Los 7 métodos de Autentificación más utilizados

Evidian white paper

Aplique su política de autenticación gracias al SSO de empresa.

EVIDIAN
A Groupe Bull Company

Sumario

EVIDIAN
A Groupe Bull Company

Índice

Advertencia

Este documento es una introducción a la problemática de fuerte autenticación y acceso a las aplicaciones objetivos.

Presenta un estudio de los siete métodos de autenticación más utilizados actualmente y describe sus mecanismos principales. Asocia las funciones principales de un motor de Single Sign-On (SSO).

No considera la problemática de los Servicios Web ni de la Federación de identidad.

Para más información sobre un método en particular, referirse a los documentos más especializados.

La buena autentificación sobre el buen puesto de trabajo

La autentificación es la primera etapa del proceso de conexión de un usuario

Toda organización que se basa en un sistema de información tiene que garantizar el proceso de conexión a los sistemas y aplicaciones.

La creación de una fuente única y fiable de las identidades, asociada a la gestión de los derechos son los dos pilares de una buena infraestructura de gestión de las identidades y accesos.

El proceso de conexión de un usuario puede entonces efectuarse. Se articula en general alrededor de 4 etapas;

Proceso inicial - común a todas las conexiones

1. Abertura de una sesión sobre del puesto de trabajo y autenticación del usuario
2. Se comprueba los derechos del usuario y lo conecta a sus recursos

Proceso de conexión a una aplicación

1. Ejecución por el usuario de una aplicación y autenticación sobre esta aplicación.
2. La aplicación comprueba los derechos del usuario y lo conecta a sus transacciones y datos.

La autenticación del usuario es uno de los puntos clave de este proceso. Es ella que debe permitir del Sistema de Información asegurarse de la identidad del usuario y asociarle sus derechos.

Existen numerosos métodos de autenticación. Cada una de estos métodos posee sus características propias.

El nivel de seguridad

Su Política de seguridad

Toda organización tiene, o debería tener, una política de seguridad relativa a la protección de los puestos de trabajo, de las aplicaciones, de los datos o también de los sistemas del SI. Esta política de seguridad puede definir niveles mínimos de autenticación en función de la criticidad del recurso utilizado.

Por ejemplo, es posible imaginar, como en muy buena película de espionaje, que se coloca un puesto de trabajo crítico en una sala protegida por un acceso controlado por un código confidencial, por la introducción de una tarjeta inteligente y por una definición biométrica del ojo derecho. La protección es entonces a su máximo, ya que para registrar es necesario proporcionar un elemento **que se sabe** (el código), **que se posee** (la tarjeta) y **que es** (el ojo).

Este mecanismo permite efectivamente proteger un puesto de trabajo pero es costoso desde un punto de vista de la aplicación (requiere una sala por PC así como los lectores adecuados) y de la explotación (¿que pasa si un usuario olvida su código, pierde su tarjeta y se devuelve tuerto del ojo derecho?).

Las leyes y reglamentaciones

Las nuevas reglamentaciones, como Sarbanes-Oxley por ejemplo, exigen de establecer mecanismos que permiten aplicar la política de seguridad y **mostrar** que se aplica efectivamente.

La autenticación del usuario es uno de los elementos claves que deben tenerse en cuenta.

Es necesario autentificar efectivamente al usuario en el lanzamiento del puesto de trabajo y/o en la conexión a su aplicación aplicando las normas de la política de seguridad y también mostrar que se aplica bien el método de autenticación.

Arbitraje con los costes de aplicación y de explotación

La instauración de una solución de autenticación fuerte debe también analizarse al aliso de los esfuerzos para su aplicación y su explotación como:

Para las operaciones iniciales

- La creación y la distribución de los soportes físicos (tarjeta, token,…) o de los elementos lógicos (certificados X.509, contraseñas, datos biométricos) a los usuarios,
- La puesta en marcha de lectores específicos, si es necesario, sobre los puestos de trabajo,
- La aplicación de la infraestructura informática adecuada (PKI, servidor Kerberos, servidor de autenticación biométrico,…),
- La integración con las aplicaciones o con el SSO de empresa,
- La formación de los usuarios.

Para las operaciones de explotación

- La gestión de un recién llegado con la atribución de sus distintos elementos,
- La gestión del olvido de un elemento lógico (olvido de la contraseña o del identificador),
- La gestión de la pérdida de un soporte físico y de su sustitución (pérdida de una tarjeta),
- La gestión de la cancelación de un soporte (código PIN invalido, datos biométricos no válidos,…).

Estos esfuerzos deben percibirse como inversiones que van a permitir proteger los datos más sensibles de la empresa y aplicar la política de seguridad correspondiente.

