¿Cuánto cuesta CAcert?

Los certificados son gratuitos.
Gracias a los voluntarios que mantienen los servicios automatizados de CAcert, podemos trabajar a muy bajo coste. Las donaciones ayudan a cubrir los gastos de CAcert, y por lo tanto son más que bienvenidas.

¿Cómo puedo contribuir en CAcert?

- Siendo miembro de la comunidad CAcert y usando nuestros certificados.
- Superando el Reto de Asegurador de CAcert y siendo así un Asegurador de CAcert.
- Apoyando CAcert en eventos y difundiendo su uso.
- Ayudando con alguna tarea de CAcert, como por ejemplo administrador de sistemas o dando soporte.

Véase: http://wiki.cacert.org/HelpingCAcert

¿Dónde puedo obtener más información?

Para más información, visita:
el sitio oficial de CAcert: http://www.cacert.org
el wiki de CAcert: http://wiki.cacert.org

CAcert cuenta con canales de charla IRC en irc.cacert.org. En ellos puedes opinar sobre sus servicios, obtener soporte técnico, o simplemente entrar en contacto con el resto de la comunidad de CAcert.

Canales:	#cacert	(Inglés)
	#cacert.ger	(Alemán)
	#cacert.fr	(Francés)

Para una conexión segura con SSL, usa el puerto 7000.

¿Que no tienes un cliente IRC? Puedes conectarte desde la interfaz web: http://irc.cacert.org

Correo electrónico de soporte:
cacert-support@lists.cacert.org

Lista de correo de soporte y discusión:
cacert-es@lists.cacert.org

Información sobre soporte:
http://wiki.cacert.org/GettingSupport

http://www.cacert.org

Soporte

Email: cacert-support@lists.cacert.org
Canal IRC: #cacert en el servidor irc.cacert.org

Huellas digitales (fingerprints)

Certificado raíz CAcert

SHA1: 13:5C:EC:36:F4:9C:B8:E9:3B:1A:B2:70:CD:80:88:46:76:CE:8F:33
MD5: A6:1B:37:5E:39:0D:9C:36:54:EE:BD:20:31:46:1F:6B

Certificado raíz CAcert Class 3

SHA1: AD:7C:3F:64:FC:44:39:FE:F4:E9:0B:E8:F4:7C:6C:FA:8A:AD:FD:CE
MD5: F7:25:12:82:4E:67:B5:D0:8D:92:B7:7C:0B:86:7A:42

Flyer-2s-3c-En 2.05 rev. 01 (June 2011)

Certificados digitales personales y para organizaciones

certificados para clientes
certificados para servidores
firma de código

X.509 ◆ SSL/TLS ◆ S/MIME
PGP ◆ GnuPG ◆ OpenPGP

http://www.cacert.org

Certificados digitales

¿Qué es CAcert?

CAcert es una organización basada en una comunidad, sin ánimo de lucro y registrada en Australia.

Los objetivos de CAcert son:

- Mejorar la seguridad en la era de las Tecnologías de la Información y la Comunicación
- Ayudar a los usuarios que quieran una mayor seguridad
- Proveer herramientas y mecanismos seguros

Campos a los que se puede aplicar:

- Asegurar servidores web usando HTTPS y cifrar el correo electrónico
- Comunicación con aplicaciones web que usen SSL/TLS
- Comunicación con VPN
- Firma de código (por ejemplo, Java)
- Firma digital de documentos

El objetivo de CAcert es hacer disponible la seguridad en el mundo de las nuevas tecnologías y conseguir que las medidas de seguridad sean asequibles para todos. CAcert es una comunidad abierta y sigue la filosofía del Código Abierto para lograr sus metas.

¿Por qué debería unirme?

Seguridad:
Permite que Internet sea seguro para ti y para los demás usuarios.

Privacidad:
Los certificados CAcert ayudan a mantener su privacidad en Internet.

Autenticación:
Demuestra que tu identidad ha sido verificada y que eres quien realmente dices ser.

