Autenticación

OAuth

- OAuth2 es un protocolo de autorización que permite a terceros (clientes) acceder a contenidos propiedad de un usuario (alojados en aplicaciones de confianza, servidor de recursos) sin que éstos tengan que manejar ni conocer las credenciales del usuario. Es decir, aplicaciones de terceros pueden acceder a contenidos propiedad del usuario, pero estas aplicaciones no conocen las credenciales de autenticación .
- Es un protocolo abierto, que permite autorización segura de una API de modo estándar y simple para aplicaciones de escritorio, móviles y web. Wikipedia
- Es un protocolo estandar para la autorización. OAuth 2.0 se enfoca en la simplicidad de desarrollo al tiempo que proporciona flujos de autorización especifica para aplicaciones web, de escritorio, mobile, etc. https://oauth.net/2/

Uso

- Para realizar autenticación en aplicaciones usando cuentas autenticadas de otras aplicaciones como el d facebook sin que la ap y Google tenga acceso a todos los datos de tu cuenta de facebook y lo que es mas importante no tiene acceso a tu **nombre de usuario** ni a tu **password** de facebook.

Metodología de autenticación sin Oauth

Compra de un producto on line

- El usuario accede a la tienda y pulsa en el botón de login.
- La tienda le pide usuario y contraseña.
- El usuario se las da y accede a sus datos y pedidos.

Inconvenientes:

- Si **hackean** la tienda tienen acceso a todos mis datos incluido **nº de tarjeta** usuario y contraseña. Además, lo normal es que los usuarios utilicen estos datos en mas servicios con lo que podrían tener acceso a mis datos en otros servicios.

Funcionamiento con OAuth

Ejemplo con una tienda online usando PayPal.

- El usuario accede a la tienda online y esta le pide que se loguee con PayPal y el usuario le dice que si.
- La tienda online le pide a PayPal los datos los datos del usuario .
- PayPal, no la tienda online, pide al usuario su nombre de usuario y contraseña.
- El usuario los pone y configura a que datos y que permisos tendrá la tienda online.
- Posteriormente PayPal y tienda online se intercambian los datos acordados.

