

Henrik Koy, Bernhard Esslinger

TeleTrust European Bridge CA

Die European Bridge CA als Enabler für sichere E-Mail mit S/MIME zwischen Unternehmen und Behörden

Die Erfahrungen im praktischen Geschäftsleben zeigen, dass verschlüsselte Kommunikation viel häufiger benötigt wird als signierte Kommunikation. Im Gegensatz zur Signatur erfordert die Verschlüsselung, dass auf der Sender-Seite bereits vor dem Versenden der Empfänger-Schlüssel vorliegt. Der sichere Austausch vertraulicher E-Mails mit Geschäftspartnern stößt dabei immer wieder auf Probleme, weil der Verschlüsselungs-Schlüssel des Empfängers nicht vorliegt oder ihm nicht vertraut wird. Die TeleTrust European Bridge CA bietet dafür kostengünstige und praxistaugliche Lösungen.

Für den normalen E-Mail-Nutzer scheidet das spontane Versenden vertraulicher Inhalte oft bereits daran, dass sich Sender und Empfänger nicht auf eine gemeinsame Lösung für sichere E-Mail einigen können. Z. B. beginnt der Sender mit „Bitte senden Sie mir eine S/MIME¹-signierte E-Mail, damit ich Ihr Zertifikat erhalte“²;

¹ S/MIME (Secure Multipurpose Internet Mail Extensions) ist ein von der IETF schon 1995 (RFC1847) und 2004 (RFC3851) verabschiedeter Standard, der von allen gängigen E-Mail-Clients unterstützt wird und der das normale E-Mail-Format MIME erweitert.

² Bei einer S/MIME-signierten E-Mail wird meistens auch das Verschlüsselungs-Zertifikat mit angehängt. Die eLearning-Software Cryptool (<http://www.cryptool.org>) bietet eine visualisierte Beschreibung

diese Anfrage wird beim Empfänger nicht verstanden und er wendet sich an seinen IT-Support. Und es kann mit der Antwort enden „Für vertrauliche Inhalte bieten wir Ihnen ein Web-Portal, auf dem Sie sich bitte registrieren“.

Der Eindruck, dass sich bis heute kein Standard für sichere E-Mail durchgesetzt hat, wird durch eine Burton-Studie von 2008 bestätigt („Secure E-Mail: Still Too Many Choices“) [1]. Die Anzahl der – meist wenig interoperablen – Verfahren hat in den letzten Jahren sogar zugenommen. Neben den bekannten Lösungen zur Nachrichten-Verschlüsselung (S/MIME und PGP) sind Lösungen für die Transport-Verschlüsselung wie Virtual Private Networks (VPN) oder TLS gesicherte SMTP-Verbindungen (STARTTLS) im Einsatz. Zusätzlich drängen neue Verfahren auf den Markt, die vor dem Lesen der vertraulichen Nachricht eine Authentisierung des Empfängers erfordern. Dazu gehören Web-Portale, die vertrauliche Inhalte bereitstellen, oder Web-Portale, die den Entschlüsselungsschlüssel der empfangenen, verschlüsselten E-Mail bereithalten. Diese Entwicklung steht einer generellen Nutzung von sicherer E-Mail eher entgegen, als sie zu vereinfachen.

Für Unternehmen ist es sehr aufwändig, alle oben genannten Lösungen gleichzeitig zu unterstützen. Die Lösungen erfor-

dern verschiedene Ansätze für das Management der eigenen Benutzer und der Partner. Beispiele sind:

- PGP: Individuelles Vertrauensmanagement von externen PGP-Schlüsseln. Managen der PGP-Schlüssel von Mitarbeitern.
- S/MIME: Vertrauensmanagement von CA-Zertifikaten. Betrieb einer hauseigenen Public Key Infrastructure (PKI), oder Nutzen der Dienste eines Trustcenters.
- VPN / TLS: Konfigurationen auf Infrastruktur-Ebene.
- Web-Portale: Management von User-IDs und Passwörtern.