La fuerte autenticación: desde la contraseña hacia la autenticación multi-factores, multi-soporte.

¿Autenticación o identificación?

Existe una diferencia muy simple entre identificación y autenticación: el comprobante.

Una identificación se basa en una simple declaración como la recepción o la lectura de un código de identificación (identificador, n° serie, código barra,…). Este código de identificación no se supone secreto. Es un dato público.

La autenticación se basa en un elemento de prueba como un secreto compartido o un secreto asimétrico. La autenticación permite asegurarse con un nivel de confianza razonable de la identidad del usuario.

Siete elementos de autenticación

Para autentificarse, un usuario proporciona en general al menos 2 elementos:

- su identificador que permite su definición.
- uno o más elementos que permiten garantizar la propia autenticación.

Encontramos así estos elementos bajo distintas formas. Ahí tienes el más ampliamente utilizados:

Tipo	Descripción
El identificador y la contraseña	El identificador y la contraseña son el par de autenticación más conocido. Simple, robusto, incluso rústico, su más grande defecto es que el nivel de seguridad depende directamente de la complejidad de la contraseña. Contraseñas simples son escasas, y contraseñas demasiado complejas conducen a los usuarios a aplicar estrategias no siempre correctas para gestionarlas: Post-it® , lista en un archivo Excel o en el SmartPhone,…
El identificador y la contraseña OTP (One-Time Password)[1]	El OTP permite asegurar el uso de la contraseña en la red. En efecto, con un sistema OTP el usuario posee un calculador especializado que le proporciona bajo petición una contraseña. Esta contraseña es válida solo durante una duración limitada, y para una única utilización. *Esta solución se aplica en general para el proceso de autenticación inicial para los accesos externos mediante IP/VPN*

[1] OTP: One-Time Password o también Contraseña de un solo uso.

Los certificados PKI sobre tarjeta inteligente o token USB	Los certificados X.509 aplican una tecnología avanzada de codificación que permite calcular o firmar mensajes sin tener que compartir de secreto. El identificador es un certificado público que es firmado y en consecuencia garantizado por una autoridad de certificación reconocida. El usuario debe proporcionar un secreto para poder utilizar los distintos elementos criptográficos: “el código PIN de su tarjeta o su tecla USB”. *Esta solución se aplica en general para el proceso de autenticación inicial o para las conexiones a las aplicaciones Red o de servicio de mensajería.*
Tecla “Confidencial Defensa”	Se trata de una declinación particular del ejemplo anterior. Es en general una llave multifunciones: almacenamiento de certificado X.509, almacenamiento de datos, recurso criptográfico etc…
El identificador y la contraseña sobre una tarjeta inteligente	El almacenamiento del identificador y la contraseña sobre una tarjeta inteligente permite suplementar la protección del proceso de autenticación. La contraseña puede así ser muy compleja y cambiada regularmente de manera automática y aleatoria. Sin la tarjeta, y sin su código PIN, no se puede acceder a la contraseña. *Esta solución se aplica generalmente para el proceso de autenticación inicial*
Biométrica	La autenticación por biométrica se basa en la verificación de un elemento del cuerpo del usuario (generalmente la huella dactilar). Puede basarse en un distribuidor central, en la puesto de trabajo o en una tarjeta inteligente para almacenar los datos biométricos del usuario. *Esta solución se aplica en general para el proceso de autenticación inicial y/o para proteger el acceso a aplicaciones muy sensibles.*
La definición sin contacto	El RFID es una tecnología que hoy se despliega en los proyectos de Identificación/Autenticación. Un chip RFID es insertada en una tarjeta y lleva un número de identificación. Este número se asocia a continuación a un usuario en un sistema informático. A la base es una tecnología de **Identificación** que puede, acoplado a una contraseña proporcionada por el usuario por ejemplo, utilizarse en procedimientos de autenticación. Existe 2 declinaciones de esta tecnología: **El RFID pasivo o HID**, que supone que la tarjeta no posee alimentación propia. La tarjeta es abastecida en la lectura por un campo electromagnético generado por el lector. *Este sistema se utiliza comúnmente para el control de acceso físico por tarjeta o el pago al restaurante de empresa. La detecta una tarjeta HID a algún centímetro.* **El RFID activo** se basa en los protocolos de comunicación RFID pero asocia a la carta una alimentación propia. Esta alimentación permite una detección de la tarjeta a más largo alcance (por ejemplo a partir de la entrada en una sala o una

	oficina). *El interés principal del RFID activo es permitir un acta de ausencia para los puestos de trabajo en zonas accesibles al público*

La autenticación multi-factores

Un factor de autenticación es un elemento **que se sabe** (código secreto), **que se posee** (apoyo físico) o **que es** (biométrica).

