

WAB III Projektarbeit:

Analyse technischer Verfahren für sichere E-Mail-Kommunikation und Bewertung der Implementierung im Privatanwenderbereich

Projektarbeit
von

Pascal Feller
Daniel Moy
Florian Schünhoff
Chi Cong Tran

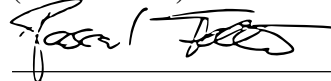
27. Juni 2014

Referent, Betreuer: Prof. Dr. - Ing. Undine Pielot


Hiermit versichern wir, dass wir die von uns vorgelegte Arbeit selbstständig verfasst haben, dass wir die verwendeten Quellen, Internet-Quellen und Hilfsmittel vollständig angegeben haben und dass wir die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht haben.

Leipzig, 27. Juni 2014

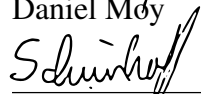
(Unterschrift)



Pascal Feller



Daniel Mø



Florian Schünhoff



Chr Cong Tran

Inhaltsverzeichnis

Abbildungsverzeichnis	II
Tabellenverzeichnis	III
Abkürzungsverzeichnis	IV
1 Einleitung	1
1.1 Motivation	1
1.2 Zielsetzung	1
1.3 Aufbau der Arbeit	1
2 Datensicherheit Einmaleins	3
3 Sicherheitsniveaus	4
4 Technologien und Verfahren	8
4.1 Kryptographie Grundlagen	8
4.1.1 Symmetrische Verschlüsselung	8
4.1.2 Asymmetrische Verschlüsselung	8
4.1.3 Digitale Signaturen	9
4.1.4 Zertifikate	10
4.2 Public Key Infrastruktur	10
4.3 Web of Trust	11
4.4 Schlüsselaustausch	12
4.4.1 RSA - Rivest, Shamir und Adleman-Kryptosystem	12
4.4.2 PFS - Perfect Forward Secrecy	12
4.5 Informationsverschlüsselung	14
4.5.1 PGP - Pretty Good Privacy	14
4.5.2 S/MIME - Secure / Multipurpose Internet Mail Extensions	15
4.6 Transportwegverschlüsselung	17
4.7 DNS - Domain Name System	18
4.7.1 DNSSEC - Domain Name System Security Extensions	19
4.7.2 DANE - DNS-based Authentication of Named Entities	19
5 E-Mail-Sicherheit in der Praxis	21
5.1 Nutzwertanalyse E-Mail-Provider	21
5.2 Provider Vergleich	23
5.2.1 Internationale Provider	23
5.2.2 EmiG - E-Mail made in Germany	25
5.2.3 Alternative Provider	28
5.2.4 De-Mail	31
6 Fazit und Ausblick	35
Literaturverzeichnis	36
Anhang	37

Abbildungsverzeichnis

1	Web of Trust Vertrauensmodell	12
2	Handshake-Protokoll mit RSA	17
3	Baumstruktur des DNS	18
4	Sicherheitsniveaus	24
5	T-Online PGP	25
6	Web.de PGP	26

Tabellenverzeichnis

1	Sicherheitsniveaus	5
2	Nutzwertanalyse der Provider	22

Abkürzungsverzeichnis

AES	Advanced Encryption Standard	MITM	Man in the Middle
BSI	Bundesamt für Sicherheit in der Informationstechnik	MAC	Message Authentication Code
CA	Certificate Authority	NSA	National Security Agency
CCC	Chaos Computer Club	OSI	Open System Interconnection
DANE	DNS-based Authentication of Named Entities	OTP	One Time Password
DHE	Diffie-Hellmann-Schlüsselaustausch	PCA	Policy Certification Authority
DKIM	DomainKeys Identified Mail	PGP	Pretty Good Privacy
DNS	Domain Name System	PFS	Perfect Forward Secrecy
DNSSEC	Domain Name System Security Extensions	PKI	Public Key Infrastructure
DTAG	Deutsche Telekom AG	RFC	Request for Comments
E2EE	End-to-End-Encryption	RSA	RSA(Rivest, Shamir und Adleman)-Kryptosystem
ECDH	Elliptic Curve Diffie-Hellman	SMTP	Simple Mail Transfer Protokoll
EmiG	E-Mail made in Germany	SSH	Secure Shell
GPG	GnuPG, GNU Privacy Guard	SSL	Secure Socket Layer
HSTS	HTTP Strict Transport Security	S/MIME	Secure/Multipurpose Internet Mail Extensions
HTTP	Hypertext Transfer Protokoll	TCP	Transmission Control Protocol
HTTPS	Hypertext Transfer Protokoll Secure	TLD	Top-Level-Domain
ICANN	Internet Corporation for Assigned Names and Numbers	TLS	Transport Layer Security
IETF	Internet Engineering Task Force	TLSA	Transport Layer Security Authentication
IP	Internet Protocol	TLS/SSL	Transport Layer Security/Secure Socket Layer
IPsec	Internet Protokoll Security	TCR	Trusted Community Representatives
ISP	Internet Service Provider	URL	Unified Ressource Locator
IMPT	Inter Mail Provider Trust	ZSK	Zone Signing Key

1 Einleitung

1.1 Motivation

E-Mails werden in der Regel unverschlüsselt und im Klartext übertragen. Somit wird es Dritten ermöglicht, an den Inhalt dieser Mails zu gelangen. Nicht nur im geschäftlichen elektronischen Schriftverkehr ist es wichtig, dass ausgetauschte Nachrichten Dritten gegenüber unzugänglich gemacht werden. Im privaten Bereich ist kann es unter Umständen auch erforderlich sein, dass die elektronische Kommunikation verschlüsselt wird, etwa bei vertraulichen Inhalten mit dem Arzt oder Behörden. Vielen Privatpersonen ist es mitunter unklar, welche Daten mitgelesen werden können. Zudem kennt nur eine geringe Anzahl der betroffenen Personen die verschiedenen Möglichkeiten zum Schutz bei der E-Mail-Kommunikation. Diese Thematik ist durch die jüngsten Enthüllen von Edward Snowden (Stand 2014) verstärkt in das Interesse der Öffentlichkeit gerückt und hat auch im privaten Umfeld die Menschen für eine gesicherte Kommunikation sensibilisiert.

1.2 Zielsetzung

Diese wissenschaftliche Arbeit setzt sich damit auseinander, welche Sicherheitsvorkehrungen eine private Person treffen kann, damit Dritten der Inhalt ihrer Mails verwahrt bleibt und damit der Empfänger sicherstellen kann, dass er die Mail vollständig und unverändert erhalten hat. Darüber hinaus wird die Funktionsweise dieser Maßnahmen erläutert. Ergänzend wird auf den Aspekt der Authentizität eingegangen, d. h. ob der Kommunikationspartner wirklich derjenige ist, für den er sich ausgibt.

Ziel dieser wissenschaftlichen Arbeit ist die Untersuchung der verschiedenen Möglichkeiten zum Schutz der Daten in der E-Mail-Kommunikation sowie die Analyse ihrer Funktionsweise.

1.3 Aufbau der Arbeit

Abgrenzung hinsichtlich wissenschaftlicher Methoden. Z.B. bei Sicherheitsbedürfnissen tiefgreifende Analyse um diese festzulegen (vgl. Zielgruppenanalyse) Bzw. In Anlehnung an...(Unternehmen) hervorheben Was ist Sicherheitsniveau, Kategorie, Bedürfnis?

In Bezug auf die Datensicherheit existieren vier verschiedene Aspekte, die unabhängig voneinander betrachtet werden können. Um ein gemeinsames Grundverständnis für die weitere Arbeit zu bekommen, werden diese Aspekte im nächsten kurz erläutert.

Die von Privatpersonen versendeten Mails haben unterschiedliche Anforderungen an die Vertraulichkeit der Nachricht. Anhand dieser Anforderungen lassen sich Sicherheitsniveaus zuordnen, die in Kapitel 3 analysiert werden.

Nachdem ein Grundverständnis für die verschiedenen Aspekte in der Datensicherheit und die unterschiedlichen Sicherheitsniveaus aufgebaut wurde, werden im fünften Kapitel die Technologien und Verfahren zum Schutz der Daten in der E-Mail-Kommunikation untersucht. In diesem Kapitel werden die kryptographischen Grundlagen und die zwei wesentlichen Arten des Vertrauensmodell erläutert. Zudem werden verschiedene Verfahren und Protokolle für den

Schlüsselaustausch und für die Verschlüsselung von Information und Transport. Das Kapitel schließt mit einer Betrachtung des Namensdienstes DNS und seinen Sicherheit erhöhenden Erweiterungen ab.

Im sechsten Kapitel werden ausgewählte Mail-Provider in der Praxis dahingehend untersucht, ob sie die in dieser Arbeit untersuchten Technologien und Verfahren einsetzen bzw. als Option anbieten. Aus dieser Analyse wird eine Nutzwertanalyse erstellt, die die Anforderungen der verschiedenen Sicherheitsniveaus anhand der vorgestellten Provider übersichtlich in tabellarischer Form darstellt.

Das letzte Kapitel schließt die Arbeit thematisch mit einer Zusammenfassung und einem Ausblick über die gegenwärtigen und möglichen Entwicklungen ab.

2 Datensicherheit Einmaleins

Im Gegensatz zum Datenschutz, der den Schutz von und den vertrauensvollen Umgang mit persönlichen Daten thematisiert, wird unter Datensicherheit der Schutz von Daten in den Aspekten Verfügbarkeit, Vertraulichkeit und Integrität verstanden¹. In der IT-Sicherheit wird zusätzlich der Aspekt der Authentizität berücksichtigt.² In diesem Abschnitt werden diese Aspekte näher betrachtet, da diese für das Verständnis der vorgestellten Techniken im weiteren Verlauf der Arbeit notwendig sind.

Verfügbarkeit Unter Verfügbarkeit wird das Vorhandensein von Infrastruktur, Software, sämtliche IT-Dienstleistungen sowie -Funktionalitäten und Daten verstanden, so dass der Anwender bei Bedarf darauf zugreifen und diese nutzen kann. Um dies zu gewährleisten, muss verhindert werden, dass

- Daten verschwinden oder nicht zugreifbar sind, wenn sie gebraucht werden,
- Programme nicht funktionsbereit sind, wenn sie aufgerufen werden sollen,
- Hardware und sonstige notwendige Mittel nicht funktionsfähig oder gar verschwunden sind, wenn sie für die Verarbeitung benötigt wird.³

Integrität Unter der Integrität der Daten wird verstanden, dass die Daten bei der Übertragung nicht unbemerkt verändert werden können und folglich wie vom Absender vorgesehen übermittelt wurden. Bei diesem Aspekt geht es demzufolge um die Unversehrtheit der Nachricht.

Vertraulichkeit Unter Vertraulichkeit versteht man den Schutz der Nachricht vor unbefugtem Zugriff durch Dritte. Nur der vorgesehen Empfänger soll in der Lage sein, den Inhalt der Nachricht zu erfahren.

Authentizität Bei der Authentizität geht es um den Nachweis, dass die beteiligten Kommunikationspartner tatsächlich diejenigen sind, für die sie sich ausgeben.

¹BSI2014.

²Berliner2014.

³Berliner2014.

3 Sicherheitsniveaus

In den nachfolgenden Kapiteln dieser Arbeit werden verschiedene Möglichkeiten der Verschlüsselung von E-Mail Kommunikation vorgestellt und jeweils passende Sicherheitsniveaus zugeordnet.

Dabei erfolgt diese Zuordnung mit dem Ziel, einen optimalen Ausgleich zwischen Notwendigkeit und Aufwand der Verschlüsselung von E-Mails zu erhalten.

Gerade im Hinblick auf den Grad der Verschlüsselung bei der E-Mail Kommunikation ist es wichtig sich darüber bewusst zu werden, wie sensibel die Information ist, die man versenden möchte. Denn jede Verschlüsselung ist mit einem bestimmten Aufwand verbunden und folglich ist abzuwägen, welcher Verschlüsselungsaufwand dem Nutzer die zu versendende Information wert ist.

Der Wert einer Information ist durch das eigene Sicherheitsbedürfnis geprägt, welches jedoch von Person zu Person in unterschiedlicher Form ausgeprägt ist.

Daher ist es den Autoren nicht möglich, eine allgemein gültige Auflistung aller möglichen Szenarien der E-Mail Kommunikation bereitzustellen, aus welcher die Teilnehmer der Zielgruppe lediglich das richtige Szenario herausuchen müssen und dadurch den optimalen Grad der Verschlüsselung erhalten.

Stattdessen wird in Tabelle 1 eine Übersicht präsentiert, die es dem Nutzer erlaubt auf Basis seines eigenen Sicherheitsbedürfnisses und mit Hilfe festgelegter Kriterien für die Übermittlung einer ganz bestimmten Information ein geeignetes Sicherheitsniveau zu bestimmen.

Die Tabelle 1 stellt im Tabellenkopf vier verschiedene Sicherheitsniveaus dar: *Streng Vertraulich*, *Vertraulich*, *Privat* und *Öffentlich*. Dabei nimmt das Sicherheitsbedürfnis sowie der Verschlüsselungsaufwand von Streng Vertraulich bis Öffentlich ab.

In der ersten Spalte sind verschiedene Merkmale aufgelistet, welche es dem Nutzer ermöglichen sollen, ein geeignetes Sicherheitsniveau zu bestimmen. Alle weiteren Felder enthalten die Ausprägung des Merkmals innerhalb des jeweiligen Sicherheitsniveaus.

Stufe	4 Streng Vertraulich	3 Vertraulich	2 Privat	1 Öffentlich
Wert der Information, Schutzwürdigkeit	Äußerst hoch	Hoch	Gering	kein hoher Wert; kein Schutz notwendig
Personenbezogene Daten	Ja	Ja	Teilweise	Nein
Einfluss auf Privatsphäre	Äußerst hoch	Hoch	Gering	Nicht vorhanden
Autorisierter Personenkreis	Sender + Empfänger; evtl. zusätzlich engste Verwandte	Verwandtschaft	Freunde + Bekannte	Jeder
Auswirkung bei Integritätsverletzung	Äußerst hoch	Hoch	Gering	Nicht vorhanden
Analogie: Übermittlung Postweg	Einschreiben oder Verzicht auf Postweg und persönliche Übergabe	Doppelte Kuvertierung oder Einschreiben	Standard Brief	Postkarte
Häufigkeit des Niveaus	Sehr selten	Selten	Häufig	Oft

Tabelle 1: Sicherheitsniveaus

Der Wert der Information und deren Schutzwürdigkeit beschreiben, wie wertvoll die zu versendende E-Mail für einen nicht rechtmäßigen Empfänger ist und welche Notwendigkeit des Schutzes daraus folgt.

Der potentielle Schaden stellt das Ausmaß dar, welches eintritt für den Fall, dass die E-Mail durch Dritte (klassische Angreifer sowie der E-Mail Provider) gelesen wird. Dieser Schaden kann verschiedener Art sein. Zum Beispiel können daraus rechtliche Konsequenzen erfolgen, es kann zu einem finanziellen Verlust führen oder mit einer Schädigung des Images des Senders einhergehen.¹ Aus dem potentiellen Schaden lässt sich außerdem gut der Einfluss auf die eigene Privatsphäre ableiten.

Das Merkmal *Personenbezogene Daten* besagt, dass die zu versendende Information personenbezogene Daten enthält und daher grundsätzlich das Sicherheitsniveau *Vertraulich* zu wählen ist.² In Abhängigkeit von der Ausprägung der anderen Merkmale, kann als resultierendes Sicherheitsniveau auch *Streng Vertraulich* oder *Privat* ermittelt werden.

Der Autorisierte Personenkreis ist eine weitere Eigenschaft anhand derer der Nutzer ein passendes Sicherheitsniveau bestimmen kann. Grundsätzlich gilt: je wertvoller die Information, desto geringer ist der Personenkreis, der Einblick in die zu versendende E-Mail erhalten darf.³ Daraus

¹Reinhausen GmbH.

²TSE.

³TSE.

folgt, dass eine streng vertrauliche Nachricht ausschließlich zwischen dem Sender und dem Empfänger ausgetauscht wird und in der Regel keine weitere Person über den Inhalt erfahren darf. Eine Ausnahme an dieser Stelle sind allenfalls engste Verwandte. Dahingegen ist für eine Nachricht, deren Inhalt prinzipiell jedermann erfahren darf, das Sicherheitsniveau *Öffentlich* zu wählen.⁴

Die *Auswirkung bei Integritätsverletzung* beschreibt das eingetretene Ausmaß, wenn die E-Mail in die Hände eines Angreifers gelangt ist.

Eine weitere Möglichkeit ein geeignetes Sicherheitsniveau zu ermitteln ist die Überlegung, wie der Inhalt der E-Mail auf dem Postweg versandt werden würde. Für eine streng vertrauliche Information würde ein Einschreiben gewählt werden oder gänzlich auf den Postweg verzichtet und stattdessen die Nachricht persönlich überbracht werden. Dahingegen ist für Information, die ohne Bedenken auf einer Postkarte übermittelt werden können, das Sicherheitsniveau *Öffentlich* zu wählen

Das letzte Merkmal beschreibt das Aufkommen der einzelnen Sicherheitsniveaus. Streng vertrauliche Informationen sind sehr selten und am häufigsten werden öffentliche Nachrichten ausgetauscht.⁵

Anhand des nachfolgenden Beispiels soll der Umgang mit der Tabelle 1 verdeutlicht werden. Hierbei ist zu erwähnen, dass das resultierende Sicherheitsniveau auf Basis des beschriebenen Sicherheitsbedürfnisses ermittelt wurde und für die gleiche Information bei anderen Nutzern unterschiedlich ausfallen kann:

Herr Meier war vor kurzem in einen Auffahrunfall verwickelt, den ein unachtsamer Autofahrer verursacht hatte. Daraufhin brachte Herr Meier sein Fahrzeug in die Werkstatt und ließ ein Gutachten des Schadens erstellen. Dieses Gutachten möchte er nun zusammen mit seinen Kontodaten via E-Mail an die Versicherung des Unfallverursachers senden.

Der Wert dieser Information ist hoch, denn einerseits sind die Kontodaten in der Nachricht vorhanden. Andererseits ist in dem Gutachten Herr Meiers Anschrift angegeben und es lässt sich aus den Fotos und der Schadenshöhe des Gutachtens ableiten, dass Herr Meier einen Luxuswagen besitzt. Daraus wiederum lassen Rückschlüsse auf seine finanzielle Situation schließen. Der potentielle Schaden, der sich daraus ergibt, ist hoch bis äußerst hoch. Denn bei ausreichender krimineller Energie können nicht nur die Kontodaten missbraucht werden, sondern mit Hilfe der Anschrift kann der Wohnsitz von Herrn Meier ausgekundschaftet und beispielsweise bei seiner Abwesenheit in sein Anwesen eingebrochen werden.

Die Anschrift stellt personenbezogene Daten dar und ermöglicht einen hohen Einfluss auf die Privatsphäre von Herrn Meier. Der Autorisierte Personenkreis für diese Nachricht beschränkt sich auf den Sender (Herr Meier), den Empfänger (die Versicherung) sowie auf seine Frau und auf die Werkstatt, die das Gutachten erstellt hat. Seinen Freunden und Kollegen hat Herr Meier zwar auch von dem Unfall erzählt. Allerdings wissen diese keine genaueren Details hinsichtlich des Schadens und dessen Höhe.

Hätte die Versicherung den E-Mail Service nicht angegeben, so würde Herr Meier die Unterlagen des Gutachtens mit einem Standard-Brief versenden. Die Kontodaten würde er mittels

⁴Reinhausen GmbH.

⁵TSE.

Einschreiben verschicken.

Somit kann als Resultat für dieses Beispiel unter dem beschriebenen Sicherheitsbedürfnis ein Sicherheitsniveau von *Vertraulich* ermittelt werden. Welches Verschlüsselungsverfahren konkret für dieses Sicherheitsniveau anzuwenden ist, wird in den nachfolgenden Kapiteln beschrieben.

4 Technologien und Verfahren

4.1 Kryptographie Grundlagen

Die Kryptographie ist die Wissenschaftslehre, die sich mit den Verfahren sowie der Anwendung von Ver- und Entschlüsselung von Informationen befasst. Dabei bedient sie sich mathematischen Hilfsmitteln, um die Daten vor Dritten unzugänglich zu machen. In diesem Kapitel werden zunächst die grundlegende Funktionsweise der Verschlüsselung untersucht, die zum Verständnis der weiteren Kapitel notwendig sind. Anschließend werden verschiedene Verfahren beleuchtet, die eine verschlüsselte und geschützte Kommunikation ermöglichen.

