PSC Advantage

AC de PSC Advantage

PSC Advantage

Version 2.0

Advantage Security S de RL de CV
Av Prolongación Paseo de la Reforma 625
Paseo de las Lomas, Santa Fe
CP 01330
Tel. 01 52 55 50 81 43 60

Tabla de contenido

AC de PSC Advantage

Descripción

AC de PSC Advantage es una solución que permite crear entornos de seguridad basados en firma electrónica avanzada 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), así como también cuenta con la capacidad de Subordinar y Subordinarse a Autoridades Certificadoras Propias y de Terceros

Cuenta con el módulo de IES (Infraestructura Extendida de Seguridad)

Características Funcionales

- ✓ Genera y resguarda las llaves privadas mediante dispositivos criptográficos (HSM).
  - Compatible con:
    - HSM que cumplan con FIPS140-2 Nivel 3, para el almacenamiento de las llaves.
    - Cuenta con los mecanismos necesarios para soportar un esquema de custodios para el acceso al dispositivo.
    - Registra y mantiene bitácoras que permitan el monitoreo de los servicios.
- ✓ Permite administrar el ciclo de vida de los certificados digitales.
- ✓ Genera certificados digitales ITU-T X509v3 para usuarios y para aplicaciones también.
- ✓ Los certificados X509v3 son compatibles con S/MIME, SSL, Firma de Código, OCSP Responder.
- ✓ Permite la generación de certificados conforme al estándar RFC3280
- ✓ Genera y publicar listas de certificados digitales revocados a través de las CRL la cual se genera de manera automática y periódicamente para que estos puedan ser verificados.

- ✓ Permite la Información en línea, sobre el estado de revocación de los certificados digitales a través del protocolo OCSP.
- ✓ Cumple con los estándares mundialmente aceptados para el tema de Autoridades Certificadoras.
- ✓ Permite definir una o más entidades emisoras, cada una con sus propiedades particulares bajo una misma jerarquía o jerarquías independientes.
- ✓ Definición paramétrica en horas de la vigencia para la generación y publicación de las listas de certificados revocados CRL (actualización automática).
- ✓ Soporta la configuración para el respaldo de la CRL.
- ✓ Definición paramétrica para procesar longitudes de llave de 512, 1024 o 2048 bits.
- ✓ Definición paramétrica para establecer la vigencia de certificados digitales emitidos.
- ✓ Capacidad de definir convenciones de números de serie y OIDs paramétricas que cumplan con lineamientos propios o establecidos por otras entidades reguladoras tales como Secretaría de Economía, Banco de México, ITFEA.
- ✓ Definición paramétrica para validar atributos (OIDs) permitidos en las solicitudes de certificados digitales así configurar si son opcionales u obligatorios y el tipo de codificación.
- ✓ Definición paramétrica de extensiones de los certificados:
  - Acceso a la información de entidad emisora. Definición de URL para consultas OCSP.
  - Identificador de clave de asunto.
  - Nombre alternativo del sujeto.
  - Nombre alternativo del emisor.
  - Puntos de distribución de CRL (CDP).
  - Bases del certificado.
  - Identificador de clave de entidad emisora.
  - Comentario de Netscape.
  - Identificación de la Políticas del Certificado.
  - Authority Info Access (AIA)
- ✓ Definición paramétrica para establecer el uso del certificado digital a través de las extensiones:
  - Netscape Certificate Type.
  - Key Usage.
  - Enhanced Key Usage.
  - Restricciones del certificado
  - EDIFACT
- ✓ Tipos de extensiones que se pueden definir para los certificados digitales.

Netscape Certificate Type
SSL Client Authentication
SSL Server Authentication
S/MIME (Client)
Object Signing

SSL CA
S/MIME CA
Object Signing CA

Key Usage
Digital Signature
Non repudiation
Key Encipherment
Data Encipherment
Key Agreement
Cert Signing
CRL Signing
Encipher Only
Decipher Only

Enhanced Key Usage
TLS Web Server Authentication
TLS Web Client Authentication
Code Signing
Secure e-mail
Time Stamping
OCSP Signing
Microsoft Strong Encryption
Encrypting File System
Microsoft Smart Card Logon
Netscape Stron Encryption

Subject Alternative Names
Issuer Alternative Names
Certificate Policies
URL
Text

CRL Distribution Point (CDP)
URL

Authority Info Access (AIA)
URL
LDAP/http Certificate address o equivalentes.

