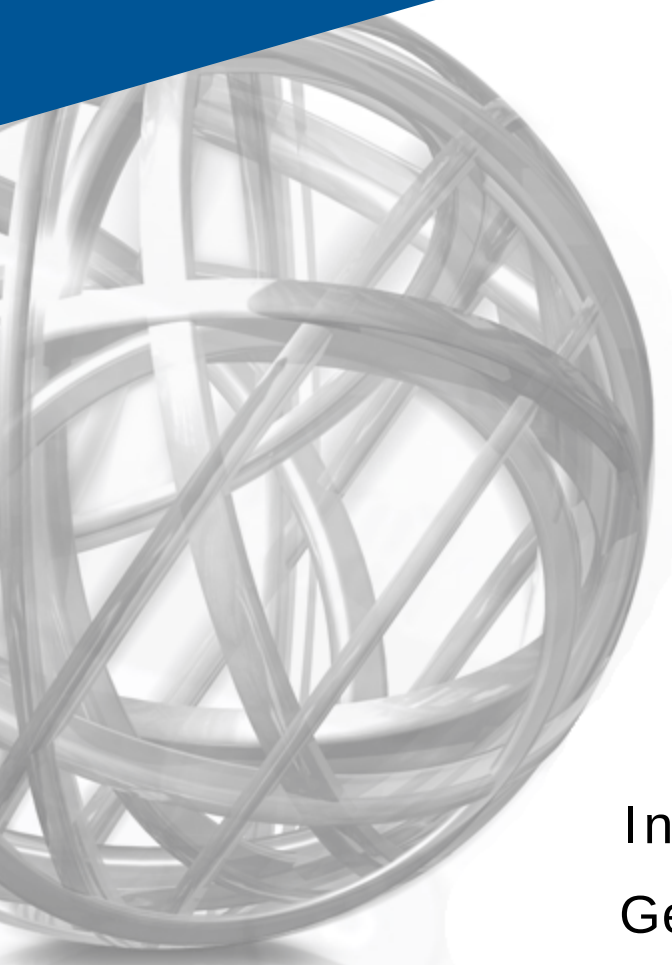
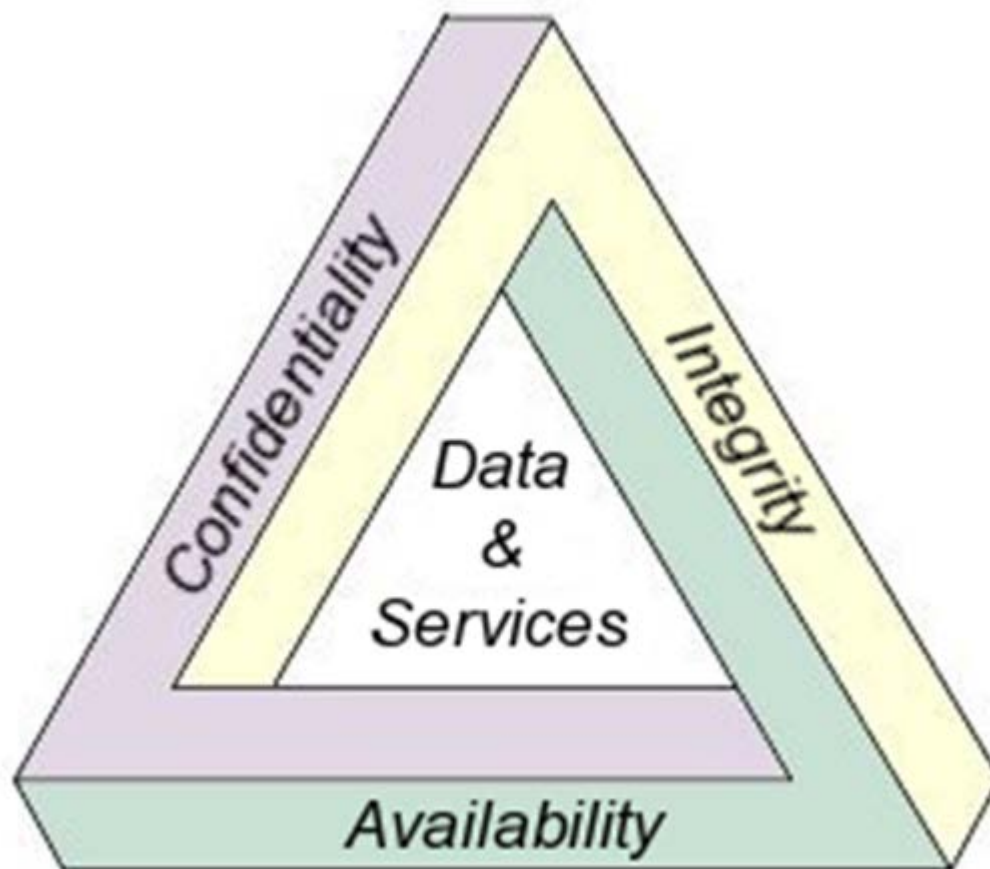




