Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

REFERENZELEMENT DKIM
DOKUMENTATION
VERSION 1.0, 27. NOVEMBER 2007

Thomas Zefferer – thomas.zefferer@iaik.tugraz.at

Zusammenfassung: Durch den ständig wachsenden Anteil von unerwünschten Emails (Spam) am gesamten Emailaufkommen ist die Entwicklung von geeigneten Gegenmaßnahmen unumgänglich. Daher wurde der von der IETF verabschiedete Standard „DomainKeys Identified Mail Signatures“, welcher der Bekämpfung von Spam und Phishing-Emails dienen soll, prototypisch umgesetzt. Auf diese Weise kann dessen Wirksamkeit beim Einsatz in der Praxis erprobt werden. Dieses Dokument beschreibt die umgesetzte Implementierung, unterstützt die BenutzerIn bei der Installation der entsprechenden Software und begleitet sie durch den nötigen Konfigurationsprozess um einen problemlosen Betrieb der Anwendung zu gewährleisten.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

DKIM-Proxy erlaubt es, durch Signieren von ausgehenden Emails deren Authentizität für Empfänger verifizierbar zu machen. Darüber hinaus können empfangene Emails auf deren Authentizität hin überprüft werden. Dieses Dokument unterstützt Sie bei der Installation und Inbetriebnahme der Software.
Der erste Abschnitt gibt eine kurze Einführung in das Thema der DomainKeys Identified Mail (DKIM) Signatures, auf dem die Funktionalität von DKIM-Proxy basiert. Der folgende Abschnitt beschreibt den Installationsprozess der Software Schritt für Schritt und unterstützt Sie bei der erfolgreichen Einrichtung der Anwendung auf Ihrem System. Der letzte Abschnitt widmet sich schließlich der Inbetriebnahme der Software und zeigt Ihnen, wie Sie die Funktionalität, die Ihnen dieses Programm bietet, nutzen können.

1.1 DomainKeys Identified Mail (DKIM) Signatures

In den letzten Jahren konnte weltweit eine massive Zunahme der Verbreitung von unerwünschten Emails (Spam) verzeichnet werden. Da das für die Übermittlung von Emails üblicherweise verwendete SMTP[1] Protokoll (RFC 2821) keine zufriedenstellenden Möglichkeiten zur Eindämmung dieses Problems bietet, werden laufend neue Verfahren erprobt, um dieser Problematik Herr zu werden. Unglücklicherweise konnte bislang noch keine geeignete Methode gefunden werden, um das Versenden von Spam gänzlich zu unterbinden. Alle bisher vorgebrachten Lösungsansätze erwiesen sich als unzulänglich oder brachten für die einzelne BenutzerIn auch beträchtliche Nachteile mit sich. Nichtsdestotrotz werden ständig neue Ansätze erarbeitet, um BenutzerInnen einen zuverlässigen Schutz vor Spam bieten zu können. Einer dieser Ansätze ist die Adaptierung eines der vielversprechendsten Vorschläge zur Eindämmung von Spam und Phishing-Emails, den von Yahoo! Inc. entwickelten DomainKeys. Die hinter diesem Namen steckende Methodik wurde von der IETF aufgegriffen, adaptiert und im Mai 2007 mit DomainKeys Identified Mail (DKIM) unter RFC 4871 als neuer Standard verabschiedet.

Mit DKIM soll vor allem das Fälschen der Absenderdomains von Emails unterbunden werden. Die Angabe einer falschen Absenderdomäne wird von Spammern üblicherweise dazu verwendet um die wahre Herkunft einer Email zu verschleiern. Da SMTP keine Möglichkeiten bietet um diese missbräuchliche Verwendung des Protokolls zu unterbinden, erweitert DKIM die Funktionalität des ursprünglichen Protokolls und erlaubt es, unter Verwendung von bekannten asymmetrischen Verschlüsselungsverfahren die angegebene Absenderdomäne einer Email zuverlässig zu authentifizieren. Dazu wird jede ausgehende Nachricht vom sendenden Mailserver mit dessen privatem Schlüssel elektronisch signiert. Der errechnete Signaturwert wird der Email zusammen mit anderen Informationen als zusätzliche Kopfzeile beigefügt und so an die EmpfängerIn übertragen. Diese kann die übermittelte Signatur mit Hilfe des öffentlichen Schlüssels des sendenden Mailservers verifizieren. Da die Signatur ausschließlich positiv verifiziert werden kann, wenn der entsprechende private Schlüssel zur Erstellung der Signatur verwendet wurde und dieser wiederum nur dem sendenden Mailserver bekannt ist, kann durch diese Methode die Absenderdomäne einer Email eindeutig authentifiziert werden.
Um das Protokoll einfach zu gestalten, verzichtet der DKIM-Standard auf eine aufwändige Public-Key Infrastruktur (PKI). Der Austausch des öffentlichen Schlüssels erfolgt über das DNS. In diesem sind die öffentlichen Schlüssel der am Protokoll beteiligten Mailserver als TXT-Resource-Records hinterlegt und können von der verifizierenden Partei durch einfache DNS-Lookups bezogen werden.

