TEMA 131

ACCESO REMOTO A SISTEMAS CORPORATIVOS: GESTIÓN DE IDENTIDADES, SINGLE SIGN-ON Y TELETRABAJO.

Versión	30.2
Fecha de actualización	02/01/2025

ÍNDICE

ÍNDICE 2
1. GESTIÓN DE IDENTIDADES – GI 3
1.1 PRODUCTOS SOFTWARE PARA LA GESTIÓN DE IDENTIDADES 4
1.2 FEDERACIÓN DE IDENTIDADES 4
2. SINGLE SIGN-ON (SSO) 6
2.1 CONFIGURACIONES SSO EN UN DOMINIO 7
2.2 CONFIGURACIONES SSO MULTI-DOMINIO 9
3. GESTIÓN DE IDENTIDADES EN LAS AAPP 9
3.1 AUTENTICA 9
3.2 CL@VE 10
3.3 NODO EIDAS 10
3.4 EIDAS2, EUID Y EUROPEAN IDENTITY WALLET 11
4. TELETRABAJO 12
4.1 MARCO NORMATIVO 12
4.2 TECNOLOGÍAS RELACIONADAS CON EL TELETRABAJO 13

1. Gestión de Identidades – GI

Por Gestión de Identidades (IdM, Identity Management en inglés) se entiende un sistema integrado por políticas y procesos organizacionales que pretende facilitar y controlar el acceso de los usuarios y aplicaciones a los sistemas de información y a las instalaciones. Comprende los procedimientos de autenticación, autorización y contabilidad (Authentication, Authorization, Accounting).

El Ciclo de vida de GI consta de:

1. Creación de usuarios y perfiles
2. Gestión del cambio y mantenimiento
3. Finalización de usuarios/perfiles

Las ventajas que aporta el sistema de gestión de identidades son:

1. Organización: control y experiencia usuario.
2. legal, ayuda a cumplir requisitos de auditoría y trazabilidad.
3. Seguridad y control.
4. Consistencia e integridad de los datos
5. Escalabilidad

Dentro de los componentes principales de estos sistemas tenemos:

1. **Directorio:** almacenamiento y acceso a la información del usuario.
    a. Ejemplos:
        i. Microsoft Active Directory
        ii. Apache Directory Server: compatible con LDAPv3 certificado por el Open Group, soporta Kerberos y NTP (Network Time Protocol).
        iii. Novell Directory Services – eDirectory.
        iv. Open DS (Producto Open Source, basado en los estándares LDAPv3 y DSMLv2 (Directory Service Markup Language). OpenDJ (a partir de 2010).
        v. Open AM Sistema de gestión de accesos opensource. Soportado por la Open Identity Platform Community.
        vi. Open LDAP 2.4.47 (liberada bajo su propia licencia OpenLDAP Public License).

2. **Metadirectorio:**
    a. Estructura formada por varios directorios con procesos de sincronización, conocidos como reglas de gobierno, establecidos en función de las fuentes de información.
    b. La mayoría de las implementaciones de metadirectorio sincronizan los datos en, al menos, un servidor basado en LDAP.
    c. Software metadirectorio:
        i. IBM Security Verify Directory Integrator (Anteriormente IBM Tivoli Directory Integrator).
        ii. GANYMEDE: licencia GNU General Public License.
        iii. Microsoft Identity Manager (MIM).
        iv. Oracle Identity Manager (OIM).
        v. OpenIAM: opensource.
        vi. Evolveum MidPoint: opensource.

