plan de innovación pública
berrikuntza publikoaren plana

EUSKO JAURLARITZA
GOBIERNO VASCO

“Recomendaciones sobre el uso de los sistemas de autenticación en los servicios electrónicos de la Administración pública vasca”

INFORME

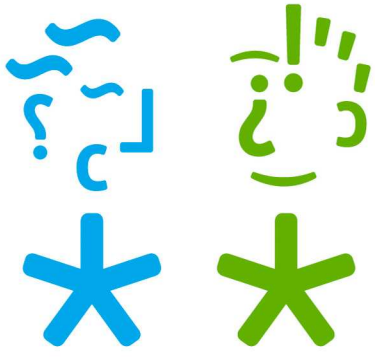
Autor: Equipo de Innovación - Sistemas de Autenticación e Identificación

Fecha de creación: Vitoria-Gasteiz, 21/12/2010

Fecha de revisión: 25/01/2011

Versión del documento: 01

Fichero: PIP-Grupo de Innovacion _Autenticacion _informe.doc



Índice de contenido

1. Introducción

La Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP) establece como un derecho de la ciudadanía la posibilidad de comunicarse con la Administración Pública mediante medios electrónicos. Se trata de una novedad verdaderamente importante, puesto que se convierte en **derecho** lo que hasta ese momento era solo una opción cuya puesta en funcionamiento quedaba fundamentalmente en manos de la Administración, y no de la ciudadanía. La institución de este derecho implica, por tanto, para la Administración, una obligación: la de dotarse de instrumentos que permitan la creación de una *"ventanilla electrónica"* a través de la cual cualquier persona se pueda comunicar con la administración cuando ella lo decida y desde donde ella quiera.

En este proceso de adaptación progresiva se incluye la necesidad de utilizar medios de identificación y autenticación que sean seguros, tanto para la Administración como para la ciudadanía.

Cuando se habla de medios de identificación y autenticación seguros habitualmente se habla de certificados digitales[1]; en este aspecto, España destaca sobre la media europea en número de DNI´s electrónicos emitidos, ya que actualmente supera los 10 millones de documentos. Sin embargo, el número de ciudadanos que lo usan es, según las últimas estadísticas, es bastante reducido. Los motivos de esta escasa utilización parecen ser:

- La poca familiaridad de los ciudadanos con su uso
- Los problemas en su utilización (problemas a la hora de instalar los lectores y el software necesario para su utilización, drivers, compatibilidad de navegadores, etc.).

2}

Según datos del INE del 2010 el uso de otros certificados de firma electrónica reconocidos es considerablemente superior al de DNI electrónico, así en Euskadi aunque el 29,7 % de la población dispone de DNI electrónico solo el 3,4% lo usa para realizar tramitaciones por internet con la Administración Pública, sin embargo el uso de otros certificados electrónicos reconocidos se eleva hasta el 11,4%. Con esto se puede concluir que las campañas de difusión, formación, asistencia en el uso y la calidad de los servicios prestados por los prestadores de servicios de certificación influyen directamente en el uso de los certificados electrónicos por parte de los ciudadanos.

Dentro de los servicios públicos digitales, en la actualidad, los titulares del DNI electrónico pueden realizar más de 1.000 actuaciones electrónicas con la Administración. Sin embargo, España, salvo en la gestión de tributos, se encuentra por detrás de muchos otros países en uso de la eAdministración por parte de la sociedad, lo que se debe a:

1. El retraso generalizado en el **uso de las TIC´s** de los usuarios
2. La **complejidad** de algunos de los procedimientos electrónicos creados (se impone un rediseño de algunos de los flujos o de la normativa que aplica a cada procedimiento, que en su momento nació sin tener en cuenta la existencia de una vía telemática).
3. La **escasa difusión** que realizan las administraciones sobre los procedimientos disponibles de forma telemática.
4. La **escasa disponibilidad** en numerosas administraciones regionales y locales.

[1] Un certificado digital es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula la identidad de cada usuario con las herramientas de firma electrónica (claves criptográficas), dándole a conocer como firmante en el ámbito telemático

En relación a la utilización de la firma electrónica, la mencionada Ley 11/2007 recoge el uso del DNI electrónico para la tramitación con la Administración. Para que los ciudadanos soliciten y obtengan el Certificado Digital es preciso que lo hagan a un Prestador de Servicios de Certificación Electrónica. En el ámbito de la CAPV destacamos la extensión de distintos tipos de tarjetas de persona física con certificado electrónico, como son la tarjeta ONA, y tarjeta de ciudadano, que permiten la relación con las administraciones públicas vascas y otros organismos a nivel estatal, en un extenso número de trámites on line.

También es necesario señalar que en el ámbito empresarial, tanto pequeña como mediana y gran empresa, la firma electrónica reconocida está implantada en un alto grado, existiendo numerosos proyectos donde la firma electrónica reconocida se ha utilizado como sistema de autenticación con éxito, como por ejemplo, Proyecto IKS de Medio ambiente del Gobierno Vasco, presentación de impuestos con las tres diputaciones vascas, solicitud de ayudas para SPRI, etc.

2. Descripción del reto

En el contexto descrito anteriormente, el Plan de Innovación Pública (PIP), impulsado por la Viceconsejería de Administración Pública del Gobierno Vasco, ha puesto en marcha un proyecto para facilitar el acceso a los servicios de la e-administración, para lo cual se pretenden **buscar sistemas de identificación y autenticación *"amigables"* para el usuario final** que, sin poner en peligro la relación entre usuario y Administración, facilite a la ciudadanía el uso de esos servicios electrónicos.

Así pues, el reto consiste en proponer **sistemas de identificación y autenticación complementarios a la firma electrónica** que cumplan los siguientes requisitos:

- Que sean **fáciles de usar** por parte de una persona sin que obligatoriamente tenga que tener grandes conocimientos relacionados con las TIC´s (Tecnologías de la Información y Comunicación).
- Que **se puedan implantar en el corto plazo**.
- Que **ofrezcan garantías** (de autenticidad, protección de datos, etc.) en proporción a las características y riesgos de cada servicio.