4.1.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird sowohl zur Verschlüsselung und Entschlüsselung ein gemeinsamer Schlüssel verwendet. Dieser Schlüssel wird auch Shared Secret genannt. Mithilfe dieses Schlüssels und einem kryptographischen Algorithmus wird die Information des Absenders, auch als Klartext bezeichnet, verschlüsselt. Ein Algorithmus transformiert dabei einen Eingabeparameter in einen Ausgabeparameter. Im Fall eines kryptographischen Algorithmus handelt es sich um eine mathematische Vorschrift, die aus dem Klartext einen sogenannten Geheimtext berechnet. Diesen verschlüsselten Text kann der Empfänger mit dem selben Schlüssel, der zur Verschlüsselung verwendet wurde, entschlüsseln. Im elektronischen Mailverkehr wirkt sich die Funktionsweise der symmetrischen Verschlüsselung nachteilig auf deren Anwendung aus. Da beide Kommunikationspartner denselben Schlüssel benötigen, muss dieser zuvor ausgehandelt und übertragen werden. Dieser Umstand stellt ein Risiko bezüglich der Vertraulichkeit dar. Jeder, der über den Schlüssel verfügt, kann auf den Inhalt der Nachricht zugreifen. Dieses Sicherheitsrisiko wird durch die asymmetrische Verschlüsselung beseitigt.

4.1.2 Asymmetrische Verschlüsselung

Wie bei der symmetrischen Verschlüsselung kommt auch bei der asymmetrischen Verschlüsselung, die auch Public-Key-Kryptography genannt wird, ein kryptographischer Algorithmus zum Einsatz. Hierbei wird jedoch statt eines gemeinsamen Schlüssels ein Schlüsselpaar verwendet. Dieser besteht aus einem öffentlichen und einem privaten Schlüssel, die mathematisch zusammenhängen. Jeder, der verschlüsselte Nachrichten empfangen möchte, verfügt über ein solches Schlüsselpaar. Der private Schlüssel wird niemals bekanntgegeben, wohingegen der öffentliche Schlüssel jedem zugänglich gemacht werden kann. Obwohl die Schlüssel zusammenhängen, kann aus der Kenntnis des öffentlichen Schlüssels nicht auf den privaten Schlüssel geschlossen werden.¹ Soll eine Nachricht durch ein asymmetrisches Verschlüsselungsverfahren verschlüsselt verschickt werden, wird zunächst der öffentliche Schlüssel des Empfängers benötigt. Zusammen mit der Nachricht wird der Geheimtext erzeugt und an den Empfänger geschickt. Zum Entschlüsseln der Nachricht wird der private Schlüssel des Empfängers verwendet, der zu dem öffentlichen Schlüssel gehört, der bei der Verschlüsselung der Nachricht verwendet wurde.

¹Schmeh2013.

Mit diesem Verfahren wurde das Sicherheitsrisiko der symmetrischen Verschlüsselung gelöst, da der öffentliche Schlüssel zum Verschlüsseln jedem bekannt sein darf. Zur Entschlüsselung wird der dazugehörige private Schlüssel benötigt, der im Besitz des Empfängers ist und niemals veröffentlicht wird. Ein Sicherheitsrisiko ergibt sich jedoch aus der Tatsache, dass ein Dritter die Übertragung des öffentlichen Schlüssels unbemerkt abfangen kann und dem Absender stattdessen seinen öffentlichen Schlüssel überträgt. Damit ist er in der Lage, alle vom Absender verschlüsselten Nachrichten ohne dessen Kenntnis zu entschlüsseln. Daher muss "bei der Verwendung eines fremden Schlüssels [...] möglichst immer die Authentizität des Schlüssels geprüft bzw. sichergestellt werden."²

Zwei Aspekte sind im Zusammenhang mit der asymmetrischen Verschlüsselung erwähnenswert. Der im Jahr 1978 erfundene asymmetrische RSA-Algorithmus, der nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman benannt, hebt sich vor allem durch seine Einfachheit hervor³ und der Diffie-Hellman-Schlüsselaustausch. Mit diesem Protokoll, das Eigenschaften von asymmetrischer Verschlüsselung aufweist, können geheime Schlüssel problemlos über einen abgehörten Kanal übertragen werden. Nach Ablauf der Vereinbarung kennen nur beide Kommunikationspartner den vereinbarten Schlüssel⁴

4.1.3 Digitale Signaturen

Asymmetrische Verschlüsselungsverfahren ermöglichen, die menschliche Unterschrift in der digitalen Welt abzubilden. Diese Funktionalität wird mit digitalen Signaturen umgesetzt. Damit eine digitale Signatur den Anforderungen einer menschlichen Unterschrift erfüllt, müssen einige Bedingungen eingehalten werden:⁵

- Sie darf nicht zu fälschen sein.
- Ihre Echtheit muss überprüfbar sein
- Sie darf nicht unbemerkt von einem Dokument zum anderen übertragen werden können.
- Das dazugehörige Dokument darf nicht unbemerkt verändert werden können.

Diese Voraussetzungen dienen dazu, die Verbindlichkeit des Absenders sowie die Integrität der Nachricht zu gewährleisten. Beim Signieren verschlüsselt der Absender seine Nachricht mit seinem privaten Schlüssel. Die resultierende Nachricht ist die digitale Signatur. In der Regel wird beim Signieren aufgrund des Rechenaufwandes für lange Nachrichten nicht die gesamte Nachricht verschlüsselt, sondern ein sogenannter Hashwert. Hashwerte sind eine Zeichenfolge mit einer bestimmten Länge, die durch eine mathematische Einweg-Hashfunktion generiert werden. Diese Funktionen haben einen Eingabeparameter und berechnen daraus einen Hashwert. Aus der Kenntnis des Hashwertes oder der Hashfunktion lässt sich der Eingabeparameter nicht ableiten, wodurch die Integrität einer signierten Nachricht gewährleistet ist. Die signierte Nachricht wird im nächsten Schritt an den Empfänger geschickt. Dieser kann nun die Verbindlichkeit der Nachricht überprüfen, indem er die Signatur mit dem öffentlichen Schlüssel des Absenders

²Ertel2012.

³Ertel2012.

⁴Stephan2011.

⁵Schmeh2013.

entschlüsselt. Anschließend berechnet er den Hashwert der erhaltenen Nachricht und vergleicht diesen mit dem zuvor entschlüsselten Signatur des Absenders. Diese Überprüfung wird dabei auch Verifizierung genannt. Stimmen beide Werte überein, kann er sicher sein, dass die Nachricht von dem Absender stammt, da nur mit dessen privatem Schlüssel die Nachricht verschlüsselt werden konnte. Zusätzlich ist damit garantiert, dass die Nachricht vollständig und ungeändert beim Absender angekommen ist.

Durch die Anwendung des asymmetrischen Verschlüsselungsverfahrens beim Signieren bleibt die Authentizität der öffentlichen Schlüssels weiterhin ein Sicherheitsrisiko. Das Risiko besteht darin, dass „man einem öffentlichen Schlüssel nicht ansieht, wem er gehört“.⁶

4.1.4 Zertifikate

Bei den bisher genannten Verfahren wurde davon ausgegangen, dass der öffentliche Schlüssel wirklich dem beabsichtigten Kommunikationspartner gehört. Die Authentizität des öffentlichen Schlüssels ist durch Szenarien wie dem Man-In-The-Middle-Angriff nicht immer garantiert. Um die Authentizität des öffentlichen Schlüssels sicherzustellen, werden Zertifikate verwendet.

Ein Zertifikat ist ein elektronisches Dokument, das einer Person zugeordnet werden kann. Dieses Dokument enthält neben den persönlichen und weiteren Informationen des Inhabers dessen öffentlichen Schlüssel. Außerdem enthält ein Zertifikat eine Signatur über all den genannten Angaben. Das Signieren wird dabei von einer vertrauenswürdigen Instanz durchgeführt, die auch Certificate Authority (CA) oder Zertifizierungsstelle genannt wird.

Zum Versenden einer verschlüsselten Nachricht wird zunächst das Zertifikat vom Empfänger besorgt. Der Absender überprüft die Authentizität des öffentlichen Schlüssels des Empfängers, indem er die Signatur unter Verwendung des öffentlichen Schlüssels der CA verifiziert. Mit der Verifizierung ist gewährleistet, dass der öffentliche Schlüssel auf dem Zertifikat dem Zertifikatsinhaber gehört.

Das Sicherheitsrisiko bezüglich der Authentizität des öffentlichen Schlüssels der signierenden Zertifizierungsstelle wird gelöst, indem ein Zertifikat über den seinen öffentlichen Schlüssel erstellt wird, das von der CA selbst signiert wurde. Dieses Zertifikat wird als self-signed bezeichnet.

4.2 Public Key Infrastruktur

In Kapitel 4.1.4 Zertifikate wurde die Definition und die Funktionsweise von Zertifikaten betrachtet. Allerdings ist der Austausch selbiger nicht ohne weiteres möglich. Denn dafür müssen sich die beiden Kommunikationspartner „kennen und einen sicheren Weg für den Austausch finden“.⁷

An dieser Stelle setzt die so genannte Public Key Infrastructure (PKI) an, die eine Vertrauenskette darstellt und den Austausch von Zertifikaten zweier Kommunikationspartner erleichtern soll.

⁶Schmeh2013.

⁷BSI.

Bei der PKI handelt es sich um eine Hierarchie von Zertifikaten, die aus verschiedenen Elementen besteht. Auf der obersten Hierarchie Ebene steht die Wurzelinstanz, welcher auf einer oder mehrerer Unterebenen verschiedene CA untergeordnet sind, die wiederum die Zertifikate der Endanwender signieren.⁸

Die Wurzelinstanz wird durch die Policy Certification Authority (PCA) verkörpert, die für alle vertrauenswürdig ist und ein so genanntes Wurzelzertifikat erstellt.⁹

Alle weiteren Zertifikate dieser Vertrauenskette werden mit dem privaten Schlüssel des Wurzelzertifikats signiert

Dies bringt eine Reihe von Vorteilen mit sich. Zum einen können der PCA verschiedenartige CA untergeordnet sein. Beispielsweise könnte eine CA SSL-Zertifikate für Webserver signieren, eine weitere CA Secure/Multipurpose Internet Mail Extensions (S/MIME)-Zertifikate ausstellen und eine dritte CA für die E-Mail Kommunikation zuständig sein.

Zum anderen können verschiedene Sicherheitspolicies für unterschiedliche CAs hinterlegt werden. So stellt die eine CA Zertifikate unter Voraussetzung einer gültigen E-Mail Adresse aus, wohingegen eine andere CA erst nach Vorlage eines Personalausweises ein Zertifikat signiert.¹⁰

Ein dritter Vorteil liegt darin, dass mit Hilfe der PKI organisatorische Strukturen, zum Beispiel die einer Unternehmung, abgebildet werden können. In solchem Falle können verschiedene CA für unterschiedliche Standorte eines Unternehmens einberufen werden, die wiederum die Zertifikate der Mitarbeiter am jeweiligen Standort signieren und deren eigenes Zertifikat durch eine übergeordnete CA oder PCA signiert wurde.

Diese Vertrauenskette kann beliebig lang fortgesetzt werden, sodass zwei Kommunikationspartner sich nicht mehr gegenseitig kennen müssen um ihre Zertifikate einander auszutauschen, sondern es ausreichend ist, wenn das Zertifikat des Kommunikationspartners entlang der PKI von einer Instanz signiert wurde, die man selbst für vertrauenswürdig befindet.

Jedoch liegen genau in dieser Vertrauenswürdigkeit auch die Nachteile der PKI. Einerseits muss eine neue CA oder PCA erst einmal bekannt gemacht werden und auf diesem Weg vertrauen erlangen.¹¹

Andererseits kommt es immer wieder vor, dass CA angegriffen werden und somit auch gefälschte Zertifikate illegal signiert werden.

4.3 Web of Trust

Das Web of Trust ist ein Vertrauensmodell, bei dem sich die Nutzer gegenseitig vertrauen und somit ein netzartiges Modell entstehen lässt. Die Grundidee ist, dass die Nutzer dieses Modells gegenseitig ihre öffentlichen Schlüsseln signieren. Im Gegensatz zum hierarchischen Verfahren gibt

⁸Schwenk.

⁹ITWissen2012.

¹⁰Schwenk.

¹¹Schwenk.

es keine zentrale Zertifizierungsstelle. Die Funktionsweise des Web of Trust wird anhand eines Beispiels erläutert.

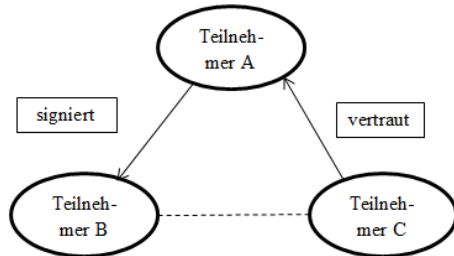


Abbildung 1: Web of Trust Vertrauensmodell¹²

Teilnehmer C möchte Teilnehmer B eine verschlüsselte Nachricht schicken. Dazu besorgt er sich zunächst das Zertifikat von Teilnehmer B. Dieser wurde zuvor von Teilnehmer A signiert. Da Teilnehmer C Teilnehmer A vertraut, beschafft sich Teilnehmer C den öffentlichen Schlüssel von Teilnehmer A und verifiziert mit diesem das Zertifikat von Teilnehmer B. Ist die Verifizierung erfolgreich, so kann Teilnehmer C den öffentlichen Schlüssel von Teilnehmer B vertrauen.

Bei diesem Modell wird zwischen zwei Arten des Vertrauens unterschieden. Einerseits existiert das Vertrauen in eine Person bzw. dessen Signatur. Andererseits besteht ein Vertrauen in einen signierten Schlüssel eines Dritten, der von einer vertrauensvollen Person signiert wurde. Beide Arten des Vertrauens können unabhängig voneinander existieren.

4.4 Schlüsselaustausch

Für die sichere Kommunikation ist ein sicherer Schlüsselaustausch die Ausgangsbasis um Angriffe zu verhindern. „erbei ist der geschützte Austausch geheimer Schlüssel symmetrischer Kryptosysteme von Interesse.“¹³

4.4.1 RSA - Rivest, Shamir und Adleman-Kryptosystem

Beim klassischen Schlüsselaustausch werden die Sitzungsschlüssel durch den Public-Key innerhalb des Server-Zertifikat übertragen.¹⁴ Dies geschieht mittels RSA(Rivest, Shamir und Adleman)-Kryptosystem (RSA)-Verfahren. Verschlüsselte Kommunikation ist jedoch nur sicher, solange die Schlüssel geheim bleiben. Die Gefahr beim klassischen RSA-PKI-Verfahren ist, dass vergangene Kommunikation nachträglich zu jedem Zeitpunkt entschlüsselt werden kann, sobald Angreifer in Besitz des Private-Key sind.

4.4.2 PFS - Perfect Forward Secrecy

Im Gegensatz zum klassischen RSA-Schlüsselaustausch ist es sinnvoller, die Sitzungsschlüssel zum Einen nicht mehr zu übertragen und zum Anderen unabhängig voneinander ständig neu zu generieren und bei Terminierung zu löschen. Realisiert wird dies durch die Protokoll-Eigenschaft

¹²Ertel2012

¹³Eckert2013.

¹⁴Boeck2013.

Forward Secrecy, die im Kryptographischen Fachjargon auch Perfect Forward Secrecy (PFS)¹⁵ genannt wird. Die „Forderung an die Verfahren und Protokolle zur Schlüsselerneuerung besteht darin dafür zu sorgen, dass die Kenntnis eines Schlüssels, also dessen Aufdeckung, nicht dazu führt, dass damit auch vorherige und nachfolgende Schlüssel direkt aufdeckbar sind.“¹⁶ Wie notwendig PFS geworden ist zeigen die jüngsten Ereignisse im Zusammenhang mit dem OpenSSL-Bug "Heartbleed", mit dem es sehr einfach war private Schlüssel von Servern auszulesen.¹⁷

Das Diffie-Hellmann-Schlüsselaustausch (DHE) Verfahren ermöglicht dabei als Basis die Aushandlung eines Sitzungsschlüssels bei dem die Kommunikationspartner verschiedene Nachrichten senden und sich auf einen Sitzungsschlüssel einigen können, ohne diesen je übertragen zu haben. Dieser Schlüssel ist auch nur für die aktuelle Verbindung gültig und wird anschließend gelöscht. Der Public-Key des Servers wird weiterhin übertragen, jedoch nur um den Schlüsselaustausch zu signieren. „geschlossene Sitzungen können somit im Nachhinein nicht mehr entschlüsselt werden.“¹⁸ Die Verschlüsselungsverfahren Transport Layer Security/Secure Socket Layer (TLS/SSL) und Internet Protokoll Security (IPsec) beherrschen bereits PFS.

Aufgezeichnete verschlüsselte Daten können somit bei Besitz des privaten Schlüssels nicht entschlüsselt werden. Zudem wird einfaches Belauschen einer aktiven Verbindung deutlich erschwert, denn es müsste die gesamte Kommunikation mit einem gezieltem Man in the Middle (MITM)-Angriff manipuliert werden. Für diese Problematik gibt es wiederum moderne Ansätze wie DNS-based Authentication of Named Entities (DANE) (Vgl. Kapitel 4.7.2), die in Kombination mit PFS aktuell bei der Verschlüsselung von Verbindungen höchsten Sicherheitsansprüchen entsprechen, indem zusätzlich die Authentizität der Kommunikation gewährleistet wird.

Nachteile gibt es lediglich bei der Verwendung des bereits überholten, und seit Jahren als geknackt bekannte DHE-Verfahren, denn dabei verzögert sich zusätzlich der Verbindungsaufbau. Die Schlüssellänge ist Minimum 1024 Bit, und längere Schlüssel mit 2048 oder 4096 Bit sind dabei nicht sicherer.¹⁹ Der moderne Nachfolger mit elliptischen Kurven Elliptic Curve Diffie-Hellman (ECDH) gilt aktuell als sicher und benötigt dabei weniger als 1024 Bit und verzögert den Verbindungsaufbau nur unweigerlich.

Obwohl es Forward Secrecy bereits seit 1999 im Transport Layer Security (TLS) Standard 1.0²⁰ vorgesehen ist, und somit essentieller Bestandteil von Verschlüsselung ist, hat sich PFS noch nicht als Standard durchgesetzt.²¹ Dies liegt zum einen an den Webservern. Mit einem Apache Webserver ist nur eine Länge des Modulo (Modulus) von 1024 Bit vorgesehen. Beim Einsatz von DHE würden Provider damit ihre Server daher unsicher betreiben. Zum Anderen sind es auf Client-Seite die Browser die DHE bzw. ECDH lange Zeit ignoriert haben. Der Internet Explorer verschlüsselte nur nach DSS, wobei der de-facto Standard für Verschlüsselung bereits RSA war. Opera unterstützte lediglich das überholte DHE-Verfahren und Safari priorisiert Forward

¹⁵Boeck2013.

¹⁶Eckert2013.

¹⁷Zhu2014.

¹⁸Schulz2014.

¹⁹Boeck2013.

²⁰Boeck2013.

²¹SSL Labs.

Secrecy niedrig und bevorzugt bei gegebener Option sogar die unverschlüsselte Kommunikation. Lediglich Firefox und Chrome unterstützen PFS in vollem Umfang.