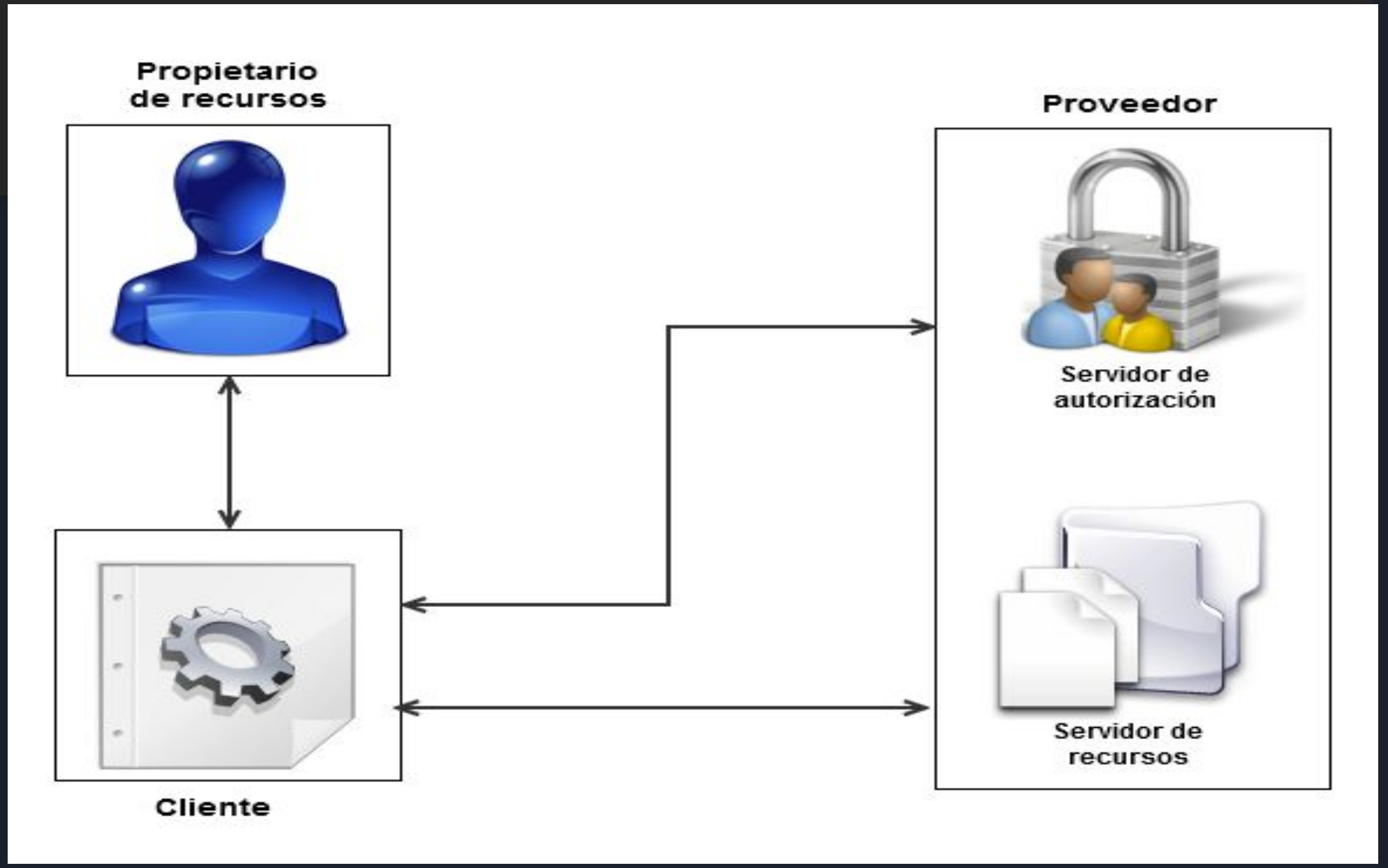
Problemas con Oauth

- Si hackean la tienda online no tienen acceso a nada, la tienda online solo tiene un token que solo sirve para acceder a PayPal desde los servidores de la tienda online y solo a una información limitada, ni al usuario, ni a la password, ni la tarjeta de crédito cosa que solo tiene PayPal.