En cuanto varios factores de autenticación registran en juego, hablamos de autenticación **multi factores**.

*Ejemplos de sistema de autenticación a **1** factor:*	▪ Identificador + contraseña (elemento **que se sabe),** ▪ Definición sin contacto (elemento **que se posee),** ▪ Biométrica o identificador + biométrica (elemento **que es).**
*Ejemplos de sistema de autenticación a **2** factores:*	▪ Tarjeta inteligente + código PIN (elementos **que se posee Y que se sabe),** ▪ Tarjeta inteligente + biométrica (elemento **que se posee Y que es),** ▪ Biométrica + contraseña (elemento **que es Y que se sabe).**
*Ejemplo de sistema de autenticación a **3** factores:*	▪ Tarjeta inteligente + cifra PIN + biométrica (elementos que se posee Y que se sabe Y que es).

La multiplicación del número de factores de autenticación aumenta el nivel de seguridad general, pero plantea los siguientes problemas:

- El ciclo de vida de cada factor debe administrarse: inicialización de las contraseñas y códigos PIN, distribución de las tarjetas inteligentes,…,
- La ergonomía de utilización puede volverse demasiado pesado para los usuarios,
- Se añaden los costes de los periféricos (tarjetas inteligentes, lectores, sensores biométricos). Además, la carga del servicio de ayuda al usuario va a aumentar para administrar el conjunto de estos métodos (desbloqueo de las contraseñas y códigos PIN, distribución de las tarjetas, formación de los usuarios a la biométrica,…).

El Token

Una vez establecida la autenticación inicial del usuario, es necesario transmitir el token a las aplicaciones.

Una de las técnicas utilizada es el “token” de autentificación. Este “token” es un conjunto de datos que contienen los elementos que comprueban la identidad del usuario y que presenta a la aplicación.

La aplicación debe poder recuperar este token, disponible sobre el puesto de trabajo, luego ir dirigido a un distribuidor especializado que confirmará la validez del token así como la identidad asociada.

Los token más comunes hoy son Kerberos y los token SAML.

El token de tipo Kerberos

Se aplican, por ejemplo, en el entorno Windows.

El token de tipo SAML (también llamada aserción SAML)

Se aplica en arquitecturas SOA/J2EE/Servicios Web.

Los límites del enfoque por token

El enfoque por token requiere que las aplicaciones sean capaces de leer el “token” y de dialogar con el servidor de autenticación. Desgraciadamente, las aplicaciones ya existentes (e incluso algunas nuevas aplicaciones) no pueden siempre adaptarse simplemente.

El SSO de empresa permite hacer el vínculo entre la autenticación inicial del usuario y las aplicaciones de la manera más universal posible. El SSO de empresa interfaz directamente la ventana de demanda de identificador/contraseña de la aplicación y no tiene necesidad de modificación ninguna.

El SSO de empresa permite aplicar la autenticación fuerte para controlar el acceso a todas las aplicaciones

El SSO de Empresa permite proporcionar automáticamente a las aplicaciones los identificadores y contraseñas que requieren a su ejecución. El SSO de empresa permite aplicar una política a la gestión y a la utilización de estos elementos.

Función de SSO y política de seguridad: un ejemplo

La definición de una política de seguridad vinculada a los accesos depende de las funcionalidades de SSO disponibles que se pueden aplicar a las aplicaciones y usuarios en función de sus tipos de acceso. Estas funcionalidades son por ejemplo:

Autoaprendizaje

Si el usuario ejecuta una aplicación integrada al sistema de SSO y para la cual el sistema de SSO no conoce aún el identificador y la contraseña que debe utilizarse, el sistema de SSO pide al usuario proporcionar su identificador y su contraseña para esta aplicación.

Cuentas múltiples

En la ejecución por el usuario de una aplicación integrada al sistema de SSO y para la cual el usuario posee varias cuentas aplicativas, el SSO ofrece al usuario la elección de la cuenta sobre la cual desea conectarse.

Cambios planeados de las contraseñas secundarias

El SSO sabe cambiar automáticamente las contraseñas en función de la política de seguridad, o atendiendo a una petición de la aplicación o generando las acciones que evidenciarán la ventana de cambio de contraseña.

El SSO permite entonces crear contraseñas de gran longitud (por ejemplo 32 caracteres) con un formato complejo y aleatorio. Entonces el usuario no tiene necesidad de administrar esta contraseña.

