ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Astrea

La identificación y autenticación por medios electrónicos

Nacho Alamillo, ***Abogado, DEA, CISA, CISM, ITIL-f, COBIT5-f***

19 de octubre de 2017

Identificación y firma: contexto europeo – 1

- Reglamento (UE) Nº 910/2014, de 23 de julio (eIDAS)
  - Construcción de un sistema público de (interoperabilidad de la) identificación electrónica en la Unión Europea; que parte de la noción de la identidad digital como bien público y, por tanto, objeto de potestad de los Estados.
  - Regulación de los servicios de confianza y su provisión y uso transfronterizos.
  - Base legal para Servicios Públicos Digitales esenciales en la Unión.
- Directamente aplicable en los Estados miembros, obliga a reformar (o desplaza) la legislación previa
  - La Ley 59/2003, de 19 de diciembre (LFE) ya ha sido modificada puntualmente, y el supervisor se encuentra evaluando la reforma global.
  - Desaparición de los certificados de firma electrónica de persona jurídica, con efecto a julio 2016.

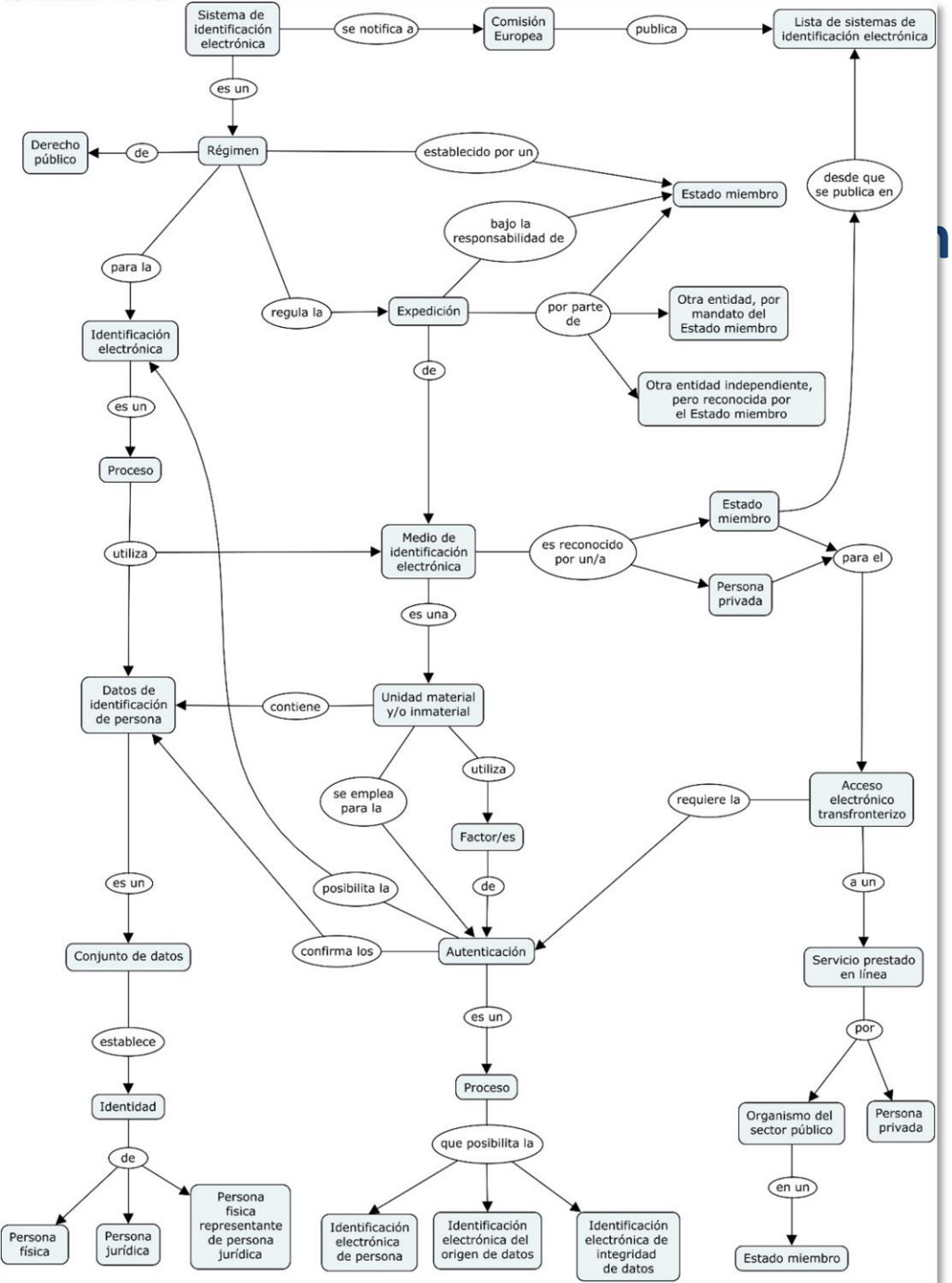
Identificación y firma: contexto europeo – 2