Abbildung 1 illustriert die Funktionsweise von DomainKeys Identified Mail.

[1] Simple Mail Transfer Protocol

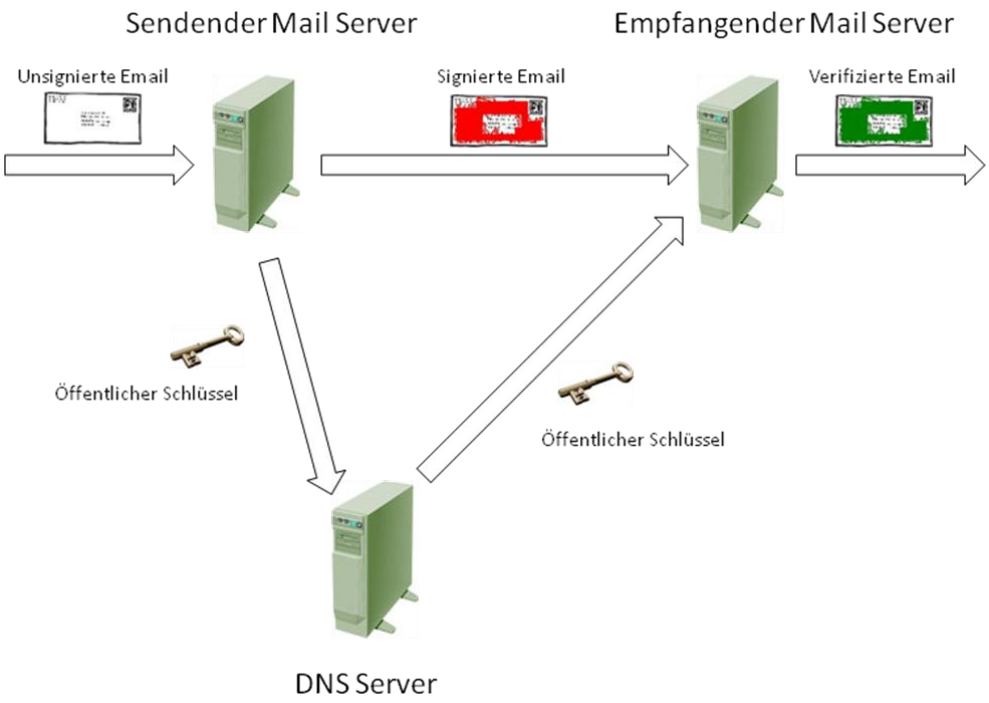

Abbildung 1 – Prinzip der DKIM Authentifizierung

1.2 DKIM-Proxy

DKIM-Proxy stellt eine Implementierung des DomainKeys Identified Mail Signatures Standards dar und setzt die, in dem Standard beschriebenen und definierten Konzepte prototypisch um. Wie der Name bereits suggeriert, ist diese Lösung als Proxy ausgeführt und kann so sehr einfach einem Email-Client (z.B. Mozilla Thunderbird, MS Outlook Express, etc..) vorgeschaltet werden. Dadurch ist es möglich, die bestehende Email-Infrastruktur um die durch den DKIM-Standard definierte Funktionalität zu erweitern, ohne umfangreiche Änderungen an bereits bestehenden Systemen durchführen zu müssen. Abbildung 2 illustriert den Einsatz von DKIM-Proxy. Die Proxy-Komponente kann dabei einfach am selben Rechner wie der Mail-Client installiert und betrieben werden.