- ✓ Definición ilimitada de entidades registradoras.
- ✓ Configuración ilimitada de agentes registradores y certificadores con perfiles predefinidos que delimitan las funciones operativas.
- ✓ Integración a servicios de directorio activo compatibles con LDAP para la publicación de certificados digitales generados.
- ✓ Integración con usuarios a través de sus interfaces web para solicitar certificados digitales a partir cualquier proveedor criptográfico compatible con CAPI de Microsoft.
- ✓ Soporta solicitudes de certificados digitales desde tokens criptográficos.

- ✓ Envío de notificaciones vía correo electrónico con contenido paramétrico a usuarios solicitantes de certificados o bien a responsables de realizar funciones de auditoría sobre la operación del sistema.
- ✓ Aplicación de firma digital a las transacciones realizadas por agentes registradores y certificadores.
- ✓ 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.
- ✓ Procesamiento de transacciones con algoritmos RSA.
- ✓ Soporta funciones paramétricas para la definición de atributos, extensiones y vigencia de certificados.
- ✓ Soportar la carga de requerimientos generados con otras aplicaciones y con su propia aplicación mientras cumplan con el estándar PKCS #10.
- ✓ Procesar requerimientos de certificados generados desde tarjetas inteligentes SmartsCards y/o Tokens criptográficos que sean compatibles con CAPI de Microsoft.
- ✓ Proveer interfaces web que se puedan ejecutar desde diversos sistemas operativos (Windows, Linux, Mac) para generar requerimientos y almacenar la llave privada de forma local en archivo formato PKCS8. Una vez generado el certificado el usuario puede encapsular su llave privada y certificado digital en el formato PKCS12.
- ✓ Permite soportar carga y validación de certificados con base a políticas definidas.
- ✓ Permite la solicitud de estampillas de tiempo de fuentes confiables como la de los PSC (Prestador de Servicios de Certificación).
- ✓ Permite la creación de creación de cuentas de administración a través de un esquema RBAC (Role Base Access Control) donde se pueden configurar atributos de Alta, Modificación, Consulta y Ejecución para los siguientes actividades de administración:
    a. Acreditación de solicitudes de certificados digitales
    b. Administración de agentes
    c. Carga de solicitudes de certificados
    d. Consulta de certificados digitales
    e. Emisión de certificados digitales

- ✓ Cuenta con un módulo de funciones de auditoría dónde todas las operaciones que se llevan a cabo en el sistema, son registradas con fines de monitoreo y auditoría.
- ✓ El módulo de auditoría de operaciones de la AC funciona a través de la emisión de recibos criptográficos (de acuerdo al RFC 3161) garantizando la integridad de las operaciones y de la base de datos.
- ✓ Cuenta con un cliente stand alone y una interface web para hacer la solicitud de certificados digitales.
- ✓ El generador de certificados tiene la capacidad de configurar dinámicamente el tamaño de la llave del certificado.

