E-MAIL-VERSCHLÜSSELUNG BEI AMNESTY

Saarbrücken, 17.05.2014

Seit kurzem stellt die deutsche Sektion von Amnesty Mitgliedern, die ehrenamtlich für Amnesty aktiv sind, **kostenlose digitale Zertifikate von CAcert** zur Verfügung. Wenn Ihr ein digitales Zertifikat haben wollt, lest bitte zunächst die nachfolgenden Hinweise, um zu verstehen, was ein digitales Zertifikat ist, wofür man es braucht, und was zu tun ist, um es zu bekommen und zu nutzen.

WAS IST EIN ZERTIFIKAT?

Ein digitales Zertifikat wird in der elektronischen Kommunikation verwendet, um die **Integrität** und **Authentizität** des übertragenen Inhalts zu bestätigen, und/oder um die **Vertraulichkeit** der transportierten Inhalte zu gewährleisten.

Integrität bedeutet, daß der übertragene Inhalt bei Sender und Empfänger derselbe ist, er also nicht auf dem Transportweg manipuliert wurde. **Authentizität** bedeutet, daß der übertragene Inhalt von der Person stammt, die als Sender angegeben wurde. Zertifikate können also bestätigen, daß ein Inhalt (z. B. eine E-Mail, eine Webseite) so, wie der Empfänger sie erhält, auch vom Sender abgeschickt wurde (Integrität), und daß dieser Sender genau der ist, der er vorgibt zu sein (Authentizität).

Zertifikate können daneben auch verwendet werden, um die **Vertraulichkeit** des übertragenen Inhalt zu garantieren. Dazu wird der Inhalt mit dem Zertifikat des Senders und dem Zertifikat des Empfängers **verschlüsselt**. Der Inhalt kann dann von niemandem außer dem Sender und dem/den Empfänger(n) gelesen werden.

Amnesty verwendet Zertifikate von CAcert, einem Zertifikatsanbieter (auch Zertifizierungsstelle, Certificate Authority, kurz: CA, genannt), der ehrenamtlich organisiert ist und kostenlose Zertifikate für jedermann ausstellt. Als Organisation hat die deutsche Amnesty-Sektion ein besonderes Verfahren (die sog. Organisations-Assurance) bei CAcert durchlaufen, durch das uns erlaubt wird, selbst Zertifikate für unsere Mitglieder und Mitarbeiter auszustellen.

WICHTIG: Die Zertifikate dürfen nur für Amnesty-eigene Domains ausgestellt werden und dürfen auch nur im Rahmen Eurer Tätigkeit für Amnesty verwendet werden. Ihr könnt also keine Zertifikate zur Verwendung für berufliche oder private Zwecke von uns bekommen.

WOFÜR BRAUCHT MAN EIN ZERTIFIKAT?

Die soeben beschriebenen Funktionen eines digitalen Zertifikats können in der Kommunikation über offene Netze wie dem Internet sehr nützlich sein: Anders als beim (leitungsbasierten) Telefonnetz, wo der Inhalt über eine direkte Leitung zwischen Sender und Empfänger ausgetauscht wird, läuft die Übertragung im (paketbasierten) Internet üblicherweise über viele Zwischenstationen (Router, Proxies, Caches usw.). Auch wenn die Inhalte dem Telekommunikationsgeheimnis unterliegen und jede Kenntnisnahme oder Manipulation durch Dritte rechtlich grundsätzlich strikt verboten ist, sind Eingriffe in den Transportweg technisch sehr leicht möglich. Die Enthüllungen von Edward Snowden haben

AMNESTY INTERNATIONAL Sektion der Bundesrepublik Deutschland e. V.
Fachkommission Internet
Zinnowitzer Straße 8 . 10115 Berlin
T: +49 30 420248-0 . F: +49 30 420248-488 . E: fk-internet@amnesty.de . W: www.amnesty.de
SPENDENKONTO 80 90 100 . Bank für Sozialwirtschaft . BLZ 370 205 00

AMNESTY INTERNATIONAL

gezeigt, daß auch die Inhalte von E-Mails durch Nachrichtendienste in großem Stil überwacht werden. Gerade Menschenrechtsorganisationen liegen dabei offenbar im Fokus des Aufklärungsinteresses.[1]

Zudem kann etwa eine Absender-E-Mail-Adresse leicht gefälscht werden und der Empfänger auf diese Weise veranlaßt werden, eine interne Information an einen unbefugten Dritten herauszugeben, weil er glaubt, sie an einen Kollegen zu schicken.

