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

PROJEKTBERICHT - REFERENZELEMENT DKIM
DOMAINKEYS IDENTIFIED MAIL (DKIM) SIGNATURES
VERSION 1.0, 28. NOVEMBER 2007

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

Zusammenfassung: Mit der steigenden Bedeutung von Email als Kommunikationsmedium sowohl für private AnwenderInnen als auch für Unternehmen, verzeichnete zugleich auch die Verbreitung von Spam ein enormes Wachstum. Aktuellen Schätzungen zufolge sind unerwünschte Spam-Emails aktuell bereits für bis zu 80% des gesamten Emailaufkommens verantwortlich und verursachen neben einer Belästigung der AnwenderInnen für Unternehmen darüber hinaus auch zunehmend finanzielle Mehrkosten.
Um diesem Trend entgegenzusteuern, wurde von der IETF mit DomainKeys Identified Mail Signatures ein neuer Standard definiert, welcher als weiteres Mittel im Kampf gegen die Verbreitung von Spam zum Einsatz kommen soll. Das Projekt „Referenzelement DKIM“ hatte zum Ziel diesen Standard zu analysieren, in einer Referenzimplementierung umzusetzen und einer Evaluierung in einer entsprechenden Testumgebung zu unterziehen.
Eine Analyse der erhaltenen Evaluierungsergebnisse zeigte, dass der Standard bislang erst eine geringe Verbreitung gefunden hat, wodurch dessen Potential – das Lösen einiger Teilprobleme der Spam-Problematik – derzeit noch nicht voll ausgeschöpft werden kann.

Inhaltsverzeichnis

Abbildungsverzeichnis

Executive Summary

Um einen möglichst tiefgehenden Einblick in den zu untersuchenden DKIM-Standard zu erlangen und einen größtmöglichen Nutzen aus der Durchführung des Projekts zu ziehen, wurden bereits im Vorfeld folgende Projektinhalte als zu erreichende Ziele definiert und im Projektantrag festgelegt.

a) Analyse von DKIM
b) Erstellen und Bewerten von Architekturoptionen (Vergleich Proxy-Ansatz mit vollständigem Mail-Exchanger)
c) Umsetzung des Referenzmoduls
d) Piloteinsatz in A-SIT und TU-Graz Umgebungen - Bewertung der Strategien
e) Bereitstellung am A-SIT – Demoserver

Eine detaillierte Analyse des DKIM-Standards wurde am Beginn des Projekts durchgeführt. Abschnitt 2.1 fasst die aus dieser Analyse erhaltenen Ergebnisse zusammen und stellt die Funktionsweise von DKIM vor. Durch die ausführliche Untersuchung des Standards konnten dessen für eine effiziente Implementierung relevanten Besonderheiten sowie Vorteile, die sich aus der Verwendung von DKIM für AnwenderInnen und Unternehmen ergeben, herausgearbeitet werden.

Basierend auf den durch die Analyse des Standards erhaltenen Erkenntnissen, wurde ein Proxy-Ansatz als zweckdienlichste Architekturoption befunden. Die für diese Entscheidung ausschlaggebenden Argumente werden in Abschnitt 2.2 erläutert. Des Weiteren wird in diesem Abschnitt illustriert, wie sich die aus dem gewählten Architekturansatz ergebende Referenzimplementierung in bestehende Email-Infrastruktursysteme integrieren lässt.

Dem gewählten Architekturansatz zugrundeliegend wurde daraufhin das Referenzelement DKIM implementiert. In Abschnitt 3 werden zunächst die Teilmodule, aus welchen die erstellte Referenzimplementierung besteht, vorgestellt und schließlich die Funktionalität, welche durch diese Module umgesetzt wird, beschrieben.

Die entwickelte Referenzimplementierung wurde schließlich in einer entsprechenden Testumgebung installiert, um den Einsatz des DKIM-Standards und die sich für eine BenutzerIn dadurch ergebenden Vorteile in der Praxis untersuchen zu können. In Abschnitt 4 sind die Erkenntnisse, die aus diesem Piloteinsatz des Referenzelements resultierten, zusammengefasst. Des Weiteren werden in diesem Abschnitt relevante Schlussfolgerungen, welche aus der Evaluierung des DKIM-Standards in der Praxis gezogen werden konnten, erläutert.

Das in diesem Projekt erstellte Referenzelement inklusive einer zugehörigen Dokumentation, die eine Beschreibung der implementierten Software sowie Hilfestellungen zur Installation und Inbetriebnahme derselben enthält, kann unter folgender URL bezogen werden:

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

Die entsprechend der gewählten Architekturoption in Form eines Email-Proxys entwickelte Referenzimplementierung des DKIM-Standards erlaubt es diesen am lokalen System zu testen, auch wenn der verwendete Email-Server selbst DKIM nicht beherrscht. Dadurch kann das Konzept von DKIM von AnwenderInnen kennengelernt werden, ohne dass diese aufwändige Änderungen an einer bereits bestehenden Email-Infrastruktur vornehmen müssen.

1 Einleitung

Seit seinen Anfängen erfreute sich das Internet durchgehend einer rasch wachsenden Anzahl an BenutzerInnen, sodass Studien zufolge heute bereits weltweit mehr als 1,2 Milliarden Menschen das Internet als Kommunikations- und Informationsmedium benutzen. In Europa ist der prozentuale Anteil der InternetnutzerInnen gemessen an der Gesamtbevölkerung noch höher und beträgt bereits über 41%. Dabei wird das Internet neben Privatpersonen vor allem auch von der Wirtschaft genutzt und stellt für diese ein Medium zunehmender Bedeutung dar. Die folgenden Graphiken verdeutlichen die aktuellen Statistiken über die Nutzung des Internets (Quelle: [Ref01]).

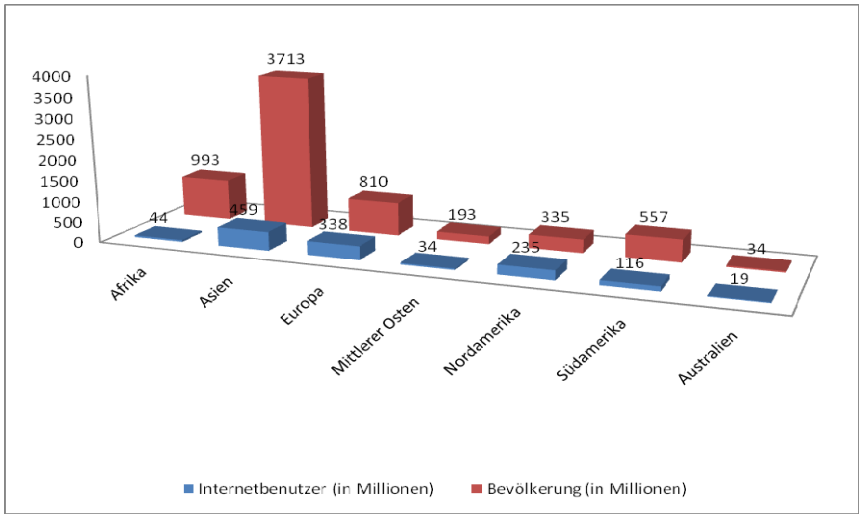

Abbildung 1 – Anzahl der Internetnutzer in Relation zur Bevölkerungszahl

Zieht man die Tatsache in Betracht, dass in Nordamerika bereits über 70% der Bevölkerung das Internet benutzen, so ist wohl auch in Europa und anderen Teilen der Welt mit einem weiteren Anstieg der Benutzerzahlen zu rechnen.
Österreich ist mit einem Anteil von 56,6% InternetnutzerInnen an der Gesamtbevölkerung im Vergleich mit den anderen EU-Ländern im guten Mittelfeld (Quelle: [Ref01]). Allerdings ist auch hier noch mit einem weiteren Anstieg an aktiven BenutzernInnen und einer daraus folgenden Zunahme der Bedeutung des Internets zu rechnen.
Zu einer der beliebtesten Anwendungen des Internets zählt zweifelsohne der Versand von Emails. Das Emailaufkommen ist wie das Internet selbst enorm gewachsen und stellt heute einen beträchtlichen Teil des gesamten über das Internet transportierten Datenvolumens dar. So wurden Schätzungen zufolge im vergangen Jahr täglich mehr als 35 Mrd. Emails versendet. Mit der zu erwartenden weiteren Verbreitung des Internets ist vorhersehbar, dass auch diese bereits jetzt enorm hohe Zahl noch weiter ansteigen wird. Durch dessen ungeheuere Beliebtheit hat sich Email auch in vielen Bereichen der Wirtschaft zu einem der wichtigsten Kommunikationsmedien entwickelt. Ausschlaggebend für den Erfolg von Email-Services sind unter anderem Geschwindigkeits- und Kostenargumente, sowie deren relativ einfache Handhabbarkeit.
Leider sind dies auch Gründe, die subversive Elemente der Gesellschaft dazu bewegen, Email-Infrastruktursysteme für ihre Zwecke zu missbrauchen. Das Versenden großer Mengen an unerwünschten Emails (z.B. mit Werbeinhalten) an eine möglichst große Zahl an EmpfängerInnen ist üblicherweise als Spam- Bulk- oder Junk-Email bekannt und konnte in den letzten Jahren ebenfalls ein enormes Wachstum aufweisen. Die folgenden Abbildungen illustrieren die ernorme Zunahme an Spam-Emails im Verhältnis zu erwünschten Emails (Quelle: [Ref06]) während der letzen Jahre. Da es schwierig bis unmöglich ist, absolute Zahlen über die Menge der weltweit versendeten Emails zu berechnen, beruhen diese Angaben auf Schätzungen. Nichtsdestotrotz ist die besorgniserregende Zunahme an unerwünschten Emails am gesamten Emailaufkommen unübersehbar.

