CAcert Waarmerkings Programma

Identiteit Verificatie Formulier (CAP) form

CAcert Inc. - P.O. Box 4107 - Denistone East NSW 2112 - Australia - http://www.cacert.org

CAcert Root Certificate ***class 1***: 135C EC36 F49C B8E9 3B1A B270 CD80 8846 76CE 8F33 ***class 3***: AD7C 3F64 FC44 39FE F4E9 0BE8 F47C 6CFA 8AAD FDCE

Het CAcert Waarmerkings Programma (CAP) heeft als doel het in een persoonlijke ontmoeting controleren van de identiteit van Internet gebruikers aan de hand van door de overheid uitgegeven foto identiteit documenten. De kandidaat vraagt de waarmerker om voor de CAcert Gemeenschap te verifiëren dat de waarmerker de kandidaat heeft ontmoet en via oorspronkelijke documenten de identiteit heeft geverifieerd. De waarmerker kan een exemplaar van de gegevens bij de kandidaat achterlaten, en kan na de ontmoeting de waarmerking voltooien en ondertekenen. Indien er enige twijfel is over de identiteit van de aanvrager, dan wijst de waarmerker geen punten toe. U wordt aangemoedigd om een waarmerkingen “wederzijds” uit te voeren.

Voor meer informatie over het CAcert Waarmerkings Programma, met inbegrip van gedetailleerde gidsen voor CAcert waarmerkers, bezoek: http://www.cacert.org

Een arbiter van CAcert kan, in het geval van een geschil, de waarmerker verzoeken om het ingevulde formulier in te leveren. Na 7 jaar kan dit formulier op een veilige manier vernietigd worden, met name om identiteits misbruik tegen te gaan, b.v. door het formulier te versnipperen of verbranden. De waarmerker bewaard nooit een kopie van het ID.

Voor het CAcert Organisatie Waarmerkings Programma is er een afzonderlijke COAP formulier.

Plaats (en gebeurtenis naam) van de persoonlijke ontmoeting:

Identiteits gegevens		points allocated
Exacte volledige naam op het ID	*Type identiteit bewijs*	max 35
Email adres	*Geboorte datum (yyyy-mm-dd)*	

Verklaring aanvrager

Zorg ervoor dat u de CAcert gemeenschap overeenkomst hebt gelezen (CCA)

☑ Hierbij verklaar ik dat de gegevens betreffende mijn identiteit correct en naar waarheid zijn ingevuld en ik verzoek de CAcert waarmerker hiervan getuige te zijn ten behoeve van het CAcert Waarmerkings Programma.

☑ Ik ga akkoord met de CAcert gemeenschapsovereenkomst (CCA).

Datum (yyyy-mm-dd) *Handtekening aanvrager*

Verklaring verzekeraar

Naam van de waarmerker *Geboorte datum (yyyy-mm-dd)*

Email waarmerker (optioneel)

☑ Ik, acterend als officiële waarmerker, bevestig hierbij dat ik de identiteit van Aanvrager heb geverifieerd en daarvan zal getuigen voor het CAcert Waarmerkings Programma en dat ik waarmerkings punten zal toekennen.

☑ Ik ben lid van de CAcert gemeenschap, ik heb minimaal 100 waarmerkings punten en ik heb de Waarmerkers Test met goed gevolg doorlopen en afgesloten.

Datum (yyyy-mm-dd) *Handtekening Waarmerker*

Certificaat Autoriteit voor gratis certificaten

"To create a community based, non-profit Certificate Authority."

CAcert is een Gemeenschap die Certificaten verstrekt. De verstrekte Individuele en Organisatie certificaten zijn kosteloos. CAcert heeft geen winst oogmerk en is gebaseerd op de principes van de Open Source gemeenschap.

Wat zijn digitale certificaten?
De digitale certificaten worden in Internetland gebruikt voor identiteits- en veiligheidsmaatregelen. De digitale certificaten zijn gestandaardiseerde X.509 certificaten.

Bijna alle communicatie hulpmiddelen zoals browsers, e-mailcliënten en Webservers ondersteunen hen. Met deze digitale certificaten, kunt u uw software documenten coderen voor beveiligde communicatie, uw tegenpartij identificeren, en aan te tonen dat documenten veilig van u afkomstig zijn.

Gebruikers zoals banken kunnen deze gebruiken om verklaringen van transactie rapporten veilig naar u te zenden. Sommige belastingafdelingen kunnen zo uw voorbereide documenten goedkeuren, en uw kunt eveneens uw advocaat bereiken met meer veiligheid en handhaving van uw privacy.