Sistemas de autenticación fáciles de usar, implantables en el corto plazo y que ofrezcan garantías

4}

3. Identificación / Autenticación

Cuando se habla de sistemas de identificación y autenticación es necesario definir previamente qué se entiende por sistema de identificación y autenticación/autorización:
Se entiende por **mecanismo de identificación** aquel del que se obtiene la **identidad** de una persona y datos relacionados con la misma (ej. nombre, dirección, teléfono, etc.) para ser utilizados en un servicio on-line.
Es importante distinguir entre identificación y autenticación-autorización:

- **Identificar.** Se puede definir como reconocer si una persona o cosa es la misma que se supone o se busca. (diccionario RAE)
- **Autenticar** podemos plantear dos definiciones:
  1. Es la acreditación por medios electrónicos de la identidad de una persona o ente, del contenido y voluntad expresa en sus operaciones, transacciones y documentos, y de la integridad y autoría de aquellos.
  2. Procedimiento de comprobación de la identidad de un usuario. Mediante el mismo se garantiza que el usuario que accede a un sistema de ordenador es quién dice ser. (diccionario jurídico Aranzadi).

Ejemplos de servicios on-line que necesitan identificar al tercero que interactúa con el servicio:

BLOG	Cuando un usuario hace un comentario en un BLOG, habitualmente se identifica para que quede constancia de quién es ese usuario que hace el comentario (esto no es óbice para que también se puedan permitir comentarios anónimos). Las herramientas para la identificación solo están en manos del usuario que las crea. En muchos casos no coincide con sus datos personales.
Algunos casos de solicitud en una tramitación	En algunos casos las solicitudes no requieren autenticación (pueden ser servicios on-line "libres" o abiertos), sin embargo, si que es necesario aportar datos de la identidad del solicitante. En otros casos se requerirá la firma electrónica reconocida.
Algunos casos de Consulta de expedientes o carpeta personales	Cuando se trata de acceder a datos (Ej.: expediente, carpeta personal, etc.), es imprescindible identificar y además autenticar. Una vez identificado el tercero que quiere utilizar el servicio on-line hay que: • **Identificarle** y **Autenticarle** en el servicio-online: dar acceso al usuario utilizando la identidad aportada. • **Comprobar si está autorizado** para consultar los datos a los que quiere acceder. En otros casos se requerirá la firma electrónica reconocida.

Como **mecanismos de identificación**:

- El DNI electrónico o la tarjeta ONA y la tarjeta ciudadano son mucho más que mecanismos de identificación ya que "aportan" a un servicio on-line además de información sobre la identidad de una persona (nombre, dni, etc.), la posibilidad de realizar firma electrónica reconocida.
- Una cuenta de una red social (Ej.: twitter, Facebook) también pueden ser utilizados como mecanismos para "aportar" datos de identidad, aunque obviamente estos datos son mucho menos fiables.

Mecanismos de identificación como el DNI electrónico, la tarjeta ONA y la tarjeta ciudadano que además de identificar, proporcionan otras funcionalidades:

- **Firmar electrónicamente,** al realizarlo con un certificado de firma electrónica reconocido, equivaldrá a la firma manuscrita.
- **Garantizar la autoría y no repudio** de documentos o acciones en servicios on-line
- **Otros relacionados con la firma:** sellados de tiempo.

En definitiva:

- Un mecanismo de **identificación** permite **conocer la identidad** y datos asociados a esta del usuario que interacciona con un servicio on-line.

A través del certificado reconocido de firma electrónica a se garantiza por un Prestador de Servicios de Certificación Electrónica la autenticidad, confidencialidad, integridad y no repudio.

- La **identidad** puede ser utilizada para **autenticar y posibilitar** al usuario en el servicio on-line y discriminar qué puede ver y qué puede hacer en el servicio.
    - En el escenario más sencillo (y más habitual), una vez identificado de un usuario, se le autentica en el servicio on-line y accediendo a sus datos.

6}

4. Análisis de algunos mecanismos de identificación

En el presente punto se analizan algunos mecanismos de identificación teniendo en cuenta:

Características de seguridad	• ¿Cómo de seguro es el sistema en cuanto a la custodia de claves? • ¿Es posible que alguien pueda suplantar a otra persona fácilmente?
Características de confiabilidad	• ¿Cómo de confiables son los datos de identidad?, ¿se puede "fiar" la administración de que quién se está identificando es quien dice ser?¿Qué papel desempeñan los Prestadores de Servicios de Certificación Electrónica como terceros que "dan fe" en el ámbito telemático o electrónico?
Retos del Despliegue	¿Cómo de fácil es el despliegue en la ciudadanía de estos mecanismos de autenticación?
Posibles utilizaciones (otros propósitos)	Los sistemas o mecanismos de identificación se pueden utilizar para diferentes propósitos: **Identificación** — Obtener datos de la identidad de la persona: nombre, apellidos, dirección, DNI, teléfono, otras direcciones de contacto, etc. **Autenticación** — Para permitir técnicamente el acceso o no acceso a aplicaciones y los datos que obran en las mismas del usuario. **Firma** — Para garantizar la autoría y no repudio de determinadas operaciones

{7

Los mecanismos de identificación analizados son los siguientes:

1	Usuario + contraseña
2	Usuario + Contraseña de identificación + contraseña de firma (OTP [2] enviada al teléfono móvil)
3	Usuario + Contraseña de identificación + Contraseña (OTP generada en un dispositivo hardware)
4	Firma electrónica avanzada (certificados software)
5	Firma electrónica reconocida (certificados en tarjeta criptográfica u otro dispositivo seguro de creación de firma)
6	Usuario + contraseña de identificación + contraseña de firma
7	Usuario + contraseña de identificación + juego de barcos

Además de estos mecanismos de identificación (casi se puede hablar de tecnologías), merece la pena estudiar otras "estrategias" de identificación delegada basadas en **convenios con otras entidades** que son las responsables de identificar al usuario –utilizando el mecanismo/tecnología que consideren oportuno- y de "pasar" la información de identificación a la Administración.

[2] **OTP** *One Time Password* – contraseña de un solo uso
La contraseña es generada por algún sistema, utilizada y descartada para usos posteriores, es decir, en la siguiente operación de identificación se genera una nueva contraseña.