Delegación de los accesos

El usuario puede, a partir de su puesto de trabajo, delegar sus accesos a otro usuario para un período dado y para una aplicación dada. El usuario delegado no tiene que conocer el identificador y la contraseña del usuario que delega para conectarse a las aplicaciones deseadas.

Integración de aplicaciones personales

El propio usuario puede integrar sus aplicaciones personales en el sistema de SSO. En ese caso, es él que define los atributos asociados a sus aplicaciones así como los identificadores y contraseñas.

Re-autenticación para acceso sensible

En la ejecución por el usuario de una aplicación integrada al sistema de SSO, este último puede pedir una re-autenticación dicha primaria (la misma que la autenticación inicial) con el fin de comprobar si el solicitante es el usuario corriente.

Controlar el acceso a una aplicación en función del puesto de trabajo

El sistema de SSO puede limitar el acceso a las aplicaciones más críticas a partir de un subconjunto dado de puesto de trabajo. Por ejemplo, las aplicaciones de I+D no pueden ser accesibles sino a partir de los puestos de trabajos de I+D.

El acceso mediante un portal Red a partir de un navegador cualquiera en Internet

Algunas aplicaciones deben poder ser accesibles mediante Internet a partir de cualquier puesto de trabajo. Es necesario mientras que los mecanismos de SSO puedan también aplicarse.

Un ejemplo de política de Seguridad de los accesos

A continuación, un ejemplo básico de política de seguridad de los accesos:

Clasificación de las aplicaciones	Atributos asociados a las aplicaciones
Normas Son aplicaciones utilizadas por todos (correo electrónico, notas de gastos…). Las contraseñas deben seguir siendo accesibles para algunos usuarios del exterior mediante un portal red seguro	▪ Se aplica el autoaprendizaje de los identificadores y contraseñas ▪ Se autoriza la delegación ▪ No hay re-autenticación en la ejecución de la aplicación ▪ Acceso Web mediante Internet
Críticas Son aplicaciones cuya utilización se limita a una familia de usuarios. Las contraseñas se ocultan con el fin de controlar su acceso mediante la solución de SSO.	▪ Las contraseñas se ocultan al usuario ▪ Los cambios de contraseña se gestionan automáticamente a la solicitud de las aplicaciones ▪ Se autoriza la delegación ▪ No hay re-autenticación en el lanzamiento de la aplicación ▪ No hay accesos Web mediante Internet

Críticas nivel superior Son aplicaciones cuya utilización se limita a una familia de usuarios. Sus accesos deben especialmente protegerse.	▪ Las contraseñas se ocultan al usuario ▪ Los cambios de contraseña se gestionan automáticamente de manera planeada ▪ La delegación está prohibida para algunos usuarios **y autorizada para otros (para los equipos de dirección)**. ▪ En la ejecución de la aplicación, el usuario debe re-autentificarse ▪ El acceso sólo se hace a partir de los puestos del servicio en cuestión o a partir de la zona en cuestión (Público front-office, back-offices,…) ▪ No hay accesos Web mediante Internet
Personales Son aplicaciones que los usuarios quieren poder integrar en su SSO.	▪ El usuario define las aplicaciones y los atributos (no hay delegación) ▪ Los usuarios definen los identificadores y las contraseñas ▪ No hay accesos Web mediante Internet

El SSO de Empresa permite integrar la autenticación fuerte en la política de seguridad

Con un SSO de Empresa, resulta posible integrar distintos métodos de autenticaciones y aplicarlos en función del tipo de puesto de trabajo. Por ejemplo, es posible aplicar

- Una autenticación biométrica para proteger los puestos y en consecuencia el acceso a las aplicaciones de I+D,
- Una autenticación RFID Activo que permite administrar el acceso a los puestos de trabajo compartidos
- Una autenticación por Identificador/OTP para proteger los accesos externos mediante IP/VPN
- Una autenticación por tarjeta inteligente X.509 para proteger los accesos Internet Web sobre un navegador cualquiera.
- Una autenticación por identificador/contraseña para los puestos “comunes”

El SSO de Empresa puede entonces administrar los accesos a las aplicaciones en función del puesto y el tipo de autenticación.

La re-autentificación

En la ejecución de una aplicación sensible, el motor de SSO puede volver a pedir una re-autentificación. Para los puestos equipados de un módulo de autenticación fuerte, es este tipo de re-autenticación que entonces se vuelve a pedir.

Esta función permite aplicar el mecanismo de autenticación fuerte a una aplicación que funciona sola con una autenticación login y contraseña, y esto sin cambos en la aplicación en cuestión.

