DNSSEC und DANE

Dimitar Dimitrov

Institut für Informatik
Humboldt-Universität zu Berlin
Seminar Electronic Identity
Dr. Wolf Müller

17. November 2014

Inhaltsverzeichnis

Motivation

DNS

Domain Name System

Was ist DNS?

Das Domain Name System ist

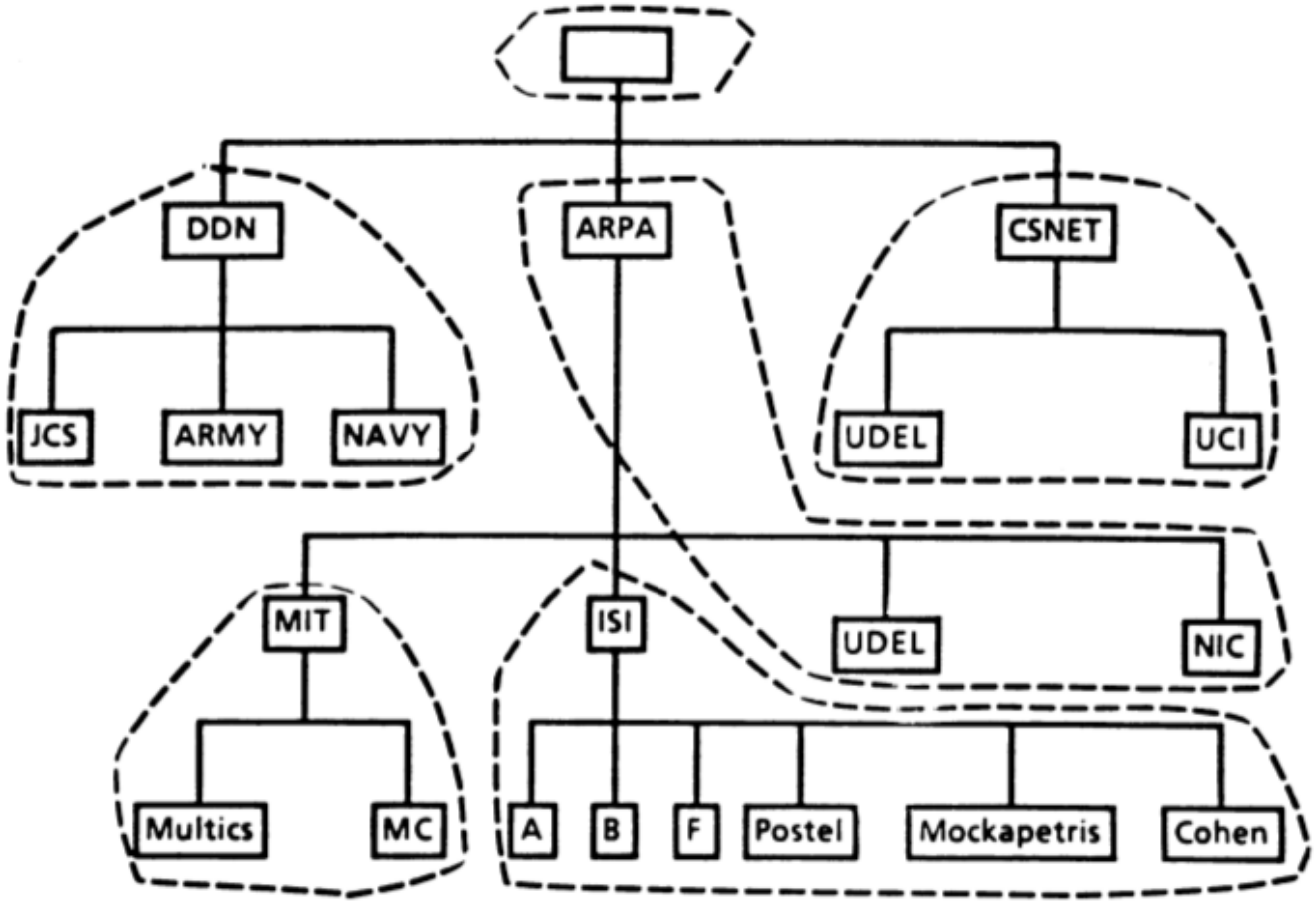
- ein sehr erfolgreicher Teil des Internets
- ein kritischer Teil des Internets
- ein „zero-security“-System

Ziele

- konsistenter Namensraum
- verteilte Datenbank/locales Caching
- für mehrere Anwendungen nützlich
- unabhähgig vom benutzten Protokoll