Dentro de estas "estrategias" de identificación delegada se podrían nombrar como ejemplos paradigmáticos:

8	Identificación delegada a una entidad en la que se confía (Ej.: Entidad Financiera)
9	Identificación delegada a una entidad en la que NO se confía (Ej.: red social)

A continuación se analiza cada uno de estos mecanismos de identificación en función de los parámetros definidos anteriormente

4.1. Características de Seguridad

En este punto se analiza **cómo de seguro es un sistema de identificación como para evitar la suplantación de identidad**. Se hace una división entre mecanismos de identificación fuertes y débiles (más seguros / menos seguros) en función del número de factores de seguridad que poseen:

Factores	**El nivel de seguridad de un sistema de identificación depende del número de factores que intervienen** y que se clasifican en:	
	Algo que el usuario **es (**biometría**)**	Huella dactilar, patrón retiniano, reconocimiento de voz
	Algo que el usuario **tiene**	Tarjeta criptográfica, *token* OTP (*One time Password* o Clave de un único uso), teléfono móvil, tarjeta de proximidad, banda magnética, certificados en software
	Algo que el usuario **sabe**	Contraseña, frase, número de identificación personal, número PIN
Nivel	**Fuerte** (más seguro)	Se utilizan por lo menos dos de los tres factores citados arriba. De este modo, si uno de los factores se ve comprometido, todavía existe un segundo factor que garantiza la seguridad
	Débil (menos seguro)	Se utiliza solo uno de los factores de autenticación

El nivel de seguridad de un sistema depende del número de factores que intervienen

8}

4.2. Características de Confiabilidad

En este punto se analiza **cómo de confiable es un sistema de identificación como para dar por buenos los datos de la identidad**. Se hace una división entre mecanismos de identificación confiables y no confiables:

Confiables	Un mecanismo de identificación puede ser confiable si se pueden dar por buenos los datos del tercero que se identifica Ej.: Para emitir el DNI o la ONA alguien ha validado físicamente que el/la solicitante es quien dice ser
NO confiable	No se puede asegurar que la persona que se identifica y sus datos son buenos Ej.: Un sistema de usuario / password donde el usuario se auto-registra (o el usuario de una red social) NO es confiable ya que NO hay garantía de que la identidad corresponda a la persona que dice ser.

Es importante señalar que aunque un sistema de identificación tenga una **seguridad** débil (Ej.: usuario – password), los datos de la identificación pueden ser **confiables**

Ej.: La identidad de un usuario que se ha autenticado con el usuario/password de la tarjeta ciudadana de Vitoria-Gasteiz ¿es **confiable** en el caso de que previamente haya identificado al ciudadano?

Hay que distinguir entre seguridad y confiabilidad del mecanismo de identificación

4.3. Otras características analizadas

Requisitos previos	Tareas a realizar para implementar el sistema de autenticación
No repudio	Hace referencia a si el usuario negar la autoría de una operación (gestión) realizada de forma telemática. Posibles valores: • Sí: El sistema de autenticación garantiza el no repudio de la gestión realizada telemáticamente. • No: El sistema de autenticación NO garantiza el no repudio de la gestión realizada telemáticamente.
Firma manuscrita	Posibles valores: • Sí: La firma electrónica realizada con el sistema de autenticación equivale a la firma manuscrita. • No: La firma electrónica realizada con el sistema de autenticación NO tiene la validez de la firma manuscrita.
Válido en otras entidades	Posibles valores: • Sí: El sistema de autenticación es válido en distintas entidades. • No: El sistema de autenticación solo es válido en la entidad propietaria.
Problemas	• Problemas en la implementación y uso del sistema de autenticación
Ventajas	• Ventajas del sistema de autenticación

{9

4.4. Tabla de mecanismos de autenticación

A continuación se resume el análisis en base a los parámetros anteriores:

	SEGURIDAD			CONFIANZA	Retos del Despliegue	USOS	
Tipo de Identificación	**Factores**	**Nivel**	**Válido en otras entidades**	**La identidad es confiable**	**Requisitos previos**	**No repudio**	**Firma manuscrita**
Usuario + Contraseña	**1 factor** [algo que se sabe]	**Débil**	**NO** Salvo convenio expreso entre las dos partes.	**Normalmente NO** (depende de si se identifica presencialmente al usuario)	• Registro previo • Procedimiento de identificación y asignación de usuarios y contraseñas consistente.	**No**	**No**
Usuario + Contraseña de identificación + contraseña de firma (OTP enviada al teléfono móvil) (1) (1) Se dispone de un usuario, una contraseña de identificación y una contraseña de firma que se envía en el momento de la identificación / firma al teléfono móvil del usuario.	**2 factores** [algo que se sabe (usuario) + algo que se tiene (móvil)]	**Fuerte**	**NO**	**SI** Para facilitar el dispositivo OTP normalmente hay que identificar presencialmente al usuario	• Registro previo con identificación presencial. • Procedimiento de identificación y asignación de usuarios y contraseñas consistente. • El usuario debe contar con un móvil y aceptar que se le envíen las contraseñas. • Sistema de generación y envío de contraseñas OTP al móvil	**No**	**No**
Usuario + Contraseña de identificación + Contraseña (OTP generada en un dispositivo hardware) (2) (2) Se dispone de un usuario, una contraseña de identificación y una contraseña de firma que genera un dispositivo que tiene el usuario.	**2 factores** [algo que se sabe (usuario) + algo que se tiene (dispositivo OTP)]	**Fuerte**	**NO**		• Registro previo con identificación presencial. • Procedimiento de identificación y asignación de usuarios y contraseñas consistente. • Distribución a los usuarios el dispositivo de generación de contraseñas OTP.	**No**	**No**
Firma electrónica avanzada (certificados software)	**2 factores** [algo que se tiene + algo que se sabe]	**Avanzada** Asegura fehacientemente la identidad del usuario	**SI**	**SI**	• Obtención de un certificado reconocido	**Sí**	**No**
Firma electrónica reconocida (certificados en tarjeta criptográfica u otro dispositivo seguro de creación de firma)	**2 factores** [algo que se tiene + algo que se sabe]	**Avanzada** Asegura fehacientemente la identidad del usuario	**SI**	**SI**	• Obtención de un certificado reconocido	**Sí**	**Sí**
Usuario + contraseña de identificación + contraseña de firma	**1 factor** [algo que se sabe (usuario + contraseñas)]	**Débil**	**NO** Salvo convenio expreso entre las dos partes.	**SI** Normalmente antes de facilitar la contraseña de firma o el juego de barcos se identifica presencialmente al tercero	• Registro previo con identificación presencial. • Procedimiento de identificación y asignación de usuarios y contraseñas consistente.	**No**	**No**
Usuario + contraseña de identificación + juego de barcos (3)	**2 factores** [algo que se tiene (juego de barcos) + algo que se sabe (usuario + contraseña)]	**Fuerte**	**NO** salvo convenio expreso entre las dos partes		• Registro previo con identificación presencial. • Procedimiento de identificación y asignación de usuarios y contraseñas consistente.	**No**	**No**

A continuación se analizan las ventajas y posibles problemas de cada uno de los sistemas de identificación analizados:

Tipo de Identificación	Ventajas	problemas
Usuario + Contraseña	✓ Uso sencillo	• Olvido de contraseñas. • Necesidad de implementar un sistema de recuperación de contraseñas. • Suplantaciones de identidad, *phishing*. • No se pueden realizar trámites para los que haga falta firma manuscrita.
Usuario + Contraseña de identificación + Contraseña de firma (OTP enviada al teléfono móvil)	✓ Uso sencillo	• Olvido de contraseña de acceso. • Acceso en consulta a datos poco seguro. • En menor medida, pero también es vulnerable al *phishing*. • Necesidad de implementar un sistema de recuperación de contraseñas. • Necesidad de implementar un sistema OTP. • No se pueden realizar trámites para los que haga falta firma manuscrita.
Usuario + Contraseña de identificación + Contraseña de firma (OTP generada en un dispositivo hardware)	✓ Uso sencillo	• Olvido de contraseña de acceso. • Acceso en consulta a datos poco seguro. • En menor medida, pero también es vulnerable al *phishing*. • Necesidad de implementar un sistema de recuperación de contraseñas. • Necesidad de implementar un sistema OTP. • Necesidad de distribuir un dispositivo generador de claves OTP. • No se pueden realizar trámites para los que haga falta firma manuscrita.
Firma electrónica avanzada (certificados software)	✓ Emitidos por Prestadores de Certificación que actúan como terceros de confianza para las dos partes ✓ Sistema con reconocimiento universal en todos los ámbitos ✓ No es posible la falsificación de la firma ✓ Funcionalidades adicionales: Cifrado de datos, firma digital	• Necesidad de instalación de los certificados de la autoridad de certificación. • No se pueden realizar trámites para los que haga falta firma manuscrita.
Firma electrónica reconocida (certificados en tarjeta criptográfica u otro dispositivo seguro de creación de firma)	✓ Ventajas de los certificados en software. ✓ Equivale a la firma manuscrita ✓ Mayor nivel de seguridad al estar el certificado albergado en un dispositivo seguro de creación de firma ✓ Los soportes físicos están evolucionando (*token* USB, teléfono móvil, memorias SD) facilitando su uso	• Necesidad de instalación de los certificados de la autoridad de certificación. • Necesidad de instalación del lector de tarjetas. • Necesidad de instalación del software de acceso al chip de la tarjeta.
Usuario + contraseña de identificación + contraseña de firma	✓ Uso sencillo	• Olvido de contraseñas. • Suplantaciones de identidad. • No se pueden realizar trámites para los que haga falta firma manuscrita.
Usuario + contraseña de identificación + juego de barcos	✓ Uso sencillo	• Olvido de contraseña de acceso. • Acceso en consulta a datos poco seguro. • No se pueden realizar trámites para los que haga falta firma manuscrita.

4.5. Retos del Despliegue

El despliegue de un sistema de identificación plantea una serie de retos, entre otros:

Infraestructura que da soporte al sistema de autenticación	¿Cómo de costosa es la infraestructura que da soporte al sistema?
Dispositivos en el cliente que se identifica	¿Es necesario instalar algún tipo de hardware en el equipo cliente que utiliza el ciudadano? ¿Cómo se distribuyen estos dispositivos? ¿Es necesaria formación específica?
Verificación de identidades	¿Cómo se verifica la identidad de la persona? Ej.: Con la identificación presencial según los requerimientos de la ley de firma electrónica. • Sistema de usuario / password donde el propio usuario se da de alta (dejar en manos del usuario todo el proceso) En principio si la identificación que requiere un acto presencial sería más costosa, pero partimos del alto número de identificaciones ya realizadas, por lo que por otra parte estaría ya realizada en parte. En el segundo caso habría que estar al coste de las aplicaciones y sería la menos segura.
Funcionalidades del mecanismo de autenticación	¿Qué actuaciones de índole jurídico permite el sistema desplegado? ¿Permite la identificación, autenticación y firma equivalente a la firma manuscrita?

12}

5. Tipos de servicios y nivel de identificación requeridos

1. Aspectos Jurídicos

Puede resultarnos esclarecedor, desde un punto de vista jurídico, lo establecido en la Ley 30/2007 de contratos del sector público (en adelante LCSP). En su disposición adicional decimonovena regula en empleo de los medios electrónicos, informáticos y telemáticos y establece que éstos se ajustarán entre otras a la siguiente norma:

- (*en el apartado f*) Todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas (es decir, tanto Administración, como empresarios-personas jurídicas- o personas físicas) que tengan **efectos jurídicos** y se emitan tanto en fase preparatoria como en las fases de licitación, adjudicación y ejecución del contrato **deben de ser autenticados mediante una firma electrónica reconocida**, de acuerdo a la Ley 59/2033, de 19 de diciembre, de firma electrónica. Los medios electrónicos, informáticos y telemáticos empleados deben poder garantizar que la firma se ajusta a las disposiciones de esta norma.

Si tenemos en cuenta, por lo tanto, las disposiciones de la Ley de Firma Electrónica, respecto de la firma reconocida, en su artículo

***"Artículo 3.** Firma electrónica, y documentos firmados electrónicamente.*

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel."

Por lo tanto la firma electrónica reconocida se caracteriza por:

- Es una firma electrónica avanzada (permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculado al firmante de manera única y a los datos a que se refiere y ha sido creada por medios que el firmante puede mantener bajo su exclusivo control)
- **BASADA EN UN CERTIFICADO RECONOCIDO**:

***"Artículo 11. Concepto y contenido de los certificados reconocidos**.*

*1. Son certificados reconocidos los **certificados electrónicos expedidos por un prestador de servicios de certificación** que cumpla los requisitos establecidos en esta Ley en cuanto a la **comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.***

2. Los certificados reconocidos incluirán, al menos, los siguientes datos:

a. La indicación de que se expiden como tales.
b. El código identificativo único del certificado.
c. La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
d. La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
e. La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
f. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
g. El comienzo y el fin del período de validez del certificado.
h. Los límites de uso del certificado, si se establecen.
i. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

- Y Generada en un dispositivo seguro de creación de firma.

Se entiende con estas características que la LCSP se refiera a la firma electrónica reconocida como instrumento más garantista, seguro y fiable, a la hora de tener en cuenta el desarrollo de las distintas manifestaciones y actos que se pueden dar en las fases preparatoria, de licitación, adjudicación y ejecución de los contratos, lo que supone un gran número de acciones que se pueden dar a lo largo del procedimiento contractual.

