ISACA
Trust in, and value from, information systems
Barcelona Chapter

Astrea

Las aplicaciones de firma y sello electrónico avanzado en el Reglamento eIDAS

Nacho Alamillo Domingo

Abogado, DEA, CISA, CISM, COBIT 5-f, ITIL-f

6 de febrero de 2018

ISACA
Trust in, and value from, information systems
Barcelona Chapter

Contenidos

- Introducción a los servicios de confianza.
- La firma y sello electrónicos.
- Los dispositivos de creación de firma y sello electrónico.
- Las aplicaciones de firma y sello electrónico.

Los servicios de confianza – 1

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS) – DO L 257 de 28/8/2014.
- Objetivo: reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión.
  - ¿Causa de imperiosa necesidad? Caso DigiNotar (2011).

Los servicios de confianza – 2

- No se define qué sea la confianza digital… ¿doctrina?
  - Componentes técnicos seguros habilitadores de transacciones basadas en riesgos (Baldwin, Shiu, & Cassasa Mont, 2000).
  - Ausencia de percepción de vulnerabilidades (Ølnes, 2001).
  - Estado interno del usuario evocado por las características de fiabilidad de la tecnología, una aceptación informada de la vulnerabilidad (Dumortier & Vandezande, 2012).
- Propuesta: Aquellas tecnologías en las que se puede confiar, por lo que modifican la percepción del usuario con respecto a la vulnerabilidad de un proceso al que se incorporan. Para ello, el usuario debe poder reconocer un servicio de confianza, de hecho, como suficientemente confiable.

Los servicios de confianza – 3

- 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.
- Es un tipo de servicio de la sociedad de la información.

La firma/sello electrónicos – 1

- La firma electrónica acredita la actuación de las personas, de acuerdo con lo dispuesto en la LFE y el Reglamento eIDAS (sólo para personas físicas, a diferencia de la LFE).
- El sello electrónico acredita el origen e integridad de los datos de persona jurídica (sólo previsto en el Reglamento eIDAS).
- Tipos de reconocimiento legal de la firma/sello
  - Reconocimiento general: principio de no discriminación.
  - Reconocimiento directo: principio de equivalencia funcional.
- Tipos legales de firma/sello electrónicos
  - Firma/sello ordinario.
  - Firma/sello avanzado.
  - Firma/sello cualificado.

La firma/sello electrónicos – 2

- Reconocimiento general: principio de no discriminación
  - La legislación establece la validez legal de la firma/sello electrónicos, y su acceso al proceso judicial, firma/sello a los que no se podrá negar efectos únicamente por el hecho de encontrarse en forma electrónica.
  - Toda firma/sello puede ser válida, pero ... ¿lo será cuando lo necesitemos?
  - A pesar de ser admitido nuestro documento firmado/sellado, ¿recibirá finalmente efectos, o será rechazado por dudas o prejuicios? ¿O por la incapacidad de demostrar que efectivamente firmó/selló la otra parte?
  - ¿Podemos confiar en el funcionamiento de las administraciones con base en la opinión y la convicción de cada juez?

La firma/sello electrónicos – 3

- Reconocimiento directo: principio de equivalencia funcional
  - La legislación define efecto típico y directo, *ex lege*, sólo a un tipo de firma/sello electrónica que se podrá emplear en todo caso y situación.
  - Por eso se llama “cualificado": se trata de la firma electrónica que es funcionalmente equivalente a la firma escrita, que cualifica para sustituir en todo caso a una firma escrita.
  - Sólo esta firma sirve para todo lo que puede hacer una persona, sin necesidad de ninguna "norma" ni contrato que autorice o limite el uso (más allá, obviamente, del contrato con el prestador de servicios de certificación que emite el certificado).
  - Más difícil puede ser, sin embargo, determinar la utilidad del sello cualificado, que es una figura nueva del Reglamento eIDAS.

La firma/sello electrónicos – 4

- Firma electrónica “ordinaria”
  - Definición
    - Art. 3.10 Reglamento eIDAS: “los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar”.
  - Todos los mecanismos de autenticación pueden ser firma electrónica ordinaria, y en especial la contraseña y otros mecanismos no criptográficos, pero siempre que atiendan a esta finalidad.
  - Habitualmente se utilizan en grupos «cerrados» de usuarios, que se autorregulan con contratos (incluso también dentro de las administraciones públicas).