- ✓ La AC de PSC Advantage se puede configurar como valor fijo o modificable la fecha de vigencia de los certificados digitales a expedir.
- ✓ La AC de PSC es capaz de generar certificados SSL para garantizar la identidad de un sitio Web.
- ✓ El acceso al portal del administrador es a través del protocolo https
- ✓ La comunicación hacia cada uno de los componentes de la AC es vía https
- ✓ El certificado digital que asegura las comunicación https, es un certificado reconocido a nivel mundial.
- ✓ La AC tiene la capacidad de configurar los campos que son obligatorios y los que son opcionales para los requerimientos de certificados.
- ✓ La AC permite configurar la vigencia de la contraseña, los intentos fallidos de acceso al sistema, y el tiempo máximo de inactividad de la sesión para cada una de las cuentas de administración.
- ✓ La AC soporta el idioma español y cuenta con una interface para personalizar la presentación de la interfaz (logo, mensajes, etc.)
- ✓ La AC cuenta con un módulo para consulta, modificación y altas de atributos de catálogos.
- ✓ La AC es capaz de emitir un comprobante de emisión de certificado digital de firma electrónica certificada.
- ✓ La AC cuenta con un módulo de workflow, donde pueda ver las peticiones que se encuentran pendientes tanto para validación de documentación o requerimientos como para generación de certificados.
- ✓ La AC permite descargar el certificado del usuario a través de una interface web usando un número de folio o campo personalizado.
- ✓ La AC maneja notificaciones por correo electrónico tanto al usuario como al administrador de la AC.
- ✓ Cuenta con la facilidad para la re-expedición de Certificados en Línea a través de WEB
- ✓ Consola Gráfica de configuración para facilitar al administrador su operación y configuración.
- ✓ Permite Establecer el Puerto TCP de operación del servicio para la comunicación con aplicaciones de acuerdo a las definiciones del cliente.
- ✓ Permite Establecer el Puerto TCP de comunicación mediante WebServices al servicio para comunicación de aplicaciones de acuerdo a las definiciones del cliente.
- ✓ Permite que el formato de string para los NAMES de los certificados digitales sean Printable String UTF8.
- ✓ Cuenta con la integración del protocolo SMTP para comunicación con servidores de correo electrónico, para el envío de notificaciones de certificación.
- ✓ Permite la personalización del mensaje de notificaciones de correo electrónico de acuerdo a las necesidades del cliente.
- ✓ Permite la emisión y administración ilimitada de certificados digitales
- ✓ Soporta 3 formatos de número de serie para los certificados digitales

- ✓ Cuenta con un módulo IES Infraestructura Extendida de Seguridad, para el registro de los certificados digitales para evitar la duplicidad de llaves.
- ✓ Soporta varios servicios de Autoridad Certificadora en el mismo equipo, cada servicio puede es independiente y se configura de manera individual.
- ✓ Soporta escalabilidad en la infraestructura en cuanto a la capacidad de atención de múltiples transacciones simultáneas.
- ✓ Soporta su configuración en ambientes distribuidos como:
    a. Clústeres y granjas, garantizando alta disponibilidad o balanceo de cargas.

- ✓ Soporta la generación y operación con llaves RSA de hasta 4096 bits tanto para llaves de usuario como de servicios.

- ✓ Permite emitir extensiones en certificados X.509 para hacer posible la conversión a certificados EDIFACT.

- ✓ Los certificados EDIFACT cumplen con las Guías de implantación mexicanas para seguridad EDIFACT normada por AMECE en los documentos:
    a. Servicio de Autenticación de Origen, Integridad y No Repudiación de Origen
    b. Llave de Seguridad y Manejo de Certificado (KEYMAN)
    c. Deberá soportar en sus diferentes operaciones al menos los siguientes estándares o algoritmos criptográficos.
    d. X.509 - IETF RFC 3280
    e. PKCS
    f. PKCS#1(RSA)
    g. PKCS#5
    h. PKCS#8
    i. PKCS#10
    j. PKCS#11
    k. PKCS#12
    l. LDAP
    m. CRL (RFC 3280, X.509)
    n. OCSP (RFC 2560)
    o. SHA1
    p. MD5
- ✓ Arquitectura Multicapas
  Soporta distribución de componentes con base a una arquitectura multicapas (Presentación, Reglas de Negocios y Datos) brindando con ello, una mayor seguridad de la información.

- ✓ Directorios que Soportados LDAP
    Active Directory Application Mode
    Open LDAP
- ✓ Permite la creación de múltiples Autoridades Registradoras

La arquitectura de AC de PSC Advantage permite la creación y administración de n cantidad de Autoridades Registradoras y Subordinadas.