Für die E-Mail Kommunikation ist PFS essenziell für die Befriedigung hoher Sicherheitsbedürfnisse. Um die dazugehörigen Sicherheitsniveaus abzudecken müssen E-Mail-Server Forward Secrecy unterstützen. Im August 2013 war PFS nur sporadisch verbreitet in der E-Mail-Kommunikationslandschaft.²² Mittlerweile wird von vielen E-Mail-Providern auch PFS angewandt. Die Umsetzung erfolgt jedoch noch zu zögerlich, wenn man die Tatsache betrachtet, dass PFS im Zusammenhang mit Heartbleed der letzte Funken Hoffnung für betroffene Nutzer war, das zumindest vergangene Kommunikation nicht entschlüsselt werden kann.²³

4.5 Informationsverschlüsselung

Für hohe Sicherheitsanforderungen entscheidend ist die Vertraulichkeit und Integrität der Datenkommunikation zwischen zwei Endpunkten. In der E-Mail-Kommunikation wird dies mit sog. Ende-zu-Ende-Verschlüsselung (englisch End-to-End-Encryption (E2EE)) und den Diensten S/MIME und Pretty Good Privacy (PGP) realisiert, die im Nachgang beleuchtet werden. Es gibt mittlerweile verschiedene Möglichkeiten E2EE umzusetzen. Im Grunde müssen durch die Nutzer jedoch Einstellungen in den E-Mailprogrammen wie Thunderbird, Outlook oder Mail.app vorgenommen werden oder zusätzliche Software installiert werden. Demzufolge besteht ein erhöhter Einrichtungsaufwand für die Nutzer zur Sicherstellung der Vertraulichkeit und um in Sicherheitsniveaus der Stufe 3 oder 4 (Vgl. s. Tab. 1 „Sicherheitsniveaus“, S. 5) zu kommunizieren. Erste E-Mail-Provider gehen zum Teil eigene Wege wenn es um die Gestaltung von benutzerfreundlicher E2EE geht. Google bspw. arbeitet an einer Erweiterung im eigenen Chrome Browser um mittels OpenPGP zu verschlüsseln.²⁴ Aber auch kleinere Anbieter sind an der Umsetzung für ihre Webmailer²⁵ und somit E2EE deutlich benutzerfreundlicher zu machen.

4.5.1 PGP - Pretty Good Privacy

Im Jahre 1991 wurde dem US Senat ein Gesetz vorgelegt, welches vorsieht, dass jede Verschlüsselungssoftware staatliche Zugriffe ermöglichen müsse. Daraufhin entwickelte Phil Zimmermann noch im selben Jahr die erste Version von PGP, die diese Hintertür nicht bot.²⁶

Die Softwarefamilie Pretty Good Privacy stellt „...Dienste zur digitalen Signatur und zur Verschlüsselung von Nachrichten...“²⁷ zur Verfügung und ist damit für die Vertraulichkeit der Informationen verantwortlich.

Allerdings wurden diese Bemühungen erst nach sieben Jahren Entwicklung, diversen Anklagen gegen Zimmermann und die anderen Beteiligten sowie das Herausbringen zahlreicher nationaler

²²Schulz2014.

²³Zhu2014.

²⁴Somogyi2013.

²⁵Posteo2013.

²⁶Schwenk.

²⁷Mueller2011.

(US-Amerikanischer) und internationaler Versionen als internationaler Standard *OpenPGP* angesehen.²⁸

Um die Integrität einer E-Mail zu gewährleisten, wird zuerst ein zufälliger Schlüssel (Shared Secret) erzeugt. Anschließend wird die E-Mail Nachricht mit diesem symmetrisch verschlüsselt. Danach wird das Shared Secret selbst mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt und der verschlüsselten E-Mail voran gehangen. Soll die E-Mail mehrere Empfänger erreichen, so wird der letzte Schritt wiederholt.²⁹

Ein entsprechendes Programm zur Implementierung des OpenPGP Standards ist GnuPG, GNU Privacy Guard (GPG). Dieses Tool ist für gängige E-Mail-Clients verfügbar und ermöglicht die Verschlüsselung und den Schlüsselaustausch so benutzerfreundlich wie möglich zu gestalten. Denn der Austausch der öffentlichen Schlüssel muss noch manuell erfolgen.

Ein Vorteil von PGP liegt darin, dass es sowohl auf dem dezentralen Vertrauensmodell Web of Trust als auch auf dem hierarchischen Vertrauensmodell der PKI basiert.³⁰ Außerdem werden die verschlüsselten Nachrichten vor dem Versenden komprimiert und verringern dadurch nicht nur Traffic, sondern verbessern somit auch den Schutz vor Angreifern.³¹ Des Weiteren steht der Sourcecode von PGP öffentlich zur Verfügung und kann beliebig auf Richtigkeit überprüft werden.³²

Der öffentliche Sourcecode stellt jedoch gleichzeitig auch einen Schwachpunkt dar, da es somit Angreifern ermöglicht wird, potenzielle Schwachstellen und Sicherheitslücken in der Implementierung aufzufinden. Vor allem mit der Zunahme neuer Features wird dieser Nachteil erheblicher, was durch Angriffe von Senderek, Klíma und Rosza bewiesen wurde.³³

Ein weiterer Nachteil liegt in der Schwierigkeit beim Austausch von Schlüsselinformationen für E2EE. Dies muss noch manuell mit Hilfe von Software erfolgen und ist daher noch nicht Standard heutiger E-Mail-Kommunikation. Es gibt zwar die Möglichkeit private Schlüssel durch Dienste³⁴ zu verteilen, jedoch ist diese Methode umstritten. Sie bietet zwar Ende-zu-Ende Verschlüsselung, allerdings ist der eigentliche Sinn des privaten Schlüssels verfehlt, wenn der Dienst bzw. Provider diesen für den Nutzer bestimmt und auf dem eigenen Server zwischenspeichert. Der Anwender hat keinen Einfluss auf den privaten Schlüssel und ist damit nicht Eigentümer dieses Schlüssels, der in Folge dessen kein Private Key ist.

4.5.2 S/MIME - Secure / Multipurpose Internet Mail Extensions

Die bislang betrachteten Verfahren bieten keine Möglichkeit einer E2EE. PGP hat als erstes Protokoll diese Lücke gefüllt. Mit S/MIME kam 4 Jahre später ein zweiter Standard hinzu.³⁵

²⁸Schwenk.

²⁹Schwenk.

³⁰Schwenk.

³¹Schwenk.

³²Schwenk.

³³Schwenk.

³⁴Bspw. iMessage von Apple für Instant Messaging

³⁵Duevel.

S/MIME ist eine Erweiterung des MIME Datentyps, der für die Signierung und/oder Verschlüsselung von Nachrichten entwickelt worden ist. Bislang konnten E-Mails nur im ASCII-Zeichensatz versendet werden. Mit dem Anbruch des digitalen Zeitalters stieg jedoch die Forderung auch andere Datentypen austauschen zu können. S/MIME setzt dieses Bedürfnis um.³⁶

Damit ein Nutzer S/MIME verwenden kann, benötigt er ein X.509 Zertifikat. Dieses wird in seiner einfachsten Form kostenlos von einer CA ausgestellt.³⁷

Das eigene Zertifikat kann Nutzer mit anderen austauschen, indem er es einer signierten E-Mail anfügt. Ein E-Mail Client kann dieses automatisch in seine Zertifikatsdatenbank ablegen. Der genaue Prozess hierfür ist im Schwenk³⁸ beschrieben.

Hat sich der Absender für die Verschlüsselung via S/MIME entschieden, sucht der Mail Client automatisch in der Zertifikatsdatenbank nach einem Zertifikat, welches die E-Mail Adresse des Empfängers enthält. Sollte ein solches Zertifikat nicht gefunden werden, wird der Nutzer darüber informiert, dass eine S/MIME Verschlüsselung nicht möglich sei. Ist ein entsprechendes Zertifikat vorhanden, wird die E-Mail hybrid verschlüsselt.³⁹

Um die Lesbarkeit von S/MIME signierten E-Mails auch für Nutzer zu gewährleisten, die dieses Verfahren nicht verwenden, stehen zwei verschiedene Datentypen zur Verfügung. Auf eine genauere Beschreibung soll an dieser Stelle verzichtet und stattdessen auf den Schwenk⁴⁰ verwiesen werden.

Der Vorteil von S/MIME liegt darin, "dass Verschlüsselung und Signatur genauso einfach zu bedienen sind, wie z.B. [...] das Anfügen eines Attachments"⁴¹. Außerdem wird S/MIME durch viele Browser by Default unterstützt.⁴² Durch die zwei verschiedenen Datentypen, können S/MIME signierte Nachrichten auch von E-Mail Clients interpretiert werden, die dieses Verfahren nicht verwenden.

³⁶Schwenk.

³⁷Duevel.

³⁸Schwenk.

³⁹Schwenk.

⁴⁰Schwenk.

⁴¹Schwenk.

⁴²Duevel.

4.6 Transportwegverschlüsselung

Das Secure Socket Layer (SSL)-Protokoll wurde zunächst durch die Firma Netscape entwickelt, um die Kommunikation über Hypertext Transfer Protokoll (HTTP)-Verbindungen abzusichern.⁴³ SSL kann auf der Sitzungs- und Präsentationsschicht des Open System Interconnection (OSI)-Referenzmodells angesiedelt werden und setzt meist auf dem Transmission Control Protocol (TCP) auf. Es hat die Aufgabe den darüber liegenden Schichten die Möglichkeit für eine authentifizierte, integritätsgeschützte und verschlüsselte Kommunikation zu geben.⁴⁴ Die Version SSL 3.0 hat sich mittlerweile als de facto Standard im Internet durchgesetzt und wird von allen gängigen Browsern unterstützt.

Das TLS-Protokoll kann als Weiterentwicklung von SSL 3.0 angesehen werden und liegt aktuell in der Version 1.2 vor. Da beide Protokolle in ihren Kernkonzepten übereinstimmen werden sie häufig synonym verwandt. Da TLS jedoch eine Weiterentwicklung von SSL ist, werden dort einige Erweiterungen eingeführt sowie unsichere Verfahren zur Berechnung von Message Authentication Code (MAC)-Werten durch neuere Varianten ersetzt.

Beide Protokolle bestehen aus mehreren Schichten bzw. Unterprotokollen wobei das Record- und das Handshakeprotokoll von besonderer Bedeutung sind. Das Record-Protokoll ist für die Fragmentierung, Authentifizierung mittels MAC und Verschlüsselung der zu übertragenden Daten zuständig. Mittels des Handshakeprotokolls werden Sitzungen zwischen den Kommunikationspartnern hergestellt. Dies bedeutet, dass die Kommunikationspartner durch den Austausch von Zertifikaten authentifziert werden können und alle Informationen, die zur Berechnung des Shared Secret für die symmetrische Verschlüsselung der Daten benötigt werden, ausgetauscht werden. Abbildung 2 verdeutlicht den schematischen Ablauf eines solchen Sitzungsaufbaus unter Verwendung von RSA für den Schlüsselaustausch.

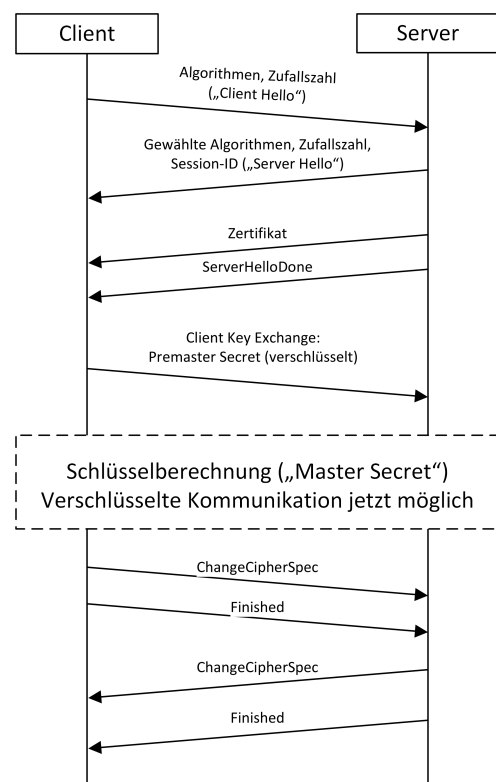


Abbildung 2: Handshake-Protokoll mit RSA⁴⁵

Durch die flexible Gestaltung des Handshake-Protokolls wird gleichzeitig auch die Komplexität von TLS/SSL stark erhöht. Dies hat zur Folge, dass durch die hohe Komplexität nicht mit Sicherheit alle Schwachstellen beim Design des Protokolls entfernt werden konnten. Außerdem ist zu bedenken, dass TLS/SSL aufgrund seiner weiten Verbreitung ein lohnendes Ziel für Angriffe

⁴³Eckert2013.

⁴⁴Eckert2013.

⁴⁵Sorge2013

ist. Die Sicherheit des Protokolls hängt dabei stark von den genutzten kryptologischen Methoden ab. Außerdem ist zu beachten, dass es sich, aufgrund der Ansiedlung des Protokolls unterhalb der Anwendungsschicht, nur um eine Verschlüsselung der transportierten Nutzdaten auf dem Transportweg handelt. Die Daten werden am Kommunikationsendpunkt entschlüsselt und anschließend an die entsprechende Anwendung weitergereicht. Dies bedeutet für die Anwendung im Bereich des E-Mailversands, dass die Nachrichten weiterhin im Klartext auf den Servern der Mailprovider vorliegen und von jedem, der berechtigten oder unberechtigten Zugang zu diesen erhält, ausgelesen werden können. Im Sinne der definierten Sicherheitsniveaus ist die SSL-Verschlüsselung daher auf der zweitniedrigsten Stufe anzusiedeln, da das Mitlesen der versandten Mails zwar erschwert, aber nicht unmöglich gemacht wird.

Auch die Authentifizierung der Kommunikationspartner mittels Zertifikaten weist dieselben Schwachstellen durch die Vertrauensbeziehung zu bekannten CAs, die unzureichend gesichert sind, auf.

4.7 DNS - Domain Name System

Das Domain Name System (DNS) ist ein wichtiger Dienst im Internet, da er dafür zuständig ist, gut merkbare Domainnamen in Internet Protocol (IP)-Adressen, und umgekehrt, aufzulösen. Um diese Auflösung bewerkstelligen zu können ist DNS in einer Baumstruktur aufgebaut.

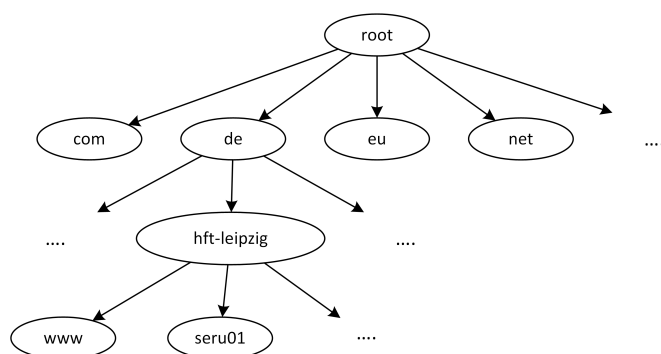


Abbildung 3: Beispielhafte Abbildung der Baumstruktur des DNS⁴⁶

Wie in Abbildung 3 veranschaulicht, ist auf der obersten Ebene der Knoten „root“ zu finden. Dies ist sozusagen die Wurzel des DNS und hier finden sich auch die Root-Server des DNS. Auf der nächsten Ebene kommen die Top-Level-Domain (TLD), anschließend folgen die Second-Level-Domains und zum Aufbau einer gängigen Unified Resource Locator (URL) für HTTP fehlt noch eine weitere Ebene, die den Hostnamen enthält. Soll ein Domainnamen aufgelöst werden, so fragt der Host zunächst einen Root-

Server. Dieser sendet ihm die Adresse des für die entsprechende TLD zuständigen Nameservers mit, an die der Client eine erneute Anfrage stellt. Auch der Nameserver der TLD verweist den Client an für die Second-Level-Domain zuständigen Nameserver. Auf diese Weise kann der Client den dargestellten Baum traversieren, bis er die gewünschte Information erhält. Die für diese Auskünfte benötigten Datensätze werden in sogenannten DNS-Records abgelegt. Das Problem ist hierbei, dass allein mit den DNS-Records nicht die Authentizität des Absenders und damit auch nicht die Integrität der Daten sicher gestellt werden kann. Dies wird jedoch für eine sichere E-Mailkommunikation benötigt, da auch die Domainnamen der Mailserver einer Zone über DNS-Records vom Typ „MX“ aufgelöst werden. Dies wird beim sogenannten DNS Cache Poisoning ausgenutzt und der Cache eines DNS-Servers manipuliert. Zumeist werden

⁴⁶Sorge2013

dabei mittels gefälschter Pakete an einen DNS-Server falsche Zuordnungen von Domainnamen auf IP-Adressen hinterlegt, um ein Opfer auf den Server des Angreifers umzuleiten.

4.7.1 DNSSEC - Domain Name System Security Extensions

Bei Domain Name System Security Extensions (DNSSEC) handelt es sich um eine Sicherheits-erweiterung des DNS. Sie beruht auf der Einführung weiterer DNS-Records. Unter anderem gibt es einen Recordtyp, der einen öffentlichen Schlüssel enthält und einen weiteren, der die Signatur eines Resource Records enthält. Ein autoritativer Nameserver kann eine Zone an einen anderen Nameserver delegieren und hält dann einen Verweis auf den entsprechenden Nameserver vor. Dadurch gibt es pro Zone des DNS maximal einen Zone Signing Key (ZSK) mit dem die Resource Records dieser Zone signiert werden, dies ist jedoch nicht zwingend notwendig. Mithilfe dieser Schlüssel und Signaturen kann nun eine Zertifikatskette aufgebaut werden. Ein Kritikpunkt an DNSSEC ist die hohe Komplexität des Systems, die durch den Aufbau der Zertifikatsketten und dem aufwändigen Austausch der Schlüssel auf Zonenebene entsteht. Diese ist jedoch der benötigten Kompatibilität mit bestehenden Systemen geschuldet und momentan alternativlos.⁴⁷ DNSSEC ist im Prinzip eine eigene PKI deren Hauptschlüssel Root DNSSEC Key die Non-Profit-Organisation Internet Corporation for Assigned Names and Numbers (ICANN) verwaltet.⁴⁸ Der „Hauptschlüssel und damit die DNSSEC-PKI [kann] als vertrauenswürdig [angesehen werden]“. ⁴⁹ Entscheidender Grund hierfür sind die 21 Trusted Community Representatives (TCR) die an der Erstellung des root key und der Signierungsprozesse partizipieren.

4.7.2 DANE - DNS-based Authentication of Named Entities

Die Basis für die Applikation DANE stellt DNSSEC und soll dabei die Schwachstellen von TLS beim Verschlüsseln des Datentransport entfernen. Denn die Authentizität der verwendeten Zertifikate kann nicht immer gewährleistet werden, und somit besteht die Gefahr der kompromittierten Daten durch MITM-Angriffe oder DNS-Cache-Poisoning. Die Schwachstellen der Zertifikatsprüfung und -aussteller⁵⁰ Stellen benötigt. Lediglich das DNS der Empfängerdomain benennt das gültige Zertifikat. Die somit veröffentlichte Prüfsumme aus dem Server-Zertifikat des Ziels kann durch den sendenden Server zutreffend identifiziert werden.

Die Aufgabe von DANE besteht darin TLS-Zertifikate über das DNS automatisch zu verteilen und zu prüfen. Dabei ist DANE nicht auf E-Mail Protokolle beschränkt sondern ist vielmehr für sämtlichen verschlüsselten Datenverkehr einsetzbar. Serverbetreiber tragen den Hash (Fingerabdruck) vom eigenen Public Key in die DNS-Zone ein damit das eigene Zertifikat prüfbar wird. Ein Sender erhält bei einer DNSSEC gesicherten DNS-Anfrage den passenden Transport Layer Security Authentication (TLSA)-Record. Für die Zertifikatsprüfung wird anschließend aus dem empfangenen PublicKey des TLS-Verbindungsaufbau auf dem Sender der Hash berechnet. Ist der Fingerabdruck dem Hash aus der DNS-Abfrage identisch ist die Verbindung vertrauensvoll. Ein durchgängig verifizierter Transport ist allerdings nur möglich wenn alle

⁴⁷Sorge2013.

⁴⁸Koetter2014.

⁴⁹Koetter2014.