Je mehr unterschiedliche Lösungen genutzt werden, desto verwirrender wird die Benutzung für den E-Mail-Nutzer. Während VPN und TLS keine Interaktion beim Benutzer erfordert, muss er bei PGP und S/MIME Nachrichten ver- und entschlüsseln, während Web-Portale eine zusätzliche Authentisierung (z. B. Benutzername und Passwort) erfordern.

Unternehmen unterstützen deshalb oft nur die Lösungen die mit ihren Partnern die besten Aussichten auf Interoperabilität bieten, und versuchen, die restlichen Standards zu vermeiden, um die Komplexität für sichere E-Mail in Grenzen zu halten.

Im Fall, dass E-Mails zwischen Unternehmen und zwischen Unternehmen und Behörden verschlüsselt werden, kommt meist S/MIME zum Einsatz, da in diesem



Prof. Bernhard Esslinger

Professor Universität Siegen und Direktor Deutsche Bank AG, Vertreter der DB in

der EBCA

E-Mail: esslinger@fb5.uni-siegen.de



Henrik Koy

Kryptographie-Experte, dbPKI, Deutsche Bank AG

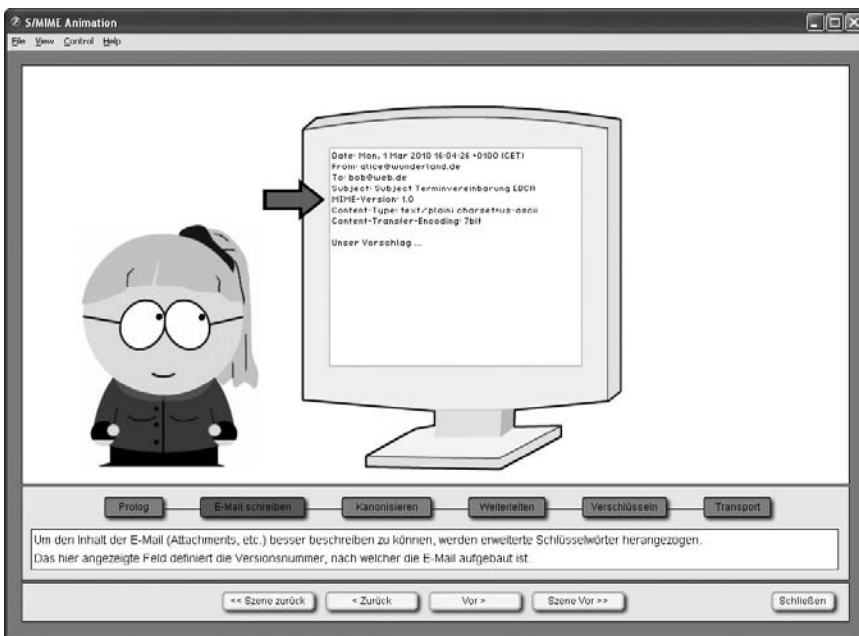
E-Mail: henrik.koy@db.com

bung des S/MIME-Protokolls. Siehe auch [Abb. 1] und [Abb. 2].

Abb. 1 | Verfassen einer S/MIME-E-Mail in CrypTool [6]



Abb. 2 | Visualisierung der S/MIME-Verschlüsselung in 6 Schritten [6]



Geschäfts-Szenario viele Partner bereits S/MIME unterstützen. Ein weiterer Grund ist, dass S/MIME X509-Zertifikate erfordert, die im Allgemeinen von PKIs aus Unternehmen oder von Trustcentern ausgestellt wurden. Dies erleichtert den Organisationen das Vertrauensmanagement.

Die TeleTrust European Bridge CA (<http://www.bridge-ca.org>) bietet für Organisationen, die S/MIME einsetzen wollen, Lösungen und hilft die notwendigen Verbesserungen umzusetzen. Große Unternehmen, wie Deutsche Bank und Siemens, aber auch Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind Teilnehmer der EBCA.

