víntegris

ISACA®
Trust in, and value from, information systems

CERTIFICADOS ELECTRÓNICOS EN ENTORNOS CORPORATIVOS.
USOS, RIESGOS , MEDIOS DE CONTROL Y AUDITORIA

Salvador Simarro Ferrer. Responsable de Consultoría en VÍNTEGRIS, S.L. CISA, MGTI.
José María Jimenez de la Concepción. Director Técnico en VÍNTEGRIS, S.L. CISA, CISSP

AENOR
ER
Seguridad Información
UNE-ISO/IEC 27001

Usos

En el ámbito que tratamos hoy consideramos como uso general de los certificados el de:

Almacenamiento e intercambio de información de forma segura en los aspectos de

✓Integridad, y Confidencialidad de la información *(Esta información también puede ser información de identificación y autenticación en sistemas de control de acceso)*

✓Disponibilidad de la información y del propio Certificado

Usos

FIRMA DE DOCUMENTOS INTERNOS, asegurando su

✓origen,

✓integridad y

✓confidencialidad

(con la necesidad, incluso, después de haber sido recibidos y abiertos en destino en caso de soluciones de correo)

Y como solución de seguridad en Work-Flows.

Usos

IDENTIFICACIÓN – y firma- DE PERSONA FÍSICA Y/O JURÍDICA en

✓Ámbitos organizativos internos

- Nivel empresa
- Nivel Grupo o Corporación (información consolidada o agregada)

✓Ámbitos organizativos externos

- Interoperabilidad entre administraciones, empresas públicas o empresas privadas afectadas por el tipo de colaboración o seguridad exigido.

✓Aplicaciones de emisión de facturas, contratos, pólizas, u otros documentos masivos y/o genéricos

Marco legal y afectación en otras leyes

Principal: Ley 59/2003, de 19 de diciembre, de firma electrónica. regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación

La legislación básica sobre firma electrónica se recoge en la *Ley 59/2003, de 19 de diciembre*, de Firma Electrónica.
Art. 3.1) La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
Además, la Ley distingue entre dos tipos de firma, la 'firma electrónica avanzada' y la 'firma electrónica reconocida':
Art. 3.2) La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
(Art. 3.3) Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
Según la ley, la **firma electrónica reconocida** es la única que puede ser considerada equivalente a la firma manuscrita:
(Art. 3.4) La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel.

Marco legal y afectación en otras leyes

Ley 59/2003, de 19 de diciembre PROPIEDADES Y REQUISITOS DE LA FIRMA ELECTRÓNICA RECONOCIDA
Una firma electrónica reconocida debe cumplir las siguientes propiedades o requisitos:

- ✓Identificar al firmante
- ✓Verificar la integridad del documento firmado
- ✓Garantizar el no repudio en el origen
- ✓Contar con la participación de un tercero de confianza
- ✓Estar basada en un certificado electrónico reconocido
- ✓Debe de ser generada con un dispositivo seguro de creación de firma

Los 4 primeros puntos son posibles gracias al uso de las **claves criptográficas** contenidas en el certificado y a la existencia de una estructura de **Autoridades de Certificación** que ofrecen confianza en la entrega de los certificados. Pero según la *Ley 59/2003*, esos 4 puntos sólo nos ofrecen una firma avanzada.
Para que la firma electrónica sea **equivalente a la manuscrita**, es decir, que una Firma electrónica sea reconocida, debe además:

Estar **basada en un Certificado Reconocido.** El certificado debe haber sido reconocido por el Ministerio de Industria y Comercio como habilitado para crear firmas reconocidas y debe estar listado en su página web como tal.

Marco legal y afectación en otras leyes

Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

En el capítulo I de la Ley se introducen los preceptos dirigidos a impulsar el empleo de la **factura electrónica** y del uso de medios electrónicos en todas las fases de los procesos de contratación y a garantizar **una interlocución electrónica** de los usuarios y consumidores con las empresas que presten determinados servicios de especial relevancia económica.

- ✓Artículo 1. Medidas de impulso de la factura electrónica y del uso de medios electrónicos en otras fases de los procesos de contratación.
- ✓ Artículo 2. Obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica.
- ✓Artículo 3. Ofertas públicas de contratación electrónica entre empresas.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD

Impacto General

Tal y como hemos visto en el uso de certificados es obligado en múltiples facetas del ámbito comercial y jurídico – además del personal-.