http://aplicacionesysistemas.com/que-es-oauth/

Quienes usan OAuth

El escenario



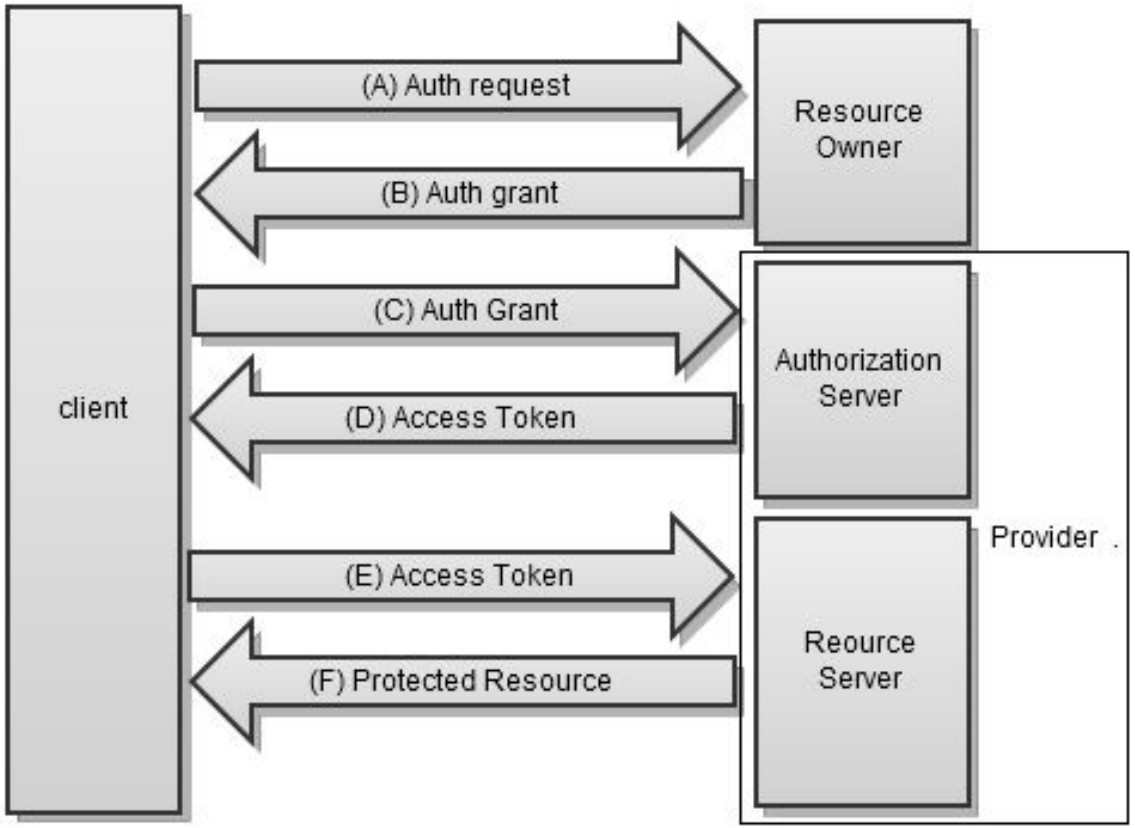
El escenario

- **Propietario de recursos**: Es una entidad capaz de dar acceso a recursos protegidos. Cuando es una persona nos referiremos a él como usuario final.
- **Cliente**. Es la aplicación que hace peticiones a los recursos protegidos en nombre de un propietario de recursos con la autorización del mismo.
- **Proveedor**
  - **Servidor de recursos**. Es la entidad que tiene los recursos protegidos. Es capaz de aceptar y responder peticiones usando un **access token** que debe venir en el cuerpo de la petición.
  - **Servidor de autorización**. En muchos casos el servidor de autenticación es el mismo que el Servidor de Recursos. En el caso de que se separen, el servidor de autenticación es el responsable de generar tokens de acceso y validar usuarios y credenciales.

El escenario

- Con este escenario surge la necesidad de implementar un protocolo de autorización, en el que el usuario final pueda autorizar a aplicaciones de terceros (consumidores) a acceder a sus datos en la aplicación proveedora sin necesidad de darle sus credenciales.

El escenario



(A) El cliente solicita autorización al propietario del recurso. La petición se puede realizar directamente al servidor de autorización en lugar de al propietario del recurso, lo que es aconsejable.
(B) El propietario del recurso concede la autorización para acceder al recurso informando al cliente uno de los cuatro tipos de autorización disponibles (authorization code, implicit, resource owner password credentials or client credentials). El tipo de concesión depende del tipo de concesión pedido por el cliente al iniciar el flujo
(C) El cliente pide al servidor de autorización un token de acceso, identificandose y presentando la autorización obtenida en el paso B.
(D) El servidor de autorización valida las credenciales del cliente y la autorización. Si son válidas devuelve un token de acceso.
(E) - (F) El cliente y el servidor de recursos ya son capaces de intercambiar peticiones seguras con el token de acceso para servir contenido protegido.

Un ejemplo de concepto

- **Usuario**: John Doe
- **Proveedor**: Facebook
- **Consumidor/cliente**: Foro
- Un usuario con cuenta en facebook, donde tiene alojados datos como sus listas de amigos, comentarios, publicaciones en el muro, etc... podría querer que un foro en el que participa acceda a su lista de amigos de FB, pero en ningún caso quiere darle al foro su nombre de usuario y contraseña de FB. Mediante OAuth2 conseguimos que el foro sea capaz solicitar datos a FB en nombre del usuario, y obtener la lista de amigos del usuario. Todas estas comunicaciones e intercambios de credenciales y autorizaciones se realizan de manera segura y en todo momento el usuario puede cancelar los privilegios del foro para pedir datos en su nombre

https://aaronparecki.com/oauth-2-simplified/

OpenID

- Es un sistema de identificación descentralizado que nos permite acceder a sitios en los cuales haya soporte para este sistema.
- Con OpenID podemos acceder a muchos sitios con un sólo nombre de usuario sin la necesidad de andar registrándonos en cada uno de ellos siempre que el sitio soporte este sistema.
- http://openid.net/

Como se usa?

- Primero tenemos que obtener una identificación de **OpenID** en cualquiera de los proveedores de identifiaciones.
- El ejemplo de uso lo vamos a hacer con el proveedor llamado myOpenID que es el que yo uso siempre. Al crearnos una cuenta en el sitio ya tendremos un nombre de usuario que será como una URL, un ejemplo sería *http://juanguis.myopenid.com*, éste nombre de usuario **nos servirá para loguearnos en todos los sitios que tengan soporte para OpenID**.
- De modo que luego cuando estemos en un sitio que soporte OpenID sólo usaremos ese nombre de usuario, y al tratar de acceder **nos redirigirá al sitio de myOpenID para que confirmemos el acceso del API a nuestra cuenta**, ahí mismo podemos elegir si queremos que sólo pueda acceder una sóla vez o para siempre. Luego cuando queramos loguearnos en el sitio que ya confirmamos como de confianza sólo ingresaremos el nombre de usuario y contraseña y accedemos directamente.