La subordinación de la Autoridad Certificadora soporta n niveles de profundidad.

- ✓ Integración transparente a los aplicativos de gestión interna de los clientes Mediante API´s (Java, C, C++,Visual Basic).

Cuenta con la capacidad de crecimiento de infraestructura
Con Modelos de Clúster Activo-Pasivo, Balanceo de Cargas, Activo-Activo, según lo requiera el cliente.

Arquitectura de la AC de PSC Advantage

Es una solución modular que puede configurarse bajo una arquitectura multicapas y cuenta con los siguientes módulos principales.

✓ Módulo criptográfico de generación de certificados digitales.

Es el componente responsable de procesar las solicitudes de emisión de certificados digitales con características previamente configuradas. Módulo Autoridad Registradora.

- Soporta su instalación en un equipo con Sistema Operativo Windows y Linux Red Hat
- Permite la Autorización de emisión de Certificados Digitales.
- Permite la Solicitud de revocación de Certificados Digitales.
- Permite las Solicitud de CRL's.
- Habilita la Búsqueda de Certificados Digitales.
- Habilita la Búsqueda de Requerimientos de Certificación (Generación Web).
- La autenticación al módulo mediante certificados digitales.
- Al momento de aprobar la emisión de un Certificado Digital permite especificar las fechas (día) de inicio y expiración usando un calendario.

✓ Módulo criptográfico de generación de certificados digitales

- Cuenta con un módulo a través del cual se pueda interactuar con dispositivos de hardware criptográficos que cuenten con la certificación FIPS-140-2 Nivel 3.
- La comunicación a los dispositivos criptográficos puede ser a través del protocolo PKCS#11.
- El módulo criptográfico permite su operación bajo el esquema de custodios

- ✓ Módulo de administración.
  - Permite configurar características operacionales de entidades emisoras y registradoras creadas en la solución.
  - Permite la Administración de Autoridades Certificadoras subordinadas
  - Permite la Administración de Autoridades Registradoras
  - Permite la Autorización de emisión de Certificados Digitales.
  - Permite la Solicitud de revocación de Certificados Digitales.
  - Permite la Solicitud de CRL's.
  - Permite la búsqueda de Certificados Digitales.
  - Soporta diferentes modelos de autenticación (login) del usuario soportando tanto autenticación por software tanto usando dispositivos criptográficos.
  - Permite al momento de aprobar la emisión de un Certificado Digital especificar las fechas (día) de inicio y expiración usando un calendario.

- ✓ Módulo de operación.
  - Permite crear entornos personalizados para administrar el ciclo de emisión de certificados digitales, desde la
    - Carga de requerimientos
    - Validaciones
    - Emisión de certificados
    - Consultas
    - Revocaciones
    - Renovaciones
  - Esto permite soportar la simplificación de funciones administrativas.

- ✓ Módulo generador de listas de certificados digitales revocados (CRL).
  - Es el componente que genera la lista de certificados digitales revocados conforme al estándar RFC 3280.

- ✓ Módulo protocolo OCSP (RFC 2560).
  - Soporta su instalación en un equipo con Sistema Operativo Windows Server 2000 o superior o Linux/Unix.
  - Permite configurar los tres esquemas de validación definidos por el RFC 3161:
    - AC que emitió el certificado en cuestión (Issuer CA)
    - Un respondedor confiable para el solicitante (Trusted Responder)

        - Un respondedor autorizado por la AC (Authorized Responder)
    - Permite dar respuesta a paquetes con múltiples certificados (emitidos por la misma o por la autoridad que defina el cliente).
    - Cuenta con API's que permiten generar las peticiones hacia el servicio para la validación de estatus.
    - Cuenta con un cliente gráfico que permite realizar consultas por certificados específicos.
    - Permite su operación y configuración en sistemas distribuidos como clusters o granjas para garantizar balanceo de cargas o alta disponibilidad.
    - Cuenta con una consola de configuración donde se establece:
        - Autoridades Certificadoras de Confianza y su configuración
        - Par de llaves para operación del servicio.
    - Permite establecer el puerto TCP de operación del servicio para comunicación de aplicaciones de acuerdo a las definiciones del cliente.
    - Permite la administración del servicio, el poder iniciarlo y detenerlo

✓ Módulo de consulta en línea de estado de certificados digitales.