Abbildung 2 – Implementierung des DKIM-Proxy

Der DKIM-Proxy übernimmt prinzipiell zwei Aufgaben. Sämtliche eingehende Emails, die vom Email-Client über POP3[2] oder IMAP4[3] empfangen werden, werden entsprechend dem DKIM-Standard verifiziert. Das Resultat der Verifizierung wird der Email als zusätzliche Kopfzeile mit dem Namen „X-DKIM-Proxy-Evaluation-Result“ beigefügt (Abbildung 3).

[2] POP3: Post Office Protocol Version 3
[3] IMAP4: Internet Message Access Protocol Version 4

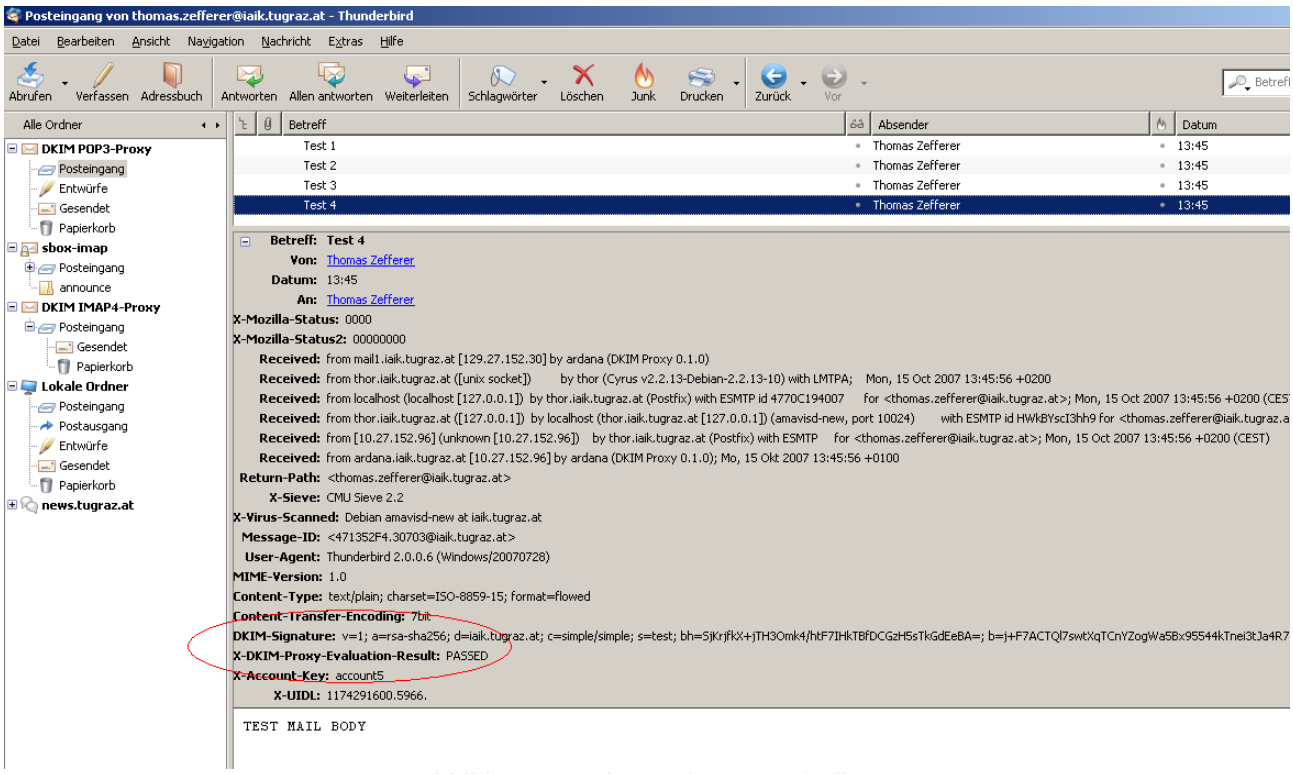

Abbildung 3 – Hinzugefügte Kopfzeilen

Prinzipiell gibt es drei mögliche Resultate:

- PASSED — Die DKIM Signatur der empfangenen Email wurde erfolgreich verifiziert
- FAILED - <Begründung> — Eine Signatur wurde gefunden, konnte aber nicht verifiziert werden. Falls vorhanden, wird die Begründung für das Scheitern der Verifikation ebenfalls angegeben.
- NOT SIGNED — Die empfangene Email ist nicht nach dem DKIM-Standard signiert

Dem Email-Client ist es dadurch möglich, unter Anwendung einer Filterfunktion sämtliche empfangenen Emails basierend auf dieser zusätzlichen Kopfzeile zu klassifizieren und geeignete Maßnahmen zu treffen. Abbildung 4 zeigt am Beispiel von Mozilla Thunderbird, wie eine derartige Filterfunktion im verwendeten Email Client erstellt werden kann.

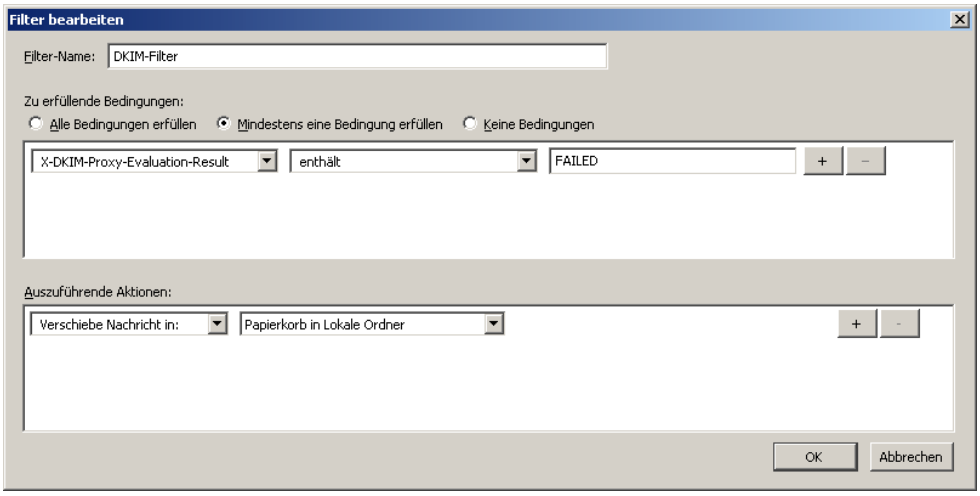

Abbildung 4 – Filter im Email-Client einrichten

Die zweite Aufgabe, welche DKIM Proxy übernimmt, ist das Signieren von Emails, die über SMTP vom verwendeten Email Client an den entsprechenden Email Server gesendet werden. Der ursprünglichen Email wird dabei entsprechend dem DKIM-Standard eine zusätzliche Kopfzeile (DKIM-Signature) mit der Signaturinformationen beigefügt (Abbildung 3). Der Empfänger kann diese Kopfzeile schließlich auswerten, die darin enthaltene Signatur verifizieren und so die Authentizität der Absenderdomain überprüfen.

2 Installation

Um DKIM-Proxy zu installieren, laden Sie bitte die notwendige Installationsdatei *dkim-proxy.msi* von der folgenden Internetseite herunter:

http://demo.a-sit.at/it_sicherheit/dkim_proxy/index.html

Nachdem Sie die Datei gespeichert und ausgeführt haben, erscheint ein Installationsdialog, der Sie durch den gesamten Installationsprozess leitet. Die einzelnen Schritte dieses Prozesses sind im Folgenden angeführt.

2.1 Starten der Installation

Nachdem das Installationsprogramm initialisiert ist, werden Sie mit folgendem Dialogfenster zur Installation von DKIM-Proxy begrüßt.

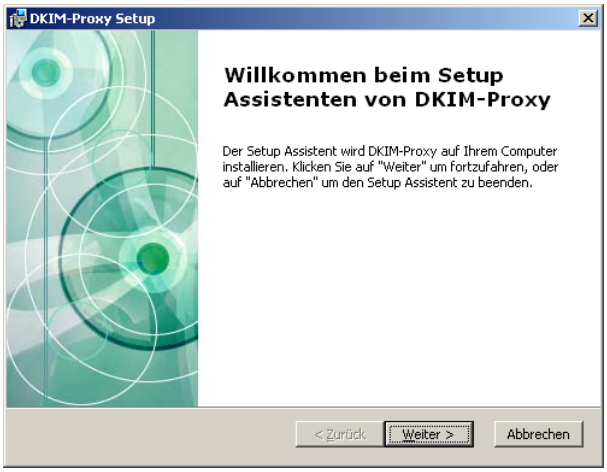

Abbildung 5 – Installation Schritt 1

Klicken Sie auf `Weiter` um den Installationsprozess zu starten.