Soluciones de Autenticación Robusta

Ing. Alvaro Fernández - CISSP
Gerente Dpto. Ingeniería
Security Advisor

Seguridad de la Información



Agenda

- Repaso de Algunos Tipos de Ataque
 - Phishing
 - Spear Phishing
 - Trojanos
 - Man-in-the-middle (MitM)
- Autenticación Tradicional
- Autenticación Robusta
- Tipos de Autenticación Robusta
- Requerimientos **SUDEBAN**
- Conclusiones

Phishing

- **Definición**
 - Password Harvesting Fishing (cosecha y pesca de contraseñas)
- **Ejecución**
 - Ingeniería Social (cuento del tío)
 - Persona o Empresa de confianza en una aparente comunicación oficial electrónica.
 - Correo Electrónico / Llamadas Telefónicas
- **Escenarios Comunes**
 - Clonación de Sitio Web
 - Envío de Correo Electrónico



Phishing - Ejemplo

Nosotras.com : para mujeres de hoy - [Video: Antes y despues de las famosas. El milagro del paso del tiempo](#) - February 15

[« Back to Spam](#) [Delete Forever](#) [Not Spam](#) [More Actions](#) ▼

Paypal Spam | X [jordi@... | X](#)

★ from **Paypal**
reply-to akstcagbitaliamnsdgs@agbitalia.it,
to jordi@...
date Feb 18, 2008 7:54 AM
subject Paypal

PayPal

Dear PayPal ® customer,

We recently reviewed your account, and we suspect an unauthorized transaction on your account.

Protecting your account is our primary concern. As a preventive measure we have temporary **limited** your access to sensitive information.

Paypal features. To ensure that your account is not compromised, simply hit "**Resolution Center**" to confirm your identity as member of Paypal.

- Login to your Paypal with your Paypal username and password.
- Confirm your identity as a card memeber of Paypal.

Please confirm account information by clicking here [Resolution Center](#) and complete the "Steps to Remove Limitations."

*Please do not reply to this message. Mail sent to this address cannot be answered.

Copyright © 1999-2007 PayPal. All rights reserved.

[↩ Reply](#) [→ Forward](#) [💬 Invite Paypal to chat](#)

Phishing - Ejemplo

PayPal - Welcome - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites RSS Mail Print W Yellow Stickies People

Address http://cgi6-secured.de/customers/Secured/Service/mysql/ssl/connection/___/wf34gPaymentLanding&sslPageName=hhpayUSf&=userhgads&secure&ssl7r2vbd7

Note that the site looks like pay pal, but the web URL is different! It should show www.paypal.com/etc....!

PayPal [Sign Up](#)

Welcome Send Money Request Money Merchant Tools A

Member Log In [Forgot your Password?](#) **Join PayPal Today**
Now over 63 million accounts
[Sign Up Now](#)

Email Address

Password

The Fast **Way** Easy
Safe to Pay

PayPal is a global leader in online payments. [Find out more](#)

Spear phishing

- Definición
 - Ataque lanzado contra un objetivo concreto.
- Ejecución
 - Se envía un correo electrónico a los empleados de una determinada empresa, suplantando la identidad de un directivo o miembro de la misma.
 - Solicita nombres de usuarios, contraseñas o cualquier información de carácter confidencial con el objetivo de obtener acceso al sistema informático de la empresa.

Phishing – Efectividad

- Gartner: phishing tradicional
 - **19 %** clics en link en e-mail
 - **3 %** entrega información personal
- Indiana University: spear phishing
 - E-mail de un amigo: **72 %** tasa de exito
 - E-mail de estudiante desconocido: **16 %** tasa de exito
- Academia militar de West Point: spear phishing
 - E-mail del coronel a los cadetes: **80 %** tasa de exito

Trojanos

■ Definición

- Es un programa informático aparentemente inofensivo
- Proviene del término Caballo de Troya
- Se diferencia de los virus en que no se reproduce infectando otros equipos

■ Función

- Monitorear
- Tomar y Enviar
- Esconderse
- Actualizarse

■ Usos Comunes

- Robo de Credenciales Bancarias / Botnets



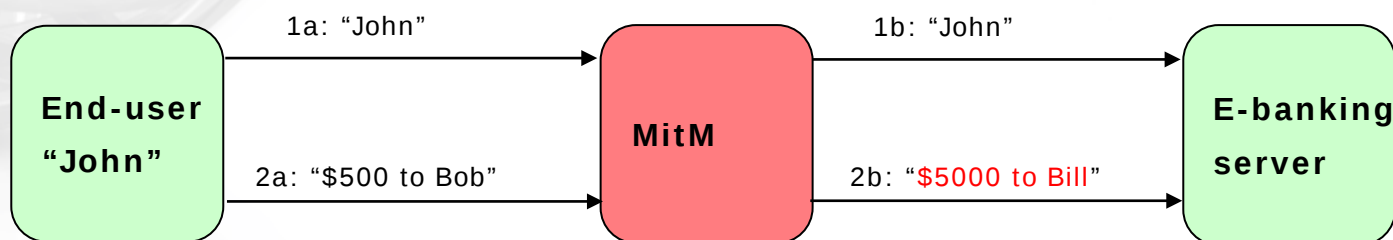
Man in the Middle (MitM)