3. **Provisión de usuarios:**
    a. Su funcionalidad es similar al metadirectorio, con mayor capacidad para la definición de las reglas de trabajo.
    b. Dentro de sus características destacan:
        i. Automatización de la propagación de cambios
        ii. Flujos de trabajo
        iii. Delegación

c. Ejemplos:
    i. Softerra Adaxes: basada en Microsoft Active Directory.
    ii. Prometheus Account Provisioning: basada en OpenLDAP y desarrollada Universidad de Edimburgo

1.1 Productos software para la gestión de identidades

1. ***IBM Security Identity and Access Manager*** (ISAM, Anteriormente IBM Tivoli identity and Access Manager). También conocido como TIM, ITIM, o ISIM, es una plataforma IAM que ofrece soluciones para la gestión de identidad y acceso, autenticación multifactor y control de acceso basado en roles. La plataforma también cuenta con herramientas de análisis de riesgos y monitoreo de actividades para ayudar a las organizaciones a detectar y mitigar posibles amenazas. Permite:
    a. Gestión ciclo de vida de la identidad
    b. La federación de identidades, la autenticación de usuarios y compartir información de atributos de confianza entre aplicaciones de servicios Web
    c. Definición de políticas de seguridad a través de múltiples aplicaciones y usuarios
2. NETIQ Advanced Authentication (anteriormente Novell Identity Manager).

1.2 Federación de Identidades

Se denomina **Federación de Identidades** al conjunto de tecnologías, normas y casos de uso que sirven para intercambiar información sobre la identidad de usuarios en diferentes dominios de seguridad.

Los componentes principales son:

1. Proveedor de Identidad (Identity Provider, IdP): autenticación de usuarios.
2. Proveedor de Servicios (Service Provider, SP): acceso del usuario a un recurso o aplicación.
3. Círculo de Confianza (Circle of Trust): entidades (compañías, departamentos, admones. públicas, etc.) que han firmado un acuerdo para suministrar una serie de servicios a sus usuarios comunes, según una relación de confianza entre ellos, es decir, es un entorno de seguridad multi-dominio donde se pueden compartir servicios a unos usuarios.

Para ofrecer federación de identidades es necesario que se establezca el círculo de confianza (dominios de seguridad que confían los unos en los otros) junto con los correspondientes acuerdos de servicio.

Dentro de un dominio sólo habrá un Proveedor de Identidad y puede haber diversos Proveedores de Servicio SP.

Círculo de confianza, pueden coexistir varios proveedores de servicios, así como varios proveedores de identidad.

1.2.1 Tecnologías para la Federación de Identidades

1. **SAML 2.0**
    a. Es un estándar abierto basado en XML desarrollado por el SSTC (Security Services Technical Committee) de OASIS (Organization for the Advancement of Structured Information Standards).
    b. Define la infraestructura de intercambio de credenciales (autenticación y autorización) entre distintos dominios de seguridad.
    c. **Tiene 4 elementos principales:** Assertions, Protocols, Bindings y Profiles. (solo esto y definición o significado, resto NO)

i. Assertions: paquetes XML contienen información de identidad, autenticación y autorización sobre un usuario.
ii. Protocols: Definen las peticiones de las Assertions y las respuestas de estas. Propio esquema XML.
iii. Bindings: Especifican uso mensajes SAML con protocolos de más bajo nivel, como HTTP o SOAP.
iv. Profiles: Combinan protocolos, bindings y assertions. Un perfil es el conjunto de elementos e interacciones entre ellos que son necesarios para satisfacer un caso concreto de utilización de SAML.
1. Tipos de perfiles (profiles):
a. Web Browser SSO Profile.
b. Assertion Query/Request Profile
c. Artifact Resolution Profile.
d. Identity Provider Discovery Profile

d. La Seguridad en SAML: Se integra con XML Encryption y XML Signature para proveer autenticación.
e. Implementaciones de SAML:
i. OpenSAML: librerías open source programadas en C++ y Java. Ej. SAML se usa si por ejemplo se usa Google o Facebook como sistema de autenticarse en cualquier otra web.
ii. Identity provider y service provider no se comunican entre si directamente.

