Nota Técnica 20.1

Compatibilidad SHA2

Izenpe

Julio 2014

Beato Tomás de Zumárraga
71 - 1ª Planta
01008 Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 06 77 23

1. Introducción

Debida a emisión de certificados con el algoritmo SHA2, y para prevenir posibles problemas de incompatibilidad, se detallan los productos que lo soportan y desde qué versión.

2. *COMPATIBILIDADES*

Navegadores

- Mozilla =>1.4
- Firefox=>1.5
- IE =>7 (en XP con SP3)

Productos

- *Java =>1.4.2*
- *OpenSSL*

>0.9.7.h Se incluye pero no habilita por defecto

(`New FIPS 180-2 algorithms (SHA-224, -256, -384 and -512`)

- *Si > 0.9.8l viene habilitado por defecto*

(`Major changes between OpenSSL 0.9.8n and OpenSSL 0.9.8o`☺

- *>0.9.8o+ → (Apache>2.0.59)*

- *IAIK-JCE => 3.0 beta 1 (18. May 2001) (por el contenedor de Izenpe)*

Sistemas.Operativos

- *Windows Server 2003 (con KB 938397 y 968730)*
- *Windows XP SP3 (incluye funcionalidad limitada de sha256 - KB 968730)*
- *Windows Server=>2008*
- *Weblogic =>10.3.1*