



CAcert.org: Unsere Mission

Errichtung einer gemeinnützigen (Non-Profit) Certificate Authority als Alternative zu den kommerziellen CAs.

Wer?

Kernmitglieder von CAcert haben im Allgemeinen einen Sicherheits- und Informationstechnologischen Hintergrund, sowie ein stärkeres Bedürfnis etwas für die Gemeinschaft zu tun.

Viele sind einfach Nutzer des Systems, welche durch dessen Nutzung zu seiner Verbreitung per 'Mund-zu-Mund-Propaganda' beitragen.

Warum?

Viele Menschen sind derzeit mit den kommerziellen Angeboten nicht zufrieden. Viele Menschen möchten sich nur mit ihnen bekannten Personen verbinden oder austauschen oder sie wollen Ihren Webmail-Zugang vor anderen Personen schützen, die potenziell Ihren Datenverkehr mitschnüffeln könnten. Warum sollte man sich an einen Dienstleister binden, der nicht so strukturiert ist, dies zu gewährleisten und dafür obendrein noch ein halbes Vermögen dafür verlangt?

CAcert Inc., ein gemeinschaftlich getragenes Projekt, ist nicht durch Profit, sondern dem Verlangen der Gemeinschaft nach Privatsphäre und Sicherheit bestimmt.

Wie?

Auf OpenSSL, PHP, ein wenig C und MySQL basierend haben wir es nicht nur fertig gebracht eine kostenlose Certificate Authority (CA) die Ihre E-Mail-Adresse oder Domäne überprüft zu errichten, sondern auch ein hoch effizientes Vertrauens-Verfahren. Unser Verfahren geht in der Feststellung Ihrer Identität über Verfahren anderer, kommerzieller CAs hinaus.

Wann und wo?

Genau jetzt passiert alles um Sie herum. Es gibt schon gesicherte Websites und geschützte E-Mail-Protokolle, auf die Leute vertrauen und von CAcert signiert sind.

Und was kann ich zum Gelingen beitragen?

Der einfachste und effizienteste Weg das zu tun ist: weitersagen. Erzähle Deinen Freunden, Kollegen und Verwandten von uns und mache mit.

Informationen



Was kann CACert Ihnen bieten, um kostenlos Ihre Privatsphäre und Sicherheit zu verbessern?

Client-Zertifikate (nicht assured)	<p><u>Vorteile:</u> Sie können digital signierte und verschlüsselte E-Mails versenden; andere können Ihnen verschlüsselte E-Mails zuschicken.</p> <p><u>Einschränkungen:</u> Das Zertifikat verfällt in 12 Monaten; nur Ihre E-Mail-Adresse kann in das Zertifikat aufgenommen werden (nicht Ihr Name)..</p> <p><u>Benötigter Nachweis:</u> Um zu bestätigen, dass eine E-Mail-Adresse wirklich zu Ihnen gehört, müssen Sie auf eine 'ping'-E-Mail antworten, die an diese Adresse geschickt wird.</p>
Bestätigte Client Zertifikate	<p><u>Vorteile:</u> So wie oben und Sie können zusätzlich Ihren Namen in das Zertifikat aufnehmen lassen.</p> <p><u>Einschränkungen:</u> Das Zertifikat läuft in 12 Monaten ab.</p> <p><u>Benötigter Nachweis:</u> So wie oben und Sie benötigen mindestens 50 Assurance Punkte, die Sie durch Treffen mit mehreren Assurern des CACert Web of Trust bekommen können. Bei so einem Treffen müssen Sie sich gegenüber dem Assurer mit einem offiziellen Lichtbildausweis ausweisen.</p>
Code signierende Zertifikate	<p><u>Vorteile:</u> Signieren Sie Ihren Code, Web Applets, Installer, etc. mit Ihrem Namen und Ort aus dem Zertifikats.</p> <p><u>Einschränkungen:</u> Certificates expires in 12 months; certificates must include your full name.</p> <p><u>Benötigter Nachweis:</u> So wie oben und Sie benötigen mindestens 100 Assurance Punkte, die Sie durch Treffen mit mehreren Assurern des CACert Web of Trust bekommen können. Bei so einem Treffen müssen Sie sich gegenüber dem Assurer mit einem offiziellen Lichtbildausweis ausweisen.</p>
Server Zertifikate (unbestätigt)	<p><u>Vorteile:</u> Ermöglichen Sie verschlüsselte Datenübertragungen für Benutzer von Web, E-Mail und anderen SSL-fähigen Diensten auf Ihrem Server; Wildcard Zertifikate sind erlaubt.</p> <p><u>Einschränkungen:</u> Das Zertifikat verfällt in 12 Monaten; nur ein Domain-Name kann in das Zertifikat aufgenommen werden (nicht Ihr eigener Name, Firmenname, Ort, etc).</p> <p><u>Benötigter Nachweis:</u> Sie müssen bestätigen, dass Sie der Besitzer (oder autorisierte Administrator) einer Domain sind, indem auf eine 'ping'-E-Mail antworten, die entweder an eine im Whois-Eintrag angegebene Adresse oder an eine laut RFC vorgeschriebene Adresse (hostmaster/postmaster/etc) geschickt wird.</p>