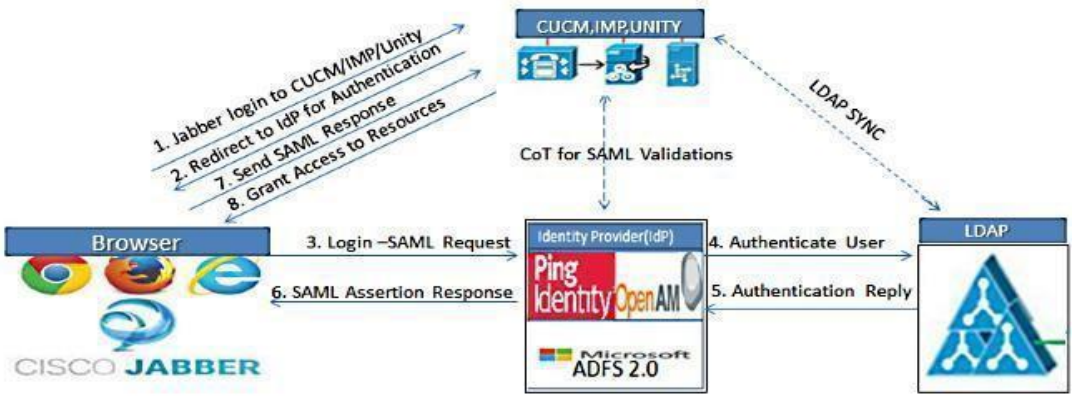

Figure :SAML Single sign SSO Call Flow for Collaboration Servers

2. **WS-*** and Windows CardSpace (ya no se usa)
3. **Facebook Connect** (también log in with Facebook)
a. Facebook Connect es una funcionalidad que permite usar, en otras páginas de Internet, la identidad de Facebook.
b. El sistema de Facebook Connect no sólo permite identificación, sino que integra información del perfil y la red de contactos del usuario en la página habilitada con Facebook Connect.
4. **OPENID**
a. OpenID es un estándar de identificación digital descentralizado.
b. A diferencia de otras arquitecturas SSO, OpenId no especifica el mecanismo de autenticación.

5. **OAUTH** (Open Authorization) – Solo Autorización
    a. Es un protocolo abierto, propuesto por Blaine Cook y Chris Messina, que permite autorización segura de una API de modo estándar y simple para aplicaciones de escritorio, móviles y web.
    b. Nace cuando se desarrollaba la implementación de OpenID para Twitter.
    c. OAuth es estándar abierto y se diferencia de OpenId y SAML en que se usa únicamente para autorización y no para autenticación puesto que en este caso el proveedor de autorización es un tercero como puede ser el sistema de autenticación de Twitter o Facebook.
    d. Este protocolo se usa de manera muy frecuente para proveer SSO a aplicaciones móviles donde los dos anteriores tienen más carencias.
    e. Última versión: OAuth 2.0. No es compatible con OAuth 1.0.
    f. Uso de OAUTH:
        i. La API Graph es la principal herramienta para que las aplicaciones puedan realizar tareas de lectura y escritura en la gráfica social de Facebook.
        ii. La API Graph de Facebook sólo admite OAuth 2.0. Google admite OAuth 2.0 como el mecanismo de autorización recomendado para todas sus API. Microsoft también admite OAuth.

6. **OpenID Connect (OIDC)**
    a. Es el protocolo de autenticación implementado utilizando el framework de autorización OAuth 2.0. El estándar controlado por OpenID Foundation.
    b. OpenID Connect es una capa de identidad sobre el protocolo OAuth 2.0
7. **Otras tecnologías** de gestión de la identidad
    a. OATH (Open Authentication), Liberty Alliance, Kantara IAF (Identity Assurance Framework), Passport (Framework de autenticación para Node.js).

2. Single Sign-On (SSO)

El inicio de sesión único (SSO) es una solución de autenticación que permite al usuario autenticarse una vez y poder acceder a varios sistemas sin la necesidad de volver a autenticarse.

Como beneficios de su uso destacan:

1. Un rápido acceso a los datos.
2. Una mejor experiencia del usuario (usabilidad) pues no necesita aprenderse listas de passwords
3. Mejor seguridad, al no tener tanto riesgo de fatiga de passwords o uso del mismo para todas las aplicaciones.
4. Facilidad de trabajo al desarrollar nuevos servicios.