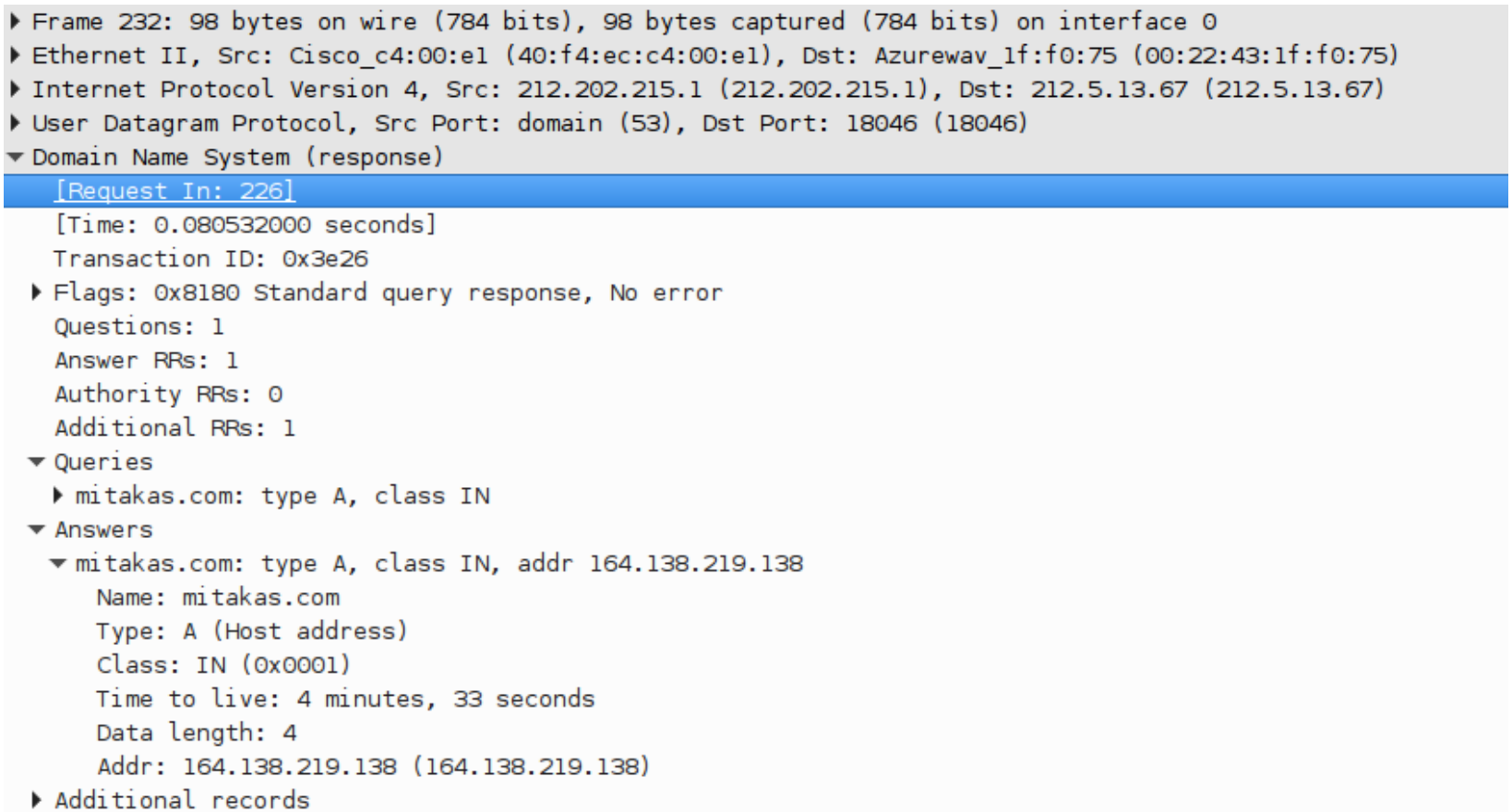
Wie ist DNS aufgebaut? I

- Domain-Namensraum



Wie ist DNS aufgebaut? II

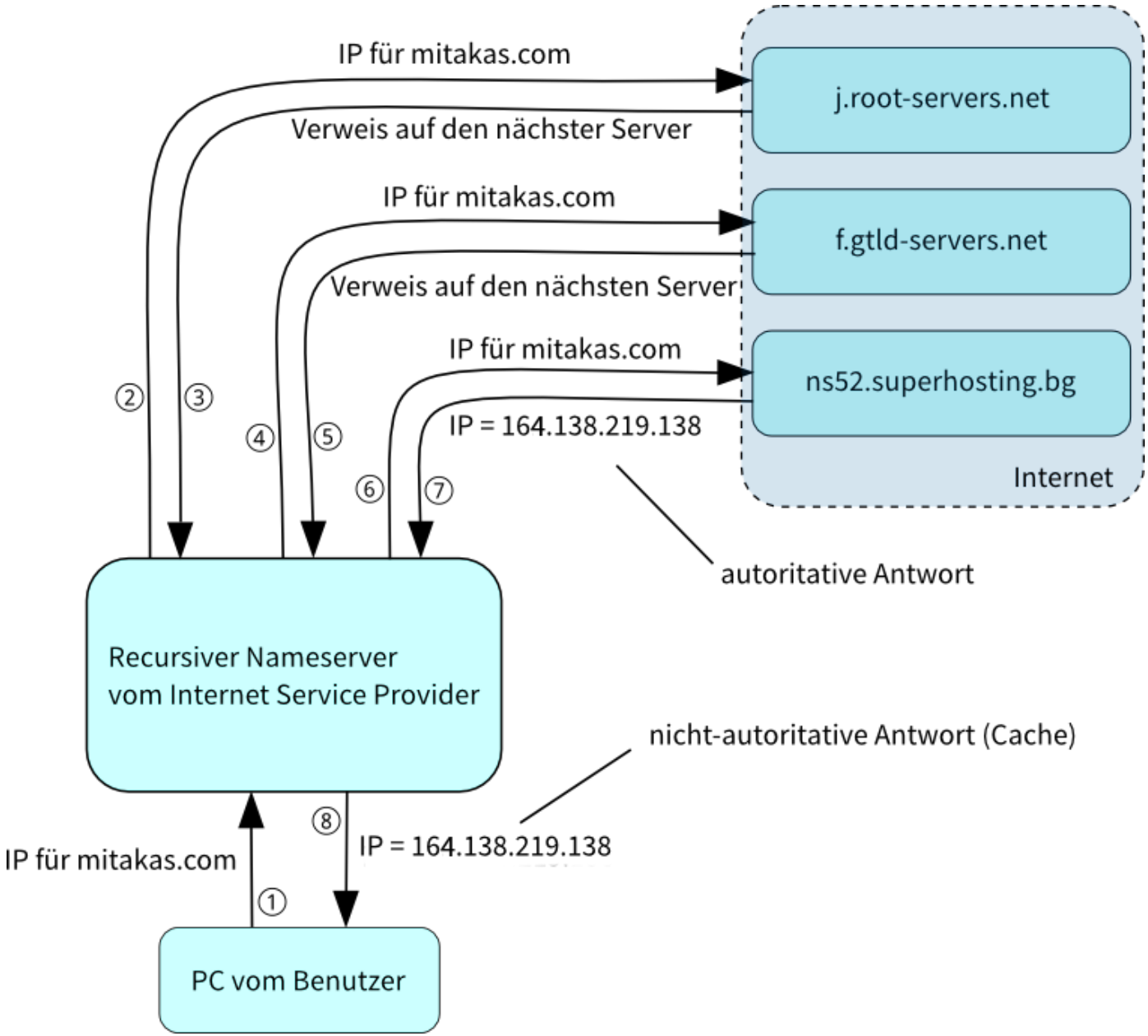
- Resource Records



A, AAAA, CNAME, MX, NS, SOA, TXT, usw.

- Nameservers und Resolvers

Wie funktioniert DNS?



Welche Probleme hat DNS?

- Packet interception
- ID guessing und query prediction
- Name chaining
- Betrayal by trusted server
- (Distributed) Denial of Service
- Authenticated denial of domain names
- Wildcards

Cache contamination von Bellovin (1990)
Kaminsky DNS Bug – CVE-2008-1447 (2008)

DNSSEC

Domain Name System Security Extensions

Was ist DNSSEC?