14}

Eso no sirve de referencia a la hora de aplicarlo a otras materias que regulan relaciones entre ciudadanos/empresas- y Administración, teniendo en cuenta los potenciales efectos jurídicos que puedan conllevar las actuaciones, manifestaciones, actos etc.

En el caso de los certificados reconocidos, que caracterizan a la emisión de firma electrónica reconocida, el aspecto fundamental es el hecho de que un tercero Prestador de Servicios de Certificación Electrónica, cuya actividad la regula las disposiciones de la Ley de Firma Electrónica, es el garante o tercero de confianza que da “fe virtual” del firmante, Prestador que lo expide, datos de verificación de firma, periodo de validez del certificado, etc. Cumpliendo los principios básicos de la firma electrónica:

- ✓ **Autenticidad**: ciudadanos y administración aseguran su respectiva identidad.
- ✓ **Confidencialidad**: nadie que no sea una de las partes de la relación puede acceder a su contenido.
- ✓ **Integridad**: nadie que no sea parte de la relación puede manipular o alterar su contenido.
- ✓ **No repudio**: ninguna de las partes puede negar que la transacción se realizó en un momento concreto y con unos contenidos específicos.

¿Quién emite los certificados Reconocidos?. Los **Prestadores de Servicios de Certificación Electrónica**, que se regulan según lo dispuesto en la Ley 59/2003 de Firma Electrónica, como terceros de confianza. La ley establece quienes serán prestadores y entre otras, las obligaciones que deben de cumplir para aquellos que emitan certificados reconocidos:

*"**Artículo 20.** Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.*

Los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

a. *Demostrar la fiabilidad necesaria para prestar servicios de certificación.*
b. *Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.*
c. *Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.*
d. *Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.*
e. *Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.*
f. *Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.*
g. *Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.*

2. Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan."

5.1. Resumen

La Administración, en función de los efectos jurídicos, deberá **establecer claramente aquellos actos o trámites en los que se puedan utilizar medios de identificación o autenticación con unos requerimientos de seguridad menores que la firma electrónica reconocida.**

6. Tipos de trámites y nivel de identificación

En los **trámites presenciales** siempre se recurre al DNI/Pasaporte/Carnet de conducir para identificar al ciudadano y a la firma manuscrita como fórmula de autenticación-autorización, por su garantía y la sencillez de uso.

Adaptar el nivel de seguridad del sistema de autenticación a las garantías requeridas por cada trámite.

Sin embargo, el equivalente en los **trámites electrónicos** –los certificados digitales– pueden ofrecer ciertas dificultades que limitan su uso. Para superar esta limitación se pueden utilizar otros sistemas de identificación cuyo uso sea más sencillo, siempre que se garanticen los requerimientos a nivel jurídico establecidos para el trámite en cuestión.

Incluso dentro de un mismo Procedimiento Administrativo, en cada uno de los trámites debería ser posible utilizar uno u otro mecanismos de identificación

A modo de ejemplo práctico, a continuación se recogen una serie de trámites básicos y habituales dentro de la Administración y se estudia el nivel de autenticación más adecuado para cada uno de ellos.

Recordar que anteriormente se analizaron los sistemas de identificación y se estableció la siguiente clasificación de los mismos:

	Sistema de identificación	Seguridad	Confiabilidad	Firma y no repudio
1	Usuario + contraseña	**Débil**	**Normalmente NO confiable** aunque depende	**NO**
2	Usuario + Contraseña de identificación + contraseña de firma (OTP enviada al teléfono móvil)	**Fuerte**	**Confiable***	**NO**
3	Usuario + Contraseña de identificación + Contraseña (OTP generada en un dispositivo hardware)	**Fuerte**	**Confiable***	**NO**
4	Firma electrónica avanzada (certificados software)	**Avanzada**	**Confiable***	**SI**
5	Firma electrónica reconocida (certificados en tarjeta criptográfica u otro dispositivo seguro de creación de firma)	**Avanzada**	**Confiable***	**SI**
6	Usuario + contraseña de identificación + contraseña de firma	**Débil**	**Confiable***	**NO**
7	Usuario + contraseña de identificación + juego de barcos	**Fuerte**	**Confiable***	**NO**

* Se consideran confiables ya que son sistemas de autenticación en los que las entidades propietarias han realizado identificaciones presenciales de los usuarios.

Las familias de procedimientos que se han tenido en cuenta son:

- Ayudas y subvenciones
- Autorizaciones y registro
- Contratación
- Sanciones
- Arbitraje denuncias y reclamaciones

Y los trámites comunes considerados en los procedimientos anteriores son:

Trámite	Seguridad mínima	Es necesaria la identificación presencial previa	Se requiere firma electrónica reconocida
Solicitud y aportación de documentación	Débil (en algunos procedimientos) / Fuerte	En algunos procedimientos	En algunos procedimientos
Modificación de datos de notificación	Fuerte	Sí	Sí
Aportación de documentación al expediente	Débil (en algunos procedimientos) / Fuerte	Sí	En algunos procedimientos
Obtener información / realizar consultas	Débil (en algunos procedimientos) / Fuerte	Sí	En algunos procedimientos
Consultar el detalle del expediente	Fuerte	Sí	Sí
Realizar pagos	Débil	Sí	No
Recoger notificaciones	Fuerte	Sí	Sí
Recoger comunicaciones	Débil	Sí	No
Solicitar aplazamientos	Fuerte	Sí	Sí
Realizar desistimientos y renuncias	Fuerte	Sí	Sí
Certificaciones	Fuerte	Sí	Sí
Presentar alegaciones o recursos	Fuerte	Sí	Sí

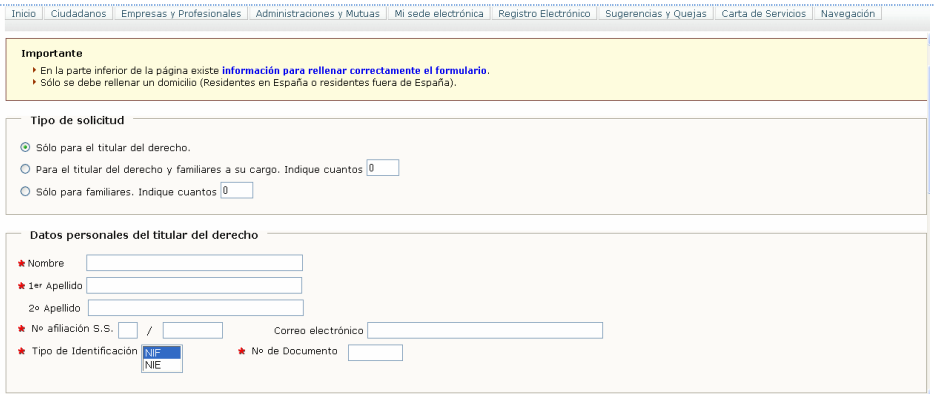
7. Casos y ejemplos

Se detallan a continuación algunos ejemplos de autenticación e identificación de otras Administraciones y entidades bancarias:

