

## Estimado Profesional,

Para garantizar la confidencialidad y la integridad de las transacciones, así como la identificación inequívoca de su autor es necesario recurrir a soluciones basadas en **Técnicas Criptográficas, Certificación Digital y Firma Electrónica**. En soluciones que redunden en la confianza de las transacciones para todos los participantes. En el marco de **Ley de Firma Electrónica publicada en 2003** se han establecido hasta la fecha las bases para conseguir extender el uso y desarrollo de estas tecnologías en la **Sociedad de la Información**.

Ocho años después, la evolución de las **TICs** hacia entornos basados en el **Cloud Computing** y la movilidad, están cambiando los paradigmas preestablecidos respecto a la **Firma Electrónica** y a la **Identidad Digital**, creando a su vez un abanico de servicios relacionados hasta ahora prácticamente desconocidos.

Conceptos como la **Firma Remota, la Gestión centralizada de claves, la Firma de Movilidad, la Firma Digitalizada, la Custodia de documentos** a largo plazo y los nuevos escenarios creados por el desarrollo de la **Administración Electrónica** y sus normas de aplicación, especialmente en lo relativo a la adecuación de los **Esquemas Nacionales de Interoperabilidad y Seguridad**, están haciendo evolucionar los recursos de **PKI** contexto basado en aplicaciones distribuidas hacia un elemento crítico de infraestructura y el consumo de servicios de **Firma Electrónica**.

Le animamos a participar y compartir sus inquietudes con los ponentes y con el resto de asistentes, entre los cuales se encuentran algunos de los que están inmersos ya en algunos de los proyectos más apasionantes de **Firma Electrónica en Arquitectura SOA**.

Confío en saludarle personalmente en el evento

Cordialmente,

**María Luisa Blasco**  
Directora General  
ATENEA INTERACTIVA  
Twitter: @AteneaI

## Dirigido a...

- Responsables de Seguridad Informática en Entidades Públicas y Privadas
- Responsables de Gestión de Identidades
- Responsables de Informática
- Responsables de Gestión Documental
- Responsables de Implantación de Soluciones de eAdministración
- Responsables de Innovación
- Responsables de Infraestructuras Tecnológicas

## Objetivos

- Conocer las ventajas de disponer de una infraestructura común de **firma electrónica** para todas las aplicaciones que requieran garantizar la confidencialidad y la integridad.
- Aprender cómo están evolucionando los recursos de **PKI** hacia un escenario de infraestructura crítica dentro de la organización.
- Informarse de la reducción de costes en desarrollo y mantenimiento aplicaciones.
- Conocer las ventajas que aporta la gestión, como elemento de **Arquitectura**, de la **Firma Electrónica** en los "procesos de despapelización"
- Informarse de cómo los sistemas basados en **Firma Electrónica en Arquitectura SOA** permiten cumplir con la normativa reciente de:
  - o Factura electrónica (**orden PRE/2971/2007**)
  - o Administración electrónica (**Ley 11/2007**)
  - o Interlocución telemática (**Ley 56/2007**)
  - o Firma electrónica (**Ley 59/2003**)
  - o Esquemas Nacionales de Seguridad e Interoperabilidad
- Aprender a aprovechar las ventajas de interoperabilidad entre las aplicaciones y plataformas.

## Inscripción e Información

**Fecha:** 17 de noviembre de 2011

**Lugar:** *Centro de formación de Atenea Interactiva*  
C/ Méndrida, 6 – 28043 Madrid

**Coste:** 450 € + IVA (18%). **Total 531 € por asistente**  
Bonificable por la Fundación Tripartita

**Inscripción:**

-Mediante el formulario web accesible en:

<http://www.ateneainteractiva.com>

-Por teléfono: **902 365 612**. Contacte con el Departamento de Eventos

-Por e-mail: Envíenos sus datos a:

[inscripciones@ateneainteractiva.com](mailto:inscripciones@ateneainteractiva.com)