- La identificación electrónica en el Reglamento eIDAS
  - Expedición, por los Estados o bajo su responsabilidad, de medios públicos de identificación electrónica, o su reconocimiento, cuando sean privados.
  - Niveles de seguridad variables (bajo, sustancial y alto), a efectos del reconocimiento mutuo transfronterizo.
  - Despliegue y operación de plataformas públicas comunes de autenticación, cuyo uso puede también autorizarse al sector privado, con base en la delegación y federación de la autenticación.
  - Reconocimiento mutuo obligatorio de los medios de identificación electrónica a partir de septiembre de 2018, o antes de forma voluntaria.

Identificación y firma: contexto europeo – 3

- La identificación electrónica en el Reglamento eIDAS
  - El Reglamento eIDAS no regula los sistemas y medios de identificación electrónica, sino que debe ser el legislador nacional quien lo haga, dentro de un amplio espacio de discrecionalidad (pero con las restricciones impuestas para que los mismo sean reconocidos e interoperables de forma transfronteriza).
  - Incluyendo la posibilidad de ser el titular del servicio, incluso en régimen monopolístico (DNI-e), en modalidades de gestión directa (Cl@ve) o indirecta, incluyendo la contratación al sector privado. También se podría acudir al "reconocimiento" de identidades privadas o público-privadas (Reino Unido, Suecia, Noruega, Dinamarca…).

…a: contexto europeo – 4



- La identificación electrónica en el Reglamento eIDAS
  - Concepto legal (simple y claro, como debe ser...)
  - Útil para la interoperabilidad y el reconocimiento mutuo.
  - Pero también en sede nacional (efecto prescriptor de las normas de interoperabilidad y seguridad), a menos que no se desee el uso transfronterizo…

Identificación y firma: contexto europeo – 5

- La identificación electrónica en el Reglamento eIDAS
  - Innovaciones relevantes en el nivel de seguridad alto, incluyendo el uso de técnicas biométricas seguras, y como novedad (eIDAS *token*), capacidades de autenticación con protección de la privacidad, limitada por ejemplo a la verificación de la edad, o del lugar de residencia, sin necesidad de divulgar datos personales innecesarios.
  - No sólo autenticación en nombre propio, sino en nombre de terceros, y también el intercambio de atributos parciales mediante conexión a fuentes auténticas, como los poderes de actuación, como se ha desarrollado en los proyectos STORK, de modo que la federación de los sistemas de gestión de identidad con estos servicios públicos permite obtener un gran valor, y reducir riesgos.

Identificación y firma: contexto europeo – 6

- Servicios de confianza
  - Sustituye a la regulación de los servicios de certificación previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.
  - Definición legal de servicio de confianza: el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:
    - a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o
    - b) la creación, verificación y validación de certificados para la autenticación de sitios web, o
    - c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.
  - Servicio de confianza cualificado: el que cumple los requisitos aplicables previstos en el presente Reglamento (y más…).
  - Es un tipo de servicio de la sociedad de la información.

Identificación y firma: contexto europeo – 7

- Nivel “ordinario” de servicio de confianza,
  - No se encuentra prácticamente regulado, y no recibe ningún reconocimiento legal en particular; y en cuyo caso, el usuario debe construir su propio estado interno de confianza respecto al servicio; p.e, contraseña de entidad financiera vs servicio de almacenamiento de documentos en la Nube.
- Nivel “cualificado” de servicio de confianza,
  - Altamente regulado, y que recibe un reconocimiento particular de efectos legales, lo cual debería suponer un incentivo a su adopción. En este caso, este reconocimiento legal explícito es el que permite al usuario reconocer el servicio como confiable, por lo que podemos asumir que estos servicios se desarrollarán antes y en mayor volumen que los que no gocen de esta condición.
    - O no… (Roßnagel, 2006), fracaso de las tarjetas criptográficas (DNI-e).
    - Obsolescencia del concepto de “documento” y “firma” (Dumortier & Vandenzande, 2012).