Ventajas de utilizar Open ID

- OpenID está que con un único nombre de usuario podrás acceder a cientos de sitios webs, sin recordar decenas de claves de acceso y usuarios diferentes.
- Es un sistema de gestión de sus datos, de forma que al autentificarte en un sitio web te preguntará que datos quieres compartir con este sitio d
- Es un estándar abierto y libre, que te permite confiar en un servidor que aloje el servidor de autentificación o incluso montar uno propio de tu máxima confianza para gestionarlo.

Autenticación SSO

- **Single sign-on** (SSO) es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación. Su traducción literal sería algo como «autenticación única» o «validación única».
- El login SSO sirve para acceder a los diferentes cuentas con un único usuario y contraseña.

Ejemplo de SSO

- Google Apps.

Se puede acceder a Gmail (gmail.com), Google Calendar (google.com/calendar), Google Maps (maps.google.com), Google Play (play.google.com), Youtube (youtube.com), Google News (news.google.com), Google Docs (docs.google.com)

Configuraciones de SSO

- **Enterprise single sign-on (E-SSO)**. Opera como una autenticación primaria; intercepta los requisitos de login que se requieren por las aplicaciones secundarias con el fin de completar los campos de usuario y contraseña. Para la correcta operación de E-SSO es necesario que las aplicaciones subyacentes permitan deshabilitar la pantalla de login.
- **Web single sign-on (Web-SSO)**. Este tipo de solución opera solamente con aplicaciones y recursos que se acceden a través de la web. El objetivo es autenticar a un usuario en varias aplicaciones en internet sin la necesidad de que lo hagan más de una vez

Configuraciones de SSO

- **Kerberos**. Es un método muy conocido y robusto para externalizar la autenticación. Los usuarios se registran en un servidor y obtienen un ticket (TGT, del término ticket-granting ticket), el cual es usado por las aplicaciones cliente para obtener acceso.
- **Identidad Federada**. Es una de las formas más nuevas de realizar tareas de SSO. Corresponde a una solución de Identity Management – o gestión de identidad – la cual permite usar las credenciales disponibles en un sistema de autenticación en otros, ya sea de una misma organización o incluso de otras empresas.
- **OpenID** es un proceso de SSO distribuido y descentralizado donde la identidad se compila en una url que cualquier aplicación o servidor puede verificar.

Doble factor de Autenticación

- Es una medida de seguridad extra que frecuentemente requiere de un código obtenido a partir de una aplicación, o un mensaje SMS, además de una contraseña para acceder al servicio.
- **Twitter**, **Google**, **LinkedIn y Dropbox**, entre otros servicios, ya ofrecen esta característica como un opcional de seguridad para las cuentas. Tanto Twitter como LinkedIn agregaron el sistema luego de ataques que alcanzaron caracter público, y otros sitios como Evernote también lo han implementado en el último año.

Doble factor de Autenticación

- Los sistemas de doble factor son mejores que la contraseñas solas, y más simples que las medidas biométricas (como pueden ser las huellas digitales o el reconocimiento facial), pero los atacantes eventualmente pueden encontrar el modo de vulnerarlos.
- Lo que el sistema garantiza es que los atacantes tendrán que trabajar más duro. Por ejemplo en un ataque reciente contra World of Warcraft, los cibercriminales crearon una replica del sitio web en la que se descargaba malware. Esto demuestra que el trabajo requerido para un atacante es mucho mayor, y eso es una buena noticia.

Doble factor de Autenticación

- Los sistemas de doble factor son mejores que la contraseñas solas, y más simples que las medidas biométricas (como pueden ser las huellas digitales o el reconocimiento facial), pero los atacantes eventualmente pueden encontrar el modo de vulnerarlos.
- Lo que el sistema garantiza es que los atacantes tendrán que trabajar más duro. Por ejemplo en un ataque reciente contra World of Warcraft, los cibercriminales crearon una replica del sitio web en la que se descargaba malware. Esto demuestra que el trabajo requerido para un atacante es mucho mayor, y eso es una buena noticia.

Es necesario usar en todas las cuentas?

- No. Idealmente, **deberías usar el doble factor de autenticación para tus cuentas más valiosas**, esto es, las que no puedes arriesgarte a que se vean comprometidas.

