Maximilian Eibl, Martin Gaedke (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 11

Einführung von DNSSEC und DANE im Bayerischen Hochschulnetz

Sven Duscha[1] Bernhard Schmidt[2] Daniel Feuchtinger[3] Helmut Reiser[4]

Abstract: Verbindungen zwischen Mailservern über das Simple Mail Transfer Protocol (SMTP) können zur Sicherung des Übertragungskanals TLS-verschlüsselt werden. Die dafür verwendeten Zertifikate basieren auf CA-Vertrauen, sind oft nicht verifizierbar oder schlicht abgelaufen. Im Gegensatz zur TLS-Verschlüsselung im Browser kann hier keine manuelle Autorisierung durch einen Mail-Administrator erfolgen, sondern muss aufgrund der Vielzahl an Mails vom Server automatisiert entschieden werden. DANE (Domain Name System based Authentification of Named Entities) erlaubt die Zuordnung (Pinning) eines Zertifikats über einen Hash im Domain Name System, so dass es einem Domainnamen direkt zugeordnet werden kann. Damit lassen sich Zertifikate verifizieren und authentifizierte TLS-Verbindungen vollautomatisch zwischen Mail Transfer Agents (MTAs) aufbauen. *Steigerung der E-Mail Sicherheit in Bayern* ist ein durch das Bayerische Wissenschaftsministerium gefördertes Projekt zur Unterstützung der Systemadministratoren der bayerischen Universitäten und Hochschulen bei der Einführung von DNSSEC und darauf aufbauend der TLS-Absicherung der Mailserverkommunikation mittels DANE. Die Unterstützung erfolgt durch Kurse, Referenzimplementierungen, einer Informationsplattform und der Unterstützung durch direkte Ansprechpartner. Wir berichten hier über die technischen Grundlagen, organisatorischen Herausforderungen und bisherige Umsetzung des Projekts.

Keywords: DNSSEC, DANE, PKIX, Zertifikate, Bayerisches Hochschulnetz

1 Einführung

Während die Ende-zu-Ende-Verschlüsselung von Emails noch wenig Verbreitung gefunden hat, hauptsächlich aufgrund der Schwierigkeiten beim Schlüsselmanagement für Kommunikationspartner, wird auf die Verschlüsselung beim Transport der Emails mehr Augenmerk gelegt. Das klassische SMTP [Po81] [HW82] als eines der erfolgreichsten Protokolle im Internet, über das nahezu der gesamte Emailverkehr abgewickelt wird, startete in seiner Konzeption als unverschlüsseltes Übertragungsprotokoll zwischen Mail Transfer Agents (MTAs) sowie MTAs und Mail User Agents (MUAs). Erst nachträglich als Protokollergänzung wurde mit der „SMTP Service Extension for Secure SMTP over TLS“ [Ho02] eine opportunistische, optionale Verschlüsselung hinzugefügt.

[1] Leibniz Rechenzentrum, Abteilung KOM, Boltzmannstr. 1, 85748 Garching, sven.duscha@lrz.de
[2] Leibniz Rechenzentrum, Abteilung KOM, Boltzmannstr. 1, 85748 Garching, bernhard.schmidt@lrz.de
[3] Leibniz Rechenzentrum, Abteilung KOM, Boltzmannstr. 1, 85748 Garching, daniel.feuchtinger@lrz.de
[4] Leibniz Rechenzentrum, Abteilung KOM, Boltzmannstr. 1, 85748 Garching, helmut.reiser@lrz.de

2 Motivation

Diese Verschlüsselung mittels SMTP over TLS leidet unter einer Reihe von Schwachpunkten. Der Verbindungsaufbau ist unverschlüsselt und unauthentifiziert. Der empfangende Mailserver signalisiert mittels eines Schlüsselworts im Klartext-Banner, ob er zu einer TLS-Verschlüsselung in der Lage wäre. Der sendende Server kann danach bei Bedarf durch das Senden des STARTTLS-Befehls eine verschlüsselte Sitzung starten. Ein Angreifer kann nun beispielsweise eine sogenannte Downgrade-Attacke auf diese Aushandlung durchführen, indem er das Schlüsselwort aus dem unverschlüsselten Datenstrom entfernt oder ersetzt und damit dem Sender signalisiert, dass kein TLS unterstützt wird [Re15b]. Dies kann beispielsweise auch bei Firewalls der Fall sein, die, um die Nachrichten unverschlüsselt auf Viren oder Malware zu prüfen, die STARTTLS Nachricht heraus filtern.

