



Validación on-line de certificados ocsp

Izenpe, S.A.
Avda. del Mediterráneo, 3
01010 - Vitoria-Gasteiz

© Izenpe, S.A. 2000

Este documento es propiedad de Izenpe, S.A. y su contenido es confidencial. Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de Izenpe, S.A.. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. Izenpe, S.A. no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.



El servicio de validación on-line de certificados OCSP proporciona un sistema fiable para verificar la validez de los certificados utilizados en transacciones electrónicas, tanto en el momento de su realización como a posteriori.

Por cada certificado implicado en una transacción, la aplicación debe enviar al servidor de validación de certificados una petición de verificación de certificado recibiendo una respuesta firmada que indica su estado actual.

OCSP presenta múltiples ventajas sobre la validación basada en listas de revocación (CRL), entre las que cabe destacar:

- Evita la necesidad de distribuir periódicamente CRLs voluminosas y no totalmente actualizadas.
- Permite la verificación a posteriori de la validez de las transacciones si se almacenan las respuestas firmadas, sin necesidad de archivar todas las CRLs.

El uso de OCSP no excluye la utilización de CRLs sino que los dos sistemas se pueden complementar. Dado que la validación con OCSP requiere que el servidor de validación siempre esté disponible, es posible mantener la validación de los certificados contra CRLs como un mecanismo alternativo que puede usarse en el caso de que la validación on-line no esté disponible de forma temporal.