DNSSEC ist eine Sammlung von Internet Standards.

- **RFC 4033** DNSSEC Introduction and Requirements
- **RFC 4034** Resource Records for DNSSEC
- **RFC 4035** Protocol Modifications for DNSSEC

Was leistet DNSSEC?

- Datenauthentizität
- Datenintegrität
- Authentizität bei nicht existierende Namen/Typen

Was ist neu bei DNSSEC?

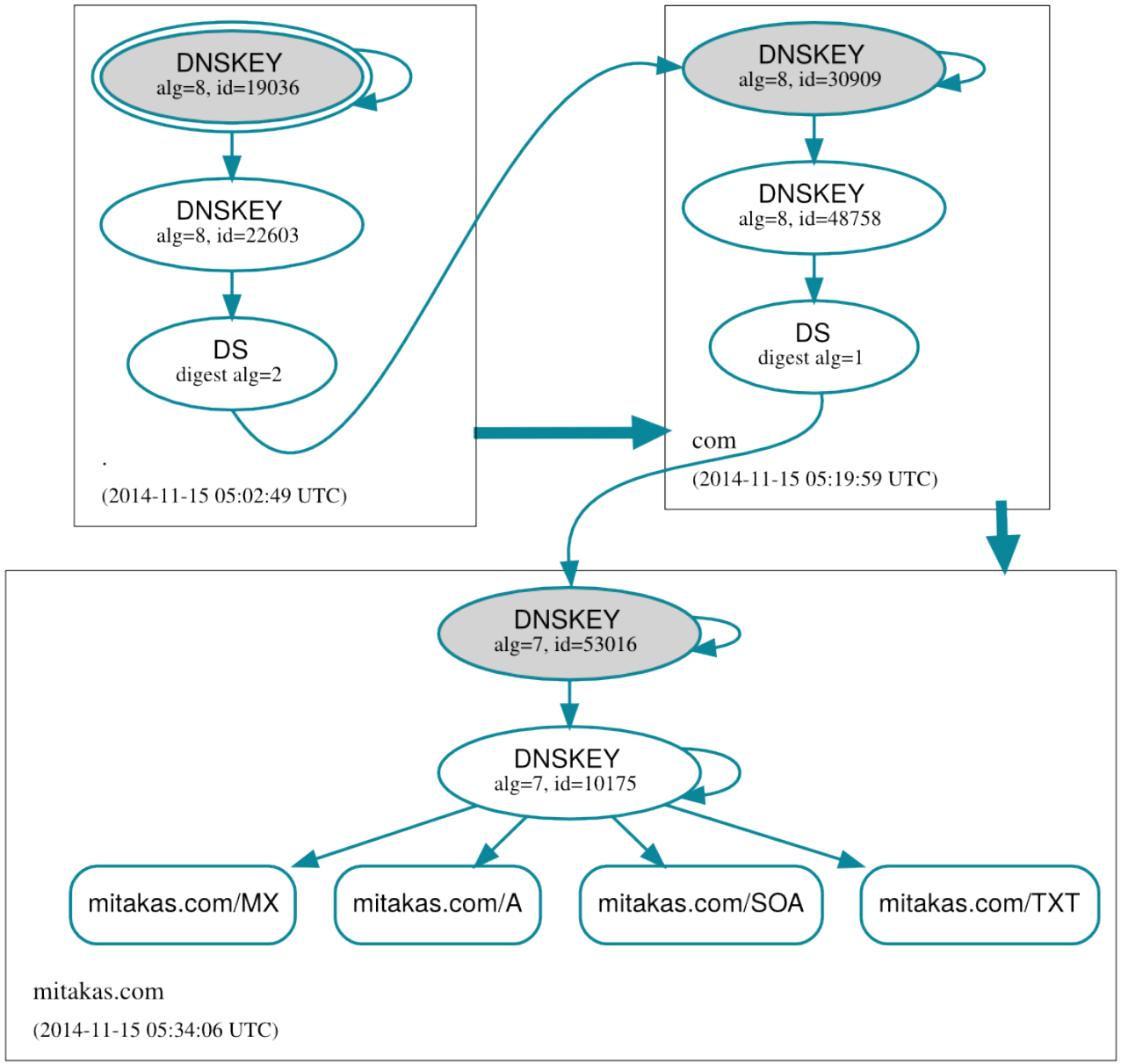
Neue Resource Records

- DNSKEY DNS Public Key
- RRSIG Resource Record Signature
- NSEC Next Secure
- DS Delegation Signer