2.2 Auswahl des Zielordners

Im nächsten Dialogfenster werden Sie aufgefordert den Ordner anzugeben, in den DKIM-Proxy installiert werden soll. Falls nicht anders gewünscht, können Sie ohne weiters den vorgeschlagenen Ordner verwenden.

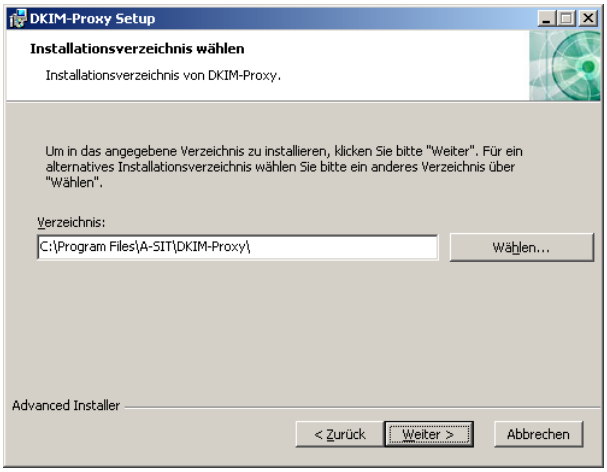

Abbildung 6 – Installation Schritt 2

Wenn Sie den bevorzugten Ordner ausgewählt haben, klicken Sie bitte auf `Weiter` um die Installation fortzusetzen.

2.3 Lizenzvereinbarung

In diesem Schritt werden Sie aufgefordert die Lizenzvereinbarung zu akzeptieren. Lesen Sie diese bitte sorgfältig durch und markieren Sie das Eingabefeld `Ich stimme der Lizenzvereinbarung zu` falls Sie mit den Vereinbarungen einverstanden sind.

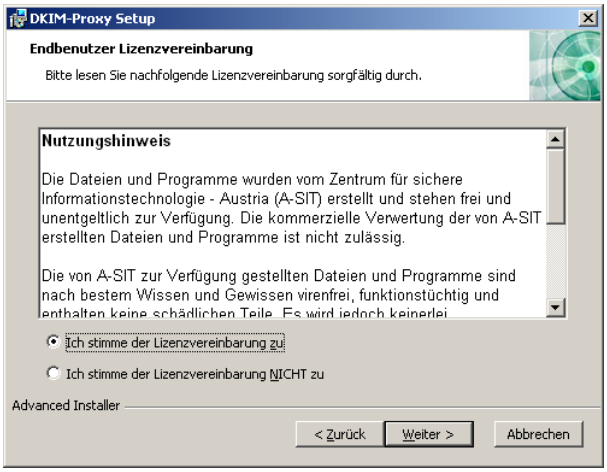

Abbildung 7 – Installation Schritt 3

Klicken Sie anschließend auf `Weiter` um den Installationsprozess fortzusetzen.

2.4 Bestätigen der Eingaben

In diesem Dialogfenster wird Ihnen mitgeteilt, dass alle benötigten Installationsparameter vorhanden sind und mit der Installation der Anwendung begonnen werden kann. Durch Betätigen der `Installieren` Schaltfläche können Sie die Installation starten.

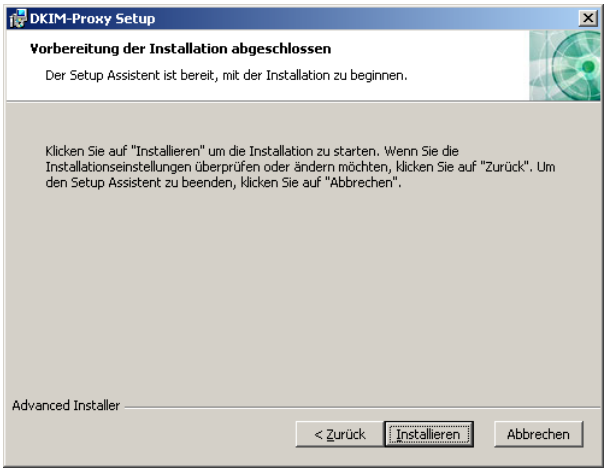

Abbildung 8 – Installation Schritt 4

2.5 Installieren der Anwendung

Die Installation selbst läuft vollkommen automatisiert ab. Da das Kopieren der benötigten Dateien eine gewisse Zeit in Anspruch nimmt, werden Sie über den aktuellen Installationsfortschritt ständig am Laufenden gehalten.

