

**ERICK RINCON CARDENAS**  
**erick.rincon@certicamara.com**

# Riesgos y requisitos de evidencia digital

- Suplantación de Identidad - Autenticidad
- Alteración de Información - Integridad
- Repudio de la Información - No repudio
  
- Requisitos de Evidencia Digital - Artículo 12 de la ley 527
- Determinación Origen del MD
- Integridad del MD
- Extremos de Conservación temporal
- Posterior Consulta
  
- Valoración Probatoria de Mensajes de Datos - Artículos 10 y 11 de la ley 527

# Autenticidad y Evidencia Digital

- La autenticidad es sólo uno de los temas asociados a la evidencia digital
- Que define el Decreto 2364 de 2012?
- Cuales son las mejores practicas internacionales o los estandares???
- Autenticidad no es lo mismos que integridad
- Código General del Proceso - Arts. 74, 84, 105, 111
- Consecuencias probatorias del manejo de evidencia digital. Se trata el asunto del manejo de evidencia?

## 2. Métodos de autenticación

- Métodos de autenticación Factor 1: Basados en algo que el usuario sabe (conoce).
  - P. Ej.: Login y Password
- Métodos de autenticación Factor 2: Basados en algo que el usuario sabe y algo que posee (tiene).
  - Se emplea algo que el usuario posee como segundo factor de autenticación.
  - Son mecanismos de doble intervención.  
P.Ej.:
    - Certificados digitales
    - Tokens OTP

## 2. Métodos de autenticación

- Métodos de autenticación Factor 3: Basados en algo que el usuario Es o Hace.

En este tipo de métodos de autenticación se enmarcan las soluciones de Biometría.

- Existen dos tipos de soluciones de biometría:
  - Biometría de características morfológicas (físicas) de las personas.
  - Biometría del comportamiento de las personas.

## 3. Factores de autenticación

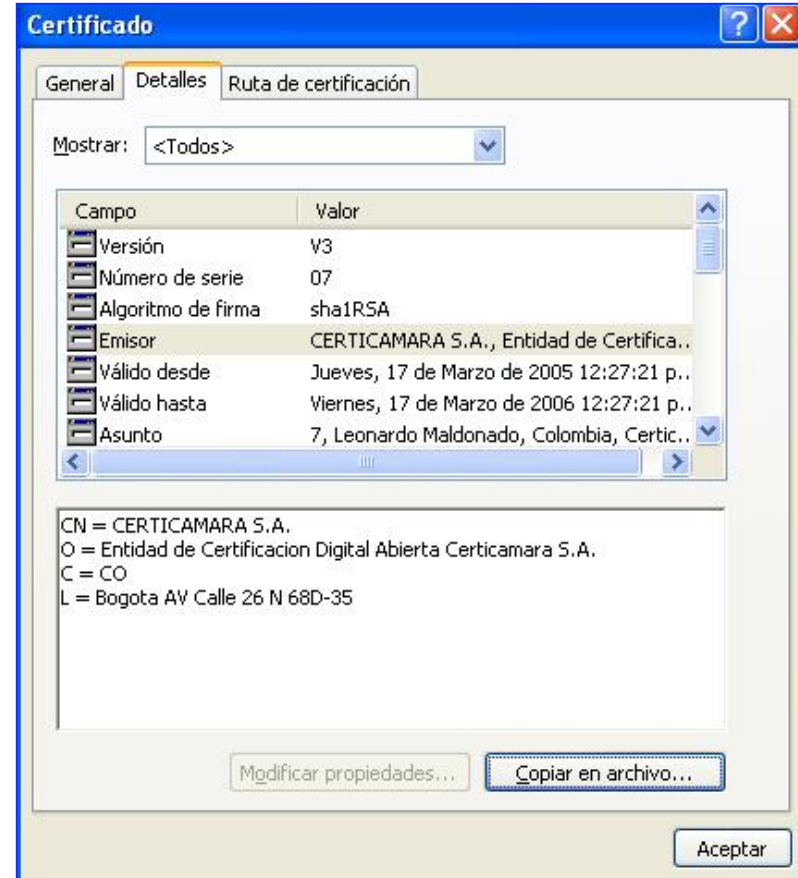
- Los factores de autenticación son:
  - Algo que el usuario SABE
  - Algo que el usuario TIENE
  - Algo que el usuario ES
  - Algo que el usuario HACE
  
- La autenticación multifactor combina dos o tres factores de autenticación para garantizar un mayor nivel de seguridad.