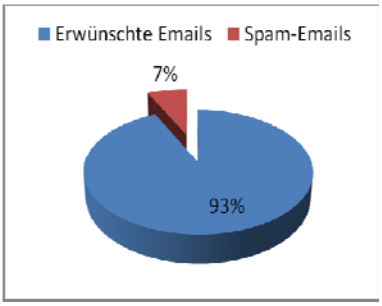

Abbildung 2 – Spam-Anteil im Jahr 2001

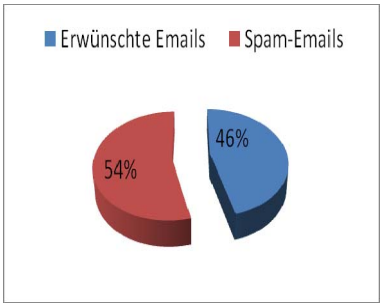

Abbildung 3 – Spam-Anteil im Jahr 2004

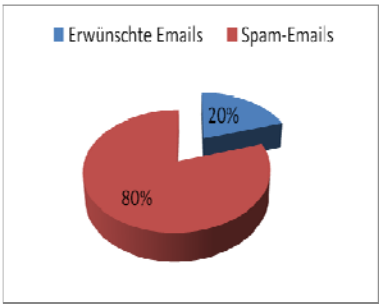

Abbildung 4 – Spam-Anteil im Jahr 2007

Was auf den ersten Blick nach einer lästigen, aber ungefährlichen Nebenerscheinung von Email-Systemen klingt, birgt bei genauerer Betrachtung doch Gefahren, die durchaus auch zu finanziellen Schäden führen können. In Anbetracht der Tatsache, dass schätzungsweise bis zu 80% der weltweit versendeten Emails als Spam einzustufen sind, wird klar, dass alleine die Verarbeitung dieser Unmengen von unerwünschten Daten für Unternehmen zu erheblichen finanziellen Mehrkosten führen kann. So errechnete eine Studie, dass Spam alleine in den USA jährlichen einen Schaden von rund 22 Mrd. US-Dollar anrichtet [Ref02]. Eine weitere finanzielle Bedrohung stellen sogenannte Phishing-Emails, die als Unterordnung von Spam-Emails gelten, dar. Diese Nachrichten enthalten üblicherweise einen Link zu einer gefälschten Web-Seite, auf welcher die BenutzerIn aufgefordert wird geheime Daten wie zum Beispiel Passwörter einzugeben. Können einer leichtgläubigen BenutzerIn auf diese Weise beispielsweise die Zugangsdaten zu deren e-banking Konto entlockt werden, kann dies zu einer massiven finanziellen Schädigung der AnwenderIn führen. Gleichzeitig wird dadurch das Vertrauen der Kundin in das Unternehmen – in diesem Fall die Bank – erschüttert, wodurch auch für dieses Nachteile entstehen.
Um BenutzerInnen des Internets vor solchen Schäden zu schützen, ist es daher unbedingt notwendig, die Verbreitung von Spam und Phishing-Emails so weit wie möglich einzudämmen. Leider verhindern die Beschaffenheit des Internets sowie das zur Übertragung von Emails verwendete SMTP Protokoll eine effiziente Bekämpfung unerwünschter Emails. Nichtsdestotrotz wurden diverse Ansätze entwickelt, die das Versenden von Spam zumindest erschweren sollen.
Eine dieser Möglichkeiten ist der Einsatz von sogenanntem schwarzen, grauen und weißen Listen, was im Allgemeinen unter den Begriffen „blacklisting“, „greylisting“ und „whitelisting“ bekannt ist. Auf schwarzen Listen sind die Adressen von bekannten VersenderInnen von Spam gespeichert. Diese Listen sind öffentlich zugänglich und können von Email-Servern, die für das Empfangen von Emails zuständig sind, online abgefragt werden. Für jede eingehende Email kann so in Echtzeit geprüft werden, ob sich deren AbsenderIn auf einer dieser schwarzen Listen befindet. Graue Listen nutzen die Tatsache aus, dass VersenderInnen von Spam oft das SMTP Protokoll nicht korrekt implementieren. Eingehende Emails werden in einer grauen Liste gespeichert und mit einer Fehlermeldung quittiert. Erst wenn der sendende Email-Server entsprechend dem verwendeten Protokoll die Email erneut sendet, wird dessen Konformität angenommen und die Nachricht akzeptiert. Optional können bereits als seriös eingestufte AbsenderInnen auch auf sogenannte weiße Listen gesetzt werden. Die Methode der Verwendung von grauen Listen bringt jedoch den Nachteil, dass gültige Emails, die von schlecht konfigurierten Mailservern gesendet wurden, fälschlicherweise ignoriert werden können.
Ein weiterer Ansatz zur Bekämpfung von unerwünschten Emails ist der Einsatz von Spam-Filtern, welche versuchen mit Hilfe von selbstlernenden Algorithmen Spam-Emails als solche zu erkennen. Der Nachteil dieses Ansatzes ist die üblicherweise hohe Fehlerrate solcher Filter. So können meist nicht alle Emails korrekt klassifiziert werden was einerseits zu „false negatives“ (Spam wird nicht erkannt) aber andererseits auch zu „false positives“ (Email wird fälschlicherweise als Spam erkannt) führen kann. Speziell der letzte Fall kann durchaus problematisch sein, wenn dadurch wichtige Nachrichten die entsprechende EmpfängerIn nicht erreichen.
Gegenwärtig stellt sich die Situation so dar, dass noch kein probates Mittel gefunden wurde, um Spam in den Griff zu bekommen. Trotz diverser Gegenmaßnahmen macht Spam noch immer rund 80% des gesamten Emailaufkommens aus und stellt zunehmend auch eine finanzielle Bedrohung für Unternehmen und private Personen dar.

Mit der Einführung von DomainKeys Identified Mail (DKIM) Signatures steht ein neues Mittel zur Bekämpfung von Spam zur Verfügung. DKIM zielt darauf ab, dem Fälschen von Absenderdomänen, welches ein von VersenderInnen von Spam bevorzugt eingesetztes Mittel zur Verschleierung der eigenen Herkunft ist, einen Riegel vorzuschieben. Ziel dieses Projekts war es, diesen vielversprechenden Ansatz in der Praxis in Form einer Referenzimplementierung umzusetzen und einer ersten Evaluierung zu unterziehen. Die Ergebnisse dieses Projekts und erste Erkenntnisse über den Einsatz des DKIM-Standards in der Praxis und dessen Nutzen für private AnwenderInnen als auch für Unternehmen werden im Folgenden in diesem Dokument erläutert.

2 Analyse des DKIM-Standards

2.1 DomainKeys Identified Mail Signatures

Um gegen die im vorigen Abschnitt beschrieben Spam-Problematik ein weiteres Mittel in der Hand zu haben, wurden im Mai 2007 DomainKeys Identified Mail (DKIM) Signatures von der IETF zum Standard erhoben. DKIM ist eine Weiterentwicklung von Yahoo!‘s DomainKeys und Ciscos Identified Internet Mail. Die aktuelle Version von DKIM, die nun unter RFC 4871 als Standard veröffentlicht wurde, ist das Resultat einer Kollaboration von mehreren Unternehmen, darunter Alt-N Technologies, AOL, Brandenburg InternetWorking, Cisco, EarthLink, IBM, Microsoft, PGP Corporation, Sendmail, StrongMail Systems, Tumbleweed, VeriSign und Yahoo!. Durch das Mitwirken dieser großen Anzahl von durchaus auch namhaften Unternehmen ist zu erwarten, dass der neue Standard auch die für dessen Etablierung nötige Unterstützung finden wird.
Prinzipiell zielt DKIM darauf ab, die Herkunft von Emails für eine EmpfängerIn verifizierbar zu machen. Dazu wird jede ausgehende Email vom sendenden Email-Server mit einem der Domäne des Email-Servers zugeordneten Schlüssel signiert. Zur Erstellung der Signatur kommt, wie in diesem kryptographischen Verfahren üblich, asymmetrische Kryptographie zum Einsatz. Die UnterzeichnerIn – in diesem Fall der sendende Email-Server – berechnet unter Zuhilfenahme des nur ihr bekannten privaten Schlüssels einen Signaturwert über die zu sendende Email und fügt diesen der Email hinzu. Der entsprechende öffentliche Schlüssel, welcher zur Verifikation der Signatur nötig ist, wird von der UnterzeichnerIn in deren DNS Server als TXT Resource Record bereitgestellt. Die EmpfängerIn der Email kann die entsprechende Signatur aus der erhaltenen Email extrahieren und den für die Verifikation benötigten öffentlichen Schlüssel aus dem DNS beziehen. Wurde die Absenderdomäne der Email gefälscht, kann nur ein falscher bzw. gar kein öffentlicher Schlüssel aus dem DNS bezogen werden. In diesem Fall kann auch die Signatur nicht positiv geprüft werden und die EmpfängerIn kann davon ausgehen, dass die erhaltene Email nicht seriös ist. Die folgende Abbildung illustriert die prinzipielle Funktionsweise des DKIM-Standards.