La firma/sello electrónicos – 5

- Firma electrónica “ordinaria”
  - Efectos jurídicos
    - Art. 25.1 Reglamento eIDAS: “No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada”.
  - Pero se le pueden negar efectos por otros motivos
    - Que no sea suficientemente segura (concepto jurídico indeterminado)
    - Que no garantice que haya sido creada por el firmante
    - Que sea reproducible
  - No se equipara directamente a la firma escrita, sino que requiere una norma jurídica de legitimación. Procesalmente, puede ser una *probatio diabolica*.

La firma/sello electrónicos – 6

- Firma electrónica avanzada
  - Definición
    - Art. 3.11 Reglamento eIDAS: “la firma electrónica que cumple los requisitos contemplados en el artículo 26”.
    - Art. 26 Reglamento eIDAS: “Una firma electrónica avanzada cumplirá los requisitos siguientes: a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable”.

La firma/sello electrónicos – 7

- Firma electrónica avanzada
  - Concepto supuestamente neutral, aunque sólo “mapea” bien con algoritmos de criptografía asimétrica.
  - Puede basarse, o no, en claves certificadas.
  - Cuando se basa en certificado reconocido, es el nivel mínimo para la tramitación por parte de los ciudadanos (FNMT-RCM Clase 2 CA, idCAT), así como para algunas categorías de trabajadores públicos (nivel medio de los perfiles de CertiCA, de acuerdo con la ley 11/2007).
  - Complementa el DNI electrónico y otros instrumentos en dispositivo seguro de creación de firma electrónica.
  - Actualmente en crisis por las restricciones al empleo de Java en los navegadores, se desplaza hacia nuevos dispositivos, principalmente con centralización de claves (“en Nube”).

La firma/sello electrónicos – 8

- Firma electrónica avanzada
  - Efectos jurídicos, de acuerdo con el artículo 25.1 Reglamento eIDAS.
  - Pero se le pueden negar efectos por otros motivos:
    - Que no sea suficientemente segura (algoritmos débiles)
    - Que no garantice que haya sido creada por el firmante (compromiso de clave)
    - Que sea reproducible (ataques por fuerza bruta)
  - No se equipara directamente a la firma escrita, pero puede hacerlo, aunque normalmente requiere una norma jurídica de autorización, o un contrato entre las partes.
  - La prueba resulta más razonable, ya que al menos disponemos de una evidencia con base matemática que vincula la identidad electrónica del firmante con el documento firmado.

La firma/sello electrónicos – 9

- Firma electrónica reconocida/cualificada
  - Definición
    - Art. 3.12 Reglamento eIDAS: “una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica”.
  - Es una firma electrónica avanzada de calidad:
    - Garantiza que ha firmado una persona física.
    - Garantiza la posibilidad de visualización del documento por el firmante.
    - Garantiza la aprobación o prestación del consentimiento.
  - Se basa en un certificado cualificado, definido legalmente.
  - Ha sido generada empleando un dispositivo cualificado de creación de firma, definido legalmente (tarjeta soporte del DNI-e, o HSM).

La firma/sello electrónicos – 10

- Firma electrónica reconocida/cualificada
  - Efectos jurídicos
    - Artículo 25.2 Reglamento eIDAS: "Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita".
    - Artículo 25.3 Reglamento eIDAS: "Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros".
  - La equiparación es *ex lege* y total, sin necesidad de ninguna otra norma jurídica de cobertura, si bien de ello no se desprende necesariamente el derecho a su uso, que quedará sujeto a pacto o a lo que establezca la normativa sectorial.

La firma/sello electrónicos – 11

- Sello electrónico de persona jurídica
  - Definición
    - Art. 3.25 Reglamento eIDAS, sello electrónico "ordinario": "datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos".
    - Art. 3.26 Reglamento eIDAS, sello electrónico avanzado: "un sello electrónico que cumple los requisitos contemplados en el artículo 36".
    - Art. 36 Reglamento eIDAS: "un sello electrónico avanzado cumplirá los requisitos siguientes: a) estar vinculado al creador del sello de manera única; b) permitir la identificación del creador del sello; c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo, y d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable."

