Representando a los
Abogados europeos

OPCIONES TECNOLÓGICAS DE CCBE EN LA IDENTIFICACIÓN ELECTRÓNICA DE LOS ABOGADOS DE LA UE

Consejo de la Abogacía Europea
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.org – www.ccbe.org

Informe

CMS Cameron McKenna LLP
Ybl Palace
Károlyi Mihály utca 12.
1053 - Budapest
Hungría
T +36 1 4834800
F +36 1 4834801
v2.0
1 Febrero de 2012
Numero de referencia: 132711.00001

Budapest - 442299.2

Por Peter Homoki, abogado senior de CMS Cameron McKenna LLP, Budapest.

Tabla de Contenidos

Tabla de Figuras

1. Resumen ejecutivo

Este informe fue encargado por CCBE por los siguientes motivos:
a) El crecimiento del uso de la tecnología significa que es solo cuestión de tiempo que los abogados lo lleven a cabo, y en su momento podrán ser obligados a conducir transacciones electrónicas transfronterizas – CCBE necesita estar preparado para solucionar esto, ya que es evidente que será un proyecto en toda la UE. (Véase b más adelante).
b) La UE ha empezado a contemplar transacciones transfronterizas electrónicas y ha invertido millones de euros en el proyecto e-CODEX para investigar cómo ocurrirá. e-CODEX es un proyecto de los Estados Miembros, con CCBE como parte activa. El proyecto e-CODEX ha alcanzado el punto donde es crucial que CCBE venga con soluciones sobre cómo un abogado probará su identidad de forma electrónica a través de las fronteras con el fin de una transacción transfronteriza.
c) Los Estados Miembros y las Abogacías miembro de CCBE tienen diferentes enfoques, y han empezado a llegar diferentes soluciones a la identidad electrónica de los abogados. Este informe tiene como objetivo investigar esos distintos enfoques mirando en la base conceptual de la identidad electrónica y la dirección en la que se dirige la tecnología, y viene con una solución que será aceptable para los miembros de CCBE y el proyecto e-CODEX para el futuro.
d) Si CCBE no aparece con una solución en un corto plazo, hay peligro de que el proyecto e-CODEX continúe con o sin CCBE, ya sea dejando fuera de la ecuación a los abogados o tomando decisiones por ellos.
e) CCBE se encuentra actualmente en una etapa similar a la de hace varias décadas en relación con las directivas de los abogados en cuanto a la circulación transfronteriza, excepto que en este momento se encuentra la importante dimensión de transacciones electrónicas transfronterizas.

Las conclusiones principales del informe son las siguientes:

a) La tecnología para la identificación electrónica se espera que cambie en el futuro próximo. Por el momento, CCBE debería continuar su apoyo a las tarjetas electrónicas (incluyendo la continuación en el nivel actual de apoyo proporcionado por la tarjeta de identidad de CCBE con un chip opcional de capacidades) mientras se tiene en cuenta que los dispositivos móviles (*smartphones, tablets*) se espera que reemplacen los ordenadores y portátiles en distintos escenarios. Cualquier apoyo por parte de CCBE en ciertas tecnologías tiene que tener en cuenta este factor en el futuro próximo, y por tanto es importante para CCBE trabajar permitiendo a los abogados identificarse de forma segura utilizando también dispositivos móviles.

b) CCBE no debería apoyar el uso obligatorio del uso de firma electrónica en todos los procedimientos electrónicos.

c) CCBE no debería apoyar el aumento de requisitos para el uso de la creación de la firma electrónica en la creación de la firma.

d) CCBE no debería apoyar en general tecnologías que garanticen la seguridad (para minimizar el riesgo de fraude en la identidad de los abogados) a un coste apropiado (que incluye el uso de credenciales existentes cuando sea posible) y que son familiares para los abogados de la UE.

e) CCBE debería hacer propuestas a los legisladores de la UE para asegurar que los abogados siempre tienen que probar su identidad (incluyendo tener una licencia válida para actuar como abogado) cuando se trata de procedimientos electrónicos de política transfronteriza.

f) identificar a una persona como un abogado debe implicar sólo los datos de los Colegios de Abogados (esta información está siendo proporcionada a nivel de la UE por los colegios de abogados que participan en Encuentra-Un-Abogado, y se espera que la UE pronto financie el segundo proyecto de Encuentra-Un-Abogado que usará el directorio electrónico de Encuentra-Un-Abogado para probar electrónicamente la identidad de un abogado en el futuro).

g) Sobre la base de la gran escala del proyecto STORK, también hemos analizado con más detalle algunos requisitos de seguridad de los procedimientos experimentales posibles (Orden de Detención Europea, Orden Europea de Pago y Procesos de Escasa Cuantía) dentro del proyecto e-CODEX. Aunque los correspondientes actos legales no den suficiente detalle del análisis técnico y la regulación, el marco proporcionado por STORK (los llamados " niveles QAA") lo hace. Es reconfortante saber que este marco es lo suficientemente flexible para dar cabida a la mayoría de las

tecnologías que esperamos estén disponibles para los abogados a medio plazo, y el nivel de seguridad recomendado se puede decidir también basándose en el impacto esperado de los riesgos relevantes (por ejemplo, una contraseña segura podría ser suficiente para la presentación de demandas de menor cuantía, pero esto no sería suficiente en relación con las órdenes de detención, donde deberían requerirse soluciones más fuertes en materia de seguridad de hardware.

2. Lista de abreviaturas

AC: Certificado de Atributo.
ACL: Acceso a la Lista de Control como se definió en X.800 3.3.2: "Una lista de entidades, junto a su acceso a los derechos, que se autorizan para tener acceso a un recurso".

Directiva 1999/93/EC: Directiva 1999/93/EC del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 sobre un marco comunitario de firma electrónica, OJ L 13, 19.1.2000, p 12-20.

Directiva 2005/36/EC: Directiva 2005/36/EC del Parlamento Europeo y del Consejo de 7 de Septiembre de 2005 sobre reconocimiento de cualificaciones profesionales, OJ L 255, 30.9.2005, p 22-142.

e-CODEX: Comunicación de Justicia electrónica a través del traspaso de datos en línea (PROGRAMA DE COMPETITIVIDAD E INNOVACIÓN MARCO, ICT Política del Programa de Apoyo).

FAL: Encuentra-Un-Abogado, un proyecto iniciado por CCBE para encontrar abogados en los estados socios de CCBE a través de la utilización de un servicio central de búsqueda.

IAM: Gestión de Identidad y Acceso

IMI: Sistema de Información del Mercado Interno

LSP: Proyecto a Larga Escala

MS: Estado Miembro. En el contexto, podría significar un estado miembro de la Unión Europea, Área Económica Europea o el país de origen de los Colegios de Abogados miembros de CCBE.

NFC: Campo de Comunicación Cercano, tecnología de corto alcance e inalámbrica de alta frecuencia que permite el cambio de datos entre dispositivos a 10 centímetros (4 pulgadas) de distancia.

OTP: Contraseña de Una Vez (ver la descripción con mayor detalle en la Sección 4.2.3.)

PCI DSS: Industria de Pago con Tarjeta a través de estándares de Seguridad de Datos

PKC: Certificado de clave pública

PMI: Privilegio de Gestión de Infraestructuras.

QAA: Calidad del Seguro de Autenticación

STORK: Programa de Seguridad de Identidad a través de Fronteras Vinculadas

UI: Interfaz del Usuario.

X.509: ITU-T X.509 (11/2008) Tecnología de la información – Interconexión de sistemas abiertos – El Directorio: Clave –pública y atribución de marcos certificados, http://www.itu.int/rec/T-REC-X.509-200811-I/en

X.800: Recomendación CCITT X.800 (1991): Arquitectura de la Seguridad para la Interconexión de Sistemas abiertos de CCITT7/56

3. Introducción

El objetivo de CCBE es pensar profundamente sobre las necesidades futuras de los abogados de la UE para identificarse electrónicamente en cualquier Estado miembro o ante diferentes foros de la UE. Para comprender la identificación electrónica de los abogados de la UE, CCBE ha pedido a la Oficina de Budapest de CMS Cameron McKenna que lleve a cabo una encuesta y un análisis de las respuestas de este tema, y resumir sus conclusiones y sus recomendaciones en un informe.

La identificación de los abogados de la UE significa tres cosas separadas: identificación de una persona en un sistema electrónico (seleccionando una entidad de un posible conjunto), autentificación del mismo proporcionando pruebas fiables para el uso de los sistemas electrónicos, y proporcionar información a la fecha sobre si la entidad que se da es en realidad la de un abogado, también llamado autorización.

Mientras que diferenciemos la identificación de la autentificación, la identificación no es necesariamente un proceso que deberíamos analizar desde un punto de vista tecnológico, así que profundizaremos primero en cuanto a la autentificación y luego en cuanto a la autorización.

En cuanto a la autentificación, se han publicado muchos análisis comparativos de técnicas de autentificación electrónica sobre la financiación por la UE. La diferencia principal en este informe es que nos gustaría tener en cuenta tanto los puntos de vista específicos de CCBE como las tendencias que se esperan en el futuro sobre la tecnología, y basados en estos resultados, nos gustaría ver este punto de vista en el futuro, que encaja en la trayectoria ya establecida por STORK, que está disponible.

Tratando de empezar desde una perspectiva reguladora, intentamos introducir una amplia variedad de credenciales de autentificación comunes, basadas en una clasificación de autentificación y formularios de forma (documentos basados en credenciales, software y credenciales de hardware, etc.) Exponemos en detalle tipos específicos de credenciales en párrafos separados, por ejemplo, chips criptográficos en tarjetas inteligentes u otros formatos, y también sobre NFC y los cambios que se podrían causar a largo plazo. Mediante la introducción de los efectos esperados de las fuerzas estratégicas de IT en el futuro cercano, llegamos a las siguientes conclusiones en cuanto a las tecnologías de autenticación:

a) La reutilización de dispositivos de seguridad (que usen un hardware específico de seguridad para tantos escenarios como sea posible) debería ser una prioridad en el futuro cercano, no siendo deseable ni a medio plazo que requiera una tarjeta inteligente separada que implique a los lectores para usos de seguridad.

b) La promesa de NFC es la posibilidad de disminuir el *grip* de los operadores móviles, y las asociaciones de tarjetas que de forma segura identifiquen al usuario, y por tanto podría ser un factor de éxito principal para permitir la reutilización de dispositivos de seguridad (véase la convergencia en el uso de los teléfonos móviles para fines de pago, donde ni el operador del móvil ni la asociación de tarjetas de pago está en una posición unilateral en los términos de uso del elemento de seguridad);

c) Si resulta que por algunas razones los dispositivos móviles y/o tarjetas de pago aún no pueden ser para fines externos a su dominio principal, eIDs llevados a cabo por los gobiernos con capacidad de chips de seguridad podría cambiar el rumbo hacia eIDs de múltiple uso.

d) El dispositivo de computación personal más ubicuo en el futuro próximo, no es el ordenador de mesa ni el portátil, será un dispositivo aún más móvil: un teléfono inteligente o una tableta. También tendrá un impacto en la forma en que las personas usan los ordenadores, y se extenderá una solución segura para el uso de la plataforma de los teléfonos inteligentes. Se acelerará aún más si en futuros gobiernos también aceptan la identificación por las redes sociales.

También intentamos poner estas conclusiones para un uso más directo, mostrando cómo estas tecnologías podrían evaluarse dentro del contexto de la autentificación por e-CODEX: es posible aceptar las soluciones de contraseña fuerte para Procedimientos de Menor Cuantía, a condición de que el procedimiento de registro llegue por sí mismo a ser más sólido. Sin embargo, dentro del marco de STORK, la Orden de Detención Europea requerirá, sin duda, certificados cualificados incluidos en un dispositivo de seguridad de hardware.

Para la autentificación de los usos de la Orden de Pago Europea, actualmente no hay ningún requisito que haga necesario el uso de un token hardware por todos los medios, por lo que un certificado de hardware parecería suficiente (pero esto no significa que las tarjetas inteligente o OTP hardware tokens no podrían ser usadas para este propósito.)

Desde el resumen de menú de las tecnologías de autentificación, tenemos que resaltar que la exigencia de los certificados de hardware-based X.509 para su autentificación o firma sería una opción muy segura y con buenas oportunidades para la interoperatibilidad y reutilización posterior (que también podrían disminuir los correspondientes costes.)

Siguiendo el esquema de las tecnologías de autentificación, volvemos al análisis de la autorización y de algunos de los problemas infraestructurales que caracterizan esta área. Es difícil definir un marco genérico legal para la autorización transfronteriza, porque la autorización depende fuertemente del área del derecho afectada en el servicio transfronterizo y de las soluciones ya existentes. Hay dos cuestiones de la autorización de gran importancia para CCBE: licencia de los abogados y mandatos. En cuanto a la licencia de los abogados, parece que la mayoría de miembros de CCBE que responden al cuestionario están dispuestos y capacitados para proporcionar datos a CCBE (algunos de los miembros de CCBE están ya proporcionando esta información eficazmente gracias a la base de datos actual Encuentra-Un-Abogado). Proporcionar una base de datos transfronteriza para el mandato de los clientes es un problema más difícil – las alternativas útiles podrían basarse en usar a terceras personas de confianza que sirvan como interfaz para los ciudadanos desconectados de los servicios de gobierno virtual, por ejemplo, un notario público o incluso otro abogado que certifique que el mandato lo dio el ciudadano ahí identificado. En cuanto a la infraestructura técnica de las autorizaciones, aunque la Infraestructura de Gestión de Privilegios fue descrita por X.509 v4 como una tecnología que tenemos que tener controlada, CCBE no está aún en posición de adaptar esta tecnología o empezar a usarla para propósitos de vida.

No esperamos que la Tarjeta Profesional Europea sea usada para fines de gobiernos electrónicos transfronterizos, porque no fue creada con ese propósito, y la expedición de este tipo de archivo electrónico normalmente necesita una solicitud previa por el abogado para subir su expediente a IMI.

Según los análisis de las respuestas y los análisis previos de la tendencia tecnológica, concluimos que:

a) actualmente, CCBE debería continuar con el apoyo al uso de los teléfonos inteligentes para identificar a los abogados, pero también tener en cuenta que todos los requisitos fijados en los actos legislativos y todas las conclusiones de LSP e-CODEX deberían *formularse de tal manera que en el futuro cercano, los abogados sean capaces de usar los elementos de seguridad en sus dispositivos móviles* y no sólo utilizar tarjetas inteligentes con lectores especiales en un ordenador de mesa o portátil.

b) Basado en las esperadas tendencias tecnológicas, es también una conclusión importante que CCBE no restringiría el apoyo al uso de la firma electrónica, porque las firmas virtuales podrían no ser una buena respuesta en todos los procedimientos electrónicos afectados, y CCBE se esfuerza para asegurar que el hardware basado en tecnologías de autentificación sin aptitudes de firma no están excluidas del nivel regulador sin razones claras y muy específicas.

c) También recomendamos no apoyar ninguna ampliación de los requisitos para el uso de dispositivos para la creación de firmas seguras. Esto podría crear no solo costes significantes e injustificados para los abogados, sino que también guiará a incrementar innecesariamente el número de dispositivos y correspondientes PINs que los abogados deberían conservar por sí mismos.

4. Perspectiva general de alto nivel sobre las tecnologías, soluciones y tendencias

4.1. Terminología: identificación, autenticación y autorización

Para profundizar en detalles técnicos, primero tenemos que hacer un borrador sobre la perspectiva general de una forma más precisa, poniendo atención a la terminología oculta.

La identificación electrónica de un abogado de la UE es una transacción electrónica por si misma y también una parte de un servicio electrónico – que en su mayoría se concentrará en los servicios electrónicos prestados por cualquier tipo de gobierno, local, federal o un cuerpo de autogobierno como un Colegio de Abogados.

Para asegurar la identificación de un abogado de la UE, tenemos que concentrarnos en dos servicios de seguridad (1) separados y muy diferentes: (a) identificación de una entidad, que en este sentido incluye la verificación de la identidad declarada; y (b) ser identificado como alguien que es abogado de la UE.

La **Identificación** trata de proporcionar una identidad de usuario para un sistema de seguridad (para el proveedor de servicios que está detrás del sistema), la búsqueda está basada en la información que se le da al sistema de una única identidad del posible conjunto de identidades a disposición del sistema. Los profesionales de la seguridad consideran la **autentificación** como a una fase diferente después de la identificación: el usuario debe dar evidencias para probar su identidad declarada en el sistema basado en algunas credenciales (2) o en la ficha. Más adelante entraremos en detalle sobre el uso normal y deseable de las credenciales (3).

Aunque hay problemas con la identificación transfronteriza de los abogados de la UE per se, ya que se diferencian de la autentificación solo estos abogados, estos problemas son de pura protección de datos, privacidad o de origen del derecho constitucional: ¿podemos usar cualquier identificador único para los abogados y otros participantes de proceso virtual, puede alguien en la UE hacer público los identificadores únicos para los propósitos de identificación transfronteriza? Podrían estos identificadores estar incluidos en por ejemplo certificados públicos X.509 usados en la autentificación? (4) Deberían estos identificadores transfronterizos únicos ser permanentes o es suficiente con que sean temporales? (5) Desde el punto de vista de este informe, solo la tecnología de autentificación electrónica es importante para analizar las elecciones de CCBE.

Por favor tenga en cuenta que los distintos pasos sobre la identificación y la autentificación mencionados más arriba, son a menudo utilizados de forma conjunta (compárese el término IAM para “gestión de identificación y autentificación”), de forma intercambiable o incluso como sinónimos.

---

1) Consulte la definición y enumeración de servicios de seguridad en la Sección 3.3.5.1 y la Sección 5 en X.800.
2) Consulte la definición de autenticación en la Sección 3.3.7 en X.800: " Consulte la autenticación del origen de datos, y la autenticación de una entidad par (peer entity authentication). Nota – En esta Recomendación el término “autentificación” no se usa en relación con la integridad de datos; el término “integridad de datos” se usa en su lugar”. Consultar la Sección 3.3.40 en X.800: "Autentificación de una entidad par: La corroboración de que una entidad par en una asociación es la que se reivindica”.
3) Todorov, Dobromir: Mecánicas de Identificación y Autentificación del usuario: Fundamentos de Gestión de Identidad, Publicaciones Auerbach, Boca Raton, 2007, p. 5. y Sección 3.3.17 en X.800: "Credenciales: Datos que se transfieren para estalecer la identidad reclamada de una entidad.”
4) Véase también:
a) Proyecto a gran escala STORK, "D2.2 Informe de la Interoperabilidad jurídica", https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578, p. 41; y
b) Proyecto a gran escala e-CODEX ("Comunicación de Justicia Virtual en línea de intercambio de datos") "D4.1 Inventario de identidad y requisitos”, WP4-REQ-F-003 "Resolución de EOPIC", WP4-REQ-NF-003 en las páginas 30 y 31, y la Sección 6.1. en la p. 48 ("Pero sólo la mitad de las credenciales MS que se basan en los certificados X.509V3 que incluyendo el EOPIC o tienen la opción de incluirlo dentro del certificado"), http://www.ecodex.eu/index.php/downloads2/category/1-deliverables?download=3:d41
5) Por favor compare las distintas conclusiones de e-CODEX en la sección a) en la nota al pie de la página 4 con las conclusiones de las p. 36-37 de STORK D2.3 – Autentificación del régimen de calidad https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577.

En los sistemas de computación general, después de que el proceso de autentificación sea satisfactorio y la identidad reclamada se verifique, se proporciona a la entidad acceso al sistema, con la previa definición de los derechos que se asignen a su identidad. Pero también es posible que el sistema no conozca al usuario de antemano, que los derechos no se establecen a priori. En este caso, además de la identificación y la autorización, el sistema también tiene que comprobar desde un directorio diferente, sistema o certificación por separado lo que el usuario particular tiene derecho a hacer en el sistema. Este paso de verificación y de asignación de derechos a un usuario particular se llama **autorización** (6).

Por lo que, si hablamos de "identificación de un abogado de la UE", no solo hablamos de identificación y autentificación de una persona, sino también sobre la verificación prioritaria de la autorización, sobre la comprobación de si esa persona identificada a través de, por ejemplo, un número común europeo de identificación personal, es de hecho un abogado en el momento del acceso o no. Sin embargo, este paso separado de autorización podría ser técnicamente muy diferente de la autentificación. Esta autorización puede ser llevada a cabo de diferentes maneras, no relacionadas:

a) Mediante documentos certificados (parecido a la comprobación de las cualificaciones según la Directiva 2005/36/EC (7)) y por la introducción manual de los resultados en el sistema de destino llevado a cabo por una persona que verifique;

b) Mediante mensajes electrónicos fiables de personas de confianza, como notarios públicos o departamentos de un Estado Miembro que han verificado la información;

c) Por un servicio web automatizado a través de un auténtico registro electrónico, como los registradores de la propiedad (parecido al servicio web Encuentra-Un-Abogado dado por los Colegios de abogados para el motor de búsqueda central);

d) Directamente por la comprobación de un atributo especial en X.509, clave certificada cualificada pública para identificar un abogado; o

e) Usando un certificado electrónico especial X.509 (llamado certificado de atributo) expedido y firmado digitalmente por un proveedor de servicios de atributo, que es normalmente válido para esa sesión de servicio electrónico (por ejemplo, sólo para unos minutos)

También debemos mencionar que, por ejemplo, en el proyecto a gran escala de e-CODEX, al menos surgen dos asuntos diferentes de la autorización, que son, al menos dos atributos que se han certificado en un servicio electrónico: uno es si la persona identificada se autoriza como abogado, y la otra si este abogado tiene algún mandato efectivo (poder) por parte del cliente en cuestión. Algunos atributos adicionales podrían ser comprobados por un servicio electrónico (8), por ejemplo, en un bufete de abogados se da un mandato, que el abogado tiene derecho a actuar en nombre de esta firma de abogados, o cuando un abogado va a ser sustituido por otro ante el tribunal, etc.