URLs para ampliar o aclara conceptos:

How Does Single Sign-On (SSO) Work? | OneLogin

The Top 11 Single Sign-On Solutions For Business | Expert Insights

2.1 Configuraciones SSO en un Dominio

Se diferencia entre los sistemas de SSO que actúan dentro de un dominio frente a aquellas configuraciones SSO que afectan a varios dominios de seguridad (realms).

1. **Kerberos**
    a. Protocolo de autenticación, desarrollado por el MIT.
    b. Autenticación (de máquinas) de redes de ordenadores que permite a dos computadores en una red insegura demostrar su identidad mutuamente y de manera segura.
    c. Funcionamiento del protocolo Kerberos
        i. Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza. Kerberos usa un tercero de confianza, denominado "centro de distribución de claves" (KDC: Key Distribution Center), el cual consta de dos partes lógicas separadas: un "servidor de autenticación" (AS o Authentication Server) y un "servidor emisor de tiquets" (TGS o Ticket Granting Server). Kerberos trabaja sobre la base de "tiquets", los cuales sirven para demostrar la identidad de los usuarios.
        ii. Para una comunicación entre dos entidades, Kerberos genera una clave de sesión, la cual pueden usar para asegurar sus interacciones.
    d. SSO basado en Kerberos
        i. Una vez ha mostrado el usuario sus credenciales, obtiene un “ticket emisor de tiquets” (TGT o Ticket Granting Ticket) del TGS. Otras aplicaciones del usuario que requieren autenticación (por ejemplo clientes de correo, wikis, sistemas de control de revisiones, etc.) usan el TGT para adquirir “tiquets de servicios” (TS o Tickets Services), que acreditan la identidad del usuario para dichas aplicaciones.
        ii. En el SSO basado en Kerberos, el usuario (cliente) tiene un programa cliente en su ordenador que se ocupa de guardar los tiquets y solicitarlos cuando el cliente vaya a acceder a un determinado servicio.

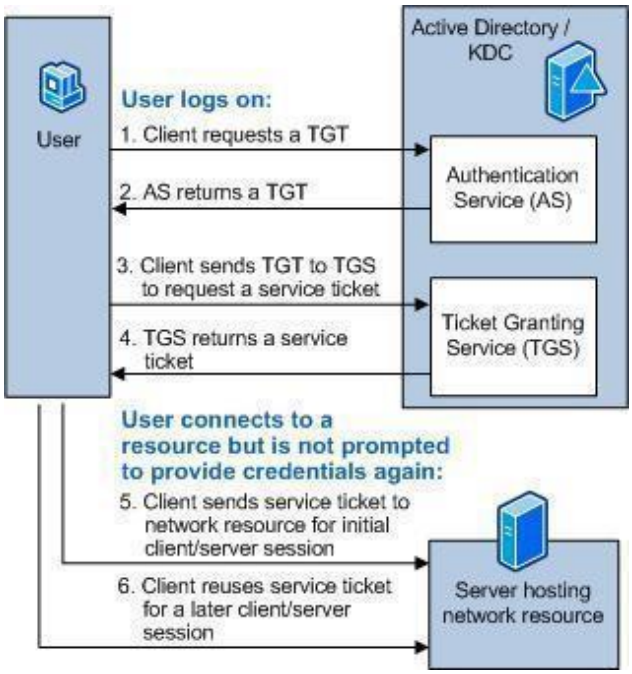

Imagen: Ejemplo de SSO basado en Kerberos con Windows

e. El proceso de Kerberos con funcionalidad SSO es la siguiente:
   i. El cliente se autentica y en el proceso de autenticación, el cliente solicita un Ticket Emisor de tiquets (TGT).
   ii. El servicio de Autenticación, al comprobar que está autenticado, le proporciona un TGT al usuario.
   iii. El software cliente del usuario utiliza su TGT para conseguir un tiquet válido para un servicio (por ejemplo, correo).
   iv. El servidor de autenticación le devuelve su tiquet válido para acceder al correo.
   v. El cliente solicita acceso al servidor de correo, enviando su TGS del correo.