2.1 Zertifkate

Nach Aushandlung der Verschlüsselung erfolgt im Regelfall eine Überprüfung des durch den Server präsentierten Zertifikats. Dabei muss das Zertifikat eindeutig dem Server zugeordnet werden, üblicherweise durch den Common-Name (CN), und die Signatur auf ihre Vertrauenswürdigkeit überprüft, d.h. auf eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA) zurückgeführt werden. Dies schlägt fehl, wenn das Zertifikat durch eine unbekannte CA oder nur selbst signiert wurde, der Common-Name nicht dem Servernamen entspricht oder das Zertifikat schlicht abgelaufen ist. Ein weiterer Schwachpunkt von SMTP mit STARTTLS ist die fehlende, konsistente Vertrauensstruktur: Alle MTAs müssten den gleichen CAs vertrauen und dürften keine Zertifikate verwenden, die nicht von einer dieser CAs ausgestellt wurden. Das ist in der Praxis nicht der Fall, ganz abgesehen davon, dass viele MTAs nur selbst erstellte (self-signed) Zertifikate verwenden.

Im Gegensatz zur Anwendung von TLS-Zertifikaten im Web bei https-Verbindungen [Re00] kann beim Mail-Austausch aufgrund der asynchronen Store-and-Forward Vermittlung dem Endnutzer kein Dialog präsentiert werden, in dem er eine Entscheidung zur Glaubwürdigkeit des Zertifikats treffen kann. Der Administrator kann diese Entscheidung aus nachvollziehbaren Skalierungsgründen nicht treffen. Bei einem nicht verifizierbaren Zertifikat müssten also entweder alle Mails zurückgehalten (und nach Ablauf der Haltezeit gelöscht) werden, oder die Sicherheit der TLS-Verschlüsselung durch das Akzeptieren beliebiger Zertifikate aufgegeben werden.

In der Vergangenheit gab es bei vielen, auch großen, CAs Fehler und Nachlässigkeiten. Dafür gibt es eine Reihe von Beispielen aus der näheren Vergangenheit [NS16]. Diese Fehler sorgen dafür, dass eine Vielzahl von Zertifikaten zurückgerufen werden muss, aber nicht nur aufgrund der Menge ist das ein Problem, siehe [La14a] und [La14b].

2.2 SMTP mit TLS

Aufgrund der im Abschnitt 2.1 beschriebenen Konzeption bietet SMTP nur ein opportunistisches Sicherheitsmodell [Du14]. Dies geht davon aus, dass bei einer umfassenden si-

cheren Kommunikation mehrere Zwischenschritte angeboten werden, um mit jedem Kommunikationspartner dabei die höchst mögliche Sicherheitsstufe zu wählen, die Kommunikation noch zulässt [Re15b].

Diese sind:

1. **Unverschlüsselt und nicht authentifiziert:** Angreifer können die gesamte Kommunikation mitlesen oder ändern, es ist unklar wer der Kommunikationspartner ist.
2. **Verschlüsselt und nicht authentifiziert:** Die Verbindung ist verschlüsselt, man ist vor passiven Angriffen geschützt, und die Integrität der Daten auf dem Übertragungsweg ist sicher gestellt.
3. **Verschlüsselt und authentifiziert:** Durch die Authentifizierung des Kommunikationspartners ist die Verbindung auch durch MITM-Attacken geschützt.

Der Versand von Emails von MUA über den Message Submission Agent (MSA) erfolgt über SMTP [Ne99], wobei hier der Einsatz von TLS über einen dedizierten Port (465) mitgeteilt werden kann. Ein MSA kommuniziert im Allgemeinen nur mit einem oder wenigen Servern des eigenen Providers, so dass hier das klassische, vom Webbrowser bekannte Modell der Zertifikatsbehandlung verwendet wird.