La firma/sello electrónicos – 12

- Sello electrónico de persona jurídica
  - Definición
    - Art. 3.27 Reglamento eIDAS, sello electrónico cualificado: "un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico".
  - Efectos jurídicos
    - Art. 35.1 Reglamento eIDAS, sello electrónico "ordinario" o avanzado: "No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado".
    - Artículo 35.2 Reglamento eIDAS: "Un sello electrónico cualificado disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado".

La firma/sello electrónicos – 13

- Sello electrónico de persona jurídica
  - Efectos jurídicos
    - Artículo 35.3 Reglamento eIDAS: “Un sello electrónico cualificado basado en un certificado cualificado emitido en un Estado miembro será reconocido como un sello electrónico cualificado en todos los demás Estados miembros”.

La firma/sello electrónicos – 14

- Validación de la firma/sello electrónicos
  - Artículos 32.1 y 40 Reglamento eIDAS
    - El proceso de validación de una firma electrónica cualificada confirmará la validez de una firma electrónica cualificada siempre que:
      - a) el certificado que respalda la firma fuera, en el momento de la firma, un certificado cualificado de firma electrónica que se ajusta al anexo I;
      - b) el certificado cualificado fuera emitido por un prestador de servicios de confianza y fuera válido en el momento de la firma;
      - c) los datos de validación de la firma corresponden a los datos proporcionados a la parte usuaria;
      - d) el conjunto único de datos que representa al firmante en el certificado se facilite correctamente a la parte usuaria;
      - e) en caso de que se utilice un seudónimo, la utilización del mismo se indique claramente a la parte usuaria en el momento de la firma;
      - f) la firma electrónica se haya creado mediante un dispositivo cualificado de creación de firmas electrónicas;
      - g) la integridad de los datos firmados no se haya visto comprometida;
      - h) se hayan cumplido los requisitos previstos en el artículo 26, en el momento de la firma.

La firma/sello electrónicos – 15

- Validación de la firma/sello electrónicos
  - Artículos 32.2 y 40 Reglamento eIDAS
    - El sistema utilizado para validar la firma electrónica cualificada ofrecerá a la parte usuaria el resultado correcto del proceso de validación y le permitirá detectar cualquier problema que afecte a la seguridad.
  - Artículos 33.1 y 40 Reglamento eIDAS
    - Solo podrá prestar un servicio de validación cualificado de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que:
      - a) realice la validación de conformidad con el artículo 32, apartado 1, y
      - b) permita que las partes usuarias reciban el resultado del proceso de validación de una manera automatizada que sea fiable, eficiente e incluya la firma electrónica avanzada o el sello electrónico avanzado del prestador cualificado de servicio de validación.
    - No se establece presunción alguna, pero facilita la prueba.

Los dispositivos de creación de firma y sello – 1

- Modalidad “ordinaria”
  - Un equipo o programa informático configurado que se utiliza para crear una firma electrónica (art. 3.22 del Reglamento eIDAS).
  - Un equipo o programa informático configurado que se utiliza para crear un sello electrónico (art. 3.31 del Reglamento eIDAS).
  - No se define para la autenticación de sitio web.
- Modalidad “cualificada”
  - Un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II (art. 3.23 del Reglamento eIDAS).
  - Un dispositivo de creación de sellos electrónicos que cumple *mutatis mutandis* los requisitos enumerados en el anexo II (art. 3.32 del Reglamento eIDAS).
  - Tampoco se define para la autenticación de sitio web.

Los dispositivos de creación de firma y sello – 2

- Requisitos Anexo II
  - 1. Los dispositivos cualificados de creación de firma electrónica garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:
    - a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas;
    - b) los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica;
    - c) exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento;
    - d) los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.

Los dispositivos de creación de firma y sello – 3

- Requisitos Anexo II
  - 2. Los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.
  - 3. La generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante solo podrán correr a cargo de un prestador cualificado de servicios de confianza.

