Especificaciones técnicas

Certificado SSL X.509 versión 3 de 2048 bits con dos campos SAN tipo wildcard

- El certificado debe soportar Múltiples dominios SSL mediante el uso de campos SAN (Subject Alternative Names). Debe soportar campos del tipo Wildcard SSL para los dominios *.mpba.gov.ar y *.mpba.gob.ar. Los nombres de dominio a incluir deben asegurar múltiples dominios de segundo nivel, como por ejemplo: simp.mpba.gov.ar, www.mpba.gov.ar, webmail.mpba.gov.ar, simp.mpba.gob.ar, www.mpba.gob.ar, webmail.mpba.gob.ar, etc.

- El certificado debe proveer validación y autenticación completa de los nombres de dominio y del organismo solicitante.

- El certificado raíz de la Autoridad Certificante (CA) y los certificados intermedios deberán encontrarse instalados en las actualizaciones de los repositorios de certificados de los principales sistemas operativos del mercado, incluidos Microsoft Windows XP Service Pack 3 o superior, Linux Debian 7 o superior, Android 4 o superior, Windows Phone 8 o superior.

- El campo Common Name (CN) del certificado será: *.mpba.gov.ar junto a los campos SAN *.mpba.gov.ar y *.mpba.gob.ar.

- El certificado emitido deberá tener una validez de 3 años.

- La Autoridad Certificante debe comunicar públicamente que no cobre licencia adicional para cada servidor en el cual se quiera instalar el certificado.

- Soporte de protocolo SHA-2.

- Soporte IDN (Internationalized Domain Names).

- Posibilidad de re-emitir el certificado sin costo adicional si fuera necesario cambiar los campos SAN durante el periodo de validez.

- Posibilidad de re-emitir el certificado sin costo adicional ante la necesidad que implique una incidencia de seguridad durante el periodo de validez.

- El certificado debe permitir agregar como mínimo 20 campos SANs, incluidos campos Wildcard, durante todo el periodo de validez.

- Debe proveer verificación de validez del certificado mediante OCSP y

- El certificado emitido debe ser generado a partir de una Solicitud de Firma de Certificado (CSR) en formato PEM (Privacy Enhanced Mail) generado por la Procuración General a partir de una clave privada de 2048 bits, mediante el software OpenSSL.

- El certificado entregado debe poder convertirse a formato PEM (Privacy Enhanced Mail), a los formatos binarios DER CRT CER y PKCS#12 (.pfx .p12) mediante el Software OpenSSL.

- El certificado emitido debe ser compatible con el Software Apache Web Server.

- El certificado emitido debe ser compatible con el Software Microsoft Internet Information Server, previa conversión del certificado a formato PKCS#12 (.pfx) mediante software OpenSSL.

- Soporte para encriptación a 128 / 256 bits o superior (dependiendo del navegador del usuario).

- Compatible con cualquier browser y servidor web que utilice el protocolo TLS v1.0 / SSL v3.0 o superior como Internet Explorer, Mozilla Firefox, Opera, Chrome, Safari incluidas las versiones para dispositivos móviles.

- Soporte técnico local durante el período de validez del certificado telefónico, e-mail y web.