Dies ist beim Mailtransport über SMTP zwischen MTAs, mit dem wir uns im Projekt „Steigerung der E-Mail Sicherheit in Bayern“ und in dieser Publikation befassen, nicht der Fall, hier wird Port 25 verwendet.

2.3 Probleme von SMTP-Verbindungen über TLS

Oft werden abgelaufene Zertifikate nicht erneuert, Common-Names im Zertifikat entsprechen nicht mehr den Servernamen oder das Zertifikat kann nicht durch eine lückenlose Zertifikatskette verifiziert werden. Es obliegt dem sendenden MTA auch bei einem Zertifikat, dessen Gültigkeit nicht verifiziert werden kann, eine opportunistische TLS-Verschlüsselung aufzubauen (Stufe 2 im Abschnitt 2.2). In einer kurzen Erhebung am Leibniz-Rechenzentrum (LRZ) waren 74% der Verbindungen beim Emailversand „Trusted“ [Re15b]. Wenn man also Mailversand nur an authentifizierte MTAs zulassen würde, führt das dazu, dass rund ein Viertel der Emails nicht versendet würden.

3 DANE und DNSSEC

DANE spezifiziert die über DNSSEC kryptographisch abgesicherte Zuordnung eines TLS-Zertifikats zu einem Server über DNS-Records vom Typ TLSA. Da dem DNS ohnehin vertraut werden muss (die MX-Records der Domain entscheiden darüber, wohin die Mails gesendet werden), ist es eine elegante Lösung, auch das Vertrauen in die TLS-Zertifikate

an das DNS zu delegieren. TLSA-Records kann der Administrator der Domain selbst erstellen und verwalten, CAs, Zertifikatsketten und zurückgerufene Zertifikate gibt es nicht mehr, der Zertifikatsrückruf wird durch den Austausch des TLSA-Records ersetzt.

Damit eine Information im DNS wiederum vertrauenswürdig ist, muss die Maildomain und (!) die Domain des Mailservers mittels DNSSEC signiert sein und validiert werden, damit die bekannten Angriffspunkte auf DNS [AM07] vermieden werden können. Dafür wird ein asymmetrisches Signaturverfahren verwendet, um die Nameserverantworten zu authentifizieren und die Datenintegrität bei der Übertragung sicher zu stellen [Ar05a] und [Ar05b]. Details hierzu und Erfahrungen aus der Praxis am LRZ wurden schon in der einer früheren Publikation veröffentlicht [Re15a].

DANE bietet nicht nur die Möglichkeit die Authentizität eines (selbst-signierten) Zertifikats unabhängig (oder als zusätzliche Absicherung zu X.509 basierten Public Key Infrastructures (PKIX)) zu garantieren, sondern signalisiert einem DANE-fähigen Sender auch außerhalb des SMTP-Protokolls die Verfügbarkeit von TLS [HS12]. Dadurch werden Downgrade-Angriffe, wie in Abschnitt 2 beschrieben, verhindert. Falls die Verifizierung fehlschlägt, kann der MTA entscheiden, ob die TLS-Verbindung abgebrochen wird [DH15].

4 Herausforderungen bei der Einführung im Bayerischen Hochschulnetz

Während die Einführung in einer einzelnen Organisation sorgfältig geplant sein muss um Ausfälle zu vermeiden, stellt die Einführung im bayerischen Hochschulnetz (BHN) noch höhere Herausforderungen:

- Universitäten und Hochschulen sind autonom
- Vielzahl an Zonen, teilweise Verwaltung für angegliederte Hochschulen
- DNS und Mail sind essentielle Dienste: Angst vor Ausfällen
- Veraltete „legacy“ Nameserver, die kein DNSSEC unterstützen
- Software, die kein DANE unterstützt, z.B. MS Exchange als MTA oder zu altes Postfix
- MTAs in anderer Zone als Hochschulen (z.B. über DFN-Mailsupport)
- Wenig Erfahrung mit DNSSEC/DANE der Administratoren und wenig Manpower
- Integration ohne große Änderungen in die bestehende DNS-Verwaltung

5 Lösungen und Hilfestellungen

Die Chief Information Officers der bayerischen Universitäten und Hochschulen (siehe Abbildung 1) haben bereits 2015 beschlossen, DNSSEC und DANE zu unterstützen.