Identificación y firma: contexto europeo – 8

- Servicios de confianza
  - Firma electrónica cualificada, reservada exclusivamente a personas físicas, que debe basarse necesariamente en un certificado cualificado de firma electrónica (artículo 3.12 del Reglamento eIDAS)
    - Impacto sobre la "firma" de persona jurídica… que ha desaparecido.
    - No se establece mayor presunción que la equivalencia a firma escrita.
  - Sello electrónico cualificado, reservado exclusivamente a entidades, que debe basarse necesariamente en un certificado cualificado de sello electrónico (artículo 3.27 del Reglamento eIDAS)
    - Impacto sobre el sello regulado en la LAE, LUTICAJ y Ley 25/2013.
    - Presunción de integridad de los datos y de la corrección del origen de los datos. Otros usos: firma de código, servicios web, etc.
  - Autenticación de sitios web (artículo 3.39 del Reglamento eiDAS)
    - Impacto en el certificado de sede electrónica.
    - No se establecen efectos jurídicos ni presunción…

Identificación y firma: contexto europeo – 8

- Servicios de confianza
  - Validación cualificada de firma/sello electrónico y conservación cualificada de firma/sello
    - Sin efectos jurídicos ni presunción expresa, pero de claro valor.
  - Sellado de tiempo electrónico
    - El sello de tiempo electrónico cualificado disfrutará de una presunción legal de exactitud de la fecha y hora que indican y de la integridad de los datos a los que esa fecha y hora están vinculados (artículo 41.2 del Reglamento eIDAS), además de que el mismo deberá ser reconocido en todos los Estados miembros (artículo 41.3 del Reglamento eIDAS).
    - Importancia extraordinaria para la prueba electrónica forense (por ejemplo, aseguramiento de *logs*) y para longevidad de firmas.
    - Debería ser de uso obligatorio para documentos administrativos (artículos 26, 36 y 88 de la LPAC).

Identificación y firma: contexto europeo – 9

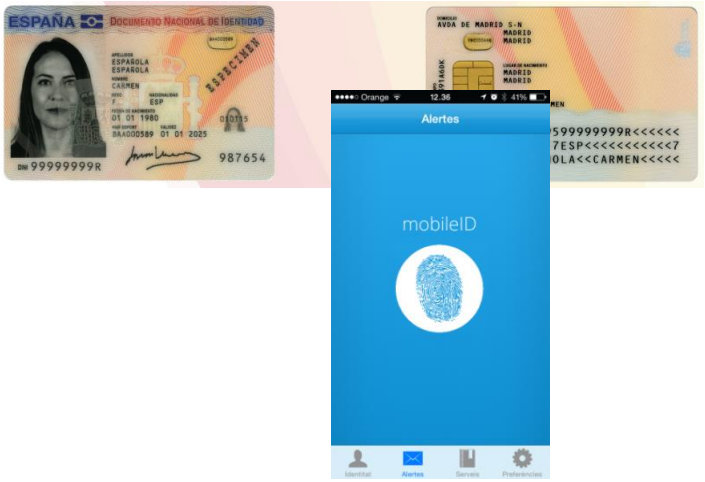
- Servicios de confianza
  - Eliminación de disfunciones
    - Artículo 30 del Reglamento eIDAS: Certificación obligatoria de los dispositivos cualificados de creación de firma/sello.
    - Artículo 28.2 del Reglamento eIDAS: Prohibición de someter a los certificados cualificados a ningún requisito adicional a los previstos en el Reglamento. Supone el fin de las "condiciones adicionales" del artículo 4 de la Ley 59/2003, así como la inaplicación del artículo 19 RD 4/2010.
    - Artículo 24.4 del Reglamento eIDAS: Obligación de los prestadores de servicios de confianza que expidan certificados cualificados a proporcionar acceso automatizado a la información de estado de los certificados a cualquier persona, de forma fiable, eficiente y gratuita, previsión legal que afecta contundentemente a modelos de negocio como el de la FNMT-RCM, que ha venido cobrando por este servicio, tanto a entidades públicas cuanto a privadas.