7.1. Administración Pública

7.1.1. Seguridad Social

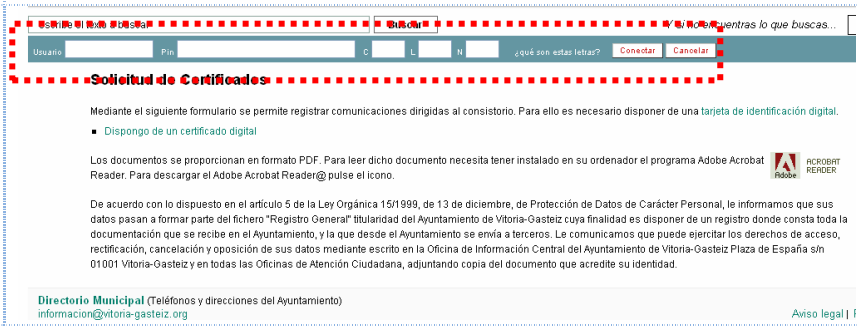
La Seguridad Social, en su Sede Electrónica, ofrece diferentes servicios en función del sistema de identificación:

Acceso a la sede electrónica	
Servicios ofrecidos en función del sistema de identificación	
Ejemplo de acceso a un servicio sin identificación	 Una vez validados los datos en la Seg. Social se procede con el trámite enviando la información al domicilio del solicitante

7.1.2. Generalitat de Catalunya

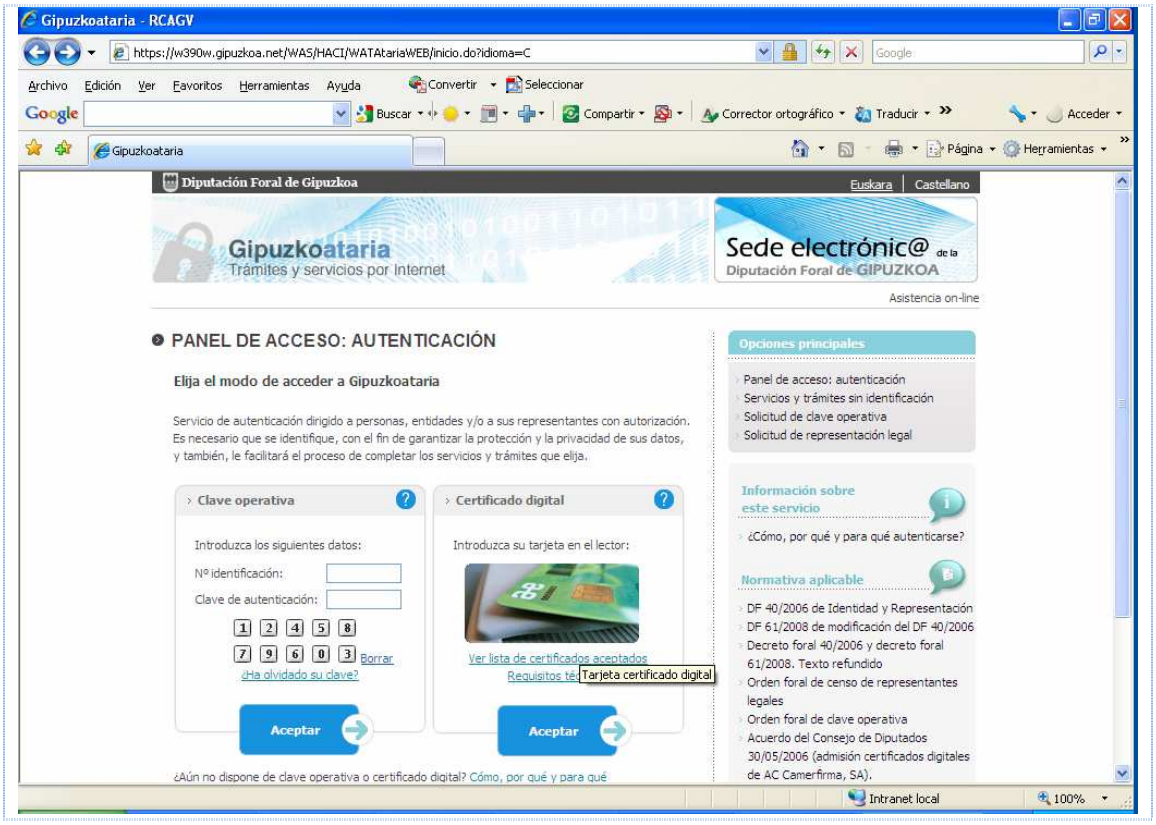
Acceso a servicios	
Consulta del estado de un expediente NO es necesaria identificación; basta con tener el identificador del expediente	
Carpeta Ciudadana Dos sistemas de acceso: • Certificado Digital • Usuario / contraseña (será sustituido próximamente por certificado digital)	

7.1.3. Ayuntamiento de Vitoria-Gasteiz

Acceso a los trámites	
Dos modos de acceso: • Certificado Digital • Tarjeta municipal ciudadana	
Identificación mediante usuario y contraseña	

20}

7.1.4. Departamento de Hacienda de la Diputación Foral de Gipuzkoa



7.2. Entidad Financiera: Vital, Kutxa, BBK y BBVA

Usuario y Contraseña o certificado digital (DNI / ONA / Izenpe) Vital, Kutxa, BBK y BBVA	

8. Conclusiones

El sistema de autenticación empleado en un servicio telemático no debe suponer un freno para su uso, por lo tanto para promover la tramitación electrónica es necesario utilizar **sistemas de autenticación sencillos** ("amigables") para la ciudadanía, siempre que garanticen de una manera **proporcional** la seguridad de los actos telemáticos (contemplando, entre otras, la Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo).

De esto se deduce que los Responsables de poner en marcha nuevos servicios electrónicos deberán estudiar y utilizar sistemas de autenticación menos exigentes en función del trámite a realizar que lo realizado hasta ahora, todo ello, en aras de fomentar el uso de los servicios telemáticos.

Los sistemas de autenticación basados en firma digital y certificados electrónicos son considerados actualmente como los más seguros y los que garantizan de manera más fiable la identidad y autenticación de la persona usuaria, ya que es el único que garantiza el no repudio, siendo la firma electrónica equivalente a la firma manuscrita.