⁵⁰Koetter2014.

beteiligten Mail-Server TLSA-Records vorhalten. Wenn eine Prüfstelle keinen besitzt „müssen [die Server] auf ungeprüftes TLS zurückfallen oder gar unverschlüsselt kommunizieren“⁵¹ Bisher ist DNSSEC noch kein Durchbruch gelungen. Aber die Situation für identifizierte, sichere E-Mail-Kommunikation ist dank DANE deutlich besser, denn „die Verwendung [...] ist u.a. schon bei IPsec, Secure Shell (SSH), PGP und S/MIME angedacht,“⁵² und für Hypertext Transfer Protokoll Secure (HTTPS) bereits 2012 standardisiert worden. Die Simple Mail Transfer Protokoll (SMTP)-Standardisierung ist in der Finalisierungsphase. Wenn sich DANE durchsetzt ist die Kommunikation nicht nur unter E-Mail-Verbünden wie E-Mail made in Germany (EmiG) gewährleistet, sondern auch mit der restlichen Welt. Bisher scheitert DANE allerdings an der Unterstützung der Browser, von denen kein gängiger DANE ohne Add-on umsetzt.

⁵¹Koetter2014.

⁵²Koetter2014.

5 E-Mail-Sicherheit in der Praxis

5.1 Nutzwertanalyse E-Mail-Provider

Die nachfolgende Nutzwertanalyse besitzt die Auswahl der Oberkriterien Vertraulichkeit und Integrität, Authentizität sowie sicherheitsrelevante Aspekte.

<Hier Nutzwertanalyse beschreiben und einbetten, ggf. im Anhang darauf verweisen> SSL-Labs-Test und CheckTLS-Test beschreiben und als Beleg nutzen

Kriterien	Gewichtung	Yahoomail		Googlemail		Hotmail		T-online		Web.de		GMX		mailbox.org		Posteo	
		NW	gew. NW	NW	gew. NW	NW	gew. NW	NW	gew. NW	NW	gew. NW	NW	gew. NW	NW	gew. NW	NW	gew. NW
Vertraulichkeit & Integrität	40%	4,6	1,84	5	2	2,8	1,12	5,2	2,08	6,2	2,48	6,2	2,48	8,6	3,44	6,5	2,6
Transportverschlüsselung Mailempfang	30%	6	1,8	6	1,8	3	0,9	7	2,1	7	2,1	7	2,1	10	3	7	2,1
Transportverschlüsselung Mailversand	30%	6	1,8	6	1,8	3	0,9	7	2,1	7	2,1	7	2,1	10	3	7	2,1
Zertifikat	10%	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1
E2EE Webmail	10%	0	0	4	0,4	0	0	0	0	0	0	0	0	0	0	3	0,3
Einrichtung E2EE	20%	0	0	0	0	0	0	0	0	5	1	5	1	8	1,6	5	1
Authentizität	30%	0	0	0	0	0	0	4,9	1,47	4,9	1,47	4,9	1,47	7,5	2,25	7,5	2,25
Digitale Signatur Webmail	20%	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Einrichtung Digitale Signatur	10%	0	0	0	0	0	0	0	0	0	0	0	0	5	0,5	5	0,5
Mailserver-Authentizität	70%	0	0	0	0	0	0	7	4,9	7	4,9	7	4,9	10	7	10	7
Sicherheitsrelevante Aspekte	30%	2,3	0,69	1,3	0,39	1,1	0,33	0,3	0,09	1	0,3	1	0,3	7,0	2,1	7,4	2,22
Verschlüsselte Speicherung	15%	0	0	0	0	0	0	0	0	0	0	0	0	8	1,2	8	1,2
Sicherheitsinformationen	25%	1	0,25	0	0	0	0	0	0	4	1	4	1	7	1,75	7	1,75
Keine E-Mailauswertung	25%	0	0	0	0	0	0	0	0	0	0	0	0	10	2,5	10	2,5
Sicherheits-Zusatzfunktionen	25%	7	1,75	4	1	4	1	0	0	0	0	0	0	5	1,25	5	1,25
Transparenzbericht	10%	3	0,3	3	0,3	1	0,1	3	0,3	0	0	0	0	3	0,3	7	0,7
Gesamt	100%	2,53		2,39		1,45		3,64		4,25		4,25		7,79		7,07	

Tabelle 2: Nutzwertanalyse der Provider

5.2 Provider Vergleich

5.2.1 Internationale Provider

Im Rahmen der Nutzwertanalyse wurden unter anderem drei der bekanntesten internationalen E-Mail Provider betrachtet: Yahooemail, Gmail und Hotmail. Die folgenden Aussagen treffen auf alle Provider gleichermaßen zu, sofern nicht ein E-Mail Anbieter explizit genannt wird.

Vertraulichkeit und Integrität

Alle betrachteten E-Mail Anbieter erhalten eine gute Punktzahl für die Transportwegverschlüsselung. Gmail und Yahoo schneiden gegenüber Hotmail etwas besser ab, da sie sowohl PFS für moderne Browser als auch die neuesten Versionen der TLS/SSL Protokolle unterstützen. Hotmail hingegen bietet PFS gar nicht an und unterstützt lediglich TLS 1.0 und SSL 3.0. Für die eingesetzten Zertifikate erhalten alle Provider wiederum volle Punktzahl.¹

Zwar haben seit den Enthüllungen von Edward Snowden zu den Machenschaften der National Security Agency (NSA) und anderen Geheimdiensten die meisten E-Mail Provider die Initiative ergriffen und auf sicherere Verfahren umgestellt². Ein voll umfänglichen Schutz durch eine E2EE wird bislang jedoch noch nicht geboten. Einzig und alleine Google hat bereits für seinen E-Mail Dienst ein AddOn in einer Alpha Version entwickelt, mit Hilfe dessen eine PGP Verschlüsselung für den Webmailer ermöglicht werde.³ Eine Beschreibung für die Einrichtung einer E2EE unter Verwendung eines Mail Clients war nicht aufzufinden.

Authentizität

Im Bereich der Authentizität schneiden alle drei betrachteten internationalen E-Mail Provider schlecht ab. Weder Gmail, noch Hotmail oder Yahooemail unterstützen eine digitale Signatur für ihre Webmailer. Darüber hinaus ist bei keinem der Anbieter eine Beschreibung für die Einrichtung einer digitalen Signatur für externe Mail-Clients zu finden.

Auch die Untersuchung der Mailserver-Authentifizierung führte zu schlechten Ergebnissen, wie der DNSSEC Analyzer von Verisign bestätigt.⁴

Sicherheitsrelevante Aspekte

Ein wesentlicher Bestandteil des Geschäftsmodells von Gmail, Hotmail und Yahooemail besteht darin, die Kommunikation seiner Nutzer zu analysieren.⁵ Daher ist es nicht verwunderlich, dass die Anbieter es sich vorenthalten in die E-Mails ihrer Nutzer schauen zu können⁶. Personalisierte Werbung ist ein erstes Indiz für diese Sicherheitslücke und wird in allen drei Fällen

¹vgl. Anhang SSL Reports

²vgl. Anhang SSL Reports

³Kirsch.

⁴vgl. Anhang DNSSEC Reports

⁵Kirsch.

⁶Schwan.

angewendet. Daraus lässt sich auch die Annahme schließen, dass die E-Mails nicht verschlüsselt gespeichert werden. Es konnten zwar keine Quellen herangezogen werden, die diese Annahme untermauern. Dafür wurden jedoch auch keine Quellen gefunden, die das Gegenteil beweisen. Laut einer Berichterstattung auf RTL ist die Situation bei Hotmail sogar verschärft:

Laut einem Bericht des 'Guardian' half der Software-Konzern (Microsoft, Anm. des Verf.) der NSA, die Verschlüsselung von Daten durch Nutzer seiner Dienste zu umgehen. So habe Microsoft vor dem Start des neuen Web-Mail-Portals 'Outlook.com' sichergestellt, dass die NSA stets einen Zugriff auf die Informationen bekommen könne, schrieb die britische Zeitung. Das Blatt beruft sich dabei auf Dokumente des Ex-Geheimdienst-Mitarbeiters Edward Snowden. In einem internen Schreiben heißt es demnach, die Behörde habe über das Überwachungsprogramm 'Prism' Zugriff auf E-Mails bei den Microsoft-Diensten 'Hotmail', 'Live' und 'Outlook.com'.⁷

Circa ein dreiviertel Jahr später wird ein weiterer Vorfall veröffentlicht, in welchem Administratoren sich direkten Zugang zu den Mailinhalten der Nutzer verschafft hätten.⁸

Darüber hinaus wurden auf den Seiten der Provider keinerlei Sicherheitsinformationen gefunden. Einzig und allein von Yahoo! wird ein kurzer Abschnitt zum Thema Phishing bereitgestellt. In Bezug auf das Bereitstellen von Sicherheits-Zusatzfunktionen können die internationalen Mail-Anbieter etwas Punkten. Alle bieten eine 2-Faktor Authentifizierung an. Außerdem hat der Nutzer die Möglichkeit sich eine Liste mit jeglichen externen Anwendungen und Webseiten anzeigen zu lassen. Mit dieser erhält er einen Überblick darüber, welche App Zugriff auf welche Nutzerdaten hat. Yahoo! kann zusätzlich mit einer Wegwerfadresse, einem Anmeldesiegel (vgl. Abbildung 4) sowie dem selbst entwickelten DomainKeys Identified Mail (DKIM) Verfahren überzeugen. DKIM basiert auf asymmetrischer Kommunikation und stellt die Authentizität von E-Mail Absendern sicher.⁹



Abbildung 4: Sicherheitsniveaus

Um das Vertrauen der Nutzer in die Provider wieder zu stärken, veröffentlichen Yahoo! und Googlemail so genannte Transparenzberichte.¹⁰ In diesen wird dargestellt, welche Behörden welche Art von Auskunft bei den Providern ersucht haben. Microsoft folgt dem Trend und hat bereits angekündigt, die Behördenanfragen für seinen E-Mail Dienst in den Transparenzbericht des Konzerns mit aufzunehmen.¹¹

⁷Guardian.

⁸Mailbox2014Microsoft.

⁹DKIM.

¹⁰Lokshin.

¹¹Herget.

5.2.2 EmiG - E-Mail made in Germany

EmiG ist eine Initiative der größten deutschen E-Mail Provider GMX, web.de und T-Online, die zusammen über 53% (Stand: 2013) der aktiven E-Mail-Konten in Deutschland betreiben.¹² Zusammen mit den Teilnehmern der freenet AG, 1&1 Internet AG und STRATO AG¹³ deckt EmiG ca. zwei Drittel der aktiven E-Mail Konten in Deutschland ab.

Das Projekt wurde im August 2013 als Reaktion der damaligen NSA-Äffäre ins Leben gerufen und hat das Ziel E-Mails zwischen den teilnehmenden Providern auf dem Transportweg mit TLS/SSL verschlüsselt versendet werden. Seit April 2014 ist das Projekt umgesetzt.

Die Nutzwertanalyse (s. Kap. 5.1 „Nutzwertanalyse E-Mail-Provider“, S. 21) wird im Folgenden zusammenfassend für die Provider der Dienste *GMX*, *web.de* und *T-online* beschrieben. Unterschiede, die sich auch auf die Bewertung auswirken werden explizit beschrieben.

Vertraulichkeit und Integrität

Bei den Providern der EmiG-Initiative ist die Vertraulichkeit durch die TLS-Transportverschlüsselung gegeben. Die Transportverschlüsselung ist allerdings nur untereinander garantiert. Die Anwender besitzen keine TLS-Garantie wenn E-Mails von oder zu Providern außerhalb des Verbunds gesendet oder empfangen werden.

Die Ergebnisse des SSL-Test (s. Kap. 5.1 „Nutzwertanalyse E-Mail-Provider“, S. 21) sind für die drei Provider ähnlich gut. GMX und WEB unterstützen Forward Secrecy mit den meisten Browsern, T-Online hingegen lässt den Schlüsselaustausch für ältere Browser über RC4 zu. Für die Anwender die innerhalb der EmiG Initiative E-Mails versenden bzw. empfangen ist die Vertraulichkeit des Kommunikationspartner im Webmailer und Outlook ersichtlich. Die Anwender sehen in der Adresszeile die E-Mail-Adresse mit einem grünen Haken versehen, sofern sie im EmiG-Verbund sind, und bekommen so visualisiert, dass die E-Mail transportverschlüsselt versendet wird. Ein zusätzlicher Gewinn an Benutzerfreundlichkeit.¹⁴

Die Integrität der E-Mail-Inhalte sind für EmiG-Provider von unterschiedlicher Bedeutung. End-to-End-Encryption (E2EE) ist mit keinem Webmail-Angebot der Provider möglich.

Das liegt an einer komplizierten Implementierung und kaum existierenden Ansätze für eine Realisierung von PGP im Webmail-Service. Im *Hilfe und Support* Bereich von T-Online ist generell keinerlei Hilfe zur Einrichtung von E2EE mittels PGP oder S/MIME zu finden. Auch wenn hierfür eine externe Mail-Applikation verwendet werden müsste, könnte technisch versierten Anwendern eine Hilfestellung bei der Einrichtung von E2EE

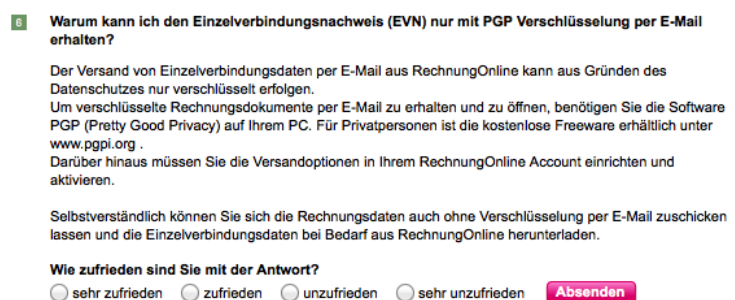


Abbildung 5: T-Online Hilfe: PGP

¹²Brandt13.

¹³Die 1&1 Internet AG ist wie GMX und web.de Teil des United-Internet-Konzern, sowie die STRATO AG eine Tochter des Betreiber von T-Online, der Deutschen Telekom AG ist.

¹⁴Zivadino14-1.

bereit gestellt werden. Lediglich ein Hinweis über Einzelverbindungs-nachweise und weshalb diese nur PGP-Verschlüsselt versendet werden dürfen ist zu finden. (s. Abb. 5 „T-Online PGP“, S. 25) Eine Information, dass es sich um Ende-zu-Ende-Verschlüsselung handelt ist dem Suchergebnis nicht zu entnehmen.

Die Provider web.de und GMX stellen dem Nutzer eine solche Hilfestellung gut sichtbar in einem eigenen Menüpunkt bereit. (s. Abb. 6 „Web.de PGP“, S. 26) Im Angebot von T-Online wird dem Nutzer, aufgrund fehlender PGP-Unterstützung, bei der Signierung von E-Mails in externen Mailanwendungen nicht geholfen. Web.de und GMX helfen zwar bei der Einrichtung von PGP, weisen jedoch nicht darauf hin, dass durch den Einsatz von PGP und E-Mail-Signierung auch die Authentizität des Empfänger und Sender ohne Verschlüsselung sichergestellt werden kann.

Generell haben die Provider der United Internet Gruppe eine informative Sicherheits-Hilferubrik. Anwenden wird bei der Einrichtung von PGP in der Mailapplikation Thunderbird aktiv unterstützt. Für die Applikationen Microsoft Outlook oder Mail.app für Mac besteht jedoch keine Hilfestellung. Auch eine Begründung hierfür ist nicht zu finden.

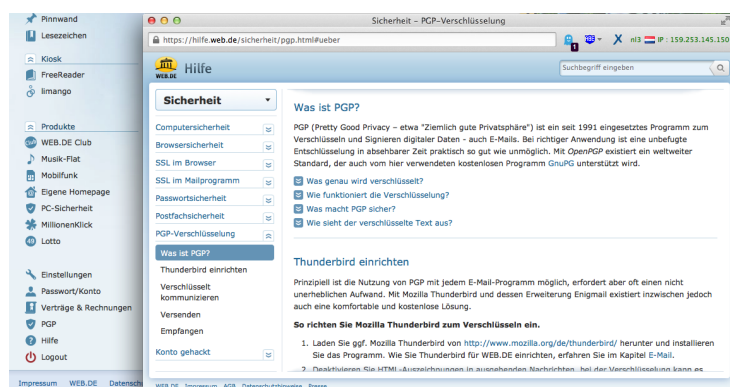


Abbildung 6: Web.de Hilfe: PGP

Authentizität

Die Serverseitige Authentizität der wird mittels dem selbst entwickelten, proprietären Verfahren *Inter Mail Provider Trust (IMPT)* sichergestellt. Dabei prüfen die Mail-Server der Teilnehmer beim Mail-Versand und -Empfang die Client- und Server-Zertifikate gegen die herausgebende CA, sowie gegen die Infrastrukturlisten. Sollten dabei Inkonsistenzen auftreten wird der Versand abgelehnt.

Dieses Vorgehen erinnert an ein geschlossene Variante von DANE (s. Kap. 4.7.2 „DANE - DNS-based Authentication of Named Entities“, S. 19), welches ähnlich zur Sicherstellung der Authentizität verfährt. Alle Partner der Initiative setzen PFS ein¹⁵ und damit eine Eigenschaft um einem höheren Schutzbedarf in zu entsprechen.¹⁶

Der Verzicht auf den offenen Standard DANE als Standard-Instrument zur Sicherstellung der Authentizität hat gewiss Nachteile für die Nutzer. Mit Inter Mail Provider Trust existiert jedoch für den E-Mail-Versand unter den EmiG-Partnern ein ähnlicher Schutz, der allerdings auch nicht immer die Authentizität der verwendeten SSL-Zertifikate gewährleisten kann.¹⁷ Die Vorgehensweise zur Entwicklung einer proprietären Lösung ist daher durchaus kritisch zu hinterfragen. United Internet möchte ggf. den Einsatz von DNSSEC und DANE in einem Review-Prozess einer Neubewertung unterziehen.¹⁸

¹⁵ Zivadino14-1.

¹⁶ Zivadino14-2.

¹⁷ Zivadino14-1.

¹⁸ Zivadino14-2.

Sicherheitsrelevante Aspekte

Für die Mails auf den EmiG-Servern der EmiG-Provider besteht keine separate verschlüsselte Speicherung der E-Mails, insofern dies durch den Nutzer nicht selbst geschehen ist. (s. Kap. 4.5.1 „PGP - Pretty Good Privacy“, S. 14) Festplatten werden nicht verschlüsselt um bei Diebstahl oder Beschlagnahme das Auslesen der Inhalte zu verhindern. E-Mails sind für Administratoren der Provider, als auch eventuell unberechtigte Dritte, die sich Zugang auf den Servern verschafft haben einsehbar.

Die Mails werden durch Viren-Scanner, Spam-Filter und wahrscheinlich Analyse-Algorithmen untersucht und ausgewertet.¹⁹ Dazu stimmt der Nutzer den entsprechenden Datenschutz Passagen in den AGBs zu. Diese gewähren den Anbietern das „[...] persönliche Daten [...] elektronisch verarbeitet werden, [und der Anbieter berechtigt ist] anonymisierte Nutzerinformationen Dritten - darunter Anzeigekunden - [...] zur Verfügung zu stellen. Die anonymisierten Daten dürfen [...] zur Erstellung von Statistiken und Trenderkennungen sowie zur Qualitätssicherung und Marktforschung verwendet werden.“²⁰

Sicherheitsbezogene Informationen sind innerhalb des Webmail-Angebote von United Internet gut auffindbar, könnten allerdings weiterführende Informationen und Anleitungen enthalten. T-Online ist beim Angebot von Informationen bzgl. E-Mailsicherheit für eigene Kunden deutlich ausbaufähig.