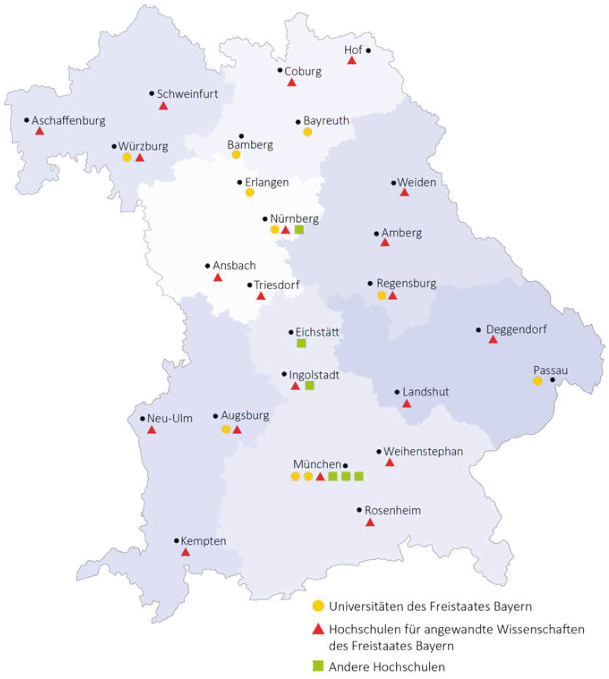

Abb. 1: Staatliche und nichtstaatliche Hochschulen und Universitäten in Bayern

Um die in Abschnitt 4 genannten Probleme anzugehen und die Einführung von DNSSEC und DANE im Bayerischen Hochschulnetz zu forcieren, hat das Bayerische Ministerium für Bildung und Kultus, Wissenschaft und Kunst[3] ein zweijähriges Förderprojekt gestartet, in dem das Leibniz Rechenzentrum der Bayerischen Akademie der Wissenschaften mit seiner Expertise den bayerischen Universitäten und Hochschulen Unterstützung und Schulung der Systemadministratoren anbieten kann.

Um den Umfang dieser Aufgabe einschätzen zu können, alle beteiligten Administratoren an einen Tisch zu bekommen und einen Überblick über die verwendeten Systeme zu erhalten, wurde 2015 eine erste Bestandsaufnahme durch Befragung der Netzwerkadministratoren durchgeführt. Diese hat das LRZ zusammen getragen und anhand dieser und den geäußerten Wünschen zur Unterstützung der beschlossenen Einführung von DNSSEC und DANE einen Projektplan erstellt.

Hierzu zählen die Bereitstellung von Dokumentation im LRZ Wiki. Da die allgemeine Suche nach DNSSEC/DANE im Internet zwar viele Treffer zu Tage fördert, aber aufgrund der schnellen Entwicklung der Standards in den letzten Jahren, und vor allem der Anpas-

[3] `https://www.km.bayern.de/`

sung in der Softwareunterstützung zum Auffinden mittlerweile veralteter Konfigurationen oder Empfehlungen führt.

Ferner wurden hier präzise Howto-Artikel geschrieben, die anhand der langjährigen Erfahrungen im Betrieb von DNSSEC, seit 2015 [Re15a], und DANE, seit 2014 [Re15b], praktische Anleitungen für Referenzimplementierungen bieten.

Da aber die Zonenverwaltung in der Hand der autonom für Ihren Netzbereich handelnden Administratoren liegt, kann hier weder eine Lösung von oben herab verbindlich bestimmt werden, noch wäre eine zentralisierte Verwaltung angebracht. Dies widerspräche auch dem hierarchischen Charakter von DNS im allgemeinen. So liegt auch die Schlüsselverwaltung in den Händen der für eine bestimmten Nameserver verantwortlichen Administratoren, eine zentrale Schlüsselverwaltung wäre hier hinderlich und auch nicht gewünscht.