2. SSO Corporativos

a. IBM Security Access Manager for Enterprise SSO (anteriormente IBM Tivoli Access Manager Enterprise SSO).
b. NetIQ Secure login (anteriormente Novell Secure Login).

3. Cookies: caso de Web SSO

a. SSO dentro de aplicaciones Web que se presentan al usuario a través de un navegador. Las aplicaciones web se encuentran dentro de un dominio de seguridad.
b. El intercambio de cookies (atributo secure, obligando a que se use https). Las peticiones del cliente son http o https y se realizan desde un navegador. El proceso que tiene lugar es el siguiente:
   i. Initial request: El navegador intenta acceder a una página foo.example.com a través de una petición http.
   ii. Redir to login Server: El servidor web foo.example.com comprueba que dicho usuario no está autenticado, por lo que solicita un http redirect para redirigir al usuario al servicio de autenticación.
   iii. Login request: El servicio de autenticación solicita al usuario que presente sus credenciales y el usuario se autentifica.
   iv. Redirect to web Server + cookie: Una vez autenticado, el servidor de autenticación le envía una petición HTTP redirect y le añade una cookie de sesión.
   v. Request + cookie: El navegador del usuario presenta una petición http y lleva incrustada la cookie de sesión.
   vi. Response: El servidor foo.example.com comprueba que la cookie de sesión es válida y no ha expirado, por lo que presenta su información al usuario.

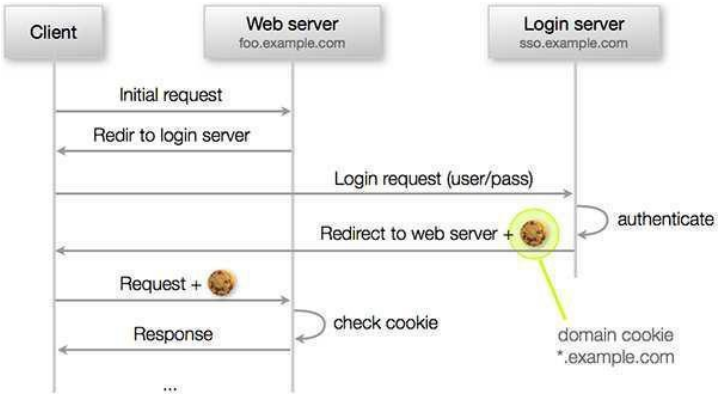

Imagen: Web SSO dentro de un dominio

c. Ataques de seguridad en Web SSO basados en cookies:
    i. Las cookies poseen ciertas vulnerabilidades y pueden sufrir ataques maliciosos por parte de terceros.
    ii. Robo de cookies:
        1. La vulnerabilidad de robo de cookies ha existido siempre. Se ha vuelto a hablar de ello al haber salido a la luz un plugin de Firefox, denominado Firesheep que permite en redes abiertas (WIFI) capturar la sesión de otros usuarios en páginas como Facebook, Yahoo!, Twitter, Linkedin...etc.
        2. El problema estaba en que estas webs sólo utilizaban https para autenticar a los usuarios, pero las cookies de sesión se intercambiaban por http.

2.2 Configuraciones SSO Multi-Dominio

El acceso a las aplicaciones y a la información en Internet requiere que el usuario pueda acceder a múltiples dominios y establecer SSO entre aplicaciones de diferentes dominios.

Para poder explicar SSO multi-dominio se usa la federación de identidades, tal y como se ha explicado en el apartado anterior.

3. Gestión de Identidades en las AAPP

3.1 AutenticA

PAe - CTT - General - AutenticA: El repositorio horizontal de usuarios de las Administraciones Publicas

AutenticA, basado en SAML, ofrece servicios de Autenticación, SSO y Autorización, de empleados públicos de las AA.PP. y usuarios relacionados, en el acceso a aplicaciones internas de las AA.PP.