## 4. Certificados de firma digital

- Un certificado de firma digital es una credencial electrónica de autenticación emitida por un Tercero de Confianza denominado Entidad de Certificación Digital (CA) por medio del cual se garantiza:
  - Que el titular del certificado es quien dice ser
  - La asociación del titular del certificado con una llave pública
- Los certificados de firma digital pueden ser empleados como mecanismos de autenticación de doble factor:
  - Algo que el usuario TIENE= certificado digital
  - Algo que el usuario SABE= clave de acceso al certificado digital.

## 4. Certificados de firma digital





## 4. Certificados de firma digital

- La autenticación con certificados digitales consiste en la generación de una firma digital como Token de autenticación empleando el certificado digital como credencial de autenticación del usuario. Este mecanismo permite obtener garantías de seguridad técnica y jurídica (de conformidad con lo establecido en la Ley 527 de 1999) de:
  - Autenticidad de origen
  - Integridad
  - No repudio

## 4. Certificados de firma digital

- La implementación de soluciones de autenticación basadas en certificados digitales implica dos procesos básicos:
  - Adaptación del sistema para generar y validar firmas digitales.
  - Otorgar certificados digitales a los usuarios. Los certificados pueden ser:
    - De vigencia prolongada: 1, 2 y 3 años.
    - De vigencia media: 1, 2 y 3 meses.
    - De vigencia transaccional: vigencia igual a la duración de la transacción.



## 5. Claves de un solo uso (OTP)

- Solución de autenticación fuerte de doble factor.
  - Algo que el usuario SABE
  - Algo que el usuario TIENE
- Se basa en la generación de claves de autenticación de un solo uso. Cada vez que el usuario se autentica el sistema le genera una nueva contraseña.
- Solución resistente a ataques de suplantación y replay.
- Solución con una gran multiplicidad de dispositivos de autenticación.