Änderungen am Protokoll

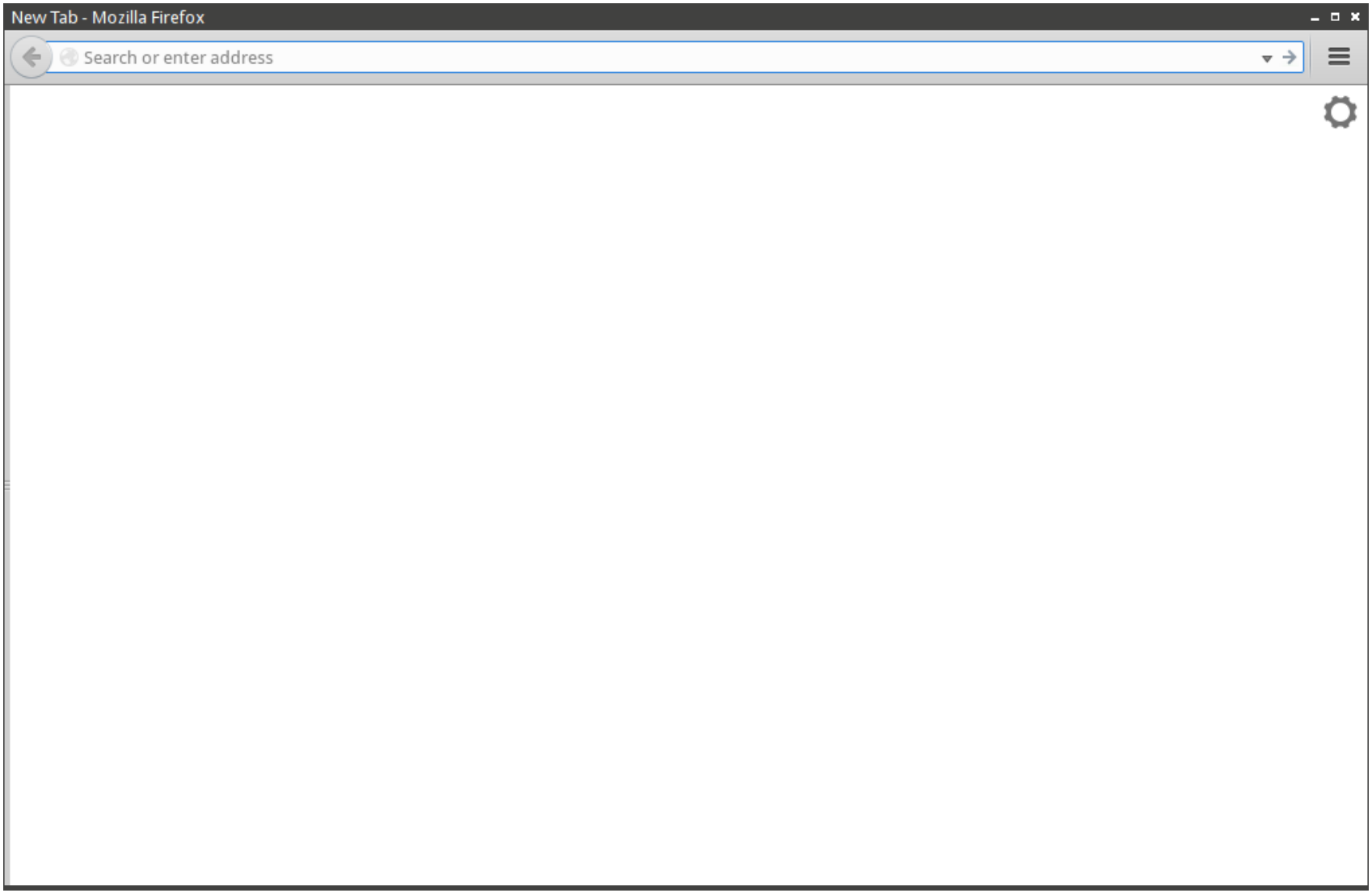
- EDNS TCP benutzen
- DO „DNSSEC OK“-Bit
- AD „Authentic Data“-Bit
- CD „Checking Disabled“-Bit

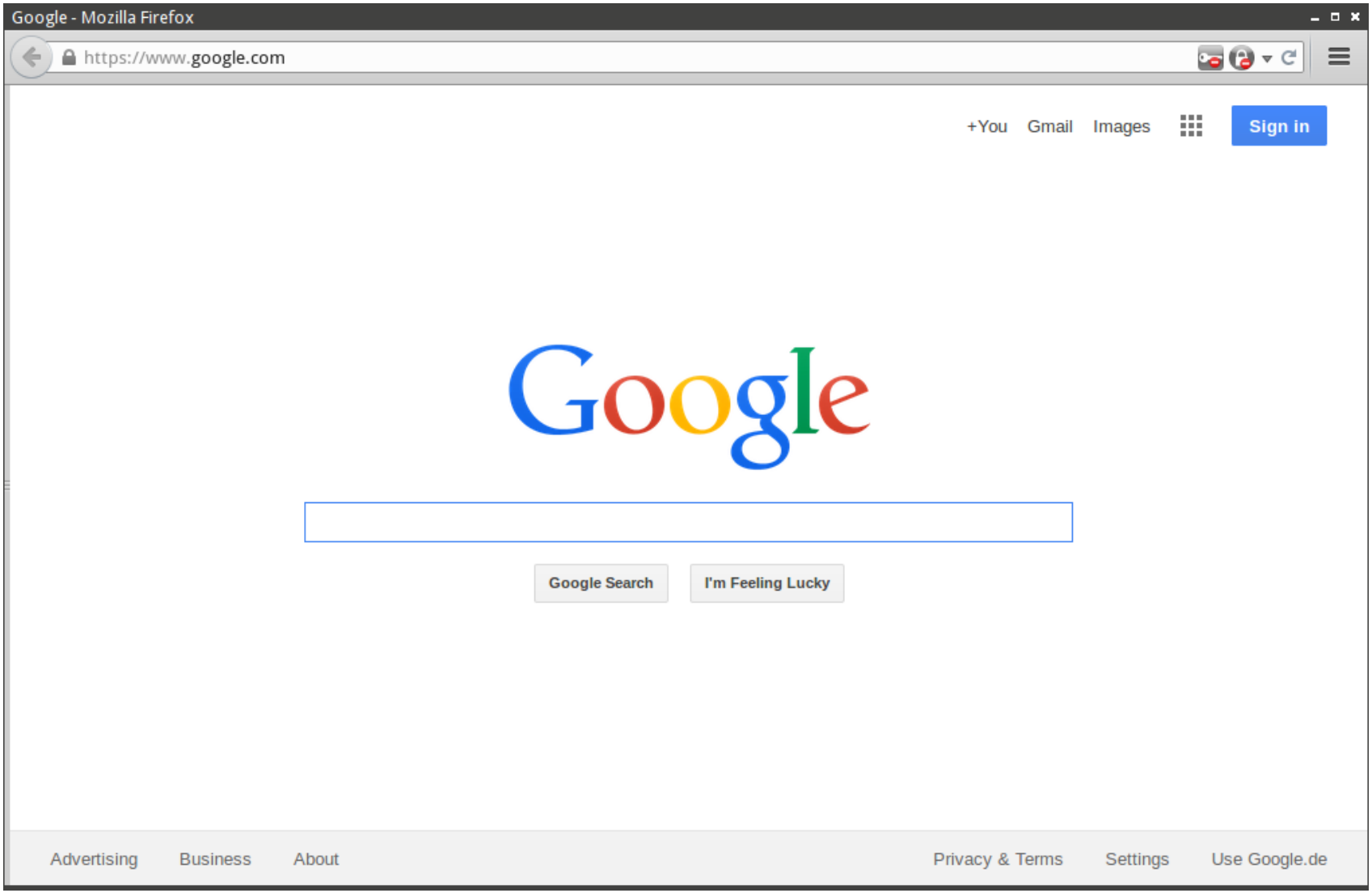
Wie funktioniert DNSSEC?