Browser-gebruikers kennen bij het gebruik het „https" in de adres URL, en het kleine hangslot pictogram. Technische mensen herkennen het gebruik bij TLS, SSL, en S/MIME als gemeenschappelijke protocollen die op deze certificaten zijn gebaseerd.
Het certificaat bestaat uit twee delen: een privé encryptiesleutel (bewaar die op een veilige plaats) en een openbare sleutel. De laatstgenoemde publieke sleutel heeft een waarmerking van een certificaat autoriteit (CA) nodig, zodat u kunt zeggen: „ja, dit certificaat niet vals en is werkelijk van mij".
Indien een document wordt ondertekend en/of is gecodeerd met het certificaat van de afzender kunt u als ontvanger de data decoderen. Met de hulp van de ondertekening met een certificaat weet u zeker dat het verstuurd is door de verzender.

Indien iemand informatie verzendt welke met een certificaat sleutel is gecodeerd, pas dan is men er zeker van dat niemand anders dan de eigenaar van het certificaat de in-formatie kan lezen. Als beide partijen hun certificaat sleutels gebruiken, dan is men er zeker van dat alleen deze twee de informatie kunnen decoderen. Men is er dan zeker van zijn dat het bericht van die bepaalde persoon kwam.

De certificaten worden gebruikt voor gegevens identificatie (wie spreekt mij toe), voor het beveiligen van informatie en/of het verbergen (het versleutelen) van de informatie voor derden.

Wat is een Certificaat Autoriteit?
Een Certificaat autoriteit (CA) geeft certificaten uit (uw openbare ondertekende sleutel) wanneer het een aantal basis controles heeft uitgevoerd. Over het algemeen moet de CA weten wie u bent en er zeker van zijn dat u persoonlijk verzoekt dit certificaat te laten ondertekenen door de CA.

CAcert gebruikt een netwerk van waarmerkers die u identificeren (Web-of-Trust), uw naam en email adres voor op het certificaat controleren en dat u met de CAcert gemeenschapsovereenkomst

akkoord gaat (de CCA).

Zodra deze informatie voldoende door CAcert is gecontroleerd, kunt u CAcert certificaten aanmaken onder uw gecontroleerde naam.

Waarom is CAcert bijzonder?
CAcert ondertekent certificaten kosteloos, gebruik makend van onze leden om de waarmerking van informatie uit te voeren. Dit staat bekend als Web-of-Trust.

Elke gebruiker, indien voldoende gewaarmerkt (het 100 waarmekings-punten niveau), en geslaagd is voor de waarmerkers test, kan dan helpen om andere, nieuwe gebruikers te waarmerken.

U kunt zo veel CAcert cliënt en server certificaten aanmaken als u nodig hebt voor: identificatie, e-mail, systeem toegang, VPNs, veilige Webservers, enz. U kunt certificaten met één van uw eigen individuele volledige namen (het Certificaat Waarmerkings Programma) of met uw organisatienaam (het organisatie waarmerkings programma) aanmaken.

Waarom CAcert?
Een Commerciële CA kan zeker van goede dienst zijn voor grote bedrijven, maar vele mensen wensen om hun vrije software zo goed mogelijk te gebruiken zonder voor elke certificaat en elk jaar weer te moeten betalen.

Wanneer de gebruikers slechts persoonlijke e-mail willen beveiligen, of de lokale websites met familie foto's, of ontwikkelaars die veilige code willen ontwikkelen als plugin voor toepassingen zoals Firefox, is er CAcert als CA met alle certificaten die zij nodig hebben: en wel kosteloos en niet discriminerend!
De certificaten van CAcert worden vrij verstrekt ongeacht het aantal, de encryptie sterkte, etc.

Hoe doet CAcert dit dan?
Gebaseerd op OpenSSL, PHP, MySQL, enz. heeft CAcert niet alleen een Certificaat Autoriteit opgezet die uw e-mail-adres of uw domein kan verifiëren, en een mechanisme gecreëerd met vertrouwensmodel om uw identiteit te waarmerken en dat kwaliteit beter is dan de service van menig commerciële CA.

Meer dan 150.000 (status van 2009) personen doen mee in de CAcert gemeenschap. Er zijn meer dan 300.000 certificaten verstrekt. Meer dan 100.000 domeinen gebruiken nu certificaten van CAcert om hun Web diensten te beveiligen. Elke maand worden er meer dan 5.000 vrije certificaten CAcert verstrekt. Meer dan 2.000 nieuwe personen sluiten zich elke maand aan.

Overal op de wereld zijn CAcert waarmerkers actief om u te helpen.