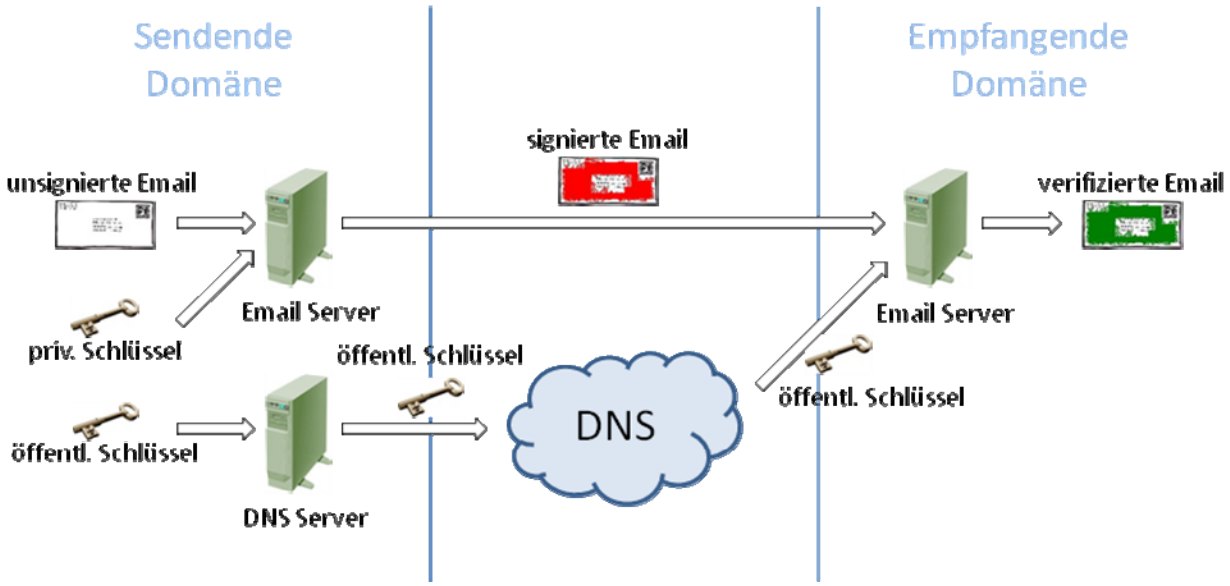

Abbildung 5 – Funktionsweise des DKIM-Standards

Die durch den DKIM-Standard festgelegte Funktionalität wird durch den sendenden bzw. den empfangenden Email-Server implementiert. Im Prinzip beschränken sich die durchzuführenden Operationen auf das Erstellen bzw. das Verifizierens eines Signaturwerts über die bearbeitete Email. Abbildung 6 illustriert die nötigen Schritte zur Erstellung der Signatur einer Email nach RFC 4871.

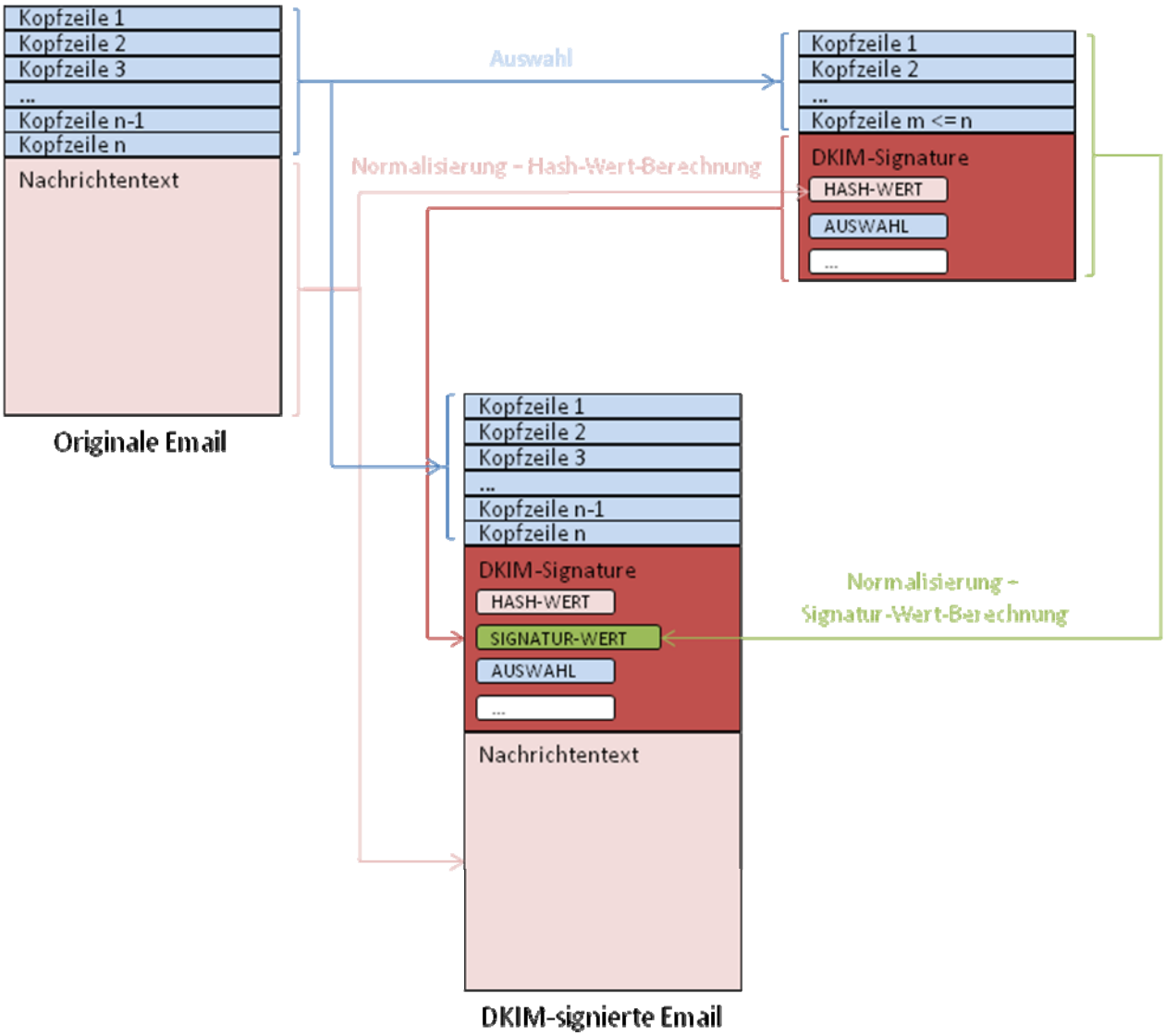

Abbildung 6 – Signaturerstellung laut DKIM-Standard

Der von der sendenden Domäne erstellte Signaturwert der Email wird dieser in Form einer zusätzlichen Kopfzeile beigefügt. Eine nach dem DKIM-Standard signierte Email ist also sehr einfach daran zu erkennen, dass ihre Kopfzeilen einen Eintrag namens „DKIM-Signature“ enthalten. Der Wert dieses Feldes enthält eine Liste, welche neben dem eigentlichen Signaturwert weitere, für die Verifikation relevante Informationen enthält. Der empfangende Email-Server kann aus dieser Liste die mitgelieferten Informationen extrahieren und damit die Korrektheit des angegebenen Signaturwerts überprüfen. Dabei versucht dieser, den von der UnterzeichnerIn vorgenommen und in Abbildung 6 dargestellten Vorgang der Signaturwert-Berechnung zu rekonstruieren. Ein typischer DKIM-Kopfzeileneintrag ist im Folgenden dargestellt, wobei die Darstellung des Signaturwerts in der letzten Zeile aus Gründen der Übersichtlichkeit gekürzt wurde. Der hier illustrierte DKIM-Kopfzeileneintrag beinhaltet unter anderem den zur Signaturerstellung verwendeten Algorithmus („rsa-sha256“), den Namen der Absenderdomäne („gmail.com“), sowie die verwendeten Normierungsalgorithmen („relaxed/relaxed“). Eine Auflistung aller Informationen, die in einem DKIM-Kopfzeilenfeld angegeben werden können bzw. müssen, kann dem DKIM-Standard [Ref03] entnommen werden.