■ Definición

- Intercepción y modificación en tiempo real de la información intercambiada entre las dos entidades sin que ninguna de ellas lo note
- Actúa como Proxy entre el usuario final y el sitio Web

■ Función

- Insertar transacciones fraudulentas
- Redirigir tráfico a un sitio fraudulento



MitM - HTML Injection

Sitio Web original



View Your Accounts 

Go to:

Username: [Forgot username?](#)

Password: [Forgot password?](#)

Need to set up online access?
[Sign Up Now](#)

Sitio web visto en una
maquina comprometida



View Your Accounts 

Go to:

Username: [Forgot username?](#)

ATM PIN:

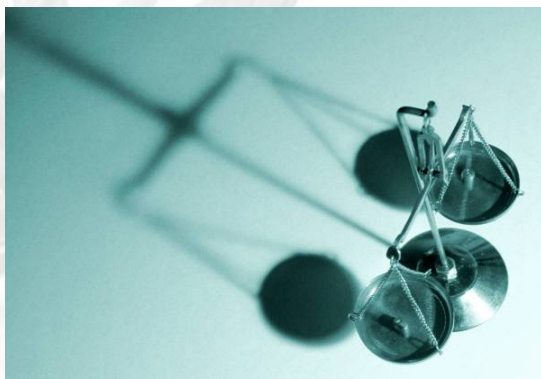
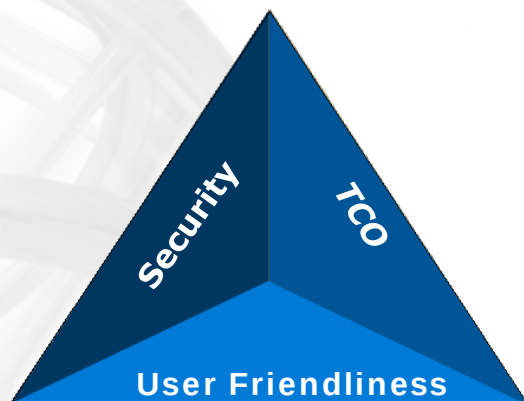
Password: [Forgot password?](#)

Need to set up online access?
[Sign Up Now](#)

Autenticación

- **Definición**
 - Proceso que verifica que el usuario es quien dice ser
- **Características**
 - Fiable
 - Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto)
 - Soportar con éxito cierto tipo de ataques
 - Ser aceptado por los usuarios que lo utilicen
- **Autenticación Tradicional**
 - Usuario / Contraseña
 - Algo que el Usuario sabe

Autenticación ... Es un balance entre ...



- Seguridad
 - Estándares/políticas
 - Procedimientos
- Costo total
 - Puesta en marcha
 - Mesa de ayuda
 - Escalabilidad
 - Precio
- Facilidad de uso
 - Aceptación del usuario
 - Portabilidad
 - Segmentación de clientes.