Hoe aanmelden
Lees, voor u zich opgeeft, bij CAcert de gemeenschaps-overeenkomst (de gebruiksovereenkomst, privacy bepalingen, arbitrage, uw aansprakelijkheid, de veiligheids maatregelen, het beleid).
Bezoek de www.cacert.org web site.
Als u akkoord gaat, klik op 'Join'. In de eerste stap van het registratie proces, worden een aantal vragen gesteld. U bent verplicht om correcte identificatie informatie in te vullen. Lees ook de CAcert privacy verklaring.

Om u te helpen en om u (b.v. bij vergeten wachtwoord) opnieuw te identificeren vraagt CAcert u om vijf vragen/antwoorden op te geven. Bij deze vragen, kunt u willekeurige of valse antwoorden geven, zolang u maar zeker bent dat u ze later kunt herinneren!

Zodra u het registratie proces hebt voltooid, zult u een "E-mail ping" ontvangen op uw email adres waarmee u zich hebt aangemeld te verifiëren. Volg de aanwijzingen in deze e-mail op om uw registratie af te maken, en uw account bij CAcert te activeren. Zodra u hebt ingeschreven, kunt u uw eerste (tijdelijk) certificaat aanmaken. In plaats van uw naam, bevat de 'Common Name' op het

certificaat de waarde "CAcert User Cert". Om één van uw volledige namen op het certificaat te krijgen, moet u zich bij het waarmerkings programma aansluiten. Wanneer u minimaal 50 waarmerkings punten hebt vergaard wordt uw naam opgenomen in uw door CAcert getekende certificaten.

Vanaf dat moment kunt u certificaten aanmaken voor al uw e-mail adressen, die u bij CAcert hebt geregistreerd.

Hoe wordt u gewaarmerkt?
Individuen
Vul voor elke waarmerking een CAcert Identiteit Verificatie Formulier (CAP) in (zie de website CAcert), breng minstens één officiële identiteitskaart met een foto (b.v. uw paspoort, identiteitskaart, rijbewijs) mee naar de waarmerking.

Bepaal de plaats en maak een afspraak met een CAcert waarmerker. De gemakkelijkste manier is op een bijeenkomst zoals een conferentie, workshop, IT beurs, enz.

Een snelle manier is om waarmerkers in uw buurt te zoeken (zie de waarmerkerslijst op de website) en maak met hen een afspraak.

Op deze wijze kunt u de Waarmerkingspunten verzamelen. Met twee ID's kunt u maximaal 35 punten van één CAcert waarmerker krijgen. Zo hebt u minimaal twee waarmerkingen nodig om 50 Punten te halen.

Met minstens 100 Waarmerkingspunten en slagen voor de waarmerkers test (zie https://cats.cacert.org) kunt u onmiddellijk beginnen andere personen te waarmerken.
Als u een waarmerking hebt uitgevoerd voordat u zich bij CAcert hebt aangemeld, maak dan alsnog zo spoedig mogelijk uw CAcert account aan en geef dit door aan uw waarmerker.

Terug thuis
Installeer uw CAcert certificaat in uw browser, e-mail programma, code-signing, time-stamping van documenten, etc. en start met het gebruik van certificaten in uw e-mail, teken uw server-software, enz. En… haal het basis CAcert Certificaat (zie www.cacert.org Web-pagina) op voor in uw browser en uw systeem.
Of nog beter: begin om het CAcert Web van Vertrouwen te vergroten, het gebruik van digitale certificaten aan te moedigen en begin andere gebruikers te helpen en... ondersteun de CAcert gemeenschap.

Ondertekening met een PGP key
U kan ook PGP public keys uitwisselen. CAcert waarmerkers zijn bereid ook uw PGP sleutel te ondertekenen.

Organisaties
Als u een organisatie bent, kunt u uw organisatie op certificaten krijgen. U hebt een bewijs nodig van de legale status van de organisatie (uitreksel van KvK) en laat de aanvraag ondertekenen door een persoon, die tekenbevoegdheid is voor uw organisatie. Het CAcert programma van organisatie waarmerkingsformulier kan hiervoor gebruikt worden.

Na de organisatie waarmerking kunt u certificaten uitgeven via uw systeembeheerder (een CAcert waarmerker), en al uw domeincertificaten vrij aanmaken.

Meer informatie nodig?
Alle instructies voor CAcert certificaten zijn beschikbaar op de website www.cacert.org. Aarzel niet om uw vragen te stellen, b.v. via de ondersteunings e-maillijst: cacert-support@lists.cacert.org.

Bezoek de http://wiki.cacert.org/ wiki pagina's of de Nederlandse website http://www.cacert.nl/

Met dank voor uw gebruik van CAcert!

Met dank voor uw steun voor dit initiatief!

 V2.3 sept 2009/pieter, june 2011