1 S/MIME für Unternehmen und Behörden

Untersucht man, welcher Standard sich für die Kommunikation zwischen Unternehmen (B2B) und zwischen Unternehmen und Behörden (B2G) am besten eignet, so finden sich starke Argumente für S/MIME:

- Nach der KES/Microsoft-Studie „Lagebericht zur Informationssicherheit“ von 2006 [2] unterstützten bereits 57% der befragten Institute S/MIME. Dieser Anteil nahm innerhalb von 2 Jahren sprunghaft zu, was einen Trend, hin zu S/MIME anzeigt.

- Die Mehrheit der befragten IT-Experten äußerte in der internationalen „Delphi-Studie 2030“ (Zukunft und Zukunftsfähigkeit der Informationstechnologien und Medien) von 2009 [3] die Einschätzung, dass sich bis 2030 durch „Digitale Zertifikate die E-Mail-Kommunikation zu einem rechtssicheren Kommunikationsstandard entwickelt hat“.
- Der Pilotversuch SPHINX [7] des BSI zeigte auf, dass eine gute Interoperabilität unterschiedlicher Hersteller erzielbar ist.
- Unternehmen und Behörden investieren in zentrale E-Mail-Gateway-Anwendungen, mit S/MIME-Verarbeitung als zentraler Komponente.
- Trustcenter bieten Public Key Infrastructure (PKI)-Lösungen an – zugeschnitten auf S/MIME.
- S/MIME wird von den gängigen E-Mail-Clients unterstützt (MS Outlook, Mozilla Thunderbird, Apple Mail, Lotus Notes).

Dieser positive Trend bestätigt sich auch anhand einer kürzlich durchgeführten Stichprobe von E-Mail-Zertifikaten bei der Gateway-Anwendung der Deutschen Bank. Dort haben sich S/MIME-Zertifikate von 978 unterschiedlichen E-Mail-Domänen angesammelt. Es wurden mindestens 27 unterschiedliche E-Mail-Gateways identifiziert.

Hieraus wird deutlich, dass Unternehmen, die sich für S/MIME entschieden haben, diesen Standard für B2B- und B2G-E-Mail-Kommunikation noch aktiver als bisher bei Ihren Partnern bewerben sollten, anstatt weiter eine hohe Heterogenität zuzulassen. Dafür sind gleichzeitig Maßnahmen notwendig, die für den E-Mail-Nutzer die immer noch bestehenden Hürden beim Versenden verschlüsselter S/MIME-E-Mails deutlich reduzieren.

2 Erfolgskriterien für S/MIME

Die folgende Analyse zeigt, dass Verbesserungen sowohl in der Awareness als auch im Schlüsselmanagement notwendig sind.

2.1 Awareness

„Eine ungeschützte E-Mail ist so offen wie eine Postkarte“. Dies ist ein gern genutzter Vergleich, um Awareness beim normalen E-Mail-Nutzer zu erzielen. Dabei wird oft vergessen, dass beim Nutzer ein Konflikt entsteht, wenn die E-Mail-Verschlüsse-

lung nicht reibungslos funktioniert. Awareness ist deshalb auch beim IT-Management notwendig. Für das reibungslose Funktionieren sind Aufgaben zentral in der IT und nicht beim Mitarbeiter vor Ort zu lösen. Z. B. sollte bei vertraulichen Geschäfts-E-Mails die sichere E-Mail-Lösung mit dem Geschäftspartner vorher abgestimmt und getestet sein.

2.2 Vertrauensmanagement

Viele Unternehmen, die S/MIME einsetzen, haben für Ihre E-Mail-Zertifikate³ eine hauseigene PKI bereitgestellt, die meist sowohl günstiger als auch besser integriert ist als dies beim Kauf von Zertifikaten öffentlicher Trustcenter der Fall wäre. Dies führt aber dazu, dass andere Organisationen solchen Zertifikaten für die Verschlüsselung und bei der Signatur-Validierung zunächst nicht vertrauen. Das gegenseitige Vertrauen dieser Zertifikate muss individuell administriert werden, was in der Regel eine Abstimmung mit dem PKI-Verantwortlichen und technische Tests erfordert. Auch Sicherheits-Prüfungen sind notwendig, da PKIs oft nur mit den Standard-Vorgaben des PKI-Herstellers betrieben werden. Es zeigt sich in der Praxis, dass diese Vorgaben nicht immer den Stand der Technik adressieren. Z. B. werden immer noch zu kurze Schlüssellängen (RSA 512 Bit) oder unsichere Hashfunktionen (MD5) verwendet.