AutenticA dispone de un repositorio horizontal de usuarios provenientes de fuentes primarias de calidad o con altas de una estructura de administradores delegados corresponsables. El servicio provee atributos de los usuarios autenticados (unidad y el puesto de destino; correo electrónico y teléfono).

La funcionalidad de autorización de usuarios es opcional por aplicación y permite gestionar los roles determinados que puede asumir un usuario en el acceso a dicha aplicación.

Admite medios de autenticación basados en certificados digitales, así como en usuario – contraseña. Está integrado con Cl@ve para aceptar también claves concertadas.

AutenticA se encuentra integrado con el Directorio Común de Unidades Orgánicas y Oficinas - DIR3.

En el caso de que AutenticA valide correctamente el usuario, redireccionará el flujo de la información a la URL de respuesta que se informa en la configuración de la aplicación.

En este momento es cuando será posible por parte de la aplicación recuperar la información que se encuentra en el LDAP de AutenticA del usuario que se validó, recogiendo el parámetro “AUTENTICA_USER_XML”

CAS (Central Authentication Service) es el protocolo que permite implementar SSO.

Cuando un usuario se conecta a una de estas aplicaciones el sistema comprueba si está autenticado y, si no lo está, lo redirige a la pantalla del servidor de autenticación. Si la autenticación es correcta el sistema de autenticación, en este caso CAS, vuelve a redirigir al usuario a la página a la que quería acceder en un primer momento.

Las aplicaciones preguntan si el usuario ya está registrado, que es tan sencillo como preguntar a la request de esta forma: request.getRemoteUser()

3.2 Cl@ve

https://administracionelectronica.gob.es/ctt/clave

Es el sistema de autenticación de ciudadanos para el acceso a los servicios públicos (Sedes electrónicas).

Los pasos de la interacción son los siguientes:

1. El ciudadano accede a un servicio de administración electrónica integrado con Cl@ve que requiere que se identifique.
2. El ciudadano es redirigido a Cl@ve, que le presenta una pantalla en la que debe seleccionar el método de identificación que quiere utilizar. Las opciones activas en la pantalla vienen condicionadas por los parámetros que el SP ha indicado en el mensaje que ha enviado a Cl@ve relativos a los IdP y niveles QAA permitidos.
3. El ciudadano selecciona el método de identificación y es redirigido al IdP correspondiente.
4. El ciudadano se autentica en el IdP seleccionado y es redirigido de nuevo a Cl@ve
5. De forma transparente, sin que sea necesario interacción, el ciudadano es redirigido de nuevo al SP.

La pasarela cuenta con un sistema de SSO para que el usuario no tenga que re-autenticarse continuamente si va a realizar varias peticiones en un breve lapso. La sesión dura 1 hora.

Fuerza al usuario a autenticarse mandando atributo “forceAuthN” con el valor “true” en la SAMLRequest que se le envía a la pasarela.

3.3 Nodo eIDAS

https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Identidad_y_firmaelectronica/Nodo-eIDAS.html

En septiembre de 2018 comenzó la obligación de reconocimiento mutuo de identidades electrónicas transfronterizas de acuerdo con el Reglamento eIDAS. Por lo cual, todos los servicios públicos deben poder ofrecer la posibilidad de identificarse con medios de identidad electrónicos de otros países, siempre que éstos hayan sido notificados a la Comisión Europea.

Para ello se ha creado un sistema europeo de reconocimiento de identidades electrónicas basado en un conjunto de nodos de interoperabilidad (nodos eIDAS) que conectan las infraestructuras nacionales de identificación electrónica entre sí.

En concreto, el nodo eIDAS (basado en SAML 2.0) español permite la aceptación del DNI electrónico en servicios de Administración Electrónica de otras administraciones europeas, así como la identificación de ciudadanos europeos en servicios públicos españoles utilizando un medio de identificación de su país de origen.

