EDI.
ACEPTACION LEGAL EQUIVALENTE

Dificultades y Métodos Modernos de Autenticación

Dificultades y Métodos Modernos de Autenticación

- “La eficiencia se basa en:

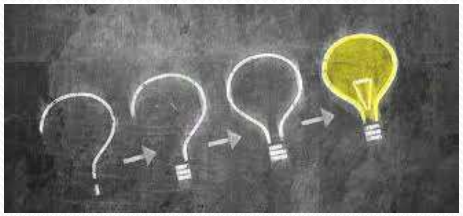
  a) la normalización,
  b) la estandarización y
  c) la simplificación”

Documento CONPES 3292/2004), del cual hace parte la VUCE

LA ACEPTACION LEGAL EQUIVALENTE VS COMERCIO ELECTRONICO

- Los requisitos legales que prescriben el empleo de la documentación tradicional con soporte de papel constituyen el principal obstáculo para el desarrollo de medios modernos de comunicación.

- Dichos impedimentos se basan en los conceptos del valor jurídico que tienen los conceptos "escrito", "firma" ,"original, AUTENTICO, INTEGRO "



FUNCIONES DEL DOCUMENTO CARTULAR

El documento en papel cumple funciones como las siguientes:

1. Documento legible para todos;
2. Asegurar la inalterabilidad a lo largo del tiempo;
3. Permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito;
4. Permitir la autenticación (validación) de los datos consignados suscribiéndolos con una firma; y
5. Debe ser aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales

LA EQUIVALENCIA FUNCIONAL NO ES ABSOLUTA

- Un equivalente informático no puede ser aplicado para todo tipo de documentos de papel.

- Debe siempre determinarse la función básica de cada uno de los requisitos de forma de la documentación sobre papel, con miras a determinar los criterios que, de ser cumplidos por el mensaje de datos lo hacen aceptable.

- **El documento electrónico con sus rasgos mínimos debe ser capaz de ser un sucedáneo efectivo del papel** no por mandato de la ley de cada país sino por cuanto es capaz de cumplir la misma función.

LA EQUIVALENCIA FUNCIONAL NO ES ABSOLUTA

- **Puede haber documentos en papel o en formato electrónico que no requieran estar autenticados** sino que simplemente consten por escrito o en un medio tangible (que se permita su conservación, exhibición, consulta y disposición) y

- otros que necesariamente deben estar autenticados (validada la identidad de quienes intervienen en el mismo.

Si se trata de una simple **función de enrolamiento** o margen estadístico o de mera información que puede ser validada por el receptor por otras vías, la autenticación no deberá ser la prioridad.

- Si por el contrario el mensaje de datos genera **responsabilidad, el nacimiento o extinción de una obligación** por parte del originador, la autenticación e integridad del mismo cobran especial relevancia.

LA EQUIVALENCIA FUNCIONAL NO ES ABSOLUTA

La equivalencia funcional la determina igualmente un sustento legal o norma que permita dejar sin margen de dudas dicha equivalencia.

El factor de riesgo más alto frente al principio de la equivalencia funcional lo determina dejar márgenes de interpretación a jueces, funcionarios o instituciones o al gobierno de turno.

La equivalencia funcional en materia de comercio nacional o trasnacional debe estar determinado igualmente por la estandarización de la forma en que el mensaje de datos debe ser originado, transmitido, autenticado e interpretado por el destinatario, siempre sobre la base de la función que va a cumplir dicho mensaje de datos

LA EQUIVALENCIA FRENTE A LAS VENTANILLAS UNICAS

- La interacción del ciudadano con las ventanillas únicas por medios electrónicos exigen documentos:

a) **Que sean susceptibles de tener equivalencia funcional respecto de la función que se desea que satisfagan.**
b) Estructurados
c) Estandarizados
d) Susceptibles de ser firmados
e) Cuyo contenido pueda ser extraído, tramitado o procesado, almacenado, y compartido con terceros nacionales y muchas veces internacionales.
f) **Susceptibles de ser autenticados respecto de su originador**
g) **Susceptibles de ser validados respecto a su no alteración después de haber sido creados por el originador.**

Manifestaciones de la Equivalencia funcional

a. Escrito: Noción de mensajes de datos y posterior consulta.

b. Original: Integridad en los mensajes de datos y en las comunicaciones electrónicas;

c. Firma: Firma electrónica vs. Firma Digital u otros mecanismos de Autenticación. Identificar y Autenticar

d. Archivo y Conservación: Evidencia digital.

¿Autenticación o Identificación?

- Suelen confundirse estos dos conceptos pero sus diferencias son manifiestas

- **Identificar** es en general exhibir una información que se supone publica al menos en la mayoría de sus partes. Es el suministro de esa información o la lectura de la misma (ejemplo código de serie o barra, etc)

- **Autenticar** exige que se valide (compruebe) una información que generalmente es una identificación a través de una información que es secreta.

- La autenticación permite asegurar con un nivel de confianza razonable la identidad del usuario dentro de un sistema o una herramienta

La autenticación Multi-factores

- Ejemplos de sistema de autenticación a 1 factor: identificador + contraseña (elemento que se sabe), definición sin contacto (elemento que se posee), Biométrica o identificador (elemento que es).