En los aspectos de relaciones con las AAPP, será potenciado – obligado- aún más. Siendo así, que

AUMENTARÁ – está aumentando- EL NÚMERO DE CERTIFICADOS EN CIRCULACIÓN Y SU USO.

Impacto General

En el ámbito de la empresa privada o corporativo, estamos viendo como está incrementando la cantidad de certificados existentes – y a gestionar- en los aspectos de :

- ✓Protección de la Propiedad Intelectual
- ✓Identificadores de personas
- ✓Identificadores de y en aplicaciones (firma de persona jurídica o de representante, Autenticado de aplicación).
- ✓Integridad de código
- ✓Firma de documentos
- ✓Firma delegada de documentos
- ✓Otros.

Riesgos

La extensión del uso de certificados y de firma electrónica requiere de la existencia de certificados instalados en los dispositivos de firma –cuya seguridad aplicable dependerá de la tipología de: los certificados, los documentos y los procesos a tratar.

El actual crecimiento propicia la existencia de certificados en múltiples estaciones de trabajo, servidores, etc., creciendo, a su vez, los riesgos derivados de un control inadecuado.
En un primer enfoque, entre otros posibles, los podemos agrupar en:

EXTRALIMITACIÓN EN EL USO.

Uso de los certificados más allá de los poderes necesarios o establecidos para los certificados.

SUPLANTACIÓN DE IDENTIDAD.

Uso por personas físicas fuera de sus funciones autorizadas *-por error de diseño de flujos , por error técnico de diseño de arquitectura, por acción voluntaria, otros-* o en nombre de otras personas.

Riesgos

INDISPONIBILIDAD DE LOS CERTIFICADOS.

La ubicación dispersa de los certificados y la falta de procedimientos de renovación acrecienta el riesgo, o bien exige medidas de seguridad inasumibles por rendimiento o por coste.

AUDITORÍA Y CONTROL del USO

La dispersión y la ubicación en dispositivos o sistemas no preparados para mantener los registros de control y auditoría referentes al uso de certificados y firmas hacen prácticamente imposible el control debido.

Riesgos

Y desde un punto de vista práctico….., lo anterior se puede plasmar a modo de resumen en:

- ¿**QUÉ CERTIFICADOS**, de los usados o existentes, **HAN SALIDO** o han sido exportados fuera de los límites "seguros" de la organización? - pensemos, para empezar

- ¿**CONOCEMOS TODAS LAS FIRMAS** y sobre qué documentos u objetos se han realizado? , **¿Cuándo?, ¿Por Quién**?

- ¿Tenemos documentados todos **LOS PROCESOS DE FIRMA** incluyendo los de firma externos? - p.e. relaciones con SEGURIDAD SOCIAL, RED, DELTA, HACIENDA, REGISTRO MERCANTIL, ETC.

- ¿Tenemos un **CONTROL SOBRE LA EXPIRACIÓN** y fechas de renovación de los certificados? ¿Se ha valorado el impacto de un **certificado de servidor CADUCADO**? Webservices sin funcionar, fallo de imagen, Pérdida de negocio..

Riesgos

- ¿**Conocemos exactamente QUIÉN** –persona física- **utiliza QUÉ** certificados en nuestra organización?

- ¿**Se han efectuado firmas no previstas y sin control**?, ¿Cómo lo sabemos?

- ¿Tenemos asegurados - disponibilidad- los certificados personales usados en relaciones externas?, **¿y en caso de baja del empleado?** Y entonces … la LOPD!!

En conclusión, es necesario implantar o mejorar, soluciones que nos permitan tener un control absoluto sobre el uso y la seguridad de los certificados.

Posibles Soluciones

- Disponer y mantener políticas, técnicas y organizativas, de instalación y uso de certificados.
- Alinear de forma inequívoca los certificados con las funciones organizativas y personales (Directorios, RRHH, organigramas, etc.).
- Uso de repositorios corporativos seguros de certificados, centralizados.
- Uso de un sistema eficiente de control de acceso.
- Disponer de herramientas de registro de eventos logs seguras para el seguimiento, control y auditoría de las operaciones efectuadas con los certificados y sobre los propios certificados.