Einen kleinen Vorsprung besitzt T-Online gegenüber United Internet beim Versuch einen Transparenzbericht zu veröffentlichen, der Anfragen von Behörden offenlegen soll. Allerdings ist der Transparenzbericht ein halbherziger Versuch offener, transparenter Kommunikation, denn die exakte Anzahl der Verkehrsdatensätze bleibt weiterhin unklar.²¹ United Internet erarbeitet derzeit noch an einem Modell, um Transparenz zu schaffen.²²

Zusammenfassung

EmiG ist im Prinzip ein deutlicher Gewinn an Sicherheit für die Kunden im Vergleich zur Zeit vor dem Projekt. Mit Rückblick auf die Zeit vor der Initiative und dem damals gebotenen Sicherheitsniveau im Jahre 2013 ist dieser Gewinn an Sicherheit jedoch kein stark herausragendes Merkmal. Höher als Sicherheitsniveau-Stufe 2 ist die E-Mail-Kommunikation nicht zu bewerten, die auch erst seit dem TLS-Verbund erreicht wird.²³ Dafür fehlen weiterhin Provider-übergreifende Bemühungen interessierten Anwendern die E2EE näher zu bringen. Es könnte durchaus mehr Energie in die Umsetzung von E2EE im Webmailer aufgewendet werden, wie es im Vergleich zu anderen Anbietern geschieht (Vgl. s. Kap. ?? „??“, S. ?? und s. Kap. 5.2.3 „mailbox.org“, S. 30)

Vor allem der Entschluss zur Inselfösung IMPT und Vernachlässigung von Standards wie DNSSEC werfen Fragen auf. Ob DANE tatsächlich eine Chance auf eine spätere Implementierung bekommt bleibt abzuwarten, denn bisher ist mit IMPT die Kommunikation mit internatio-

¹⁹**Kurz13.**

²⁰**Web2012.**

²¹**Beuth14.**

²²**Boehm14.**

²³Zum Vergleich: 2013 war Stufe 1 das maximale Sicherheitsniveau für Anwender der größten E-Mail-Provider Deutschlands.

nen Anbieter und garantierter Transportverschlüsselung rhetorisch ausgeschlossen.²⁴ Fakt ist bisher das die Aufnahme und Erstzertifizierung neuer Mail-Provider, die am Beitritt der Initiative interessiert sind, Kosten in Höhe von 9.500 bis 30.000 Euro²⁵ verursacht und mit zusätzlichen manuellen Aufwand bei der Konfiguration der SMTP-Mailserver verbunden sind. Daher wächst die Initiative nur langsam.

Auch Vorwürfe, dass EmiG scheinbar keine kleineren E-Mail-Provider zulassen möchte wurden veröffentlicht.²⁶ Ob EmiG tatsächlich ein offener Verbund ist, oder sich nur als solcher verkauft bleibt zur Zeit auch unbeantwortet.

Inwieweit die Initiative letztendlich die Hauptaufgabe hat Anwendern ein deutliches Plus an Sicherheit zu gewährleisten werden erst die nächsten Monate zeigen können. Die geplante Einreichung der Initiative, das eigens entwickelte Verfahren als Request for Comments (RFC) beim Internet Engineering Task Force (IETF) „(...)“, dem für Internet-Standards verantwortlichem Gremium, (...)“²⁷ standardisieren zu lassen ist der richtige Weg zur Beantwortung vieler Fragen. Ob andere E-Mail-Provider diesen Standard nutzen werden, wenn man zusätzliche Kosten und Aufwand betrachtet, bleibt abzuwarten. Auch die Kompatibilität zwischen DNSSEC und IMPT kann ein Entscheidungskriterium sein.

Bisher betreibt EmiG einen hohen Marketingaufwand mit breitangelegter TV Kampagne und dazugehörigen, typisch unklaren Äußerungen, hinter denen vermutlich auch strategisch, politische Interessen der Anbieter liegen.

Die Haltung, Anwender auf der Internetseite²⁸ nicht über alle Sicherheitsaspekte zu informieren und im Werbespot²⁹ den Großteil technisch nicht versierter Anwender in falscher Sicherheit wiegt hinterlässt ebenfalls Fragen. Für eine sichere und Provider-unabhängige E-Mail-Kommunikation sollte es im Informationszeitalter nicht 15 Jahre für den Einsatz von Sicherheitsstandards benötigen. Ob EmiG sich nur als offener Verbund verkauft oder tatsächlich ist, wird gleichermaßen in den nächsten Monaten zuverlässiger beantwortet werden können.

5.2.3 Alternative Provider

Als alternative Provider werden zwei kleine Anbieter, die bereits aktiv am Markt sind, untersucht. Hierbei handelt es sich um die beiden in Berlin ansässigen Provider *Posteo* und *mailbox.org*. Diese Anbieter positionieren sich bewusst im Kontrast zu den großen Mail Providern als Alternativen, die einen hohen Wert auf die Privatsphäre ihrer Kunden legen und daher möglichst wenig Daten ihrer Nutzer protokollieren und die Mails der Nutzer nicht auswerten.³⁰

posteo

Posteo ist ein kleiner, deutscher Mailprovider, der 2009 gegründet wurde und von der Posteo e.K. betrieben wird.³¹ Laut eigenen Angaben verzeichnet das Unternehmen einen Nutzerzuwachs um

²⁴Zivadino14-1.

²⁵Zivadino14-3.

²⁶Zivadino14-4.

²⁷Zivadino14-2.

²⁸<http://www.e-mail-made-in-germany.de/Verschluesselung.html>

²⁹<http://www.e-mail-made-in-germany.de/Wechseln.html>

³⁰Posteo2013a; Mailbox2014.

³¹Posteo2013b.

mehr als 100% pro Jahr.³² Er probiert sich bewusst von den Konkurrenten abzusetzen durch das Angebot von innovativen Sicherheitsfunktionen und die garantierte Werbefreiheit. Die Kosten deckt Posteo dadurch, dass für die Nutzung des Dienstes eine monatliche Gebühr erhoben wird. Diese kann auf unterschiedliche Weise bezahlt werden und kann durch die Löschung der Beziehungsdaten zwischen Zahlungseingang und Postfach nach erfolgter Zahlung nicht zurückverfolgt werden. Dadurch soll eine anonyme Nutzung des Postfachs ermöglicht werden, da auch bei der Registrierung keine persönlichen Daten angegeben werden müssen.³³ Nachfolgend wird die durchgeführte Nutzwertanalyse für Posteo beschrieben.

Vertraulichkeit und Integrität Der Zugriff auf den Server von Posteo erfolgt immer über eine mit TLS und PFS gesicherte Verbindung, unabhängig davon, ob ein Mailprogramm oder der Webmailer genutzt wird. Dies wird durch den Einsatz von HTTP Strict Transport Security (HSTS) erzwungen. Beim eigentlichen Versand und Empfang von Mails geht Posteo jedoch nicht ganz so strikt vor und nutzt eine verschlüsselte Verbindung lediglich, wenn dies durch den Kommunikationspartner ebenfalls unterstützt wird. Das Zertifikat, das Posteo bei der Transportverschlüsselung einsetzt, ist ein sogenanntes erweitertes Zertifikat, das es dem Anwender auf einen Blick ermöglichen soll den Betreiber der aufgerufenen Webseite bzw. des Servers zu identifizieren.³⁴

Im Webmailer ist es momentan nicht möglich, die Mails mittels E2EE zu versenden, aber die sichere Speicherung des privaten Schlüssels des Nutzers noch Probleme, so dass nicht feststeht zu welchem Zeitpunkt diese Funktion zur Verfügung stehen wird.³⁵ Über die Verschlüsselungsmöglichkeiten per PGP und S/MIME und die damit verbundenen Vor- und Nachteile in Bezug auf anonyme Kommunikation wird auf der Webseite von Posteo ausführlich informiert. Eine konkrete Hilfestellung zur Einrichtung der Verschlüsselungsverfahren zur Nutzung mit einem Mailprogramm wird bisher nicht gegeben. Stattdessen wird auf die Seite von *Netzpolitik.org*³⁶ und dem Mailprogramm *Thunderbird* der Mozilla Foundation³⁷ verlinkt.

Authentizität Auf die Möglichkeiten, die Mails vor dem Versand digital zu signieren und wie dies im Mailprogramm durchgeführt werden kann, werden auf der Posteo-Seite ein paar Informationen gegeben. Eine Anleitung, wie das Signieren durchgeführt wird sucht der Nutzer allerdings vergeblich. Auch die Tatsache, dass eine Verschlüsselung im Webmailer bisher nicht möglich ist, lässt darauf schließen, dass ebenfalls keine Signaturen erstellt werden können. Eine direkte Information hierzu gibt es aber nicht. Bei der Authentifizierung ihrer Server ist Posteo jedoch hochaktuell und hat als einer der ersten³⁸ Anbieter in Deutschland DANE umgesetzt.³⁹

³²Posteo2013b.

³³Posteo2013a.

³⁴Posteo2013c.

³⁵Posteo2013c.

³⁶<https://netzpolitik.org/2013/anleitung-so-verschlusselt-ihr-eure-e-mails-mit-pgp>

³⁷http://www.thunderbird-mail.de/wiki/Mailverschlüsselung_mit_S/MIME

³⁸Auch Mailbox.org setzt seit Mai 2014 DANE ein(Mailbox2014a), so dass nicht zweifelsfrei belegt werden kann, wer diese Funktion zuerst genutzt hat.

³⁹Zivadino14-5.

Zusätzliche sicherheitsrelevante Aspekte Im Bereich der zusätzlichen sicherheitsrelevanten Aspekte kann Posteo durch die Verschlüsselung seiner Festplatten mit Advanced Encryption Standard (AES) punkten. Hierdurch sind die gespeicherten Mails vor Zugriffen geschützt, falls die Festplatten geklaut oder beschlagnahmt werden sollten. Die Mails selbst werden jedoch nicht extra verschlüsselt gespeichert, wodurch sie für Personen, die sich unberechtigten Zugriff auf die Server im laufenden Betrieb verschaffen können, auslesbar sind. Die Möglichkeit für eine zusätzliche Verschlüsselung der Mails ist jedoch ebenfalls für die Zukunft geplant.⁴⁰ Insgesamt wäre es wünschenswert, wenn Posteo bei dem geäußerten Anspruch auf hohen Datenschutz und Wahrung der Privatsphäre seiner Nutzer, diesen gut verständliche Anleitungen für die Einrichtung und Nutzung von Verschlüsselungsverfahren und digitalen Signaturen geben würde. Wie bereits zu Beginn der Ausführungen zu den alternativen Providern erwähnt garantiert Posteo seinen Nutzern Werbefreiheit. Aus diesem Grund werden die Mails weder beim Versand noch beim Empfang durch Posteo analysiert. Eine weitere Sicherheitsfunktion ist das sogenannte IP-Stripping. Hierbei wird die IP-Adresse des Absenders durch die IP-Adresse des Mailservers von Posteo ersetzt. Somit ist eine Rückverfolgung zum Absender aufgrund der IP-Adresse nicht möglich.⁴¹ Auch was die Veröffentlichung eines Transparenzberichts angeht ist Posteo vorbildlich und hat als erster deutscher Anbieter diesen veröffentlicht und damit die großen Konkurrenten wie beispielsweise die Deutsche Telekom AG (DTAG) als Betreiber von T-Online unter Zugzwang gesetzt.

mailbox.org

Mailbox.org startete im Februar 2014 als neuer E-Maildienst der Heinlein Support GmbH, die mit JPBerlin bereits seit über 20 Jahren als Internet Service Provider (ISP) auftritt und E-Mailpostfächer anbietet. Die Abgrenzung zur Konkurrenz erfolgt, wie auch bei Posteo, über die explizite Betonung des Datenschutzes und der Privatsphäre des Kunden. Dies ist unter anderem am Werbespruch zu erkennen, der „damit Privates privat bleibt“ lautet. Auch bei Mailbox.org gibt es kein kostenloses Angebot zur Nutzung des E-Maildienstes, dafür aber ebenso das Versprechen von Werbe- und insbesondere auch hohem Spamschutz.⁴² In den folgenden Abschnitten wird die Durchführung der Nutzwertanalyse für Mailbox.org beschrieben.

Vertraulichkeit und Integrität Bei Mailbox.org können die Nutzer nur auf verschlüsseltem Weg auf die Server zugreifen um ihre Mails abzurufen. Hierbei werden die neuesten Versionen von TLS mit PFS unterstützt und der Aufbau von unverschlüsselten Verbindungen durch den Einsatz von HSTS unterbunden. Auch beim Versand und Empfang von Mails bietet Mailbox.org die Möglichkeit eine unverschlüsselte Kommunikation zu unterbinden.⁴³

⁴⁰Posteo2013c.

⁴¹Posteo2013a.

⁴²Mailbox2014.

⁴³Mailbox2014b.

Bei der Information der Nutzer über die Einrichtung und Nutzung von Verschlüsselungsmethoden zur E2EE bietet Mailbox.org eine Anleitung für viele Plattformen und auch einen gut verständlichen Stiftfilm zur Erklärung, wie E2EE funktioniert. Eine Nutzung der E2EE im Webmailer ist aber wie bei den anderen Providern nicht möglich.

Authentizität Zur Authentifizierung seiner Mailserver setzt Mailbox.org DANE ein und unterstreicht hiermit seinen Anspruch als Anbieter für die sichere Kommunikation per E-Mail. Aus dem gleichen Grund scheint es selbstverständlich, dass Mailbox.org ebenfalls Informationen zu den Möglichkeiten der digitalen Signatur vermittelt. Doch auch hier wäre eine genauere Anleitung zur Nutzung dieser wünschenswert um diese technische Maßnahme für die Nutzer einfach einsetzbar zu machen. Dazu würde auch eine Implementierung dieser Funktion im Webmailer gehören. Hierzu sind aber auf der Website des Mailproviders keine Angaben zu finden, ob eine Umsetzung geplant ist.

Zusätzliche sicherheitsrelevante Aspekte Mit der Möglichkeit der Zweifaktorauthentifizierung mit einem One Time Password (OTP) hebt sich Mailbox.org ebenfalls von vielen Konkurrenten ab. Zur Nutzung dieser Funktion muss ein USB-Gerät, ein sogenannter Yubikey, mit dem Account verbunden werden. Dadurch ist es möglich, sich auch von unbekannten und damit potenziell unsicheren Rechnern sicher an seinem Account im Webfrontend anzumelden. Ebenfalls positiv hervorzuheben ist die regelmäßige Berichterstattung über Probleme und Erweiterungen des Funktionsumfangs, auch gerade im Hinblick auf neu eingeführte Sicherheitsmaßnahmen.

5.2.4 De-Mail

=====COMMENT

Absprache Keyserver bei De-Mail

=====COMMENT END

Seitdem am 3. Mai 2011 das De-Mail-Gesetz in Kraft getreten ist, können die darauf basierenden De-Mail-Dienste genutzt werden. Das ursprünglich unter dem Projektnamen „Bürgerportale“ entwickelte Konzept hat zum Ziel, eine elektronische und rechtlich verbindliche Kommunikation zu ermöglichen. Dadurch werden die Vorteile der „*Schnelligkeit der E-Mail in Verbindung mit der Sicherheit eines Briefes und der Nachweis eines Einschreibens*“⁴⁴ genutzt. Obwohl die Nutzung von De-Mail nicht komplizierter als die Nutzung herkömmlicher E-Mails ist, sind beide Kommunikationsmittel nicht interoperabel, d. h. De-Mail-Nachrichten können nicht als herkömmliche E-Mails empfangen und versendet werden und umgekehrt. De-Mail-Nachrichten können jedoch Empfängern anderer De-Mail-Anbieter verschickt werden. Die per De-Mail verschickten Nachrichten bleiben im Verbund der De-Mail-Provider. Um als De-Mail-Anbieter akkreditiert zu werden, müssen künftige De-Mail-Anbieter sich eine Reihe von Sicherheitsanforderungen erfüllen und einen Prüfungsprozess absolvieren. Nach erfolgreicher Prüfung werden die Anbieter durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditiert.

Um sich in das De-Mail-Konto anzumelden gibt es grundsätzlich zwei verschiedene Anmeldeverfahren. In der Stufe „normal“ meldet sich der Nutzer mit seinem Benutzernamen und Passwort an.

⁴⁴BSIDeMail.

Meldet sich der Nutzer im „hohen“ Sicherheitsmodus an, wird zusätzlich zum Benutzernamen und Passwort ein sogenannter Token benötigt. Bei dieser sogenannten Zwei-Faktor-Authentifizierung wird der Anmeldevorgang durch einen Gegenstand, der im Besitz des Nutzers ist, zusätzlich gesichert. Abhängig von dem Anmeldeverfahren können verschiedene Versandoptionen genutzt werden:

- **Versandbestätigung:** Bei Wahl dieser Option wird eine Versandbestätigung vom Versanddienst des Absenders erzeugt und dem Absender per Nachricht zugestellt.
- **Eingangsbestätigung:** Bei Wahl dieser Option wird eine Zugangsbestätigung vom Postfachdienst des Empfängers erzeugt und dem Absender sowie dem Empfänger der ursprünglichen Nachricht per Nachricht zugestellt.
- **Persönlich:** Die Wahl dieser Option bedeutet, dass das erforderliche Anmeldeniveau des Empfängers mindestens "hoch" sein muss, um die Nachricht lesen zu können. Um diese Option wählen zu können, muss auch das Anmeldeniveau des Absenders "hoch" sein.
- **Absender-bestätigt:** Mit der Wahl dieser Option bringt der Absender zum Ausdruck, dass er sich verbindlich an den von ihm versendeten Nachrichteninhalte gebunden fühlt. Um diese Option wählen zu können, muss das Anmeldeniveau des Absenders "hoch" sein. Der Empfänger erfährt, dass der Absender beim Versand der Nachricht "hoch" angemeldet war.⁴⁵

Bei den ersten beiden Optionen „*sendet der De-Mail-Anbieter Ihnen [den Nutzer, Anm. der Autoren] eine qualifiziert elektronisch signierte Bestätigung darüber, wann und an wen Sie die De-Mail verschickt haben bzw. wann die Nachricht im Postfach des Empfängers einging*“.⁴⁶

Die derzeit bekannteren De-Mail Diensteanbieter sind die Telekom mit Ihrem eigenen Mailservice und die United Internet AG mit 1&1, web.de und gmx.de. Weitere Diensteanbieter sind die Mentana-Claimsoft GmbH sowie die T-Systems International GmbH⁴⁷.

Die drei Sicherheitsaspekte Vertraulichkeit, Integrität und Authentizität sind im Umgang mit De-Mail wesentlich⁴⁸. Im Folgenden werden diese drei Aspekte im Zusammenhang mit De-Mail näher untersucht.

Bevor De-Mail genutzt werden kann, wird ein De-Mail-Konto mit einer De-Mail-Adresse benötigt, nach dessen Registrierung eine Identifikation notwendig ist. Die Überprüfung der Identität erfolgt beim De-Mail-Anbieter. Der Nutzer muss sich dabei mit einem gültigen Ausweisdokument identifizieren lassen. Auch eine Identifizierung über die „*Online-Ausweisfunktion (eID-Funktion) im neuen Personalausweis (nPA)*“⁴⁹ ist möglich. Dieses Verfahren dient dazu, die Authentizität des Nutzers festzustellen.

⁴⁵BSIMerkmale.

⁴⁶BSIDeMail.

⁴⁷BSIDiensteanbieter.

⁴⁸BSIGGrundlagen.

⁴⁹BSIDeMail.

De-Mails werden auf dem ganzen Transportweg verschlüsselt übertragen, um die Mail vor unberechtigten Zugriff zu schützen. Auf dem Transportweg liegt die De-Mail für einen kurzen Zeitabschnitt unverschlüsselt vor, wenn sie den De-Mail-Anbieter erreicht.⁵⁰ In diesem Moment wird die De-Mail auf Schadsoftware untersucht. Sollte die De-Mail Schadsoftware enthalten, wird der Empfänger beim Erhalt der Nachricht davor gewarnt. Im Vergleich zur herkömmlichen Mail-Verschlüsselung werden auch die Metadaten verschlüsselt.⁵¹ Darüber hinaus existiert die Möglichkeit, eine End-to-End-Verschlüsselung zu nutzen. Dabei müssen beide Kommunikationsteilnehmer eine separate Verschlüsselungssoftware verwenden. Durch diese zusätzliche Maßnahme sind auch die De-Mail-Anbieter nicht in der Lage, die Nachrichten zur Schadsoftware-Überprüfung kurzzeitig zu entschlüsseln.

Die Integrität einer De-Mail gewährleistet, indem der De-Mail-Anbieter nach Eingang der versendeten Nachricht eine Prüfsumme oder elektronische Signatur erzeugt und diese dem Empfänger übermittelt. Die De-Mail kann daher während der Übertragung nicht modifiziert werden, ohne dass der Empfänger es merkt.