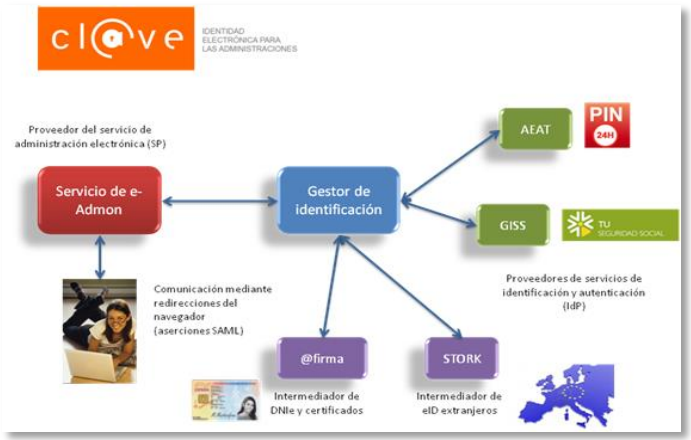
Identificación y firma: contexto europeo – 10

- Creación de la firma/sello electrónicos a distancia
  - Novedad del Reglamento eIDAS, que permite la creación y gestión centralizada de claves de firma/sello electrónicos, como Cl@ve firma.
  - Considerando 51 Reglamento eIDAS
    - "Debe ser posible para el firmante confiar a un tercero los dispositivos de creación de firmas electrónicas cualificados, a condición de que se apliquen los procedimientos y mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de la firma electrónica y que la utilización del dispositivo cumple los requisitos de la firma cualificada".
    - Diversos casos de uso posibles, incluyendo el empleo de sistemas confiables de gestión de clave privada centralizada, donde la clave privada es accedida a distancia por el usuario, pero para la generación de firma electrónica con una aplicación instalada localmente en su sistema; o en que la propia firma se genera a distancia.

Identificación y firma: nuevo régimen en España – 1

- El panorama español se presenta fragmentario y complejo
  - DNI-e, regulado en Ley Orgánica 4/2015, de 30 de marzo, de Seguridad Ciudadana (y, de momento, en Ley 59/2003): arts. 8 y ss.
  - "Resto" de identidades y firmas de ciudadanos para su uso en sector público, "apoderamientos" e intercambio de atributos, en la Ley 39/2015, de 1 de octubre (LPAC).
  - Y la identidad y firma de la propia Administración, en la Ley 40/2015, de 1 de octubre (LRJSP).





Identificación y firma: nuevo régimen en España – 2

- Mantenimiento del derecho “a la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley” (artículo 13.g LPAC), ya previsto en la LAE, aunque con un evidente retroceso con respecto a la misma.
- Nueva obligación *ex lege* de relación exclusivamente electrónica con las AAPP, artículo 14.2, sujetos que no tienen derecho a la asistencia en las oficinas presenciales, y por tanto deben ser capaces de emplear estos sistemas.
- En el caso de personas físicas no obligadas (artículo 14.3 de la LPAC), se puede sustituir esta firma por la del funcionario actuante (artículo 12), pero debiéndose generar prueba, por lo que se podría inaplicar y generar firma biométrica presencial.

Identificación y firma: nuevo régimen en España – 3

- Nueva regla general, en el artículo 11.1 LPAC: "Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley".
- Artículo 10.1 LPAC: "Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento".

Identificación electrónica del interesado – 1

- Artículo 9.2 LPAC: "los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad".
  - Certificados de firma y certificados de sello, inclusive sin dispositivos cualificados; y "sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan".
  - Si se admite un sistema de claves concertadas, es también obligatorio admitir el uso de certificados de firma o de sello.
  - Esta regla no existe en el caso de la admisión de sistemas de firma electrónica.

Identificación electrónica del interesado – 2

- Artículo 9.2 LPAC…
  - Pero no se dice dónde se deben establecer las condiciones de dicho registro, ni establece requisitos mínimos para el sistema o los medios de identificación electrónica.
  - No presupone que el sistema o el medio sea público, sino que deja espacio para la admisión de los del sector privado.
  - ¿Deberían cumplirse las condiciones del Reglamento eIDAS y el Reglamento de ejecución 2015/1502?
    - En principio, sólo si se quiere reconocimiento transfronterizo.
    - Pero también en caso contrario, dada la nueva redacción del control 4.2.1 [op.acc.1] del Anexo II del ENS, mapeo de niveles de seguridad entre el ENS y el Reglamento eIDAS, en relación con las comunicaciones electrónicas, dimensión de autenticidad.

