

CID identitySemantics

Validación semántica de certificados digitales



“Garantice que cumple los requisitos normativos. Compruebe si realmente está utilizando los certificados digitales para el propósito con el que fueron creados por sus emisores”

Validación Criptográfica

- ✓ Integridad certificado
- ✓ Cumplimiento estándar x.509
- ✓ Certificado emitido por un prestador admitido

Validación Operacional

- ✓ Fecha de caducidad
- ✓ Estado de revocación
- ✓ Nivel de confianza del emisor
- ✓ Comprobación de la estructura del certificado acorde con lo establecido por el Prestador

Validación Semántica

- ✓ Actualización continua de las reglas de validación y sus políticas de aplicación mediante seguimiento de las políticas de los PSCs
- ✓ Información sobre las restricciones de uso del certificado
- ✓ Descubrimiento y actualización continua de información que puede extraerse del certificado

Nunca fue tan fácil integrar autenticación robusta mediante certificados digitales en cualquier aplicación corporativa. Mediante esta herramienta **fácil de integrar (basada en SOA), es posible realizar de forma totalmente transparente una validación completa del certificado así como una captura de datos para la aplicación que lo utilice.**

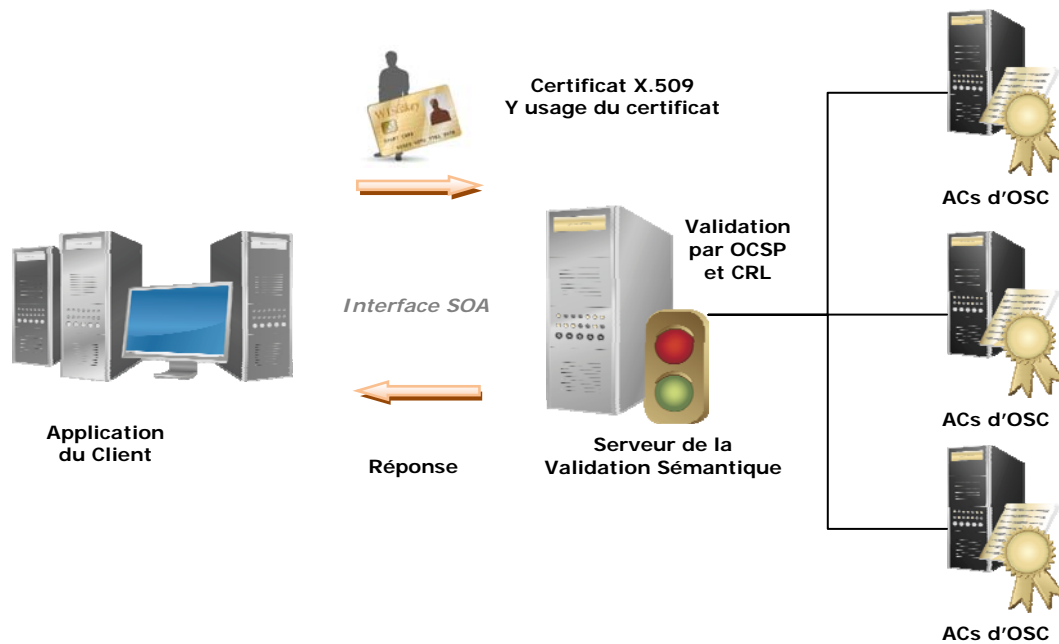
CID identitySemantics es una herramienta de seguridad, diseñada como un servicio, que permite **analizar el estado de un certificado digital** que cumpla con el formato x.509 **desde todos los posibles puntos de vista** que pueden interesar a la lógica de una aplicación o un proceso de negocio.

El cliente, mediante la definición de una política de seguridad (plantillas XML), define los siguientes parámetros:

- ∞ Prestadores de Servicios de Certificación (PSCs) admitidos.
- ∞ Políticas de certificación admitidas de cada prestador.
- ∞ Usos admitidos de los certificados dentro de sus sistemas de información.

Como respuesta se obtiene un informe completo sobre el estado del certificado:

- ∞ **Validez Operacional**
- ∞ **Validez Criptográfica**
- ∞ **Verificación legal**
- ∞ **Obtención información semántica**



Usos principales

- **Securización de acceso a web:** utilización certificados digitales para acceder a páginas o servicios web.
 - Banca electrónica.
 - Portales de ciudadano.
 - Ventanilla electrónica de compañías de servicios.
 - Comercio electrónico....
- **Sistemas de firma electrónica reconocida:** en el momento de realizar la firma, o bien para realizar la verificación de la misma es necesario comprobar el estado del certificado y sus limitaciones de uso.
 - Factura electrónica.
 - Firma de contratos.
 - Registro de entrada/salida.
 - Flujos documentales...
- **Autenticación robusta para terceras aplicaciones:** proxy de autenticación segura basado en certificados digitales para integrar con aplicaciones con autenticación básica (user/password, etc).