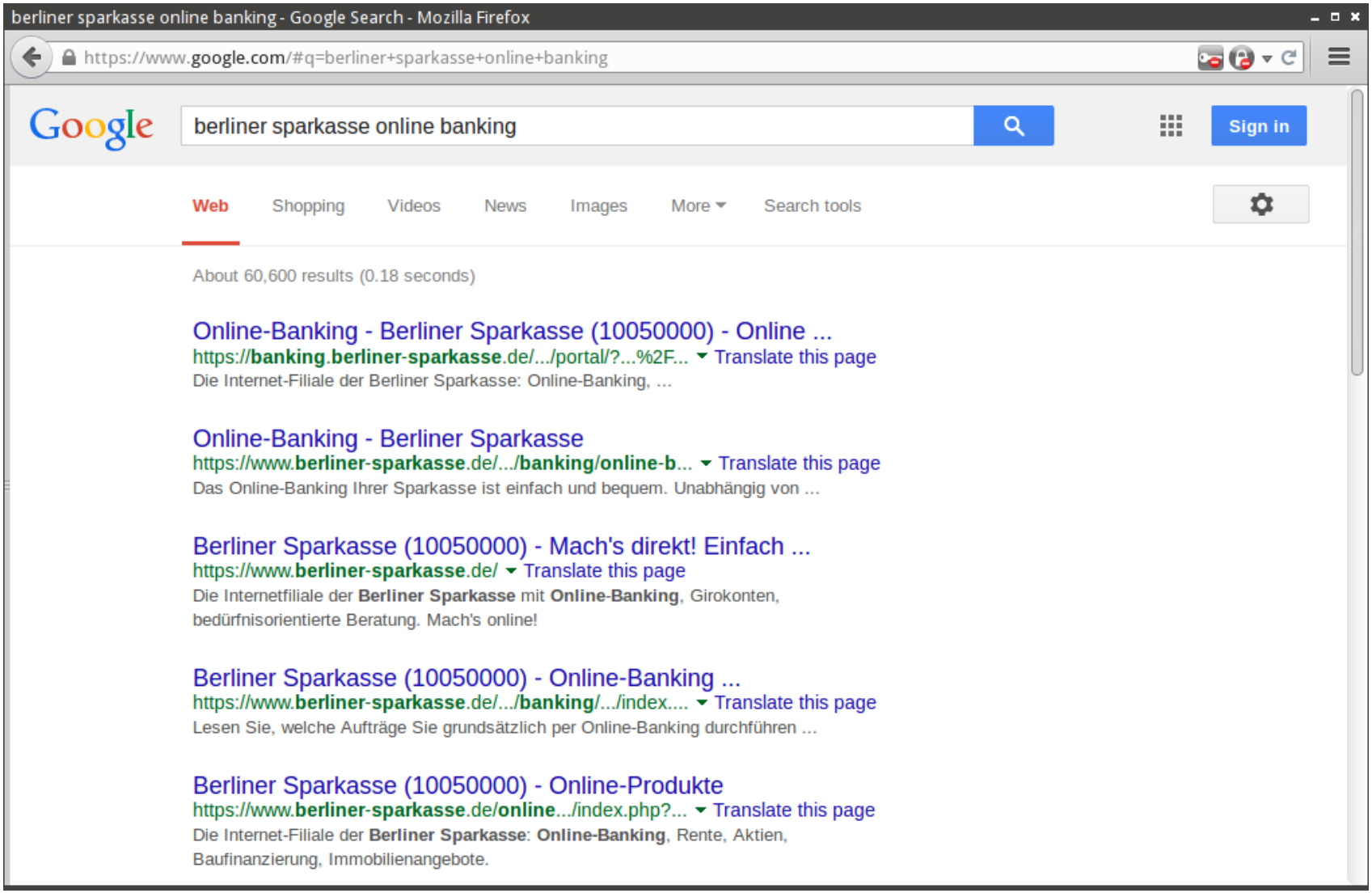


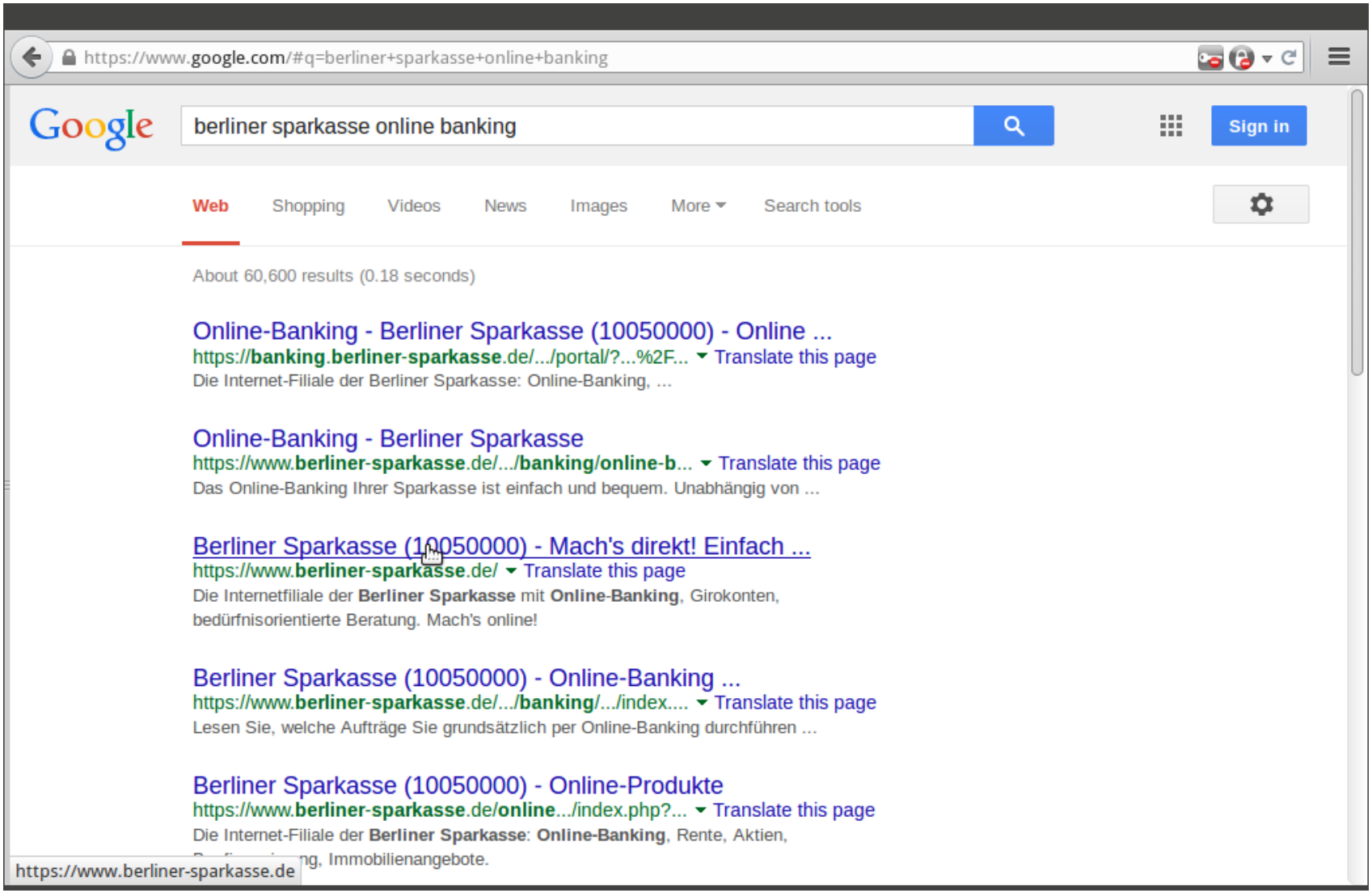
Welche Probleme hat DNSSEC?

