



NOTA TÉCNICA: CAMBIOS EN EL ROOT PROGRAM DE APPLE 2022

Izenpe

© Izenpe s.a. 2022

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.

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

www.izenpe.eus
izenpe@izenpe.eus



Introducción

Apple utiliza infraestructura de clave pública para proteger y mejorar la experiencia de los usuarios de Apple. Los sistemas operativos y las aplicaciones de Apple (como Safari y Mail) utilizan un almacén común para los certificados raíz; para que los certificados raíz de las diferentes entidades de certificación estén incluidas en ese almacén, las entidades de certificación deben cumplir una serie de condiciones técnicas recogidas en el documento *Root Program* de Apple:

(https://www.apple.com/certificateauthority/ca_program.html)

El 1 de febrero de 2022 entró en vigor una nueva versión del documento, en la que se indica entre otros cambios que los certificados que permitan realizar firmas SMIME (firmas de correo electrónicos) y que sean emitidos a partir del 1 de abril de 2022 no pueden tener una vigencia superior a 1185 días.

Impacto en Izenpe

Los únicos perfiles de certificados emitidos por Izenpe que tiene utilidades de firma SMIME son los certificados profesionales.

PROFESIONAL					
Breve descripción	Soporte	Identificador de política	OID política	Nivel identificación eIDAS	Tipo firma eIDAS
Personal de Entidad Pública	Chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.4.14.1	Alto	Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.4.14.2	Sustancial	Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Alto (con tarjeta virtual) Sustancial (con Giltza)	Avanzada
Corporativo cualificado	Chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.2.19.1 1.3.6.1.4.1.14777.4.2	Alto	Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.19.2	Sustancial	Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Alto	Cualificada

Para cumplir con las exigencias del *Root Program* de Apple, reduciremos la vigencia de estos certificados de 4 años a 3 años, y este cambio será efectivo a partir del 31 de marzo.