Identificación electrónica del interesado – 3

- Artículo 9.2 LPAC…
  - No se regula qué tipo de instrumento jurídico se precisa: ¿norma reglamentaria? En el caso de la AGE, iniciativa Cl@ve
    - Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.
      - Resolución de 17 de noviembre de 2011, de la Presidencia de la AEAT.
      - Resolución de 4 de junio de 2014, del INSS.
      - Resolución de 24 de julio de 2014, de la TGSS.
    - Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve.

Identificación electrónica del interesado – 4

- Artículo 9.2 LPAC…
  - No se regula qué tipo de instrumento jurídico se precisa: ¿norma reglamentaria? En el caso de la Comunidad Autónoma de Galicia, iniciativa Chave365
    - Orden de 6 de febrero de 2014 por la que se aprueba el protocolo de identificación y firma electrónicas de la Administración general y del sector público autonómico de Galicia.
    - Resolución conjunta de 3 de septiembre de 2015, de la Vicepresidencia y Consellería de Presidencia, Administraciones Públicas y Justicia y de la Agencia para la Modernización Tecnológica de Galicia, por la que se acuerda la puesta en funcionamiento de Chave365, servicio de claves concertadas de la Administración general y del sector público autonómico de Galicia.

Identificación electrónica del interesado – 5

- Artículo 9.3 LPAC: Los sistemas admitidos por la AGE se imponen también a las demás AAPP, salvo prueba en contrario
  - Implementación del artículo 6.1 del Reglamento eIDAS (hay que suponer…), a efectos de extender el reconocimiento de sistemas de identificación electrónica de los restantes Estados Miembros.
  - ¿Y los sistemas y medios emitidos o admitidos por otras Administraciones, se pueden emplear en la AGE? Por cierto, ¿estaría el Estado obligado a notificar dichos sistemas a la Comisión, a efectos de su reconocimiento transfronterizo, o es una decisión puramente discrecional?
  - ¿Pueden ser empleados para todos los trámites? ¿O hay que considerar el nivel de seguridad que corresponda?
  - ¿Y los sistemas del sector privado? ¿Incluso aunque tengan coste para la Administración?

Firma electrónica del interesado – 1

- Artículo 11.2 LPAC: "…sólo requerirán a los interesados el uso obligatorio de firma para: a) Formular solicitudes; b) Presentar declaraciones responsables o comunicaciones; c) Interponer recursos; d) Desistir de acciones; e) Renunciar a derechos."
  - Transformación digital del procedimiento, con menos acreditación documental, y mayor prueba basada en la identidad.
  - Valoración positiva de la medida.
  - Afecta al régimen, entre otros, de la notificación, desapareciendo la firma del acuse de recibo (en línea con la regulación del servicio de entrega electrónica certificada del Reglamento eIDAS).
- También se exige firma para el apoderamiento electrónico.

Firma electrónica del interesado – 2

- Artículo 10.2 LPAC: Las AAPP admitirán sistemas de firma o sello electrónico cualificado o avanzado basado en certificado cualificado, expedidos por prestadores en la Lista de confianza; así como sistemas de clave concretada u otros que consideren válidos.
  - A diferencia del régimen de identificación (o del régimen de la Ley 11/2007), NO existe ninguna obligación de las AAPP de admitir sistemas de firma o sello avanzado, pudiendo emplear sólo sistemas de clave concertada.
  - Impacta sobre la aplicación de los artículos 27 y 37 del Reglamento eIDAS, por lo que tampoco es obligatorio admitir firmas electrónicas de ciudadanos de otros Estados miembros.
  - Hay que entender que sin perjuicio de normas sectoriales (como contratación administrativa, facturación electrónica…).