Los 7 métodos de autentificación más utilizados

La infraestructura de autentificación Windows

La puesta en marcha de una autenticación fuerte en un entorno Windows requiere integrarse a la infraestructura de autenticación de Windows. Es necesario sustituir a veces o suplementar a los componentes Windows existentes. Estos componentes son, por ejemplo:

- El módulo de autentificación[2] del PC que se encarga de la autenticación inicial y la gestión de las excepciones inicializado por “Ctrl+Alt+Supr”. Es él que debe alimentar los logs de seguridad para la parte autentificación inicial además de las autenticaciones a las aplicaciones.
- El directorio de los usuarios que puede ser un Directorio Activo.
- La infraestructura Microsoft PKI que permite gestionar los certificados X.509.

Además, cuando se establecen lectores específicos (biométrica, tarjeta inteligente,…) es necesario instalar sobre Windows los componentes (los drivers) que permitirán gestionar el diálogo con estos elementos.

(1) Identificador y contraseña

Este método no requiere ninguna modificación de la infraestructura de autenticación Windows existente. Basta con instalar sobre el puesto de trabajo el módulo de SSO de Empresa para aplicar la política de seguridad de los accesos.

(2) Identificador y OTP (One-Time Password)

Arquitectura y principio

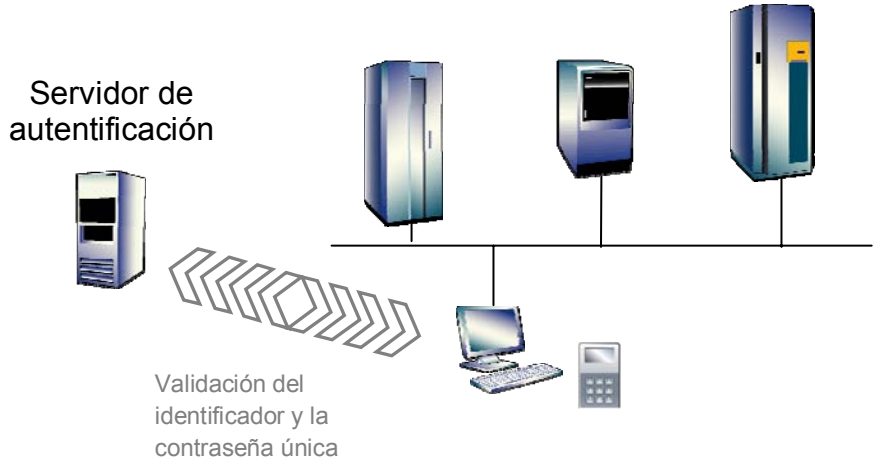
El usuario posee un “calculador” específico que va a permitirle proporcionar una contraseña válida durante un período limitado.

Para poder utilizar su calculador, debe entrar previamente una contraseña. El calculador le proporciona entonces a cambio una contraseña de un solo uso que el usuario va, a su vez, a proporcionar al módulo de autenticación del PC.

El módulo de autenticación dialoga a continuación con el servidor OTP para asegurarse de la validez de la información proporcionada y para aceptar o no la conexión.

[2] Este módulo también se conoce bajo el nombre de GINA.

Figura 1: Mecanismos OTP



Uno de los usos principales de este sistema por las organizaciones es la protección de los accesos sobre IP/VPN a partir de los PC situados fuera de la oficina.

Puesta en marcha y explotación

Esta solución supone en general la aplicación de uno o más servidores específicos de autenticación accesibles en 24x7.

Cada usuario debe poseer una calculadora específica y la contraseña asociada.

Es necesario establecer los procedimientos de gestión de las solicitudes usuarios a raíz de la pérdida o el olvido de una calculadora o al olvido de una contraseña.

(3) El Token USB o tarjeta inteligente PKI

Las soluciones a base de PKI comienzan a desplegarse efectivamente para garantizar las autenticaciones iniciales.

La aplicación de una solución a base de tarjeta inteligente y certificado supone la agregación de varios componentes

- La tarjeta con su lector así como el código informático asociado que debe instalarse sobre el puesto de trabajo.
- La infraestructura de certificado X.509 debe proporcionar los distintos componentes de una infraestructura PKI: la Autoridad de Certificación y la Autoridad de Registro.
- El CMS (Card Management System) que va a administrar la atribución de las tarjetas.
- El módulo de autenticación Windows.
- El servidor de autenticación.

Los distintos tipos de tarjetas

Hay principalmente dos grandes familias de tarjeta:

- Las tarjetas inteligentes criptográfica () que requieren un lector. Permiten integrar otras tecnologías para otros usos, como, por ejemplo: una antena sin contacto (acceso físico), o una pista magnética (cantina, gestión del tiempo).
- Los TokenUSB (con chip) que no necesitan lector y pueden conectarse directamente al PC con los pilotos convenientes. Estos token USB pueden aportar funciones complementarias como un disco externo.