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=gmail.com; s=beta;
    h=domainkey-signature:received:received:message-id:date:from:to:subject;
    bh=HEWxNGYlwwFsV8iuarerZLzAhVJZ+IAzIzLKkUVMxT8=;
    b=WUH9tESHGeKHSNN1UdJp3rykIACJyPE0 … 81QTsjO9QSB86G8gwrIO9+EIoZLMcF5JhnI=
```

Die Erstellung einer korrekten und für die EmpfängerIn verifizierbaren DKIM-Signatur gliedert sich prinzipiell in die folgenden in Abbildung 6 illustrierten Schritte.

1) Der Nachrichtentext der erstellten Email wird mit einem der laut Standard definierten Algorithmen normiert. Diese Normierung betrifft hauptsächlich die Entfernung unnötiger Zeilenumbrüche und Leerzeichen. Da mehrere Normierungsalgorithmen zur Verfügung stehen, muss der Name des verwendeten Algorithmus dem erstellten DKIM-Kopfzeileneintrag beigefügt werden.
2) Über den normierten Nachrichtentext wird ein Hash-Wert berechnet. Neben dem erhaltenen Hash-Wert selbst muss auch der zur dessen Berechnung verwendete Algorithmus dem DKIM-Kopfzeilenfeld beigefügt werden.
3) Der eigentliche Signaturwert wird ausschließlich über bestimmte, von der UnterzeichnerIn ausgewählte Kopfzeilenfelder gebildet. Der so gebildete zu signierende Text muss jedoch zumindest das „From“-Feld, sowie als letzten Eintrag das zu erstellende DKIM-Kopfzeilenfeld, das zum Zeitpunkt der Signaturerstellung bis auf den Signaturwert selbst bereits vollständig erstellt sein muss, enthalten.
4) Vor der Berechnung des Signaturwerts wird der zu signierende Text wiederum normiert. Der Normierungsalgorithmus, sowie die Namen der zur Signaturberechnung herangezogenen Kopfzeilenfelder müssen dem DKIM-Kopfzeileneintrag ebenfalls beigefügt werden.
5) Die Signatur selbst wird dann über einen Hash-Wert der ausgewählten und normierten Kopfzeilenfelder berechnet. Hash- und Signaturalgorithmus müssen dem DKIM-Kopfzeileneintrag ebenfalls beigefügt werden.
6) Der berechnete Signaturwert wird in den DKIM-Kopfzeileneintrag eingefügt. Dieser DKIM-Kopfzeileneintrag wird dann der zu übertragenden Email beigefügt.

Eine auf diese Art und Weise signierte Email kann schließlich an die EmpfängerIn gesendet werden, welche die Authentizität der Absenderdomäne der Email mit Hilfe der erstellten DKIM-Signatur verifizieren kann. Die Verifikation der erhaltenen Signatur gliedert sich in die folgenden Schritte.

1) Aus der erhaltenen Email werden alle DKIM-Signaturen extrahiert um sie im Folgenden überprüfen zu können. Falls die Nachricht mehr als eine Signatur enthält, ist es der PrüferIn überlassen, in welcher Reihenfolge die gefundenen Signaturen evaluiert werden.
2) Die extrahierte DKIM-Signatur wird auf Korrektheit überprüft. Dabei wird das entsprechende Kopfzeilenfeld auf syntaktische Korrektheit überprüft und festgestellt, ob alle zur Verifikation benötigten Daten vorhanden sind.
3) Vor der eigentlichen Überprüfung des Signaturwerts wird der benötigte öffentliche Schlüssel bezogen. Prinzipiell wird die Methode, mit welcher der Schlüssel abgefragt werden kann, von der UnterzeichnerIn im DKIM-Signatur Kopfzeilenfeld angegeben. Derzeit ist im Standard jedoch nur das DNS als Medium zum Schlüsselaustausch spezifiziert.
4) Der erhaltene Schlüssel und die mitgelieferten Metainformationen werden auf deren syntaktische Korrektheit überprüft.
5) Mit Hilfe der von der UnterzeichnerIn angegebnen Informationen wird die signierte Nachricht rekonstruiert, normiert und ein eigener Signaturwert berechnet. Dieser Signaturwert wird mit dem von der UnterzeichnerIn erstellten und übermittelten Signaturwert verglichen. Stimmen die Werte überein, konnte die Herkunft der Email erfolgreich authentifiziert werden.
6) Abhängig vom erhaltenen Ergebnis können optional entsprechende Schritte eingeleitet werden, um die untersuchte Nachricht entsprechend einer festzulegenden Strategie weiterzuverarbeiten.

2.2 Implementierungsansatz und Projektziel

Ziel dieses Projekts war es, neben der Analyse des DKIM-Standards eine Referenzimplementierung desselbigen zu erstellen, diese Implementierung in einer Testumgebung zu installieren und die Effizienz des Standards in der Praxis zu erproben.
Da unter anderem eine Anforderung an die Implementierung darin bestand, eine leichte Integrierbarkeit des erstellten Elements in bestehende Infrastruktursysteme zu gewährleisten, wurde entschieden, die durch den Standard vorgegebene Funktionalität in Form eines Proxys umzusetzen. Ein Proxy kann einer bestehenden Infrastruktur ohne großen Aufwand als zusätzliche Komponente beigefügt werden, was zu einer einfachen Installation der zu erstellenden Implementierung beitragen sollte. Die folgende Abbildung illustriert die Architektur, die sich aus dem Einsatz der Proxy-Komponente ergibt.

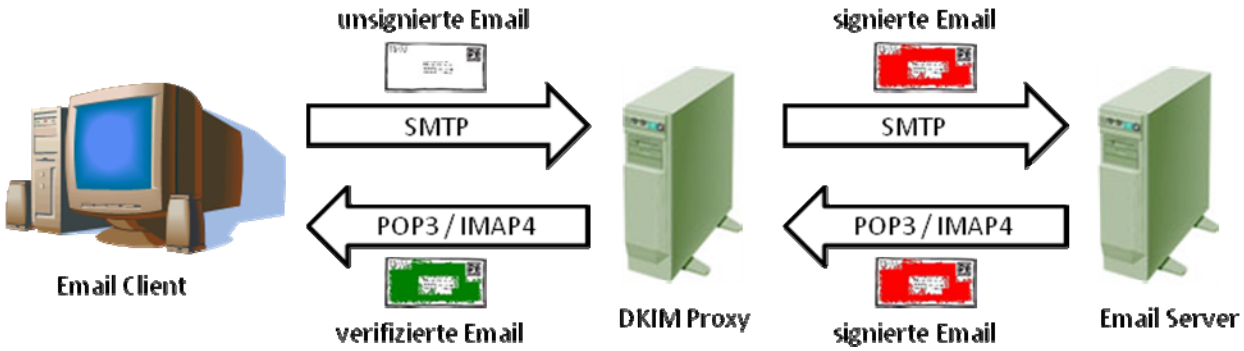

Abbildung 7 – Architektur unter Einbeziehung der Proxy-Komponente

Der Email-Client sendet neu erstellte Nachrichten über SMTP an den Proxy anstelle des Email-Servers. Der Proxy verhält sich in diesem Fall wie ein Email-Server und nimmt die Nachricht entgegen. Mit Hilfe des privaten Schlüssels der Domäne wird die Nachricht vom Proxy laut DKIM-Standard signiert und schließlich an den eigentlichen Email-Server weitergeleitet. Gegenüber dem Email-Server verhält sich der Proxy in diesem Fall wie ein Client.
Umgekehrt werden empfangene Emails durch den Proxy via POP3 oder IMAP4 vom Server abgeholt. Der Proxy übernimmt die Verifikation der DKIM-Signatur, sofern diese vorhanden ist und leitet die Nachricht schließlich an den Email-Client weiter. Wiederum stellt sich der Proxy gegenüber dem Email-Server als Client und gegenüber dem Email-Client als Server dar. Die Umsetzung der durch den DKIM-Standard festgelegten Funktionalität geschieht also für Email-Server und Client völlig transparent.

3 Referenzimplementierung

3.1 Referenzelement DKIM

Entsprechend der in Abschnitt 2.2 erläuterten Architektur, wurde ein Programm entwickelt, welches die Funktionalität der Proxy-Komponente übernimmt. Dieses Programm kann sehr einfach auf jedem beliebigen Rechner installiert werden, um die ihm zugedachten Aufgaben zu erfüllen. Die Installation wird durch Starten der entsprechenden Installationsdatei gestartet, woraufhin die BenutzerIn mit interaktiven Dialogen durch den Installationsprozess geleitet wird. Eine detaillierte Beschreibung des Installationsvorgangs kann der Programm-Dokumentation entnommen werden.