Sin embargo, a pesar del alto nivel de distribución, (10 millones de DNI´s electrónicos distribuidos, y 270.000 certificados de ciudadano emitidos por IZENPE) a fin de conseguir unos niveles de uso mayores, se ve necesario una evolución de los dispositivos hardware y software actuales necesarios para su uso, acompañados por campañas de divulgación y formación que acerquen estos nuevos sistemas y los ya existentes (tarjeta criptográfica) a la sociedad. Se ha llegado a la conclusión de que el principal obstáculo actualmente para la difusión de la firma electrónica es la necesidad de instalar software y hardware adicional en los equipos informáticos del usuario, en concreto, el lector de tarjetas (que es el dispositivo que posibilita la lectura del certificado). Este hecho supone una traba adicional para las personas que quieren hacer uso de los servicios de la Administración, sobre todo si el nivel de informatización del usuario es escaso y no existen canales de soporte y ayuda adecuados. Además, la frecuencia de uso de muchos de los trámites no suele ser elevada, con lo que se añade la problemática del olvido de contraseñas y del propio uso.

Para conseguir un incremento en el uso de los servicios telemáticos (objetivo final del Plan de Innovación Pública, PIP) además de evolucionar los sistemas de autenticación, y realizar campañas de difusión y formación de los soportes actuales (tarjeta criptográfica), el Grupo de Trabajo considera necesario que dichos servicios telemáticos se den a conocer a los ciudadanos, se encuentren accesibles, sean amigables para el usuario y sean fiables.

En función de todo lo comentado en los apartados anteriores, el equipo de innovación traslada las siguientes propuestas que pueden ser el punto de partida para mejorar el acceso de la sociedad a la eAdministración:

Relacionadas con la identificación:

- Adecuar la **fortaleza del mecanismo de identificación en función de los trámites**. Utilizar para cada trámite electrónico sistemas de autenticación cuyas garantías sean proporcionales a las requeridas por el propio trámite en varios aspectos: la seguridad del acceso al dato, la garantía requerida de identificación y el riesgo de un acceso indebido o un repudio. Los sistemas menos seguros son también los más sencillos y su utilización facilitará el acceso a la eAdministración a un mayor número de personas, no obstante, por ejemplo en el sistema de usuario/contraseña considerado como un sistema de identificación "sencillo", habría que tener en cuenta que plantea otros problemas como olvido de contraseñas, gestión de múltiples contraseñas, lo cual cuestiona su sencillez inicial.

  A continuación mencionamos sólo los métodos de identificación más significativos:

  - Sin autenticación (no se solicitará identificación a no ser que sea estrictamente necesario);
  - Autenticación débil o fuerte (se proponen varios métodos de identificación):
    - usuario/contraseña
    - se podría usar la autenticación utilizando las entidades financieras como terceros de confianza;
    - certificado;
  - Firma electrónica reconocida (en sus mismos formatos, ONA, DNIe, Token USB...)

- Utilizar otras **entidades como terceros de identificación** (entidades financieras, compañías telefónicas, o similares) a la hora de validar la identificación de la persona usuaria. Este punto implicaría realizar acuerdos (convenios) con esas entidades, tal y como ya se ha realizado con la Pasarela de Pagos.

- Potenciar el papel de la entidad **Izenpe** (prestador de servicios de certificación electrónica) a la hora de poner en marcha nuevas iniciativas, nuevos servicios electrónicos de las Administraciones públicas vascas, así como nuevos sistemas de identificación.

Relacionadas con el hardware y software asociados a los certificados:

- Implantar **nuevos sistemas de autenticación** como pueden ser, por ejemplo, el teléfono móvil (con certificado incluido), los *"token usb"*, tarjeta de juego de barcos, etc. En ese sentido, y según distintos estudios, estos nuevos sistemas pueden sustituir, o complementar, a corto o medio plazo a los sistemas actuales (tarjetas criptográficas) debido principalmente a su amplia difusión (especialmente en el caso del teléfono móvil) y, por lo tanto, su familiaridad por parte del usuario final. Actualmente, además, estos sistemas ya nos garantizan la seguridad exigida por la normativa vigente.

- Fomentar, debido su elevada distribución, el uso del certificado electrónico en soporte de tarjeta criptográfica, realizando campañas de difusión y formación utilizando por ejemplo la red de centros KZGUNEA.

Relacionadas con la difusión de los sistemas de acceso electrónico dentro de la administración:.

- Promover el uso de los certificados de firma electrónica entre el **personal interno** (funcionariado) de la administración vasca a la hora de tramitar los procesos internos de la misma. (p.ej.: solicitar y aceptar comisiones de servicios; realizar peticiones de traducciones; cumplimentar la justificación de horario...). De esta forma el personal interno se convertiría en "agente difusor" del uso de estos nuevos medios.

- Desarrollar un aplicativo común con el **sistema de acceso** para todos los servicios electrónicos de la Administración de la CAPV y que contaría con las diferentes formas de acceso (usuario/password, certificado, mediante un tercero certificador) para su uso por parte de todas las administraciones interesadas, con vistas a una racionalización de los recursos, una unificación en los criterios de uso y un único gestor del sistema de acceso.

- Apoyar la creación de **proyectos pilotos** para la divulgación y puesta en marcha de nuevas iniciativas que permitan la divulgación de los servicios electrónicos y los nuevos sistemas de autenticación en ámbitos internos (concursos internos del Gobierno, etc.)

Relacionadas con la difusión de los sistemas de acceso electrónico fuera de la administración:

- Realizar **campañas de difusión**, centrándonos en los servicios y las ventajas que ofrece el acceso telemático para la sociedad. En este sentido, es conveniente desarrollar un buen "Plan de Gestión del Cambio". Para ello, se podría seguir el modelo plasmado en el "Metodología de Gestión del Cambio para proyectos PLATEA": identificación de líderes, facilitadores, etc.

- Apoyar la formación de **proyectos pilotos** para la divulgación y puesta en marcha de nuevas iniciativas que permitan (y hagan familiarizarse a la ciudadanía con los nuevos servicios de la eAdministración) la divulgación de los servicios electrónicos y los nuevos sistemas de autenticación; en ámbitos externos (OPEs del IVAP, etc.). Asimismo, permitirán identificar dificultades o necesidades de la ciudadanía para facilitar posteriormente una mayor divulgación de estos sistemas.