La infraestructura de PKI

Una infraestructura a llave pública por regla general está formada por tres entidades distintas:

La autoridad de registro (S.A.). Esta entidad se encarga de las operaciones administrativas como la verificación de la identidad del usuario o el seguimiento de las solicitudes.

La autoridad de certificación (CA). Esta entidad se encarga de las tareas de creación de certificados o firma de las listas de revocación.

La autoridad de depósito (AD). Esta entidad se encarga de la conservación en seguridad de los certificados.

Las funciones del CMS

Un Card Management System debe poder efectuar las siguientes funciones:

- Creación de una tarjeta para un nuevo empleado: asociación de la tarjeta a un empleado y, dialogar con la CA del PKI para recuperar el certificado del empleado y ponerlo en la tarjeta
- Préstamo de una tarjeta temporal a un empleado cuando el empleado olvida su tarjeta
- Puesta en lista negra (blacklist) de una tarjeta perdida (o retirada de la lista negra si se encuentra)
- Desbloqueo a nivel local o a distancia de un código PIN que un usuario “invalidó”

Debe ser utilizable por el servicio de help-desk para gestionar las funciones de desbloqueo de un código PIN y por las estructuras de servicio en los distintos lugares para la creación, la asignación o el préstamo de una tarjeta.

El módulo de autentificación

El módulo de autentificación del puesto debe autentificar al usuario:

1. Pide el identificador y el código PIN de la tarjeta
2. Comprueba ante el CMS que la tarjeta no está en la “lista negra” de las tarjetas

3. Recupera el certificado público en la tarjeta, comprueba su firma y comprueba que no se publica en la "lista negra"
4. Pide a la carta firmar un *desafío* y comprueba (o hace comprobar por un servidor) que la firma corresponde bien al certificado público

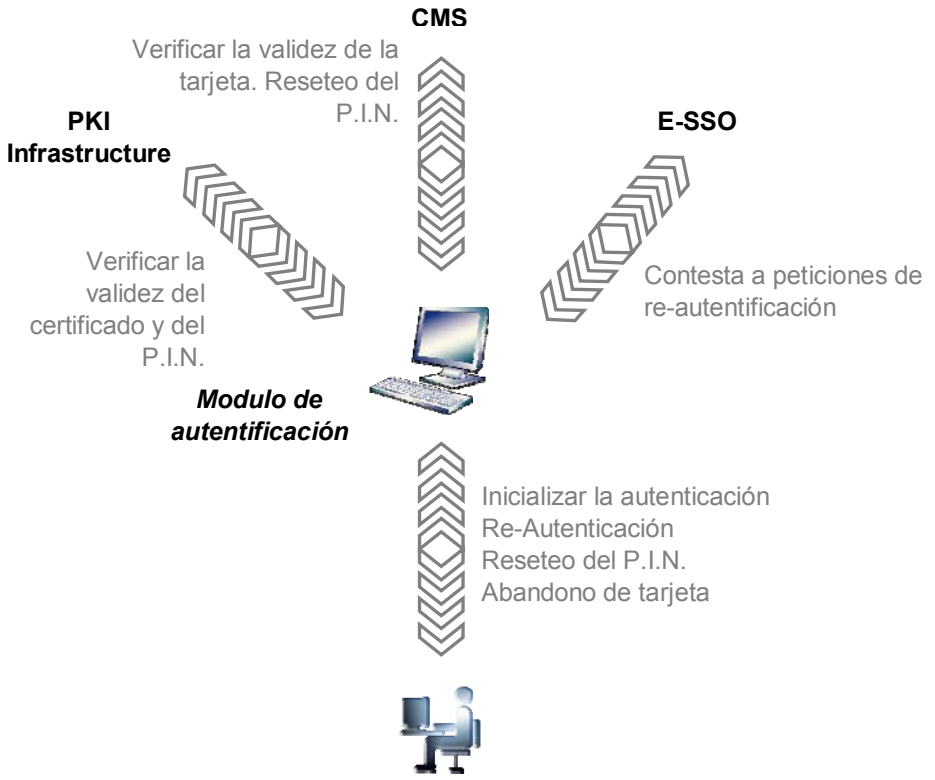
En caso de validación de los elementos, este módulo autoriza el acceso al puesto de trabajo bajo la identidad requerida.