Aunque la mayoría de la parte técnica de esta informe es sobre las tecnologías de autenticación, y más concretamente, en los dispositivos de seguridad emitidos a los clientes, también entraremos en detalle sobre las técnicas de autorización y si CCBE podría estar en cualquier situación para apoyar las técnicas de autorización.

---

(6) Consultar la Sección 3.3.10 en X.800: "La concesión de derechos que incluye la concesión de acceso basada en el acceso a los derechos".
(7) Directiva 2005/36/EC del Parlamento Europeo y el Consejo de 7 Septiembre de 2005 sobre el reconocimiento de cualificaciones profesionales.
(8) Véase e-CODEX entregable D7.1 Gobierno y Definición de Directrices, p. 40, Sección 5.3.1.1

4.2. El propósito del informe en relación con las tecnologías de autentificación

Se han publicado dentro de la UE, análisis de técnicas de autentificación electrónica, numerosos, de gran alcance y comparativos, y tenemos que mencionar específicamente dos papeles financiados por la UE, la propuesta IDABC (9) y la más reciente STORK Entregable D2.3 Autentificación del régimen de calidad (10). Ambos informes pueden verse como proveedores de un menú de alternativas, también para sus lectores.

Así que, para crear cualquier valor posible para CCBE, no queremos repetir ni el enfoque, ni la metodología ni los resultados de los documentos, pero si es posible, aún se basan en ellos. Por tanto, primero daremos una visión fácil de las tecnologías de autenticación posibles (e intentaremos no ser demasiado técnicos al mismo tiempo), luego echaremos la vista hacia el futuro de la tendencia de la Tecnología de la Información que afecta al uso de estas tecnologías, y también haremos un inventario sobre cómo encaja todo esto en el antes mencionado STORK entregable D2.3 (que se basa en la propuesta IDABC también mencionada). Finalmente, desde el punto de vista de CCBE, incluimos el requerido "menú de alternativas".

La autentificación es considerada como un servicio de seguridad y por tanto siempre es parte de un sistema más amplio. De este modo, las tecnologías usadas para la autentificación y la seguridad de la autentificación no pueden ser analizadas sólo con ver la prueba que proporciona el usuario. Deberíamos tener en cuenta dónde y cómo esta evidencia se emite, comprueba, cómo funciona el protocolo, etc.

Sin embargo, restringiremos nuestro enfoque de credenciales por varias razones:

a) La credencial elegida y los riesgos asociados tienen un impacto considerable en los niveles superiores de arquitectura de autentificación también, es decir, una credencial robusta es una precondición para una arquitectura de autentificación robusta;
b) Análisis de una tecnología de alto nivel requeriría el análisis de cierto mercado líder de productos de software IAM, arquitectura de la tecnología de la Información muy genérica o requisitos muy específicos de CCBE
c) Análisis de la calidad de la autentificación en los entregables de STORK enfocado principalmente a las credenciales y el proceso de registro, con solo un pequeño desvío en el área de seguridad del protocolo de autentificación utilizado(11);
d) No consideramos el proceso de registro llevado a cabo con anterioridad a la emisión de la credencial como un proceso tecnológico, así que lo excluimos de nuestra revisión, aunque un proceso de registro de confianza sea un requisito previo para una autentificación segura.
e) La razón de realizar un borrador de este informe no era proporcionar una base técnica para implementar algún protocolo específico de autentificación segura en nombre de CCBE o de los colegios de abogados, sino ayudar a CCBE "a pensar más ampliamente en las necesidades futuras de los abogados de la UE para identificarse electrónicamente", y el más caro actualmente, el factor más decisivo para proporcionar un ambiente informático seguro para un número indefinido de servicios de gobierno virtual paneuropeo que se encuentra en el lado del cliente, con provisión de credenciales;

La siguiente figura es de un STORK entregable "D5.1 Evaluación y valoración de los modelos de referencia existentes y especificaciones comunes" (12), e ilustra como el nivel de las credenciales se refiere a otros niveles del servicio de autentificación.

---

(9) Interoperabilidad de la identificación electrónica PEGS – Propuesta de un mecanismo de autentificación a multinivel y cartografía de los sistemas de autentificación existentes, diciembre de 2007, http://ec.europa.eu/idabc/servlets/Docbf72.pdf?id=29622
(10) https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577
(11) Véase la sección 2.4.2 del entregable e-CODEX D2.3 – autentificación del régimen de calidad, https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

(12) p. 40, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1440

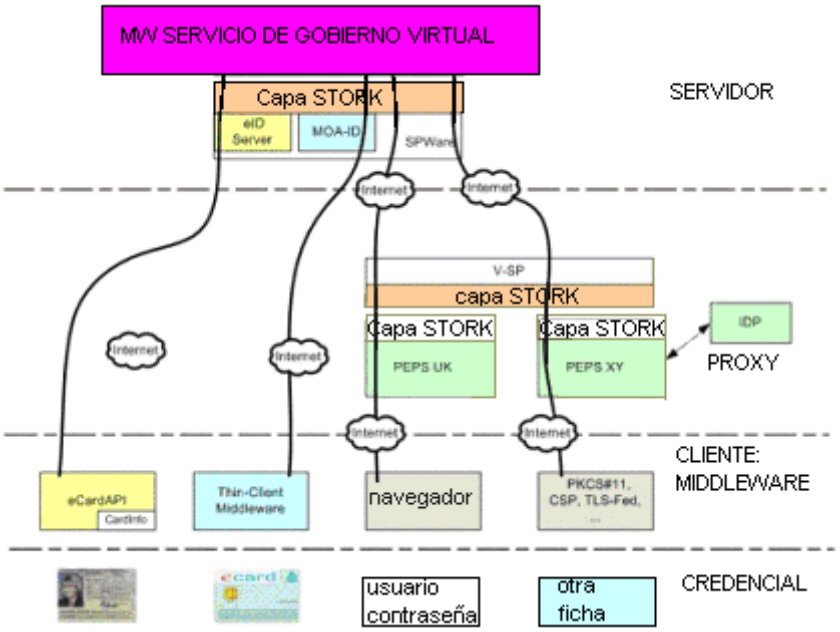


Figura 1 Credenciales y otros niveles técnicos de autentificación

4.2.1. Una breve visión de las credenciales

Para seguir más de cerca el punto de vista de un abogado, parece que sería útil iniciar la visión desde una perspectiva normativa. Desafortunadamente, no hay requisitos legales de una autentificación segura a nivel de la UE. Aparte de los actos jurídicos que prescriben ciertas tecnologías y aparte de la Directiva 1999/93/EC (en su mayoría específica para un determinado tipo de credencial), no hay requisitos de autentificación en los actos legales de la UE.

El requisito similar más cercano dentro de la legislación secundaria de la UE es el requisito genérico del artículo 57 (1) a) de la directiva de servicios de pago (13) asegurando *"los elementos de seguridad personalizados del instrumento de pago no son accesibles otros distintos de los del servicio de pago del usuario habilitado para utilizar el instrumento de pago […]"* No forma parte del acervo comunitario, pero algunos principios establecidos por el Comité de Basilea para la banca electrónica (Principios de Gestión de Riesgos para la Banca Electrónica) cubren un requisito similar: *"Los bancos deberían tomar las medidas apropiadas para autentificar la identidad y la autorización de los clientes con los que se desarrolla su negocio a través de internet (14)"*

Pero podemos encontrar un buen punto de partida para la presentación de credenciales en un documento normativo aplicable a las instituciones financieras de US (15) "Las agencias consideran un factor único de autenticación, como el mecanismo de control único, para ser inadecuado para las transacciones de alto riesgo que implique el acceso a la información *del cliente o el movimiento de los fondos a otras partes". […]*

---

(13) Directiva 2007/64/EC del Parlamento Europeo y del Consejo de 13 de noviembre de 2007 sobre servicios de pago en el Mercado interno que modifica las Directivas 97/7/EC, 2002/65/EC, 2005/60/EC y 2006/48/EC y revocando la Directiva 97/5/EC, OJ L 319, 5.12.2007, p. 1-36.

(14) Principio 4 dentro de los Principios de Gestión de Riesgos para la Banca Electrónica, Mayo de 2001, p. 17., disponible en: http://www.bis.org/publ/bcbs82.pdf. Ver también la provisión de los requisitos de Basilea II (sirve como base para la "directiva MiFID" 2004/39/EC) que nombra al robo de la identidad como lo hace el Basilea II: "fraude externo para la gestión de riesgos operacionales" en el Comité de Basilea sobre la Supervisión Bancaria: Convergencia Internacional de Medidas de Capital y Estándares de Capital, Anexo 7, disponible en: http://www.bis.org/publ/bcbs107.pdf.

(15) Consejo de Instituciones Financieras Federales de examen: Autentificación en un Medioambiente de Banca por Internet, p. 3. http://www.ffiec.gov/pdf/authentication_guidance.pdf. Véase también Dobromir, Todorov op. cit., p. 18-19

Los métodos de autentificación que dependen de más de un factor son más difíciles de transigir que los métodos de que dependen de un factor único." Y también "la autentificación de un factor único no es suficiente, las instituciones financieras deberían implementar la autentificación de factores múltiples, la seguridad a capas, *u otros controles razonablemente calculados para atenuar aquellos riesgos"*

Para tener una visión general de las credenciales, es útil iniciar la categorización con los llamados factores de autentificación. El mismo documento describe a los factores de la siguiente forma:

"Las metodologías de autentificación existentes incluyen tres "factores" básicos:
• *Algo que el usuario conoce (por ejemplo la contraseña o el PIN);*
• *Algo que el usuario tiene (por ejemplo Tarjeta de Cajero Automático, Tarjeta Inteligente); y*
• *Algo que el usuario es (por ejemplo característica biométrica, como la huella dactilar (16)).*"

Es importante tener en cuenta de antemano que la diferencia entre estos factores es en muchos casos subjetiva, no es clara, y no tienen definiciones universalmente aceptadas. Por tanto, empezamos cada factor con una corta descripción sobre cómo entendemos la definición. La credencial se define como "datos que son transferidos para establecer la identidad reclamada de una entidad (17)", una característica común a todas las credenciales es que ciertos datos específicos han de transmitirse para la autentificación – la diferencia es cómo los datos se protegen de diferentes riesgos de seguridad.

Cubriremos los tipos de credenciales más importantes basadas en estas categorías, pero tenemos que mencionar que el factor "algo que el usuario conoce" no es realmente dependiente de la tecnología, y no se verá afectado por ningún cambio tecnológico futuro.

Tal y como hemos visto de los requisitos de FFIEC, normalmente más de una de las credenciales mencionadas más arriba se utilizan en el proceso de seguridad. (Esto es también la razón por la que necesitamos entrar con códigos PIN o biométricos al acceder incluso a dispositivos de hardware de seguridad, como las tarjetas inteligentes u OTP supplying tokens.

4.2.2. Algo que sabes

Consideramos un factor de autentificación que "tú sabes" si durante el proceso de autentificación la persona física usuaria tiene que introducir algunos datos de su memoria (y no, por ejemplo, basado en la información que la persona lee de ciertos dispositivos, que discutimos bajo el nombre de "algo que tu tienes"). Aquí, la hipótesis es que para que sea seguro, los datos que se usen para la autentificación, no deberían ser revelados a personas que no estén autorizadas.

También conocido como la contraseña, el código PIN e información similar (patrón de gesto o teléfono con pantalla multi-táctil.) Evidentemente, no hay técnicas que intervengan en este factor de autentificación. Podemos diferenciar entre contraseñas basadas en su fuerza, que significa, cómo de fácil es adivinar o espiar su contenido.

---

(16) Hay otros factores adicionales no mencionados arriba, por ejemplo, alguien que te conoce, algún sitio en el que estás, etc. No serían realmente útiles en la panorámica de las tecnologías asociadas, por lo que no los mencionamos.
(17) Véase el pie de página 3 arriba.

4.2.3. Algo que tienes / posees

Consideramos un factor de autentificación que "tú posees" si durante el proceso de autentificación, la persona física tiene que proporcionar una prueba de su posesión introduciendo capacidades en el sistema informático utilizado. Esta es la categoría más heterogénea de credenciales, así que para dar una visión general, es indispensable crear nuevas categorías (características) de estas credenciales y mostrar las clases más populares mostrando la distinción de estas diferentes características.

Para esta categoría de credenciales, los datos usados para los fines de credenciales está protegida mediante el uso de características físicas únicas distintas a las biométricas (4.2.4) o ciertos dispositivos físicos o no que proporcionan ayuda al usuario para proteger el secreto de datos (y por lo tanto, seguridad). Las claves físicas pueden clasificarse en el grupo anterior, siempre que se utilicen en un proceso de autentificación conectado a un sistema informático (como ejemplo, podría ser una cerradura electrónica o similar).

La mayoría de las credenciales de "algo que tienes/posees" pertenecer al último grupo, por lo que tenemos que diferenciar aún más estas credenciales basadas en cómo proteger el secreto, y cómo los datos a proteger se entregan al sistema de autentificación desde el dispositivo.

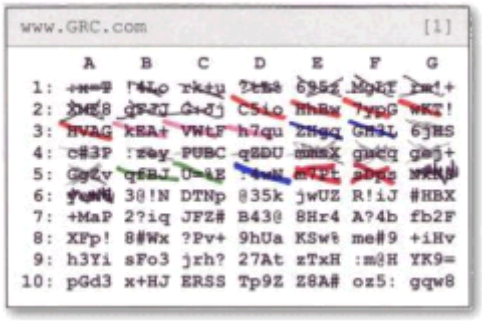
En cuanto a "cómo proteger el secreto", un método simple es confiar en barreras físicas para la protección del secreto, por ejemplo, usando teclas/llaves impresas guardadas en un supuesto lugar seguro, o incluso en el ordenador, en un lugar con control de acceso personal. En la mayoría de los casos que son importantes, los mecanismos para la seguridad de datos se usan para la protección del secreto, y estos mecanismos pueden variar desde almacenar el secreto en un área segura de almacenamiento en un ordenador medio hasta almacenar el secreto en un dispositivo de seguridad separado o un conjunto de mecanismos, que podría ser cualquier cosa, desde una memoria especial, un chip instalado en el ordenador (por ejemplo, una tarjeta inteligente) o un entorno informático seguro separado que se compone de varios servidores de un ordenador físico, etc.

Cuanto menos acceso tenga el usuario a este dispositivo de seguridad (cuanto mayor sea su restricción de acceso a la extensión necesaria), más seguridad tendrá el dispositivo, así que lo normal es no enviar el secreto fuera del dispositivo: se usa el dispositivo de seguridad para entregar tales respuestas para la autentificación a) de la que todavía es muy difícil adivinar el secreto original b) El sistema de autentificación puede decidir si el dispositivo que proporciona la respuesta estaba en posesión del secreto. Esto puede hacerse a través de datos previamente compartidos por el sistema de autentificación y el dispositivo de seguridad (incluyendo el uso de claves criptográficas u otros parámetros secretos) o mediante el uso de criptografía de clave pública. (18).

Los medios de reparto de datos del sistema de autentificación son muchos y dependen del método de protección del secreto. El reparto funciona de forma diferente si el usuario recibe la credencial de un dispositivo y se requiere la interacción del usuario para introducir la credencial en el sistema (por ejemplo, leyéndolo de un papel o de un ordenador especial y escribirlo), y de diferente forma es si el sistema de autentificación recibe esta credencial de forma totalmente automática, ya sea desde una interfaz de radio para distancias cortas o de un mensaje IP a través de internet, etc.

Para dar una buena visión general de todos estos posibles métodos de las credenciales de "algo que tienes/posees", vamos a mostrar algunos tipos de credenciales, enseñar a qué categoría de las anteriores pertenecen, y entrar en detalle sobre ciertas tecnologías importantes.

Un lugar no sofisticado de la credencial "algo que tienes/posees" es un papel impreso enviado al usuario, donde éste introduce los códigos de acceso y las contraseñas de una vez, ya sea en un orden establecido o al azar según sea requerido por el servidor de autentificación) (19). Esto se llama normalmente código de acceso de bloc de notas (passcode scratch pad) o de números de transacción de autentificación. Esta credencial está claramente protegida por la asunción de la seguridad física en este documento, y no hay intención de ir a más detalle sobre el método de reparto utilizado.



Ejemplo figura 2 OTP – Bloc de notas

Incluso esto tiene ciertas ventajas sobre las contraseñas fuertes tradicionales, llamadas contraseñas estáticas. El inconveniente más grave de las estáticas, incluso con contraseña fuerte, es la posibilidad de una repetición. Si no hay protección separada en el protocolo contra la repetición, es posible que alguien esté realizando escuchas informáticas en un canal no cifrado (por ejemplo, en el ordenador del usuario o en el servidor o entre ellos) que tiene la posibilidad de reutilizar esa información sometida introduciéndola en el sistema (incluso si no tiene la contraseña, pero el código hash se transmitió para ese acceso) (20).

El riesgo de repetición puede ser mitigado por soluciones como ésta, y se llaman "contraseñas de una vez" (one time passwords "**OTP**") mediante el uso de contraseñas dinámicas (cambiantes). (El riesgo de repetición también puede reducirse por otras partes del proceso de autenticación, por ejemplo la unicidad del mensaje que debe ser firmado por la clave privada –secreta- garantizada por los datos de tiempo o por un número de serie tipo de datos llamado nonce).

Otro ejemplo de dispositivos no electrónicos que proporciona OTPs y que se considera como una credencial de "algo que tienes/posees" es una "red única" expedida para el usuario. Por ejemplo, en el caso de una solución llamada ArrayShield, los usuarios primero tienen que registrar un patrón (por ejemplo, introducir el primero de los caracteres en la esquina baja izquierda y luego poner tres caracteres a la derecha, y al final, un carácter arriba), y los usuarios recibirán una tarjeta específica (una máscara) donde los campos vacíos serán translúcidos, y algunos campos permanecerán fijos. Al acceder, se verá una tabla generada de forma aleatoria de 5x5 campos, se pone la máscara en este campo del monitor y se introducen los caracteres que se vean en la pantalla para como las contraseñas de una vez(21). En este caso, la credencial está protegida por ambos, la seguridad física de la máscara y además por algo que el usuario conoce (el orden de entrada de los números), por otra parte es parecido en el bloc de notas. Pero en la práctica las OTPs basadas en la red única no son muy usadas (al contrario de los códigos de acceso del bloc de notas.

Las contraseñas de una vez enviadas en forma de **mensaje de texto a los teléfonos móviles** para la lectura humana y su escritura, son también un método frecuentemente usado en "algo que tienes/posees", donde la se genera contraseña dinámica para la entrada a un sistema diferente y se envía al usuario a través del teléfono móvil. Por lo tanto, el secreto para la generación de OTP está protegido en un ordenador de confianza, y se supone que el canal de entrega para la OTP al usuario se hace a través de un medio de confianza y que el teléfono móvil lo posee la persona correcta. Aquí, la compensación para una mayor protección del secreto es el coste del canal de entrega y el inconveniente de tener que escribir manualmente el mensaje de texto dentro del sistema de autentificación.

---

(18) No vemos necesario entrar en detalle sobre la criptografía de clave pública, pero la generación de la clave pública y privada está basada en un número común y la posibilidad de encontrar la única conexión entre las dos claves, como número común para la generación de clave podría ser un dato compartido entre el dispositivo que mantiene la clave privada y el sistema de autentificación que mantiene la clave pública.
(19) También llamada tarjeta de red única, por ejemplo https://www.grc.com/ppp15/56
(20) El riesgo de repetición es la razón por la que la simple firma digital de un formulario de inscripción web no es deseable, y no se considera seguro, ya que se debe tener cuidado para incluir una información de una sola vez en el formulario firmado, por ejemplo la fecha y tiempo exacto o parecido o mejor aún, para usar el par de claves (keypair) X.509 específicamente para la autenticación y no para propósitos de firma digital. Cuando se use la firma digital, queremos garantizar que no se rechace ese documento, y la no unicidad del resultado.
(21) http://www.arrayshield.com/products/howitworks/16/56

Desde luego también hay credenciales donde no se necesita manual de entrada. Hay métodos de autentificación para teléfonos móviles inteligentes con internet u otra conexión de datos que no use mensajes de texto, pero los métodos de comunicación datos específicos de teléfonos móviles, por ejemplo WAP entre un teléfono móvil y un servidor, etc. (en estos casos normalmente, y necesariamente, toda la comunicación de la autentificación se lleva a cabo usando estos canales de datos de móviles).