Kritik

Linus Neumann vom Chaos Computer Club (CCC) im Jahre 2013 in zwei Stellungnahmen zu Gesetzesvorhaben der Bundesregierung bzgl. der rechtsverbindlichen Kommunikation Kritik gegenüber den gegebenen Anforderungen von De-Mail geäußert.⁵² Zum einen sei die Authentizität beim Versenden einer De-Mail-Nachricht nicht immer gegeben. Lediglich einmalig bei der Registrierung wird die Identität des Nutzers überprüft.⁵³ Beim Versenden erfolge keine weitere Überprüfung der Authentizität. Werden die Zugangsdaten abgefangen, hätten Angreifer Zugriff auf das Konto und Nachrichten als vermeintlich rechtmäßigen Absender verschicken. Selbst die Anmeldung mittels der Zwei-Faktor-Authentifizierung biete nicht genügend Schutz, da nach einmaliger Anmeldung „mehrere De-Mails ohne erneute Authentifizierung gesendet werden“⁵⁴ können. Dazu bieten sich Angriffsszenarien wie dem Man-in-the-Middle-Angriff an, um an die Zugangsdaten zu gelangen.

Ein ähnliches Problem ergibt sich im Zusammenhang mit der Integrität einer De-Mail-Nachricht. Nach dem Versand der Nachricht wird die De-Mail vom De-Mail-Anbieter signiert. Dies garantiert zwar, dass die Nachricht unterwegs nicht verändert wurde. Mittels den oben beschriebenen Angriffsszenarien kann der Angreifer eine Nachricht verschicken und der Empfänger geht fälschlicherweise davon aus, dass die Nachricht unverändert wurde.⁵⁵

Die Vertraulichkeit durch die Verschlüsselung sei zwar gegeben, durch die kurzzeitige explizite Entschlüsselung beim De-Mail-Anbieter sei diese nicht konsistent.⁵⁶ Unbefugte hätten theoretisch

⁵⁰BSIDeMail.

⁵¹BSIMerkmale.

⁵²Neumann2013a; Neumann2013b.

⁵³Neumann2013b.

⁵⁴Neumann2013b.

⁵⁵Neumann2013b.

⁵⁶Neumann2013a.

die Möglichkeit, an den Inhalt der Nachricht zu gelangen.

Laut Neumann sei es noch nicht zu spät für die Nachbesserung des De-Mail-Gesetzes.⁵⁷ Er empfiehlt eine standardmäßige Ende-zu-Ende-Verschlüsselung⁵⁸ sowie die Einhaltung der Vorgaben des Signaturgesetzes.⁵⁹

⁵⁷Neumann2013a.

⁵⁸Neumann2013a; Neumann2013b.

⁵⁹Neumann2013a.

6 Fazit und Ausblick

Die Durchführung der Nutzwertanalyse hat gezeigt, dass es große Unterschiede zwischen den Angeboten der Mailprovider hinsichtlich der Umsetzung von Sicherheitsverfahren gibt. Den meisten Providern scheinen aber die Sicherheitsprobleme bewusst zu sein und auch die Enthüllungen durch Edward Snowden haben sie veranlasst, die in den Protokollen vorhandenen Sicherheitsverfahren auch einzusetzen. Dies wird nicht zuletzt durch die Gründung der EmiG-Initiative deutlich.

Trotzdem muss man die in der Nutzwertanalyse festgestellte Situation als Momentaufnahme werten, da in diesem Markt, wie generell im IT-Bereich, sehr viel Bewegung ist. Dies lässt sich daran festmachen, dass neben den untersuchten, alternativen Mail Providern, die in Deutschland ansässig sind, auch weitere Anbieter wie *Protonmail.ch* aus der Schweiz oder *startmail.com* der Suchmaschine *ixquick* demnächst in den Markt eintreten und eine automatische E2EE der E-Mails versprechen, ohne dass der Nutzer zusätzliche Software benötigt.¹ Dadurch soll die Privatsphäre der Nutzer geschützt werden und das Mitlesen von Mails durch unberechtigte Dritte verhindert beziehungsweise erschwert werden.

Doch auch die großen Provider probieren hier nicht in den Anschluss zu verlieren. So hat Google bereits eine erste Testversion eines Browser-Addons zur Mailverschlüsselung im Browser veröffentlicht, die eine E2EE stark vereinfachen soll. Die Entwicklung in der nächsten Zeit wird zeigen, ob die großen Mailprovider durch die alternativen Provider dazu gezwungen werden, ebenfalls verstärkt Informationen und Unterstützung bei der Verschlüsselung von E-Mails zu bieten oder ob sich das Interesse der Öffentlichkeit für Themen des Datenschutz wieder legen wird.

Insgesamt lässt sich sagen, dass die bisher durchgeführten Schritte der meisten Provider zur Transportverschlüsselung von E-Mails ein Schritt in die richtige Richtung sind, diese den Nutzer jedoch nicht in falscher Sicherheit wiegen dürfen. Aufgrund der Tatsache, dass eine E2EE momentan noch mit einigen technischen Hürden verbunden ist und einen Komfortverlust, in Bezug auf die Lesbarkeit der Nachrichten auf unterschiedlichen Endgeräten mit sich bringt, ist der Einsatz der E-Mail zur Kommunikation auf der definierten Sicherheitsstufe 4 nur in manchen Fällen geeignet. An dieser Stelle muss jeder einzelne Nutzer selbst abwägen, wie wichtig für ihn die übermittelte Information ist und ob er zu deren Schutz die bestehenden Komforteinbußen hinnehmen kann und will.

¹Vgl. <http://www.protonmail.ch> und <http://beta.startmail.com>

Literaturverzeichnis

Anhang



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [mail.yahoo.com](#) > 98.136.189.41

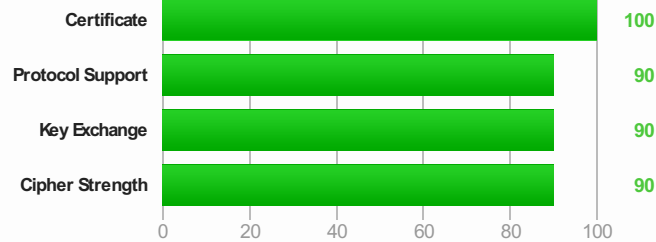
SSL Report: [mail.yahoo.com](#) (98.136.189.41)

Assessed on: Mon Jun 23 10:00:00 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication



Server Key and Certificate #1

Common names	*.login.yahoo.com
Alternative names	*.login.yahoo.com *.mail.yahoo.com *.edit.yahoo.com *.login.yahoo.net login.yahoo.com mail.yahoo.com mail.yahoo-inc.com fb.member.yahoo.com login.korea.yahoo.com api.reg.yahoo.com edit.yahoo.com watchlist.yahoo.com edit.india.yahoo.com edit.korea.yahoo.com edit.europe.yahoo.com edit.singapore.yahoo.com edit.tpe.yahoo.com legalredirect.yahoo.com me.yahoo.com open.login.yahooapis.com subscribe.yahoo.com edit.secure.yahoo.com edit.client.yahoo.com btedit.client.yahoo.com verizon.edit.client.yahoo.com na.edit.client.yahoo.com au.api.reg.yahoo.com au.reg.yahoo.com profile.yahoo.com static.profile.yahoo.com openid.yahoo.com
Prefix handling	Not required for subdomains
Prefix handling	Both (with and without WWW)
Valid from	Tue Apr 08 00:00:00 UTC 2014
Valid until	Thu Apr 09 23:59:59 UTC 2015 (expires in 9 months and 20 days)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	VeriSign Class 3 Secure Server CA - G3
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)



Certificates provided	3 (4761 bytes)
Chain issues	None
#2	
Subject	VeriSign Class 3 Secure Server CA - G3 SHA1: 5deb8f339e264c19f6686f5f8f32b54a4c46b476
Valid until	Fri Feb 07 23:59:59 UTC 2020 (expires in 5 years and 7 months)
Key	RSA2048 bits
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA1withRSA

#3

Subject	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27
Valid until	Sun Nov 07 23:59:59 UTC 2021 (expires in 7 years and 4 months)
Key	RSA2048 bits
Issuer	VeriSign / Class 3 Public Primary Certification Authority
Signature algorithm	SHA1withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	*.login.yahoo.com SHA1: d18dc6f40afeee834c1c793bff47dd2eae2481e6 RSA2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Secure Server CA - G3 SHA1: 5deb8f339e264c19f6686f5f8f32b54a4c46b476 RSA2048 bits / SHA1withRSA
3	In trust store	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 4eb6d578499b1cc5f581ead56be3d9b6744a5e5 RSA2048 bits / SHA1withRSA

Path #2: Not trusted (Algorithm constraints check failed: MD2withRSA)

1	Sent by server	*.login.yahoo.com SHA1: d18dc6f40afeee834c1c793bff47dd2eae2481e6 RSA2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Secure Server CA - G3 SHA1: 5deb8f339e264c19f6686f5f8f32b54a4c46b476 RSA2048 bits / SHA1withRSA
3	Sent by server	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27 RSA2048 bits / SHA1withRSA
4	In trust store	VeriSign / Class 3 Public Primary Certification Authority SHA1: 742c3192e607e424eb4549542be1bbc53e6174e2 RSA 1024 bits / MD2withRSA WEAK KEY IN MOZILLA'S TRUST STORE MORE INFO »

Path #3: Trusted

1	Sent by server	*.login.yahoo.com SHA1: d18dc6f40afeee834c1c793bff47dd2eae2481e6 RSA2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Secure Server CA - G3 SHA1: 5deb8f339e264c19f6686f5f8f32b54a4c46b476 RSA2048 bits / SHA1withRSA
3	Sent by server	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27 RSA2048 bits / SHA1withRSA
4	In trust store	VeriSign / Class 3 Public Primary Certification Authority SHA1: a1db6393916f17e4185509400415c70240b0ae6b RSA 1024 bits / SHA1withRSA WEAK KEY IN MOZILLA'S TRUST STORE MORE INFO »

Configuration



Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	Yes
SSL 2	No



Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH 256 bits (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH 256 bits (eq. 3072 bits RSA)	FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)			128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)			256
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH 256 bits (eq. 3072 bits RSA)	FS	256
TLS_RSA_WITH_RC4_128_SHA (0x5)			128
TLS_RSA_WITH_RC4_128_MD5 (0x4)			128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)			128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)			256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)			112



Handshake Simulation

Android 2.3.7 No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	FS RC4	128
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	FS RC4	128
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	FS RC4	128
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	FS RC4	128
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	FS	128
BingBot Dec 2013 No SNI ²	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	FS	128
BingPreview Dec 2013	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Chrome 34 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	FS RC4	128
Firefox 29 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	FS	128
Googlebot Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	FS RC4	128
IE 6 / XP No FS ¹ No SNI ²	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	FS	128
IE 8 / XP No FS ¹ No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	FS	128
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	FS	128
Java 6u45 No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	FS RC4	128
Java 8b132	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128

OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Safari 5.1.9/OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Safari 6/iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 7/iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Safari 6.0.4/OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Safari 7/OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Yahoo Slurp Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
YandexBot May 2014	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info) SSL 3: 0xc011, TLS 1.0: 0xc011
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	With modern browsers (more info)
Next Protocol Negotiation	Yes http/1.1 http/1.0
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Mon Jun 23 09:57:48 UTC 2014
Test duration	79.73 seconds
HTTP status code	200
HTTP server signature	ATS
Server hostname	ats1.member.vip.gq1.yahoo.com
PCI compliant	Yes
HIPS-ready	No

SSL Report v1.10.11

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [gmail.com](#) > 74.125.239.53

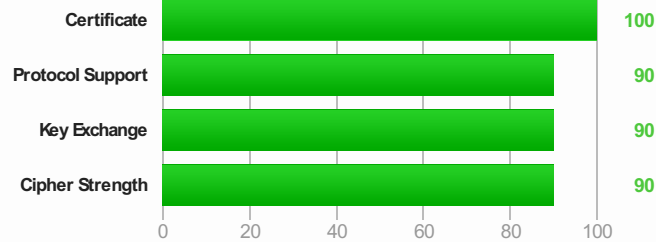
SSL Report: [gmail.com](#) (74.125.239.53)

Assessed on: Mon Jun 23 06:26:19 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This site works only in browsers with SNI support.

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication



Server Key and Certificate #1

Common names	www.gmail.com
Alternative names	www.gmail.com
Prefix handling	Not valid for "gmail.com" CONFUSING
Valid from	Wed Jun 04 09:24:23 UTC 2014
Valid until	Tue Sep 02 00:00:00 UTC 2014 (expires in 2 months and 10 days)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	Google Internet Authority G2
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	3 (3073 bytes)
Chain issues	None
#2	
Subject	Google Internet Authority G2 SHA1: d83c1a7f4d0446bb2081b81a1670f8183451ca24
Valid until	Sat Apr 04 15:15:55 UTC 2015 (expires in 9 months and 15 days)

Key	RSA2048 bits
Issuer	GeoTrust Global CA
Signature algorithm	SHA1withRSA
#3	
Subject	GeoTrust Global CA SHA1: 7359755c6df9a0abc3060bce369564c8ec4542a3
Valid until	Tue Aug 21 04:00:00 UTC 2018 (expires in 4 years and 1 month)
Key	RSA2048 bits
Issuer	Equifax / Equifax Secure Certificate Authority
Signature algorithm	SHA1withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	www.gmail.com SHA1: d338b65dc27ae61a2dfaca502fa544f17b4104aa RSA2048 bits / SHA1withRSA
2	Sent by server	Google Internet Authority G2 SHA1: d83c1a7f4d0446bb2081b81a1670f8183451ca24 RSA2048 bits / SHA1withRSA
3	In trust store	GeoTrust Global CA SHA1: de28f4a4ffe5b92fa3c503d1a349a7f9962a8212 RSA2048 bits / SHA1withRSA

Path #2: Trusted

1	Sent by server	www.gmail.com SHA1: d338b65dc27ae61a2dfaca502fa544f17b4104aa RSA2048 bits / SHA1withRSA
2	Sent by server	Google Internet Authority G2 SHA1: d83c1a7f4d0446bb2081b81a1670f8183451ca24 RSA2048 bits / SHA1withRSA
3	Sent by server	GeoTrust Global CA SHA1: 7359755c6df9a0abc3060bce369564c8ec4542a3 RSA2048 bits / SHA1withRSA
4	In trust store	Equifax / Equifax Secure Certificate Authority SHA1: d23209ad23d314232174e40d7f9d62139786633a RSA 1024 bits / SHA1withRSA WEAK KEY IN MOZILLA'S TRUST STORE MORE INFO »

Configuration



Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3 ²	Yes
SSL 2	No

(2) This site requires support for virtual SSL hosting, but SSL 2.0 and SSL 3.0 do not support this feature.



Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13)	ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	ECDH 256 bits (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128

TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH 256 bits (eq. 3072 bits RSA) FS	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH 256 bits (eq. 3072 bits RSA) FS	128



Handshake Simulation

Android 2.3.7 No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
BingBot Dec 2013 No SNI ²	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
BingPreview Dec 2013	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Chrome 34 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Firefox 29 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Googlebot Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
IE 6 / XP No FS ¹ No SNI ²	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 8 / XP No FS ¹ No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Java 6u45 No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Java 8b132	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Yahoo Slurp Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
YandexBot May 2014	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info) SSL 3: 0xc011, TLS 1.0: 0xc011
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	With modern browsers (more info)
Next Protocol Negotiation	Yes spdy/3.1 spdy/3 http/1.1
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Mon Jun 23 06:24:47 UTC 2014
Test duration	46.141 seconds
HTTP status code	301
HTTP forwarding	https://mail.google.com
HTTP server signature	sffe
Server hostname	nuq04s19-in-f21.1e100.net
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11

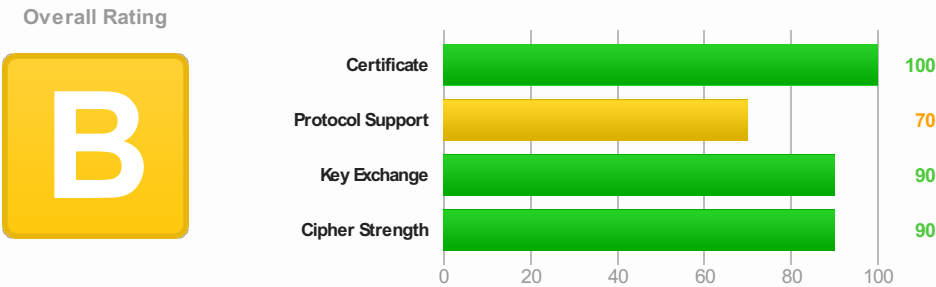
You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [hotmail.com](#) > 157.55.152.112

SSL Report: [hotmail.com](#) (157.55.152.112)

Assessed on: Sun Jun 22 15:28:01 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication



Server Key and Certificate #1

Common names	mail.live.com
Alternative names	mail.live.com m.mail.live.com contacts.live.com hotmail.co.jp hotmail.co.uk hotmail.com hotmail.live.com hotmail.msn.com people.live.com www.hotmail.com www.hotmail.msn.com www.mail.live.com home.live.com www.live.com dvt.mail.live.com snt002.afx.ms snt002.mail.live.com snt110.afx.ms snt110.mail.live.com snt111.afx.ms snt111.mail.live.com snt112.afx.ms snt112.mail.live.com snt113.afx.ms snt113.mail.live.com snt114.afx.ms snt114.mail.live.com snt115.afx.ms snt115.mail.live.com snt116.afx.ms snt116.mail.live.com snt117.afx.ms snt117.mail.live.com snt118.afx.ms snt118.mail.live.com snt120.afx.ms snt120.mail.live.com snt121.afx.ms snt121.mail.live.com snt122.afx.ms snt122.mail.live.com snt123.afx.ms snt123.mail.live.com snt124.afx.ms snt124.mail.live.com snt125.afx.ms snt125.mail.live.com snt126.afx.ms snt126.mail.live.com snt127.afx.ms snt127.mail.live.com snt128.afx.ms snt128.mail.live.com snt129.afx.ms snt129.mail.live.com snt130.afx.ms snt130.mail.live.com snt131.afx.ms snt131.mail.live.com snt132.afx.ms snt132.mail.live.com snt133.afx.ms snt133.mail.live.com snt134.afx.ms snt134.mail.live.com snt135.afx.ms snt135.mail.live.com snt136.afx.ms snt136.mail.live.com snt137.afx.ms snt137.mail.live.com snt138.afx.ms snt138.mail.live.com snt139.afx.ms snt139.mail.live.com snt140.afx.ms snt140.mail.live.com snt141.afx.ms snt141.mail.live.com snt142.afx.ms snt142.mail.live.com snt143.afx.ms snt143.mail.live.com snt144.afx.ms snt144.mail.live.com snt145.afx.ms snt145.mail.live.com snt146.afx.ms snt146.mail.live.com snt147.afx.ms snt147.mail.live.com snt148.afx.ms snt148.mail.live.com
Prefix handling	Both (with and without WWW)
Valid from	Tue May 21 00:00:00 UTC 2013

Valid until	Fri May 22 23:59:59 UTC 2015 (expires in 10 months and 33 days)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	VeriSign Class 3 Extended Validation SSL SGC CA
Signature algorithm	SHA1withRSA
Extended Validation	Yes
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	3 (6062 bytes)
Chain issues	None

#2

Subject	VeriSign Class 3 Extended Validation SSL SGC CA SHA1: b18039899831f152614667cf23ffcea2b0e73dab
Valid until	Mon Nov 07 23:59:59 UTC 2016 (expires in 2 years and 4 months)
Key	RSA2048 bits
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA1withRSA

#3

Subject	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27
Valid until	Sun Nov 07 23:59:59 UTC 2021 (expires in 7 years and 4 months)
Key	RSA2048 bits
Issuer	VeriSign / Class 3 Public Primary Certification Authority
Signature algorithm	SHA1withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	mail.live.com SHA1: 9872bc7b7244dfef5e019acf73bad250ecaf9f80 RSA2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Extended Validation SSL SGC CA SHA1: b18039899831f152614667cf23ffcea2b0e73dab RSA2048 bits / SHA1withRSA
3	In trust store	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 RSA2048 bits / SHA1withRSA

Path #2: Not trusted (Algorithm constraints check failed: MD2withRSA)

1	Sent by server	mail.live.com SHA1: 9872bc7b7244dfef5e019acf73bad250ecaf9f80 RSA2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Extended Validation SSL SGC CA SHA1: b18039899831f152614667cf23ffcea2b0e73dab RSA2048 bits / SHA1withRSA
3	Sent by server	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27 RSA2048 bits / SHA1withRSA
4	In trust store	VeriSign / Class 3 Public Primary Certification Authority SHA1: 742c3192e607e424eb4549542be1bbc53e6174e2 RSA 1024 bits / MD2withRSA WEAK KEY IN MOZILLA'S TRUST STORE MORE INFO »