Para las Administraciones Públicas, la integración con el nodo eIDAS español se realizará a través del sistema Cl@ve. La nueva versión de Cl@ve 2.0 sustituirá la conexión de STORK por el nodo eIDAS.

3.4 eIDAS2, EUid y European Identity Wallet

El 30 de abril de 2024 se publicó en el Diario Oficial de la Unión Europea el **Reglamento (UE) 2024/1183 (eIDAS2)** por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del **marco europeo de identidad digital.** Entró en vigor el 20 de mayo de 2024.

Según el Reglamento, los Estados miembros de la UE deben proporcionar a los ciudadanos Carteras de Identidad Digital de la UE hasta 24 meses después de la adopción de Actos de Ejecución, en los que se establezcan las especificaciones técnicas y la certificación de las mismas.

*Para más información del **eIDAS2**, consultar los temas 80 y 81.*

Para más información: https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation

El 4 de diciembre de 2024, se publicaron los 5 actos de implementación correspondientes al primer lote, entrando en vigor a los 20 días de su publicación:

- Reglamento de Ejecución (UE) 2024/2979 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la **integridad y las funcionalidades básicas de las carteras de identidad digital europea**.
- Reglamento de Ejecución (UE) 2024/2977 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los **datos de identificación de la persona y las declaraciones electrónicas de atributos** expedidos a **carteras de identidad digital europea**.
- Reglamento de Ejecución (UE) 2024/2980 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las **notificaciones a la Comisión relativas al ecosistema de la cartera de identidad digital europea**.
- Reglamento de Ejecución (UE) 2024/2982 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los **protocolos y las interfaces que admitirá el marco europeo de identidad digital**.
- Reglamento de Ejecución (UE) 2024/2981 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la **certificación de las carteras de identidad digital europea**.

3.4.1 Cartera Digital Europea

Definida en el artículo 3.42. del **Reglamento (UE) 2024/1183:**

*42) **"cartera europea de identidad digital",** medio de identificación electrónica que permite al usuario almacenar, gestionar y validar de forma segura datos de identificación de la persona y declaraciones electrónicas de atributos con el fin de proporcionarlos a las partes usuarias y a otros usuarios de carteras europeas de identidad digital, así como firmar por medio de firmas electrónicas cualificadas o sellar por medio de sellos electrónicos cualificados;*

La **Cartera de Identidad Digital de la UE** se ha diseñado como un método cómodo y seguro para que los ciudadanos y las empresas europeas autentifiquen su identidad, utilizando su DNI digital para interactuar tanto en el sector público como en el privado. Los usuarios pueden almacenar en la cartera diversos documentos digitales, desde credenciales académicas a abonos de transporte, y utilizarlo para iniciar sesión en plataformas privadas, como las redes sociales. Este método es más seguro y fácil de usar que la gestión de numerosas contraseñas.

Antes de su despliegue en los Estados miembros, la cartera de identidad digital de la UE se está probando en cuatro proyectos a gran escala que se lanzaron el 1 de abril de 2023. El objetivo de estos proyectos es poner a prueba las carteras de identidad digital en situaciones reales que abarquen diferentes sectores. En ellos participan más de 250 empresas privadas y autoridades públicas en veinticinco Estados miembros, Noruega, Islandia y Ucrania.

La Comisión Europea facilitará asimismo un prototipo de cartera de identidad digital de la UE (EUDI), tal como se especifica en la propuesta de Reglamento sobre la Identidad Digital Europea.

Las principales funcionalidades ofrecidas por la Cartera Digital Europea son las siguientes:

- Autenticación. Acceso a servicios online tanto públicos como privados sin necesidad de gestionar contraseñas.
- Almacenamiento de documentos digitales.
- Compartición de documentos digitales y credenciales.
- Firma electrónica de documentos.