- Es el 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 2560.

✓ Módulo de publicación de certificados digitales.

- Es el componente responsable de procesar perfiles de publicación de certificados digitales que cumplan con lineamientos establecidos por entidades reguladoras como Secretaría de Economía, Banco de México, ITFEA, IES Infraestructura de Seguridad Extendida o realizar la integración con otras aplicaciones.
    - Las transacciones entre la Autoridad Registradora, los servicios de validación y la Autoridad Certificadora son y pueden ser firmados electrónicamente de acuerdo a los algoritmos utilizados en ITFEA para la generación de certificados.

✓ Módulo de Certificación Automática

La AC cuenta con un módulo a través del cual puedan existir usuarios pre-autorizados y de esta manera sea automática la generación de su Certificado Digital. Este módulo permite:

- La emisión de certificados para usuarios previamente autorizados.
- Establecer la vigencia de los certificados digitales emitidos por defecto.
- Que los datos de los usuarios se encuentren almacenados en tablas específicas en base de datos.
- Que la autenticación de los usuarios pre-autorizados este basada en un nombre de usuario y contraseña o el los datos que el cliente señale.

✓ Modulo Llamadas Externas

- La AC cuenta con un módulo que permite agregar funcionalidad mediante llamadas a una librería dinámica que exporta funciones de acuerdo a una interfaz específica.

- El uso de la librería específica se puede configurar en la interfaz de configuración de la Autoridad Certificadora.

- Las llamadas podrán realizarse al momento de emitir, revocar, re-expedir, renovar, o en todos los casos.

✓ Módulo de emisión masiva de certificados digitales.

- Es un componente que permite procesar solicitudes de certificados digitales por lotes.

✓ Módulo orquestador de transacciones.

- Es el componente responsable de procesar las peticiones realizadas a través de las interfaces de la entidad emisora y registradora.

✓ Interfaces Web Services.

- Es la interfaz que habilita funciones propias de la entidad emisora y registradora y que pueden ser integradas desde otras aplicaciones del cliente.
- Las características de los módulos permiten configurar entornos que operen en alta disponibilidad, replicación de datos y pueden ser escalables.
- Dentro de esta funcionalidad, se pueden tomar datos de los catálogos del cliente, para mostrarlos en los formularios de generación y solicitud de un requerimiento, así como también insertar datos en cualquier solución de firmado.

- Permite establecer el puerto TCP de operación de los Web Services para comunicación de aplicaciones de acuerdo a las definiciones del cliente.
- Proveer los servicios sin depender de un servidor Web y la funcionalidad ofrecida para procesar solicitudes de:
  - Emisión de Certificados Digitales.
  - Revocación de Certificados Digitales.
  - Consulta/reporte de Certificados Digitales

✓ Interfaz Web Módulo para usuarios.

- Es el componente que publica los medios para que los usuarios puedan realizar la solicitud, consulta y revocación de certificados digitales en línea y vía Web.
- Habilita la Generación de llaves y Requerimiento de Certificación con soporte de múltiples CSP (Cryptographic Service Provider), además de su envío a la Autoridad Certificadora. Envío a la Autoridad Certificadora del Requerimiento de Certificación a partir de archivo en formato PKCS#10.
- Permite la Instalación de Certificados Digitales.
- Habilita la Consulta de Certificados Digitales y opción a descarga de los mismos
- Permite la Solicitud y descarga de una CRL.
- Permite Solicitar y descargar del Certificado Digital de Autoridad Certificadora.
- Permite la Revocación de Certificados Digitales a partir de una clave de revocación.
- Permite la Revocación de Certificados Digitales a partir de su autenticación al servidor Web utilizando SSL con autenticación de usuarios.
- Interface Web Gráfica y personalizable de acuerdo a la imagen de la institución.
- La aplicación de generación de llaves e instalación de certificados digitales soporta el uso de tarjetas inteligentes o dispositivos criptográficos.
- La aplicación Web está basada en componentes de tipo CGI.
- La aplicación Web funciona en sistemas operativos Windows