Autenticación Robusta

Something you have



Something you know



Strong User Authentication
= more than one of these elements

**Something
you have**

**Something
you Know**

**Something
you are**

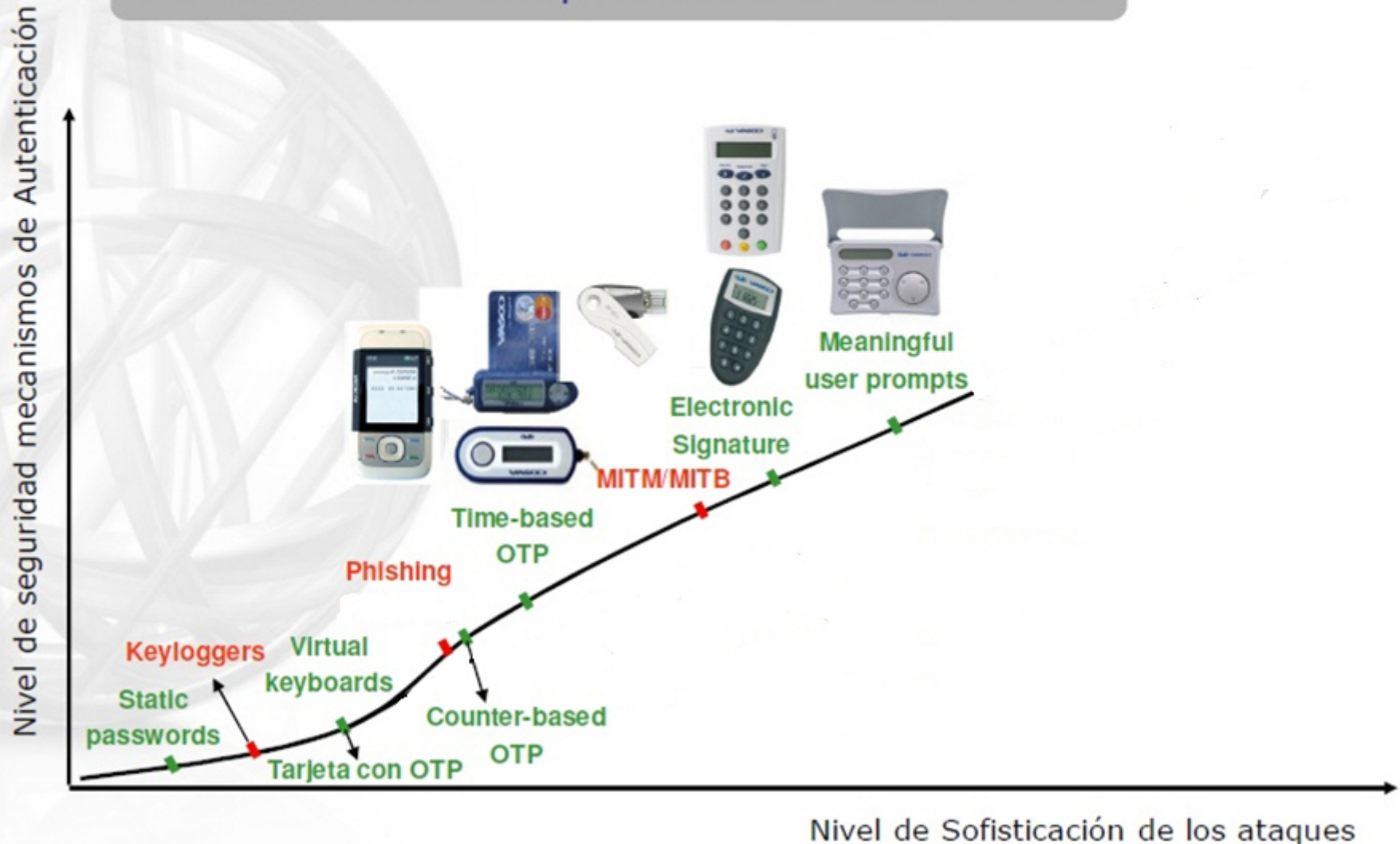
Something you are



Autenticación Robusta



Evolución de los dispositivos de autenticación:



Tarjeta de Coordenadas

■ Características

- La contraseña se utiliza una única vez, y se genera una contraseña nueva para la próxima
- Costo económico muy bajo
- Se puede clonar
- El usuario la lleva en su billetera

Brindarle el mejor servicio es trabajar por usted.

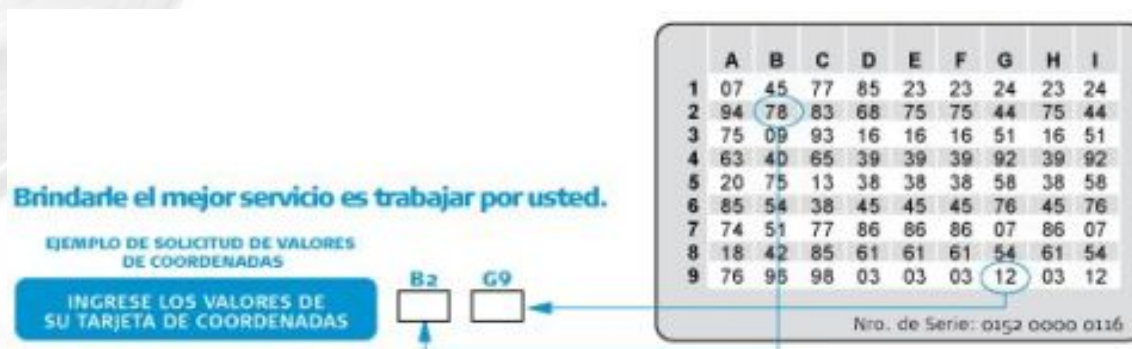
EJEMPLO DE SOLICITUD DE VALORES DE COORDENADAS

INGRESE LOS VALORES DE SU TARJETA DE COORDENADAS

B2 G9

	A	B	C	D	E	F	G	H	I
1	07	45	77	85	23	23	24	23	24
2	94	78	83	68	75	75	44	75	44
3	75	09	93	16	16	16	51	16	51
4	63	40	65	39	39	39	92	39	92
5	20	75	13	38	38	38	58	38	58
6	85	54	38	45	45	45	76	45	76
7	74	51	77	86	86	86	07	86	07
8	18	42	85	61	61	61	54	61	54
9	76	95	98	03	03	03	12	03	12