Los dispositivos de creación de firma y sello – 4

- Requisitos Anexo II
  - 4. Sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:
    - a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;
    - b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

Los dispositivos de creación de firma y sello – 5

- Requisitos legales (artículos 29 y 39.1 del Reglamento eIDAS)
  - 1. Los dispositivos cualificados de creación de [firmas/sellos] electrónicas cumplirán los requisitos establecidos en el anexo II.
  - 2. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los dispositivos cualificados de creación de firmas electrónicas. Se presumirá el cumplimiento de los requisitos establecidos en el anexo II cuando un dispositivo cualificado de creación de [firmas/sellos] electrónicas se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Los dispositivos de creación de firma y sello – 6

- Certificación de los dispositivos (artículos 30 y 39.2 del Reglamento eIDAS)
  - 1. La conformidad de los dispositivos cualificados de creación de firmas electrónicas con los requisitos que figuran en el anexo II será certificada por los organismos públicos o privados adecuados designados por los Estados miembros.
  - 2. Los Estados miembros notificarán a la Comisión los nombres y direcciones de los organismos públicos o privados a que se refiere el apartado 1. La Comisión pondrá la información a disposición de los Estados miembros.

Los dispositivos de creación de firma y sello – 7

- Certificación de los dispositivos (artículos 30 y 39.2 del Reglamento eIDAS)
  - 3. La certificación contemplada en el apartado 1 se basará en los elementos siguientes:
    - a) un proceso de evaluación de la seguridad llevado a cabo de conformidad con las normas para la evaluación de la seguridad de los productos de tecnología de la información incluidos en la lista que se establecerá de conformidad con el párrafo segundo, o
    - b) un proceso distinto del proceso contemplado en la letra a), con tal de que ese proceso haga uso de niveles de seguridad equivalentes y que los organismos públicos o privados a los que se refiere el apartado 1 notifiquen ese proceso a la Comisión. Podrá recurrirse a ese proceso únicamente a falta de las normas a que se refiere la letra a) o cuando esté en curso el proceso de evaluación de la seguridad a que se refiere la letra a).

Los dispositivos de creación de firma y sello – 8

- Certificación de los dispositivos (artículos 30 y 39.2 del Reglamento eIDAS)
  - La Comisión establecerá, por medio de actos de ejecución, la lista de las normas para la evaluación de la seguridad de los productos de tecnología de la información a que se refiere la letra a). Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.
  - 4. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 47, en lo que respecta al establecimiento de criterios específicos que deben satisfacer los organismos designados a que se refiere el apartado 1 del presente artículo.
  - La certificación **no alcanza a las aplicaciones de creación de firma/sello**, sólo al dispositivo.

Los dispositivos de creación de firma y sello – 9

- Certificación de los dispositivos (artículos 30 y 39.2 del Reglamento eIDAS)
  - Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento eIDAS
    - Cuando los datos de creación de firma electrónica o los datos de creación de sello electrónico se conservan íntegramente, aunque no necesariamente de forma exclusiva, en un entorno gestionado por el usuario: EN 419 211, partes 1 a 6, según aplique.
    - Cuando un prestador cualificado de servicios de confianza gestione los datos de creación de firma electrónica o los datos de creación del sello electrónico en nombre de un firmante o de un creador de un sello: niveles de seguridad equivalentes a EN 419 211, partes 1 a 6, según aplique.