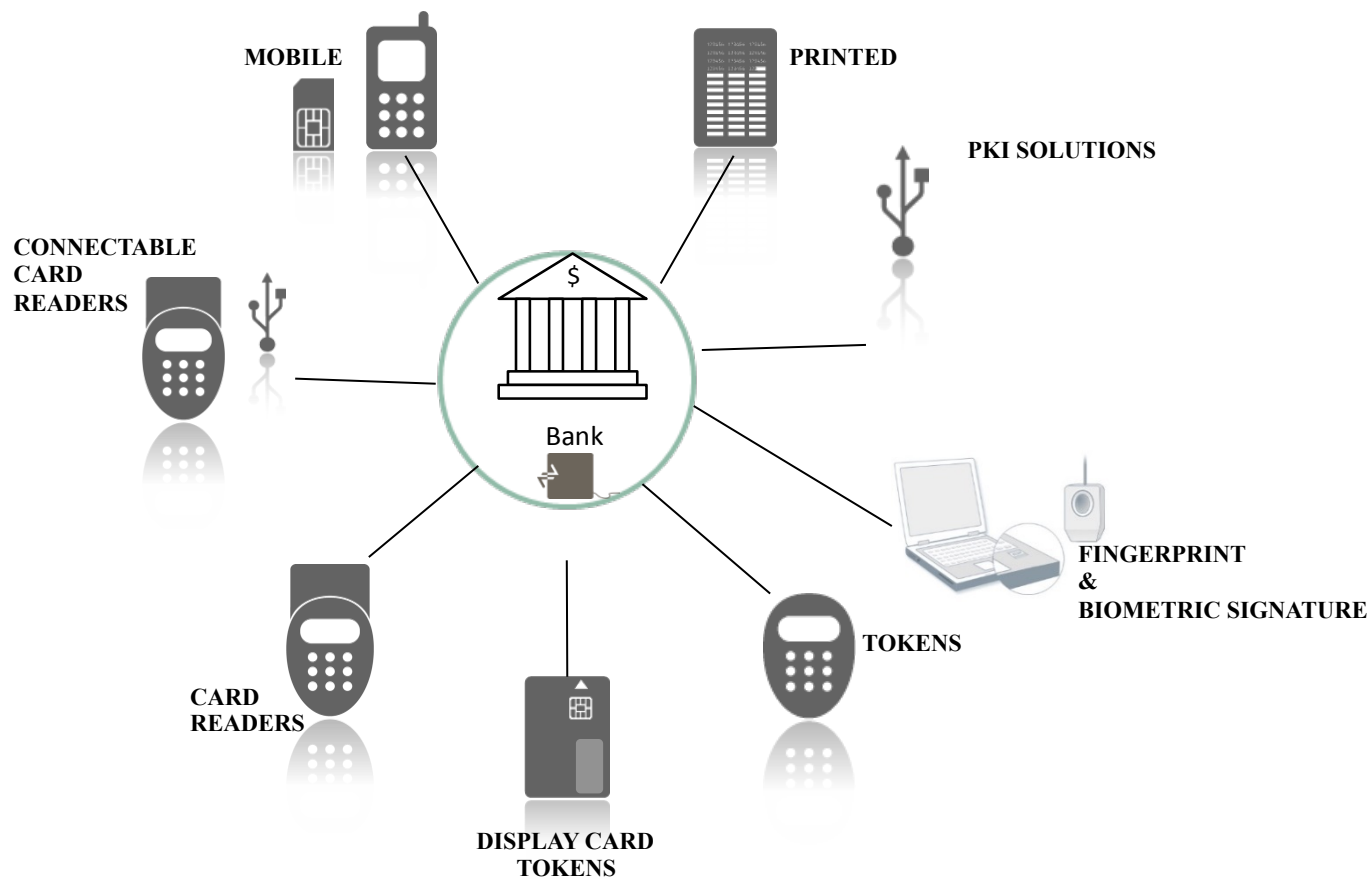


CAMARA  
DE COMERCIO  
DE CALI

**certicámara.**

Validez y seguridad jurídica electrónica

## 5. Claves de un solo uso (OTP)



## 5. Claves de un solo uso (OTP)





CAMARA  
DE COMERCIO  
DE CALI

## 5. Claves de un solo uso (OTP)



## 5. Claves de un solo uso (OTP)







CAMARA  
DE COMERCIO  
DE CALI

**certicámara.**

Validez y seguridad jurídica electrónica

## 5. Claves de un solo uso (OTP)

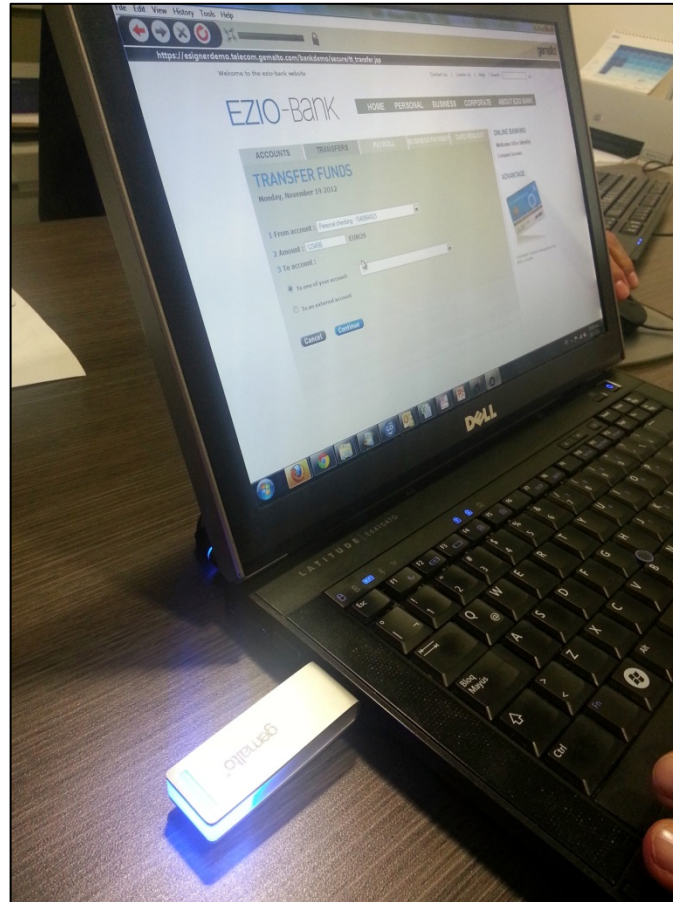




## 5. Claves de un solo uso (OTP)



## 5. Claves de un solo uso (OTP)



## 5. Claves de un solo uso (OTP)

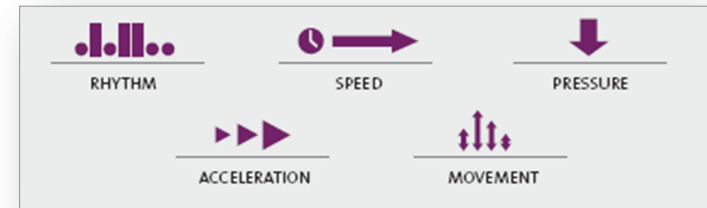
- Fácil integración mediante servicios Web y componentes API.
- Dos tipos de modelos de prestación del servicio:
  - Instalación en sitio de la infraestructura
  - Servicio en la nube

## 6.1. Firma Biométrica



## 6.1. Firma Biométrica

- Firma con parámetros biométricos
- Autenticación en tiempo real
- Registro de perfiles
- Comparación de firmas
- Estático a Estático
- Dinámico a Dinámico
- Estático a Dinámico
- Fácil integración a través de Web Services



## 6.1. FirmaBiométrica

- Solución de servidor y en la nube
- Convierte diferentes formatos a PDF y PDF/A
- Firmar de documentos
- Agregar sello seco
- Adjuntar certificados digitales y estampas



**Signatory:** Product Management

**Time:** UTC 2009-07-23, 06:30:30

Click to Verify 