Insbesondere die richtige Handhabung des Schlüsselmanagements und die Durchführung von Key Rollovers ergibt sich erst in der Praxis. Hier soll den Systemadministratoren eine mühevolle Einarbeitung, mit Fehlversuchen und Sackgassen, sowie daraus resultierende Ausfälle der DNS- und Mailinfrastruktur ihrer Hochschulen erspart werden. Beispielsweise die Empfehlung, dass ein, zwischen die DNS-Verwaltung und den öffentlichen Nameserver geschalteter, „signing proxy“ am sinnvollsten ist, erschließt sich nur aus der Praxis, wird aber nicht in den diversen Anleitungen im Internet erwähnt. So können die bestehenden Werkzeuge zur Zonenverwaltung weiter verwendet werden, und die Schnittstellen zum und vom „signing proxy“ sind als einfacher Zonentransfer realisiert (siehe Abbildung 2).

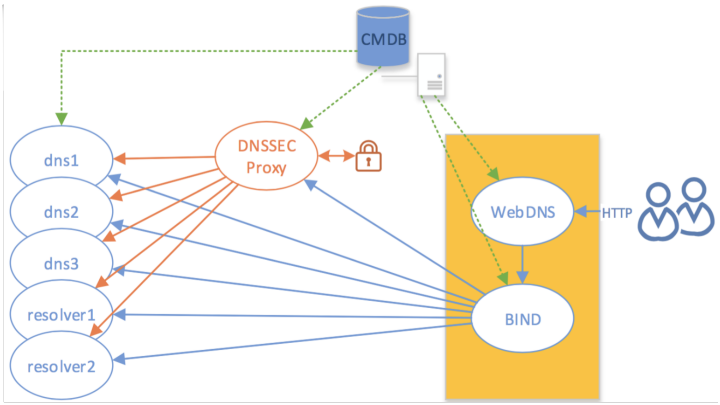

Abb. 2: Am LRZ verwendetes DNSSEC Signing Proxy Konzept mit BIND Nameservern. Die technischen Details sind in [Re15a] beschrieben.

So können auch die Systemadministratoren leichter von einer Einführung überzeugt werden, da dies vorerst keinen Eingriff in die bestehenden Systeme bedeutet. Wenn eine ungenutzte oder neu registrierte Domain dann als Testdomain verwendet werden kann, können dort selbst Erfahrungen im praktischen Betrieb gesammelt werden, ohne gleich ins kalte Wasser zu springen.

Von den Hochschulen und Universitäten wurden auch der Wunsch nach direkten Ansprechpartnern im LRZ und Kursen zur Schulung der Administratoren geäußert. Oben

genannte Howtos und die Zusammentragung von Online-Tutorials, die sich auf den aktuellen Stand der Software beziehen, erlauben das Selbststudium, aber eine konzentrierte Schulung in Form eines Kurses und der Möglichkeit Fragen zu stellen ist für den Einstieg effektiver.

Schon am Anfang des Projektes im November 2016 wurde ein zweitägiger Kurs am LRZ gegeben, an dem 12 Administratoren, hauptsächlich aus dem südbayerischen Raum, teilnahmen. Neben theoretischen und technischen Hintergründen wurde die Möglichkeit geboten auf eigens eingerichteten virtuellen Maschinen[4] Zonen zu signieren, Fehler zu debuggen, DANE einzurichten und den verifizierten TLS-Versand von Mails mit Postfix zu konfigurieren.

Daneben berichteten Kollegen, die für die Einrichtung von DNSSEC und DANE am LRZ verantwortlich waren, über Gründe für bestimmte Implementationsentscheidungen, Fallstricke und Erfahrungen aus dem Praxisbetrieb.

Um den nordbayerischen Adminstratoren eine weite Anreise zu ersparen, wurde derselbe Kurs, noch im März 2017, zusammen mit dem Regionalen Rechenzentrum Erlangen (RRZE)[5] veranstaltet. Hier berichtete der DNS-Administrator des RRZE auch über die Konfiguration von DNSSEC mit OpenDNSSEC[6], und die Unterschiede zu BIND9.

