Propuesta de acoplamiento de la firma electrónica avanzada en procesos de negocio

Víctor Bravo

Contenido

- El componente y el sistema
- Puntos de atención
- Método de acoplamiento

Casos de Estudio

- Flujo de Orden de compra
- Tres casos
- Algunos resultados
- Conclusiones

Modelo actual de firma electrónica

Algunas consideraciones sobre la firma manuscrita

Firma Manuscrita

Rasgos positivos

- Elementos biométricos
- Longeva
- Lápiz y papel
- Culturalmente aceptada

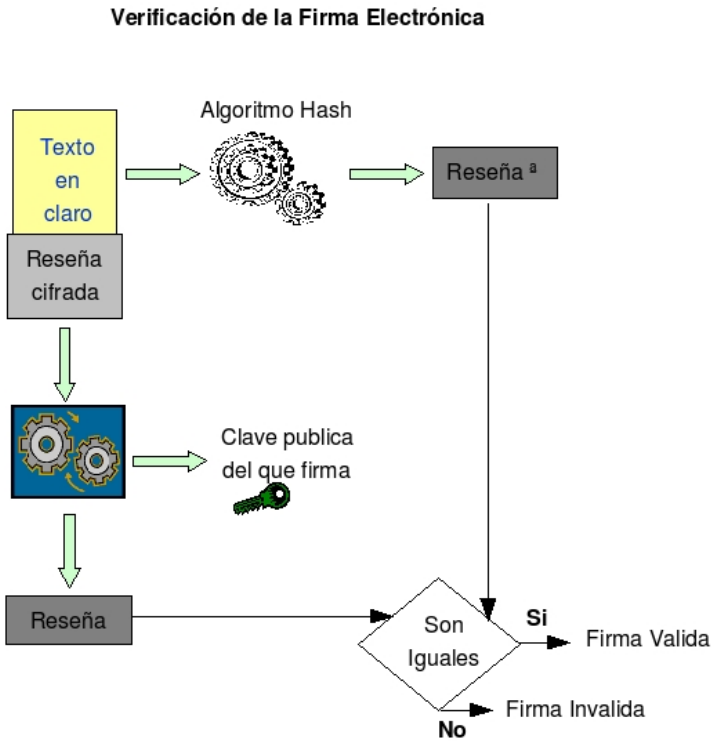
Rasgos negativos

- Principio de buena fe
- No integrada a sistemas informáticos
- Desconocimiento "a priori" de la identidad del firmante
- Acto de firma es presencial
- No hay un tercero de confianza

La firma electrónica en términos matemáticos

reseña Protocolo criptrográfico : hash + cifrado asimétrico.

Firma electrónica en procesos de negocio



Estándares

- PKCS #7 (RFC 2315)
- S/MIME (RFC 3875)
- XMLSig (RFC 3275)
- CADES, XADES (RFC 5126, W3C Note 20 February 2003)
- PADES, PDF/A (ISO 32000)

Implementaciones

- Motores criptrográficos (OpenSSL, CrytoAPI)
- Navegadores, Clientes de correo
- Adobe®Reader®, MS Office®
- Xyzmo
- @Firma
- iText
- BDoc*

Enfoque

- Basada en PKI
- Metáfora de la **firma**
- Remota
- Tarjetas Inteligentes
- Formato
- Ergonómica y acceso ubicuo
- Otros (Longeva, por lote, sellado de tiempo, cofirma, firma en cascada)