# 6.1. FirmaBiométrica


certicámara.

AUTORIZACIÓN DÉBITO AUTOMÁTICO

Validez y seguridad jurídica electrónica

Solicitud:  /  /

Número Solicitud:

INFORMACIÓN BÁSICA DEL TOMADOR DE LA PÓLIZA			
Obrando en:	Primer Apellido	Segundo Apellido	Nombre(s)
*Nombre propio: <input type="checkbox"/>	SILVA	TORRES	GIOVANNI
**Representante Legal: <input checked="" type="checkbox"/>	Razón social completa (Persona Jurídica): EMPRESA DEMOSTRACIÓN		
Tipo de Identificación:	Dirección: CR 7 No 26 20		
C.C. <input type="checkbox"/> NIT. <input checked="" type="checkbox"/>	Ciudad: BOGOTÁ   Departamento: CUNDINAMARCA		
C.E. <input type="checkbox"/> Otro. <input type="checkbox"/>	Tel. Casa: 57 1 2373340   Celular: 3105598455   Correo Electrónico: giovanni.silva@certicamara.com		
Tel. Oficina: 57 1 3790300	Ext.	* Copia de la cédula del Tomador de la póliza al 150%	
* Copia de la cédula del Representante Legal y Camara y Comercio con vigencia no mayor a 90 días.			
INFORMACIÓN DE LA PÓLIZA			
Sucursal: AV CHILE	Ramo: SEGUROS	Número Póliza: BOG   1   4   7   0   0   1   1	
INFORMACIÓN DE LA CUENTA			
Entidad Financiera:** BANCO DE FINANCIAMIENTO	Tipo de Cuenta:	Ahorros <input type="checkbox"/>	Día de Cobro: 25
Número de cuenta	Corriente <input checked="" type="checkbox"/>		
5   0   0   0   1   9   9   8   9   1   3   2   4   7   8			
GIOVANNI SILVA TORRES			
Nombre Titular de la Cuenta	Click to Verify 		Aprobado
C.C. ó NIT.			