Para más información:

https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

4. Teletrabajo

4.1 Marco Normativo

El Consejo de Ministros, en 2005, aprobó el Plan Concilia que recoge una serie de medidas para hacer posible la conciliación en el ámbito público.

ORDEN APU/1981/2006, de 21 de junio, por la que se promueve la implantación de programas piloto de teletrabajo en los departamentos ministeriales. (APU: Ministerio de Administraciones públicas)

Ley 10/2021, de 9 de julio, de trabajo a distancia. BOE-A-2021-11472 Ley 10/2021, de 9 de julio, de trabajo a distancia. Esta ley deroga el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.

Se recomiendan los siguientes enlaces para tener información resumida del contenido de la ley:

Ley de Teletrabajo en España: todo sobre la regulación del trabajo a distancia

La nueva Ley del teletrabajo y trabajo a distancia: qué es y puntos principales

Algunos conceptos y definiciones:

- **Teletrabajo:** es aquél que se realiza "mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación."
- **Trabajo a distancia:** es aquel trabajo que "se presta en el domicilio de la persona trabajadora o en el lugar libremente elegido por esta, durante toda su jornada o parte de ella, de modo no ocasional". Es interesante destacar que de acuerdo con esta definición es la regularidad (no la intensidad) la que caracteriza el trabajo a distancia.
- **Trabajo presencial:** sería el que "se presta en el centro de trabajo o en el lugar determinado por la empresa."

La ley marca la regularidad del Trabajo a Distancia mediante este criterio: si se presta en un periodo de tres meses; como mínimo durante el 30% de la jornada laboral o bien proporcionalmente a la duración del contrato de trabajo.

4.2 Tecnologías relacionadas con el Teletrabajo

4.2.1 Desktop sharing

El acceso remoto permite a los usuarios conectarse a su propio escritorio mientras están físicamente lejos de su ordenador. Los sistemas que soportan el X Window System, típicamente los basados en Unix, tienen esta capacidad incorporada. Las versiones de Windows cuentan con una solución incorporada para el acceso remoto bajo la forma de Remote Desktop Protocol.

Algunos productos relacionados con esta tecnología:

1. El producto Virtual Network Computing (VNC), de fuente abierta, proporciona la solución multiplataforma-plataforma para la conexión remota.
2. DameWare Mini Remote Control: Herramienta comercial con licencia propietaria.
3. Vinagre, TightVNC, RdesKtop herramientas de código abierto.
4. Microsoft Teams

4.2.2 VDI Virtual Desktop infrastructure

Término acuñado por VMware. Hospeda un sistema operativo para ordenadores de escritorio en una máquina virtual (VM) que opera desde un servidor centralizado.

En los últimos años, algunas organizaciones de gran tamaño han empezado a utilizar VDI como alternativa al modelo de computación basado en servidores usado por Citrix y Microsoft Terminal Services.

Alternativas VDI:

- VMWare Horizon
- Citrix Virtual APPs y Desktops
- VDI Solutions: Comparing Top 6 Solutions

4.2.3 VPN

Una red privada virtual se basa en un protocolo denominado protocolo de túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.

Implementaciones: El protocolo estándar de facto es IPSEC para implementar una red privada virtual. Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS.

- IPsec VPN
  - IPsec (abreviatura de Internet Protocol security), protocolos capa de red, cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.
  - IPsec puede utilizarse para crear VPNs en los dos modos (transporte o extremo a extremo; túnel a varias máquinas).
- Open VPN -Licencia GPL
  - OpenVPN es una solución multiplataforma (entorno Windows, mac, linux...) de conectividad basada en software SSL (Secure Sockets Layer) para ofrecer redes privadas virtuales.
  - OpenVPN es una excelente solución para VPNs que implementan conexiones de capa 2 o 3, y usa los estándares de la industria SSL/TLS para cifrar.
  - El mayor inconveniente es que no posee interoperabilidad con IPsec VPN.


preparatic
¿Tienes alguna sugerencia de mejora?
Háznoslo saber escaneando el código o haz clic en la imagen