Debe también gestionar otros acontecimientos:

- La pérdida o el olvido del código PIN. El módulo de autentificación debe poder permitir al usuario de recuperar una contraseña o un código PIN respondiendo a algunas cuestiones sin necesidad de llamar al Help desk
- El reseteo a distancia del código PIN de una tarjeta por el help desk.
- La protección del puesto de trabajo cuando se quita la tarjeta del lector: cierre de la sesión Windows, o bloqueo simple.
- La posibilidad de permitir el "Cambio rápido de usuario" que cambia rápidamente el contexto del SSO de empresa y abre las aplicaciones en el contexto de seguridad personal del usuario.

El módulo de autenticación está en el centro de una autentificación a base de PKI.

Figura 2: El módulo de autenticación del puesto en el centro de la autenticación fuerte



(4) La Llave "Confidencial Defensa"

La llave "confidencial defensa" es una declinación particular del ejemplo anterior. Es en general una llave multifunciones: almacenamiento de certificado X.509, almacenamiento de datos, recurso criptográfico para el cifrado al instante del disco duro o cualquier otro componente como el VoIP o de flujos aplicativos PC/Servidor.

Con el fin de eliminar los riesgos de "key loggers"[3], el código PIN de la llave se compone sobre la propia llave con el fin de evitar el uso del teclado.

Esta llave es capaz de transportar de manera segura los distintos elementos del SSO de empresa que se vuelve entonces portable y utilizable sobre cualquier puesto.

Este tipo de llave, verdadera caja fuerte electrónica, permite poner en marcha una solución portable, integrada y asegurada de Autenticación fuerte y SSO de Empresa.

(5) La tarjeta inteligente con identificador y contraseña

Una solución más ligera permite utilizar la tarjeta inteligente para almacenar el identificador y la contraseña Windows del usuario. A la autenticación del usuario, el módulo de autenticación del puesto va a utilizar estos elementos para autentificar al usuario para el directorio LDAP.

La tarjeta se utilizará entonces para proteger los datos de seguridad, como por ejemplo, las contraseñas SSO.

No se necesita infraestructura PKI; sólo el CMS y el SSO de Empresa siguen siendo necesarios.

(6) Las soluciones biométricas

Las soluciones biométricas utilizan lectores biométricos para controlar los accesos físicos.

Hay relativamente pocos proveedores de lectores biométricos. Algunos fabricantes de portable proponen una opción para integrar este tipo de lector en el cuerpo del portable.

Las soluciones de biométrica se utilizan en general dentro de la empresa para proteger el acceso a las aplicaciones más sensibles. No hay actualmente normas aplicadas por los navegadores del mercado que permitirían controlar los accesos a partir de cualquier PC en Internet.

---

[3] el "key logger" es un código malware que se instala sobre el PC que registra las teclas usadas por el usuario y enviadas a un servidor.

Las tres familias de solución de biométrica

El almacenamiento y la gestión de los datos biométricos se chocaron con las normas legales de protección del individuo. Algunos países, por ejemplo, no autorizan la instauración de bases de datos centrales de datos biométricos.

Las soluciones de biométrica permiten aplicar tres tipos diferentes de arquitecturas.

	Almacenamiento de los datos de biométrica	**Verificación de la autenticación**
Solución a base de servidor	En el servidor	Por el servidor
Solución puesto de trabajo	Sobre el puesto de trabajo del usuario	Por el puesto de trabajo
Solución a base de tarjeta criptográfica	En la tarjeta criptográfica	Por la tarjeta inteligente o por el puesto de trabajo

Las soluciones de biométrica con servidor

Se basan sobre los componentes siguientes;

- Un servidor central,
- Un módulo de alta de las firmas biométricas,
- Un módulo de autentificación específico para gestionar la autentificación.

Las soluciones locales

Estas soluciones evitan el almacenamiento centralizado de las firmas biométricas almacenando todo dato sensible sobre el puesto de trabajo del usuario.

Si esta solución es más aceptable desde un punto de vista legal en numerosos países, plantea el problema de la movilidad de los usuarios en la empresa.

Las soluciones de biométrica con tarjeta inteligente.

Estas soluciones evitan también la utilización de un servidor central, dando al mismo tiempo al usuario la posibilidad de desplazarse en la empresa. En efecto, sus firmas biométricas se conservan sobre su tarjeta inteligente y lo siguen sobre todos los puestos de trabajo.

Si esta solución esta a la más desplegada en numerosos países, requiere el uso de un “Card Management System” para el gestión de las tarjetas y de disponer de todos los periféricos necesarios sobre los distintos puestos de trabajo.

(7) El RFID Activo

Las soluciones a base de RFID Activo aplican el protocolo RFID para identificar al usuario sin contacto físico, a algunos metros de distancia.