Factores de autenticación

- Un sistema de doble autenticación es aquel que utiliza dos de los tres factores de autenticación que existen para validar al usuario. Estos factores pueden ser:
- Algo que el usuario sabe (conocimiento), como una contraseña.
- Algo que el usuario tiene (posesión), como un teléfono o token que le permite recibir un código de seguridad.
- Algo que el usuario es (inherencia), o sea, una característica intrínseca del ser humano como huellas dactilares, iris, etc.
- Por lo general, los sistemas de doble autenticación suelen utilizar los factores conocimiento (nombre de usuario y contraseña) y posesión (teléfono o token para recibir código de seguridad).

Tipos de amenazas informáticas que utilizan los cibercriminales para vulnerar contraseñas

- FUERZA BRUTA: software que utiliza un “diccionario” cargado de contraseñas comúnmente utilizadas, con el objetivo de descifrar la clave de la víctima a través de comparaciones y pruebas sucesivas.
- MALWARE (CÓDIGO MALICIOSO): programa diseñado para realizar diversas acciones maliciosas, como el robo de contraseñas y credenciales de acceso.
- PHISHING: falsificación de una entidad de confianza, como bancos y redes sociales, por parte de un cibercriminal. De este modo, el atacante busca manipular a la víctima para que ingrese sus credenciales de acceso en un sitio falso pero que luce idéntico al original.

Tipos de amenazas informáticas que utilizan los cibercriminales para vulnerar contraseñas

- ATAQUES A SERVIDORES: vulneración de un sistema informático utilizado para almacenar la base de datos de credenciales de acceso de un determinado servicio.

Tarjeta de coordenadas

- La tarjeta de coordenadas es una herramienta de seguridad adicional al PIN o clave de seguridad bancaria requerida para realizar operaciones que impliquen movimiento de fondos o contratación de productos y servicios a través de servicios a distancia (banca electrónica o banca telefónica).

- Conforma un segundo factor de autenticación (algo que uno tiene) de la cuenta bancaria, pero a diferencia del PIN, que es fijo, es dinámica. Cuando una clave es dinámica es más difícil para los estafadores electrónicos (Phishing o correos fraudulentos) robar claves para hacer transferencias por Internet. Cada vez que lo intenten necesitarán una coordenada distinta, que es aleatoria y vence con cada sesión.

Tarjeta de coordenadas

- La Tarjeta de Coordenadas es una tarjeta de plástico, del tamaño de una tarjeta de crédito, que contiene una matriz o serie de números (generalmente pares de datos) impresos, es decir, ordenados en filas y columnas. Las filas están tituladas con números ascendentes a partir del 1 y las columnas con letras ascendentes alfabéticamente comenzando desde la A. En algunas entidades, el orden es inverso: en las filas se encuentran las letras por orden alfabético, y en las columnas los números. Para una tarjeta de 100 coordenadas se necesitan 10 filas (del 1 al 10) y 10 columnas (de la A a la J). La primer celda se llamará A1 y la última J10

Funcionamiento de la TC

- Al solicitar una transacción protegida por Tarjeta de Coordenadas (generalmente una transferencia bancaria electrónica, ya sea pago de impuestos y servicios, pago de compras, pago de sueldos, cambio de domicilio, etc) el sistema requerirá el número que se encuentra impreso en alguna celda. Por ejemplo, si tenemos la Tarjeta de Coordenadas del ejemplo, si solicita A8 se debe introducir el número 05, si solicita G3 se debe introducir el número 64, etc. Este procedimiento se repetirá y si las respuestas son correctas, podrá realizar la operación requerida. En caso contrario, se le denegará.

Tarjeta de Coordenadas de ejemplo

	A	B	C	D	E	F	G	H	I	J
1	89	56	41	13	26	23	16	10	87	78
2	06	46	69	89	62	80	81	96	87	13
3	33	46	05	99	14	63	64	45	18	66
4	56	52	04	56	92	27	85	99	59	47
5	02	24	58	67	79	31	49	55	52	09
6	68	26	62	05	60	32	53	08	99	47
7	37	49	45	90	39	33	85	13	22	11
8	05	77	72	24	31	35	06	48	80	95
9	33	62	89	08	85	91	21	87	30	97
10	16	50	68	58	65	96	91	74	55	65

Token de seguridad

- Un ***token* de seguridad** (también ***token* de autenticación** o ***token criptográfico***) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Token de seguridad

Tipos de token de seguridad

- **Dispositivos:**
  Existen tokens que se conectan directamente al ordenador o que lo hacen por métodos como bluetooth, aunque aquí también podríamos incluir los mensajes al móvil.
- **- Contraseñas:**
  Los tokens de seguridad más populares son los que se conocen como OTP Tokens (**One-Time Password**).