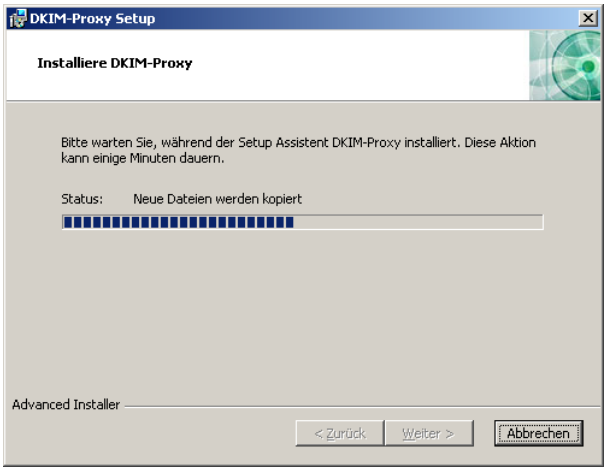

Abbildung 9 – Installation Schritt 5

2.6 Beenden der Installation

Nachdem alle Dateien kopiert, sowie die nötigen Verknüpfungen erstellt wurden, können Sie das Installationsprogramm durch Betätigen der `Fertigstellen` Schaltfläche abschließen. DKIM-Proxy ist nun auf Ihrem System installiert. In Ihrem Startmenü wurde unter `Programme` ein Ordner `DKIM-Proxy` angelegt, über den Sie die einzelnen Module der Anwendung schließlich starten können.

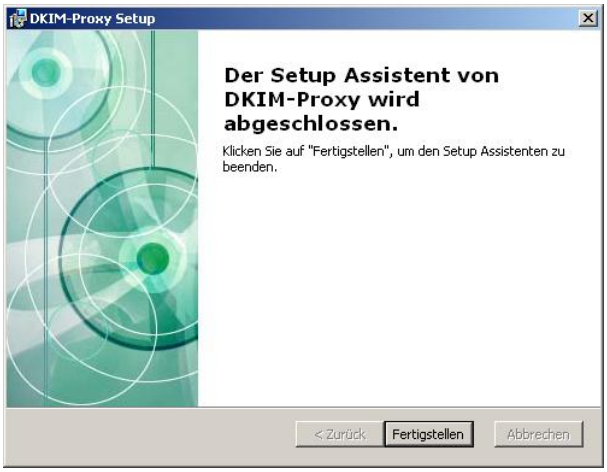

Abbildung 10 – Installation Schritt 6

3 Inbetriebnahme

3.1 Generieren der Schlüssel

Wie in Abschnitt 1 erläutert, greift das durch den DKIM-Standard definierte Signaturverfahren auf ein Schlüsselpaar, bestehend aus einem geheimen (privaten) und einem öffentlichen Schlüssel zurück. DKIM-Proxy bietet daher die Möglichkeit, ein solches Schlüsselpaar zu generieren. Die Erstellung der Schlüssel kann mit dem Programmmenüeintrag `RSA Schlüsselpaar erstellen` gestartet werden. Nach erfolgreicher Generierung der Schlüssel beendet sich das Programm wieder von selbst. Im Ordner, in den Sie DKIM-Proxy installiert haben, finden Sie daraufhin einen Unterordner `keys`, der zwei Dateien enthält.

- `private_key.private`: Dies ist eine passwortgeschützte Datei, die Ihren geheimen privaten Schlüssel enthält. Dieser Schlüssel wird benötigt, um ausgehende Emails zu signieren.

