



## PRINCIPALES VENTAJAS

### *Costos Bajos*

El servicio de AC de PSC Advantage, ofrece un costo bajo de propiedad al compararlo con las implementaciones de PKI independientes:

### *Reduce la exposición a los riesgos*

Al delegar las tareas y procesos de seguridad clave a un reconocido líder del sector, la empresa minimiza los riesgos asociados al funcionamiento de la AC.

### *Ayuda al cumplimiento de la legislación vigente.*

Las empresas, gobiernos estatales, pueden aprovechar la infraestructura técnica y operativa en la que se encuentra la AC para así cumplir con la normativa específica a la cual se sujetan.

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.

## EL SERVICIO DE 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, ahorrando los elevados gastos que supondrían el diseño, aprovisionamiento, contratación de personal y mantenimiento de su propia infraestructura de PKI.

## 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.