Um eine Manipulation oder unbefugte Kenntnisnahme von Inhalten zu verhindern, werden Zertifikate verwendet.

Bei den Zertifikaten, die der Mitgliedschaft von der FK Internet angeboten werden, handelt es sich um **Client-Zertifikate**. Client-Zertifikate sind digitale Zertifikate, die jeweils von genau einer, im Zertifikat bezeichneten Einzelperson verwendet werden können, um die eigenen Inhalte zu schützen. Client-Zertifikate werden hauptsächlich beim E-Mail-Versand verwendet. Sie können dort zwei Funktionen erfüllen:

- Schutz vor **Manipulation**: Um diese Funktion zu erfüllen, wird das Client-Zertifikat als elektronische Signatur verwendet, d. h. die E-Mail wird mit dem Zertifikat „unterschrieben". Da der zur Überprüfung des Zertifikats notwendige Teil öffentlich ist (ein Zertifikat setzt sich zusammen aus einem privaten - nur dem Zertifikatsinhaber bekannten - und einem öffentlichen - allen bekannten - Schlüssel), kann im Grunde jeder die **Integrität** und **Authentizität** einer so signierten E-Mail überprüfen. Anders als bei der Verschlüsselung (dazu sogleich) muß der Empfänger dabei selbst kein Zertifikat besitzen; er muß lediglich in der Lage sein, das Zertifikat des Senders zu überprüfen. Das ist heute mit jedem gängigen E-Mail-Programm (z. B. Thunderbird, Outlook, Evolution usw.) möglich.

- Schutz vor **unbefugter Kenntnisnahme**: In diesem Kontext werden die Client-Zertifikate von Sender und Empfänger verwendet, um die **Vertraulichkeit** einer E-Mail zu gewährleisten. Zu diesem Zweck wird der Inhalt mit dem privaten Schlüssel des Sender-Zertifikats und dem öffentlichen Schlüssel des Empfänger-Zertifikats **verschlüsselt**. Sowohl Sender als auch Empfänger müssen also ein Zertifikat besitzen, um die Verschlüsselungsfunktion nutzen zu können. Eine so verschlüsselte E-Mail kann von niemandem außer von Sender und Empfänger gelesen werden, da sie nur einen Haufen scheinbar sinnloser Zeichen enthält. Nur wenn der Empfänger die E-Mail mit seinem eigenen privaten Schlüssel und dem öffentlichen Schlüssel des Sender-Zertifikats wieder entschlüsselt, kann er die Zeichenansammlung wieder in den ursprünglichen Klartext verwandeln. Auch die Ver- und Entschlüsselung von E-Mails wird von allen heute gängigen E-Mail-Programmen beherrscht.

WIE BEKOMME ICH EIN DIGITALES ZERTIFIKAT?

Wenn Ihr ein digitales Zertifikat für Eure Tätigkeit für Amnesty nutzen wollt, könnt Ihr dieses mit Hilfe des im Intranet aufrufbaren **Antragsormulars** (https://intranet.amnesty.de/Antrag-S-MIME-Zertifikat.933.0.html) beantragen. Hinweise zum Ausfüllen des Formulars findet Ihr auf der Formularseite.

1 Siehe http://www.amnesty.org/en/for-media/press-releases/usauk-snowden-alleges-spy-agencies-have-targeted-human-rights-defenders-201.