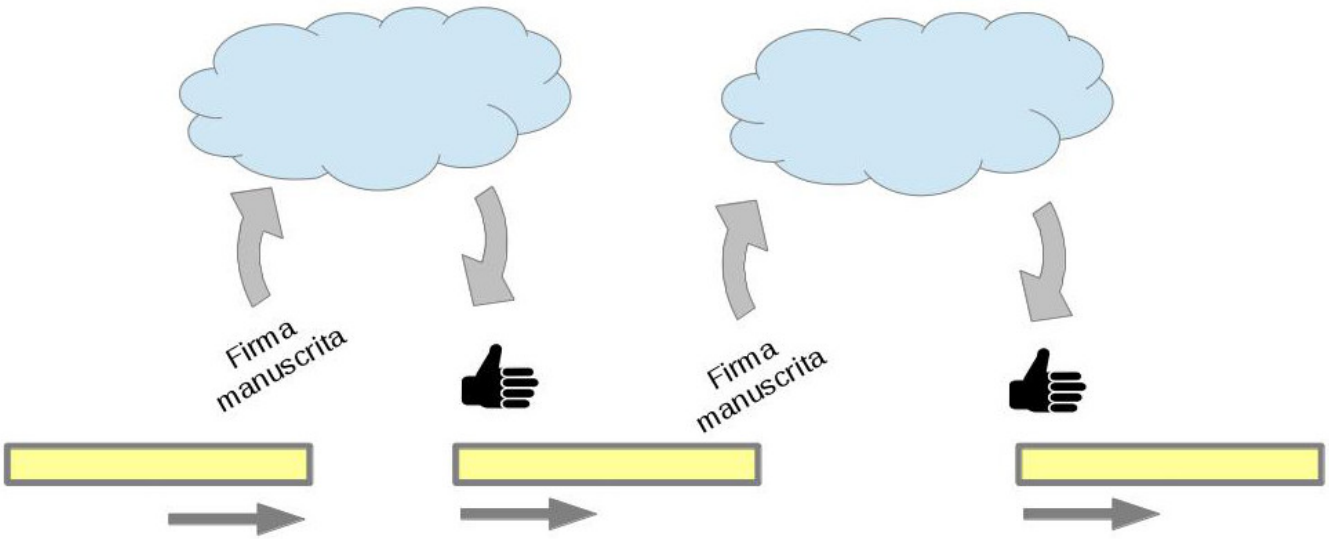
Acoplamiento de la firma electrónica

Primitivas

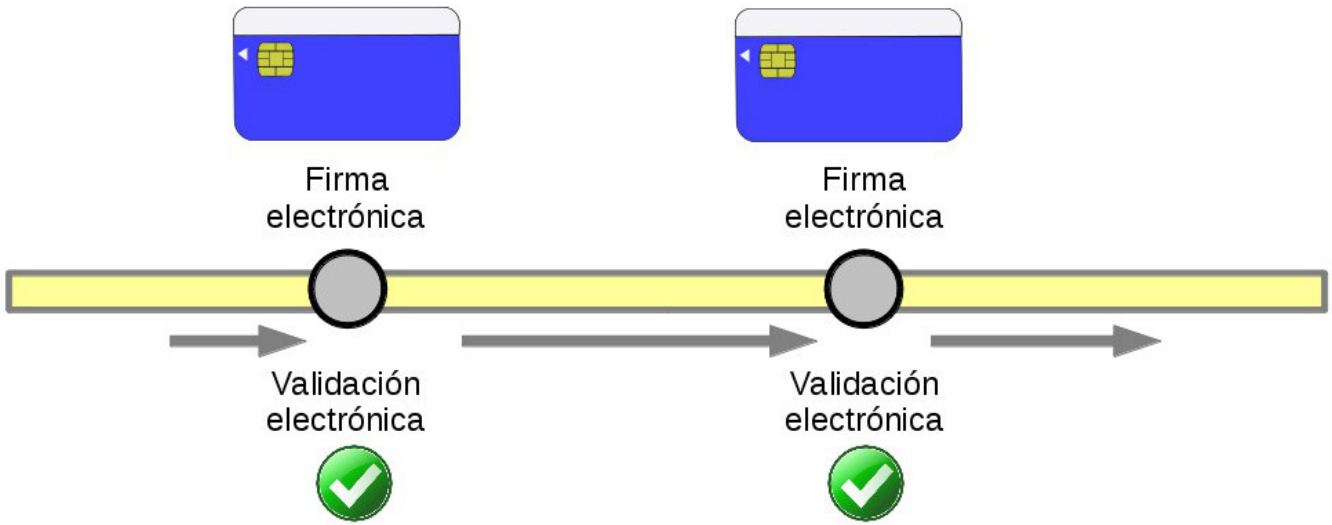
```
# Firmar
Bdoc.presign()
Bdoc.postsign()
# Validar
Bdoc.validateOffline()
Bdoc.validate()
# Gestionar
Bdoc.saveDocument()
Bdoc.getDocument()
Bdoc.getCertificate()
```