Una credencial muy similar es cuando un ordenador o portátil específico (previamente matriculado) tiene que ser usado en el proceso de autentificación (como prueba de posesión), y ciertas características de estos ordenadores se usan para la verificación (por ejemplo un único identificador del sistema operativo o el hardware o la tarjeta de red, y una combinación de estos, etc.) Los tres métodos anteriormente citados están basados en una única identificación de los dispositivos y la suposición de la posesión física de éstos.

Volviendo a las credenciales menos tangibles "algo que tienes/posees", una clave par pública y privada guardada en el disco duro del ordenador y protegida por, por ejemplo el sistema operativo es un ejemplo de un software basado en las credenciales. Sin embargo, todas las plataformas de ordenadores actualmente no son inherentemente seguras, y hay un considerable riesgo en la práctica, por ejemplo, la escucha informativa ilegal en el uso del teclado, en la información mostrada, en los documentos almacenados, etc. Estos riesgos no pueden ser efectivamente mitigados en los medios de software diarios sin restricción del uso cotidiano del ordenador al que estamos acostumbrados.

Por tanto, para los entornos normales de la informática y para las aplicaciones sensibles de seguridad, normalmente es mejor incorporar los elementos que son realmente importantes desde el punto de vista de la seguridad con fines distintos, ambiente de informática endurecido, diseñado especialmente para cada uso. A medida que los sistemas son más pequeños, pueden llegar a ser más rentables y convenientes, así que echaremos un vistazo de cerca en el extremo más pequeño en la gama de estos sistemas.

Un grupo muy distinto de estos dispositivos son los llamados hardware OTP tokens. Algunos de estos dispositivos son similares a los mensajes de texto de los teléfonos móviles o el bloc de notas OTP en el sentido de que muestran el número que el usuario tiene que escribir en el sistema de autentificación (por ejemplo, RSA's SecureID o Vasco's Digipass).

Figura 3 Un hardware OTP token (Vasco's Digipass)

Sin embargo, hay también hardware OTP tokens que se conectan a un ordenador y automáticamente envían el OTP necesario al ordenador a través del Puerto USB cuando la autentificación sea requerida.

Figura 4 Un hardware diferente basado en OTP (Yubikey)

Al final de la escala están estos sistemas en chip o microcontroladores. Si estos microcontroladores se ponen en un formato de tarjeta, los llamamos **tarjetas inteligentes** (22) (cuando se usan en teléfonos móviles para propósitos de identificación definidos en los estándares GSM, las tarjetas inteligentes se llaman tarjetas SIM). Desde luego, no tiene importancia si el chip se integra en una tarjeta de plástico o no, ni si cada chip de seguridad se integra directamente en los dispositivos móviles como teléfonos o tabletas (23). Incluso las tarjetas microSD insertadas en ranuras de memoria estándar de teléfonos o tabletas menos avanzados, pueden proporcionar estos elementos llamados seguros. Los chips cifrados en estos elementos seguros (incluso en tarjetas microSD (24)) son capaces de crear una firma digital, así que realmente no hay diferencia material entre los chips de tarjetas inteligentes y estos dispositivos más orientados a móviles.

No importa cómo de seguros sean estos dispositivos, requerir **dispositivos separados** para propósitos de seguridad **incrementa los costes y disminuye la tasa de adopción.** También tenemos que tener en cuenta que en el presente la mayoría de estos elementos de seguridad son **dispositivos de un solo propósito**. Por tanto, la posesión de un dispositivo de seguridad hace que sea menos probable que un usuario esté dispuesto a comprar el siguiente (si tiene alguna elección), y menos probable llevar el dispositivo con él donde quiera que vaya. Cuanto más costosos y voluminosos sean los dispositivos, más serio llega a ser el asunto.

Esto ocurre cuando la conectividad y la interoperabilidad de las credenciales llega a ser muy importante y este es un factor que CCBE debería tener en cuenta muy seriamente cuando decida sobre apoyar a ciertas tecnologías.

Creemos que es una prioridad máxima elegir elementos de seguridad de confianza que pueden ser usados para tantos propósitos como sea posible y esto es por lo que elementos de seguridad existentes en los dispositivos móviles son una forma de avanzar más que las tarjetas inteligentes que requieren lectores de tarjeta especiales.

---

(22) A veces los chips que proporcionan solo memoria pasiva también se llaman tarjetas inteligentes, pero nosotros no lo consideramos esto como inteligente, no tienen capacidad informática.
(23)TazTag,Tazpad,http://www.taztag.com/index.php?option=com_content&view=article&id=104:tazpad&catid=38:slideshow
(24) Incluso las tarjetas microSDs son originariamente un dispositivo de sólo memoria, el chip de seguridad dentro de ellos puede ser capaz de hacerlo , por ejemplo,
http://www.oberthur.com/get_downloadsection_file.aspx%3Fid%3D355&sa=U&ei=mSoDT7jYKIXP4QSN3syNCA&ved=0CA8QFjAA&usg=AFQjCNGNLpNcC3vOtkkGxrQHbuYTpjDxcg

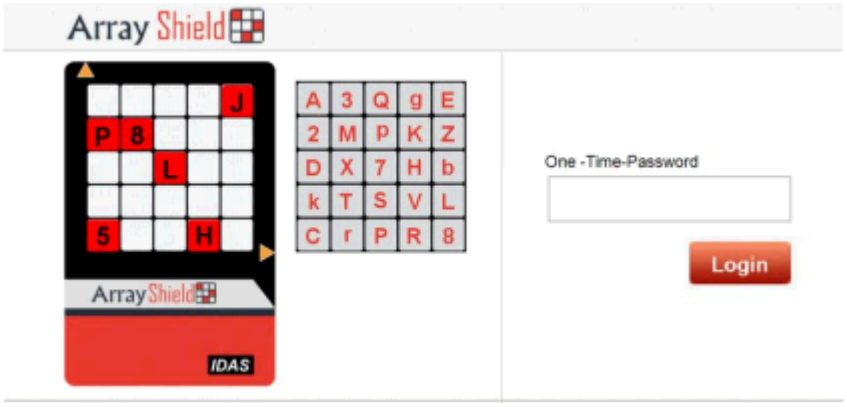


Figura 5 ejemplo OTP – ArrayShield

Posibilidades para una mayor interoperabilidad y la reutilización de dispositivos de seguridad

Si echamos un vistazo a la puntuación bruta de los chips de seguridad emitidos cada año, parece que actualmente el número de tarjetas SIM es el más alto: 4 millones de tarjetas SIM han sido enviadas a todo el mundo en 2010, se esperaban que fueran enviados 1 billón de pagos a través tarjetas con microcontroladores en 2011. En comparación: 190 millones eID con microcontroladores fueron vendidas sólo en Alemania en 2010 (25). Teniendo en cuenta el bajo porcentaje en los Estados Unidos de pago con tarjeta con microcontroladores y la necesidad de VISA y MarsterCard, el número de pagos con microcontroladores aumentará de corma significante en los próximos años (26). (no vemos un incremento parecido en la magnitud de eIDs emitido en los próximos años.)

Desafortunadamente, incluso si tenemos uno o dos chips de seguridad a nuestra disposición, ciertas circunstancias harán imposible usar este chip de seguridad por otros propósitos de los que tenían originariamente.

Las tarjetas SIM en nuestros teléfonos móviles sólo son accesibles a través del operador móvil, y la identificación a través de la tarjeta SIM siempre requiere su cooperación, y los operadores móviles siempre han retenido un gran sustento en esta infraestructura (27).

De forma similar, las tarjetas de pago con capacidades EMV (tarjetas de débito, tarjetas de crédito, etc.) sólo podrían usarse en relación a los términos y condiciones definidas por las asociaciones de tarjetas Visa y MasterCard (por ejemplo *Transacción Brand Value* según las normas de MasterCard (6.3. (28)) Quizás esto es necesario para asegurar la seguridad de los pagos, pero hasta ahora, nadie tenía una opción.

Esta situación puede verse como algunos atascos que plagan los dispositivos de seguridad de los móviles. Estos problemas pueden ser resueltos haciendo la interoperabilidad más deseosa para los que controlan estos atascos, o utilizando, dispositivos nuevos, más abiertos, o dispositivos bajo el control del gobierno.

---

(25) El Informe Anual de Gemalto 2010, ampliando los límites de Seguridad Digital, p. 15., disponible en: http://www.gemalto.com/investors/download/gemalto_ar2010_print.pdf

(26) Véase la resolución del Consejo Europeo de Pagos sobre el marco de la tarjeta SEPA, que introdujo en 2006 un plazo que desde el 1 de Enero de 2011, los bancos adquirientes pueden – y en muchos países de la UE, ya lo hacen – rechazan productos no compatibles con EMV (tarjetas de pago que no contienen un microcontrolador seguro)), http://www.europeanpaymentscouncil.eu/knowledge_bank_download.cfm?file=Cards SCF 006 09 v 2 1.pdf. Lo mismo se espera que ocurra en los Estados Unidos desde el 1 de Octubre de 2015, sólo para tarjetas VISA. http://corporate.visa.com/media-center/press-releases/press1142.jsp

(27) Esto es lo que hace posible que los operadores tomen un 40% - 50% de los pagos de los móviles en los que se identificó al usuario mediante la tarjeta SIM en Hungría.

(28)http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf&sa=U&ei=KZAZT7zA8XQsgbp8ahI&ved=0CBAQFjAA&usg=AFQjCNHil7tf9jYFzCZrBhwvYwV2UGC2Rg19/56

Los nuevos teléfonos móviles contienen frecuentemente elementos seguros independientes de la tarjeta SIM. Los fabricantes de teléfonos móviles incluyen sus capacidades en sus modelos de alta gama y algunos proveedores de sistema operativo para teléfonos inteligentes también están empezando a exigir esas capacidades en sus teléfonos.

Cuando se utilizan interfaces de radio de baja potencia, la interoperabilidad de los dispositivos de seguridad se hace más simple haciendo el formato físico del dispositivo que contiene el chip de seguridad menos importante y las transacciones basadas en estos dispositivos se hacen, al mismo tiempo, más rápido (un ejemplo para cada solución es el campo cercano de comunicaciones que puede mostrar el camino a seguir) (29).

NFC puede ser una posibilidad donde ni los operadores móviles, ni las asociaciones de tarjetas están en posición de controlar un atasco, y por medio de sus capacidades técnicas, están forzados a cooperar en este nivel también (si es realmente posible sin comprometer la seguridad de sus dispositivos) – si no cooperan, hay también controladores de NFC capaces de manejar múltiples chips, y hacer posible el uso del mismo dispositivo móvil para diferentes propósitos. (Véase Mastercard PayPass incorporado en teléfonos con capacidad "Google Wallet" y VISA payWave en microSD.) Sin embargo, NFC no está exenta de un desafío, y puede volverse un atasco en el futuro, por ejemplo, por medio de ciertas empresas que controlan las patentes clave necesarias para el uso de esta tecnología.

Incluso si el uso múltiple de los chips de seguridad está de alguna forma impedido por, tanto operadores móviles como asociaciones de tarjetas, eIDs con capacidad de chip de seguridad, emitidos por cierto MSs podría (debería) usarse también para la autentificación de los abogados. Esto podría significar tarjetas emitidas en Austria, Bélgica, Portugal, Alemania, Estonia, y a partir de 2012 Lituania, o pasaportes virtuales, o permisos de residencia de la UE electrónicos, tarjetas electrónicas para el registro de vehículos, etc.

4.2.4. Algo que eres

También conocido como biometría. Los únicos medios técnicos implicados en este factor es cómo la máquina lee el valor requerido del usuario, y se basan en la suposición de que algunas características de ciertas personas pueden ser medidas con mayor precisión que cómo estas características pueden ser forjadas a ese nivel de tecnología.

Tenemos que destacar que aunque algunas técnicas de biometría son capaces de identificar (no solo autentificar) directamente a las personas, este enfoque no sería aceptable fuera del alcance de la ley o dentro del ámbito forense. Si alguien empieza a usar la biométrica para la identificación de personas, estos datos serían válidos para casi toda la vida de una persona, sin posibilidad de revocarla, y podría haber sólo una credencial para cualquier persona biológica, que es culturalmente inaceptada en la mayoría de los países.

Sin embargo, la biométrica aún puede ser usada de forma efectiva para los propósitos de autentificación como a) sólo está conectado directamente a identificadores no biométricos de una persona y b) tanto tiempo como teóricamente sea posible para emitir identidades separadas múltiples para una persona biológica, y es posible para una persona biológica usar credenciales para la misma identidad. Como ya hemos mencionado, no es seguro basar una autentificación sólo en lo que el usuario posee, y sin recurrir a la biometría, códigos PIN y contraseñas, nunca podrían ser retiradas. Serían el único camino para asegurar el segundo factor requerido para la autentificación, y todos sabemos que cuantos más códigos PIN tenemos y contraseñas, tendemos a usar el mismo o a olvidar los diferentes códigos

Hay inconvenientes serios para la biométrica:

a) La mayoría de ellos necesitan una interfaz especial para humanos (a diferencia de los PINs, contraseñas), que es una barrera considerable para su adopción.

(29) Las ventajas de NFC en comparación con la conexión inalámbrica de Internet es principalmente la simplicidad de la comunicación. La comunicación a través de la conexión inalámbrica a Internet requiere mucha más energía y potencia informática, con muchas más capas de protocolos y servicios posibles a tener en cuenta, que lo que es necesario para dos microcontroladores para comunicarse entre ellos a través de NFC. La baja potencia de las comunicaciones de NFC lo hace más seguro en el sentido de que el usuario puede estar seguro de que estas comunicaciones entre máquinas sólo ocurrirá dentro de una distancia corta.

Hay inconvenientes serios para la biométrica:

a) La mayoría de ellos necesitan una interfaz especial para humanos (a diferencia de los PINs, contraseñas), que es una barrera considerable para su adopción.

b) Las tecnologías que se usan para la biométrica varia mucho en función de su efectividad (falsa tasa de aceptación y falsa tasa de rechazo), y la correspondiente seguridad que ellos proveen, con qué facilidad es posible falsificar uno u otro, con que frecuencia ciertas características cambian con el tiempo o con la situación (condiciones médicas), qué facilidad hay para obtenerla por otros medios (huellas dactilares, fotos de alta resolución del iris y de la cara, no podemos mantenerlo en secreto). En cuanto a la efectividad de ciertas tecnologías, es muy difícil verificar de forma fiable las reclamaciones del proveedor, y por tanto, hay un gran riesgo de que ciertas suposiciones no se harán realidad a largo plazo.

c) Hemos mencionado la imposibilidad de revocar la biometría, así que si cualquiera de los supuestos fallan como hemos escrito anteriormente, es posible que toda la infraestructura de la biometría, incluyendo los lectores caros, tengan que ser reemplazados.

d) también es importante que la biometría puede usarse sin ser consciente de hacerlo, por lo que no es necesariamente lo mismo que dar un PIN, que sabemos que actualmente estamos dando un consentimiento para ser autentificados. Por ejemplo, el reconocimiento del iris trabajar del mismo modo que una verificación de "campo cercano" como NFC con dispositivos de hardware de seguridad, incluso de metros de distancia (pero esto puede resolverse teóricamente al exigir ciertos requisitos complementarios biométricos, por ejemplo, gestos o palabras que pueden ser consideradas como aprobaciones.)

En resumen, el uso de técnicas biométricas no está todavía totalmente madurado. Incluso si hay resultados prometedores con, por ejemplo, reconocimiento a través del iris (30), y tenemos ya varios lectores de huellas para los usuarios finales, podemos esperar que los PINs y las contraseñas se utilicen para los próximos años. Pero es una tendencia clara que la biométrica se incorpore en los dispositivos móviles y podría llegar a ser un sustituto para al menos algunos de los códigos PIN que usamos (31).

4.2.5. Tendencias genéricas de la Tecnología de la Información que afectan al futuro de las credenciales de autentificación

Mientras proporcionen una visión general de las tecnologías de autentificación actualmente disponibles, también hemos mencionado alguno de los cambios esperados, véase la descripción de NFC y el uso de la biométrica.

Si intentamos ver los cambios esperados en este área de tecnología, no es suficiente ver el futuro desde la perspectiva de la industria, también tenemos que tener en cuenta las tendencias generales de la industria de tecnología de la información. Las tendencias de la Tecnología de la Información genérica se deciden por los efectos que actualmente se ven a largo plazo, fuerzas estratégicas que dan forma a la industria de Tecnología de la Información. Por ejemplo si las tabletas son una fuerza estratégica porque cambian dramáticamente UI con el usuario y en una considerable tasa de adopción – pero las tarjetas inteligentes con lectores especiales no encajan del todo en esta dirección estratégica, así que cuando se apoyan a las tarjetas inteligentes, tenemos que tener esto en cuenta ya que pueden inhibir el uso de las tabletas mediante los abogados y el uso de un único dispositivo de seguridad para los abogados en múltiples propósitos.

---

(30) http://www.theregister.co.uk/2001/05/18/iris_recognition_is_best_biometric/

(31) Véase Gemalto Pasaportes Electrónicos, p. 32.; http://www.oberthur.com/press_page.aspx?id=383&otherid=112&menuId=182&divisionId=0, Tecnologías Oberthur y AuthenTec Team Up para demostrar el acceso por huella digital habilitada para servicios basados en NFC, disponible en: http://www.oberthur.com/press_page.aspx?id=383&otherid=112&menuId=182&divisionId=0

Para identificar las fuerzas estratégicas, hemos usado las observaciones clave de la encuesta estratégica Gartner 2012 (32), así como informes anuales de los proveedores líderes en el mercado del mercado de los chips de seguridad (33).

Dentro de las 10 mejores tecnologías de 2012 por Gartner, cinco estrategias podrían tener un impacto considerable en las tecnologías de autentificación y el uso de las credenciales "Tabletas y más allá", "Aplicaciones móviles e Interfaz", "experiencia de usuario contextual y social", "computación en nube" e "Internet de las cosas". A continuación, echaremos un vistazo más de cerca a cada una de ellas.

a) "Tabletas y más allá" y "Aplicaciones móviles e Interfaz",

En cuanto a Tabletas y más allá, Gartner ha resaltado que "los usuarios pueden elegir entre varios factores formales en lo que respecta a la computación en móvil", "debería esperar para gestionar un entorno diverso con dos a cuatro clientes inteligentes hasta el 2015", "los empleados que traen sus propios teléfonos inteligentes y tabletas al lugar de trabajo". En cuanto a las Aplicaciones móviles e interfaces, el mensaje clave importante para CCBE es que con ventanas, iconos, menús y punteros serán reemplazados por interfaces de teléfonos móviles".

Tenemos que enfatizar que no sólo se espera que el número de teléfonos inteligentes vendidos aumente en los próximos años, pero su tasa de incremento acelerará y también se espera que ni el ordenador de mesa ni el portátil sea el dispositivo de computación personal más ubicuo en el futuro cercano.

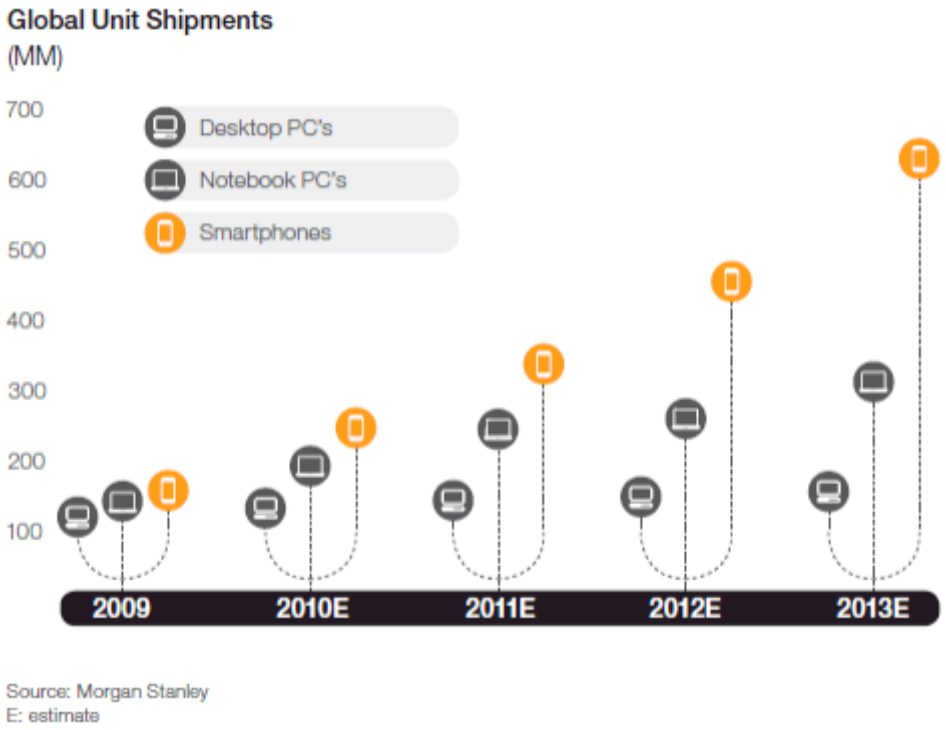


Figura 6 Gráfico esperado de envío de unidades globales (34)

(32) Gartner Identifica las 10 mayores tecnologías estratégicas para el 2012, http://www.google.hu/url?q=http://www.gartner.com/it/page.jsp%3Fid%3D1826214&sa=U&ei=dfUXT7LnNoTP4QSsx5TsDQ&ved=0CBcQFjAA&usg=AFQjCNGqctNH8hbBLq3Icg_MPQlhGup8Lw
(33) Gemalto op. cit.; Giesecke & Devrient Informe Anual 2010, Preguntas//Respuestas, Mercados//Soluciones, disponible en: http://www.gi-de.com/gd_media/media/en/documents/brochures/corporate/AnnualReport_2010.pdf;Oberthur Informe de la actividad de las tecnologías de 2010, http://www.oberthur.com/UserFiles/File/Activity%20Report/OT_AR2010_Locked_UK.pdf
(34) Gemalto Informe Annual de 2010, extendiendo los límites de la Seguridad Digital, p 15.

