



A medida que el comercio, la comunicación y la colaboración en línea se convierten en la forma preferida de hacer negocios, la seguridad en la red es imprescindible, para que de esta manera los proveedores, clientes y socios puedan autenticarse a través de un acceso seguro.

LA AC DE PSC ADVANTAGE

Es una solución que permite a las empresas establecer una infraestructura de llave pública PKI y un sistema de Autoridades de Certificación (AC), conservando el control total de la política de seguridad, los modelos de autenticación y la administración del ciclo de vida del certificado digital, junto con los robustos servicios de procesamiento de certificados de alta disponibilidad, este servicio permite una implantación más rápida y reduce los costos operativos, a la vez que proporciona una plataforma basada en estándares que se integra con soluciones listas para su uso.

LA AC DE PSC ADVANTAGE

Permite a una empresa implantar la infraestructura de clave pública fácilmente en las instalaciones del cliente.

Es una solución que permite crear entornos de seguridad basados en firma electrónica a través de la emisión de certificados digitales.

Haciendo uso de los certificados digitales, las personas cuentan con una identificación digital con la cual pueden realizar operaciones electrónicas con validez legal, siendo así la forma reconocida por entidades públicas y privadas de reemplazar la manera de celebrar acuerdos que tradicionalmente se realizaban a través de una firma autógrafa.

Con la **AC DE PSC ADVANTAGE** podrá administrar el ciclo de vida de un certificado digital (solicitud, registro, emisión, renovación, revocación, reemisión).

Actualmente se tiene disponible la versión 2.0 de esta solución.

AC DE PSC ADVANTAGE®

CARACTERÍSTICAS

- ☑ Permite definir múltiples entidades emisoras de certificados digitales, cada una con propiedades y parámetros particulares de operación, bajo una misma jerarquía o jerarquías independientes.
- ☑ Definición paramétrica para procesar solicitudes de certificados digitales con longitudes de llave de 512, 1024 o 2048 bits.
- ☑ Definición paramétrica de vigencia para las listas de certificados digitales CRL.
- ☑ Definición paramétrica para establecer vigencia de los certificados digitales.
- ☑ Capacidad de definir convenciones de números de serie paramétricas que cumplan con los lineamientos propios o establecidos por otras entidades reguladoras de firma electrónica avanzada.
- ☑ Definición paramétrica para validar atributos en las solicitudes de certificados digitales.
- ☑ Definición paramétrica de extensiones informativas tales como acceso a la información de entidad emisora, identificador de clave de asunto, nombre alternativo del sujeto, nombre alternativo del emisor, puntos de distribución de CRL, bases del certificado, identificador de clave de la entidad emisora, comentario de Netscape.
- ☑ Definición paramétrica para establecer el uso del certificado digital a través de las extensiones tipo certificado, Netcape, Uso de Llave, Uso Mejorado de Llave, Restricciones del Certificado, EDIFACT, etc.

☒ Creación y configuración ilimitada de entidades registradoras.

☒ Configuración ilimitada de agentes registradores y certificadores con perfiles predefinidos para delimitar funciones operativas

☒ Integración a servicios de directorio activo compatibles con LDAP.

☒ Interfaces Web para solicitar certificados digitales a partir de cualquier proveedor criptográfico compatible con CAPI de Microsoft

☒ Soporte a solicitudes de certificados digitales desde tokens o smartcards criptográficos.

