

Documentación » Biblioteca PHP » Legacy OpenSSL

Legacy OpenSSL

Nota sobre el uso de OpenSSL 3

Anonymous · 08/10/2026

Legacy OpenSSL

A partir de OpenSSL 3, ciertos algoritmos que anteriormente eran estándar han sido considerados inseguros o “no compatibles”, entre ellos la encriptación de certificados PKCS#12 con 40BitRC2 que es utilizada por los certificados digitales que se utilizan con el SII.

Para que se puedan utilizar los certificados digitales, se debe editar la configuración de OpenSSL en `/etc/ssl/openssl.cnf` para activar los proveedores *legacy*.

```
[default_conf]
openssl_conf = openssl_init

[openssl_init]
providers = provider_sect

[provider_sect]
default = default_sect
legacy = legacy_sect

[default_sect]
activate = 1

[legacy_sect]
activate = 1
```

Revisar compatibilidad con OpenSSL 3

Ejecutar:

```
openssl pkcs12 -in certificadoDigital.pfx -info -nokeys -nocerts
```

Nota: la extensión puede ser `.pfx` o `.p12`.

Si en la respuesta está presente PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC indica que se está utilizando 40BitRC2 en el certificado digital para encriptarlo, lo cual es obsoleto e inseguro.

Referencias

- https://wiki.openssl.org/index.php/OpenSSL_3.0#Providers
- <https://stackoverflow.com/a/74416513>
- <https://stackoverflow.com/a/72600724>

Última actualización el 08/10/2026