- Ejemplos de sistema de autenticación a 2 factores:

Tarjeta inteligente + código PIN (elementos que se posee Y que se sabe), Tarjeta inteligente + biométrica (elemento que se posee Y que es), Biométrica + contraseña (elemento que es Y que se sabe).

- Ejemplo de sistema de autenticación a 3 factores: Tarjeta inteligente + cifra PIN + biométrica (elementos que se posee Y que se sabe Y que es).

¿Cuáles son los métodos mas comunes de autenticación ?

1. **El identificador y la contraseña , sistema PKI, sistema RFDI, NFC, Biométricos**

- El identificador y la contraseña son el par de autenticación más conocido. Simple, por no decir rústico, su más grande defecto es que el nivel de seguridad depende directamente de la complejidad de la contraseña.

- Contraseñas simples son escasas ya por seguridad y el sistema de ingreso hoy en día las exige alfanuméricas con mínimos de caracteres.

- Contraseñas complejas conducen a los usuarios a aplicar estrategias no siempre correctas para recordarles: Post-it® , lista en un archivo Excel o en el SmartPhone,

- No permite garantizar el no repudio perse pues puede ser rechazado sobre la base de intrusiones no autorizadas

- No permite garantizar que el mensaje de datos no haya sido alterado después de firmado

El identificador y la contraseña OTP (One-Time Password

- "One-Time Password" describe un número de seis dígitos que se muestra en una pantalla utilizando una llave-anillo como el token de seguridad o una aplicación de teléfono inteligente conocido como un identificador de software.

- Las contraseñas generadas sólo son eficaces para un período fijo de tiempo y dejan de ser válidos una vez que el usuario inicia sesión, haciéndolos excepcionalmente útil contra el software espía como los programas clave de registro.

- No permite garantizar el no repudio per se pues puede ser rechazado sobre la base de intrusiones no autorizadas

- No permite garantizar que el mensaje de datos no haya sido alterado después de firmado

El identificador y la contraseña sobre una tarjeta inteligente

- Es la utilización de una tarjeta inteligente que en combinación con un identificador y un pasword mejora la protección del proceso de autenticación.
- La contraseña puede así ser muy compleja y cambiada regularmente de manera automática y aleatoria. Sin la tarjeta, y sin su código PIN, no se puede acceder a la contraseña. Esta solución se aplica generalmente para el proceso de autenticación inicial
- No permite garantizar el no repudio per se pues puede ser rechazado sobre la base de intrusiones no autorizadas
- No permite garantizar que el mensaje de datos no haya sido alterado después de firmado

BIOMETRICA, RFDI, NFC Y OTROS

- No permiten garantizar el no repudio per se pues puede ser rechazado sobre la base de intrusiones no autorizadas

- No permiten garantizar que el mensaje de datos no haya sido alterado después de firmado

Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)

1. Por “firma electrónica” se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;

2. Por “certificado” se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

3. Cumplimiento del requisito de firma 1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso:

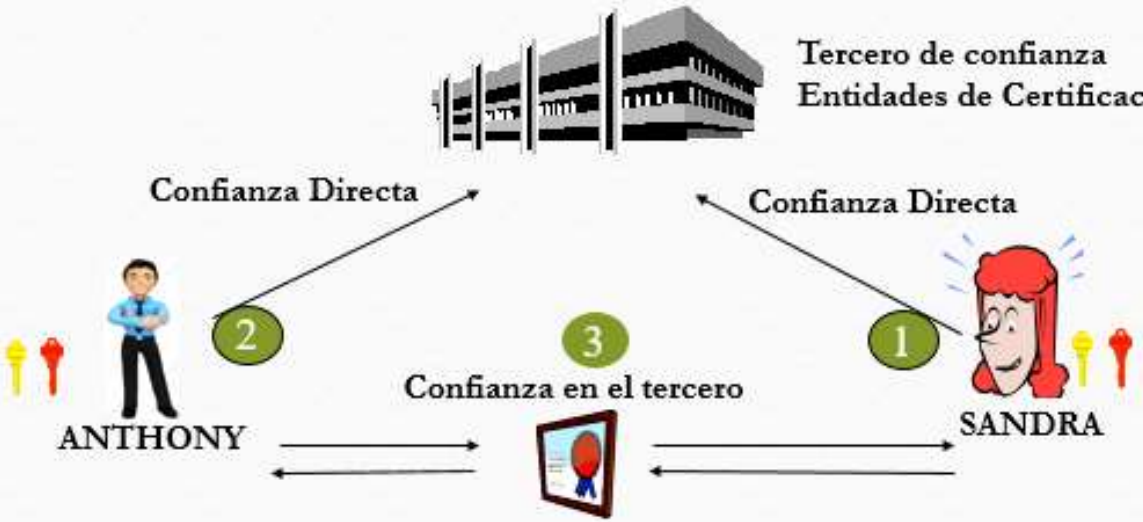
    - Sea fiable y
    - Resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje

FIRMA DIGITAL

≠

CERTIFICADO DIGITAL

ESQUEMA DE ENTIDAD DE CERTIFICACIÓN

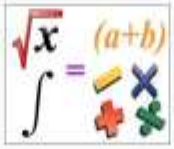


DEMOSTRACIÓN PROCESO DE FIRMA

Mensaje de datos

MP3, PDF, Correo Electrónico

Procedimiento matemático



Algoritmo SHA & RSA

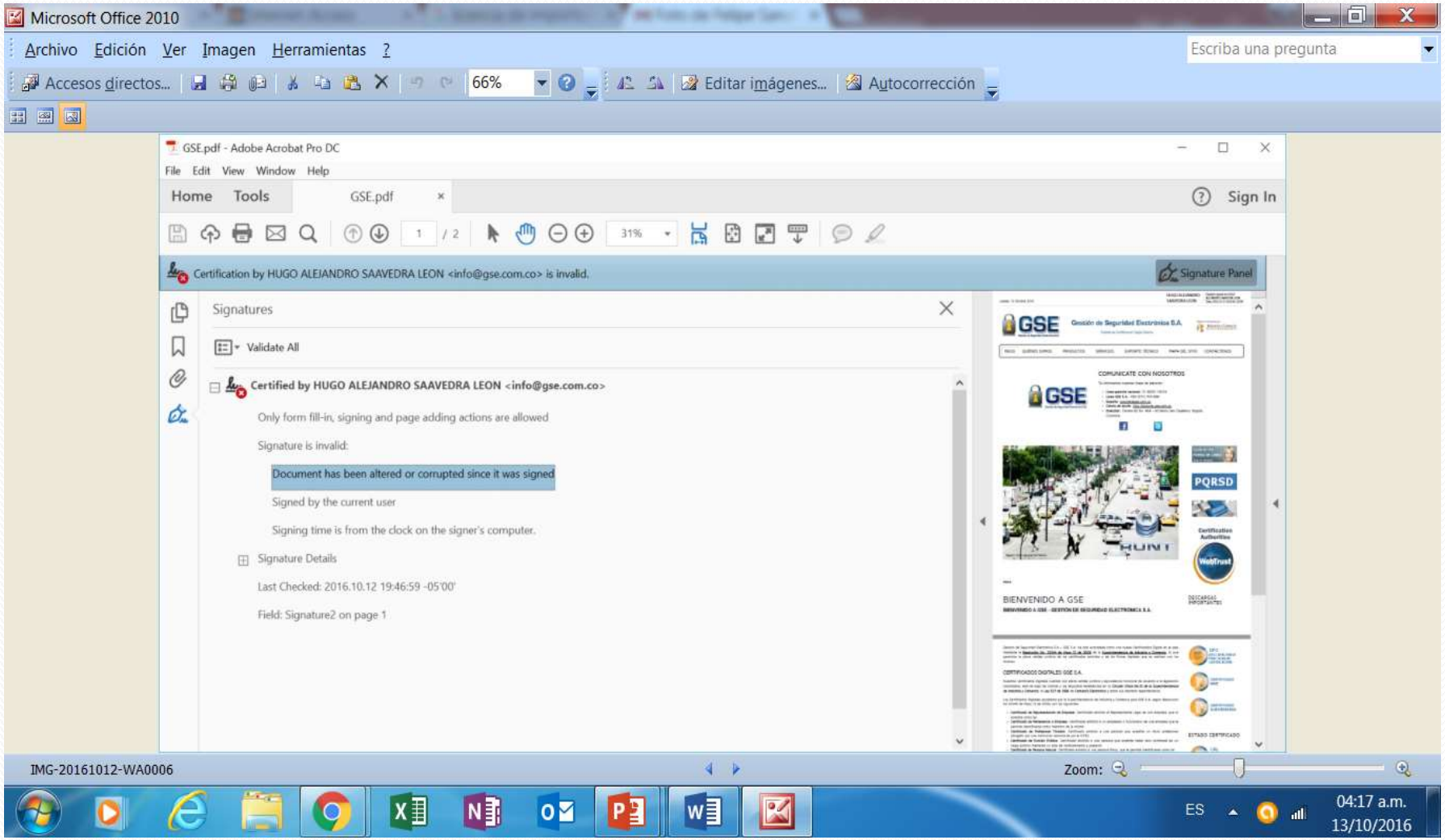
Clave del iniciador

Certificado Digital

FIRMA DIGITAL

Documento firmado Digitalmente

Documento alterado después de Firmado Digitalmente.



Cuadro comparativo métodos de Autenticación

METODO AUTENTICACIÓN	INTEGRIDAD	NO REPUDIO	AUTENTICACION
IDENTIFICADOR Y CLAVE	X	X	✓
PIKI. (CERTIFICADOS DIGITALES)	✓	✓	✓
OTP (ONE TIME PASSWORD)	X	X	✓
RFDI	X	X	✓
TARJETA MAS IDENTIFICADOR Y CLAVE	X	X	✓
BIOMETRICO	X	X	✓
NFC	X	X	✓

GRACIAS

info@gse.com.co

felipe.Sanchez@gse.com.co