- ✓ Interfaz de Desarrollo.
  - La AC cuenta con herramientas y servicios que permite su integración a aplicaciones propietarias o de terceros,
  - Soporta su operación en Sistemas Operativos Windows y Linux Red Hat
  - Cuenta con API's en Java y .NET que proveen de las siguientes funcionalidades:
    - Emisión de Certificados Digitales.
    - Consulta de Certificados Digitales.
    - Revocación de Certificados Digitales.
    - Consulta de CRLs.

- ✓ Certificados Digitales X509
  - Soporta los siguientes estándares o algoritmos criptográficos en su operación.
  - X.509 – (RFC 3280)
  - En las siguientes versiones del certificado X.509 V1 y V3.

Ejemplo:

1. Versión
   V3
2. Serial Number
   Número secuencial del Certificado Digital emitido por la AC.
3. Signature Algorithm
   SHA256withRSAEncryption y SHA1withRSAEncryption
4. Issuer Distinguished Name
   CN=AC DNIE XXX OU=EMPRESA O= DGRNPIP C=MX S=DF
5. Validity
   Not Before: Jul 1 16:04:02 2011 GMT Not After : Dec 31 16:04:02 2012 GMT
6. Subject
   CN=APELLIDO1 APELLIDO2, NOMBRE(S) G=NOMBRE SN= FECHA DE NACIMIENTO C= MX
7. Subject Public Key Info
   Algoritmo: RSA Encryption y Longitud clave: 1024 bits

V2

1. issuerUniqueIdentifier
   RFC

2. subjectUniqueIdentifier
   CURP

Anexo y en las Extensiones de X509 v3 es donde se colocarán el resto de los datos personales.