Aber auch für Trustcenter-Zertifikate ist PKI-Vertrauensmanagement notwendig. Trustcenter verkaufen z. B. Zertifikate unter dem Namen „Digitale Zertifikate für sichere E-Mails“ als „Class 1“-Zertifikate bezeichnet. Das Trustcenter prüft bei der Registrierung lediglich die Existenz der angegebenen E-Mail-Domäne. Erst wenn man sich die Zertifikatsrichtlinien für „Class 1“-Zertifikate der Trustcenter genauer ansieht wird klar, dass Personendaten im Zertifikat ungeprüft sind⁴. Der Gebrauchswert solcher Zertifikate ist im Betrieb stark eingeschränkt. Abhängig von den Richtlinien in der eigenen Orga-

nisation kann man für solche Zertifikate das Vertrauen im besten Fall in Ausnahmefällen konfigurieren.

Für Zertifikate einer hauseigenen PKI wie auch für Trustcenter-Zertifikate ist individuelles Vertrauensmanagement notwendig, d.h. dass jedes Unternehmen für sich entscheidet, welcher CA es vertraut. Innerhalb einer PKI sollten E-Mail-Zertifikate von einer dedizierten Zertifizierungsstelle (Certification Authority, CA) ausgestellt werden, so dass sich die Prüfung auf diese CA beschränken lässt. Für einen E-Mail-Grundschutz sind die folgenden Fragen zu klären: Wer darf unter welchen Voraussetzungen ein Zertifikat erhalten, wie können Zertifikate und Sperrinformationen abgerufen werden, und wie erreiche ich einen PKI-Ansprechpartner. Eine CA sollte hier klare und verständliche Antworten bereitstellen.

2.3 Verteilung/Austausch von E-Mail-Zertifikaten

Der Austausch von S/MIME-Zertifikaten wird oft durch eine S/MIME-signierte E-Mail mit der Aufforderung „Bitte antworten Sie mit einer signierten E-Mail“ initiiert. Solange der Angesprochene nicht antwortet, kann der Sender die E-Mail mit vertraulichem Inhalt nicht verschlüsseln. Der als Standard vorgesehene Weg, Zertifikate im Internet über ein LDAP-Verzeichnis zur Verfügung zu stellen, stößt in der Praxis ebenfalls auf Probleme. Viele Unternehmen und Behörden sehen datenschutzrechtliche Probleme, Zertifikate ohne Einwilligung der Zertifikats-Halter zu veröffentlichen, oder scheuen die Investition, ein eigenes LDAP-Verzeichnis aufzubauen. Auf der anderen Seite werden LDAP-Verbindungen in vielen Infrastrukturen standardmäßig von der Firewall blockiert und die Freischaltung einzelner LDAP-Verbindungen erfordert administrativen Aufwand.

Diese Hürden werden oft als Hindernisgrund für die weitere Verbreitung von S/MIME genannt. Ansätze zu deren Lösung sorgen dafür, die Veröffentlichung von Zertifikaten zu erleichtern, die Anzahl der Zugangspunkte für Zertifikate zu verringern und die datenschutzrechtlichen Probleme zu adressieren.

2.4 Von PKI-Inseln zu vernetzten, föderativen Strukturen

Für sichere E-Mail ist der Betrieb einer hauseigenen PKI nur dann sinnvoll, wenn

den ausgestellten E-Mail-Zertifikaten von den Zertifikats-Nutzern (Sendern) vertraut wird, und wenn das jeweils aktuelle Zertifikat für die Benutzung zeitnah abrufbar ist. Diese Anforderungen werden in der Praxis zwischen der PKI und der Zertifikats-nutzenden Organisation bilateral abgestimmt. Die Aufgabe wird schwieriger, je größer die Anzahl der beteiligten PKIs und Zertifikats-Nutzer ist.