<p>Bestätigte Server Zertifikate</p>	<p><u>Vorteile:</u> So wie oben.</p> <p><u>Einschränkungen:</u> So wie oben, allerdings ist das Zertifikat 24 Monate gültig.</p> <p><u>Benötigter Nachweis:</u> So wie oben und Sie benötigen mindestens 50 Assurance Punkte, die Sie durch Treffen mit mehreren Assurern des CAcert Web of Trust bekommen können. Bei so einem Treffen müssen Sie sich gegenüber dem Assurer mit einem offiziellen Lichtbildausweis ausweisen.</p>
<p>Werde Assurer im CAcert Web of Trust</p>	<p><u>Vorteile:</u> Die Erlaubnis, andere neue CAcert Benutzer zu assure; zur Stärkung und erweiterung des CAcer Web of Trust beitragen.</p> <p><u>Einschränkungen:</u> Die Anzahl der Assurance Punkte die Sie besitzen, begrenzt die maximale Anzahl an Punkten die Sie an andere Benutzer vergeben können.</p> <p><u>Benötigter Nachweis:</u> Sie benötigen mindestens 100 Punkte, die Sie durch ein Treffen mit einem Assurer des CAcert Web of Trust erhalten können. Dieser prüft Ihre Identität anhand eines offiziellen Lichtbildausweises; ODER, wenn es nicht möglich ist einen Assurer in Ihrer Gegend zu treffen, dann können Sie sich mit zwei Trusted Third Party Assurer (zwei vertrauenswürdigen Dritten Parteien wie z. B. Notaren, Anwälten, Bank-Managern, etc.) treffen, die dann Ihre Identität überprüfen.</p>
<p>Werde Mitglied der CAcert Association</p>	<p><u>Vorteile:</u> Sie dürfen mitentscheiden wie CAcert (eine in Australien als gemeinnützig eingetragene Organisation) betrieben wird; Sie können sich in den CAcert Vorstand wählen lassen.</p> <p><u>Einschränkungen:</u> Keine.</p> <p><u>Benötigter Nachweis:</u> Keine; Mitgliedsbeitrag beträgt \$10 USD pro Jahr.</p>

(*) Bitte beachten Sie, dass im Gegensatz zu den Zertifikaten der grossen Zertifizierungsstellen wie Verisign das Root-Zertifikat von CAcert momentan nicht in die bekannten Browsern und E-Mail-Programmen, etc. aufgenommen wurde. Das bedeutet, dass jeder, dem Sie eine signierte E-Mail senden oder der auf Ihre SSL-verschlüsselte Webseite zugreift, zunächst das CAcert Root-Zertifikat installieren muss. Ansonsten wird bei jedem Zugriff eine Sicherheitswarnung angezeigt, die besonders unerfahrene Benutzer abschrecken kann.



Datenschutzrichtlinien

Diese Policy beschreibt, welche Informationen CACert über Sie sammelt, wenn Sie eine CACert Webseite besuchen. Im weiteren wird beschrieben wie diese Informationen benutzt werden und wie Sie dies kontrollieren können.

Wir sammeln zwei Arten von Informationen über unsere Anwender: 1) Daten, die der Anwender beim Registrieren bei der Webseite preisgibt oder wenn Sie uns ein E-Mail über das Kontaktformular schreiben; und 2) Zusammengefasste Protokolle über die Verwendung der Website.

Persönliche Informationen

Wenn Sie uns über das Kontaktformular eine Mitteilung schicken, müssen Sie Ihren Namen und Ihre E-Mail-Adresse angeben. Wenn Sie sich an der Webseite anmelden, müssen Sie Ihren Namen, E-Mail Adresse, Geburtsdatum, und einige Passwort-Vergessen-Fragen und zugehörige Antworten angeben.

Wir geben Ihre Informationen nicht an irgendeine andere Organisation weiter.

Zusammengefasste Tracking Information

Wir analysieren die Besuchernutzung, indem wir Informationen über z. B. Seitenaufrufe, Spitzenwertmessungen, Suchbegriffe und gewählte Linksaufzeichnungen. Wir benutzen diese Informationen, um unsere Seiten zu verbessern. Wir geben diese anonymen statistischen und demographische Daten in gesammelter Form an Werbeanbieter und andere Geschäftspartnern weiter. Wir geben keine Informationen an Werbeanbieter weiter, die einen bestimmten Benutzer identifizieren können.

Cookies

Manche unserer Werbeschaltungen verwenden Werbeserver von Dritten, um die Werbung anzuzeigen. Diese Werbung kann Cookies enthalten. Diese Werbeserver empfangen diese Cookies, wir haben keinen Zugriff darauf.

Wir verwenden keine Cookies, um persönliche Informationen abzuspeichern. Wir verwenden Sessions, und wenn Cookies in Ihrem Browser aktiviert sind, speichern wir die Session-ID in einem Cookie. Wir schauen nicht nach anderen Cookies außer der Session-ID. Sollten Cookies deaktiviert sein, dann wird keinerlei Information auf Ihrem Computer gespeichert oder abgefragt.

Benachrichtigung bei Veränderungen

Wenn wir entscheiden die Datenschutzrichtlinien zu ändern, werden alle Änderungen auf www.CAcert.org bekanntgegeben. Wenn wir uns zu einer Änderung bzgl. der Verwendung der persönlichen Daten entscheiden, werden die betroffenen Benutzer per E-Mail verständigt. Die Benutzer werden die Möglichkeit haben, Ihre Daten von der neuen Verwendung auszuschließen.

Eigene Daten ändern, korrigieren oder löschen

Sie können Ihre Informationen jederzeit ändern, hinzufügen und löschen, loggen Sie sich bei 'Mein Konto' ein, und klicken Sie dann auf 'Meine Details'.

Wenn Sie uns schriftlich kontaktieren wollen, schreiben Sie bitte an:

CACert Inc.
P.O. Box 81
Banksia NSW 2216
Australia