6 Fortschritt des Projekts

Mittlerweile läuft das Projekt seit einem halben Jahr, damit ist ein Viertel der Projektlaufzeit[7] verstrichen. Vor allem die Kurse mit den praktischen Übungen wurden von den Teilnehmern als sehr hilfreich angesehen. Zusammen mit den Howto-Artikeln zur Einrichtung von DNSSEC und DANE am Beispiel von BIND 9.9.5 und Postfix 2.11 haben die Administratoren einen guten Einstieg in eigene Tests und die Möglichkeit, die Umstellung der eigenen Domänen möglichst reibungslos zu planen.

Darüber hinaus steht das LRZ jederzeit als Ansprechpartner zur Verfügung und kann Hilfestellung bei Problemen leisten, telefonisch oder über das Incident Ticket System.

Derzeit wird ein Konzept des gegenseitigen Monitorings der Korrektheit der DNSSEC Konfiguration erarbeitet, mit dem die Teilnehmer, die DNSSEC signierte Zonen betreiben, im Fehlerfall benachrichtigt werden. So wird die tagelange Nichterreichbarkeit ganzer Domains aufgrund abgelaufener Schlüssel verhindert.

Im Falle von DANE ergeben sich organisatorische Probleme, wenn der Mailserver in einer anderen Zone liegt. Dies ist bei einigen durch den DFN betriebenen Mailservices der Fall. Der für das Zertifikat hinterlegte TLSA-Eintrag muss hier in der Zone, in der der Mailserver erreichbar ist, hinterlegt und mit DNSSEC signiert sein.

[4] Debian "Jessie"basiert, mit BIND 9.9.5 und Postfix 2.11, Konfiguration über Ansibleskripte
[5] `https://www.rrze.fau.de/`
[6] `https://www.opendnssec.org/`
[7] 1.10.2016-30.9.2018, `https://www.lrz.de/forschung/projekte/forschung-netz/DNSSEC_DANE/`

Ein weiteres Problem stellen oben genannte nicht DNSSEC oder DANE-fähige Softwareversionen dar. Während zur DNSSEC-Unterstützung meist nur ein Upgrade des jeweiligen Nameservers notwendig ist, wiegt schwerer, dass Microsoft Exchange kein ausgehendes DANE unterstützt. Wenngleich mit dem Betrieb eines weiteren virtuellen oder physischen Servers verbunden, kann dies doch mit einem nachgeschaltetem Postfix-Server als Mail Relay elegant gelöst werden. Diese Lösung wird auch am LRZ betrieben.

7 Fazit

Obwohl DNSSEC und DANE keine „rocket science“ sind, erfordern sie doch als neue Technologien Einarbeitung und Sorgfalt bei der Konfiguration. Um den Administratoren eine mühevolle Einarbeitung und Fehler zu ersparen ist dieses, durch das Bayerische Wissenschaftsministerium geförderte, Projekt extrem wichtig für eine reibungslose und zügige Einführung von DNSSEC und DANE im Bayerischen Hochschulnetz.

Das Ziel des Projektes ist eine möglichst flächendeckende Einführung von DNSSEC und DANE im BHN. Dies wird aktiv unterstützt durch die beschriebenen Maßnahmen und Infrastrukturen sowie einer regelmäßige Abstimmung mit den Administratoren, Feedback, Erfassung der Fortschritte in der Konfiguration der Nameserver mit DNSSEC und einer schnellen Hilfestellung im Problemfall.

Trotz der durchweg positiven Reaktionen der teilnehmenden Hochschulen, von denen ein Großteil an unseren Schulungen teilgenommen hat, ist bisher nur an einigen wenigen Hochschulen die Umstellung auf DNSSEC erfolgt. DANE wird von den am LRZ betriebenen Mailservern abgesehen, sonst bisher nur von der FAU unterstützt.

Oft wurden als Gründe das Abwarten größerer anderer geplanter Updates oder Zeitmangel genannt, da anderen Maßnahmen eine höhere Priorität zugewiesen wurde. Die Einführung von DNSSEC und DANE stellt somit weniger ein technisches Problem, als ein organisatorisches Problem dar.