Variable personalizada 1
Variable personalizada 2

Diagrama General de la Autoridad Certificadora de PSC Advantage

En el siguiente diagrama se muestra la arquitectura de Advantage PKI

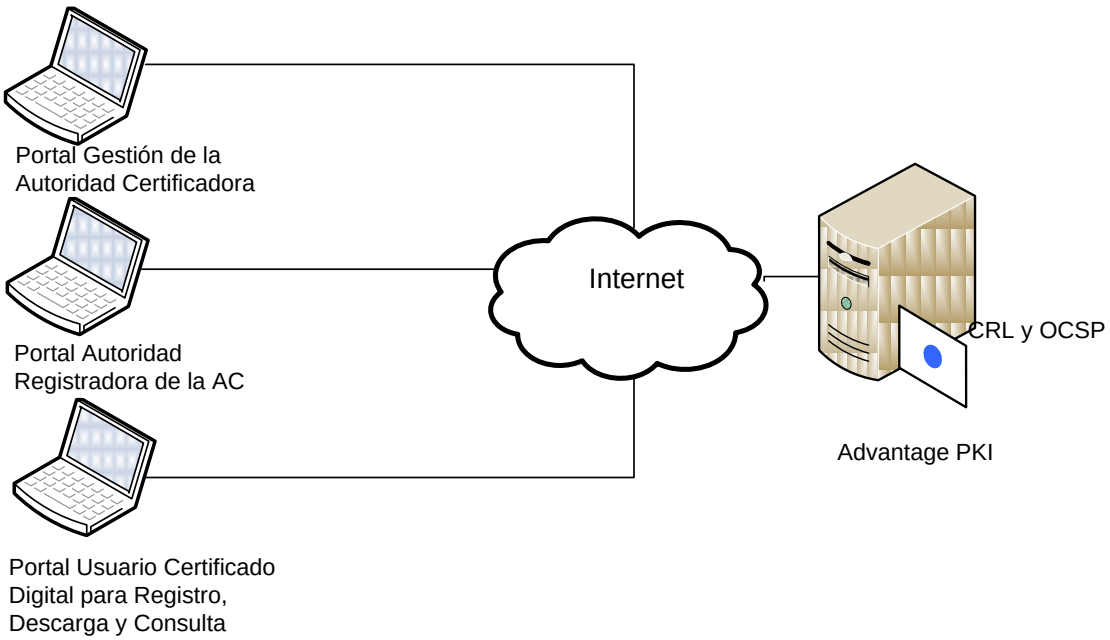
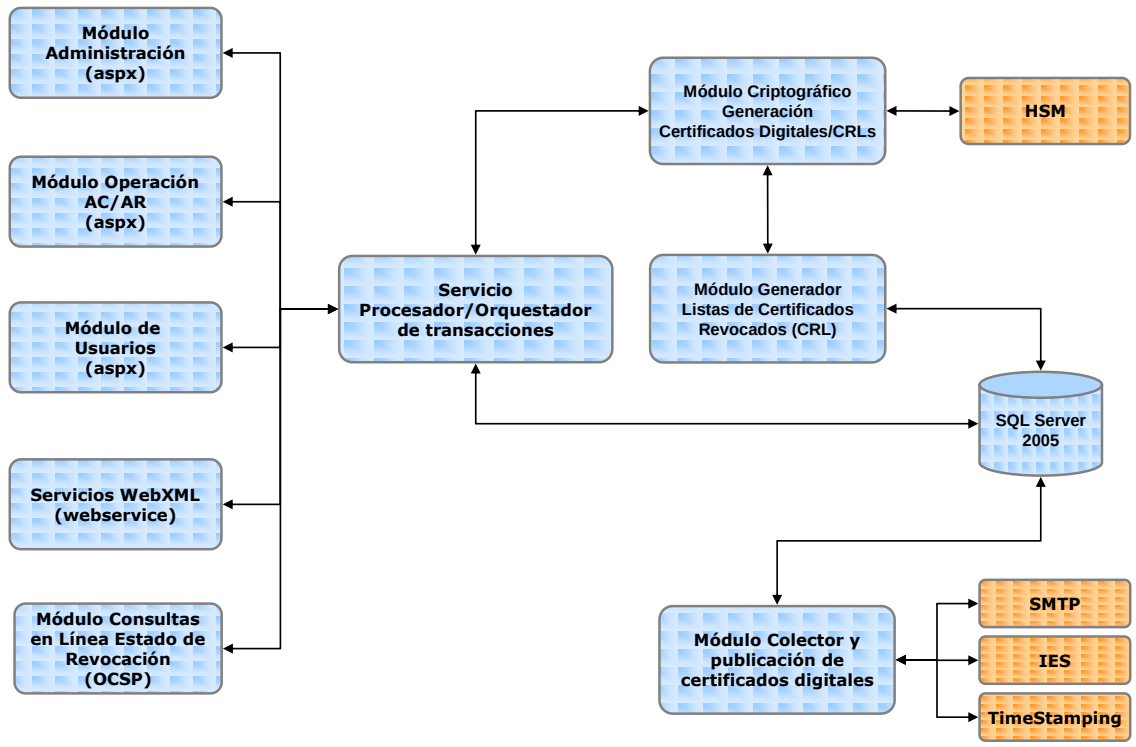


Diagrama General de los Componentes de la AC de PSC Advantage



Requerimientos de Instalación y Operación – Modalidad Inhouse

Todos los componentes operan bajo los siguientes requerimientos tecnológicos.

- ✓ Servidores Windows 2000/2003/2008 a 32 o 64 bits., Linux Red Hat o Linux SUSE a 32 y 64 bits.
- ✓ Base de datos SQL Server
- ✓ Microsoft Internet Information Services (IIS).
- ✓ Integración con Hardware Criptográfico con interfaces compatibles PKCS11 para la administración de llaves raíz (opcional).
- ✓ Procesador de doble núcleo a 3.2 GHz a 32 Bits
- ✓ RAM de 8 Gb
- ✓ Disco Duro de 160 Gb