Firma electrónica del interesado – 3

- Y además, artículo 10.3 LPAC: "Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados".
  - Sustitución de la firma electrónica avanzada basada en certificado electrónico cualificado por identificación electrónica basada en certificado electrónico cualificado.
  - Orden HAP/2194/2013, de 22 de noviembre, por la que se regulan los procedimientos y las condiciones generales para la presentación de determinadas autoliquidaciones y declaraciones informativas de naturaleza tributaria, modificada por Orden HAP/455/2014, de 20 de marzo, y por Orden HAP/1846/2014, de 8 de octubre.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Astrea

Firma electrónica del interesado – 4

- […] artículo 10.3 LPAC…
  - Posibilidad de emplear una re-autenticación como medio de firma, en línea con la nueva definición de firma electrónica “ordinaria” del Reglamento eIDAS.
  - Pero ¿cómo se incorpora al expediente la acreditación de las restantes actuaciones? ¿Dónde ha ido a parar la integridad del documento? Contradictorio con artículo 10.1 LPACAP.
  - Si firmamos con un mecanismo de contraseña o de autenticación basada en certificado, ¿cómo practicamos la prueba documental? ¿Estamos abocados al fin del documento en beneficio de la pericia basada en el log?
  - En todo caso, hay que recordar lo que establece el control 5.7.4 [mp.info.4] del ENS sobre firma electrónica, que continúa siendo aplicable, en relación con nacionales y extranjeros.
    - Obligación de uso de firma o sello cualificado, sólo en nivel alto.

Firma electrónica del interesado – 5

- […] artículo 10.3 LPAC…
  - Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos
    - Producción de firma electrónica ordinaria, ya que el procedimiento previsto “sirve para firmar”, empleando, entre otros medios, el medio de identificación del firmante, un proceso previo de verificación previa de los datos a firmar y un proceso de expresión del consentimiento.
    - Complementa Cl@ve firma, que genera firma electrónica avanzada respaldada por certificado cualificado.
    - El sistema genera determinados logs, y documenta la presentación; en ambos casos, con garantías de seguridad alineadas con el Reglamento eIDAS, como el uso de sellos electrónicos de tiempo.

Identificación de la Administración Pública – 1

- Artículo 38.4 LRJSP. Seguridad de la sede electrónica
  - Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.
- Artículo 38.6 LRJSP. Seguridad de la sede electrónica
  - Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente.
  - No se debería acudir a nada que no sea un certificado de autenticación de sitio web cualificado, por falta de garantías, y bloqueo por parte de las aplicaciones informáticas de navegación web.

Identificación de la Administración Pública – 2

- Artículo 40.1 LRJSP. Sistemas de identificación
  - Las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

Firma electrónica de la Administración Pública – 1

- Artículo 41 LRJSP. Actuación administrativa automatizada
  - 1. […] cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.
  - 2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Astrea

Firma electrónica de la Administración Pública – 2

- Artículo 42 LRJSP: Mantenimiento de los mecanismos de sello electrónico y código seguro de verificación para la actuación administrativa automatizada – ¿estos documentos tienen garantizada la libre circulación en la UE?
  - El CSV, desde luego no, por no encontrarse cubierto por la Decisión 2011/130/UE (ámbito Directiva de servicios) ni Decisión de Ejecución (UE) 2015/1505 (ámbito Reglamento eIDAS, aplicable con carácter horizontal).
  - Nótese que el CSV, visto desde la perspectiva del Reglamento eIDAS, es un sello electrónico, pero no basado en certificado.
  - El sello electrónico basado en certificado, sólo si se homologa al sello de persona jurídica del Reglamento eIDAS, como se ha hecho en la Norma Técnica de Interoperabilidad de firma y sello electrónico, y de certificados de la Administración.

Firma electrónica de la Administración Pública – 3

- Artículo 43 LRJSP: Firma electrónica de titular del órgano (novedad, aunque ya se expedía), o del empleado público.
  - Mantenimiento de la regla de que cada AP decide qué sistemas de identificación y firma electrónica suministra.
- Artículo 45 LRJSP: También serán las AAPP las que deciden qué trámites o informes incorporan firma electrónica reconocida.
  - Nada aporta en este sentido el artículo 26.2 LPAC, sobre documento electrónico, que tampoco exige garantía real (=criptográfica) de la fecha, garantía que por cierto se ha regulado también en el Reglamento eIDAS.
  - Hay que entender que esta decisión se tomará de acuerdo con el ENS, que por fortuna algo dice al respecto… aunque no siempre sea fácil de aplicar.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Astrea

Gracias por vuestra atención

Para más información…

Nacho Alamillo: nacho@astrea.cat