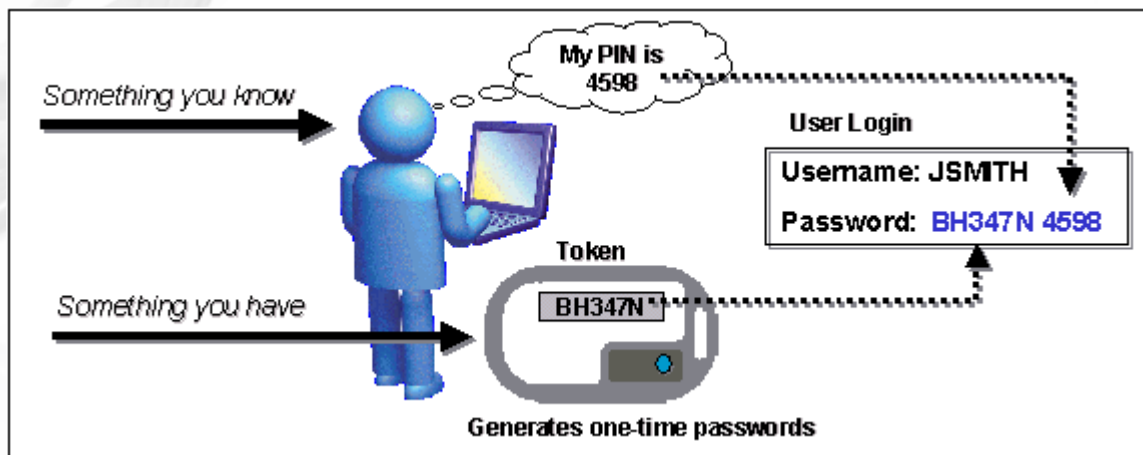
Nro. de Serie: 0152 0000 0116



One Time Password (OTP)

■ Características

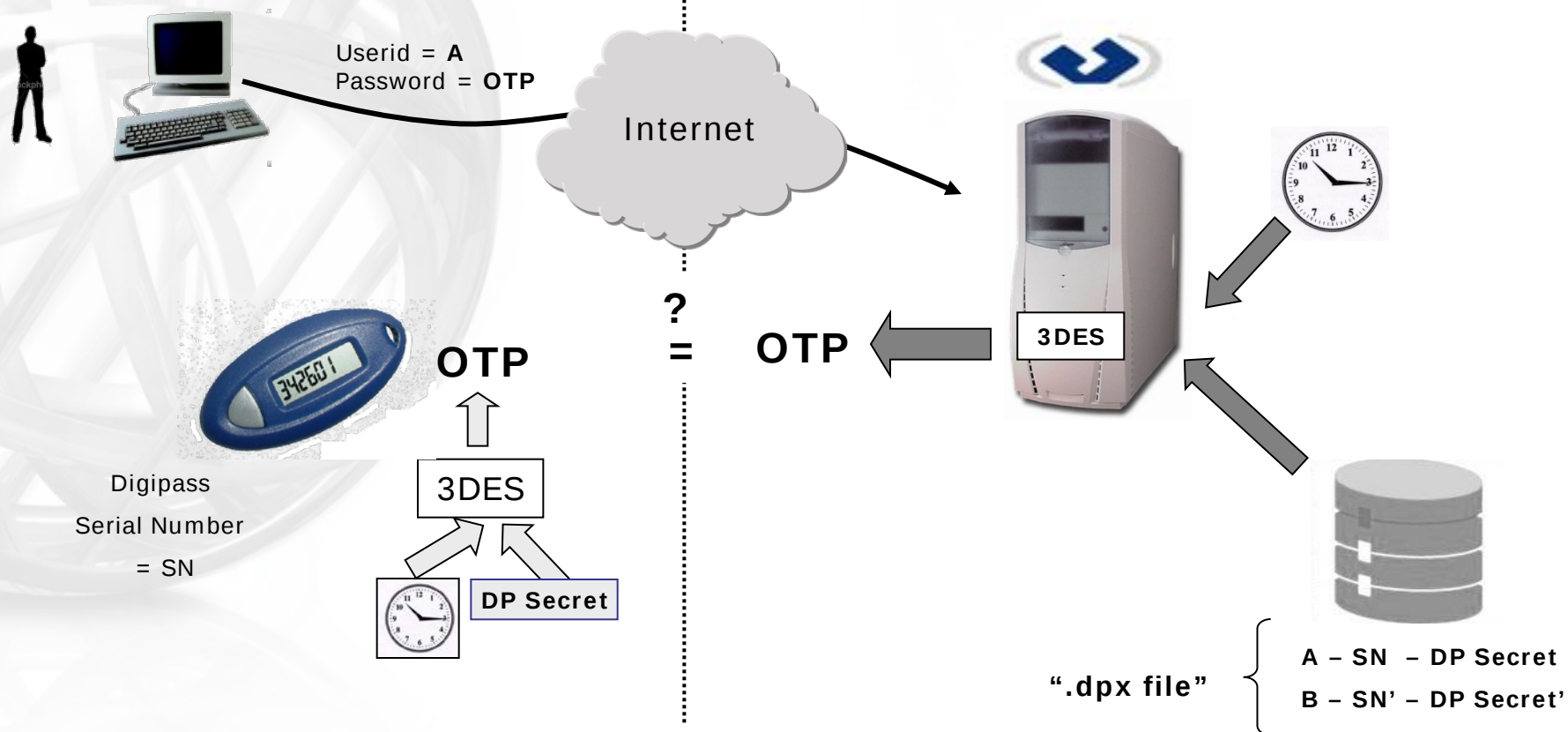
- La contraseña se utiliza una única vez, y se genera una contraseña nueva para la próxima
- En caso de que sea interceptada y haya sido usada, ya no funcionará
- No se puede clonar
- No se necesitan drivers