La tarjeta del usuario posee una alimentación propia que le permite dialogar con una antena conectada al PC.

El PC es entonces capaz de detectar la llegada o la salida de un usuario sin que este tenga que hacer ninguna acción en particular. Es posible modificar los distintos parámetros que regulan las reacciones del PC como:

1. La distancia de detección de la llegada de un usuario y la distancia de detección de la salida de un usuario
2. La acción que debe aplicarse en la salida de un usuario: cierre de la sesión Windows, bloqueo de la sesión o también dejar el PC en este mismo estado
3. La acción que debe aplicarse en la llegada de un usuario: pedir la contraseña Windows o no, liberar la pantalla …
4. La acción que debe aplicarse cuando se detecta varios usuarios al mismo momento

Estos distintos parámetros permiten describir distintas situaciones de uso como, por ejemplo: el “cambio rápido de usuario” en el servicio de las Urgencias de un hospital o también la protección de un puesto de trabajo en la zona pública de una agencia bancaria.

Los elementos de una solución de RFID Activo

Los principales elementos de una solución de RFID Activo son:

- Los elementos físicos como las tarjetas de los usuarios y la antena para cada PC
- El módulo de autenticación que debe instalarse sobre el PC
- El sistema de gestión de las tarjetas que, además de las tareas de gestión corrientes, dialoga con el módulo de autenticación de los puestos para la definición de las tarjetas, y la gestión de los identificadores y contraseñas de apertura de sesión.

Un ejemplo de política de autenticación

Con el ejemplo de una organización que, por razones legales y tras un grave incidente que causa el robo de datos sensibles, debe aplicar una política de autenticación avanzada. Decide entonces establecer las normas siguientes para la autenticación inicial.

1. El identificador y la contraseña corresponde al medio normal de autenticación. La contraseña deberá tener al menos 10 caracteres, incluir al menos 2 numéricos y 2 alfabéticos. Se deberá cambiar de contraseña cada mes.
2. Las aplicaciones Web accesibles desde Internet deben ser protegidas por una tarjeta inteligente criptográfica con certificado X.509 (PKI)
3. La biométrica se utiliza internamente para proteger las aplicaciones de I+D
4. El RFID Activo se utiliza para proteger los PC de las oficinas ubicadas en zona “Espacio Abierto” público. Solo algunas aplicaciones son accesibles a partir de estos PC.

Es el SSO de empresa que va a permitir aplicar efectivamente esta política.

Norma 1: política de cambio de contraseña

La política de contraseña así definido es extremadamente complicada. Un usuario no puede aplicarse para todas las sus aplicaciones. Es el SSO de empresa que va a encargarse de mantener esta politica.

Por el contrario, el usuario **deberá y podrá** aplicar efectivamente esta política para su autentificación Windows.

Norma 2: Acceso a las aplicaciones Web mediante Internet

El acceso Web del motor de SSO va a permitir establecer una autenticación con tarjeta X.509 sin tener que modificar las aplicaciones que podrán funcionar con su identificador y contraseña. Estos últimos son los mismos que los proporcionados por el usuario desde su PC dentro de la organización o por Internet.

Norma 3: Protección de las aplicaciones más sensibles por biométrica

El motor de E-SSO va a permitir limitar el acceso a las aplicaciones I+D a los puestos de I+D equipados de lectores biométricos para la autenticación. Un usuario podrá utilizar un PC normal para conectarse a sus aplicaciones clásicas o utilizar un PC con lector biométrico cuando desea conectarse a sus aplicaciones I+D, además de sus aplicaciones.

Norma 4: el acceso en zona pública

El SSO de empresa permitirá a los usuarios utilizar la definición por tarjeta RFID activa para acceder a las solas aplicaciones autorizadas en zona pública.

El SSO de empresa integra la autenticación fuerte en la política de seguridad

Poner en marcha una solución de autentificación avanzada para la autentificación inicial no sirve para nada si no se soluciona los problemas de autentificación para el acceso a las aplicaciones.

El SSO de empresa va a permitir desplegar eficazmente una política global de autenticación sobre el Sistema de Información:

- Gestión y protección de los accesos a las aplicaciones
- Filtrado de las aplicaciones en función del PC y el método de autenticación asociado
- Consolidación de la información de logs (auditoria) para todos los tipos de autentificación (inicial y a las aplicaciones).

Evidian puede ayudarles a establecer un proyecto de autentificación de sus usuarios y control de acceso a sus aplicaciones.

Para más información, pueden contactar:
http://www.evidian.com/evidian/contacts.php&c=lbstrauth

Para más información, consultar el sitio www.evidian.com/

Correo electrónico: info@evidian.com