Path #3: Trusted

1	Sent by server	mail.live.com SHA1: 9872bc7b7244dfef5e019ac773bad250ecaf9f80 RSA 2048 bits / SHA1withRSA
2	Sent by server	VeriSign Class 3 Extended Validation SSL SGC CA SHA1: b18039899831f152614667cf23ffcea2b0e73dab RSA 2048 bits / SHA1withRSA
3	Sent by server	VeriSign Class 3 Public Primary Certification Authority - G5 SHA1: 32f30882622b87cf8856c63db873df0853b4dd27 RSA 2048 bits / SHA1withRSA
4	In trust store	VeriSign / Class 3 Public Primary Certification Authority SHA1: a1db6393916f17e4185509400415c70240b0ae6b RSA 1024 bits / SHA1withRSA WEAK KEY IN MOZILLA'S TRUST STORE MORE INFO »

Configuration



Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3	Yes
SSL 2	No



Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA(0x35)	256
TLS_RSA_WITH_RC4_128_SHA(0x5)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA(0xa)	112
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014) ECDH 384 bits (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013) ECDH 384 bits (eq. 7680 bits RSA) FS	128
TLS_RSA_WITH_RC4_128_MD5(0x4)	128



Handshake Simulation

Android 2.3.7 No SN ¹ ²	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Android 4.0.4	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Android 4.1.1	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Android 4.2.2	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Android 4.3	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Android 4.4.2	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
BingBot Dec 2013 No SN ¹ ²	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
BingPreview Dec 2013	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Chrome 34 / OS X R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Firefox 29 / OS X R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
Googlebot Oct 2013	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
IE 6 / XP No FS ¹ No SN ¹ ²	SSL 3	TLS_RSA_WITH_RC4_128_SHA(0x5)	No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
IE 8 / XP No FS ¹ No SN ¹ ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA(0x5)	No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
IE 11 / Win 7 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
IE 11 / Win 8.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	No FS	128

IE Mobile 11 / Win Phone 8.1	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Java 6u45 No SNI ²	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Java 8b132	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
OpenSSL 1.0.1e	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 7 / iOS 7.1 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Safari 7 / OS X 10.9 R	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Yahoo Slurp Oct 2013	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
YandexBot May 2014	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x5, TLS 1.0: 0x2f
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	No WEAK (more info)
Next Protocol Negotiation	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Sun Jun 22 15:23:43 UTC 2014
Test duration	42.179 seconds
HTTP status code	302
HTTP forwarding	https://login.live.com
HTTP server signature	Microsoft-IIS/7.5
Server hostname	origin.sn145w.snt145.mail.live.com
PCI compliant	Yes
RPS-ready	No

Copyright © 2009-2014 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > email.t-online.de

SSL Report: email.t-online.de (62.153.158.211)

Assessed on: Mon Jun 23 08:07:45 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication



Server Key and Certificate #1


Common names	email.t-online.de
Alternative names	email.t-online.de
Prefix handling	Not required for subdomains
Valid from	Fri Mar 28 13:34:11 UTC 2014
Valid until	Sat Mar 28 23:59:59 UTC 2015 (expires in 9 months and 8 days)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	TeleSec ServerPass Extended Validation Class 3 CA
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	3 (4484 bytes)
Chain issues	Contains anchor
#2	
Subject	TeleSec ServerPass Extended Validation Class 3 CA SHA1: c6d43f5978e02e1fc64cf6fa94ac4b4d3adc8593
Valid until	Sun Feb 11 23:59:59 UTC 2024 (expires in 9 years and 7 months)




Key	RSA2048 bits
Issuer	T-TeleSec GlobalRoot Class 3
Signature algorithm	SHA256withRSA
#3	
Subject	T-TeleSec GlobalRoot Class 3 In trust store SHA1: 55a6723ecbf2eccdc3237470199d2abe11e381d1
Valid until	Sat Oct 01 23:59:59 UTC 2033 (expires in 19 years and 3 months)
Key	RSA2048 bits
Issuer	T-TeleSec GlobalRoot Class 3 Self-signed
Signature algorithm	SHA256withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	email.t-online.de SHA1: 43f7a752d54fd1fa2a56cf70285c0e619632a35f RSA2048 bits / SHA256withRSA
2	Sent by server	TeleSec ServerPass Extended Validation Class 3 CA SHA1: c6d43f5978e02e1fc64cf6fa94ac4b4d3adc8593 RSA2048 bits / SHA256withRSA
3	Sent by server In trust store	T-TeleSec GlobalRoot Class 3 SHA1: 55a6723ecbf2eccdc3237470199d2abe11e381d1 RSA2048 bits / SHA256withRSA

Configuration			
	Protocols		
	TLS 1.2		Yes
	TLS 1.1		Yes
	TLS 1.0		Yes
	SSL 3		Yes
	SSL 2		No
	Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)		
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	ECDH 256 bits (eq. 3072 bits RSA) FS	256
	TLS_RSA_WITH_AES_256_CBC_SHA(0x35)		256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)	ECDH 256 bits (eq. 3072 bits RSA) FS	128
	TLS_ECDHE_RSA_WITH_RC4_128_SHA(0xc011)	ECDH 256 bits (eq. 3072 bits RSA) FS	128
	TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)		128
	TLS_RSA_WITH_RC4_128_SHA(0x5)		128
	Handshake Simulation		
	Android 2.3.7 No SNI²	TLS 1.0 TLS_RSA_WITH_AES_128_CBC_SHA(0x2f) No FS	128
	Android 4.0.4	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014) FS	256
	Android 4.1.1	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014) FS	256
	Android 4.2.2	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014) FS	256
	Android 4.3	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014) FS	256
	Android 4.4.2	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014) FS	256
	BingBot Dec 2013 No SNI²	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014) FS	256
	BingPreview Dec 2013	TLS 1.0 TLS_RSA_WITH_AES_256_CBC_SHA(0x35) No FS	256
	Chrome 34 / OS X R	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014) FS	256

Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Firefox 29 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Googlebot Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE 6 / XP No FS ¹ No SNI ²	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE 8 / XP No FS ¹ No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Java 6u45 No SNI ²	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	FS	128
Java 8b132	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
YandexBot May 2014	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	No FS	256

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0xc014, TLS 1.0: 0xc014
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	With modern browsers (more info)
Next Protocol Negotiation	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=31536000
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Mon Jun 23 08:06:44 UTC 2014
Test duration	61.342 seconds

HTTP status code	200
HTTP server signature	Apache
Server hostname	-
PCI compliant	Yes
HPS-ready	No

SSL Report v1.10.11



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > navigator.web.de

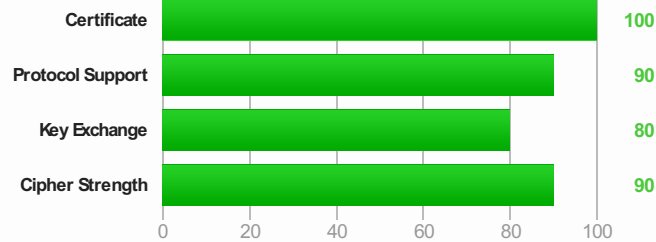
SSL Report: navigator.web.de (217.72.194.207)

Assessed on: Mon Jun 23 08:05:27 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication



Server Key and Certificate #1

Common names	*.web.de
Alternative names	*.web.de
Prefix handling	Not required for subdomains
Valid from	Wed Apr 09 05:48:51 UTC 2014
Valid until	Tue Apr 14 23:59:59 UTC 2015 (expires in 9 months and 25 days)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	TeleSec ServerPass DE-2
Signature algorithm	SHA256withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	3 (4514 bytes)
Chain issues	Contains anchor
#2	
Subject	TeleSec ServerPass DE-2 SHA1: 98662c9a0d0947e3de928afe4c15c80b384e8cca
Valid until	Tue Jul 09 23:59:00 UTC 2019 (expires in 5 years)
Key	RSA2048 bits
Issuer	Deutsche Telekom Root CA2

Signature algorithm

SHA256withRSA

#3

Subject

Deutsche Telekom Root CA2 In trust store
SHA1: 85a408c09c193e5d51587d added 61330fd8cde37bf

Valid until

Tue Jul 09 23:59:00 UTC 2019 (expires in 5 years)

Key

RSA2048 bits

Issuer

Deutsche Telekom Root CA2 Self-signed

Signature algorithm

SHA1withRSA

Certification Paths

Path #1: Trusted

1

Sent by server

*.web.de
SHA1: 302c44fcc58726fea8318824dec97c0a1a565888
RSA2048 bits / SHA256withRSA

2

Sent by server

TeleSec ServerPass DE-2
SHA1: 98662c9a0d0947e3de928afe4c15c80b384e8cca
RSA2048 bits / SHA256withRSA

3

Sent by server

In trust store

Deutsche Telekom Root CA2
SHA1: 85a408c09c193e5d51587d added 61330fd8cde37bf
RSA2048 bits / SHA1withRSA

Configuration

Protocols

TLS 1.2

Yes

TLS 1.1

Yes

TLS 1.0

Yes

SSL 3

Yes

SSL 2

No

Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

ECDH 256 bits (eq. 3072 bits RSA)

FS

256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)

ECDH 256 bits (eq. 3072 bits RSA)

FS

256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

ECDH 256 bits (eq. 3072 bits RSA)

FS

256

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)

DH 1024 bits (p: 128, g: 1, Ys 128)

FS

256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)

DH 1024 bits (p: 128, g: 1, Ys 128)

FS

256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)

DH 1024 bits (p: 128, g: 1, Ys 128)

FS

256

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)

DH 1024 bits (p: 128, g: 1, Ys 128)

FS

256

TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)

256

TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)

256

TLS_RSA_WITH_AES_256_CBC_SHA (0x35)

256

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)

256

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)

ECDH 256 bits (eq. 3072 bits RSA)

FS

112

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)

DH 1024 bits (p: 128, g: 1, Ys 128)

FS

112

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)

112

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

ECDH 256 bits (eq. 3072 bits RSA)

FS

128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)

ECDH 256 bits (eq. 3072 bits RSA)

FS

128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

ECDH 256 bits (eq. 3072 bits RSA)

FS

128

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)

DH 1024 bits (p: 128, g: 1, Ys 128)

FS

128

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)

DH 1024 bits (p: 128, g: 1, Ys 128)

FS

128

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)

DH 1024 bits (p: 128, g: 1, Ys 128)

FS

128

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(0x45)	DH 1024 bits(p: 128, g: 1, Ys 128)	FS	128
TLS_RSA_WITH_AES_128_GCM_SHA256(0x9c)			128
TLS_RSA_WITH_AES_128_CBC_SHA256(0x3c)			128
TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)			128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(0x41)			128



Handshake Simulation

Android 2.3.7 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(0x16)	FS	112
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xc030)	FS	256
BingBot Dec 2013 No SNI ²	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x39)	FS	256
Chrome 34 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Firefox 29 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Googlebot Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE 6 / XP No FS ¹ No SNI ²	SSL 3	TLS_RSA_WITH_3DES_EDE_CBC_SHA(0xa)	No FS	112
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE 8 / XP No FS ¹ No SNI ²	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA(0xa)	No FS	112
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Java 6u45 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(0x16)	FS	112
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA(0xc012)	FS	112
Java 8b132	TLS 1.2	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA(0xc012)	FS	112
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x39)	FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xc030)	FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xc028)	FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xc028)	FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xc028)	FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)	FS	256
YandexBot May 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x39)	FS	256

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(R) Denotes a reference browser or client, with which we expect better effective security.


(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0xc014, TLS 1.0: 0xc014
TLS compression	No
RC4	No
Heartbeat (extension)	Yes

Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
Next Protocol Negotiation	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Mon Jun 23 08:03:58 UTC 2014
Test duration	88.669 seconds
HTTP status code	403
HTTP server signature	Apache
Server hostname	navigator.web.de
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [gmx.net](#) > 213.165.65.50

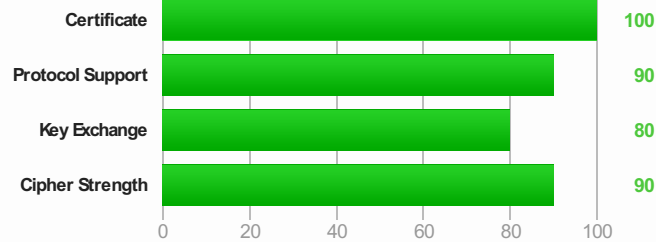
SSL Report: [gmx.net](#) (213.165.65.50)

Assessed on: Sun Jun 22 09:21:13 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication



Server Key and Certificate #1

Common names	gmx.net
Alternative names	gmx.cc gmx.co.in gmx.de gmx.info gmx.it gmx.lu gmx.org gmx.ph gmx.se gmx.sg gmx.tn gmx.tw gmx.li gmx.at gmx.biz gmx.com.tr gmx.ch gmx.dk gmx.net
Prefix handling	Non-prefixed access only, but DNS not configured for prefix
Valid from	Tue May 20 00:00:00 UTC 2014
Valid until	Thu May 19 23:59:59 UTC 2016 (expires in 1 year and 10 months)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	Thawte SSL CA
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	3 (3573 bytes)
Chain issues	None
#2	
Subject	Thawte SSL CA SHA1: 73e42686657aece354fbf685712361658f2f4357
Valid until	Fri Feb 07 23:59:59 UTC 2020 (expires in 5 years and 7 months)

Key

RSA 2048 bits

Issuer

thawte Primary Root CA

Signature algorithm

SHA1withRSA

#3

Subject

thawte Primary Root CA
SHA1: 1fa490d1d4957942cd23545f6e823d0000796ea2

Valid until

Wed Dec 30 23:59:59 UTC 2020 (expires in 6 years and 6 months)

Key


RSA 2048 bits

Issuer

Thawte Premium Server CA

Signature algorithm

SHA1withRSA



Certification Paths

Path #1: Trusted

1

Sent by server

gmx.net
SHA1: 7a65a93a1a4732cba669f9d76d0e4197959f476a
RSA 2048 bits / SHA1withRSA

2

Sent by server

Thawte SSL CA
SHA1: 73e42686657aece354fbf685712361658f2f4357
RSA 2048 bits / SHA1withRSA

3

In trust store

thawte Primary Root CA
SHA1: 91c6d6ee3e8ac86384e548c299295c756c817b81
RSA 2048 bits / SHA1withRSA

Path #2: Trusted

1

Sent by server

gmx.net
SHA1: 7a65a93a1a4732cba669f9d76d0e4197959f476a
RSA 2048 bits / SHA1withRSA

2

Sent by server

Thawte SSL CA
SHA1: 73e42686657aece354fbf685712361658f2f4357
RSA 2048 bits / SHA1withRSA

3

Sent by server


thawte Primary Root CA
SHA1: 1fa490d1d4957942cd23545f6e823d0000796ea2
RSA 2048 bits / SHA1withRSA

4

In trust store

Thawte Premium Server CA
SHA1: 627f8d7827656399d27d7f9044c9feb3f33efa9a
RSA 1024 bits / MD5withRSA
WEAK KEY IN MOZILLA'S TRUST STORE [MORE INFO »](#)

Configuration



Protocols

TLS 1.2

Yes

TLS 1.1

Yes

TLS 1.0


Yes

SSL 3

Yes

SSL 2

No



Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

128

TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x39)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

256

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(0x16)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

112

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)

EC DH 256 bits (eq. 3072 bits RSA)

FS

128

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0xc014)

EC DH 256 bits (eq. 3072 bits RSA)

FS

256

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA(0xc012)

EC DH 256 bits (eq. 3072 bits RSA)

FS

112

TLS_RSA_WITH_AES_256_CBC_SHA(0x35)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA(0xa)	112
TLS_RSA_WITH_AES_256_CBC_SHA256(0x3d)	256
TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	128
TLS_RSA_WITH_AES_128_CBC_SHA256(0x3c)	128



Handshake Simulation

Android 2.3.7 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Android 4.0.4	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Android 4.1.1	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Android 4.2.2	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Android 4.3	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Android 4.4.2	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
BingBot Dec 2013 No SNI ²	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)	FS	128
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Chrome 34 / OS X R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Firefox 29 / OS X R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Googlebot Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
IE 6 / XP No FS ¹ No SNI ²	SSL 3	TLS_RSA_WITH_3DES_EDE_CBC_SHA(0xa)	No FS	112
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)	FS	128
IE 8 / XP No FS ¹ No SNI ²	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA(0xa)	No FS	112
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)	FS	128
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)	FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)	FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)	FS	128
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(0xc013)	FS	128
Java 6u45 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Java 7u25	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Java 8b132	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
OpenSSL 1.0.1e	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
Yahoo Slurp Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128
YandexBot May 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33)	FS	128

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(R) Denotes a reference browser or client, with which we expect better effective security.


(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	Supported DoS DANGER (more info)
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x33, TLS 1.0: 0x33
TLS compression	No
RC4	No
Heartbeat (extension)	No

Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
Next Protocol Negotiation	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 1.3 TLS 1.98 TLS 2.98
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Sun Jun 22 09:16:47 UTC 2014
Test duration	81.731 seconds
HTTP status code	301
HTTP forwarding	http://www.gmx.net
HTTP server signature	Apache
Server hostname	gmx.net
PCI compliant	Yes
RIPS-ready	No

SSL Report v1.10.11



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > mailbox.org

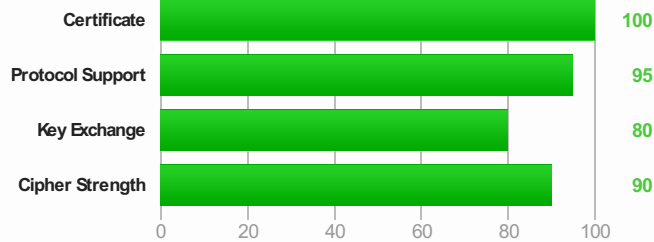
SSL Report: mailbox.org (80.241.60.194)

Assessed on: Mon Jun 23 09:42:25 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication



Server Key and Certificate #1

Common names	*.mailbox.org
Alternative names	*.mailbox.org mailbox.org
Prefix handling	Both (with and without WWW)
Valid from	Wed May 14 14:52:09 UTC 2014
Valid until	Tue May 14 14:52:09 UTC 2019 (expires in 4 years and 10 months)
Key	RSA 4096 bits
Weak key (Debian)	No
Issuer	SwissSign Server Silver CA2008 - G2
Signature algorithm	SHA1withRSA
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	3 (4896 bytes)
Chain issues	Contains anchor
#2	
Subject	SwissSign Server Silver CA2008 - G2 SHA1: 95eef9f8bb003d337c47b0f9a947ffafe02725c3
Valid until	Fri Jul 07 17:07:16 UTC 2023 (expires in 9 years)

Key

RSA2048 bits

Issuer

SwissSign Silver CA - G2

Signature algorithm

SHA1withRSA

#3

Subject

SwissSign Silver CA - G2 In trust store
SHA1: 9baae59f56ee21cb435abe2593dfa7f040d11dcb

Valid until

Sat Oct 25 08:32:46 UTC 2036 (expires in 22 years and 4 months)

Key

RSA4096 bits

Issuer

SwissSign Silver CA - G2 Self-signed

Signature algorithm

SHA1withRSA

Certification Paths

Path #1: Trusted

1

Sent by server

*.mailbox.org
SHA1: 0c6479b4e783dbb3f2162c5d0d2570011fa2dab3
RSA4096 bits / SHA1withRSA

2

Sent by server

SwissSign Server Silver CA2008 - G2
SHA1: 95eef9f8bb003d337c47b0f9a947ffafe02725c3
RSA2048 bits / SHA1withRSA

3

Sent by server

In trust store

SwissSign Silver CA - G2
SHA1: 9baae59f56ee21cb435abe2593dfa7f040d11dcb
RSA4096 bits / SHA1withRSA

Configuration

Protocols

TLS 1.2

Yes

TLS 1.1

Yes

TLS 1.0

Yes

SSL 3

No

SSL 2

No

Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

EC DH 256 bits(eq. 3072 bits RSA)

FS

256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)

EC DH 256 bits (eq. 3072 bits RSA)

FS

256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

128

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

128

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

EC DH 256 bits (eq. 3072 bits RSA)

FS

128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)

EC DH 256 bits (eq. 3072 bits RSA)

FS

128

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

112

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)

EC DH 256 bits (eq. 3072 bits RSA)

FS

112

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

EC DH 256 bits (eq. 3072 bits RSA)

FS

256

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

128

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)

DH 1024 bits(p: 128, g: 1, Ys 128)

FS

128

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

EC DH 256 bits (eq. 3072 bits RSA)

FS

128

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)

256

TLS_RSA_WITH_AES_256_CBC_SHA (0x35)

256

TLS_RSA_WITH_3DES_EDE_CBC_SHA(0xa)	112
TLS_RSA_WITH_AES_128_CBC_SHA(0x2f)	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(0x41)	128



Handshake Simulation

Android 2.3.7 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Android 4.0.4	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Android 4.1.1	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Android 4.2.2	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Android 4.3	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Android 4.4.2	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	FS	256
BingBot Dec 2013 No SNI ²	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Chrome 34 / OS X R	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Firefox 29 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	FS	128
Googlebot Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
IE 6 / XP No FS ¹ No SNI ²	Protocol or cipher suite mismatch			Fail ³
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE 8 / XP No FS ¹ No SNI ²	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS		112
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	FS	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	FS	128
IE Mobile 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	FS	256
IE Mobile 11 / Win Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	FS	128
Java 6u45 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Java 7u25	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Java 8b132	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
OpenSSL 1.0.1e	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112
YandexBot May 2014	TLS 1.0	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	FS	112

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers tend to retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x16
TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)

OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
Next Protocol Negotiation	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes max-age=15768000
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Mon Jun 23 09:40:54 UTC 2014
Test duration	91.421 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	www.mailbox.org
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.10.11



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > posteo.de

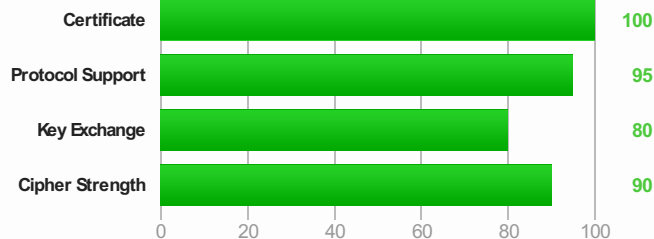
SSL Report: posteo.de (89.146.220.134)

Assessed on: Mon Jun 23 02:32:38 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

This server is not vulnerable to the [Heartbleed attack](#).