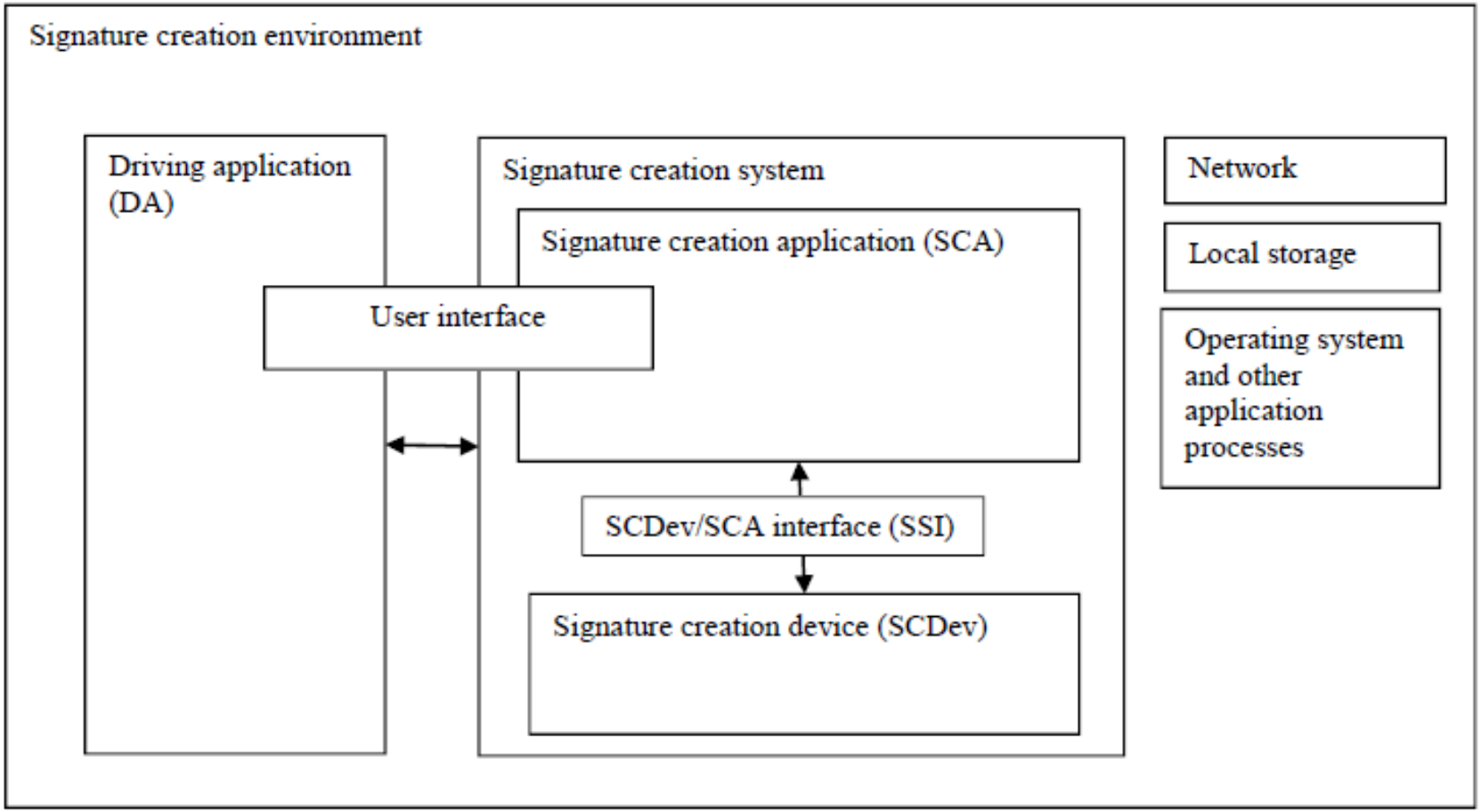
Los dispositivos de creación de firma y sello – 10

- Publicidad de los dispositivos (artículos 31 y 39.3 del Reglamento eIDAS)
  - 1. Los Estados miembros comunicarán a la Comisión, sin retrasos indebidos y no más tarde de un mes después de que haya concluido la certificación, información sobre los dispositivos cualificados de creación de [firmas/sellos] electrónicas que hayan sido certificados por los organismos a que se refiere el artículo 30, apartado 1. También notificarán a la Comisión, sin retrasos indebidos y no más tarde de un mes después de que haya expirado la certificación, información sobre los dispositivos de creación de firmas electrónicas que hayan dejado de estar certificados.