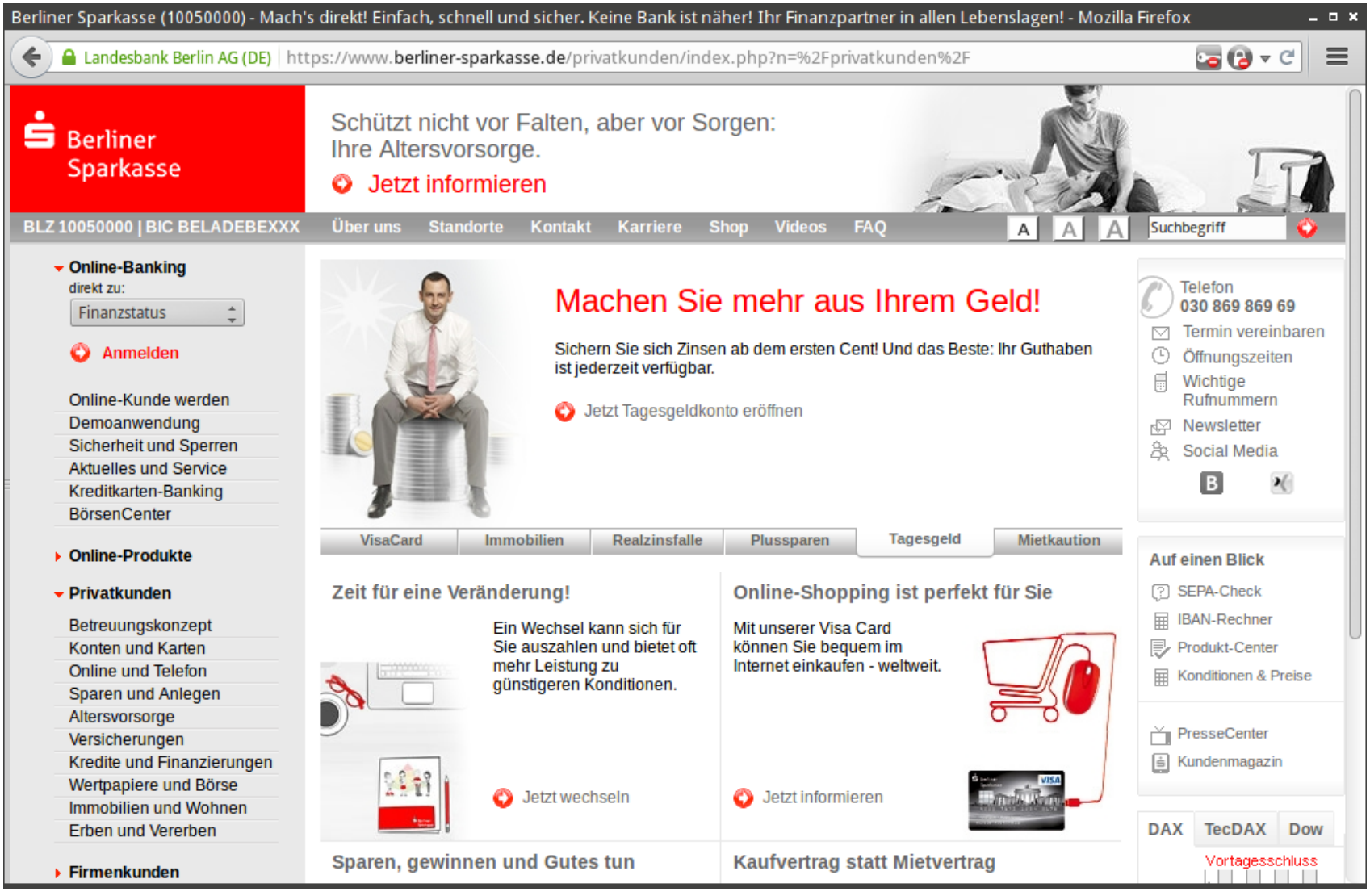
- Implementationsaufwand
- Größe der Zonen und Antworten
- Aufwand für Validierung
- Rollover von Schlüssel
- Zone Walking