Esto también tendrá un impacto sobre como la gente usará los ordenadores en sus lugares de trabajo, y con la expansión de los teléfonos móviles, la solución de seguridad utilizable en la plataforma de los teléfonos inteligentes también se expandirá. Si esto es así, las expectativas de los usuarios van a ser que va a ser más fácil utilizar las soluciones seguras de los teléfonos móviles en otras plataformas de computación, por ejemplo, identificando a ellos mismos para los propósitos de e-CODEX. Se puede esperar que los usuarios prefieran usar los teléfonos inteligentes basados en soluciones de seguridad a las soluciones actuales de tarjetas inteligentes que requieran lectores separados.

b) Experiencia contextual y social del usuario

Como Gartner ha dicho "Un sistema contextualmente preocupado anticipa las necesidades del usuario y de forma preactiva sirve el contenido más apropiado y a gusto del usuario" basado en el entorno del usuario, conexiones, etc.

Un sistema contextualmente preocupado podría hacer más simple la autentificación si, por ejemplo, la localización del usuario se tiene en cuenta como un factor secundario, o en caso de dudas, la información de contexto social se usa para la verificación, la denominada autentificación social. (por ejemplo, si un usuario se conecta a partir de un nuevo dispositivo no utilizado anteriormente, el usuario tiene que reconocer algunos de sus supuestos amigos (35)). Los sistemas contextualmente preocupados podrían también emitir una credencial más simple o más segura. Esta fuerza estratégica podría tener un efecto más diferente en cuanto a la autorización, la autorización se basará en las mismas fuentes de datos que se usen para el contexto.

En cuanto a la experiencia social del usuario, Gartner ha mencionado que "las aplicaciones asumen las características de las redes sociales". También podemos esperar a largo plazo, que poco a poco los servicios de los gobiernos virtuales sean proporcionados directamente a los usuarios de las redes sociales, es decir, que los gobiernos renuncien a la gestión de su propia identidad en ciertos dominios y acepten las aseveraciones de las redes sociales a través de los mecanismos de autentificación de la red social. Sin embargo, esto depende fuertemente de los mecanismos de seguridad que la red social usa, y estos son, por el momento, no tan fuertes como requieren los servicios más seguros del gobierno virtual (36).

Si los gobiernos aceptaran la identificación a través de las redes sociales, y las redes sociales continúan fortaleciendo los requisitos de la autentificación y más extensamente aceptan, por ejemplo, elementos de seguridad en teléfonos móviles como credenciales, esto acelerará más los cambios mencionados en relación a "Tabletas y más allá".

c) Internet de las cosas

Lo más destacado de Gartner en cuanto al Internet de las cosas es que "*más y más dispositivos estarán conectados a otros a través del canal común de Internet, y […] que estas tecnologías alcanzarán una crítica colectiva y un momento económico crítico sobre los próximos años*". Las técnicas mencionadas por Gartner son sensores integrados, NFC y reconocimiento de imagen.

En cuanto a las tecnologías de autentificación (y también autorización), los sensores integrados y el reconocimiento de imagen, jugará el mismo papel que hemos descrito en conexión con los sistemas contextualmente preocupados. Otros efectos esperados de IoT ya han sido descritos en 4.2.3 y 4.2.4, que es, en relación a NFC y la biometría.

d) Computación en nube

La entrega más generalizada de la computación como un servicio más que como un producto, también significa un cambio de "seguridad fronteriza". En la seguridad fronteriza, alguna seguridad de la autentificación se basa en factores físicos, como podrías acceder a un sistema desde una sala específica o desde un ordenador específico, y la entrada a éste último fue precedida por mecanismos fiables de control de acceso.

(35) http://www.facebook.com/blog.php?post=486790652130

(36) Hay un mensaje de texto basado en dos factores de autentificación para Facebook en ciertos países, por el momento, https://blog.facebook.com/blog.php?post=10150153272607131

Sin embargo, usando la computación en nube, más equipamientos distintos y localizaciones serán utilizadas para acceder a los mismos servicios, y esto también fortalece los requisitos de la "identidad basada en la seguridad".

Así, la computación en nube también hace a la identificación y a la autentificación más frecuente de lo que realmente es, y refuerza los problemas actuales con la autentificación: mayor insatisfacción al tener que usar los PINs y contraseñas, para requerir a los usuarios que tengan diferentes dispositivos de seguridad que tengan acceso a diferentes identidades, y más riesgos usando los mismos PINs y contraseñas.

4.2.6. La guía e-CODEX y STORK en relación con la autentificación

En este capítulo, examinamos los resultados de LSPs e-CODEX y STORK hasta ahora, y vemos como estos instrumentos impactan en las elecciones de CCBE, y cómo podemos tomar los resultados de LSPs en cuenta cuando se proporciona una visión general de las tecnologías.

e-CODEX

Desde la perspectiva de CCBE, LSP e-CODEX parecían tener el mayor impacto y más directo en los procedimientos electrónicos de los abogados a través de la UE, e-CODEX sólo tiene importancia indirecta en cuanto a que la tecnología de autentificación debería apoyar CCBE.

La razón para esto es que en la etapa actual (37), e-CODEX sólo se vuelve a referir a STORK en cuanto a las técnicas de autenticación aceptables (38): *"Debido al hecho, de que no hay solución nacional existente que pueda ser cambiada, actualmente solo hay STORK que proporciona una solución adecuada para una autentificación transfronteriza."* Por tanto, la única contribución de e-CODEX en el presente estado, es la lista de procedimientos electrónicos que tenemos que tener en cuenta para encontrar las propias técnicas de autentificación, donde los abogados participarán de forma electrónica. De la lista de los procedimientos electrónicos aplicables (piloto esperado) de e-CODEX (39), las siguientes deberían ser de principal interés para los abogados, y de este modo, a CCBE:

a) Regulación (EC) 861/2007 del Parlamento Europeo y del Consejo de 11 de Julio de 2007 que establece un procedimiento europeo de Reclamaciones de Menor Cuantía (*"procedimiento de menor cuantía*") (40);

b) Regulación (EC) 1896/2006 del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 que crea un Proceso Monitorio Europeo ("*EPO*") (41);

c) Decisión Marco del Consejo 2002/584/JHA relativa a la orden de detención europea ("*EAW*").

La seguridad requerida del servicio de autentificación depende del riesgo de identidad que no es de confianza en el procedimiento electrónico, y por tanto usamos el método de gestión de riesgo. STORK define un método de evaluación de riesgo, así que después de introducir los resultados de STORK, volvemos a analizar los requisitos de estos procedimientos de gestión de riesgo más tarde.

---

(37) Hemos tenido en cuenta los últimos entregables recibidos de CCBE en cuanto a e-CODEX, por ejemplo D10.2 Finalización de Requisitos y Descripción de Escenarios de Prueba, pero de conformidad con el email de Peter Homoki de 11/01/2012 17:43 a Alonso Hernández-Pinzón y su respuesta, e-CODEX WP no ha cubierto todavía el asunto de identificación y eIDs, y por tanto tampoco el de la autentificación, sólo el uso de la firma electrónica. Antes de cerrar este informe, no hemos recibido más entregables de e-CODEX en este asunto.
(38) Sección 5.1.2 del entregable D 4.1 Identidad virtual: Inventario y requisitos de los documentos, http://www.e-codex.eu/index.php/downloads2/category/1-deliverables?download=3:d41, p. 45. Véase también la Sección 3.7.2. del Entregable D7.1 Gobierno y Definición de Directrices, http://www.ecodex.eu/index.php/downloads2/category/1-deliverables?download=1:deliverable-71, p. 32.
(39) Apéndice III del Entregable D7.1., op. cit., p. 89.
(40) OJ L 199, 31.7.2007, p. 1-22.
(41) OJ L 399, 30.12.2006, p. 1-32.

Sin embargo, tenemos que llamar la atención en el hecho de que también hemos leído algunas comunicaciones molestas desde el grupo de e-CODEX sobre cómo ellos imaginan actualmente el trabajo de la identificación. Por tanto tiempo como la identificación de los abogados sea exclusivamente llevada a cabo sólo por MSs (y no según el llamado modelo STORK completo) (42), hay también un riesgo considerable de que los abogados y colegios de abogados no tengan mucha s opciones en las tecnologías utilizadas, sólo para elegir desde el menú proporcionado por su host MSs, que limitará la interoperabilidad transfronteriza.

STORK

El alcance de STORK fue limitado para proporcionar un marco transfronterizo para tantas soluciones de autentificación nacional como fuese posible. Por tanto, el resultado de STORK incluye una descripción del software necesario, protocolos y marco arquitectónico, pero no excluye los procesos de autentificación de baja seguridad, y *no hace recomendaciones para evitar ciertos tipos de credenciales que proporcionen baja seguridad.*

En STORK, las credenciales solo fuera analizadas con la visión sobre cómo las recomendaciones del protocolo y del marco afectan a la elección de las credenciales – y en este aspecto, STORK ha demostrado que las soluciones proporcionadas por STORK están de acuerdo con estas especificaciones relativas a las credenciales.

Por tanto, STORK por si mismo no afecta directamente a la elección de CCBE en el apoyo a ciertos tipos de credenciales para abogados. Sin embargo, STORK contiene una "calidad del modelo de seguridad de la autentificación", que es, un modelo para evaluar qué tipo de tecnologías podrían ser evaluadas como más seguras que otras. Las provisiones de la autentificación dentro de la nueva regulación que se espera que reemplace la directiva 1999/93/EC, se rumorea que está basada en STORK, por tanto este modelo en STORK afectaría a las decisiones de CCBE.

El modelo de seguridad de la autentificación de STORK (Entregable D2.3 – esquema autentificador de calidad (44) define un "STORK a nivel QAA". En nuestra opinión esto debería haberse llamado algo como "nivel de seguro requerido basado en los riesgos del procedimiento" y un diferente nivel debería haber sido formulado para el nivel que es el resultado de los procesos de evaluación. Es confuso que ambos niveles, el requerido y el final (actual) se llame STORK QAA. Esto podría ser una razón para el hecho de que las directrices para la evaluación del riesgo de impacto en STORK estén menos detalladas que la propuesta IDABC (45), o de los Estados Unidos OMB M4-4 (46). Desde la perspectiva de un abogado, tenemos que admitir que el OMB M4-4 se usa más que la propuesta IDABC, porque en STORK QAA y en la propuesta IDABC, no hay guías detalladas con respecto a requerir el procedimiento de "alta seguridad", si se causa algún posible riesgo de daño personal al afirmar falsamente una entidad se considera necesaria una "alta seguridad". (La propuesta IDABC fracasa al dar cualquier guía de correlación entre la "escala de gravedad de impacto" y diferentes tipos de daños, y es sólo en OMB M4-4 donde hay específicas guías que muestran que los riesgos, por ejemplo, la seguridad personal, debería tomarse en cuenta de forma más seria en clasificaciones de impacto que por ejemplo, de la confidencialidad o la pérdida financiera.)

---

(42) Véase MW y modelos PEPS en STORK, https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577.
(43) Véase trabajo STORK asunto Item 3.2.3 Tarjeta de ciudadanía Europea, https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1396, trabajo STORK asunto 3.2.2 tarjetas de información, https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1395, Trabajo STORK asunto 3.3.3 RFID y NFC https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1382.
(44) https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577
(45) Interoperabilidad de eID para PEGS – Propuesta para un mecanismo de autentificación a múltiple nivel y mapa de existentes mecanismos de autentificación, Deciembre de 2007, http://ec.europa.eu/idabc/servlets/Docbf72.pdf?id=29622
(46) Véase la Tabla 1 en la Oficina Ejecutiva del Presidente, Oficina de Gestión y Presupuesto: Memorándum a los Directores de todos los Departamentos y Agencias, 16 de diciembre de 2003, M-04-04, Guía de autentificación virtual para las agencias federales, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf, p. 7.

Para la ilustración y porque usaremos este QAA en secciones posteriores de este informe, citamos dos tablas de STORK D2.3 debajo (tabla 1 y tabla 12 en STORK D2.3):

Riesgo basado en el nivel requerido de seguridad (niveles STORK QAA)	Descripción
1	No/poca seguridad
2	Poca seguridad
3	Seguridad importante
4	Alta seguridad

Tabla 1 Niveles QAA exigidos

Niveles de evaluación basados en los resultados de la evaluación:

		Niveles de seguridad para la fase de autentificación electrónica			
		EA1	EA2	EA3	EA4
Niveles de seguridad para la fase de Registro	RP1	STORK QAA Nivel 1	STORK QAA Nivel 1	STORK QAA Nivel 1	STORK QAA Nivel 1
	RP2	STORK QAA Nivel 1	STORK QAA Nivel 2	STORK QAA Nivel 2	STORK QAA Nivel 2
	RP3	STORK QAA Nivel 1	STORK QAA Nivel 2	STORK QAA Nivel 3	STORK QAA Nivel 3
	RP4	STORK QAA Nivel 1	STORK QAA Nivel 2	STORK QAA Nivel 3	STORK QAA Nivel 4

Tabla 2 Niveles de evaluación QAA

La composición de los niveles de evaluación en STORK es la siguiente (de la figura 2 de STORK D2.3):

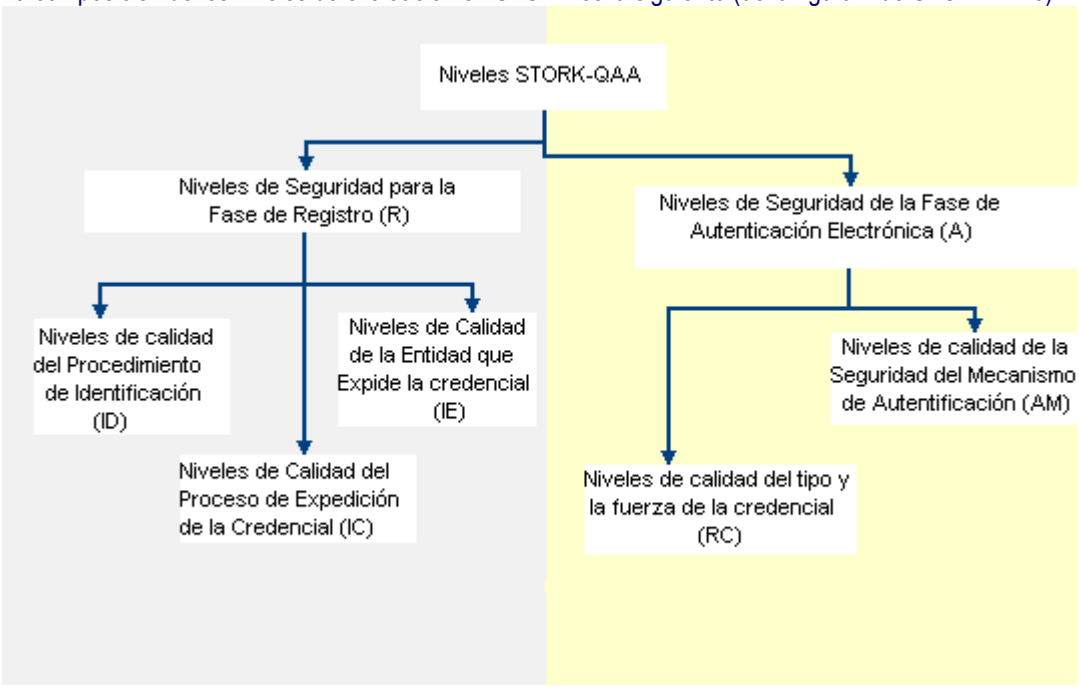


Figura 7 Composición de Niveles de evaluación QAA

Para incorporar los resultados de STORK e E-CODEX en este informe para proporcionar una vista general de las tecnologías, no vemos necesario explicar (repetir) los elementos individuales de la composición del nivel de evaluación.

Por tanto, solo analizaremos lo que los niveles QAA requieren como autenticación para los procedimientos pilotos de e-Codex, y qué tecnologías cumplirían esos requisitos.

Teniendo en cuenta la definición mínima de "seguridad nula o mínima" de STORK D2.3, es claro que la autentificación no será adecuada para los propósitos de e-CODEX. Teniendo en cuenta que en el caso de un robo eID, una persona podría ser también detenido ilegalmente, también es claro que se requiere un nivel bastante alto de seguridad en el caso de *EAW*, probablemente *QAA nivel 4*.

Por tanto, la única cuestión que queda es si:

a) *QAA nivel 3* es suficiente para *EPO y Procedimientos de Menor Cuantía*; y

b) Debería haber alguna *diferencia entre EPO y Procedimientos de Menor Cuantía*, por ejemplo QAA de nivel 3 del Procedimiento de Menor Cuantía (teniendo en cuenta el límite del valor envuelto en este procedimiento) y el nivel 4 para EPO, o nivel 2 para los Procedimientos de Menor Cuantía y el nivel 3 o 4 para EPO. En vista de lo anterior, exploramos lo que significaría que prescriba cada nivel QAA para una solución de autenticación dada:

a) QAA de Nivel 4
Para cumplir con el nivel 4 de QAA, la credencial ha de ser un *certificado cualificado e incluido en un dispositivo de hardware* (pero este dispositivo de hardware no es necesariamente un dispositivo seguro de creación de firma, RC4). Para proveer a este nivel, también tenemos que echar un vistazo al protocolo de autenticación (AM4, EAL4+ o superior de CC), pero *este aspecto no está afectado por las credenciales usadas,* sólo con mirar la solución total de la autentificación, de principio a fin.

b) Nivel 3 de QAA
Este nivel también está realizado por *certificados de software* (independientemente de ser cualificado o no), no SSCD basado en certificados de hardware y por cualquier tipo de contraseñas una vez provisto el instrumento. (RC3).

La entidad que emite la credencial debería estar sujeta a la acreditación del gobierno o supervisión (IE3). Hay una posibilidad de emitir una credencial sin la presencia física del sujeto para la verificación. La condición previa para la no presencia física está vagamente definida en STORK D2.3, por lo que no se recomienda el apoyo a esta versión. (Basado en la versión de registro en línea de ID3, en este tipo de registro online, la firma digital de cualquier tipo de CSP sería suficiente para la validación, y con independencia de cualquier tipo de mecanismo de seguridad usado o no en la firma digital subyacente (47)). Sin embargo, si una credencial fue emitida sobre la base de un certificado cualificado previamente expedido, entonces la nueva credencial emitida puede ser aceptada al correspondiente nivel sin registro separado.

Después de la creación de la credencial, podría ser tanto (a) enviado por correo certificado a la dirección oficial de la entidad (siempre que sea una "dirección oficial" en el Estado Miembro), o (b) poner a disposición para su descarga, una contraseña física que se de previamente al demandante (IC3).

c) Nivel 2 de QAA
En este nivel, incluso una *contraseña sencilla es suficiente para los propósitos de autentificación,* cuando las medidas se hayan tomado para asegurar la fuerza de esta contraseña (por ejemplo, una longitud mínima y complejidad).

Registro sin presencia física también es posible y no sólo basado en un certificado previo, sino en una simple comprobación de ciertos datos introducidos (por ejemplo, enviando un número de pasaporte y verificar en una base de datos si ese número de pasaporte corresponde a otra identificación personal de datos ya presentada). (ID2).

(47) Op. cit. p. 20 (iii) (e).

Después de crear la credencial, puede ser simplemente descargada de un enlace enviado a una dirección de correo electrónico durante el proceso de registro (IC2).

Basado en la información anterior, parece que el nivel 2 de QAA por sí mismo podría no ser suficiente incluso para los Procedimientos de Menor Cuantía, y podría requerir más fuerza al menos en la relación con el proceso de registro para ser aceptable) (requisito ID3 e IC3, con contraseña fuerte de sólo en nivel RC2). Refuerzos similares podrían requerirse para EPO si el nivel 3 de QAA es para que sea aceptado (IC4 y/o ID4). No se requieren credenciales más fuertes hasta que el proceso de registro dé el correspondiente seguro.

Nuestra conclusión en este aspecto es el siguiente:

a) Es factible aceptar incluso soluciones de contraseñas fuertes en Procedimientos de Menor Cuantía (sobre la condición de que el procedimiento de registro en sí mismo es más fuerte que el requerido básicamente para el Nivel 2 de QAA);

b) EAW requerirá certificados cualificados incluidos en un dispositivo de seguridad de hardware, sin tener en cuenta si estos dispositivos son dispositivos seguros de creación de firma o no;

c) Un certificado de software o un hardware OTP token tendrá que ser emitido para su uso con EPO, o esto podría ser sustituido mediante el uso de cualquier otro hardware más fuerte basado en token a la disposición de los abogados (ya sea basado en una tarjeta inteligente, un teléfono móvil o una tableta con elementos seguros de chip activo).