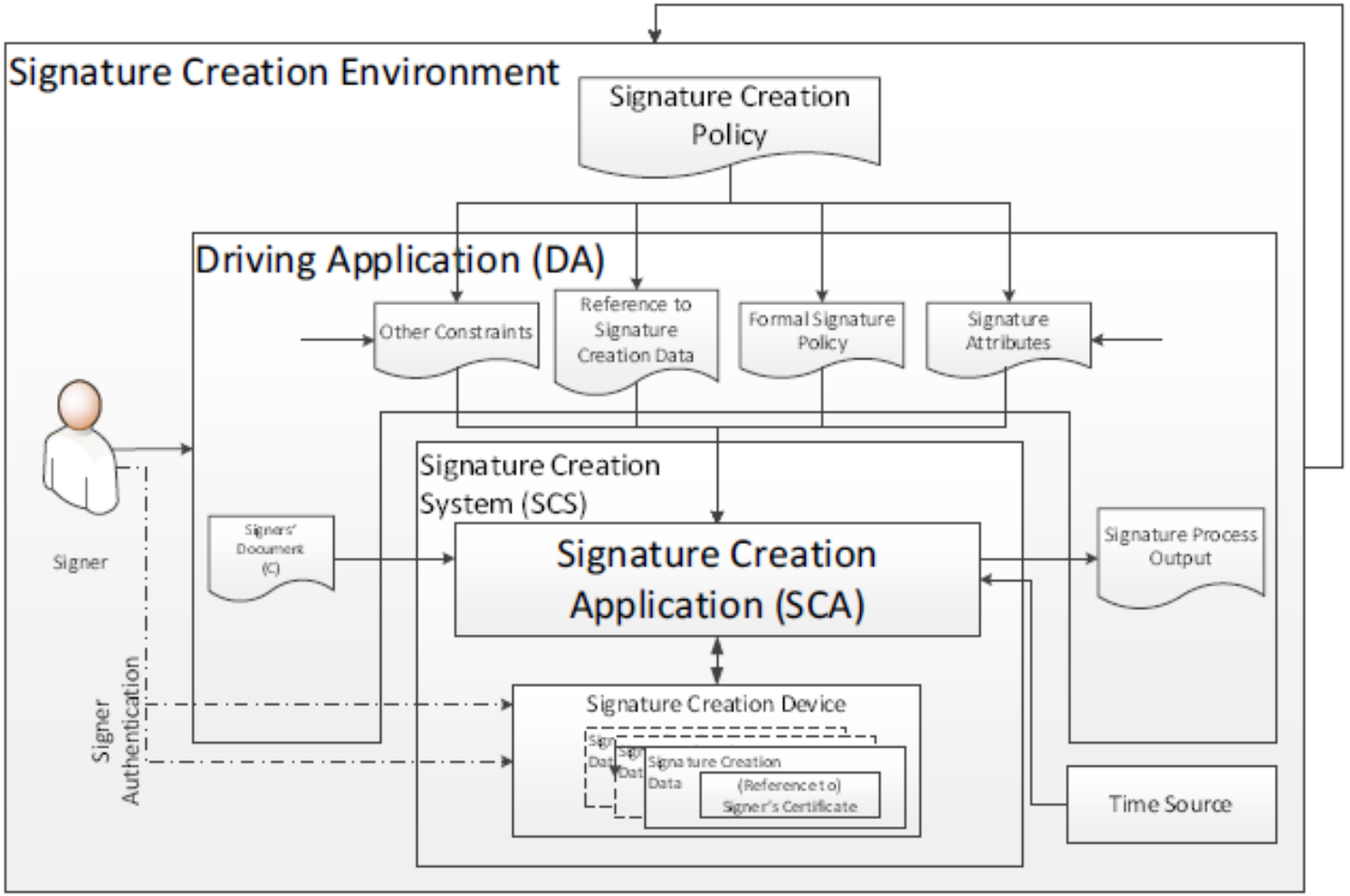
Los dispositivos de creación de firma y sello – 11

- Publicidad de los dispositivos (artículos 31 y 39.3 del Reglamento eIDAS)
  - 2. Sobre la base de la información recibida, la Comisión establecerá, publicará y mantendrá una lista de dispositivos cualificados de creación de [firmas/sellos] electrónicas certificados.
  - 3. La Comisión podrá, mediante actos de ejecución, definir los formatos y procedimientos aplicables a efectos del apartado 1. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