SIEMPRE EVALUANDO LA EFICIENCIA

Nuestra Experiencia

Auditoria de Gestión de Certificados Digitales

- Revisiones de estado y Normativas de Uso de Certificados Digitales

Consultoría y Soluciones de Uso de Certificados Digitales

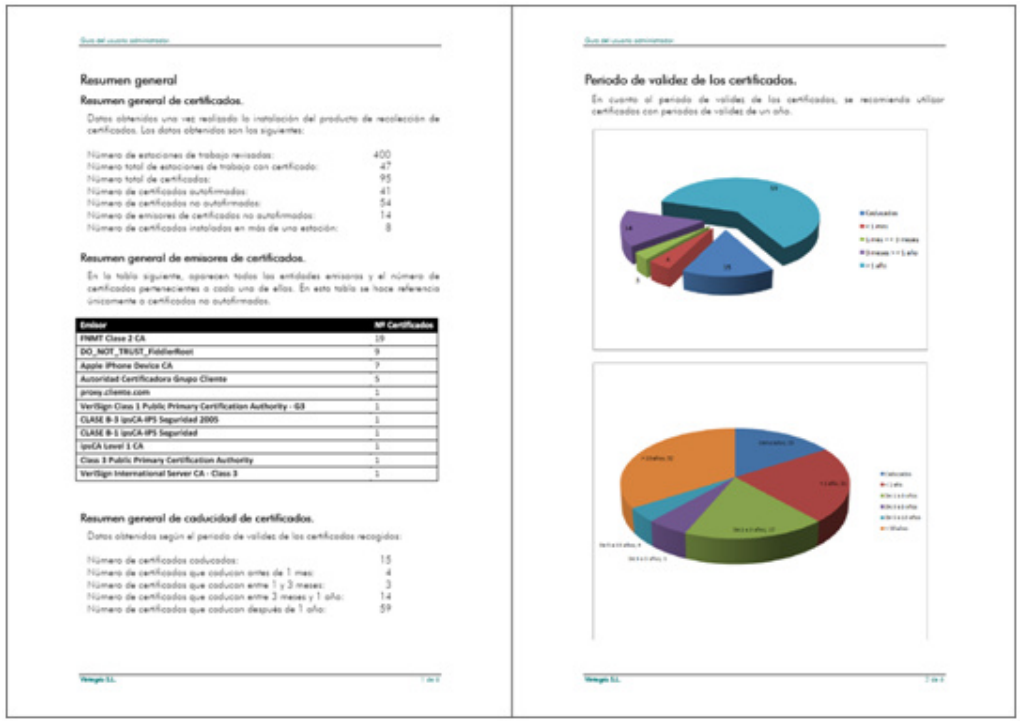
- Definición y Establecimiento de Normas de Uso de Certificados Digitales
- Tecnologías de descubrimiento de certificados y centralización de uso de certificados

Auditoria de Gestión de Certificados Digitales

- Revisión de Normas del cliente (si tiene)
- Inventario de certificados del cliente (si tiene)
- Revisión de los certificados instalados en la entidad con objeto de obtener Inventario Actualizado:
  - Certificados de Servidor
  - Certificados Personales/P.F./P.J.

Se utilizan tecnologías de "Discover":

- Certificados de servidor
- Certificados instalados por estación
- Estaciones más críticas
- Longitudes de clave, algoritmos
- Inventario de Emisores



Resumen general

Resumen general de certificados.

Datos obtenidos una vez realizado la instalación del producto de recolección de certificados. Los datos obtenidos son los siguientes:

Número de estaciones de trabajo revisadas:	400
Número total de estaciones de trabajo con certificado:	47
Número total de certificados:	95
Número de certificados autofirmados:	41
Número de certificados no autofirmados:	54
Número de emisores de certificados no autofirmados:	14
Número de certificados instalados en más de una estación:	8

Resumen general de emisores de certificados.

En la tabla siguiente, aparecen todas las entidades emisoras y el número de certificados pertenecientes a cada una de ellas. En esta tabla se hace referencia únicamente a certificados no autofirmados.

Emisor	Nº Certificados
FNMT Clase 2 CA	19
DO_NOT_TRUST_FiddlerRoot	9
Apple iPhone Device CA	7
Autoridad Certificadora Grupo Cliente	5
proxy.cliente.com	1
VeriSign Class 1 Public Primary Certification Authority - G3	1
CLASE B-3 IpsCA-IPS Seguridad 2005	1
CLASE B-1 IpsCA-IPS Seguridad	1
IpsCA Level 1 CA	1
Class 3 Public Primary Certification Authority	1
VeriSign International Server CA - Class 3	1

Resumen general de caducidad de certificados.

Datos obtenidos según el periodo de validez de los certificados recogidos:

Número de certificados caducados:	15
Número de certificados que caducan antes de 1 mes:	4
Número de certificados que caducan entre 1 y 3 meses:	3
Número de certificados que caducan entre 3 meses y 1 año:	14
Número de certificados que caducan después de 1 año:	59

Periodo de validez de los certificados.