- `public_key.txt`: Diese Datei enthält den zu Ihrem privaten Schlüssel gehörenden öffentlichen Schlüssel in Base64-Codierung. Um von Ihnen signierte Emails verifizieren zu können, müssen die Empfänger über DNS[4] auf diesen Schlüssel zugreifen können. Sorgen Sie bitte dafür, dass dieser Schlüssel in Ihrem DNS Server als TXT-Resource-Record unter einem frei wählbaren Selector bereitgestellt wird. Dabei sind die durch den DKIM-Standard vorgegebenen Standards einzuhalten:

  - Der Schlüssel muss in der Subdomäne `_domainkey` abgelegt werden. Zum Beispiel muss für die Domäne `example.com` und einen gewählten Selector `foo.bar` der Schlüssel für einen DNS Lookup unter `foo.bar._domainkey.example.com` abrufbar sein.
  - Der im Resource Record abgelegte Text muss folgender Syntax folgen:
    `v=DKIM1\; k=rsa\; p=<pub_key>`
    Dabei ist `<pub_key>` durch die Base64 Repräsentation des öffentlichen Schlüssels, welche aus der generierten Datei `public_key.txt` entnommen werden kann, zu ersetzten.

In der Regel werden mehrere Email-Clients von der selben Domäne aus ihre Emails versenden. Da alle Clients hierfür dasselbe Schlüsselpaar verwenden, muss die Schüsselgenerierung nur einmal durchgeführt werden. Allen anderen Clients kann der benötigte private Schlüssel dann durch Kopieren der entsprechenden Datei in den Ordner `keys` zugänglich gemacht werden.

3.2 Ändern der Konfiguration

Nachdem DKIM-Proxy mit dem notwendigen privaten Schlüssel ausgestattet worden ist, müssen Sie noch einige grundlegende Konfigurationen vornehmen, bevor DKIM-Proxy schlussendlich verwendet werden kann. Nachdem Sie den Konfigurationseditor über den Programmmenüeintrag

[4] DNS: Domain Name System

`Kofigurations-Editor` gestartet haben, öffnet sich ein Fenster, in dem Sie den Proxy für einzelne Protokolle aktivieren, bzw. die Namen oder IP-Adressen der verwendeten Mailserver angeben können. Abbildung 11 zeigt die Benutzerschnittstelle, über die Sie Ihre Konfiguration festlegen können. Falls Sie einen Proxy durch markieren der entsprechenden `Proxy aktiv` Schaltfläche aktivieren, achten Sie bitte darauf, dass auch alle übrigen Angaben zu diesem Protokoll korrekt sind. Tragen Sie bitte unbedingt Ihre Absenderdomäne, und den korrekten „Selector“, unter dem ihr eigener öffentlicher Schlüssel im DNS abgelegt ist, ein. Diese Information muss Emails, die von Ihnen signiert werden, beigefügt werden, um es dem Empfänger zu ermöglichen, Ihren öffentlichen Schlüssel zu beziehen.