Notwendig sind deshalb übergreifende Vereinbarungen zwischen den PKI-Betreibern: Diese müssen einfach zu erfüllen sein, und sie müssen die Schutz-Anforderungen für den Geschäftsvorfall sichere E-Mail adressieren. Für alle Parteien sollten keine weiteren Hürden bestehen, E-Mail-Zertifikaten ihrer Kommunikationspartner zu vertrauen. Weiter erfordert es zentrale technische Lösungen, die die Abrufbarkeit von Zertifikaten unterstützen. Die drei oben genannten Erfolgskriterien lassen sich leichter gemeinsam in föderativen Strukturen umsetzen. Die European Bridge CA versteht ihre Aufgabe darin, diese Anforderungen zusammen mit ihren Teilnehmern zu adressieren und zu lösen.

3 S/MIME-Lösungen der European Bridge CA

Die TeleTrusT European Bridge CA (EBCA) wurde 2001 gegründet, um übergreifendes Vertrauen in die X.509-Zertifikate von Behörden und Unternehmen zu etablieren [4]. Träger der European Bridge CA ist der IT-Sicherheitsverband TeleTrusT Deutschland e.V. Die EBCA dient als Brücke zwischen den beteiligten Organisationen. Ziel ist es, den sicheren E-Mail-Austausch zu ermöglichen, ohne dass die Beteiligten untereinander Vereinbarungen treffen müssen. Der Kasten [Mitgliedsbeiträge] enthält einen Überblick über die Kosten einer Mitgliedschaft.

Die Teilnehmer der EBCA einigten sich auf einen Katalog von Anforderungen für den Betrieb einer PKI, die die Sicherheitsanforderungen, insbesondere für sichere E-Mail in Geschäftsprozessen, adressieren⁵. Teilnehmer bestätigen gegenüber der EBCA durch eine Selbsterklärung die Einhaltung dieser Anforderungen. Zusätzlich werden S/MIME-Interoperabilitätstests zwischen Teilnehmern durchgeführt.

Die Teilnehmer der TeleTrusT-EBCA treffen sich mehrmals im Jahr im Board

³ Ein E-Mail-Zertifikat enthält den von einer CA bestätigten öffentlichen Schlüssel des Zertifikats-Halters. Der Versender braucht für die E-Mail-Verschlüsselung den öffentlichen Schlüssel des Empfängers.

⁴ Siehe z. B. CPS rel. 3.8.1 von VeriSign: "The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate." [8]

⁵ Siehe <http://bridge-ca.org/html/teilnahme.html>

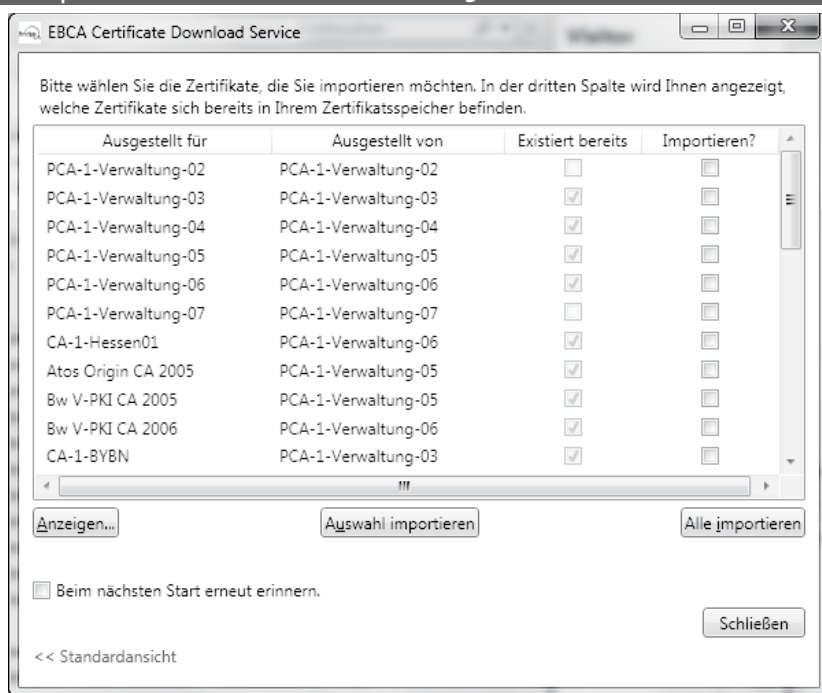
Tabelle 1 | Mitgliedsbeiträge für die EBCA