4.2.7. Un menú como resumen de las posibles opciones de autenticación.

CCBE claramente quería tener un menú como resumen de las opciones de autenticación disponibles. Por favor, tenga en cuenta que la mayoría de los rankings a continuación son sólo estimaciones, no hay coste total exacto de los cálculos de propiedad llevados a cabo (48)

Como hemos mencionado anteriormente, es muy difícil dar una vista general significativa de, por ejemplo, todos los tipos posibles de hardware en que se basan OTPs y todos los posibles hardwares en que se basan los certificados X.509. Por tanto, en cuanto a ciertas técnicas, tenemos que dar dos resultados (1-2, 2-3, 3-4, 4-5).

Tecnica	Ranking TCO para la vida completa de la credencial (El más bajo€ = 5) (1-5)	Ranking de tiempo de vida esperado (más corto = 1) (1-4)	Nivel de Seguridad (más bajo = 1) (1-5)	Ranking de Facilidad de Uso incluyendo cómo los abogados de la UE son familiares con él. (poco familiar=1) (1-3)	Nivel de QAA que puede encontrarse con esta credencial (1-4)	Comentarios
Contraseña fuerte	4	1	1	3	2	Aunque son usados frecuentemente, loas contraseñas fuertes no son fáciles de usar (son seguras o fáciles de usar)
Ventanilla única (Unique Grid)	2	2	2	1	2	e.g. ArrayField
Bloc de notas con las claves de acceso de una vez	5	2	1-2	2	2	
Tokens basados en la identificación de ordenadores	4	4	2	1	2	
Mensajes de teléfonos móviles basados en OTP	3	4	3	3	2	Cuanto más se use esta solución, más cara llegará a ser.
Hardware basado en OTP	3	2-3	3	2	2	
Software solo de certificado X.509	5	2	2-3	2	3	La seguridad depende en gran medida del proveedor del servicio de certificación usado y en su práctica. El punto crítico en la seguridad es sin embargo, la protección de la clave privada en el dispositivo del usuario final. Si esta es una plataforma de confianza, la seguridad sería casi la misma que para los certificados X.509 basados en HW.
certificados X.509 basados en HW (para autentificación o firma)	1-2	3	4-5	2	4	Buenas oportunidades para la interoperabilidad en 5 años: a este nivel de generalidad (por ejemplo, sin requerir, por ejemplo, tarjetas inteligentes), la definición de esta credencial parece ser la prueba más futura. Si reusamos las credenciales se llegará a que sea posible , esta podría llegar a ser una solución considerable más barata.
Credencial en 1999/93/EC SSCD	1	3	5	3	4	Es possible que los chips de seguridad futuros usados en las comunicaciones NFC no serán certificados como SSCDs y esto podría poner en peligro la reutilización de las credenciales existentes de los abogados. Si los chips usados en las comunicaciones NFC pueden ser utilizados y certificados como SSCD, Entonces esto podría llegar a ser una solución más barata considerable.

Tabla 3 Perspectiva de las Tecnologías de autentificación

---

(48) Estos cálculos habrían dependido de escenarios de uso específico y ofertas de producto, que no era posible dentro del marco de un mes para el analisis.

Intentaremos dar más orientación en cuanto a las sugeridas tecnologías de autentificación, pero en estas recomendaciones, también intentaremos tener en cuenta tanto las posibilidades de CCBE (capítulo 5) como las respuestas de los Colegios de Abogados (capítulo 6).

4.3. Una visión general de alto nivel de la autorización (ser abogado, tener el mandato de un cliente etc.)

Tras una fundación terminológica, estaremos mirando a los problemas específicos de la autorización transfronteriza relativa a los servicios de gobierno virtual, e introducir ciertos enfoques posibles a los medios técnicos de cada autorización, concretamente la Infraestructura de Gestión de Privilegios (PMI) basada en el standard X.509 y la Tarjeta Professional Europea.

Como mencionamos anteriormente, hay numerosos métodos sobre cómo podemos comprobar en un sistema de computación quién tiene derecho a llevar a cabo cada función (49). Radicalmente los diferentes métodos se usan para comprobar los derechos de acceso a ciertos archivos más que para comprobar los derechos de acceso a los servicios web para los usuarios autentificados, con requisitos de tiempo muy diferentes, mecanismos de revocación, etc.

Un enfoque usado frecuentemente para la autorización se basa en "bases de información de control de acceso" (50), donde el sistema comprueba los derechos individuales conferidos a ciertas entidades en las listas de control de acceso u otras matrices de acceso. Un enfoque diferente se basa en las "capacidades" de una entidad, lo que significa que la autorización depende sobre la posesión y presentación de ciertos tokens (parecido a las credenciales usadas en la autentificación.) (51).

4.3.1. Autorización transfronteriza de la UE en servicios de gobierno virtual

La unidad de eGovernment y la Dirección General de Sociedad de la Información de la Comisión Europea establecen en su hoja de ruta que MSs debería guardar guardar estas autorizaciones relativas a las complejidades dentro de sus fronteras y los Estados Miembros deberían proporcional todos los servicios online requeridos por dichas autorizaciones, incluyendo mandatos, etc. (52).

Sin embargo, sobre la base de las entregas en LSPs STORK, e-CODEX y DIM, parece que esta pregunta no se resuelve remitiéndolas a los Estados Miembros, es simplemente evitada.

Primero, hay un problema sobre que ¿un derecho invididual (A) conferido en un Estado Miembro Número 1, tiene significado efectivo en un Estado Miembro Número 2? Esto depende sobre cuántos derechos y roles son materialmente armonizados en los Estados Miembros. ¿Son esos derechos todavía lo mismo bajo una jurisdicción diferente? ¿Podemos decir que si los notarios públicos han de escriturar el acceso al Registro en el Estado Miembro Número 1 los notarios públicos del Estado Miembro Número 2 deberían tener el mismo acceso? Está claro que no pueden ser lo mismo, pero podemos considerarlos lo mismo para ciertas razones prácticas, que está, dentro de cierto contexto y dominio.

¿Podemos resolver este problema diciendo que los derechos serán definidos por el Estado Miembro donde se proporciona el servicio del gobierno virtual y que el principio de "trato nacional" y "no discriminación" de los usuarios de diferentes Estados Miembros resolverá los problemas pendientes?

---

(49) Véase la Sección 4.1.
(50) Véase la Sección 5.3.3.2 en X.800.
(51) Sección 3.3.12. en X.800: "capacidad: Un token usado como identificador de un recurso que su posesión del token confiere derechos de acceso al recurso"
(52) Un mapa para un marco eIDM panaeuropeo para el año 2010, p. 4. "Principios fundamentales para un sistema IDM panaeuropeo", Sección 4-5: "4. En cuanto al mandato /representación de las autorizaciones, cada Estado Miembro debería proporcionar los medios para gestionar las competencias de los usuarios identificados dentro de sus fronteras, desde el momento en que estas autorizaciones no están sujetas a la aprobación por o sobre la autoridad de otro Estado Miembro." "5. Cada Estado Miembro debería apoyar los mecanismos de identidad, competencia y mandatos, de validación en línea, si quieren proporcionar servicios eIDM".
http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

Nadie ha esperado que, por ejemplo, los principios de "libertad de bienes, personas y servicios" dentro del Tratado que establece la Comunidad Económica Europea de 1957 podría resolver todo el problema. Por tanto, nuestro punto de vista es que también sería ingenuo pensar que podemos dar un corte claro y una solución universal para *todos* los problemas de autorización en conexión con los servicios de gobiernos virtuales.

Esto no es solo una cuestión de tecnología, también depende fuertemente en el área del derecho afectada en el servicio transfronterizo y las soluciones previas. Por tanto no podemos esperar ninguna solución significante de LSP STORK, porque STORK es independiente de los procesos legales, que pretende ser una solución genérica. STORK Entregable D2.2 – "Informe sobre la interoperabilidad legal" (53) ha confirmado expresamente esto en cuanto a la manipulación universal de delegaciones y mandatos (54).

Lo que efectivamente puede tener por objetivo es armonizar el fondo técnico para ciertas autorizaciones específicas, por ejemplo, las autorizaciones necesarias en procedimientos cubiertos por el LSP e-CODEX. Si estas autorizaciones se manejan de la manera más flexible, más adelante, esto podría servir como base financiera y regulatoria para la infraestructura de la autorización en el futuro.

4.3.2. Autorización en e-CODEX

En cuanto a e-CODEX, la posición de CCBE es que "la identidad virtual de los abogados debería ser comprobada en las aplicaciones de justicia virtual transfronteriza y prueba del mandato del cliente que dependerá de los requisitos nacionales", (55) porque eso era lo que vino de las respuestas de los Colegios de Abogados Miembros, como se ilustra en las siguientes tablas 4 y 5 (66):

CASOS / **RESPUESTAS**	**CASOS CIVILES**: ¿Cree su delegación que un abogado debería tener que acreditar la identidad de abogado en procedimientos electrónicos transfronterizos civiles?	**CASOS CIVILES**: ¿Cree su delegación que un abogado debería tener que acreditar que ellos actúan por el cliente particular en cuanto a las materias concernientes a las reclamaciones electrónicas transfronterizas civiles?	**CASOS PENALES**: ¿Cree su delegación que un abogado debería tener que acreditar la identidad de abogado realizando representaciones en procedimientos electrónicos transfronterizos penales?	**CASOS PENALES**: ¿Cree su delegación que un abogado debería tener que acreditar que ellos actúan por el cliente particular en cuanto a las materias concernientes a los procedimientos electrónicos transfronterizos penales?
SI	16 Delegaciones	16 Delegaciones	16 Delegaciones	12
NO	0 Delegaciones	6 Delegaciones	0 Delegaciones	4
DESCONOCIDO	1 Delegación (Latvia)	0 Delegaciones	1 Delegación (Latvia)	1 Delegación (Irlanda)

Tabla 4 Respuestas en e-CODEX a la confirmación electrónica

(53) https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578
(54): Véase p. 37-38., 3.3.1.: Delegación, mandatos y representación son una gran parte de la ley civil que significa que puede haber diferencias significantes entre los estados miembros de la UE. También en el sector público podemos esperar significantes diferencias sobre cómo la representación se lleva por varios estados miembros. En algunos informes nacionales presentados pro los periodistas se abordan los aspectos de la representación. Más allá de esto no podemos sacar conclusiones definitivas sobre representación y delegación de eIDs.
(55) TEMA 7 - SP/PS 25-26.11.2011, e-CODEX actualizado por CCBE 10/11/2011, p.2.
(56) Op. cit.

CASOS	**CASOS CIVILES**: ¿Cuándo se clasifican documentos por	**CASOS CIVILES**: ¿Cree su delegación ¿Cuándo se clasifican	**CASOS PENALES**: ¿Cuándo se hacen representaciones a las autoridades	**CASOS PENALES**: ¿Cuándo se hacen representaciones a las autoridades

RESPUESTAS	primera vez ante un Tribunal (o similar), ¿los abogados tienen que acreditar su identidad de abogado en los casos civiles en su Estado Miembro?	documentos por primera vez ante un Tribunal (o similar), ¿los abogados tienen que acreditar que actúan por el cliente particular en cuanto a esta materia en procedimientos civiles en su estado miembro?	competentes por privara ver en nombre del cliente, tienen los abogados que probar su identidad como abogados en los casos penales en su país?	competentes por privara ver en nombre del cliente, tienen los abogados que probar que actúan por el cliente en particular en esta materia en casos penales en su país?
SI	4 Delegaciones	7 Delegaciones	7 Delegaciones	9 Delegaciones
NO	13 Delegaciones	10 Delegaciones	10 Delegaciones	7 Delegaciones
DESCONOCIDO	0 Delegaciones	0 Delegaciones	0 Delegaciones	1 Delegación (Irlanda)

Tabla 5 Respuestas de e-CODEX al papel en el que se basa la confirmación

Esta afirmación de CCBE contradice con la necesidad actual de e-CODEX publicada, que dice que *"estas cuestiones serán acordadas en una fase posterior del proyecto"* (57). Incluso esta frase en el entregable e-CODEX fue un resultado de la clara obligación de CCBE sólo por la necesidad de la identificación de los abogados como en el procedimiento electrónico (verificando sus capacidades como abogados).

Aparte de esta frase anterior, en cuanto a la autorización, e-CODEX sólo se refiere al PERMISO habitual como la posible base tecnológica para las fundaciones de la autorización ver e-CODEX D4.1 p. 45. http://www.e-codex.eu/index.php/downloads2/category/1-deliverables?download=3:d41. Tenemos que mencionar que este PERMISO habitual se basa en los certificados de atributo y los proveedores de servicios de certificación de atributos detallados en el siguiente capítulo.

Sin embargo el PERMISO habitual, no es en si mismo una solución a todas las preguntas, y no da ningunas directrices sobre a quién y qué fuente de autorización será.

Si el enfoque problemático de e-CODEX mencionado en la página 24 se utiliza, donde sólo los Estados Miembros proporcionan información en cuanto a la identidad de los abogados, entonces no habrá ninguna fuente única de autoridad sobre la validez de las licencias de abogados, pero cada Estado Miembro tiene que suplir esta información (incluso si eventualmente se basa en el registro central de los Colegios de abogados dentro de ese Estado Miembro).

Pero parece más eficiente tener una fuente única de autoridad. Esta fuente de autoridad tendrá que ser designada, y se necesitará que se de información regularmente a esta fuente. Un candidato posible es el "Sistema de Información del Mercado Interior" (IMI), incluso más si la Tarjeta Profesional Europea se utiliza ampliamente.

Pero también es posible que CCBE pudiera estar en la fuente de una posición autoritaria. Identificar a una persona como un abogado requiere datos de los Colegios de Abogados de CCBE. A partir de las respuestas al cuestionario adjunto a este informe, una gran mayoría de miembros de CCBE están dispuestos y capaces de proporcionar estos datos a CCBE. Algunos de los miembros de CCBE ya proporcionan esta información a CCBE. Algunos de los miembros de CCBE ya proporcionan esta información sobre casi 7x24 de las bases a CCBE, gracias a la disponibilidad actual de la base de datos Encuentra-Un-Abogado.

(57) e-CODEX D7.1 Definición de Gobierno y de Directrices, 5. Interoperabilidad organizativa – Requisitos legales, p. 40., 5.3.1.1, disponible en http://www.e-codex.eu/index.php/downloads2/category/1-deliverables?download=1:deliverable-71

En cuanto al otro atributo (autorización) de mandatos y representaciones, siguen faltando algunos bloques importantes de construcción.

Mientras los abogados puedan ser fácilmente identificados, para tener una prueba electrónica de algún mandato de un cliente, podría requerirse alguna forma de identificar y autenticar al cliente, con toda la infraestructura necesaria relativa para la posibilidad de revocar rápidamente el mandato. Esto es, tener una autorización robusta para el mandato del cliente, también necesitaremos una identificación robusta pero no sólo para los abogados, si no para todos los ciudadanos.

En algunos países, esto podría basarse en la identificación electrónica de los ciudadanos, pero en este momento, no podemos pensar en ninguna solución a nivel de la UE.

Una alternativa útil podría ser contar con uno o más terceros de confianza que podrían servir como una interfaz para los ciudadanos sin conexión a los servicios de gobierno electrónico: un notario público, una empresa de propiedad estatal, o incluso otro abogado que podría certificar que el mandato se dio por el ciudadano identificado. Pero en el momento actual, probablemente no podamos decir nada más que la Unidad de Gobierno virtual de la Comisión dijo: "Los Estados miembros tienen que proporcionar una solución para esto". (58)

4.3.3. Un certificado de atributo como base para la autorización

En el capítulo 4.1. hemos incluido dos métodos diferentes para usar el estándar X.509 para la autorización. Se trata de un uso directo del certificado de clave pública emitido para un abogado y para proporcionar un atributo especial diciendo que la persona identificada en el certificado es un abogado. Por ejemplo, en el campo del asunto, podríamos tener: T= "abogado", NÚMERO DE SERIE = "Budapesti Ugyvedi Kamara, número de registro: 16411", E = peter.homoki@homoki.net, CN = Dr. Homoki Péter, donde CN identifica el nombre civil del sujeto, T y número de serie y número de registro identifica al sujeto como un abogado.

Hay ciertos límites a este uso de certificado de clave pública X.509. Un límite es que cuanta más información pongamos en el certificado de clave pública, más difícil será crear un certificado unitario donde toda la información pueda leerse por todos los países interesados. Otro límite es que cuanta más información pongamos en el certificado de clave pública, más corta será la validez esperada. Si alguno de los datos adicionales en el certificado cambia, el certificado de clave pública X.509 por completo, ha de ser revocado y publicado con nuevos datos, y esto va a ser muy costoso sobre una base panamericana. Y si no revocamos el certificado debido a cambios en cierta información, las partes que lo reciban estarán menos dispuestas a aceptar el certificado de clave pública para certificar esta información adicional.

Para hacer frente a estos problemas, el organismo de estandarización de la Unión Internacional de Telecomunicaciones (Agencia Especial de las Naciones Unidas) ha aceptado una nueva (v4) versión para el estándar X.509 de 2001, donde además de la anterior Infraestructura de Clave Pública (ICP) y certificados de clave pública (CCP), una Infraestructura de Gestión de Privilegios (IGP) y **Certificados de Atributo ("AC")** también se regulan.

STORK D2.2 también confirma este enfoque: "ellos pueden querer *establecer un atributo a un nivel más alto de garantía que el ofrecido por la Identificación electrónica (por ejemplo, la dirección, e incluso nombre, presentado en una tarjeta inteligente que puede estar obsoleta (59)]"*

Mientras que el criptosistema multiusuario (PKC) sirve para los propósitos de autentificación, AC sirve para el propósito de la autorización. Este CA no está firmado y emitido por las autoridades de certificación, sino por las autoridades de atributo.

---

(58) https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578
(59) STORK D2.2 – Informe sobre la Interoperabilidad Legal, 3.4.3, p. 42., https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=57833/56
En este momento, *no se conoce todavía, la cantidad de conocimiento técnico y gastos que alguien necesita para ser una autoridad de atributo*. Actualmente parece que el Reglamento que reemplaza la Directiva 1999/93/EC no va a entrar en detalles en cuanto a las autoridades de atributo. Desde un punto de vista infraestructural, no hay mucha diferencia de una infraestructura de autoridad de atributo a la de una autoridad de certificación, que indica que estas *autoridades de atributo también serán empresas especializadas*. "Sólo" firman un certificado digitalmente, y mantienen

un registro actualizado para los propósitos de suspensión y revocación, que no necesariamente requeriría una infraestructura compleja, pero para hacerlo de forma segura, han de invertirse muchos recursos (incluyendo una respuesta rápida y la seguridad del proceso de firma).

Así que actualmente, no creemos que sea práctico que las autoridades actuales que gestionan los registros auténticos o la presten un acceso central a dichos registros (como CCBE para FAL 2.0) sean autoridades de atributo por ellas mismas, pero lo más probable es que servirán como una fuente de autoridad para ciertas capacidades para el apoyo de la PMI.

Por lo tanto, parece más factible conectar estas autoridades de atributo de X.509 con los auténticos registros ya existentes en muchos de los países. La mayoría de estos registros auténticos aún no proporcionan información automática de forma electrónica, y si lo hacen, hay una solución uniforme para el tratamiento de la validez de sus afirmaciones. La manipulación de la validez de las autorizaciones dependerá de la base de datos que la parte de verificación use, cómo almacenan la parte válida de la respuesta. Sin embargo, X.509 basados en ACs son los más emitidos con una validez a corto plazo, por ejemplo, por minutos, donde no hay necesidad para separar la infraestructura de revocación para ACs, y aún así, con un archivo a largo plazo de ACs como cualquier otro documento firmado digitalmente, podemos fácilmente demostrar después que AC fue válido en el momento de su emisión, independientemente de cualquier copia de seguridad de la base de datos.

STORK D2.2 también se refiere a este posible uso futuro de las autorizaciones: "*en muchos de los estados miembros estudiados, existen los registros auténticos que ofrecen el acceso a las empresas autorizadas a los datos auténticos que pertenecen a los ciudadanos. Al menos Austria, Bélgica, Francia, Italia, Islandia, Luxemburgo, Eslovenia, los Países Bajos y Suecia, ofrecen auténticos registros amplios que pueden ser consultados para verificar u obtener atributos actualizados. Los regímenes de acceso a estos registros difieren significativamente entre los estados miembros. En algunos casos el registro está abierto a la consulta por cualquier persona, en otros casos el acceso está totalmente confinado a las entidades autorizadas*" (60).

En resumen, creemos que PMI es una tecnología que tenemos que vigilar y una pronta introducción de ésta podría acelerar la interconexión con los servicios de los gobiernos electrónicos, pero por el momento, CCBE no está en posición de adaptar esta tecnología o empezar a usarla para los propósitos de e-CODEX.

4.3.4. Tarjeta Profesional Europea y las enmiendas propuestas al Artículo 4.a. de la Directiva 2005/36/EC.

En la Directiva 2005/36/EC (61), el Parlamento Europeo y el Consejo alentó a las asociaciones profesionales y a las organizaciones a introducir la Tarjeta Profesional Europea ("EPC") para facilitar la movilidad de los profesionales a través de acelerar el intercambio de información entre el Estado Miembro de acogida y el Estado Miembro de origen.