Nach Abschluss der Installation findet sich im Startmenü unter Programme ein neuer Eintrag „DKIM-Proxy“. Unter diesem Menüpunkt können die drei im Folgenden beschriebenen Teilmodule der Anwendung DKIM-Proxy gestartet werden.

3.1.1 RSA Schlüsselpaar erstellen

Wie bereits in Abschnitt 2.1 erläutert, werden zur Umsetzung des DKIM-Standards zwei Schlüssel benötigt. Zum Anbringen der Signatur wird ein geheimer privater Schlüssel verwendet, während für die Signaturverifikation der zugehörige und für jedermann über das DNS zugängliche öffentliche Schlüssel zum Einsatz kommt. Mit dem Menüeintrag „RSA Schlüsselpaar erstellen“ können zwei entsprechende Schlüssel generiert werden. Das Programm beendet sich nach erfolgreicher Erstellung des Schlüsselpaars von selbst. Im Programmverzeichnis von DKIM-Proxy finden sich nach einer erfolgreichen Generierung der Schlüssel im Unterverzeichnis „keys“ zwei Dateien.

- Die Datei „private_key.private“ enthält den für die Signaturerstellung benötigten geheimen Schlüssel. Diese Datei ist ihrerseits mit einem Passwort verschlüsselt.

- Die Datei „public_key.txt“ enthält den zum privaten Schlüssel gehörigen öffentlichen Schlüssel in Base64-Codierung. Dieser Schlüssel muss im DNS-Server der eigenen Domäne als TXT Resource Record zugänglich gemacht werden. Einzelheiten über das Format des Records können der Programmdokumentation bzw. dem DKIM-Standard entnommen werden.

Es ist durchaus auch möglich, in einer Domäne mehrere Instanzen von DKIM-Proxy zu betreiben, welche alle auf dasselbe Schlüsselpaar zurückgreifen. Die Generierung eines Schlüsselpaars ist daher nur einmal nötig. Allen übrigen Instanzen kann der benötigte private Schlüssel durch Kopieren der entsprechenden Datei in das Unterverzeichnis „keys“ zur Verfügung gestellt werden.

3.1.2 Konfigurations-Editor

Bevor die Proxy-Komponente in Betrieb genommen werden kann, müssen noch einige grundlegende Einstellungen vorgenommen werden, um eine korrekte Funktionalität von DKIM-Proxy zu gewährleisten. Diese Einstellungen können über ein graphisches Benutzerinterface konfiguriert werden, das über den Menüpunkt „Konfigurationseditor“ aufgerufen werden kann. Abbildung 8 zeigt das entsprechende Interface.
Die konfigurierbaren Einstellungen gliedern sich in die vier Rubriken „POP3“, „IMAP4“, „SMTP“, sowie „DKIM Einstellungen“. Unter letzterer können die Domäne, in dem DKIM-Proxy betrieben wird, sowie der Selector, unter dem der öffentliche Schlüssel im DNS-Server hinterlegt ist, eingetragen werden. Die anderen drei Rubriken entsprechen den von DKIM-Proxy unterstützten Protokollen zur Übertragung von Emails. Die Proxy-Funktion lässt sich getrennt für jedes der Protokolle mit Hilfe der „Proxy aktiv“ Schaltfläche aktivieren. Des Weiteren kann für jedes Protokoll der entsprechende Email-Server (Name bzw. IP-Adresse, sowie Port), an den DKIM-Proxy Kommandos und Daten weiterleiten soll, angegeben werden. Schließlich kann auch noch der Port, unter dem sich der Client zum Proxy verbinden wird, konfiguriert werden.
Eine genauere Beschreibung des Konfigurationsvorgangs kann auch der Dokumentation von DKIM-Proxy entnommen werden.

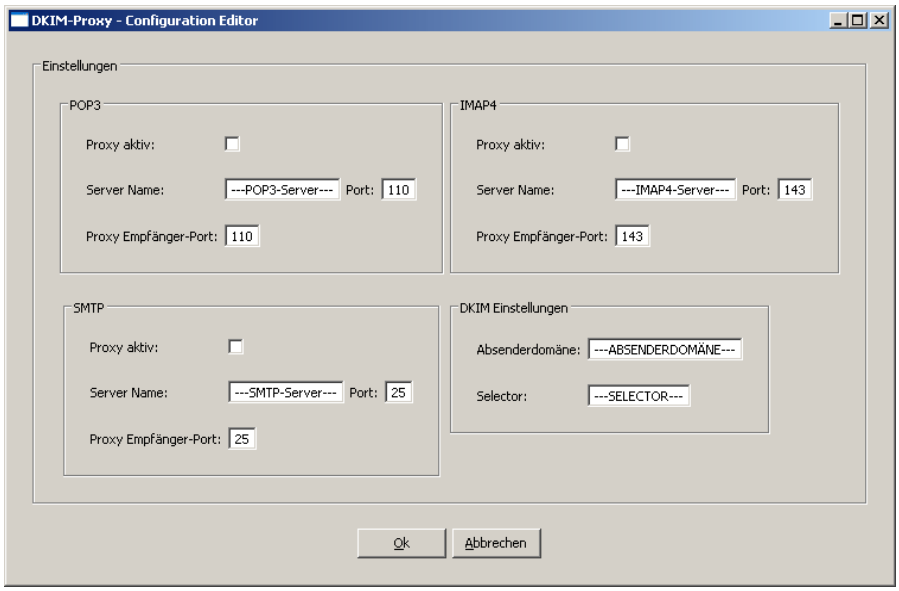

Abbildung 8 – Benutzer-Interface des Konfigurations-Editors

3.1.3 DKIM-Proxy

Nachdem sichergestellt ist, dass die benötigten Schlüssel vorhanden, sowie die Applikation korrekt konfiguriert ist, kann die eigentliche Proxy Komponente unter dem Menüpunkt „DKIM-Proxy“ gestartet werden. Nachdem DKIM-Proxy erfolgreich gestartet wurde, erscheint in der System-Leiste ein Symbol, das anzeigt dass DKIM-Proxy läuft (Abbildung 9).

Abbildung 9 – DKIM-Proxy in der Systemleiste

DKIM-Proxy ist ab diesem Zeitpunkt bereit Verbindungen von Email-Clients entgegenzunehmen und Emails nach dem DKIM-Standard zu verarbeiten.
Ausführlichere Informationen zur Inbetriebnahme von DKIM-Proxy können wiederum der Dokumentation entnommen werden.

3.2 Implementierte Funktionalität

Die durch DKIM-Proxy implementierte Funktionalität besteht prinzipiell aus zwei Aspekten.
Zum einen werden sämtliche ausgehende Emails nach dem DKIM-Standard signiert und um das entsprechende DKIM-Signature Kopfzeilenfeld erweitert. Die Herkunft einer von DKIM-Proxy verarbeiteten ausgehenden Email ist damit von der EmpfängerIn der Email eindeutig verifizierbar.
Zum anderen werden sämtliche, über DKIM-Proxy empfangenen Emails entsprechend dem DKIM-Standard überprüft. Prinzipiell gibt es drei mögliche Ergebnisse der Verifikation.

1) NOT SIGNED - Die untersuchte Email enthält keine DKIM-Signatur
2) PASSED - Die untersuchte Email konnte erfolgreich verifiziert werden
3) FAILED - Die untersuchte Email enthält eine DKIM-Signatur, die aber nicht verifiziert werden konnte

Um dem Email-Client dieses Ergebnis mitteilen zu können, wird der untersuchten Email ein zusätzliches Kopfzeilenfeld namens „X-DKIM-Proxy-Evaluation-Result“ beigefügt. Der Wert dieses Kopfzeilenfeldes entspricht dem Ergebnis der Signaturverifikation. Abbildung 10 zeigt eine von der Domäne „gmail.com“ signierte und von DKIM-Proxy positiv verifizierte Email. Schlägt die Verifikation einer untersuchten Email fehl, wird neben dem Wert „FAILED“ zusätzlich der Grund für das Scheitern der Signaturverifikation angegeben, sofern dieser bekannt ist.
Dem Email-Client ist es nun überlassen, ob und wie er diese zusätzliche Information verwendet. Beispielsweise könnte ein Filter im Email-Client so konfiguriert werden, dass alle Emails, die ein X-DKIM-Proxy-Evaluation-Result Kopfzeilenfeld mit dem Wert „FAILED“ besitzen, als Spam markiert und in einen entsprechenden Ordner verschoben werden.

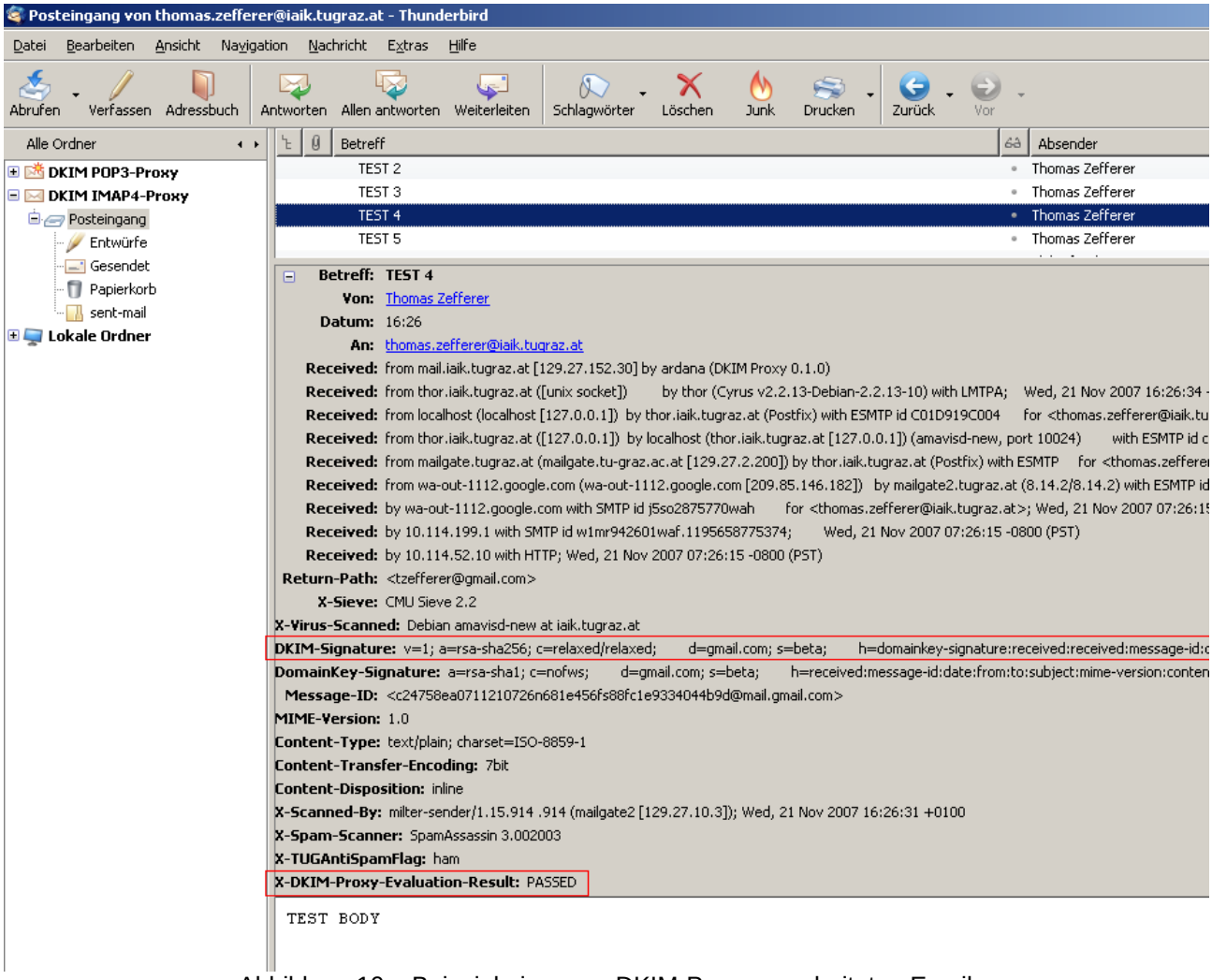

Abbildung 10 – Beispiel einer von DKIM-Proxy verarbeiteten Email

4 Evaluierungsphase

Um den umgesetzten Standard in der Praxis erproben und erste Rückschlüsse auf dessen Effizienz gewinnen zu können, wurde die entwickelte Referenzimplementierung „DKIM-Proxy“ in einer Testumgebung eingerichtet. Dazu wurden Instanzen von DKIM-Proxy auf mehreren Rechnern einer Domäne installiert und die Ergebnisse der lokal durchgeführten Signaturverifikationen statistisch erfasst und ausgewertet. Um repräsentative sowie statistisch aussagekräftige Zahlen zu erhalten, wurden insgesamt über 2000 Emails einer entsprechenden Verifikation unterzogen. Die Ergebnisse dieser Verifikationen sowie die wichtigsten daraus ableitbaren Schlussfolgerungen sind in diesem Abschnitt zusammengefasst.