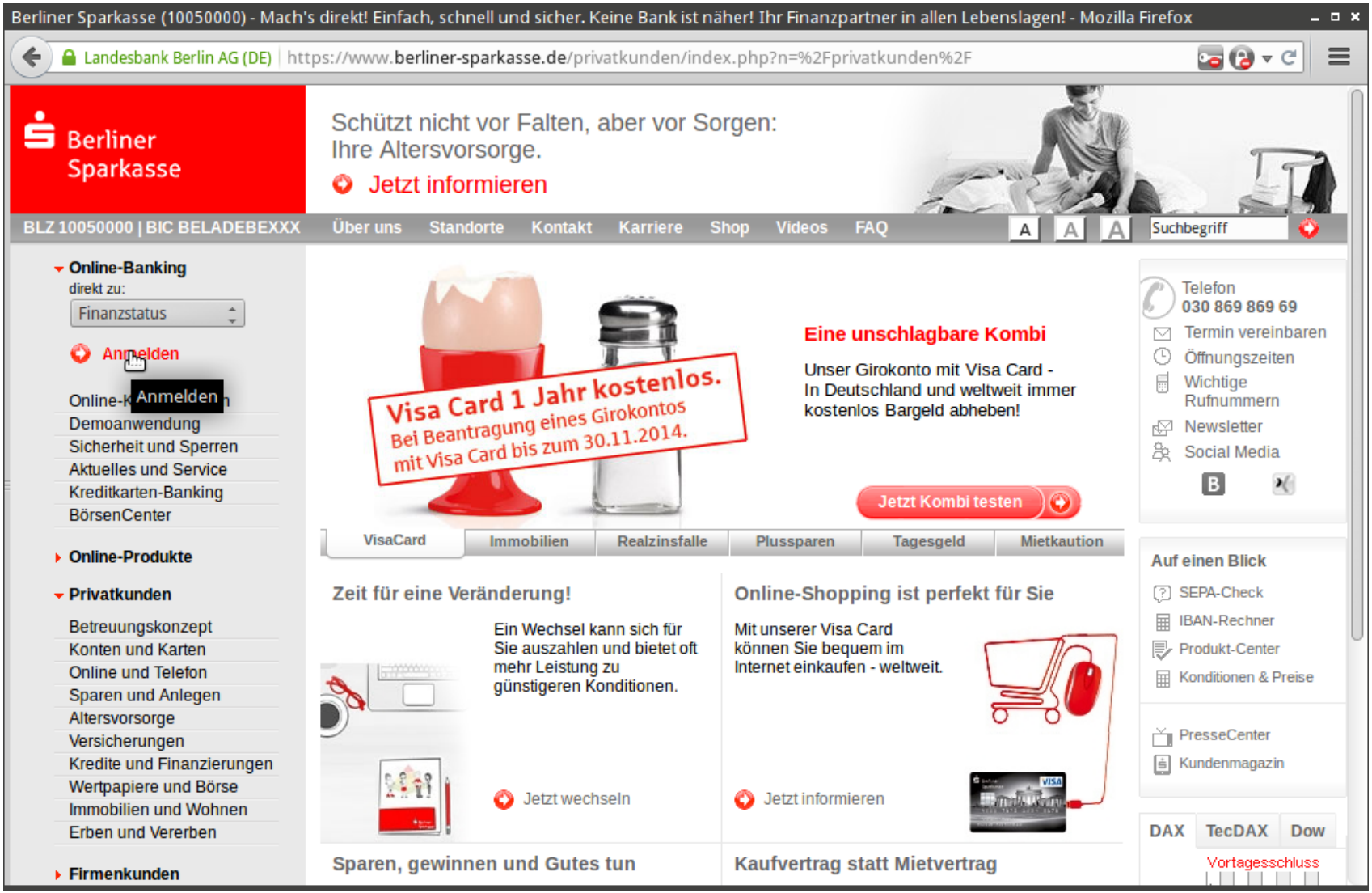

New Tab - Mozilla Firefox
Search or enter address

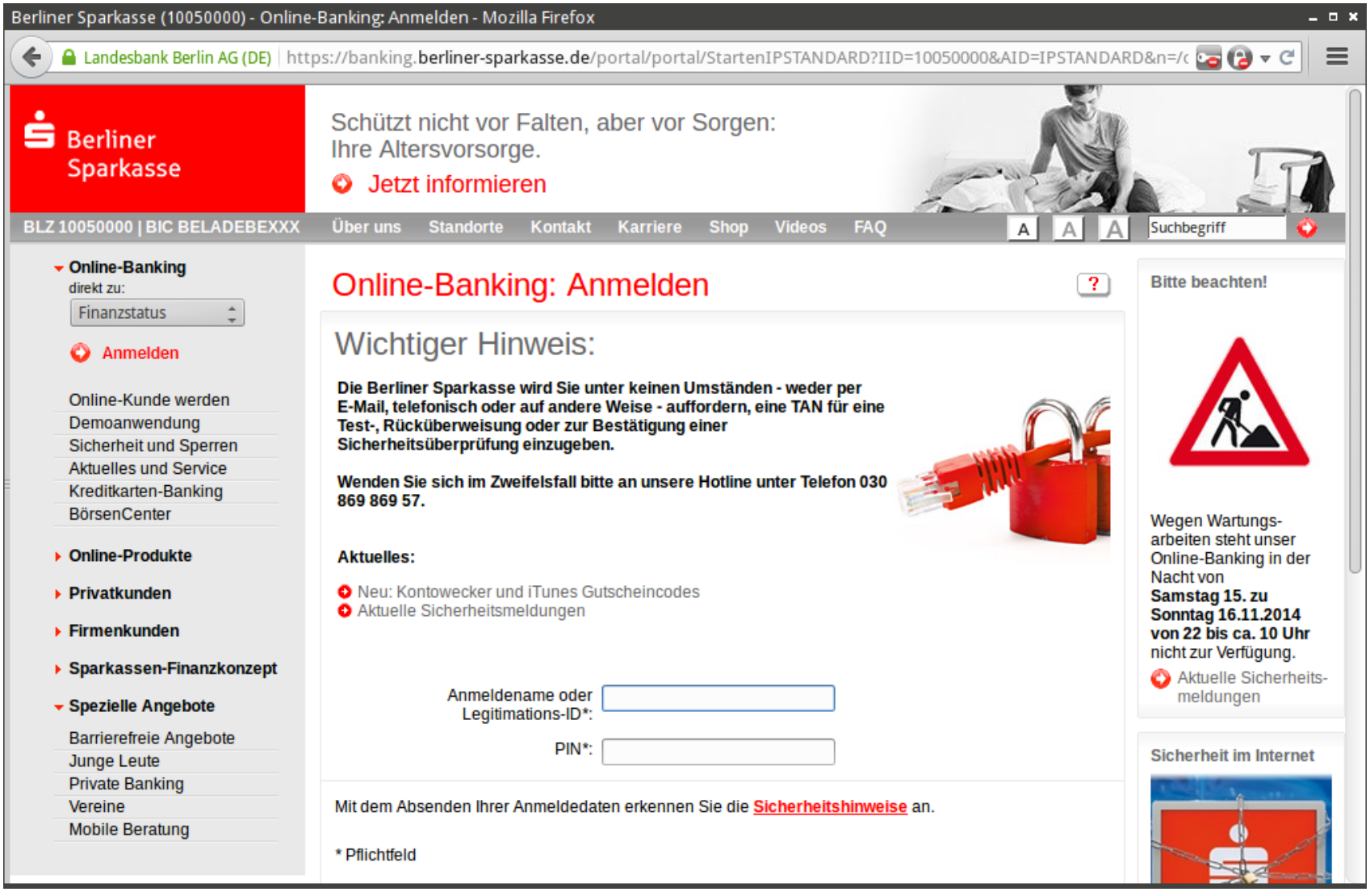

Google - Mozilla Firefox
https://www.google.com
+You
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Advertising
Business
About
Privacy & Terms
Settings
Use Google.de