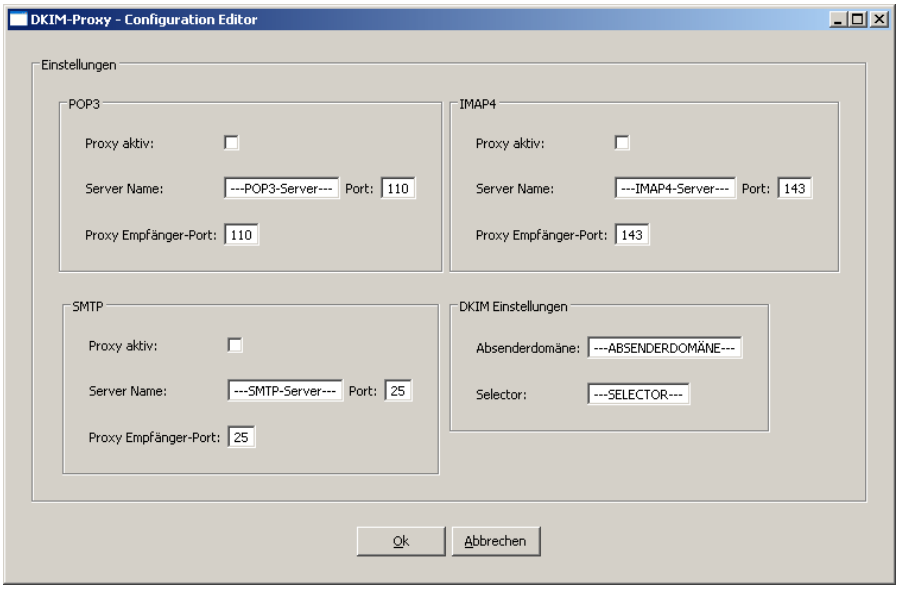

Abbildung 11 - Konfigurationseditor

Nachdem Sie alle Einträge vollständig konfiguriert haben, ändern Sie die Einstellungen Ihres Email-Clients derart, dass Sie als Mailserver (SMTP, POP3, IMAP4) nun den Rechner, auf dem DKIM-Proxy installiert ist, angeben. Dabei kann entweder dessen IP-Adresse, der Rechnername, oder einfach „localhost“ angegeben werden, falls DKIM-Proxy am lokalen System installiert wurde. Emails werden dann statt an den Mailserver, an DKIM-Proxy gesendet, welcher die Email signiert und schließlich an den tatsächlichen Mailserver weiterleitet. Dementsprechend werden empfangene Emails über DKIM-Proxy umgeleitet, wo diese verifiziert werden.

Achtung: Falls Sie Emails über IMAP4 von Ihrem Mailserver beziehen, konfigurieren Sie Ihren Mailclient so, dass immer eine Kopie der Email vom Server bezogen und lokal auf Ihrem System gespeichert wird. Andernfalls kann es abhängig vom verwendeten Email-Client und aufgrund der Eigenschaften des IMAP4-Protokolls vorkommen, dass das Resultat von durchgeführten Verifikationen der betreffenden Email nicht beigefügt werden kann.

Haben Sie alle Konfigurationen vorgenommen, können Sie DKIM-Proxy starten. Bitte beachten Sie, dass nach erfolgtem Start der Anwendung jede weitere Änderung der Konfiguration erst mit einem Neustart von DKIM-Proxy wirksam wird.

3.3 Starten und Beenden von DKIM-Proxy

Nachdem Sie das Schlüsselpaar erstellt, bzw. den privaten Schlüssel in den Ordner `keys` kopiert haben, können Sie DKIM-Proxy starten. Dazu wählen sie im Programmmenü den Eintrag `DKIM-Proxy` aus. Daraufhin erscheint in Ihrer Systemleiste ein Icon, das Ihnen anzeigt, dass DKIM-Proxy läuft. Sie können nun Emails über DKIM-Proxy senden und empfangen.

Abbildung 12 – DKIM-Proxy in der Systemleiste

Eine Aufzeichnung der durchgeführten Signaturprüfungen können Sie im Unterordner `stats`, welcher sich in Ihrem Programmordner befindet, einsehen.

Um DKIM-Proxy zu beenden, klicken Sie mit der rechten Maustaste auf das entsprechende Systemleisten-Icon und wählen Sie im erscheinenden Menü `DKIM-Proxy beenden`. Daraufhin wird DKIM-Proxy heruntergefahren und beendet.

4 Entfernen von DKIM-Proxy

Möchten Sie DKIM-Proxy von Ihrem System entfernen, wählen Sie bitte im Programmmenüeintrag von DKIM-Proxy die Option `DKIM_Proxy deinstallieren` aus. Nachdem Sie den Wunsch, die Anwendung von Ihrem System zu entfernen, bestätigt haben, wird DKIM-Proxy automatisch entfernt. In der Regel werden die Ordner, in denen sich die von DKIM-Proxy verwendeten Schlüssel sowie die Log- und Statistikdateien befinden, nicht gelöscht. Falls Sie diese Daten nicht mehr benötigen, entfernen Sie diese Verzeichnisse bitte manuell.

Historie

Version	Datum	Kommentar
0.1	15.10.2007	Erste Fassung
Ersteller		
Thomas Zefferer		
Version	**Datum**	**Kommentar**
0.2	23.10.2007	Überarbeitung Abschnitt 3.2
Ersteller		
Thomas Zefferer		
Version	**Datum**	**Kommentar**
0.3	24.10.2007	Überarbeitung Abschnitt 3.2
Ersteller		
Thomas Zefferer		
Version	**Datum**	**Kommentar**
1.0	27.11.2007	Erweiterung und Korrekturen
Ersteller		
Thomas Zefferer		