La forma de la tarjeta original prevista no fue establecida en la Directiva, pero era evidente que cierta información se incluiría en apariencia, por ejemplo universidad o institución a la que se asistió, cualificaciones obtenidas, experiencia, etc. (62).

---

(60) STORK D2.2 – Informe sobre Interoperabilidad Legal, 3.4.3, p. 42., https://www.eidstork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578

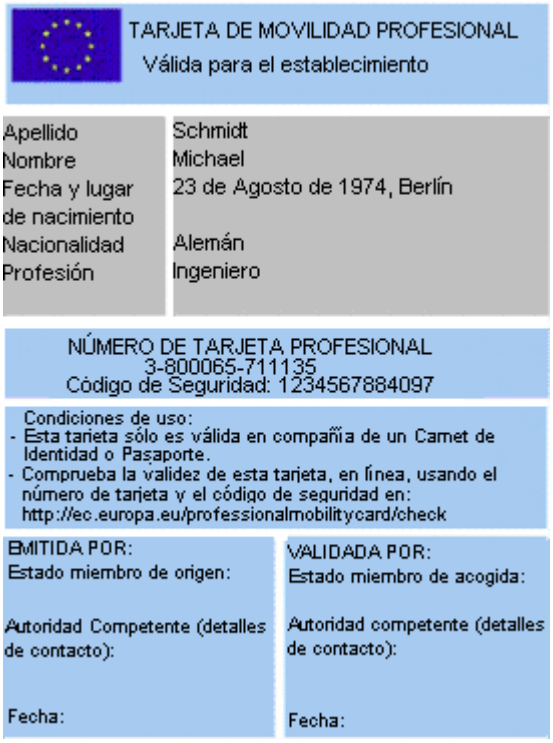
(61) Preámbulo 32 de la Directiva 2005/36/EC.

(62) Op. cit.

La Comisión Europea hizo grandes esfuerzos por elaborar una propuesta sobre la directiva modificada 2005/36/EC (63), llevando a cabo estudios sobre los posibles usos futuros de estos EPCs.

Tanto las enmiendas propuestas y los casos llevados hasta la fecha (64) todavía dejan algunas preguntas sin respuesta, pero parece que EPC será primero y ante todo un certificado electrónico sólo en el sentido de que a

petición del profesional, la autoridad nacional competente comprueba si tiene derecho de ejercer la profesión y si es afirmativo, carga un archivo al sistema IMI de la Comisión Europea. Después, habrá una interfaz pública para tanto el profesional, como para los posibles empresarios y consumidores con la base de datos IMI sirviendo como fondo. Con el uso de esta interfaz, el profesional puede imprimir una tarjeta en papel (certificado, ver figura 8) o solicitar la impresión de una tarjeta de plástico (ver figura 9), y tanto consumidores como empresarios comprobarán la validez de la tarjeta de movilidad profesional en ésta página web.


TARJETA DE MOVILIDAD PROFESIONAL
Válida para el establecimiento

Apellido	Schmidt
Nombre	Michael
Fecha y lugar de nacimiento	23 de Agosto de 1974, Berlín
Nacionalidad	Alemán
Profesión	Ingeniero

NÚMERO DE TARJETA PROFESIONAL
3-800065-711135
Código de Seguridad: 1234567884097

Condiciones de uso:
- Esta tarjeta sólo es válida en compañía de un Carnet de Identidad o Pasaporte.
- Comprueba la validez de esta tarjeta, en línea, usando el número de tarjeta y el código de seguridad en: http://ec.europa.eu/professionalmobilitycard/check

EMITIDA POR:	VALIDADA POR:
Estado miembro de origen:	Estado miembro de acogida:
Autoridad Competente (detalles de contacto):	Autoridad competente (detalles de contacto):
Fecha:	Fecha:

Figura 8 EPC en papel / formato electrónico

---

(63) Propuesta de Directiva del Parlamento Europeo y del Consejo modificando 2005/36/EC sobre reconocimiento de cualificaciones profesionales y Reglamentos […] sobre cooperación administrativa a través del Sistema de Información del Mercado Interno.

(64) La información más útil en este tema estaba disponible en el informa del Grupo de Dirección de EPC, veáse el último informe en http://ec.europa.eu/internal_market/qualifications/docs/professional_cards/steering_group_13092011_meeting_report_en.pdf 35/56

Figure 9 EPC en formato plástico

Es importante que la interfaz pública para el público general no contenga otra información que la validez de EPC, y si una autoridad revoca la licencia de un profesional, EPC por sí mismo deberá ser revocado también. Sin embargo, el uso de EPC no es obligatorio, y estará disponible sólo para aquellas profesiones que deseen tener una tarjeta, y solo para aquellos abogados que quieran tener un EPC. Por tanto, la publicación de la validez de una licencia de un abogado no es automática y por ello, si un abogado tiene que usar un servicio de gobierno virtual en un país diferente, por ejemplo, a través de e-CODEX, es posible que la base de datos IMI no contenga ninguna información sobre el abogado, incluso si el abogado tiene licencia. Por esta razón no esperamos que EPC sea usado para los propósitos transfronterizos de los gobiernos virtuales.

También es aparente que aunque este EPC sea solamente un certificado electrónico, claramente no será un certificado de atributo PMI. El párrafo 4 del artículo 4c de la propuesta requiere que EPC "sea válido por tanto tiempo como su titular conserve el derecho de ejercicio en el Estado Miembro de origen", que también se contradice con el estándar X.509 que dice que "los certificados de atributo son inherentemente a plazo corto (a veces en minutos, pero definitivamente más corto que la validez del certificado de clave pública del titular, que no puede ser más largo (65)". Por tanto, este certificado electrónico será más como un registro auténtico, y también está claro que esta tarjeta no será una identificación electrónica por si misma.

Una descripción detallada del procedimiento de EPC sin que se establezca en ningún Estado Miembro diferente se encuentra más abajo: (66)

---

(65) ITU-T X.509 (11/2008) Tecnología de la Información – Interconexión de sistemas abiertos – El Directorio: marcos de clave pública y certificados de atributo, http://www.itu.int/rec/T-REC-X.509-200811-I/en

(66) Todas las cifras se copian del informe del Grupo de Dirección de EPC, op. cit.

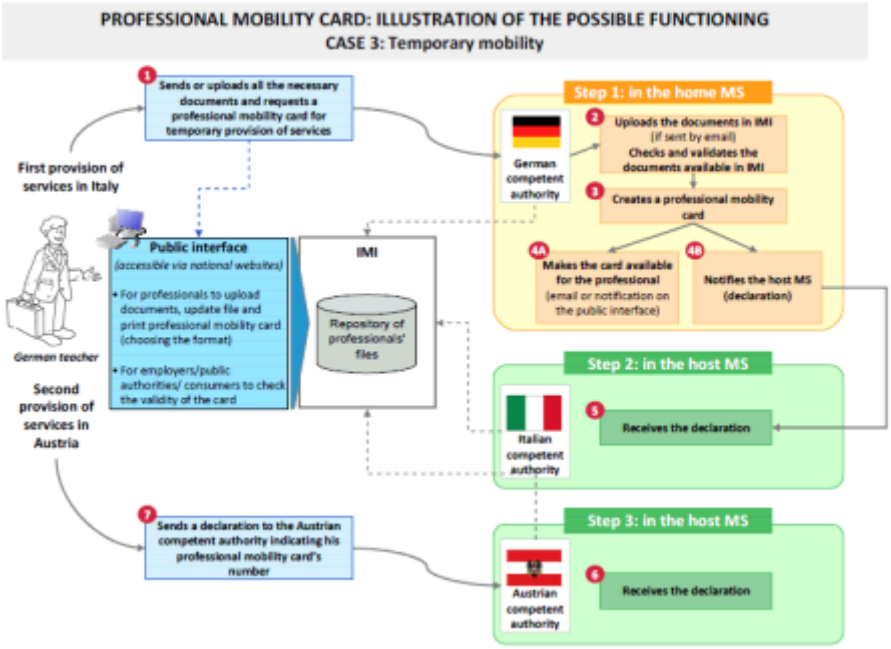


Figure 10 Procedimiento de EPC (Movilidad temporal)

5. Posibles elecciones de CCBE en apoyo a las tecnologías de autenticación y autorización

Basado en el resumen previo de medios técnicos, en este capítulo, nos gustaría reducir aún más las opciones de CCBE sobre la base de su papel, medios y medidas a su disposición.

CCBE es una organización representativa de abogados de la UE a través de sus miembros, las Abogacías europeas, siendo una asociación sin ánimo de lucro. Por tanto, los medios teóricamente posibles a su disposición para apoyar ciertas tecnologías, son en nuestra opinión, los siguientes:

a) Hacer propuestas a la asamblea legislativa de la UE (por ejemplo, la Comisión Europea (67), y los participantes LSP como los de e-CODEX;
b) Influir en la práctica de los abogados de la UE a través de sus Colegios de Abogados, emitiendo recomendaciones, documentos de posición, declaraciones o por el Código de Conducta para los Abogados Europeos, etc. (68);
c) Prestar un servicio no obligatorio para los Colegios de Abogados (por ejemplo Encuentra-Un-Abogado antes de ser asumido por la Comisión Europea);
d) En teoría, también podría ser posible actuar como una organización de grupo de compras grupo no obligatorio para sus miembros (aunque no hay ningún precedente para esto, y no es probablemente lo más deseado).

CCBE, claramente, no está en posición de tener un efecto en la práctica de los gobiernos proporcionando servicios de gobierno electrónico o cualquier participante independiente en el mercando, por ejemplo, productores de dispositivos, desarrolladores de software, organismos de estandarización (otros que no sean los participantes del mercado que se especializan en la provisión de servicios a los abogados y despachos de abogados.)

Nuestra conclusión es que CCBE podría apoyar cierta autentificación de las tecnologías de las siguientes formas:

a) Emitiendo una recomendación a los abogados de la UE o Colegios de Abogados a través de la formulación de **requisitos técnicos** de autentificaciones (incluidas las tecnologías sugeridas usadas para las credenciales);
b) Emitiendo una recomendación a Colegios de abogados en cuanto a los servicios de **gobierno electrónico** que ellos proporcionan a sus miembros.
c) A través de **comunicaciones enfocadas** y coordinadas con la Comisión Europea y otros tomadores de decisiones internacionales donde se solicita la opinión de CCBE.
d) Proporcionando una **autenticación central** o **un servicio de autorización** para los Colegios de abogados miembros o terceros interesados, como gobiernos nacionales o la Comisión Europea.
e) Comprando ciertas capacidades electrónicas de sus miembros o de los abogados de la UE, su uso espera grandes volúmenes que se pueden conseguir a nivel de toda la UE

Estudiamos las opciones posibles a) – c) con mayor profundidad. Tanto la prestación de una autentificación central o servicio de autorización (ejemplo FAL 2.0.) y una central de compras podrían ser una herramienta efectiva para el apoyo de ciertas tecnologías, pero cualquier aspecto a tener en cuenta mientras se usan estos medios de regulación ya son explicados en los otros tres enfoques, y la practicabilidad de estos últimos dos enfoques depende realmente de los recursos financieros otorgados a CCBE (ya sea por sus miembros o las partes externas como la Comisión Europea).

5.1. CCBE formula requisitos técnicos

Nuestro punto de partida es llevar a cabo cualquier transacción, incluyendo transacciones electrónicas, que hay que tener en cuenta cómo se manejan la cooperación de las partes y los riesgos de seguridad. Deberíamos echar un vistazo a la cantidad de requisitos definidos por la cooperación y seguridad de las transacciones electrónicas donde estos riesgos de seguridad son actualmente la mayor preocupación.

Teniendo en cuenta el número de transacciones electrónicas y el posible impacto de riesgos, el riesgo más afectado en las transacciones electrónicas es actualmente el pago electrónico y las transacciones electrónicas de servicios bancarios.

Compañía	Volúmen de pagos (billiones)	Volúmen total (billiones)	Total de transacciones (billiones)	Tarjetas (milliones)
Visa Inc	$ 3,273	$ 5,191	70.8	1,897
MasterCard	2,047	2,727	34.8	975
American Express	702	713	4.8	91
Discover	107	114	1.8	56
JCB	87	93	0.9	64
Diners Club	26	27	0.2	6

Tabla 6 El número anual de transacciones de pago electrónico (69)

(67) Ejemplo "Posición de CCBE sobre Identificación electrónica, Autentificación y firmas", http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_02052011_CCBE_Pos1_1304344346.pdf.

(68) Carta de los Principios Fundamentales de la Profesión Jurídica europea y el Código de Conducta para los abogados Europeos, http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_Code_of_conductp1_1306748215.pdf, La Declaración de Perugia, http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/perugia_enpdf1_1182334218.pdf, Guía jurídica de CCBE sobre compra de productos manufacturados en una empresa extranjera para economizar costes, http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_Guidelines_on_leg1_1277906265.pdf etc.

(69) Cf. VISA INC. (V) 10-K presentado el 18/11/2011.

Las normas de seguridad en el campo del pago electrónico son muy detalladas, esencialmente cubre todas las partes de la transacción desde un extremo a otro, y la cantidad de miles de páginas (70). Pero incluso con cada detalle considerable, el fraude de tarjetas y el fraude de banca por internet es una parte aceptada de nuestra vida, por ejemplo, el Informe Anual del Consejo de Pago de Reino Unido en 2010 mostró que la cantidad de fraude con tarjetas fue de £ 440,1 millones de todo tipo de fraudes, £ 266,4 millones de fraude telefónico, por internet y correo electrónico (71).

Si asumimos que las transacciones electrónicas que no sean las mencionadas anteriormente de transacciones electrónicas de pago tienen riesgos similares, parece obvio que las normas de seguridad no deben ser menos que estricta y detallada para estas transacciones. Por ejemplo, en una encuesta de EEUU, de lejos, la forma más común de robo de identidad era el uso de la identidad legítima de un contribuyente para presentar de manera fraudulenta una declaración de impuestos y solicitar un reembolso, siendo más frecuente que los fraudes bancarios o de tarjetas de crédito (72). En conclusión, sabemos que la prescripción de los requisitos de seguridad solo tiene sentido si podemos tener en consideración el proceso total de la transacción electrónica (de un extremo a otro), y si regulamos sólo unos pocos puntos críticos, generalmente vistos como requisitos de una transacción, podríamos perder la atenuación de riesgos de seguridad importantes mientras al mismo tiempo se crean algunas barreras técnicas.

Si no hay experiencia técnica en un cuerpo para lograr una visión clara de los asuntos técnicos de que se trate, entonces las normas no deberían tomar la forma de reglamentos técnicos (ya sea de carácter prescriptivo o recomendación), pero que se recurra a métodos más suaves de regulación.

Esta es una razón por la que no podemos considerar insignificante para CCBE formular ciertos requisitos como los certificados electrónicos cualificados emitidos para los abogados, por ejemplo, Marco para establecer un Sistema Europeo de Tarjetas de Identidad Electrónicas ("Marco CCBE") (73).

Este enfoque podría haberse visto como viable en 2007, pero actualmente pensamos que incluso un colegio de abogados nacional es capaz de certificar que ciertas políticas de certificación cumplen con los estándares de CCBE, si la interoperabilidad de Identificación Electrónica se llevara a cabo, sería más probable que se realice a través del enfoque recomendado por STORK, que es mediante el uso de puertas de enlace o a través de un software personalizado que será proporcionado por proveedores de servicio técnico. No queremos insinuar que los Colegios de Abogados o sus compañías afiliadas no podrían servir como proveedores de servicios técnicos, solo que basado en las respuestas de nuestro cuestionario, no es una opción para la mayoría de los colegios de abogados. Vamos a tratar de arrojar algo de luz sobre la viabilidad de esta opción desde un enfoque diferente. El objetivo final de CCBE podría ser tener a los abogados identificados electrónicamente y de una forma fiable en el conjunto de la Unión Europea, porque esto podría ayudar tanto al trabajo de los abogados como a aumentar el prestigio de la profesión. Este último objetivo podría ser alcanzado por la especificación de ciertas soluciones técnicas con suficiente detalle: no hay suficientes detalles para la interoperabilidad técnica ni en la Directiva 1999/93/EC, ni en el Marco de CCBE.

---

(70) por ejemplo, MasterCard Incorporated, MasterCard Rules 7 Diciembre de 2011, disponible en http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf; MasterCard Incorporated, Maestro Global Rules 11 noviembre de 2011, http://www.mastercard.com/us/merchant/pdf/ORME-Entire_Manual.pdf etc.

(71) http://www.paymentscouncil.org.uk/files/payments_council/new_website/annual_fraud_review.pdf, o datos Húngaros parecidos para la primera mitad de 2011 http://www.mnb.hu/Root/Dokumentumtar/MNB/Statisztika/mnbhu_statisztikai_idosorok/mnbhu_penzadatok/mnbhu_bkkartya visszaeles_2011/visszaelesek_a_bankkartya_uzletagban_2011_I_felev.pdf.

(72) http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf ver también la guía del contribuyente para el robo de identidad en http://www.irs.gov/newsroom/article/0,,id=251501,00.html

(73) http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/en_guidelines_framew1_1192450932.pdf, y las correspondientes normas técnicas en http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/en_annex_technical_s1_1192451405.pdf

Tenemos suficientes detalles que estarán disponibles cuando prescriba el uso de, por ejemplo, las tarjetas PenalNet, y una tarjeta PenalNet también estará considerada como una firma electrónica cualificada en los estados miembros con una referencia de atributo de ser un abogado. Pero una tarjeta PenalNet no puede asegurar que pueda utilizarse para fines ajenos a PenalNet, ni posiblemente, fuera de otros Colegios de Abogados miembros, ni ante CCBE, ni sus miembros tiene autoridad para hacerlo. CCBE no tiene efecto en la mayoría de los proveedores de servicios de gobierno virtual, por lo que cualquier tipo de soluciones técnicas recomendadas por CCBE será probablemente limitada dentro de nuestra profesión.

Por tanto, la mera regulación de los dispositivos de seguridad del cliente no es suficiente. Tenemos que tener en consideración que CCBE no pudo llegar a la meta de la interoperabilidad, incluso mediante la especificación de un middleware como STORK. STORK no ha resuelto la cooperación transfronteriza de las autentificaciones con sólo especificar un protocolo común y publicar una barra de herramientas para el middleware: todo estado miembro que desee aceptar STORK compatible con las credenciales también tiene que hacer algunos desarrollos. Así que si queremos que los proveedores de servicio del gobierno virtual fuera de los Colegios de Abogados acepten alguna solución prescrita por CCBE, estos proveedores de servicio necesitarán invertir algún tiempo y dinero en Él. La estandarización de las transacciones electrónicas no ha avanzado lo suficiente para hacer esta opción viable por el momento.

Así que en nuestra opinión, no importan los requisitos técnicos que formule CCBE, simplemente, no está en posición de asegurar el uso de su propia solución por los proveedores del servicio de gobierno electrónico fuera de sus miembros.

5.2. Requisitos relacionados con los servicios de gobierno virtual proporcionados por los miembros de CCBE

Basado en las respuestas, el 44% de los miembros (8 de cada 18 Colegios de Abogados) proporciona servicios a los abogados en los que los abogados tienen que identificarse de forma electrónica.

Aunque es posible para CCBE influenciar la identificación de las tecnologías que se usa, no vemos ninguna razón para hacerlo, otras diferentes a las razones ya examinadas en 5.1. Sin embargo, esto podría cambiar si se genera una considerable demanda por los abogados de la UE para acceder al Colegio de Abogados de un país diferente (para establecer propósitos y la utilización correspondiente de las tarjetas EPC, etc.)

Actualmente, sería prematuro para CCBE influir en las tecnologías usadas por los Colegios de Abogados que proporcionen acceso a sus propios servicios.

5.3. Comunicaciones coordinadas y enfocadas con los reguladores europeos

CCBE puede comunicar su interés a la legislatura a nivel europeo, tanto por sus respuestas de regulación que reemplacen la Directiva 1999/93/EC, como expresando su opinión a través de proyectos financiados por la UE como e-CODEX.

STORK no regula actualmente esta tecnología, certificado o contenido, sólo regula el marco para la cooperación. Aunque e-CODEX no contenga aún requisitos técnicos, lo hará una vez completado. Por tanto, la tecnología final aún puede cambiar. En los procesos de e-CODEX, los abogados tienen papeles destacados, el proyecto completo está actualmente bajo planificación y los recursos son presupuestados para requisitos de cambio y desarrollo comunicados durante las consultas con CCBE, por tanto las recomendaciones son probablemente mejor recibidas que los servicios existentes de los gobiernos electrónicos.

Por tanto, como e-CODEX es uno de los primeros gobiernos electrónicos transfronterizos de su especie, el resultado de este proyecto también puede servir como base para (a) implementación transfronteriza de nuevos procedimientos electrónicos o (b) una base para el acceso a las bases de datos a nivel de la UE donde la capacidad de un abogado

como tal, será más estrictamente verificada en el futuro (por ejemplo, Red Europea de Registros de la Asociación de Voluntades (74)).