Certificados de correo y servidores gratuitos

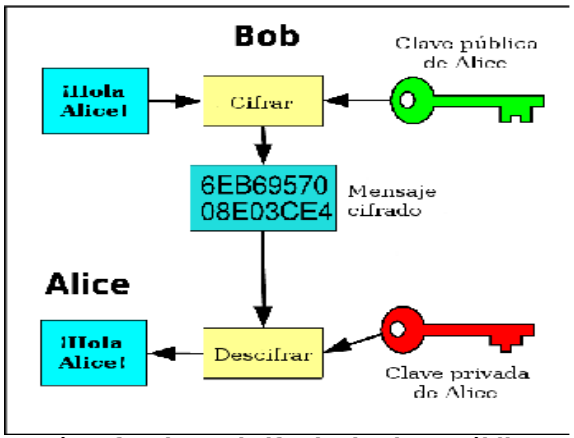
Los certificados X.509 se pueden usar para firmar correos electrónicos usando S/MIME y para que los servidores, web o de correo por ejemplo, puedan ofrecer conexiones seguras. La mayoría de las Autoridades Certificadoras que existen, te suelen pedir altos precios por hacer el trabajo de un notario: verificar tu identidad y si un sitio web o una dirección de correo electrónico te pertenece realmente. CAcert te lo ofrece gratis.

¿Cómo funciona CAcert?

Para unirte a CAcert necesitas crearte una cuenta personal en http://www.cacert.org. Sólo necesitas especificar tu nombre completo, fecha de nacimiento y correo electrónico. Puedes añadir tantas direcciones de correo como quieras para certificados de cliente y también tantos nombres de dominio como quieras para certificados de servidor.
Una vez hecho, puedes empezar a emitir certificados tú mismo usando la interfaz web. Para incluir tu nombre en el certificado es necesario que tu identidad haya sido verificada. Contacta con los Aseguradores (puedes hacerlo usando el buscador de Aseguradores disponible en la web) o encuéntralos en alguno de los eventos.

Firma de claves PGP gratuita

¿Tienes claves PGP/GnuPG/OpenPGP? Un Asegurador puede firmar tus claves con la clave PGP de CAcert.



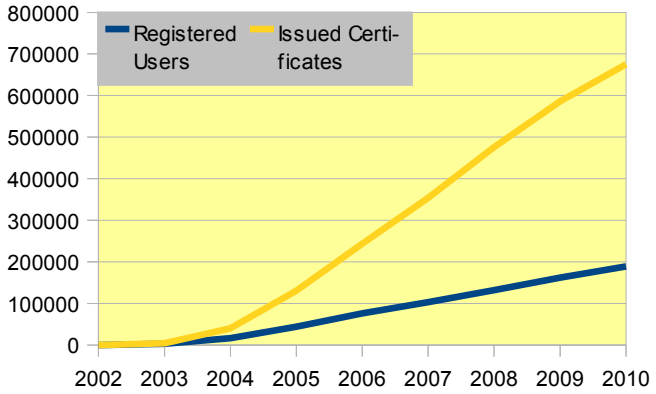
Cómo funciona el cifrado de clave pública

Firmado de código

Puedes firmar digitalmente tu software usando certificados de CAcert para identificarlo y autenticarlo.

Organizaciones

Para compañías y organizaciones, CAcert tiene un programa de Aseguración de Organizaciones. Una vez asegurado, podrás emitir certificados que contengan el nombre de la organización y los empleados o miembros de la organización podrán tener sus propios certificados emitidos por la organización.



Crecimiento de CAcert desde su fundación en 2002

¿Qué software soporta certificados CAcert?

Puedes usar certificados de cliente CAcert en todo software que soporte certificados X.509 (S/MIME).
Por ejemplo:

- Microsoft Outlook y Office
- Mozilla Thunderbird y Firefox
- OpenOffice.org

Puedes usar certificados de servidores en todo software que soporte certificados basados en SSL.
Por ejemplo:

- Servidor web Apache
- Microsoft Internet Information Services
- Servidores de correo como Postfix, Sendmail, Courier...
- OpenSSL/OpenVPN