4.1 Statistische Auswertung der Testergebnisse

Die Auswertung der erhaltenen Verifikationsergebnisse zeigte, dass nur ein kleiner Bruchteil der untersuchten Emails auch tatsächlich nach dem DKIM-Standard signiert war. Die folgende Abbildung illustriert das Verhältnis zwischen signierten und unsignierten Emails.

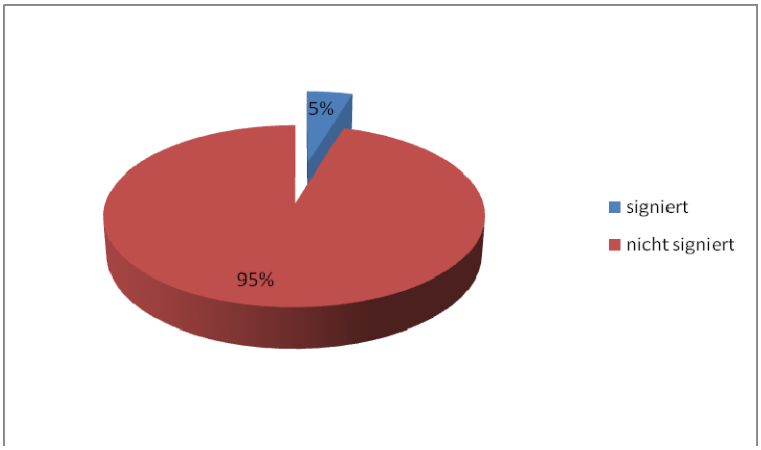

Abbildung 11 – Anteil der nach DKIM signierten Nachrichten

Insgesamt wiesen nur 5% der untersuchten Emails eine entsprechende DKIM-Signatur auf. Dies ist wohl darauf zurückzuführen, dass der Standard noch relativ neu ist. Zwar gibt es bereits entsprechende Implementierungen, welche auch relativ einfach in bestehende Email-Infrastruktursysteme integriert werden können, allerdings scheint es, dass der DKIM-Standard bei den jeweiligen BetreiberInnen und AdministratorInnen dieser Systeme noch nicht die nötige Akzeptanz gefunden hat.
Eine Analyse der wenn auch spärlich vorhandenen DKIM-Signaturen zeigte, dass ein Großteil (85%) der Signaturen auch verifizierbar war und somit eine erfolgreiche Authentifizierung der Absenderdomäne durchgeführt werden konnte. Das folgende Diagramm veranschaulicht den Anteil der verifizierbaren DKIM-Signaturen.

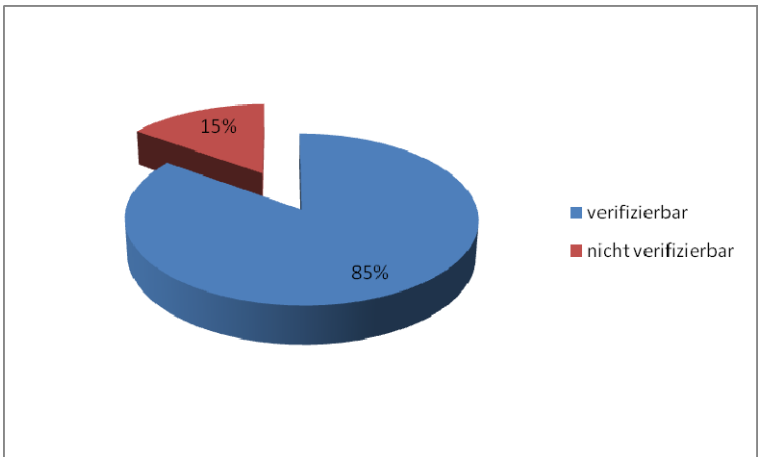

Abbildung 12 – Anteil der verifizierbaren Nachrichten

Prinzipiell kann die Verifikation eine DKIM-Signatur aus unterschiedlichen Gründen fehlschlagen. Eine Auflistung der während der Evaluierung der erhaltenen Signatur möglichen Fehler ist im DKIM-Standard gegeben und beinhaltet unter anderem Probleme, die während des Beziehens des öffentlichen Schlüssels auftreten können, syntaktisch inkorrekte DKIM-Signatur Kopfzeilenfelder oder eine – wenn auch nur geringfügige – Änderung der Email während deren Übertragung. Während der in der Evaluierungsphase dieses Projekts durchgeführten Signaturverifikationen traten zwei Fehlerklassen auf, die eine positive Authentifizierung der Absenderdomäne verhinderten. Zum einen hielten einige der übermittelten DKIM-Signaturen die durch den Standard definierten Vorgaben nicht vollständig ein und übertrugen nicht alle zu einer Verifikation notwendigen Informationen. Zum anderen konnten einige der erhaltenen Signaturwerte nicht positiv verifiziert werden, obwohl die entsprechende Email zweifelsohne aus einer vertrauenswürdigen Domäne gesendet wurde. Grund für das Fehlschlagen des Authentifizierungsvorgangs war, dass der während des Verifikationsprozesses erstellte Signaturwert der rekonstruierten Nachricht von dem durch die AbsenderIn übermittelten Signaturwert abwich. Die folgende Abbildung illustriert die prozentuelle Verteilung der aufgetretenen Fehler.

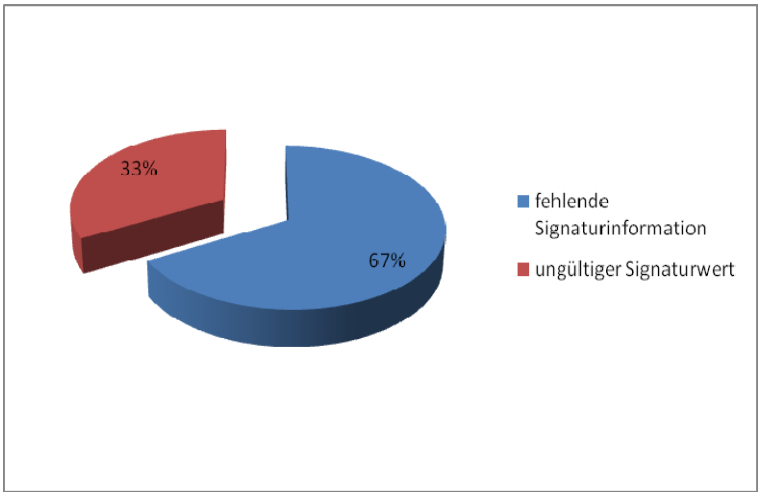

Abbildung 13 – Prozentuelle Verteilung der aufgetretenen Fehler

4.2 Analyse und Schlussfolgerungen

Obwohl der Standard, welcher die Verwendung von DomainKeys Identified Mail Signatures spezifiziert noch relativ neu ist, konnten durch die während der Evaluierungsphase erhaltenen statistischen Daten bereits erste Einblicke in die Funktionsweise von DKIM und dessen Praxistauglichkeit gewonnen werden. So zeigte sich, dass eine EmpfängerIn durch die Verwendung dieses Standards durchaus in der Lage ist, die Authentizität von Absenderdomänen zu verifizieren. Den Vorteilen, die sich für private AnwenderInnen und Unternehmen durch die Verwendung dieses Standards ergeben, stehen jedoch auch einige Bedenken, was die Zuverlässigkeit und Sicherheit dieses Standards anbelangt, gegenüber.
Eine unbestrittene Stärke des DKIM-Standards ist zweifelsohne die Tatsache, dass dieser in bestehende Email-Systeme integriert werden kann, ohne bereits in Verwendung befindliche Protokolle wie SMTP ändern oder anpassen zu müssen. Durch die von diesem Standard spezifizierte Ende-zu-Ende Signatur ist es theoretisch auch völlig irrelevant, wie viele Mailrelays sich zwischen AbsenderIn und EmpfängerIn befinden und ob diese den Standard ebenfalls beherrschen, da die Signatur ein integraler Bestandteil der Email selbst ist. Wichtig ist einzig und alleine, dass die AbsenderIn bzw. die EmpfängerIn den DKIM-Standard implementieren.
Ein weiterer Vorteil von DKIM ist die Verwendung des DNS zum Austausch der für erfolgreiche Signaturverifikationen benötigten öffentlichen Schlüssel. Da jede sendende TeilnehmerIn, die den DKIM-Standard implementiert, selbst ein entsprechendes Schlüsselpaar erstellen und den Schlüssel zur Verifikation über das DNS bereitstellen muss, kann auf eine aufwändige Public-Key Infrastructure (PKI) und den Einsatz von sogenannten Certification Authorities (CA) verzichtet werden, was unter anderem auch zu einer Kostenersparnis führt. Den Vorteilen, die sich durch den

Einsatz des DNS ergeben, stehen jedoch auch einige Bedenken gegenüber, auf die teilweise bereits im RFC des DKIM-Standards hingewiesen wird. So beruht die Funktionalität von DKIM auf der Annahme, dass der öffentliche Schlüssel zur Signaturverifikation stets korrekt über das DNS bezogen werden kann. Diese Annahme ist jedoch nicht zulässig, da das DNS erwiesenermaßen anfällig für diverse Attacken von potentiellen AngreiferInnen ist [Ref04]. Gelingt es einer AngreiferIn beispielsweise durch DNS-Spoofing die Sicherheit dieses Systems zu untergraben, ist sie in der Lage korrekt verifizierbare Emails im Namen einer anderen Domäne zu versenden. Im DKIM-Standard selbst wird in diesem Zusammenhang auf DNS Security (DNSSEC) [Ref05] und auf die damit erhoffte Steigerung der Sicherheit von DNS verwiesen. Darüber hinaus wird im RFC des DKIM-Standards sinngemäß festgehalten, dass DKIM nicht dazu gedacht ist, einen starken kryptographischen Beweis über Urheberschaft oder Inhalt einer Email zu erbringen. Ein weiterer Nachteil der Verwendung des DNS zum Schlüsselaustausch ist die Tatsache, dass im Prinzip jede Verifikation eine separate DNS-Abfrage auslöst. Eine große Anzahl von gezielt ausgesendeten, gefälschten DKIM-Signaturen könnte damit zu einem merklichen Anstieg von DNS-Abfragen und in weiterer Folge zu einer Denial-Of-Service Attacke führen.