Fundación Tripartita  
FUE LA FUNDACIÓN EN EL 2003

# Firma Electrónica en Arquitectura SOA

## SERVICIOS PKI



Madrid, 17 de noviembre de 2011

# Programa de la Jornada

## 1. Service-oriented architecture

- Iniciación a SOA
- Descripción de entornos típicos de SOA

## 2. Cumplimiento de obligaciones con SOA

- Sector Privado: cumplimiento de las obligaciones de Interlocución Telemática de la Ley 56/2007 con SOA
- Sector Público: cumplimiento de las obligaciones de Administración Electrónica de la Ley 11/2007 con SOA

## 3. Conceptos de firma electrónica y PKI

- Propiedades de la firma electrónica
- Conceptos criptográficos
- Los certificados electrónicos. Tipos
- El proceso de firma electrónica
- Legislación

## 4. La firma electrónica como elemento de arquitectura

- La firma electrónica como servicio
- Servidores de firma y validación
- Repositorios de claves centralizados
- Despliegue de PKIs internas
- Dispositivos criptográficos. HSM

## 5. Servicios avanzados de PKI

- Firmas remotas y "upgrade" de firmas.
- Servicios de validación de firmas y certificados centralizados. CRL, OCSP, SCVP
- Servicios de sellado de tiempo.
- Firma en entornos móviles. Posibles enfoques
- Firma manuscrita digitalizada y servicios PKI avanzados. Unión necesaria

## 6. Formatos y estándares de firma

- Tipos de firma "legales"
- Formatos básicos
- Formatos AdES. XAdES, CAdES y PAdES
- Estándar DSS (Digital Signature Services). Descripción y perfiles
- Firmas longevas, la importancia de la firma en la conservación de documentos
- La importancia de las políticas de firma

## 7. Firma e identidad electrónica en las Administraciones Públicas

- La firma electrónica en la Ley 11/2007, el ENI y el ENS. Norma CCN-STIC-807
- Procesos de firma automatizados. Sello de órgano y CSV
- Servicios de firma y validación disponibles para Administraciones Públicas
- Identidad Digital y Administración Pública
- Políticas de firma en las AAPP. Descripción y diseño.
- Interoperabilidad. TSLs. Proyecto Stork

## Horario

<b>9:00 - 9:30</b>	Acreditaciones
<b>9:30 - 11:00</b>	Ponencias y Sesiones de Trabajo
<b>11:00-11:30</b>	Coffe Break
<b>11:30-14:00</b>	Ponencias y Sesiones de Trabajo
<b>14:00-16:00</b>	Pausa Comida
<b>16:00-18:00</b>	Ponencias y Sesiones de Trabajo
<b>18:00-18:30</b>	Coloquio y Clausura

## Ponentes

### D. Julián Inza



Actualmente es Presidente del **Grupo Interactiva**.

Pionero de la Certificación Digital, ha sido director general de Camerfirma, director de Estrategia Tecnológica de Banesto, Technology Senior Vicepresident de Mobipay International y Director Gerente de FESTE. Es coordinador del Foro de la Firma Electrónica, coordinador del Foro de las Evidencias Electrónicas, profesor del Instituto de Empresa y miembro del Comité Editorial de Financial Tech Magazine. Es el creador del concepto de Diplomática Digital.

En AENOR es miembro del CTN-50, en ASIMELEC es Presidente del Esquema de Certificación de PSCs y Coordinador del Grupo de Trabajo de eFactura. En OASIS es co-Chairman del UBL-Security-SC.

**Blog:** "*Todo es Electrónico*" <http://inza.wordpress.com>

**Twitter:** @julianinza

### D. Fernando Pino



Licenciado en Derecho en la Universidad Complutense de Madrid y Master en Informática y Derecho por el Instituto Español de Informática y Derecho, desarrollando su especialidad en criptología y seguridad informática. Ha participado en diferentes jornadas relativas a la protección de datos, firma electrónica y seguridad de la información. Ha trabajado en AC Camerfirma durante cuatro años, desarrollando labores de consultoría y formación en PKI.

Actualmente, Fernando es auditor CISA y desarrolla su carera en **Albalia Interactiva** como Director de Tecnología Legal.

**Twitter:** @fpinosola