Der Jahresbeitrag für eine Teilnehmerorganisation wird nach deren Nutzerzahl (Mitarbeiterzertifikaten) erhoben. Es gilt folgende Staffelung:

Anzahl ausgestellter Zertifikate	Teilnehmerbeitrag pro Jahr
0-100	2.500 EUR
101-300	4.000 EUR
301-1.000	6.500 EUR
1.001-2.000	9.500 EUR
2.001-5.000	13.000 EUR
ab 5.001	17.500 EUR

In bestimmten Ausnahmefällen, z.B. für gemeinnützige Organisationen oder zeitliche begrenzte Nutzungen, kann der Teilnehmerbeitrag reduziert werden.

Abb. 3 | Mozilla Add-In für das Vertrauensmanagement von CA-Zertifikaten der EBCA



und in der AG-Technik, um neue Lösungen für das Vertrauensmanagement und die gegenseitige Verfügbarkeit von Zertifikaten zu entwickeln. Dabei ist die AG-Technik der EBCA auch offen für Nicht-Teilnehmer und Förderer aus der Industrie. Im Folgenden werden die EBCA-eigenen Lösungen vorgestellt.

3.1 Die EBCA-Zertifikatsrichtlinie als Rahmenwerk für einheitliche PKI-Richtlinien

Ein wesentlicher Baustein für das Vertrauen ist die nach außen transparente Darstellung des Betriebs der eigenen PKI und die zuverlässige Identifikation der Zertifikats-Halter. Die EBCA bietet ein Rahmenwerk für die Vergleichbarkeit der Prozes-

se und Richtlinien, wie eine PKI betrieben wird.

Für die Betriebs-Dokumentation einer PKI gilt der RFC3647 als ein international anerkanntes Rahmenwerk. Diese Struktur bezieht sich auf zwei Dokumente:

- Die Zertifikatsrichtlinie (Certificate Policy, CP) beschreibt Vorgaben, die von einer CA erfüllt werden müssen.
- Die Betriebsrichtlinien bei der Zertifikats-Ausstellung (Certification Practice Statement, CPS) beschreiben, wie die Vorgaben einer CP umgesetzt werden.

Die EBCA erstellte eine RFC3647-konforme Zertifikatsrichtlinie für Teilnehmer der EBCA, die die PKI-relevanten Beitrittsanforderungen im Rahmen dieser Richtlinie formuliert. Diese Richtlinie soll die Teilnehmer unterstützen, ihre eigenen PKI-Richtlinien konform nach RFC3647

zu erstellen, um so eine bessere Vergleichbarkeit bei allen PKI-Teilnehmern zu erzielen.

3.2 Identifikation der Zertifikats-Halter wichtig für das Vertrauen zwischen PKIs

Bevor ein CA-Zertifikat von den Herstellern in einen der verschiedenen Zertifikatsspeicher (in Betriebssystemen wie z. B. MS Windows, in Anwendungen wie z. B. Web-Browser, oder in Plattformen wie Java) eingebunden wird, muss die CA hohe Anforderungen an den sicheren eigenen Betrieb erfüllen. Die Einhaltung der Anforderungen muss über regelmäßige, unabhängige Audits nachgewiesen werden. Dies impliziert aber nicht, dass auch hohe Anforderungen an die Identifizierung der Zertifikats-Halter gestellt werden. Für Unternehmen ist aber gerade das Kriterium der Identifizierung entscheidend wichtig.

Teilnehmer der EBCA versichern, dass Zertifikats-Halter zuverlässig identifiziert werden. Der Charakter (z. B. Server-, Rollen-, Organisationszertifikate) solcher Zertifikate muss für die Empfänger eindeutig erkennbar sein. Zertifikate von EBCA-Teilnehmern bieten hier ein hohes Sicherheitsmerkmal.