Neben den eben aufgezeigten Schwachpunkten betreffend das DNS und den damit verbundenen potentiellen Problemen beim Schlüsselaustausch lässt der DKIM-Standard noch weitere Szenarien zu, die eine Beeinträchtigung der Zuverlässigkeit von DKIM mit sich bringen können. Wie in Abschnitt 2.1 erläutert, geht in die Signaturerstellung einer Email unter anderem auch ein Hash-Wert über den Nachrichtentext der Email ein. Im DKIM-Standard ist spezifiziert, dass die Anzahl der in die Hash-Berechnung eingehenden Bytes optional beschränkt werden kann. Damit soll verhindert werden, dass Signaturen von an sich authentischen jedoch beispielsweise durch Mailing-Listen leicht veränderten oder erweiterten Emails brechen. Dieses Feature ermöglicht es jedoch AngreiferInnen, einer bereits signierten Email zusätzlichen Inhalt beizufügen, ohne damit eine erfolgreiche Verifikation der DKIM-Signatur in irgendeiner Weise zu beeinträchtigen. Dieses Feature sollte daher wenn überhaupt, dann nur mit größtmöglicher Vorsicht verwendet werden.
Im DKIM-Standard selbst wird auch vor der Möglichkeit von Replay-Attacken gewarnt. Es ist generell denkbar und möglich, dass eine AngreiferIn eine bereits gültig signierte Email an eine große Anzahl an EmpfängerInnen weiterleitet, was an sich an der Gültigkeit der DKIM-Signatur nichts ändert.
Ein weiteres Problem, mit dem sich DKIM konfrontiert sieht, besteht darin, dass existierende Standards es Mail Transfer Agents (MTA) erlauben, die Reihenfolge von Kopfzeilenfeldern zu verändern. Dies ist im Zusammenhang mit DKIM-Signaturen problematisch, wenn zur Signaturerstellung mehrere Kopfzeilenfelder gleichen Namens herangezogen wurden. Wird deren Reihenfolge während der Übermittlung zur EmpfängerIn geändert, ist es für diese unmöglich die originale Email korrekt zu rekonstruieren und so die erhaltene DKIM-Signatur positiv zu verifizieren.
Ein weiterer Kritikpunkt an DKIM ist die Tatsache, dass das Verfahren kein „Early-Reject“ unterstützt. Das bedeutet, dass eine Email komplett übertragen werden muss, bevor deren DKIM-Signatur überprüft und so festgestellt werden kann, ob die AbsenderIn vertrauenswürdig ist. DKIM kann daher nur bedingt dafür eingesetzt werden, um Rechenleistung, die durch die Verarbeitung von Spam anfällt, einzusparen. Darüber hinaus wird sogar im DKIM-Standard selbst davon abgeraten, dass Emails, deren DKIM-Signaturen nicht erfolgreich verifiziert werden können, nur aufgrund dessen verworfen werden. Das Vorhandensein einer gültigen DKIM-Signatur sollte also auf keinen Fall als hartes Filterkriterium herangezogen werden.

In Anbetracht all dieser durchaus stichhaltiger Argumente bleibt abzuwarten inwieweit sich DKIM zu einem geeigneten Mittel zur Bekämpfung von Spam entwickeln wird können. Vor allem wenn VersenderInnen von Spam eigene Domänen registrieren, sind sie dadurch natürlich auch in der Lage ihre Emails mit korrekten DKIM-Signaturen zu versehen. Das Vorhandensein einer verifizierbaren DKIM-Signatur impliziert daher nicht, dass es sich bei der entsprechenden Email nicht um Spam handeln kann. Genauso wenig kann davon ausgegangen werden, dass es sich bei einer Email, deren DKIM-Signatur nicht verifizierbar ist, oder die gar keine DKIM-Signatur enthält, um Spam handelt.
In letzter Zeit ist zudem der Trend zu beobachten, dass vermehrt Spam über sogenannte Bot-Netze versendet wird. Darunter versteht man ein Netz von Rechnern, welche für deren BenutzerInnen unbemerkt von einer AngreiferIn kontrolliert und für deren Zwecke missbraucht

werden. Auch in diesem Fall können die von DKIM zur Verfügung gestellten Möglichkeiten nicht dazu beitragen die Verbreitung von Spam-Email Sendungen zu unterbinden.
Durchaus vielversprechend dürfte der Einsatz von DKIM dagegen im Kampf gegen Phishing-Emails, einer Unterordnung von Spam, sein. Das Ziel von diesen Emails ist es, durch Vortäuschen einer anderen AbsenderIn (z.B. Hausbank), der die Zielperson vertraut, dieser Informationen (z.B. Zugangsdaten zu ihrem e-banking Konto) zu entlocken. In diesem Szenario könnte DKIM durchaus erfolgreich zum Einsatz kommen und das Vorgeben einer falschen Absenderdomäne aufdecken.
Ob und inwieweit DKIM im Kampf gegen Phishing eine Rolle spielen kann, wird die Zukunft zeigen. Für den Erfolg des Standards ist es als ersten Schritt zweifelsohne wichtig, dass möglichst viele Email-Server den DKIM-Standard unterstützen. Erst wenn genügend viele Domänen DKIM verwenden, kann dem Fehlen einer DKIM-Signatur eine genügend große Bedeutung zugewiesen werden um eine Spam-Warnung oder andere Maßnahmen zu rechtfertigen. Dies ist derzeit sicher noch nicht der Fall und wurde auch durch die statistische Auswertung der in der Evaluierungsphase des Projekts erhaltenen Ergebnisse untermauert. Sollte DKIM in Zukunft die nötige Akzeptanz finden, was aufgrund der großen Anzahl an namhaften Unternehmen, die bei der Entwicklung des Standards beigetragen haben, nicht unwahrscheinlich ist, kann dieser neue Standard dazu beitragen, Teilprobleme der Spam-Problematik zu lösen. Ein Allheilmittel gegen die missbräuchliche Verwendung der gesamten weltweiten Email-Infrastruktur will und kann DKIM aber nicht sein.

5 Zusammenfassung

Das Projekt „Referenzelement DKIM“ befasste sich mit der Untersuchung von DomainKeys Identified Mail (DKIM) Signatures, einem Vorschlag zur Signierung von Emails, welcher im Mai 2005 von der IETF unter RFC 4871 zum Standard erhoben wurde. Dieser Standard ermöglicht es Domänen, die Authentizität eigener gesendeter Emails für die entsprechenden EmpfängerInnen verifizierbar zu gestalten. Dazu wird jede ausgehende Email vor deren Übermittlung von der sendenden Domäne signiert. Der zur Signaturverifikation benötigte Schlüssel wird über das DNS angeboten und ist so eindeutig einer Domäne zugeordnet. Dadurch ist es für eine AngreiferIn unmöglich in einer Email eine Absenderdomäne vorzutäuschen und trotzdem eine gültige und verifizierbare DKIM-Signatur aufzubringen.
Ziel dieses Projekts war es, diesen neuen Standard zu analysieren, in Form einer Referenzimplementierung umzusetzen und einer ersten Evaluierung zu unterziehen. Dadurch sollten dessen Stärken und Schwächen analysiert, sowie dessen Relevanz für die heimische Wirtschaft abgewogen werden.