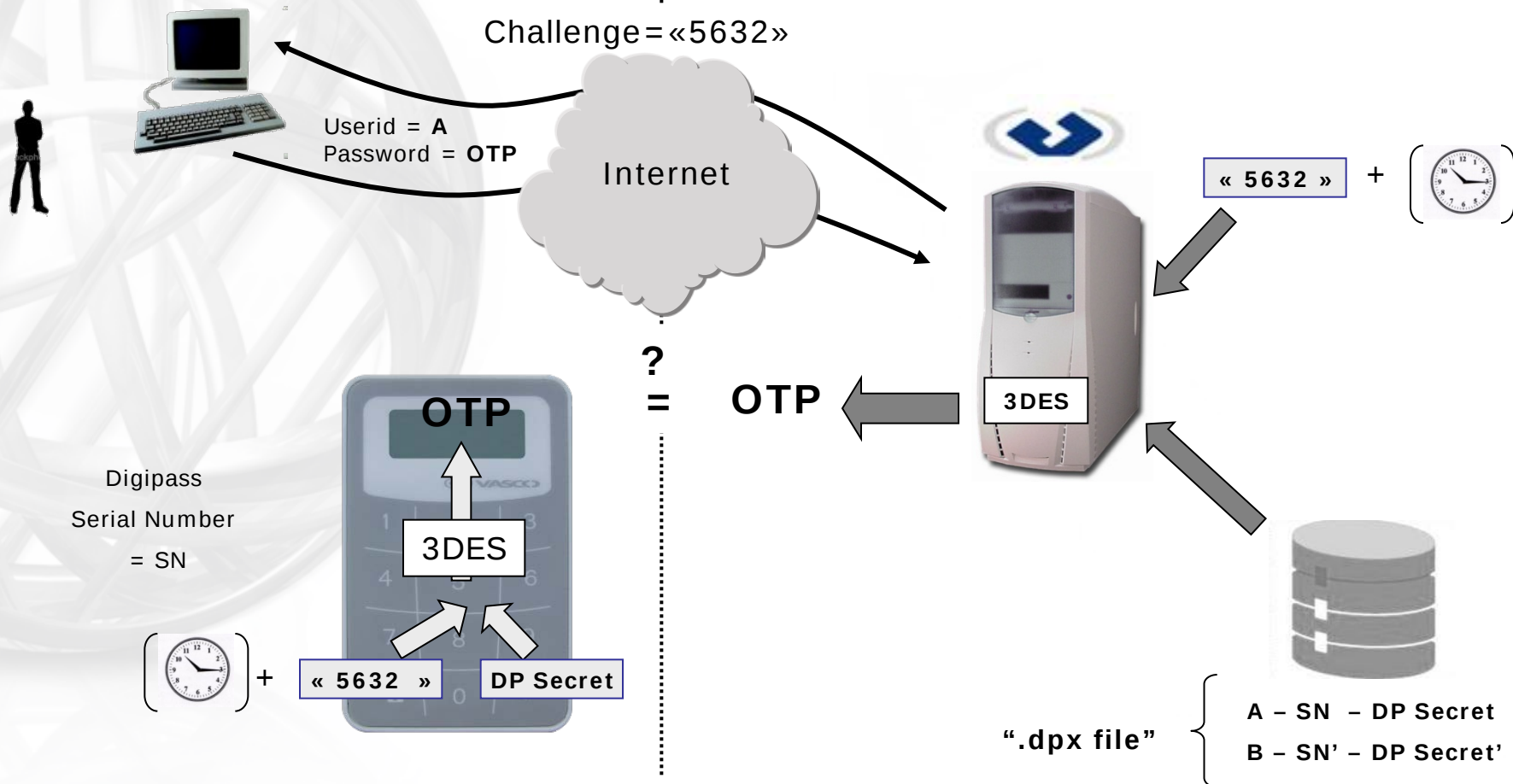
Tipos de OTP

- **Basadas en Eventos**
 - Validas hasta ser usadas o hasta que la próxima sea usada
 - Su tiempo de vida es controlado por el usuario
- **Basadas en Tiempo**
 - Se vuelve invalida pasado un tiempo predeterminado
 - Su tiempo de vida es controlado por el servidor
- **Basadas en Desafío / Respuesta**
 - Solo una OTP es valida en un momento determinado (sin ventana de tiempo)
 - Su tiempo de vida es controlado por el servidor