3.3 Signierte CA-Liste

Die EBCA erstellt eine signierte Liste von CA-Zertifikaten der Teilnehmer, die die hohen Anforderungen des Betriebs und der Identifikation erfüllen. Diese Liste steht als PKCS#7-signierte Liste öffentlich zur Verfügung. Das PKCS#7-Format ermöglicht für Organisationen einen einfachen und erprobten Zugang zu den Zertifikaten. Die EBCA realisiert damit einen öffentlichen Zertifikatsspeicher, der die Sicherheitsanforderungen für Geschäftsprozesse erfüllt.

Für End-Benutzer ist der Import und das Vertrauen in CA-Zertifikate, die nicht bereits vorkonfiguriert sind, ein aufwändiger Vorgang. Das Institut für Internetsicherheit der Fachhochschule Gelsenkirchen [9] hat im Auftrag der EBCA und in Kooperation mit dem BSI ein neues Werkzeug zum Download und zur Installation von CA-Zertifikaten entwickelt, das die standardisierte CA-Liste der EBCA nutzt.

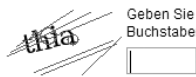
Über eine Management-Konsole können CA-Zertifikate individuell und sicher in den Schlüsselspeicher des E-Mail-Pro-

Abb. 4 | Öffentliches Abrufen von E-Mail-Zertifikaten


Öffentlicher Verzeichnisdienst für Zertifikate

Mit dem nachfolgenden Link können Sie aktuelle Nutzerzertifikate aus allen an der EB-CA angeschlossenen Verzeichnisdienste abfragen. [Verzeichnisdienstabfrage](#)

Geben Sie die links gezeigten Buchstaben in das Feld ein:



Um nach Zertifikaten zu suchen, geben Sie bitte eine vollständige und gültige eMail Adresse an.

 © 2009 Secardeo GmbH, Ismaning

gramms importiert werden. Durch die Signatur bleibt der Schutz der über diese Werkzeuge verteilten Zertifikate erhalten. Außerdem wird die automatische Aktualisierung der CA-Liste unterstützt:

- Für Mozilla Firefox und Mozilla Thunderbird wurde hierfür ein Add-In entwickelt [Abb. 3]. Benutzer werden benachrichtigt, wenn eine neue Version des Add-Ins verfügbar ist.
- Microsoft-Clients werden durch einen Plug-In-Agenten mit der Liste der aktuellen CA-Zertifikate versorgt. Der Agent prüft regelmäßig auf einem vorkonfigurierten Server nach einem Listen-Update und benachrichtigt den Benutzer über die Verfügbarkeit einer neuen Liste.

Diese Lösung ist neu für das Vertrauensmanagement von Zertifikaten, und könnte auch in anderen Szenarien wertvoll sein.

3.4 Bridge-LDAP

Für eine bessere Verfügbarkeit der E-Mail-Zertifikate der EBCA-Teilnehmer wurde der Bridge-LDAP-Service eingeführt. Ziel ist es, möglichst alle Verschlüsselungszertifikate der EBCA-Teilnehmer über eine einzige zentrale Adresse abrufbar zu machen. Der Abruf erfolgt über LDAP oder manuell über die EBCA-Webseite: https://www.bridge-ca.org/html/verz_dienst.html [Abb. 4].

Kern des Bridge-LDAP-Service ist die von der Firma Secardeo [5] entwickelte certBox Appliance. LDAP-Anfragen sind nur für vollqualifizierte E-Mail-Adressen zulässig. Der Bridge-LDAP besteht aus den folgenden drei Komponenten:

- *Certificate Proxy*: LDAP-Anfragen werden an dieser Schnittstelle angenommen und beantwortet.
- *Certificate Broker*: Die E-Mail-Domäne der LDAP-Anfrage wird ausgewertet und basierend auf frei konfigurierbaren Richtlinien erfolgt eine Anfrage an den richtigen LDAP-Server des EBCA-Teilnehmers.
- *Certificate Store*: EBCA-Teilnehmer ohne eigenes LDAP-Verzeichnis können ihre Zertifikate auf den Certificate Store der certBox hochladen. Dies ist eine kostengünstige Alternative gegenüber der Bereitstellung eines eigenen LDAP-Verzeichnisses.