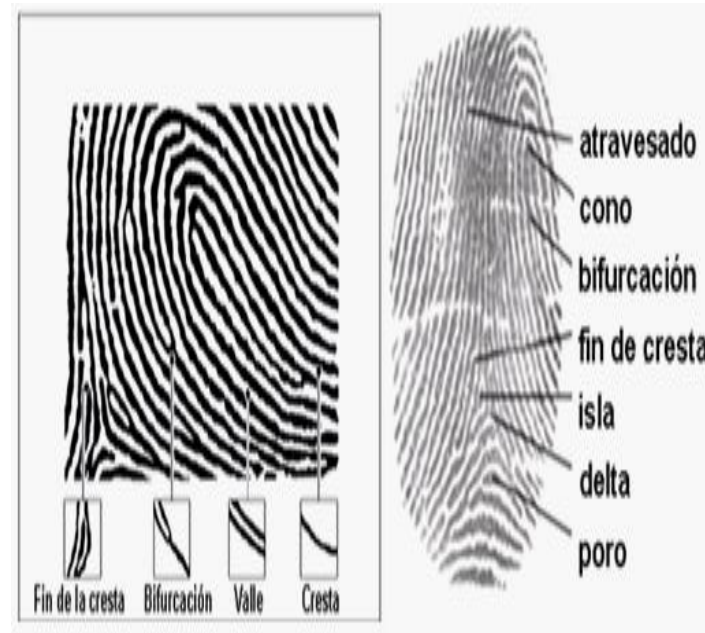




CAMARA  
DE COMERCIO  
DE CALI

## 6.2. Huella Biométrica

- Identificación plena del usuario mediante el análisis biométrico de su huella dactilar contra el registro decadactilar de la BD de la Registraduría Nacional del Estado Civil.
- Conforme al Decreto Ley 019 de 2012, se suprime el requisito de imposición de huella dactilar en tinta, reemplazándolo por la obligación expuesta en el artículo 18, verificación de huella dactilar por medios electrónicos.





## 6.2. Huella Biométrica

- Autenticación con huella dactilar:
  - Fácil integración mediante servicios Web.
  - Integración con múltiples dispositivos de captura de huella, incluyendo dispositivos móviles.
  - Verificación contra la BD de la RNEC.
  - Firma electrónica empleando huella dactilar biométrica.

### ¿Por qué necesito un certificado digital SSL?

- Para proteger a mis clientes y mi información sensitiva
- Para aumentar la confianza y la seguridad de mis clientes
- Incrementar el número de transacciones en mi sitio
- Evitar la perdida de clientes por falta de confianza
- Destacarse frente a los competidores - Obtener una ventaja competitiva
- Requerido para el cumplimiento de PCI (Payment Card Industry)



## 7. Certificados SSL

¿Cómo se consigue realmente la confianza y la sensación de seguridad?



- Autenticación del vendedor (“somos quien aseguramos ser”)
- • Cifrado y protección de datos (“protegemos sus datos”)
- • Mejora de la imagen de la marca (“respetamos su confidencialidad”)
- • Fomento de la confianza (“puede comprar aquí con toda tranquilidad”)

## 7. Certificados SSL

La tecnología SSL (Secure Socket Layer) protege sus transacciones en línea y ayuda a incrementar la confianza en su sitio Web de 3 maneras:



**1.** Un certificado SSL habilita el cifrado de información sensible durante las transacciones en línea.



**2.** Cada certificado digital es una credencial única que identifica al propietario del certificado.



**3.** Una Autoridad de Certificación autentica la identidad del propietario del certificado digital antes de que este sea emitido.

### Principales características de los certificados SSL:

- Autenticación empresarial completa
- Barra de direcciones verde
- Cifrado de 40 bits a 256 bits
- Escaneo diario de malware
- Garantía de US\$1.500.000 dólares
- Escaneo de Vulnerabilidades
- Sello Norton Secured
- Seal-In-Search
- Verificador de instalación