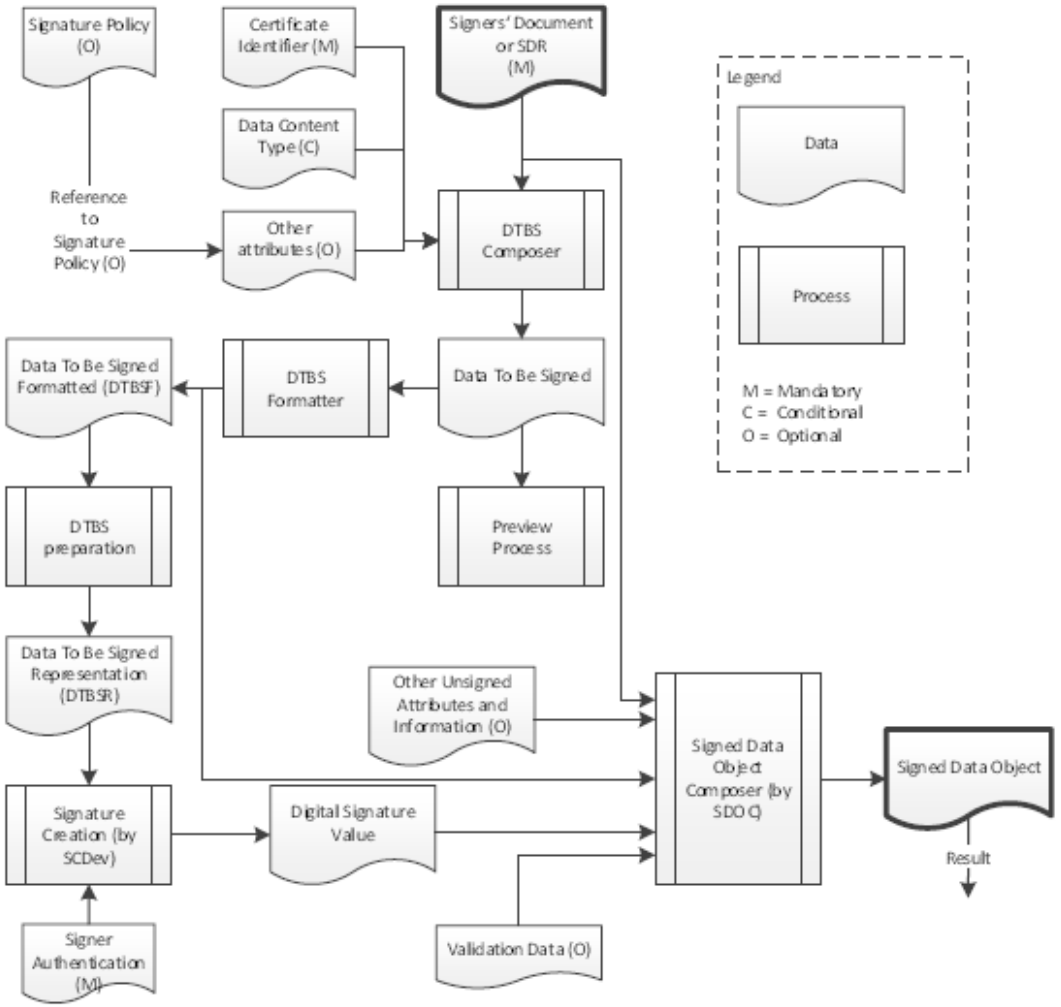
Las aplicaciones de creación de firma y sello – 1



Las aplicaciones de creación de firma y sello – 2



Las aplicaciones de creación de firma y sello – 3



Las aplicaciones de creación de firma y sello – 4

- Objetivos de control específicos (ETSI TS 119 101)
  - Asegurar que las funcionalidades principales de la aplicación se encuentran documentadas.
  - Asegurar que el formato de firma es apropiado para los tipos de datos del documento a firmar/sellar y resulta conforme a cualquier requisito legal o de negocio.
  - Asegurar que el verificador no puede malinterpretar el documento del firmante/creador de sellos debido a falta de información sobre el tipo de datos del documento, sintaxis errónea, presentación defectuosa o falta de presentación.
  - Asegurar que la firma/sello es aplicada al documento del firmante/creador de sellos correcto.