WICHTIG: Jedes Client-Zertifikat muß einer E-Mail-Adresse zugewiesen sein. Diese E-Mail-Adresse darf durch **genau eine** Person genutzt werden, die im voraus bekannt sein muß und während der Laufzeit des Zertifikats **nicht verändert** werden darf. Nur wenn das gewährleistet ist, kann das Zertifikat seine Funktion, die Authentizität des Absenders zu bestätigen, erfüllen! Vorsicht daher bei reinen Funktions-E-Mail-Adressen wie info@amnesty-hintertupfing.de, bezirkssprecher@amnesty-niemandsland.de oder presse@amnesty-helgoland.de! Selbst wenn auf diese E-Mail-Adressen immer nur eine Person zur gleichen Zeit Zugriff hat: Bezirkssprecher, Pressesprecher oder IT-Administratoren können sich ändern, und wenn dann nicht sichergestellt ist, daß die E-Mail-Adresse mit dem neuen Namen verknüpft und das alte Zertifikat zurückgezogen wird, gilt der alte Funktionsträger weiterhin als Sender einer E-Mail unter dieser Adresse, auch wenn sie in Wirklichkeit vom neuen Funktionsträger versandt wurde. Dies kann auch rechtliche Auswirkungen haben, da das Zertifikat grundsätzlich auch Beweisfunktionen im Rechtsverkehr entfalten kann.

HINWEIS: Wir können Zertifikate nur für E-Mail-Adressen ausstellen, die in einer auf die deutsche Amnesty-Sektion registrierten Domain liegen. Das bedeutet, daß Ihr z. B. nicht Eure private GMX-/web.de-/Googlemail-Adresse oder die E-Mail-Adresse, die Ihr bei Eurem Arbeitgeber/Eurer Uni habt, angeben könnt, da wir für diese keine Zertifikate ausstellen dürfen. Nur E-Mail-Adressen, die Ihr in der Domain Eurer Gruppen-/Bezirkshomepage anlegt, können von uns ein Zertifikat erhalten. Gültige Adressen wären also z. B.: rolf.mueller@amnesty-wuerzburg.de oder beate_mayer@amnesty-saarbruecken.de.

Wir überprüfen Eure Angaben im Antragsformular, insbesondere durch einen Abgleich mit den Einträgen in der Mitgliederdatenbank. Wenn alles stimmt, erhaltet Ihr von uns eine E-Mail an die angegebene Adresse mit einer **verschlüsselten Datei**, die das beantragte **Zertifikat** enthält. Falls noch etwas unklar ist oder Informationen fehlen, melden wir uns natürlich bei Euch.

Die Zertifikatsdatei könnt Ihr entschlüsseln mit dem **Paßwort**, das sich zusammensetzt aus

- dem **ersten Teil** des Paßwortes, das Ihr auf der Bestätigungsseite nach Absenden des Antrags im Intranet angezeigt bekommen und Euch hoffentlich sicher notiert habt,
- dem **zweiten Teil** des Paßwortes, das Ihr per Post an die zu Eurer Person in der Amnesty-Mitgliederdatenbank eingetragenen Adresse geschickt bekommt.

Bitte gebt die beiden Teile des Paßwortes beim Installieren des Zertifikats (siehe dazu den folgenden Abschnitt „Wie nutze ich das Zertifikat?“) **unmittelbar hintereinander** ein, also ohne ein Leerzeichen oder ein sonstiges Zeichen dazwischen.

WIE NUTZE ICH DAS ZERTIFIKAT?

Wenn Ihr das gewünschte Zertifikat erhalten habt, könnt Ihr es sofort einsetzen. Dazu müßt Ihr es zuallererst in Eurem E-Mail-Programm (z. B. Thunderbird, Outlook, Windows Mail, Apple Mail o. ä.) installieren.

Wie das geht, erfahrt Ihr für eine Reihe gängiger E-Mail-Programme in den auf unserer Infoseite zu Zertifikaten (http://www.amnesty-intern.de/Zertifikate) verlinkten Tutorials.

EXKURS: WELCHE WEITEREN NUTZUNGSMÖGLICHKEITEN GIBT ES FÜR DIE ZERTIFIKATE?