Die Bridge-LDAP ist die Antwort der EB-CA, um die Verfügbarkeit von E-Mail-Zertifikaten zu verbessern.

3.5 Gelebter Erfahrungsaustausch

Zur TeleTrusT-EBCA gehören zwei Gruppen, die sich regelmäßig treffen: Im Board und in der Arbeitsgruppe Technik werden Probleme der PKI-Betreiber und PKI-Nutzer formuliert und gemeinsam Lösungen entwickelt. Diese Lösungen sind branchenübergreifend einsetzbar.

In den Sitzungen werden praktische Lösungen für die Teilnehmer erarbeitet. Diese Lösungen führen meist dazu, dass auch Nicht-Teilnehmer von den Lösungen profitieren können.

4 Fazit

Die EBCA arbeitet an praktischen Lösungen für die gegenseitige und organisationsübergreifende Nutzbarkeit von Zerti-

fikaten. Sind diese Lösungen vorhanden, funktioniert das eingangs geschilderte Szenario viel einfacher: Der Benutzer gibt wie in jeder E-Mail die Empfängeradresse ein und markiert sie zusätzlich als zu verschlüsseln – mehr muss er nicht tun. Die Schlüsselaustausch-Interaktion erfolgt automatisch und authentisch im Hintergrund. Am Beispiel S/MIME zeigt sich die Leistungsfähigkeit des EBCA-Modells. Ihre Lösungen führen zu föderativen Strukturen und einer enger werdenden Vernetzung von PKI-Inseln.

Die Teilnehmer der EBCA gehen hier „scheinbar“ in Vorleistung. Sie erleichtern ihren Geschäftspartnern das Vertrauensmanagement und ermöglichen ihnen den Zugang zu ihren Zertifikaten – auch wenn diese Geschäftspartner nicht Teilnehmer der EBCA sind. Doch man kann dies auch als einen Mehrwert betrachten: Der strategische Einsatz von Zertifikaten für die organisationsübergreifende sichere Kommunikation bei Geschäftsprozessen wird gefördert. Aus „Trittbrettfahrern“ werden Teilnehmer, wenn sie nicht nur fremde Zertifikate nutzen wollen, sondern auch wollen, dass ihren **eigenen** Zertifikaten ohne großen Aufwand vertraut wird.

Die TeleTrusT-EBCA als Brückenbildner zwischen PKI-Inseln wird mit jedem neuen Mitglied effizienter und der Nutzen steigt für alle PKI-Teilnehmer.

Literatur

- [1] Randall Gamby, „Secure E-Mail: Still Too Many Choices“, Burton Group, In-Depth Research Report, Version 2.0, Jun 13. 2008.
- [2] <kes>/Microsoft-Sicherheitsstudie, „Lagebericht zur Informationssicherheit“, <kes> 2006 #4/6
- [3] Internationale Delphi Studie 2030, „Zukunft und Zukunftsfähigkeit der Informations- und Kommunikationstechnologien und Medien“, Seite 93, 2009.
- [4] TeleTrusT European Bridge CA <http://www.bridge-ca.org>
- [5] Secardeo GmbH <http://www.secardeo.de/>
- [6] Kostenloses Kryptologie-Lernprogramm Cryptool, Version 1.4.30 <http://www.cryptool.org>
- [7] Pilotversuch Sphinx https://www.bsi.bund.de/DE/Themen/weitereThemen/VerwaltungsPKIVPKI/SPHINX/sphinx_node.html
- [8] VeriSign Certification Practice Statement, Version 3.8.1, Effective Date: February 01, 2009. http://www.verisign.com/repository/CPV3.8.1_final.pdf
- [9] Fachhochschule Gelsenkirchen, Institut für Internetsicherheit <https://www.internet-sicherheit.de>