Literaturverzeichnis

[AM07] Ariyapperuma, S.; Mitchell, C. J.: Security Vulnerabilities in DNS and DNSSEC. In: Proceedings of the The Second International Conference on Availability, Reliability and Security. ARES '07, IEEE Computer Society, Washington, DC, USA, S. 335–342, 2007, ISBN: 0-7695-2775-2, URL: http://dx.doi.org/10.1109/ARES.2007.139.

[Ar05a] Arends, R.; Austein, R.; Larson, M.; Massey, D.; Rose, S.: DNS Security Introduction and Requirements, RFC 4033, http://www.rfc-editor.org/rfc/rfc4033.txt, RFC Editor, März 2005, URL: http://www.rfc-editor.org/rfc/rfc4033.txt.

[Ar05b] Arends, R.; Austein, R.; Larson, M.; Massey, D.; Rose, S.: Resource Records for the DNS Security Extensions, RFC 4034, http://www.rfc-editor.org/rfc/rfc4034.txt, RFC Editor, März 2005, URL: http://www.rfc-editor.org/rfc/rfc4034.txt.

[DH15] Dukhovni, V.; Hardaker, W.: The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance, RFC 7671, RFC Editor, Okt. 2015.

[Du14] Dukhovni, V.: Opportunistic Security: Some Protection Most of the Time, RFC 7435, RFC Editor, Dez. 2014.

[Ho02] Hoffman, P.: SMTP Service Extension for Secure SMTP over Transport Layer Security, RFC 3207, http://www.rfc-editor.org/rfc/rfc3207.txt, RFC Editor, Feb. 2002, URL: http://www.rfc-editor.org/rfc/rfc3207.txt.

[HS12] Hoffman, P.; Schlyter, J.: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, RFC 6698, http://www.rfc-editor.org/rfc/rfc6698.txt, RFC Editor, Aug. 2012, URL: http://www.rfc-editor.org/rfc/rfc6698.txt.

[HW82] Harrenstien, K.; White, V.: NICNAME/WHOIS, RFC 812, RFC Editor, März 1982.

[La14a] Langley, A.: No, don't enable revocation checking, https://www.imperialviolet.org/2014/04/19/revchecking.html, 2014.

[La14b] Langley, A.: Revocation still doesn't work, https://www.imperialviolet.org/2014/04/29/revocationagain.html, 2014.

[Ne99] Newman, C.: Using TLS with IMAP, POP3 and ACAP, RFC 2595, http://www.rfc-editor.org/rfc/rfc2595.txt, RFC Editor, Juni 1999, URL: http://www.rfc-editor.org/rfc/rfc2595.txt.

[NS16] for Network, E. U. A.; Security, I.: Certificate Authorities - The Weak Link of Internet Security, https://www.enisa.europa.eu/publications/info-notes/certificate-authorities-the-weak-link-of-internet-security, 2016.

[Po81] Postel, J.: Simple Mail Transfer Protocol, RFC 788, RFC Editor, Nov. 1981.

[Re00] Rescorla, E.: HTTP Over TLS, RFC 2818, http://www.rfc-editor.org/rfc/rfc2818.txt, RFC Editor, Mai 2000, URL: http://www.rfc-editor.org/rfc/rfc2818.txt.

[Re15a] Reiser, H.; Feuchtinger, D.; Hommel, W.; Schmidt, B.; Storz, M.: DNSSEC - Konzepte und Betriebsaspekte des Domain Name Systems der Zukunft. Praxis der Informationsverarbeitung und Kommunikation 38/1-2, S. 71–81, 2015, URL: http://www.degruyter.com/view/j/piko.2015.38.issue-1-2/pik-2015-0005/pik-2015-0005.xml.

[Re15b] Reiser, H.; Feuchtinger, D.; Hommel, W.; Schmidt, B.; Storz, M.: E-Mail made in Science - Sicherheit für den E-Mail Transport mit DANE TLSA. Praxis der Informationsverarbeitung und Kommunikation 38/1-2, S. 23–41, 2015, URL: http://www.degruyter.com/view/j/piko.2015.38.issue-1-2/pik-2015-0004/pik-2015-0004.xml.