OTP Basada en Tiempo

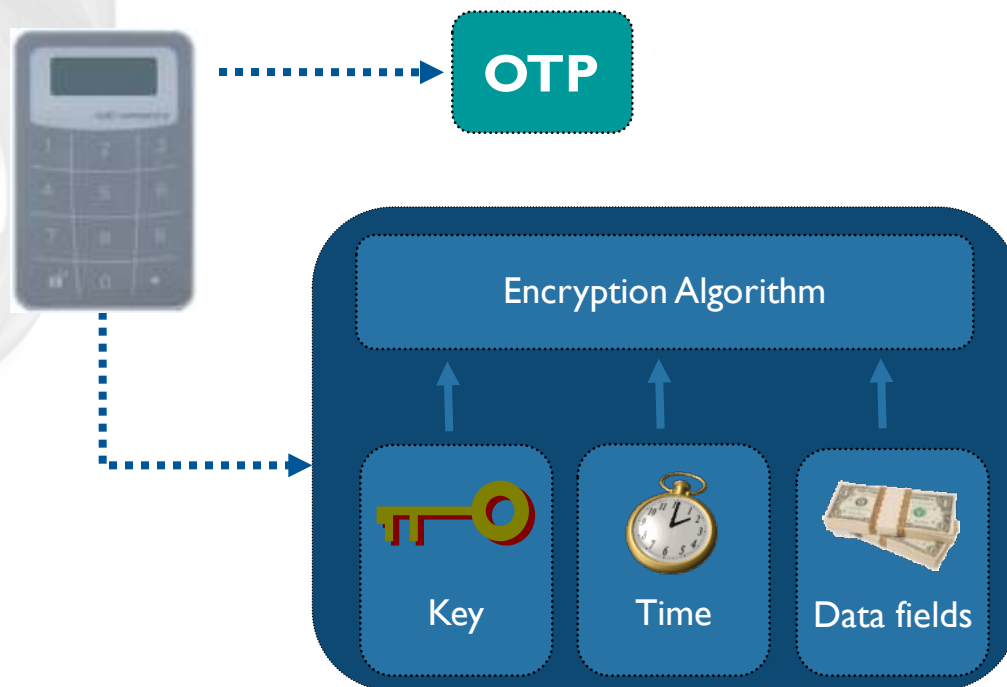


OTP Basada en Desafío / Respuesta

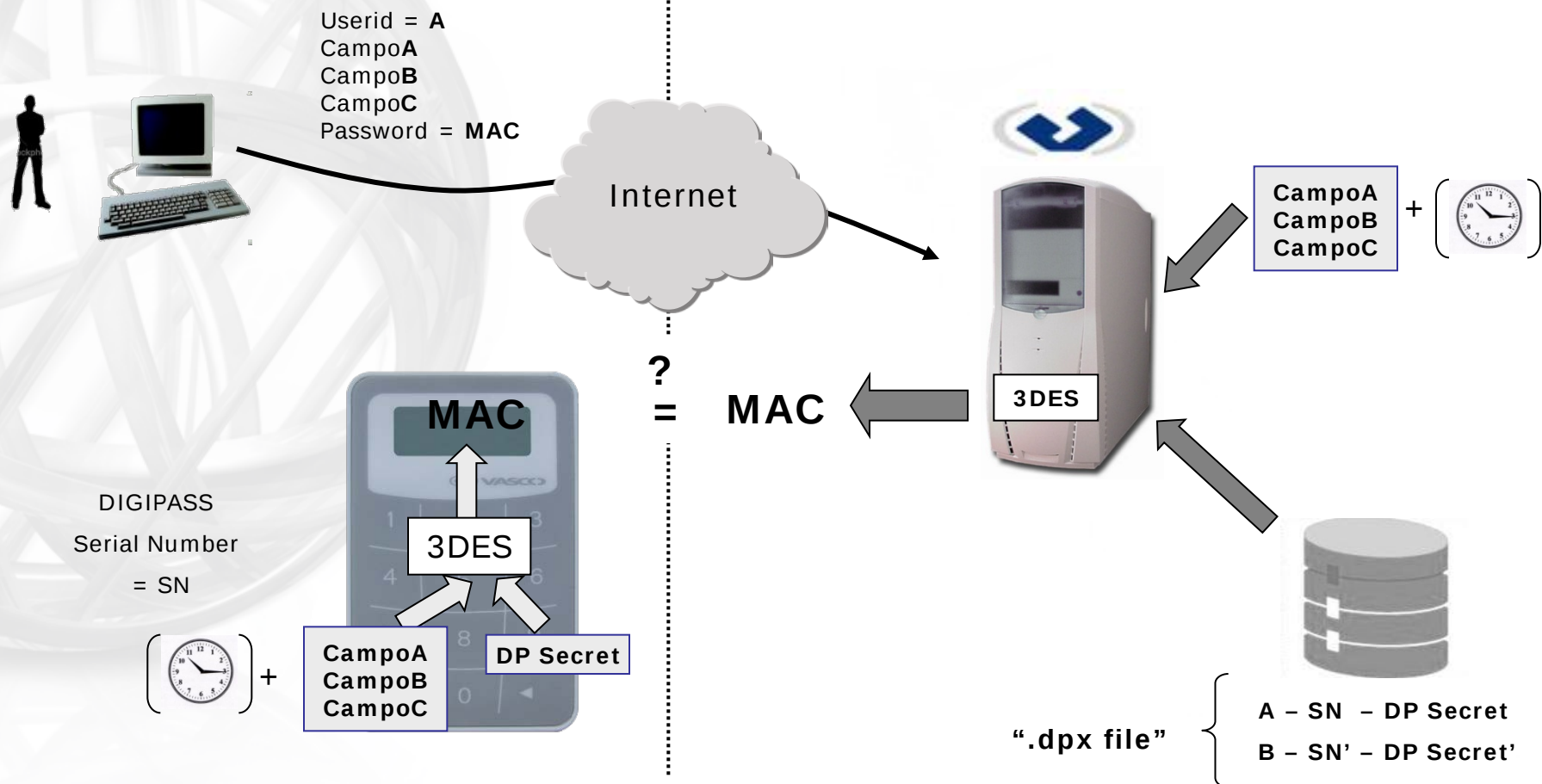


Firma Electrónica

- Digipass calcula la firma electrónica
- Medida contra MitM



Firma Electrónica



Autenticación de Servidor

- Características

- El Servidor despliega el siguiente OTP
- Solamente el Servidor lo puede conocer
- El Usuario puede validar que esta interactuando con el Servidor correcto
- Combate el Phishing



Requerimientos SUDEBAN Venezuela

Resolución 641.10 de 23 Dic. 2010

• Los Bancos e Inst. Financieras deben utilizar factores de Autenticación fuerte Para Banca Electrónica. (Agosto 2012)

Operaciones	Factores Requeridos *	
	Factor Base	Factor Adicional
Afiliación y desafiliación de Productos Y servicios	2	3, 4 o 5
Mantenimiento de productos, Servicios y Programaciones de pago.	2	3, 4 o 5
Pagos o transferencias a terceros.	2	3, 4 o 5
Apertura de Segundas cuentas o productos financieros	2	3, 4 o 5
Actualización de datos de la ficha del cliente a través de Banca por Internet.	2	4

Factor de Autenticación	Explicación
Factor 1	Información Básica del Cliente (Preguntas de Validación).
Factor 2	Claves Estáticas (Vencen cada 180 Días).
Factor 3	Claves Dinámicas (OTP) Soluciones Vasco.
Factor 4	Certificados Digitales (PKI). Soluciones Vasco.

VASCO

- Fundada en 1997
- Headquarters: Chicago, USA y Zurich, Suiza
- Compañías que confían en Vasco: 10.000