Funcionamiento

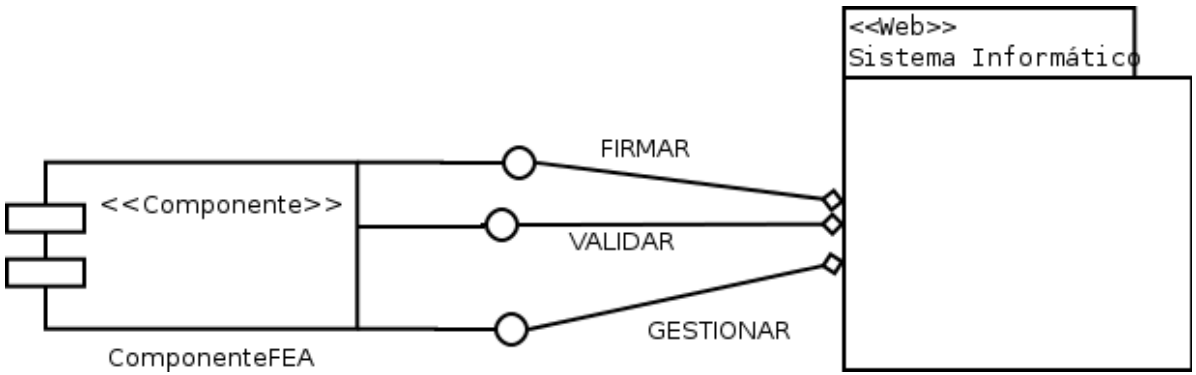
Usual



Firma/validación electrónica



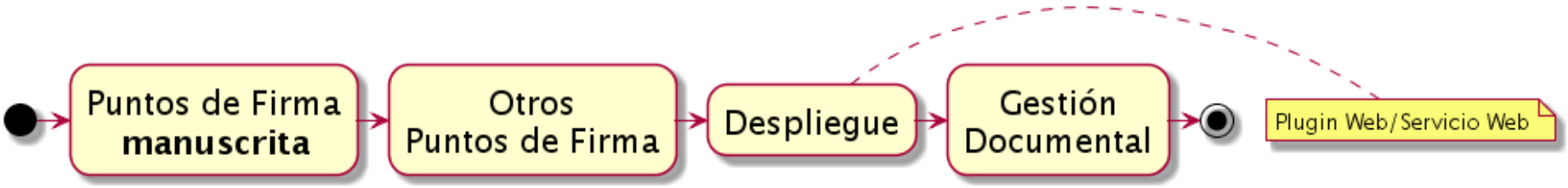
El componente y el sistema



Puntos de atención

- Generación / Identificación de datos dentro del documento
- Tamaño del documento (Plugin)
- Ver / imprimir la firma electrónica
- Contenedor de certificados válidos y OCSP (como en el navegador)
- Flujos de trabajo

Método de acoplamiento



Casos de Estudio

Flujo de Orden de compra

1. Generar requisición
    a) **Firma** del Solicitante
2. Obtener 2 cotizaciones
3. Seleccionar una cotización (acta)
    a) **Firma** analista de Compras
4. Generar orden de compra
    a) **Firma** Gerente

Tres casos

Sistema	Lenguaje	Tipo/Documento	Tipo/Conexión
SAID	PHP	PKCS#7	Servicio Web
OpenERP	Python	XaDES	paquete
SAFET	XML/Python	XaDES	paquete

Table 1: Acoplamiento de la firma electrónica

Algunos resultados

- Integración rápida
- Reducción de falsos positivos
- Reducción del uso de papel
- Espacio de archivo
- Disponibilidad de información
- Auditorías

Conclusiones

- Paradigma de "Componente" acorde con FE
- Identidad Digital
- Ergonomía
- La FE como *catalizador* de Procesos
- Integración con flujos de trabajos (workflow)

www.victorbravo.info

@victorrbravo