Relacionadas con la legislación vigente:

- Modificar y **adecuar el Decreto 232/2007**, de 18 de diciembre, por el que se regula la utilización de medios electrónicos, informáticos y telemáticos (MEIT) en los procedimientos administrativos (así como toda la normativa derivada) para su adaptación a las nuevas propuestas recogidas en este documento. Se trataría de permitir que la forma de acceso a un servicio electrónico sea proporcional al nivel de protección de los datos a los que se accede, a las garantías de identidad requeridas y al riesgo de un acceso indebido en cada trámite. Estableciendo, por ejemplo, la obligatoriedad del uso de la firma electrónica reconocida únicamente en trámites que requieran altas garantías de identificación y no repudio.

Relacionadas con la presentación de los servicios a la ciudadanía:

- Revisar el **diseño de las aplicaciones webs** actuales (y sus sistemas de acceso y validación de las mismas) para que contemplen distintas vías de validación y/o autenticación: habilitando e informando a la persona que acceda a la aplicación (cuando así corresponda) las opciones o trámites que podrá realizar en cada momento o en función de su perfil. Asimismo, dependiendo del tipo de tramitación o del momento de la misma se podrían habilitar

sistemas mixtos. P.ej. se comienza con identificación débil y en algún momento se puede cambiar a certificado.

- Implantar un **sistema de acceso único** (portal) para todos los trámites del Gobierno Vasco tanto telemáticos como no telemáticos, ordenados tanto por Departamento, como por tema, en el que la persona usuaria pueda elegir el que más le conviene.
    - Antes de entrar al trámite se le informará de lo que se va a encontrar y de los requisitos para su tramitación (si necesita usuario / password, ONA, DNI, etc.)
    - En el acceso a cada trámite se le solicitaría el nivel de identificación adecuado al mismo.
- Los módulos de software creados para los distintos sistemas de validación se podrían utilizar en cada uno de los trámites necesarios. Asimismo estos módulos de software podrían ser utilizados por las entidades que los necesitaran, de esta forma se optimizan los recursos.
- La creación de este sistema de acceso único para todos los servicios electrónicos de la Administración de la CAPV permitiría crear un sistema "amigable", ya que haría que el usuario siempre se encontrara con la misma pantalla de identificación para cualquier trámite con la Administración. Esta pantalla de identificación ofrecería al usuario las distintas alternativas de identificación consensuadas por las Administraciones Publicas y en función del sistema de identificación elegido el usuario podría realizar unos trámites u otros. Igualmente, evitaría a los Departamentos y Organismos Autónomos del Gobierno Vasco (y entidades dependientes), la realización de sus propios sistemas de acceso e identificación, con el consiguiente ahorro de costes y unificación de criterios de uso. Se pueden tomar como ejemplo los siguientes: Generalitat de Cataluña, Ayuntamiento de Vitoria-Gasteiz, Departamento de Hacienda de la Diputación Foral de Gipuzkoa.)

26}

9. Anexo I: Grupo de Trabajo

Las reuniones celebradas por los miembros del Grupo de Trabajo han sido las siguientes:

- 24/noviembre/2010
- 02/diciembre/2010
- 16/diciembre/2010
- 22/diciembre/2010

Y la relación de las personas que han participado en dicho Grupo, encargado de elaborar este informe, han sido las siguientes:

Nombre	Entidad
José Ramón Guinea	DIAE
Pablo Pérez	DIT
Iosu Uribe	IVAP
Cristina Jaén	IVAP
Alejandro Lara	EJIE
Jesús Mª Igartua	Izenpe
Silvia Pagola	Izenpe
Roberto Cacho	Bizigune
Alfredo Alday[3]	O-satek

[3] Acudió como invitado especial para informar a los miembros del grupo de trabajo sobre las principales características del proyecto *O-sarean* de Osatek (reunión realizada el 16 de diciembre)

10. Anexo II: Legislación y documentación

Se recoge a continuación relación de documentos normativos (leyes, decretos y demás normas) que se han consultado o se han tenido en cuenta a la hora de abordar el desarrollo de este trabajo.

10.1. Legislación Estatal

- Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre. (BOE 12-04-2010)
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad (ENI) en el ámbito de la Administración Electrónica. (BOE 29-01-2010). (Texto consolidado por el BOE)
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica. (BOE 29-01-2010). (Texto consolidado por el BOE)
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP). (BOE 18-11-2009)
- Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas. (BOE 30-05-2009)
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. (BOE 29-12-2007). (Texto consolidado por el BOE)
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (BOE 23-06-2007). (Texto consolidado por el BOE)
- Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión. (BOE 08-10-2005)
- Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica. (BOE 28-05-2005). (Texto consolidado por el BOE)
- Ley 59/2003, de 19 de diciembre, de firma electrónica. (BOE 20-12-2003). (Texto consolidado por el BOE)
- Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos. (BOE 28-02-2003) (Texto consolidado por el BOE)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (BOE 12-07-2002). (Texto consolidado por el BOE)

10.2. Legislación Autonómica

- Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.
- Orden de 26 de febrero de 2010, de la Consejera de Justicia y Administración Pública aprobando el Manual de Seguridad PLATEA.
- Orden de 15 de enero de 2009, de la Vicepresidenta del Gobierno, por la que se regula el régimen de admisión de los certificados electrónicos.
- Decreto 108/2004, de 8 de junio, del Modelo de Presencia en Internet de la Administración Pública de la Comunidad Autónoma de Euskadi.
- Orden de 11 de abril de 2008, de la Consejera de Hacienda y Administración Pública, que establece el registro y cobro automatizados de los ingresos de derecho público de la Administración General de la Comunidad Autónoma de Euskadi y de sus Organismos Autónomos a través del Sistema Integral de Pagos y Cobros de la Administración.
- Orden de 11 de abril de 2008, de la Consejera de Hacienda y Administración Pública, reguladora del servicio de colaboración en la gestión recaudatoria de la Hacienda General del País Vasco.
- Orden de 11 de abril de 2008, de la Consejera de Hacienda y Administración Pública, reguladora del pago de ingresos de derecho público de la Hacienda General del País Vasco a través de la Pasarela de Pagos.
- Decreto 72/2008, de 29 de abril, de creación, organización y funcionamiento de los registros de la Administración General de la Comunidad Autónoma de Euskadi y sus Organismos Autónomos.
- Decreto 232/2007, de 18 de diciembre, por el que se regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos.
- Resolución de 9 de febrero de 2006, de la Directora de Informática y Telecomunicaciones, aprobando el documento que establece la Plataforma Tecnológica para la E-Administración (PLATEA).