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication



Server Key and Certificate #1

Common names	www.posteo.de
Alternative names	www.posteo.de posteo.de m.posteo.de lists.posteo.de autodiscover.posteo.de mx01.posteo.de mx02.posteo.de mx03.posteo.de mx04.posteo.de
Prefix handling	Both (with and without WWW)
Valid from	Wed Apr 16 13:03:06 UTC 2014
Valid until	Sat Apr 16 16:23:04 UTC 2016 (expires in 1 year and 9 months)
Key	RSA2048 bits
Weak key (Debian)	No
Issuer	StartCom Extended Validation Server CA
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



Additional Certificates (if supplied)

Certificates provided	2 (3547 bytes)
Chain issues	None
#2	
Subject	StartCom Extended Validation Server CA SHA1: 9850463b55049f836cd63f69b30bd9e2c64d4274
Valid until	Tue Jan 01 06:00:00 UTC 2019 (expires in 4 years and 6 months)



Key	RSA 2048 bits
Issuer	StartCom Certification Authority
Signature algorithm	SHA1withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	www.posteo.de SHA1: 3a89d8addca7235c8f44e9dd2e856a31d2d3c970 RSA 2048 bits / SHA256withRSA
2	Sent by server	StartCom Extended Validation Server CA SHA1: 9850463b55049f836cd63f69b30bd9e2c64d4274 RSA 2048 bits / SHA1withRSA
3	In trust store	StartCom Certification Authority SHA1: a3f1333fe242bfcfc5d14e8f394298406810d1a0 RSA 4096 bits / SHA256withRSA

Path #2: Trusted

1	Sent by server	www.posteo.de SHA1: 3a89d8addca7235c8f44e9dd2e856a31d2d3c970 RSA 2048 bits / SHA256withRSA
2	Sent by server	StartCom Extended Validation Server CA SHA1: 9850463b55049f836cd63f69b30bd9e2c64d4274 RSA 2048 bits / SHA1withRSA
3	In trust store	StartCom Certification Authority SHA1: 3e2bf7f2031b96f38ce6c4d8a85d3e2d58476a0f RSA 4096 bits / SHA1withRSA

Configuration



Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No



Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH 256 bits (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH 256 bits (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH 256 bits (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 1024 bits (p: 128, g: 1, Ys 128)	FS	128
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)	ECDH 256 bits (eq. 3072 bits RSA)	FS	128

TLS_RSA_WITH_RC4_128_SHA(0x5) 128



Handshake Simulation

Android 2.3.7 No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
BingBot Dec 2013 No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
BingPreview Dec 2013	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
Chrome 34 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Firefox 24.2.0 ESR / Wn 7	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Firefox 29 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
Googlebot Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 6 / XP No FS ¹ No SNI ²	Protocol or cipher suite mismatch		Fail ³
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 8 / XP No FS ¹ No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 8-10 / Wn 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 11 / Wn 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
IE 11 / Wn 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
IE Mobile 10 / Wn Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE Mobile 11 / Wn Phone 8.1	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS	128
Java 6u45 No SNI ²	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
Java 8b132	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) FS	128
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256
OpenSSL 1.0.1e	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) FS	256
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS	256
Yahoo Slurp Oct 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
YandexBot May 2014	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) FS	256

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers tend to retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No
Forward Secrecy	With modern browsers (more info)

Next Protocol Negotiation	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	Yes
Strict Transport Security (HSTS)	Yes max-age=31536000; includeSubDomains
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	TLS 2.98
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Mon Jun 23 02:31:22 UTC 2014
Test duration	75.884 seconds
HTTP status code	301
HTTP forwarding	http://posteo.de
HTTP server signature	Apache
Server hostname	mail.posteo.de
PCI compliant	Yes
RPS-ready	No

SSL Report v1.10.11


[Back to Verisign Labs Tools](#)
Domain Name: Detail: [more\(+\)](#) / [less\(-\)](#)

Time: 2014-06-26 11:14:45 UTC, NTP stratum 3

Analyzing DNSSEC problems for [mail.yahoo.com](#)

.	<ul style="list-style-type: none"> ✓ Found 3 DNSKEY records for . ✓ DS=19036/SHA1 verifies DNSKEY=19036/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
com	<ul style="list-style-type: none"> ✓ Found 1 DS records for com in the . zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=40926 and DNSKEY=40926 verifies the DS RRset ✓ Found 2 DNSKEY records for com ✓ DS=30909/SHA256 verifies DNSKEY=30909/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=30909 and DNSKEY=30909/SEP verifies the DNSKEY RRset
yahoo.com	<ul style="list-style-type: none"> ✗ No DS records found for yahoo.com in the com zone ✗ No DNSKEY records found ✓ mail.yahoo.com is a CNAME to login.yahoo.com ✗ No RRSIGs found ✗ No DS records found for yahoo.com in the yahoo zone ✗ No DNSKEY records found ✓ login.yahoo.com is a CNAME to ats.login.lgg1.b.yahoo.com ✗ No RRSIGs found ✗ No DS records found for yahoo.com in the yahoo zone ✗ No DNSKEY records found
lgg1.b.yahoo.com	<ul style="list-style-type: none"> ✗ No DS records found for lgg1.b.yahoo.com in the yahoo.com zone ✗ No DNSKEY records found ✓ ats.login.lgg1.b.yahoo.com is a CNAME to ats.member.g02.yahoodns.net ✗ No RRSIGs found
.	
net	<ul style="list-style-type: none"> ✓ Found 1 DS records for net in the . zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=40926 and DNSKEY=40926 verifies the DS RRset ✓ Found 2 DNSKEY records for net ✓ DS=35886/SHA256 verifies DNSKEY=35886/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=35886 and DNSKEY=35886/SEP verifies the DNSKEY RRset
yahoodns.net	<ul style="list-style-type: none"> ✗ No DS records found for yahoodns.net in the net zone ✗ No DNSKEY records found ⚠ Query to ns2.yahoo.com/68.142.255.16 for g02.yahoodns.net/DNSKEY timed out or failed
g02.yahoodns.net	<ul style="list-style-type: none"> ✗ No DS records found for g02.yahoodns.net in the yahoodns.net zone ✗ No DNSKEY records found ✓ ats.member.g02.yahoodns.net is a CNAME to any-ats.member.a02.yahoodns.net ✗ No RRSIGs found
yahoodns.net	<ul style="list-style-type: none"> ✗ No DS records found for yahoodns.net in the yahoodns zone ✗ No DNSKEY records found
a02.yahoodns.net	<ul style="list-style-type: none"> ✗ No DS records found for a02.yahoodns.net in the yahoodns.net zone ✗ No DNSKEY records found ⚠ yf2.yahoo.com serial (1403781789) differs from yf1.yahoo.com serial (1403781779) ✓ any-ats.member.a02.yahoodns.net A RR has value 98.139.21.169 ✗ No RRSIGs found

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Want a second opinion? Test mail.yahoo.com at [dnsviz.net](#).

DNSSEC Analyzer r81 2014-04-17 17:57:35

[↓ Advanced options](#)

© 2011-2013 VeriSign, Inc. All rights reserved.

VERISIGN, the VERISIGN logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.


[Back to Verisign Labs Tools](#)
Domain Name: Detail: [more\(+\)](#) / [less\(-\)](#)

Time: 2014-06-23 09:35:06 UTC, NTP stratum 3

Analyzing DNSSEC problems for [gmail.com](#)

.	<ul style="list-style-type: none"> ✓ Found 3 DNSKEY records for . ✓ DS=19036/SHA1 verifies DNSKEY=19036/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
com	<ul style="list-style-type: none"> ✓ Found 1 DS records for com in the . zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=40926 and DNSKEY=40926 verifies the DS RRset ✓ Found 2 DNSKEY records for com ✓ DS=30909/SHA256 verifies DNSKEY=30909/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=30909 and DNSKEY=30909/SEP verifies the DNSKEY RRset
gmail.com	<ul style="list-style-type: none"> ✗ No DS records found for gmail.com in the com zone ✗ No DNSKEY records found ✓ gmail.com A RR has value 74.125.29.83 ✗ No RRSIGs found

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Want a second opinion? Test gmail.com at [dnsviz.net](#).

DNSSEC Analyzer r81 2014-04-17 17:57:35

[↓ Advanced options](#)
[Legal Notices](#) // [Privacy](#) // [Repository](#) // [Contact Us](#) // [Site Map](#)

© 2011-2013 VeriSign, Inc. All rights reserved.

VERISIGN, the VERISIGN logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

[Back to Verisign Labs Tools](#)Domain Name: Detail: [more\(+\)](#) / [less\(-\)](#)

Time: 2014-06-26 11:04:07 UTC, NTP stratum 3

Analyzing DNSSEC problems for [hotmail.com](#)

.	<ul style="list-style-type: none">✓ Found 3 DNSKEY records for .✓ DS=19036/SHA1 verifies DNSKEY=19036/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
com	<ul style="list-style-type: none">✓ Found 1 DS records for com in the . zone✓ Found 1 RRSIGs over DS RRset✓ RRSIG=40926 and DNSKEY=40926 verifies the DS RRset✓ Found 2 DNSKEY records for com✓ DS=30909/SHA256 verifies DNSKEY=30909/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=30909 and DNSKEY=30909/SEP verifies the DNSKEY RRset
hotmail.com	<ul style="list-style-type: none">✗ No DS records found for hotmail.com in the com zone✗ No DNSKEY records found✓ hotmail.com A RR has value 157.55.152.112✗ No RRSIGs found

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Want a second opinion? Test hotmail.com at [dnsviz.net](#).

DNSSEC Analyzer r81 2014-04-17 17:57:35

[↓ Advanced options](#)[Legal Notices](#) // [Privacy](#) // [Repository](#) // [Contact Us](#) // [Site Map](#)

© 2011-2013 VeriSign, Inc. All rights reserved.

VERISIGN, the VERISIGN logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

[Back to Verisign Labs Tools](#)Domain Name: Detail: [more\(+\)](#) / [less\(-\)](#)

Time: 2014-06-26 11:12:58 UTC, NTP stratum 3

Analyzing DNSSEC problems for [email.t-online.de](#)

.	<ul style="list-style-type: none">✓ Found 3 DNSKEY records for .✓ DS=19036/SHA1 verifies DNSKEY=19036/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
de	<ul style="list-style-type: none">✓ Found 1 DS records for de in the . zone✓ Found 1 RRSIGs over DS RRset✓ RRSIG=40926 and DNSKEY=40926 verifies the DS RRset✓ Found 2 DNSKEY records for de✓ DS=24220/SHA256 verifies DNSKEY=24220/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=24220 and DNSKEY=24220/SEP verifies the DNSKEY RRset
t-online.de	<ul style="list-style-type: none">✗ No DS records found for t-online.de in the de zone✗ No DNSKEY records found✓ email.t-online.de A RR has value 62.153.158.211✗ No RRSIGs found

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Want a second opinion? Test email.t-online.de at [dnsviz.net](#).

DNSSEC Analyzer r81 2014-04-17 17:57:35

[↓ Advanced options](#)[Legal Notices](#) // [Privacy](#) // [Repository](#) // [Contact Us](#) // [Site Map](#)

© 2011-2013 VeriSign, Inc. All rights reserved.

VERISIGN, the VERISIGN logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

[Back to Verisign Labs Tools](#)Domain Name: Detail: [more\(+\)](#) / [less\(-\)](#)

Time: 2014-06-26 11:07:26 UTC, NTP stratum 3

Analyzing DNSSEC problems for [navigator.web.de](#)

.	<ul style="list-style-type: none">✓ Found 3 DNSKEY records for .✓ DS=19036/SHA1 verifies DNSKEY=19036/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
de	<ul style="list-style-type: none">✓ Found 1 DS records for de in the . zone✓ Found 1 RRSIGs over DS RRset✓ RRSIG=40926 and DNSKEY=40926 verifies the DS RRset✓ Found 2 DNSKEY records for de✓ DS=24220/SHA256 verifies DNSKEY=24220/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=24220 and DNSKEY=24220/SEP verifies the DNSKEY RRset
web.de	<ul style="list-style-type: none">✗ No DS records found for web.de in the de zone✗ No DNSKEY records found✓ navigator.web.de A RR has value 217.72.194.207✗ No RRSIGs found

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Want a second opinion? Test navigator.web.de at [dnsviz.net](#).

DNSSEC Analyzer r81 2014-04-17 17:57:35

[↓ Advanced options](#)[Legal Notices](#) // [Privacy](#) // [Repository](#) // [Contact Us](#) // [Site Map](#)

© 2011-2013 VeriSign, Inc. All rights reserved.

VERISIGN, the VERISIGN logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

[Back to Verisign Labs Tools](#)Domain Name: Detail: [more\(+\)](#) / [less\(-\)](#)

Time: 2014-06-26 11:02:06 UTC, NTP stratum 3

Analyzing DNSSEC problems for [gmx.net](#)

.	<ul style="list-style-type: none">✓ Found 3 DNSKEY records for .✓ DS=19036/SHA1 verifies DNSKEY=19036/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
net	<ul style="list-style-type: none">✓ Found 1 DS records for net in the . zone✓ Found 1 RRSIGs over DS RRset✓ RRSIG=40926 and DNSKEY=40926 verifies the DS RRset✓ Found 2 DNSKEY records for net✓ DS=35886/SHA256 verifies DNSKEY=35886/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=35886 and DNSKEY=35886/SEP verifies the DNSKEY RRset
gmx.net	<ul style="list-style-type: none">✗ No DS records found for gmx.net in the net zone✗ No DNSKEY records found✓ gmx.net A RR has value 213.165.65.50✗ No RRSIGs found

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Want a second opinion? Test gmx.net at [dnsviz.net](#).

DNSSEC Analyzer r81 2014-04-17 17:57:35

[↓ Advanced options](#)[Legal Notices](#) // [Privacy](#) // [Repository](#) // [Contact Us](#) // [Site Map](#)

© 2011-2013 VeriSign, Inc. All rights reserved.

VERISIGN, the VERISIGN logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

[Back to Verisign Labs Tools](#)

Domain Name:

Detail: [more\(+\)](#) / [less\(-\)](#)

Time: 2014-06-25 17:10:45 UTC, NTP stratum 3

Analyzing DNSSEC problems for [mailbox.org](#)

.	<ul style="list-style-type: none">Found 3 DNSKEY records for .DS=19036/SHA1 verifies DNSKEY=19036/SEPFound 1 RRSIGs over DNSKEY RRsetRRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
org	<ul style="list-style-type: none">Found 2 DS records for org in the . zoneFound 1 RRSIGs over DS RRsetRRSIG=40926 and DNSKEY=40926 verifies the DS RRsetFound 4 DNSKEY records for orgDS=21366/SHA256 verifies DNSKEY=21366/SEPFound 3 RRSIGs over DNSKEY RRsetRRSIG=9795 and DNSKEY=9795/SEP verifies the DNSKEY RRset
mailbox.org	<ul style="list-style-type: none">Found 1 DS records for mailbox.org in the org zoneFound 1 RRSIGs over DS RRsetRRSIG=23273 and DNSKEY=23273 verifies the DS RRsetFound 3 DNSKEY records for mailbox.orgDS=38499/SHA256 verifies DNSKEY=38499/SEPFound 3 RRSIGs over DNSKEY RRsetRRSIG=5719 and DNSKEY=5719 verifies the DNSKEY RRsetmailbox.org A RR has value 80.241.60.194Found 2 RRSIGs over A RRsetRRSIG=5719 and DNSKEY=5719 verifies the A RRset

Move your mouse over any or symbols for remediation hints.

Want a second opinion? Test mailbox.org at [dnsviz.net](#)

DNSSEC Analyzer r81 2014-04-17 17:57:35

[↓ Advanced options](#)

[Legal Notices](#) // [Privacy](#) // [Repository](#) // [Contact Us](#) // [Site Map](#)

© 2011-2013 VeriSign, Inc. All rights reserved.
VERISIGN, the VERISIGN logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

[Back to Verisign Labs Tools](#)Domain Name: Detail: [more\(+\)](#) / [less\(-\)](#)

Time: 2014-06-26 11:11:20 UTC, NTP stratum 3

Analyzing DNSSEC problems for [posteo.de](#)

.	<ul style="list-style-type: none">✓ Found 3 DNSKEY records for .✓ DS=19036/SHA1 verifies DNSKEY=19036/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
de	<ul style="list-style-type: none">✓ Found 1 DS records for de in the . zone✓ Found 1 RRSIGs over DS RRset✓ RRSIG=40926 and DNSKEY=40926 verifies the DS RRset✓ Found 2 DNSKEY records for de✓ DS=24220/SHA256 verifies DNSKEY=24220/SEP✓ Found 1 RRSIGs over DNSKEY RRset✓ RRSIG=24220 and DNSKEY=24220/SEP verifies the DNSKEY RRset
posteo.de	<ul style="list-style-type: none">✓ Found 1 DS records for posteo.de in the de zone✓ Found 1 RRSIGs over DS RRset✓ RRSIG=34065 and DNSKEY=34065 verifies the DS RRset✓ Found 2 DNSKEY records for posteo.de✓ DS=53881/SHA256 verifies DNSKEY=53881/SEP✓ Found 2 RRSIGs over DNSKEY RRset✓ RRSIG=23244 and DNSKEY=23244 verifies the DNSKEY RRset✓ posteo.de A RR has value 89.146.220.134✓ Found 1 RRSIGs over A RRset✓ RRSIG=23244 and DNSKEY=23244 verifies the A RRset

Move your mouse over any or symbols for remediation hints.

Want a second opinion? Test posteo.de at [dnsviz.net](#).

DNSSEC Analyzer r81 2014-04-17 17:57:35

[↓ Advanced options](#)[Legal Notices](#) // [Privacy](#) // [Repository](#) // [Contact Us](#) // [Site Map](#)

© 2011-2013 VeriSign, Inc. All rights reserved.

VERISIGN, the VERISIGN logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.