Las aplicaciones de creación de firma y sello – 5

- Objetivos de control específicos (ETSI TS 119 101)
  - Asegurar que el firmante/creador de sellos no firma/sella inadvertidamente otros objetos de firma/sello inválidos creados por terceros, y que el firmante/creador de sellos es capaz de conocer qué firmas/sellos han sido validados o dejados sin validar.
  - Asegurar que el firmante/creador de sellos no altera el documento a firmar/sellar de forma accidental.
  - Asegurar que la aplicación de creación de firma/sello recibe suficiente información para ser capaz de presentar de forma precisa el documento a firmar/sellar en la interfaz de usuario.
  - Asegurar que un documento a firmar/sellar con contenido oculto capaz de modificar la presentación del documento sin afectar a su validez criptográfica no engaña al verificador y/o al firmante/creador de sellos.

Las aplicaciones de creación de firma y sello – 6

- Objetivos de control específicos (ETSI TS 119 101)
  - Asegurar que el firmante/creador de sellos no firma/sella inconscientemente un contenido o un compromiso.
  - Asegurar que la firma/sello se aplica sobre los atributos correctos y que los mismos no son alterados accidental o maliciosamente.
  - Asegurar que se utiliza un certificado correcto y no expirado. Si es posible, asegurar que el certificado no se encuentra revocado en el momento de la creación de la firma/sello.
  - Asegurar que la firma/sello incluye el certificado de firma/sello correcto, o la referencia al mismo, y que esta información está protegida frente a ataques de sustitución.
  - Asegurar que la firma/sello contiene todos los atributos necesarios para el propósito de la firma/sello, y que el firmante es consciente del propósito de su firma.

Las aplicaciones de creación de firma y sello – 6

- Objetivos de control específicos (ETSI TS 119 101)
  - Asegurar que el firmante/creador de sellos conoce qué política se aplica, caso que haya varias disponibles.
  - Asegurar que la política explícita de creación de firma es trasmitida a las partes que confían.
  - Asegurar que el proceso de creación de firma/sello sigue la secuencia prevista de eventos.
  - Asegurar que cada firma/sello creado es resultado de una invocación explícita de firma.
  - Impedir periodos de inactividad prolongada tras la autenticación del firmante/creador de sellos.
  - Impedir situaciones de engaño al firmante/creador de sellos que permitan el acceso a información confidencial por parte de terceros.

Las aplicaciones de creación de firma y sello – 7

- Objetivos de control específicos (ETSI TS 119 101)
  - Asegurar que todos los algoritmos empleados resultan apropiados para las necesidades de negocio.
  - Asegurar que sólo el usuario legítimo de dispositivo de creación de firma/sello puede solicitar la creación de firmas digitales.
  - Asegurar que los ataques de fuerza bruta son contrarrestados.
  - Asegurar que no es posible observar los datos de autenticación del firmante/creador de sellos.
  - Asegurar que un atacante no puede inyectar en la aplicación componentes falsificados de firma/sello.
  - Asegurar la correcta composición de la representación de los datos a firmar/sellar.
  - Asegurar que se emplea un dispositivo de creación apropiado (por ejemplo, cualificado).

Las aplicaciones de creación de firma y sello – 8

- Objetivos de control específicos (ETSI TS 119 101)
  - Asegurar que se emplea el dispositivo de creación de forma correcta.
  - Asegurar que la comunicación entre la aplicación y el dispositivo de creación de firma/sello se encuentra protegida.
  - Asegurar que un proceso de firma por lotes no es menos seguro que un proceso donde cada documento sería firmado/sellado de forma independiente, y que no se firman/sellan documentos no pretendidos por el firmante/creador de sellos.

Las aplicaciones de creación de firma y sello – 9

- Uso de terceros interpuestos
  - De especial valor en ausencia de *driving applications* cuya seguridad haya sido certificada (por ejemplo, mediante Common Criteria).
  - Actúan como control compensatorio general, desde la perspectiva de los contenidos a firmar/sellar puestos a disposición de forma previa.
  - Acreditan el tiempo en que suceden los eventos.
  - Almacenan los documentos firmados/sellados, con garantía frente a incidencias criptográficas.
  - Sus garantías se proyectan también sobre procesos que no se basan en el uso de firmas digitales.

ISACA
Trust in, and value from, information systems
Barcelona Chapter

Astrea

Gracias por su atención

¿Dudas?

Nacho Alamillo: nacho@astrea.cat