Qué aspectos debería tener en cuenta CCBE cuando proporcione opiniones a los reguladores Europeos y proyectos financiados por la UE? Cuando exprese su opinión, creemos que CCBE debería tener en cuenta los siguientes elementos genéricos:

(i) Las soluciones sugeridas deberían ser suficientemente **seguras** para minimizar el riesgo de fraudes con la identidad de los abogados, teniendo en cuenta los posibles impactos de cualquier robo de identidad;
(ii) La autenticación e identificación debería permanecer a un coste adecuado para los abogados de la UE (que incluye que los abogados no deberían estar obligados a comprar un Nuevo dispositivo porque permita la mayor implementación del proyecto e-CODEX);
(iii) Las técnicas usadas deberían ser **familiares** con los abogados de la UE.
(iv) Debería tenerse un cuidado especial para hacer posible que los abogados utilicen las credenciales existentes cuando sea posible;
(v) Si la introducción de una nueva credencial fuera necesario, sería deseoso usar una solución para que los abogados puedan utilizarse para otros propósitos y usar una solución preparada para el futuro (por ejemplo, no apoyar los requisitos que excluyan el uso de elementos móviles seguros como credenciales).

http://www.europa-nu.nl/id/vi7jgt803jzl/list_of_existing_projects_in_the_field,
http://www.ccbe.org/fileadmin/user_upload/NTCdocument/Study_EJustice_2_De1_1246866101.pdf

6. Análisis de las respuestas del cuestionario

El cuestionario en línea presentado a los Colegios de Abogados de CCBE está copiado en el Anexo 1. Hemos insertado todas las respuestas de la encuesta en el Anexo 2, en una tabla para una comparación rápida y visión general, y en varias tablas y gráficos para una comparación visual. Además proporcionamos a CCBE con la base de datos completa de las respuestas en un archivo de texto (valores separados por comas, CSV) para cualquier uso posterior.

Para incrementar la legibilidad, en este capitulo, sólo damos una amplia visión de las respuestas, y no copiamos todos los gráficos y tablas a este capítulo del análisis. Esto también significa que una parte considerable del análisis se incluye sólo en el anexo 2. Nos referimos a las cuestiones basadas en función de sus números en la encuesta en el Anexo 1, la abreviatura Q3 podría dar una respuesta, Q19 fue sólo para fines de gestión de calidad y para proporcionar otros comentarios. Hemos recibido 18 respuestas, pero dos de los que respondieron representaban a Alemania, así que al estar buscando diferencias en los distintos Estados Miembros, hemos contado esas dos respuestas como sólo una.

6.1. Práctica actual en los Estados Miembros para comprobar la identidad de los abogados de forma electrónica

Los propósitos de Q3 y Q6 eran llegar a conocer mejor la experiencia general de los abogados en un determinado Estado Miembro como un abogado. Q3 fue una pregunta genérica para ver cómo de extendida está la comprobación de la identidad de los abogados en cada Estado Miembro, Q6 era sobre el método actual por la que se lleva a cabo, y no está necesariamente restringido a la comprobación de la identificación del abogado de forma electrónica.

De los 17 Estados Miembros, en 6 no existe procedimiento electrónico donde la identidad del abogado se compruebe de forma electrónica (35%). La mayoría (53%) de los que responden tienen certificados de clave pública que contienen un atributo con referencia al asunto del certificado de ser un abogado. Estos datos no están completamente en línea con las respuestas recibidas de los Estados Miembros a principios de 2011, con relación al cuestionario e-CODEX (ver la Tabla 7 abajo), donde de 33 encuestados, sólo 7 afirmaron que hay este tipo de PKCs.

PAÍS	TIENEN LOS ABOGADOS EN ESTE PAÍS, CERTIFICADOS DIGITALES QUE MUESTREN SU CONDICIÓN DE ABOGADOS?	SI ES ASÍ, QUIÉN EMITE ESTOS CERTIFICADOS DIGITALES?
Austria	Sí	Colegios de Abogados
Bélgica (Balonia y Bruselas)	No	
Bélgica (Flandes)		
Bulgaria		
Chipre	No	
República Checa	Sí	Colegio de Abogados Checo
Dinamarca	No	
Estonia	No	
Finlandia	No	
Francia	Sí	Colegio de Abogados Francés
Alemania		
Grecia		
Hungría	Sí	Proveedores del servicio de certificación después de que el Colegio certifique la condición de abogado.
Alemania		
Grecia		
Hungría	Sí	Proveedores del servicio de certificación después de que el Colegio certifique la condición de abogado.
Islandia	No	
Irlanda		
Italia	Sí	Compañías licenciadas en cooperación con Colegios de abogados Nacionales y locales
Liechtenstein	No	
Lituania		
Luxemburgo	No	
Malta	No	
Noruega		
Polonia	No	
Portugal		
Rumania		
República Eslovaca	No	
Eslovenia	No	
España	Sí	Colegio de Abogados
Suecia	No	
Suiza	Sí	Emitido por una compañía licenciada por el Colegio de Abogados suizo.
Los Países Bajos		
Reino Unido	No	
Reino Unido (Escocia)	No, pero están trabajando en ello.	El Colegio de Abogados de Escocia

Tabla 7 Respuesta al cuestionario e-CODEX

Las respuestas a esta pregunta también confirman la viabilidad de una capacidad en línea a nivel de la UE para comprobar la licencia de los abogados, pero esta pregunta fue respondida con más profundidad respecto a la pregunta 9 (viabilidad de proporcionar a CCBE con una información de validez actualizada), aunque esto claramente no funciona con todos los miembros de CCBE.

6.2. ¿Su gobierno proporciona identidad electrónica para los ciudadanos, o lo hará en el futuro? (Pregunta 4)

El propósito de esta pregunta era evaluar las experiencias generales de los Estados Miembros en servicios de gobierno electrónico relativos a la identificación y si es necesario, verificar desde el punto de vista de un abogado la información ya contenida en e-CODEX y las encuestas STORK.

Tres entes de los que respondieron dijeron que no hay identidad de gobierno virtual en sus Estados Miembros (ni tampoco será introducida en un futuro cercano, como en Letonia), pero basando la información en e-CODEX D4.1. y en otras fuentes, tres de los que respondieron parece que no entendieron la pregunta, o a pesar de haber IDs en estos países, estos IDs no se usan frecuentemente o no son conocidos. Es también digno de mención que en base a 10 respuestas, hay tarjetas inteligentes basadas en eIDs.

6.3. ¿Algún servicio de gobierno virtual utilizado en su país que proporcione un servicio web fiable u otra interfaz de base de datos para la consulta automática frecuente utilizada en la información de negocio, y cuál es gratuita para el público? (Pregunta 5)

Nuestro propósito con esta pregunta era conocer las experiencias generales de los Estados Miembros en relación a las autorizaciones utilizadas en los servicios de gobierno virtual, y si ya hay soluciones nacionales que podrían servir como una base fiable para la comprobación automática de ciertos atributos de forma electrónica (a través de auténticos registros que proporcionen respuestas automatizadas o certificados de atributo, etc.). Tenemos que admitir que esta pregunta fue bastante difícil de entender, y se dieron numerosas respuestas que no pusieron apoyar el propósito mencionado anteriormente, pero era una consecuencia necesaria de autorizaciones que no se presentan como un concepto diferente en la administración pública.

En cuanto a la mayoría de las respuestas, no existía todavía este tipo de sistemas (desde luego, había muchos registradores de empresa, etc., pero siempre y cuando no se pueda consultar de forma automática, no serán de mucha ayuda para posibles usos futuros de las autorizaciones.) Notable diferencia hay en Letonia, Polonia, Portugal (Citius) y quizás España (asistencia jurídica).

En Letonia, hay un servicio público web para los registradores de autorizaciones (poderes de los abogados) y para documentos inválidos, que podría servir como una base fuerte para la consulta automática de las autorizaciones. La falta de un registro centrar para los poderes de los abogados es uno de los temas más importantes en e-CODEX, así que las experiencias en Letonia en este aspecto podrían no ser valiosas. También es importante que las órdenes electrónicas para procedimientos de pago en Polonia, el proxy de un abogado (poder) se comprueba de forma automática.

El ejemplo español de asistencia jurídica podría ser útil como un ejemplo de cooperación amplia y automática de los diferentes registros públicos cuando se decida si proporcionar asistencia jurídica a un ciudadano o no.

6.4. Capacidad técnica del abogado las tecnologías con las que los abogados están familiarizados (Preguntas 7, 8 y 14-16)

Las preguntas 7 y 8 eran relativas a las capacidades tecnológicas de los abogados, una en cuanto al uso de Identificación Electrónica como abogados, y otra en cuanto al uso de Identificación Electrónica como un ciudadano normal en su vida cotidiana.

En la pregunta 7, el que responde puede designar más de una tecnología (así en la Figura 13, % significa qué % de todos los 18 que respondieron, contestaron que ellos usan esta tecnología como abogados.) La mayoría de los que respondieron indicaron que ellos utilizan firmas electrónicas cuando trabajan como abogados (50%).

El segundo mayor número de respuestas fue para la "otra categoría", que muestra que la categorización no estaba suficientemente clara. De las "otras" respuestas, hay que mencionar que los certificados de software no tienen una clase separada, y por tanto dos de los que respondieron tuvieron que incluir su respuesta en la categoría "otros". (La respuesta de la República Checa en cuanto a las cajas de datos debería ser considerado, en nuestra opinión, basándose en el método actual de autentificación cuando el abogado requiere acceso a la "caja de datos", por ejemplo, mediante una contraseña emitida al abogado.)

Es importante destacar que la mayoría de los que responden (83% de todos los que responden) han indicado que están usando algún tipo de hardware token (tarjetas inteligentes, OTP tokens etc.) cuando se identifican como abogados, y parece que solo una pequeña minoría de los que responden usan la autentificación o con el medio básico de identificarse usando sus direcciones de correo electrónico normales (4 respuestas de este tipo en total).

En la pregunta 8, se les pidió a los abogados que ordenaran las tecnologías que usan en su vida diaria (no necesariamente como abogados), y todas las clasificaciones dieron ciertos resultados a las tecnologías actuales (ponderadas en función de su rango), y la suma de las puntuaciones decide la clasificación general de las tecnologías. Basado en las respuestas, las tarjetas inteligentes que se usan para firmas electrónicas son ganadores relativos, pero si tomamos tarjetas inteligentes en una sola categoría (y no diferenciamos entre tarjetas inteligentes para la autentificación y para propósito de firma), su rango es aún más fuerte.

Los abogados utilizan más teléfonos inteligentes y tabletas en su vida diaria, pero quizás la clasificación es un poco engañosa, ya que no es muy probable que estos dispositivos se usen en procedimientos de identificación (se usan para propósitos de comunicación y trabajo, pero probablemente, no como credenciales).

Las preguntas 14 a 16 se utilizaron como apoyo a nuestro análisis de tendencias tecnológicas, y para comprobar si cualquier sugerencia electrónica relativa a las futuras credenciales están en línea con las expectativas actuales de los abogados o no, y para ver si los abogados están preparados para aceptar tendencias generales en la informática.

En cuanto al uso futuro, las tarjetas inteligentes están a la cabeza de nuevo: 13/18 de los que respondieron lo consideran que es probable que en tres años, los abogados usen esta tecnología para los procedimientos electrónicos, y la mayoría (7) de estas 13 respuestas que apoyan las tarjetas inteligentes, confirman que los abogados ya las están utilizando.

Parece que 8 de 18 de los encuestados esperan que tabletas y los teléfonos móviles con elementos seguros para que se utilicen para el acceso a servicios en línea, y hay una mayor incertidumbre en este sentido en cuanto a las tarjetas inteligentes.

6.5. ¿Podría el Colegio de Abogados proporcionar a CCBE con una licencia de abogado actualizada? (Pregunta 9)

Con esta pregunta, queremos comprobar la viabilidad de la autorización de CCBE de los abogados que dan los Colegios de Abogados (también el despliegue de FAL y la creación de FAL 2.0). Exceptuando a Italia, el resto de respuestas (94%) fueron positivas. La razón de la inhabilitación de Italia se encuentra en el hecho de que todavía no tienen base de datos central distinta a la de los propósitos del sistema electrónico nacional de procedimientos civiles.

(Basado en esta información, parece que esto es sólo es cuestión de desarrollo y protección de datos de los asuntos nacionales que de algunas políticas estrictas subyacentes.)

6.6. ¿Mantiene el Colegio de abogados un sistema donde los abogados se identifiquen con medios electrónicos y cuáles son los costes en Euros por cada abogado de estos sistemas? (Preguntas 10 – 13)

De las 18 respuestas, sólo 8 Colegios de Abogados (44%) mantienen un sistema donde se comprueba la identidad del abogado.

Hay una desviación considerable en cuanto a los costes por abogados en los sistemas, las cuotas por abogado están establecidas desde 1 € a 60 € por abogado, desde prácticamente cero costes de mantenimiento (por abogado) a 100 € / por abogado y por año, y algunos de estos costes anuales se cargan a los abogados. Es muy difícil sacar conclusiones significativas a partir de estos datos que no justifiquen de manera más fuerte, el análisis detallado de los sistemas proporcionados por los Colegios de Abogados a sus miembros. (Fue la petición de CCBE a responder las preguntas 11-13)

6.7. Ventajas e inconvenientes de los actuales sistemas nacionales de identificación electrónica para abogados

No podemos llegar a una conclusión que afecte a este informe basado en las respuestas 17-18 (que preguntó CCBE para incluirlas en el cuestionario), excepto los múltiples Colegios de Abogados que indican su afán de ayudar a otros Estados Miembros en el suministro de identificación o servicios de Autorización.

6.8. Conclusiones – Enfoque propuesto para CCBE

Basado en las conclusiones de las Secciones 4.2.5-4.2.7, 4.3, y 5, y basado en el analisis de las respuestas, pensamos que actualmente, CCBE debería primero y ante todo, apoyar el uso de las tarjetas inteligentes en la identificación de los abogados, pero también tener en cuenta que todos los requisitos establecidos en los actos legislativos y todas las conclusiones en LSP e-CODEX deberían formularse de tal manera que en un futuro cercano, los abogados deberían de ser capaces de usar elementos de seguridad en sus dispositivos móviles y no sólo tarjetas inteligentes que se utilizan con lectores especiales en un ordenador de mesa o un portátil.

Basado en las esperadas tendencias tecnológicas, también es una conclusión importante que el apoyo de la firma electrónica y principalmente el de la firma digital (QES o AES) podría no ser una buena respuesta en todos los procedimientos electrónicos, y CCBE debería siempre hacer esfuerzos para asegurar que otro hardware token basado en tecnologías de autentificación sin capacidades de firma no sean excluidos en el plano normativo sin razones claras y muy buenas.

A diferente nivel de este mismo problema, también recomendamos no apoyar ninguna ampliación de requisitos para usar dispositivos de creación de firma segura (SSCD) para la creación de firmas. Esto no sólo podría crear costes para los abogados injustificados y significantes, sino que también contribuye al "PIN, contraseña y hardware token fatigue" que podemos esperar que sea un gran dolor de cabeza para los abogados en los próximos años. Es posible que SSCDs se mantenga en un lugar especial para usos especiales, y no esté disponible para una audiencia más amplia: por lo que siempre que los abogados tengan que usar una, tendrá costes extras, y podría requerir el mantenimiento de un ordenador de escritorio independiente, etc.

Anexo 1: Cuestionario de CCBE sobre la Identidad Virtual de los Abogados
[Una copia del cuestionario]

Descripción del cuestionario

CCBE está actualmente participando en un proyecto Europeo a gran escala llamado e-CODEX, cuyo objetivo es proporcionar acceso a los sistemas legales en toda Europa.

La participación en este proyecto ha hecho que CCBE piense más ampliamente en las necesidades futuras de los abogados de la UE para identificarse electrónicamente a través de las fronteras en otros Estados Miembros y, más específicamente, qué tipo de enfoque tecnológico y contextual sería más adecuado para los Colegios de Abogados.

Para tener una visión bien fundada sobre el fondo técnico de cómo se identifican los abogados como tal en cada Estado Miembro, nos gustaría pedirle su participación en este cuestionario electrónico.

El número total de preguntas es 19. Para cada conjunto de preguntas, después de que haya revisado sus respuestas para asegurar la precisión, haga clic en "SIGUIENTE" al final de la página web para continuar con el siguiente conjunto de preguntas. Si ha completado todo correctamente en la página, se pasará a la página siguiente.

Si ha rellenado un bloque de forma incorrecta o no ha completado un bloque, un texto en rojo resaltará el problema y proporcionará una guía sobre cómo corregir el error. Tras corregir el problema, haga clic en "SIGUIENTE" de nuevo para pasar a la página siguiente. Después de completar la última pregunta, haga clic en "ENVIAR" para enviarnos su cuestionario completo.

Aviso importante: Por favor tenga en cuenta que, dependiendo del navegador que utilice, la respuesta a estas preguntas en más de dos horas podría causar algunos problemas técnicos, y por tanto - si esto le afecta – tiene que tenerlo en cuenta para evitarlo.

Preguntas generales

1) Por favor, díganos el nombre del Colegio de Abogados en nombre de la que rellena esta encuesta. _____

2) Por favor, díganos su nombre y su dirección de correo electrónico.
_____

Cuestiones en cuanto a los desarrollos en su Estado Miembro

3) ¿Podría nombrar los procedimientos judiciales más importantes en su país donde la identificación del abogado y su capacidad de actuar como tal se comprueba de forma electrónica? Por favor no nombre más de cinco procedimientos. Si hay un enlace público al procedimiento o al servicio, por favor indíquenos también el enlace.

4) ¿Proporciona su gobierno identidad electrónica para los ciudadanos o lo hará en un futuro? Si es así, que tipo de tecnología se usa/usará?

5) ¿Hay algún servicio de gobierno virtual, bien utilizado en su país, que proporcione un servicio web de confianza u otra interfaz de base de datos para la consulta automática utilizada frecuentemente en información de negocios, y que sea gratis para el público? Nos gustaría identificar posibles enfoques nacionales y precedentes (historia) para la verificación de los papeles. Por ejemplo, Hay una base de datos pública sobre las autorizaciones (delegaciones) para actuar en nombre de alguien? O hay algún motor de búsqueda bien utilizado de un Gobierno electrónico donde pueda buscar diferentes tipos de licencias, por ejemplo, un motor de búsqueda central para diferentes tipos de proveedores de servicios profesionales (no sólo abogados, sino también auditores, contadores, etc.)? Si es así, por favor, describa el tipo de información proporcionada.

6) Si lo conoce, por favor describa cómo se comprueba la validez de la capacidad del abogado para actuar ("licencia") de forma electrónica en un procedimiento judicial en su Estado Miembro. ¿Cuál es el papel de su Colegio de Abogados en el suministro de información sobre la validez de la licencia del abogado?

Por ejemplo, su Colegio de Abogados suministra la información válida al proveedor de servicios del procedimiento electrónico cada semana, o proporciona un servicio web de 7x24 para responder preguntas sobre validez casi a tiempo real. O su Colegio de Abogados emite un certificado de firma digital del abogado para ese procedimiento, y su Colegio de Abogados retira el certificado si el abogado no ejerce.

7) Por favor, indique que tipo de tecnologías electrónicas son usadas efectivamente en su país cuando los abogados se identifican como tales en procedimientos judiciales.

[ ] Firma electrónica a través de tarjetas electrónicas u otro hardware token (cualificado o avanzado)

[ ] Identificación a través de aplicaciones de un teléfono inteligente o tableta.

[ ] Identificación Electrónica (autentificación) a través de cualquier hardware token que no sean tarjetas inteligentes, teléfonos inteligentes o tabletas.

[ ] Otros factores multiples de autentificación sin tarjeta inteligente (nombre de usuario y contraseña o código PIN etc. en conjunto con contraseñas de una vez o hardware token etc.)

[ ] Nombre de usuario y contraseña o código PIN (sin hardware token, por ejemplo, factor simple de autentificación)

[ ] Email sin identificación segura del abogado (dirección de correo electrónico normal y/o firma)

[ ] Otro:

[ ] Ninguno

8) Por favor, ordene los siguientes elementos según cuánto usan los abogados estas técnicas en su vida cotidiana en su ciudad, cómo se han acostumbrado a usarlas.

Su respuesta a esta pregunta es importante para nosotros para estimar mejor el posible escenario futuro al que se enfrenta CCBE en tres años (dónde están las cosas ahora y dónde esperamos que estén más adelante).

_____Tarjetas inteligentes usadas para firma electrónica
_____ Tarjetas inteligentes para la autentificación electrónica (para el acceso a servicios en línea)
_____Teléfonos inteligentes o tabletas
_____Hardware based tokens (dispositivos de seguridad) proporcionando contraseñas de una vez
_____Teléfono móvil proporcionando contraseñas de una vez
_____Otros hardware based tokens que permiten la autentificación de múltiples factores, no mencionados antes.

Cuestiones relativas a desarrollos dentro de su Colegio de Abogados

9) ¿Sobre la base de sus capacidades técnicas actuales, sería posible que su Colegio de Abogados ofrezca a CCBE información válida actualizada de manera electrónica, en cuanto a la licencia de un abogado registrado en su Colegio de Abogados?

Por ejemplo, ¿Usted o su Colegio de Abogados tiene una base de datos completa y fiable sobre todos los abogados de su Estado Miembro de forma electrónica? ¿Son todos los Colegios de Abogados capaces de proporcionar ese acceso ahora o en un futuro cercano?