Mit den CAcert-Zertifikaten lassen sich noch weitere Funktionen erfüllen, die aber nicht ganz so einfach zu realisieren sind bzw. in der Regel für die Amnesty-Arbeit nicht erforderlich sind. Wenn Ihr eine solche Funktion nutzen möchtet, könnt Ihr Euch aber gerne an uns wenden: fk-internet@amnesty.de.

- **Server-Zertifikate**: Diese Art von Zertifikaten wird insbesondere dazu verwendet, sichere Verbindungen zu Webservern anzubieten. Server-Zertifikate erfüllen dabei alle eingangs genannten Funktionen gleichzeitig: Sie bestätigen einerseits, daß der Webserver tatsächlich der ist, der er behauptet zu sein (Authentizität). Die übertragenen Inhalte können auch von niemandem auf dem Weg manipuliert werden, da dies zu einer fehlerhaften Checksumme führen und die Verbindung abgebrochen würde (Integrität). Schließlich wird die Verbindung zwischen dem Nutzer der Website und dem Webserver auch verschlüsselt; die übertragenen Inhalte werden so vor Kenntnisnahme durch Dritte geschützt (Vertraulichkeit). Es ist also lediglich erkennbar, daß mit der IP-Adresse des Nutzers eine Verbindung zur IP-Adresse des Webservers aufgebaut wird, aber nicht mehr, welche Inhalte (Webseiten) auf diesem Webserver der Nutzer ansieht und welche Inhalte (z. B. Formulardaten) er an den Webserver schickt. Ganz besonders nützlich ist diese Funktion dann, wenn die auf dem Webserver liegenden Daten nur einem bestimmten Personenkreis zugänglich sein sollen, wie das z. B. beim Amnesty-Intranet (https://intranet.amnesty.de) der Fall ist. Für das Amnesty-Intranet wird seit langem eine mit einem Server-Zertifikat gesicherte Verbindung verwendet. Mit den jetzt auch für Gruppen und Bezirke erhältlichen Server-Zertifikaten könnt Ihr z. B. in ähnlicher Weise „interne“ Bereiche auf Euren Gruppen- oder Bezirkshomepages einrichten und sicher sein, daß Ihr keine unerwünschten Mitleser habt.

  Wenn Ihr erwägt, ob Ihr ein solches Zertifikat braucht, denkt bitte daran: Viele Informationen, die Ihr aus dem Intranet oder auf anderem Wege vom SdS erhaltet, sind als „intern“ gekennzeichnet, d. h. sie dürfen nicht außerhalb der Mitgliedschaft weitergegeben werden. Personenbezogene Daten sind darüber hinaus schon allein wegen der geltenden Datenschutzgesetze vor Kenntnisnahme durch Dritte besonders zu sichern, sofern der Betroffene nicht explizit in die Veröffentlichung eingewilligt hat. Das gilt nicht nur für Daten von Dritten, z. B. Interessenten, Spendern, Hilfesuchenden (etwa Asylbewerbern, die in Eurer Asylsprechstunde waren) oder sonstigen Kontakten, sondern auch für Mitgliederdaten! Ein Server-Zertifikat, verbunden mit einem passwortgesicherten Bereich auf Eurer Website, ermöglicht es Euch, diese Daten dennoch „im Internet“ abzuspeichern und für den berechtigten Personenkreis verfügbar zu halten.

- **Secure single sign-on:** Client-Zertifikate können nicht nur dazu verwendet werden, E-Mails zu signieren oder zu verschlüsseln, sondern auch dazu, sich auf einer Website ohne Verwendung von Benutzername/Paßwort einzuloggen. Dazu muß das Client-Zertifikat in dem Browser installiert werden, mit dem auf die Website zugegriffen werden soll. Wird die Website aufgerufen, tauscht der Browser das Zertifikat mit der Website aus, die dadurch verifizieren kann, daß der Nutzer berechtigt ist, die gewünschte Seite anzusehen.

- **Programmcode signieren:** Wenn Ihr Programmcode geschrieben habt, könnt Ihr diesen mit einem Zertifikat signieren, sofern das Zertifikat diese Funktion vorsieht. Nutzer dieses Programmcodes können mit Hilfe des Zertifikats verifizieren, von wem der Code stammt.