☒ Envío de notificaciones vía correo electrónico con

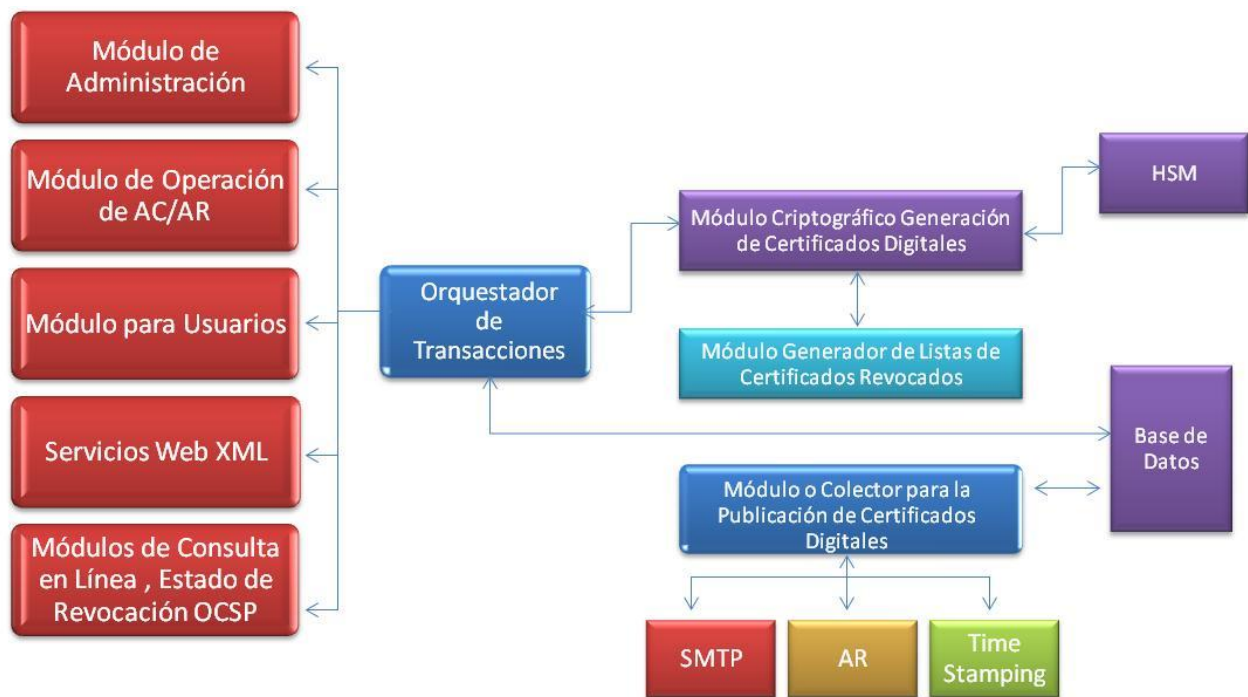
contenido paramétrico a usuarios solicitantes de certificados digitales o bien a responsables de realizar funciones de auditoría sobre la operación del sistema.

☒ Registro de transacciones realizadas por agentes registradores y certificadores utilizando firma electrónica avanzada.

☒ Validaciones de cada uno de los atributos de las solicitudes de certificados digitales recibidos desde la interfaz web o desde archivos de requerimientos conforme al estándar PKCS10.

☒ Capacidad de definir convenciones de números de serie paramétricas que cumplan con los lineamientos propios o establecidos por otras entidades reguladoras de firma electrónica avanzada.

ARQUITECTURA



MÓDULOS PRINCIPALES

1) Módulo Criptográfico de Generación de Certificados Digitales

Componente responsable de procesar las solicitudes de emisión de certificados digitales.

2) Módulo de Administración

Permite configurar características operacionales de entidades emisoras y registradoras creadas en la solución.

3) Módulo de Operación

Permite crear entornos personalizados para administrar el ciclo de emisión de certificados digitales.

4) Módulo Generador de CRL

Componente que genera la lista de revocación de certificados conforme al estándar RFC 3280.

5) Módulo de Consulta en Línea de Certificados Digitales OCSP

Módulo responsable de atender peticiones de consulta en línea del estado de revocación que guardan los certificados digitales administrados en la entidad emisora y cumple con la especificación del RFC 3280.

6) Módulo Colector para Publicación de Certificados Digitales

Componente responsable de procesar perfiles para condicionar la publicación de certificados digitales.

7) Módulo para Usuarios

Componente que publica los medios para que los usuarios puedan realizar la solicitud, consulta, renovación y revocación de los certificados digitales.

8) Módulo de Emisión Masiva de Certificados Digitales

Componente que permite procesar solicitudes de certificados digitales por lotes.

9) Módulo Orquestador de Transacciones

Componente responsable de procesar las peticiones realizadas a través de las interfaces de entidad emisoras y receptora.

ESPECIFICACIONES TÉCNICAS

✓ ESCALABLE

Su arquitectura modular permite crear ambientes de operación bajo configuraciones de alta disponibilidad, garantizando así la estabilidad de la solución para presentes y futuros requerimientos.

✓ FLEXIBLE

Está diseñada para ser integrada fácilmente a cualquier ambiente en producción.

✓ INTEGRACIÓN CON DISPOSITIVOS DE SEGURIDAD DE HW – HSM

Garantiza la operación y administración de las llaves raíz de la Entidad Emisora de Certificados Digitales en Dispositivos HSM.