10) ¿Tiene su Colegio de Abogados un sistema en el que los abogados se identifiquen de forma electrónica? (en lugar de que se ejecute, por ejemplo, a través del gobierno o de otra autoridad)?

[ ] Si (por favor responda también a las preguntas 11-13)

[ ] No (por favor responda a la pregunta 14)

11) ¿Cuál era el coste estimado por abogado (en euros) de la creación de este sistema? Por favor rellene esto solo si la respuesta a la pregunta anterior era sí.

_____

12) ¿Cuál es el coste estimado por abogado (en euros) de la creación de este sistema? Por favor rellene esto solo si la respuesta a la pregunta 10 era sí.

_____

13) ¿Hay una cuota (por año, mes, etc.) que el abogado tenga que pagar por usar este sistema? Por favor rellene esto solo si la respuesta a la pregunta 10 era sí.

_____

Cuestiones relativas a los desarrollos futuros

14) Cómo ve de probable que en 3 años los abogados de su país utilicen tarjetas inteligentes en procedimientos electrónicos? (Ya sea para firma o sólo para identificación). Por "utilizar", nos referimos a la mayoría de los abogados no ve, en general, estos requisitos técnicos como desiguales, injustos o desproporcionados para acceder al servicio electrónico.
( ) Ya se usa
( ) Muy probable
( ) Probable
( ) No es probable, no es seguro
( ) No procede, no lo sé

15) Cómo ve de probable que en 3 años los abogados de su país utilicen un procedimiento electrónico en el que se requiera un teléfono electrónico o una tableta para el acceso a los servicios en línea?
( ) Ya se usa
( ) Muy probable
( ) Probable
( ) No es probable, no es seguro
( ) No procede, no lo sé

16) Can you think of any other specific hardware based tokens in your country that lawyers will be familiar with in 3 years' time and that enables multi-factor authentication? If yes, please specify.

16) ¿Puede pensar algún otro tipo de hardware basado en tokens en su país en el que los abogados se familiaricen en 3 años y que permita múltiples factores de autentificación? Si es así, por favor especifíquelo.

Conclusiones

17) ¿Cuáles son las ventajas de su sistema nacional actual de identificación electrónica de abogados (si es que tiene este sistema)?

18) ¿Cuáles son las desventajas de su sistema nacional actual de identificación electrónica de abogados (si es que tiene este sistema)?

19) Si tiene más comentarios en cuanto a las cuestiones mencionadas o sobre el fondo técnico de la identificación transfronteriza de abogados, por favor comparta esta información con nosotros (opcional)

Anexo 2: Respuestas al cuestionario resumidas en tablas y cuadros

Presencia del gobierno que proporcionó identificación electrónica a los ciudadanos (pregunta 4) (Presence of government provided e-Id for citizens (Q4))	**Cuenta**	**Porcentaje %**
Si	14	82%
No	3	18%

Teniendo en cuenta el lanzamiento inminente dela Identificación Electrónica en Letonia, hemos contado su respuesta como un "sí".

Presencia del gobierno que proporcionó identificación electrónica a los ciudadanos (pregunta 4) (Presence of government provided e-Id for citizens (Q4))

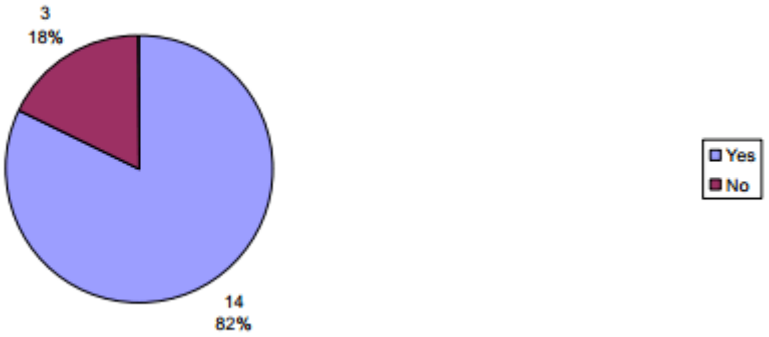


Figura 11 Cuadro de respuestas a la pregunta 4

¿Cómo se comprueba la validez de la licencia del abogado? (Pregunta 6)	Cuenta	Porcentaje %
El certificado de clave pública del abogado (utilizado para identificarlo) contiene esta información.	9	53%
Puede comprobarse solo en la web del Colegio de Abogados.	3	18%
De otra forma automática a través de los Tribunales	2	12%
Solo a través de soluciones que no sean "en línea" o soluciones que no están completas.	3	18%

Tabla 8 Tabla de Respuestas a la Pregunta 6

Respuestas de los dos Colegios de Abogados de alemania contados como uno.

¿Cómo se comprueba la validez de la licencia de un abogado?

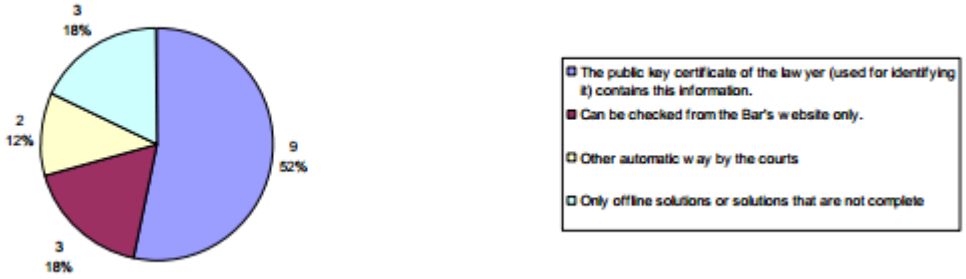


Figura 12 Cuadro de Respuestas a la Pregunta 6

Tecnologías usadas para la identificación de los abogados en un Estado Miembro (Pregunta 7)	Cuenta	% de participación de todas las respuestas
Firma electrónica a través de tarjetas inteligentes u otro hardware token (cualificado o avanzado)	9	50%
Identificación a través de aplicaciones específicas de teléfonos inteligentes o tabletas	1	5.6%
Identificación electrónica (autentificación) a través del uso de cualquier hardware token distinto a las tarjetas inteligentes, teléfonos inteligentes o tabletas.	2	11.1%
Otro multi factor de autentificación sin tarjeta inteligente (nombre de usuario y contraseña o código PIN, etc. junto a una contraseña de una vez o un hardware token etc.)	3	16.7%
Simple nombre de usuario y contraseña o código PIN (sin hardware token, por ejemplo, factor de autentificación único).	2	11.1%
Correo electrónico sin identificación segura del abogado (correo electrónico normal y/o firma)	2	11.1%
Otro	7	38.9%
Ninguno	4	22.2%

Tabla 9 Tabla de repsuestas a la Pregunta 7

Lista de "otras" respuestas a la Pregunta 7:
(Vea la respuesta a la pregunta número 6 más arriba)
Cajas de datos (Data boxes)
ERV: Certificados de software
Ver pregunta 6

Emitimos la tarjeta de identificación de CCBE pero no somos conscientes de su uso para procedimientos judiciales nacionales.

El procedimiento ante el Tribunal requiere un nombre de usuario, una contraseña general y un certificado digital especial, que es individual protegido por una contraseña separada y podría descargarse de la página web del Tribunal tras crear una cuenta de abogado y verificar luego su identidad

Para la pregunta 8, no se utiliza ninguno de los elementos enumerados. Al tener que dar una respuesta alternativa, esto se hace, aunque no es correcto.

Tabla 10 Lista de "otras" Respuestas a la pregunta 7

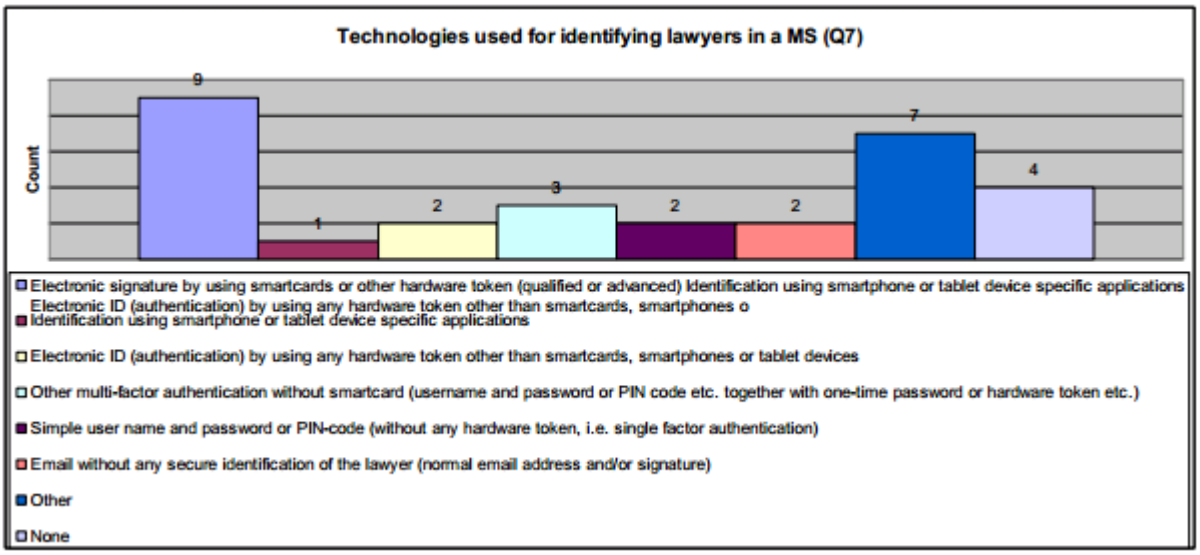


Figura 13 Tabla de respuestas a la pregunta 7

Clasificación de las tecnologías usadas en la vida cotidiana de los abogados (Pregunta 8)	Puntuación total	Posición
Tarjetas inteligentes utilizadas para firma electrónica	64	1
Tarjetas inteligentes utilizadas para autentificación electrónica (para acceder a los servicios en línea)	48	2
Teléfonos inteligentes o tabletas	48	2
Hardware based tokens (dispositivos de seguridad) proporcionando contraseñas de una vez	36	3
Teléfonos móviles que proporcionen contraseñas de una vez	36	3
Otrro hardware based tokens que permite la autentificación de múltiples factores, no reflejado arriba.	36	3

Tabla 11 Tabla de respuestas a la pregunta 8

¿Es viable que un Colegio de Abogados proporcione a CCBE una información válida actualizada, de forma electrónica, en cuanto a la licencia de abogado? (pregunta 9)	Cuenta	Porcentaje %
Sí	16	94%
No	1	6%

Tabla 12 Tabla de respuestas a la pregunta 9

Las respuestas de dos Colegios de Abogados alemanes se cuentan como una. Las respuestas que dicen “esta solución se proporcionará a partir de 2012” se contaron como un sí. Las respuestas del delegado español se contaron como un sí.

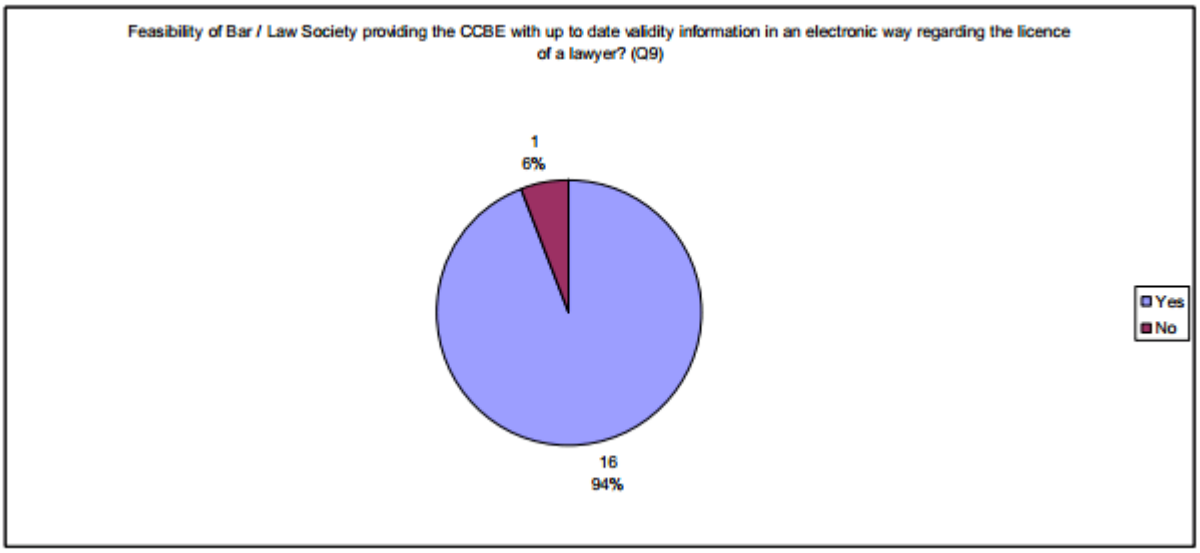


Figura 14 Cuadro de respuestas a la pregunta 9

Colegio de abogados que mantenga un sistema donde los abogados se identifiquen a través de medios electrónicos (Pregunta 10)	Cuenta	Porcentaje %
Sí	8	44.4%
No	10	55.6%

Tabla 13 Tabla de respuestas a la pregunta 10

Colegio de abogados que mantenga un sistema donde los abogados se identifiquen con medios electrónicos (pregunta 10)

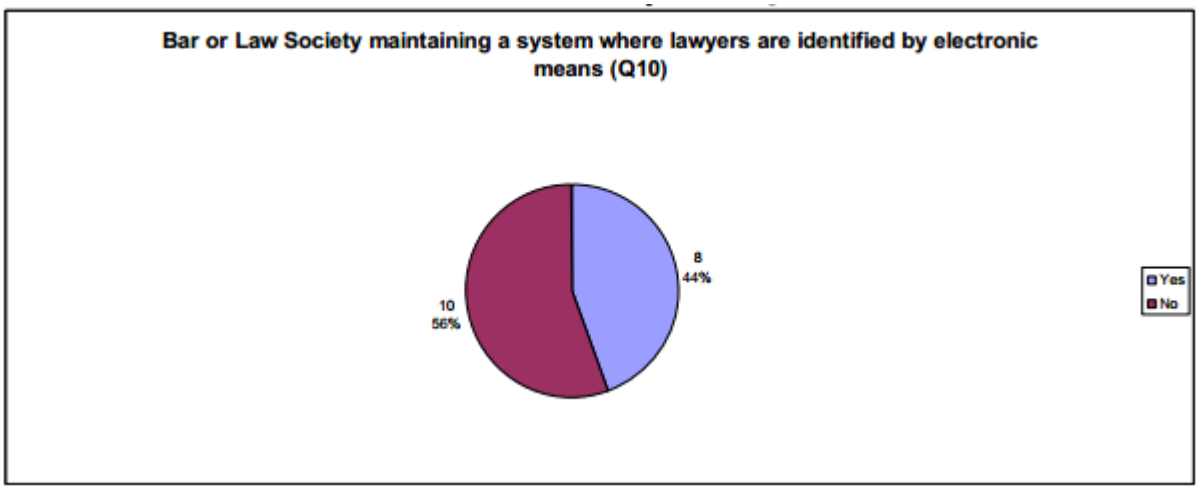


Figura 15 cuadro de respuestas a la pregunta 10

Probabilidad de que los abogados en su país usen tarjetas inteligentes en los procedimientos electrónicos en tres años (pregunta 14)	Cuenta	Porcentaje %
Ya se usa	7	38.9%
Muy probable	3	16.7%
Probable	3	16.7%
No es probable, no es seguro	3	16.7%
No es aplicable, no se sabe	2	11.1%

Tabla 14 Tabla de respuestas a la pregunta 14

Probabilidad de que los abogados en su país usen las tarjetas inteligentes en procedimientos electrónicos en tres años (pregunta 14)

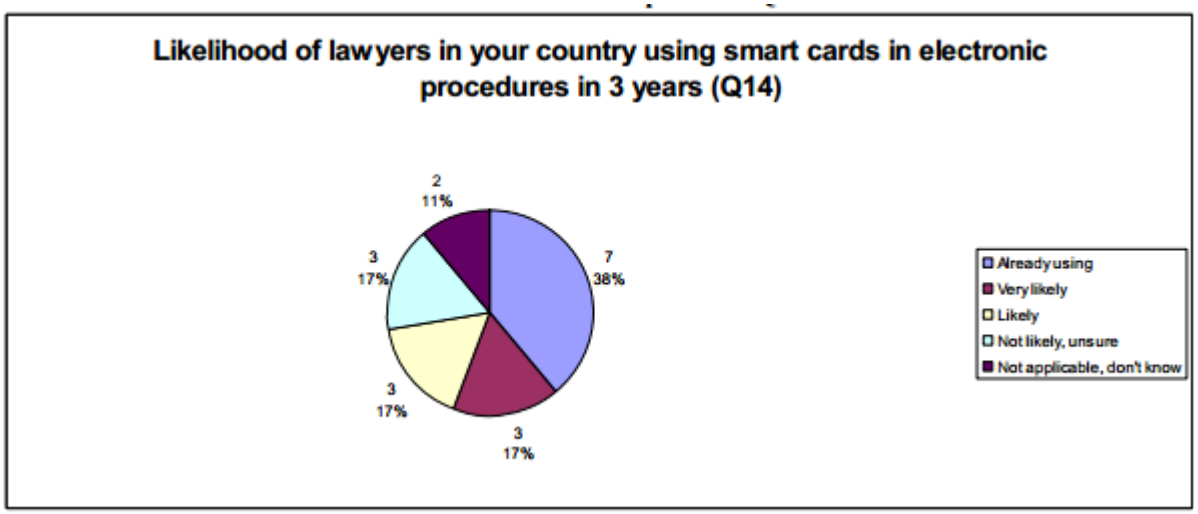


Figura 16 Cuadro de respuestas a la pregunta 14

Probabilidad de que los abogados en su país usen tabletas o teléfonos inteligentes en los procedimientos electrónicos en tres años (pregunta 15)	Count	Percentage %
Ya se usa	5	5.6%
Muy probable	4	22.2%
Probable	3	16.7%
No es probable, no es seguro	6	33.3%
No es aplicable, no se sabe	4	22.2%

Tabla 15 Tabla de respuestas 15

Probabilidad de que los abogados en su país usen tabletas o teléfonos inteligentes en los procedimientos electrónicos en tres años (Pregunta 15)

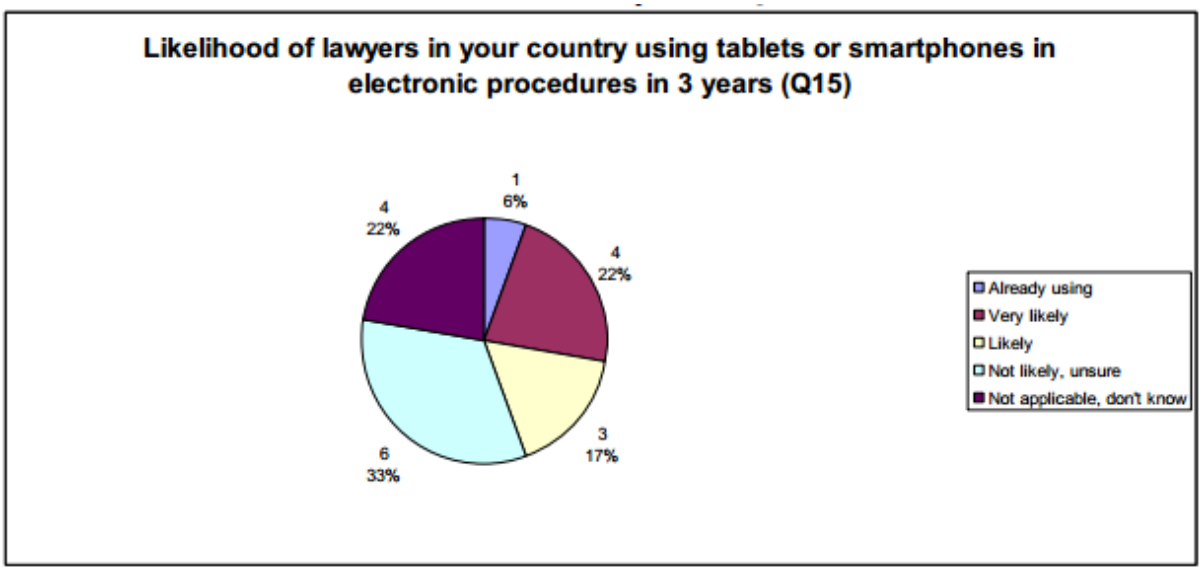


Figura 17 Cuadro de respuestas a la pregunta 15

Otro hardware based tokens en su país con los que se familiarizarán los abogados en 3 años (Pregunta 16)	Cuenta
OTP tokens 1	1
Una tarjeta inteligente combinado con un OTP-token	1
Seguridad de los dispositivos móviles	1

Tabla 16 Tabla de respuestas a la pregunta 16

Presencia del gobierno que proporciona identificación electrónica a los ciudadanos	Cuenta	Porcentaje %
Sí	15	53%
No	2	18%

Respuestas de dos Colegios de abogados de Alemania se contaron como una. Las respuestas que dicen "esta solución se proporcionará a partir de 2012" se contaron como un sí