- Foco exclusivo en autenticación robusta



Servidor de Autenticación

Front-End Integration



Web-based Administration

- User & DIGIPASS Administration
- Reporting

Apache Tomcat Webserver

Webservice

Webservice

SEAL

Customer Web Applications

Outlook Web Access
CITRIX applications

RADIUS

RADIUS Client



RADIUS
via Windows API
via Custom API

Back-End Authentication

- RADIUS
- Windows
- Legacy

ODBC



Database

PostgreSQL

Digipass para Móviles

- **Necesidades de Mercado**
 - Autenticación sin hardware
 - Autenticación de usuario y transacciones
 - Fácil Uso
 - Fácil de Desplegar
 - Fácil de Integrar
- **Soporte para:**
 - Java Phones (all MIDP2)
 - BlackBerry
 - Iphone
 - Windows Mobile
 - Android
 - Symbian



Banking References Global

Cuentas Globales



Cuentas USA



Cuentas LATAM

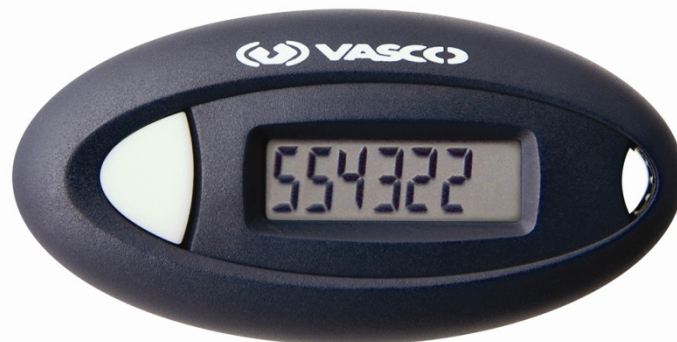


Otras Cuentas Globales



Security Advisor

- Fundada en el 2000
- Presencia Regional (Uruguay, Argentina y Chile)
- Foco exclusivo en Seguridad de la Información
- Representación exclusiva de Vasco
- Alguno Clientes Vasco en Uruguay:
 - Banco República
 - BBVA
 - Discount Bank
 - Coca Cola
 - HSBC
 - Antel
 - Itau



Conclusiones

- Autenticación Robusta
 - *Fiable*
 - *Económicamente factible*
 - *Soportar con éxito cierto tipo de ataques*
 - *Ser aceptado por los usuarios que lo utilicen*

- Implementación Habitual
 - *Algo que se sabe más algo que se tiene*

www.sadvisor.com



La clave de tu negocio