Motiviert durch die Analyse des Standards und nach Abwägung diverser Alternativen wurde schließlich entschieden, die Referenzimplementierung in Form eines Proxy-Ansatzes zu erstellen. Dies sollte eine einfache Integrierbarkeit in bereits bestehende Infrastruktursysteme gewährleisten und stellte sich zudem als praktikabelste Lösung dar.
Das nach diesem Ansatz entwickelte Referenzelement besteht insgesamt aus drei Modulen, welche unterschiedliche Teilfunktionalitäten implementieren. So wurde ein Schlüsselgenerator entwickelt, mit dem das benötigte Schlüsselpaar bestehend aus einem privaten Schlüssel zur Signaturerstellung und einem zu veröffentlichenden Schlüssel zur Signaturverifikation erstellt werden kann. Das zweite implementierte Modul dient der Festlegung der Konfiguration des Referenzelements, welches dann an einem beliebigen Rechner der Domäne installiert werden kann. Die Konfiguration kann dabei über ein graphisches Benutzerinterface angepasst werden. Das dritte Modul beinhaltet schließlich das eigentliche Referenzelement des DKIM-Standards und besteht aus einem Proxy, zu welchem sich Email-Clients verbinden können. Der Proxy nimmt zu sendende Emails von Clients über SMTP entgegen und fügt diesen Emails eine entsprechende DKIM-Signatur hinzu. Die so signierte Email wird schließlich an einen konfigurierbaren Email-Server der Domäne weitergeleitet. Äquivalent dazu werden Anfragen zum Download neuer Nachrichten vom Client an die Proxy Komponente gerichtet. Der Proxy leitet diese Anfragen zu einem konfigurierbaren Email-Server der Domäne weiter und nimmt die retournierten Nachrichten vom Server entgegen. Diese Nachrichten werden vom Proxy auf vorhandene DKIM-Signaturen überprüft. Nachdem gefundene DKIM-Signaturen verifiziert wurden, wird das Ergebnis der Verifikation der Email selbst als zusätzliches Kopfzeilenfeld beigefügt. Schließlich wird die so verifizierte Email an den Client übermittelt, welcher das durch den Proxy angefügte Verifikationsergebnis auswerten und entsprechende Schritte einleiten kann.
Nach erfolgter Fertigstellung des Referenzelements wurde die entwickelte Lösung in einer Testumgebung installiert um den Einsatz des DKIM-Standards in der Praxis zu erproben. Dazu wurde der erstellte Proxy auf einer Reihe von Rechnern in einer Domäne lokal installiert. Sämtliche, an diesen Rechnern durchgeführten DKIM-Signaturverifikationen wurden protokolliert und deren Ergebnisse statistisch erfasst. Dabei stellt sich heraus, dass derzeit nur ein sehr geringer Anteil von 5% aller empfangenen Emails nach dem DKIM-Standard signiert war. Dies lässt sich darauf zurückführen, dass der Standard noch relativ neu ist und erst von einer geringen Anzahl von Domänen unterstützt wird. Inwieweit die Verbreitung von DKIM steigen wird, ist schwer zu prognostizieren und wird unter anderem von der Akzeptanz, die diesem neuen Verfahren entgegengebracht werden wird, abhängen. Immerhin konnten 85% der signierten Emails auch erfolgreich verifiziert und damit die Absenderdomänen dieser Email authentifiziert werden. Die restlichen 15% der signierten Emails konnten nicht positiv verifiziert werden, obwohl deren Absenderdomänen zweifelsohne vertrauenswürdig waren. Hier scheiterte die Überprüfung der DKIM-Signatur an der Übermittlung von unvollständigen Signaturinformationen, bzw. an der nicht durchführbaren korrekten Rekonstruktion des zu signierenden Textes, was zu einem Brechen der Signatur führte.
Generell bietet DKIM einige interessante und durchaus positive Aspekte, die dessen Benutzung für BetreiberInnen von Email-Infrastruktursystemen interessant machen könnte. So sind der Verzicht auf eine teuere und aufwändige PKI sowie die leichte Integrierbarkeit des Standards in bestehende

Systeme durchaus Punkte, die für eine Integration des Standards in eigene Email-Systeme sprechen. Demgegenüber stehen allerdings einige Bedenken betreffend diverser Teilaspekte des Standards. So ist beispielsweise generell der Austausch des öffentlichen Schlüssels über das DNS problematisch, da dieses System erwiesenermaßen nicht den erforderlichen Schutz gegenüber Angriffen verschiedenster Art bieten kann und somit ein korrektes Beziehen des zur Verifikation nötigen öffentlichen Schlüssels nicht gewährleistet werden kann.
DKIM wird aller Voraussicht nach nicht dazu im Stande sein das Spam-Problem in all seinen Facetten zu lösen. Allerdings könnten mit Hilfe von DKIM durchaus Teilerfolge im Kampf gegen Phishing-Emails erzielt werden, da der Standard eine Möglichkeit bietet, die Absenderdomäne einer Email eindeutig zu authentifizieren. Der Erfolg des Standards wird jedoch maßgeblich von dessen Akzeptanz und der damit zusammenhängenden Verbreitung abhängen. Durch das Mitwirken vieler namhafter Unternehmen bei der Erstellung des Standards ist jedoch zu erwarten, dass DKIM zumindest in der Wirtschaft die für eine erfolgreiche Etablierung nötige Unterstützung finden wird.

Glossar

Abkürzung	Bedeutung
CA	Certification Authority
DKIM	DomainKeys Identified Mail
DNS	Domain Name System
DNSSEC	Domain Name System Security
IETF	Internet Engineering Task Force
IMAP4	Internet Message Access Protocol Version 4
IP	Internet Protocol
MTA	Mail Transfer Agent
PKI	Public Key Infrastructure
POP3	Post Office Protocol Version 3
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SMTP	Simple Mail Transfer Protocol

Referenzen

[Ref01]	World Internet Usage Statistics News and Population Stats [http://www.internetworldstats.com/stats.htm]
[Ref02]	Spam-Mails kosten Amerika 22 Milliarden Dollar pro Jahr [http://www.netzwelt.de/news/69747-spammails-kosten-amerika-22-miliarden.html]
[Ref03]	RFC 4871 – DomainKeys Identified Mail Signatures [http://www.ietf.org/rfc/rfc4871.txt?number=4871]
[Ref04]	RFC 3833 - Threat Analysis of the Domain Name System (DNS) [http://www.apps.ietf.org/rfc/rfc3833.html]
[Ref05]	RFC 4033 - DNS Security Introduction and Requirements [http://www.ietf.org/rfc/rfc4033.txt]
[Ref06]	Spam in Zahlen [http://www.lifego.de/specials/spam_zahlen/spam-in-zahlen.html]

Historie

Version	Datum	Kommentar
0.1	20.11.2007	Festlegung der Struktur
Ersteller		
Thomas Zefferer		
Version	**Datum**	**Kommentar**
0.2	26.11.2007	Fertigstellung der Inhalte
Ersteller		
Thomas Zefferer		
Version	**Datum**	**Kommentar**
0.3	27.11.2007	Anmerkungen
Ersteller		
Herbert Leitold		
Version	**Datum**	**Kommentar**
1.0	28.11.2007	Korrekturen und letzte Anpassungen
Ersteller		
Thomas Zefferer		