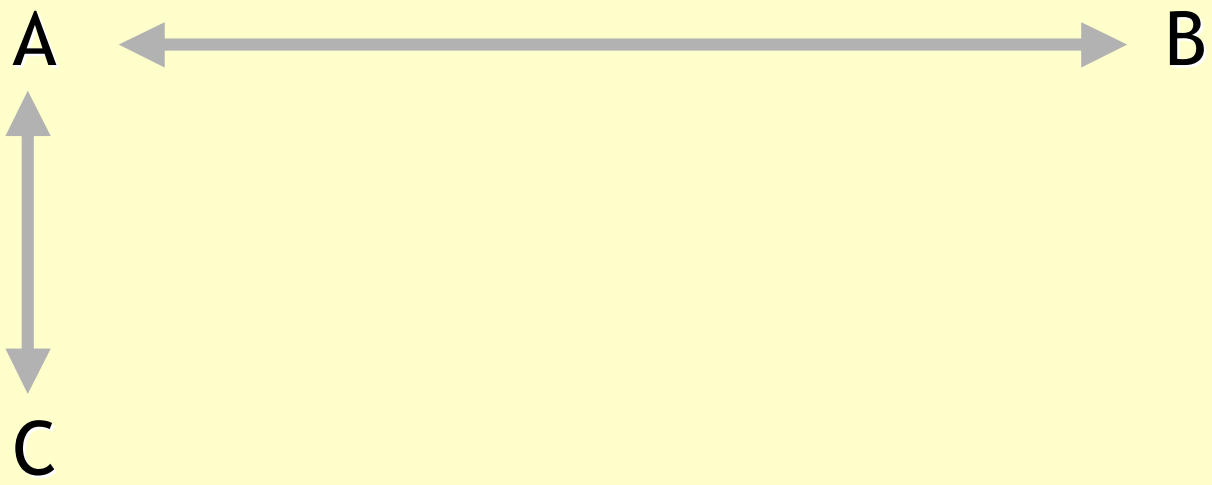
Ejemplo de diálogo entre dos participantes 1 y 2 usando el PAQUETE DE CLAVES:



3. Ejemplo de Diálogo entre tres participantes en una operación con autenticación en Internet.

UNA SOLUCIÓN

El diálogo se descompone en dos diálogos similares al del ejemplo 2.



Donde A también hace el papel de Entidad Validadora y de Intermediación para esta operación desarrollada bajo el procedimiento de autenticación.

DIVERSID AUTENTICACIÓN

Resumen Sistema 1/2

- Las claves se componen de números obtenidos aleatoriamente.

- Cada mensaje intercambiado en la realización de una operación puede estar acompañado de una clave diferente que lo valida para el receptor.

- Cada mensaje puede encriptarse con una clave distinta.

- Una operación utiliza un paquete de claves que una vez usado quedará marcado para impedir su reutilización

- El proceso de autenticación no considera identificado al llamado hasta que se recibe del llamado la clave que le corresponde según el paquete de claves en uso

Resumen Sistema 2/2

- Al no utilizar ninguna variable temporal no tiene un límite para el tiempo de respuesta a los mensajes que componen el diálogo.

- Protege la identidad e información sensible de sus usuarios permitiendo la encriptación.

- Uno de los juegos de las claves usadas en los diálogos está almacenado en un dispositivo de bolsillo que no está accesible. El otro juego reside en un sistema seguro que deberá soportar y aplicar los procedimientos de seguridad necesarios para impedir su acceso (servidores seguros).

DIVERSID AUTENTICACIÓN

Aplicaciones del sistema de autenticación

- Accesos seguros en Internet e Intranet
- Compras y pagos por Internet
- Pagos en Comercios
- Operaciones en Cajeros Automáticos
- Banca telefónica
- Operaciones con móviles
- Correo electrónico autenticado
- Domótica