En cuanto al periodo de validez de los certificados, se recomienda utilizar certificados con periodos de validez de un año.

víntegris

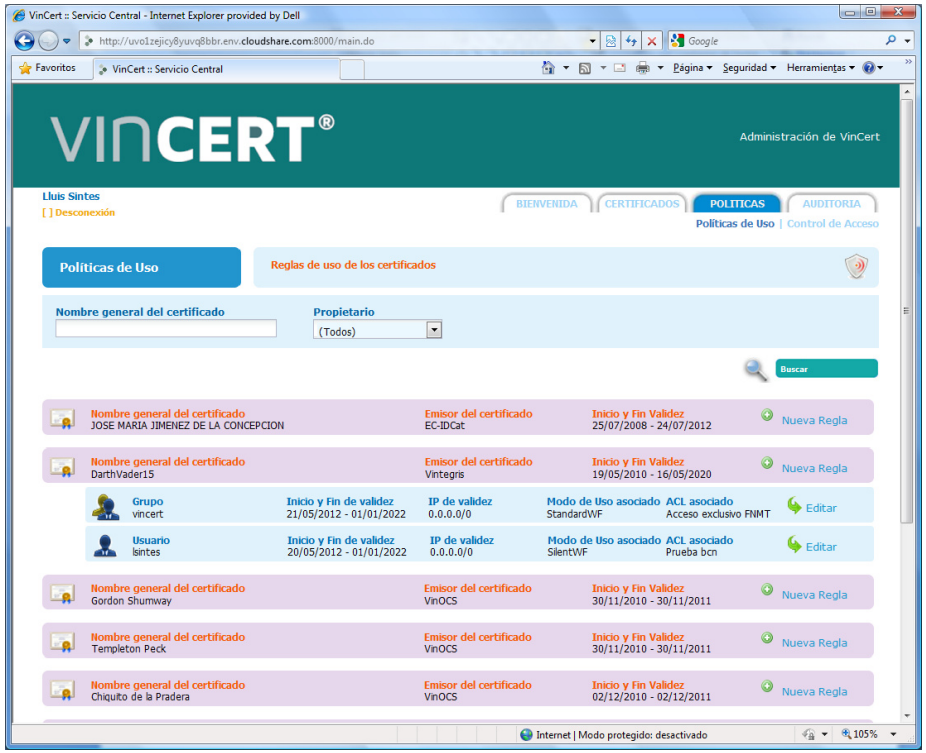
ISACA
Trust in, and value from, information systems

¿Qué nos encontramos como resultado de los descubrimientos en conclusión con los clientes?

- Más certificados instalados de los que es consciente el cliente o tiene inventariados
- Certificados críticos de servidor a punto de caducar (servicios SSL)
- Certificados personales a punto de caducar
- Certificados instalados en las estaciones de trabajo que no tienen ninguna relación con la actividad habitual de la corporación.
- Certificados instalados en estaciones, no inventariados, y que sí que tienen importancia en la actividad de la empresa.
- Certificados personales instalados en estaciones donde en principio no deberían de estar.
- Estaciones de trabajo "críticas": Aquellos terminales donde se concentra gran cantidad de certificados personales físicos o jurídicos.
- En algunos casos, certificados generados con CA interna de la entidad que se desconoce dónde está.

Tecnología Existente en Mercado

- Descubrimiento de Certificados
- Control de Uso de Certificados
- Gestión y Ciclo de Vida de Certificados
- HSM's



vintegris

ISACA®
Trust in, and value from, information systems

Puntos de Reflexión y Discusión

- Es de suma importancia estar preparados adecuadamente para gestionar y utilizar de forma segura y eficiente las necesidades de firma electrónica y usos de certificados en nuestras organizaciones.

- Uno de los elementos determinantes para un uso eficaz y seguro es la tecnología de soportes de los certificados. Pensemos que no es lo mismo distribuir y mantener 15000 certificados o identificadores en una tarjeta personal que en software.
  - (Con PIN o sin PIN)
  - (O bien el uso de HSM en ciertos tipos de proceso)

- Como profesionales de la auditoría y el control, ¿qué niveles y medidas de seguridad debemos exigir a las implementaciones de uso de firma y certificados?

vintegris

ISACA
Trust in, and value from, information systems

Gracias por su Atención

salvador.simarro@vintegris.com
jose.jimenez@vintegris.com

AENOR
Seguridad Información
UNE-ISO/IEC 27001