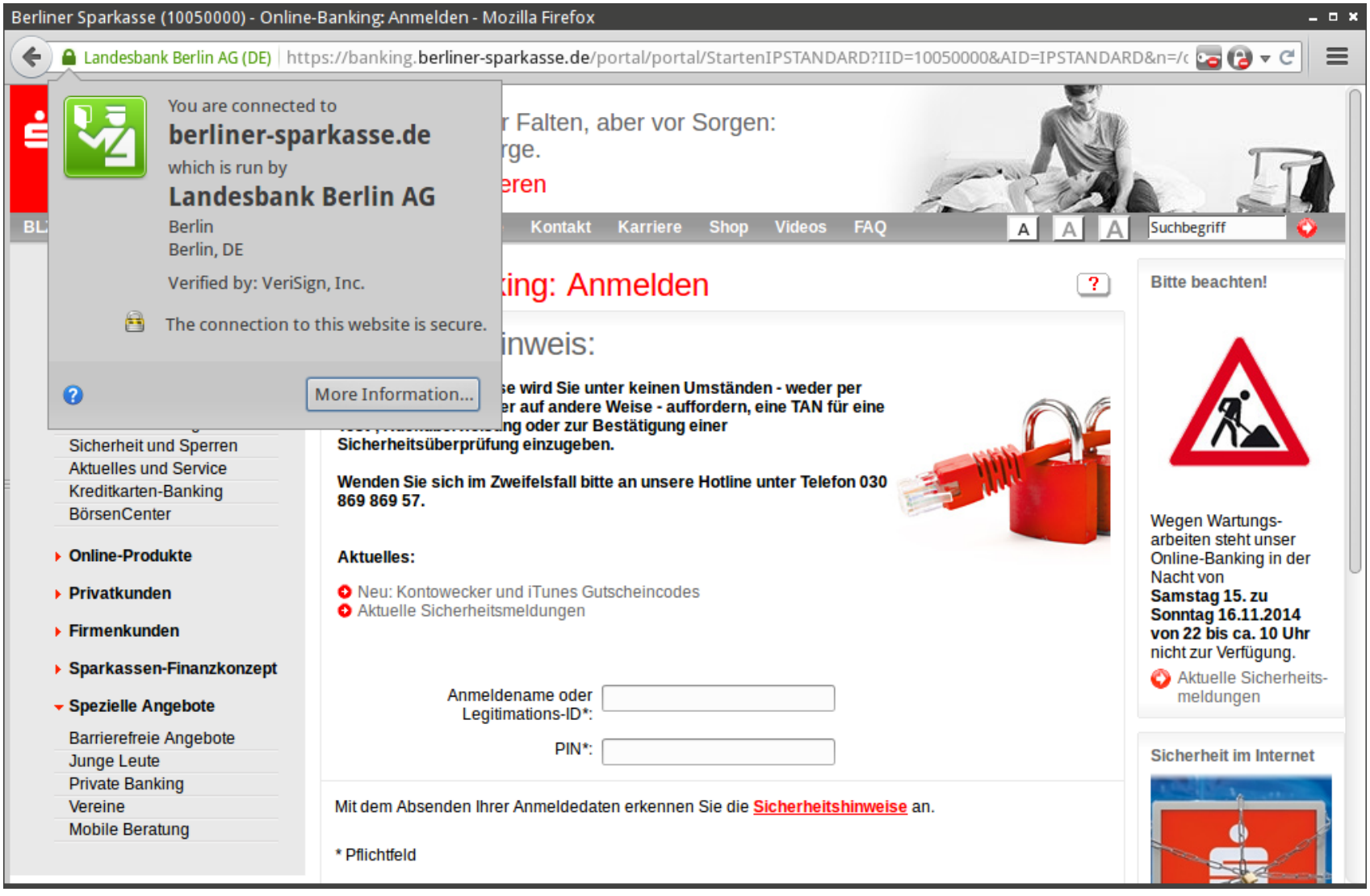

berliner sparkasse online banking - Google Search - Mozilla Firefox
https://www.google.com/#q=berliner+sparkasse+online+banking
Google
berliner sparkasse online banking
Sign in
Web
Shopping
Videos
News
Images
More
Search tools
About 60,600 results (0.18 seconds)
Online-Banking - Berliner Sparkasse (10050000) - Online ...
https://banking.berliner-sparkasse.de/.../portal/?...%2F... Translate this page
Die Internet-Filiale der Berliner Sparkasse: Online-Banking, ...
Online-Banking - Berliner Sparkasse
https://www.berliner-sparkasse.de/.../banking/online-b... Translate this page
Das Online-Banking Ihrer Sparkasse ist einfach und bequem. Unabhängig von ...
Berliner Sparkasse (10050000) - Mach's direkt! Einfach ...
https://www.berliner-sparkasse.de/ Translate this page
Die Internetfiliale der Berliner Sparkasse mit Online-Banking, Girokonten, bedürfnisorientierte Beratung. Mach's online!
Berliner Sparkasse (10050000) - Online-Banking ...
https://www.berliner-sparkasse.de/.../banking/.../index.... Translate this page
Lesen Sie, welche Aufträge Sie grundsätzlich per Online-Banking durchführen ...
Berliner Sparkasse (10050000) - Online-Produkte
https://www.berliner-sparkasse.de/online.../index.php?... Translate this page
Die Internet-Filiale der Berliner Sparkasse: Online-Banking, Rente, Aktien, Baufinanzierung, Immobilienangebote.

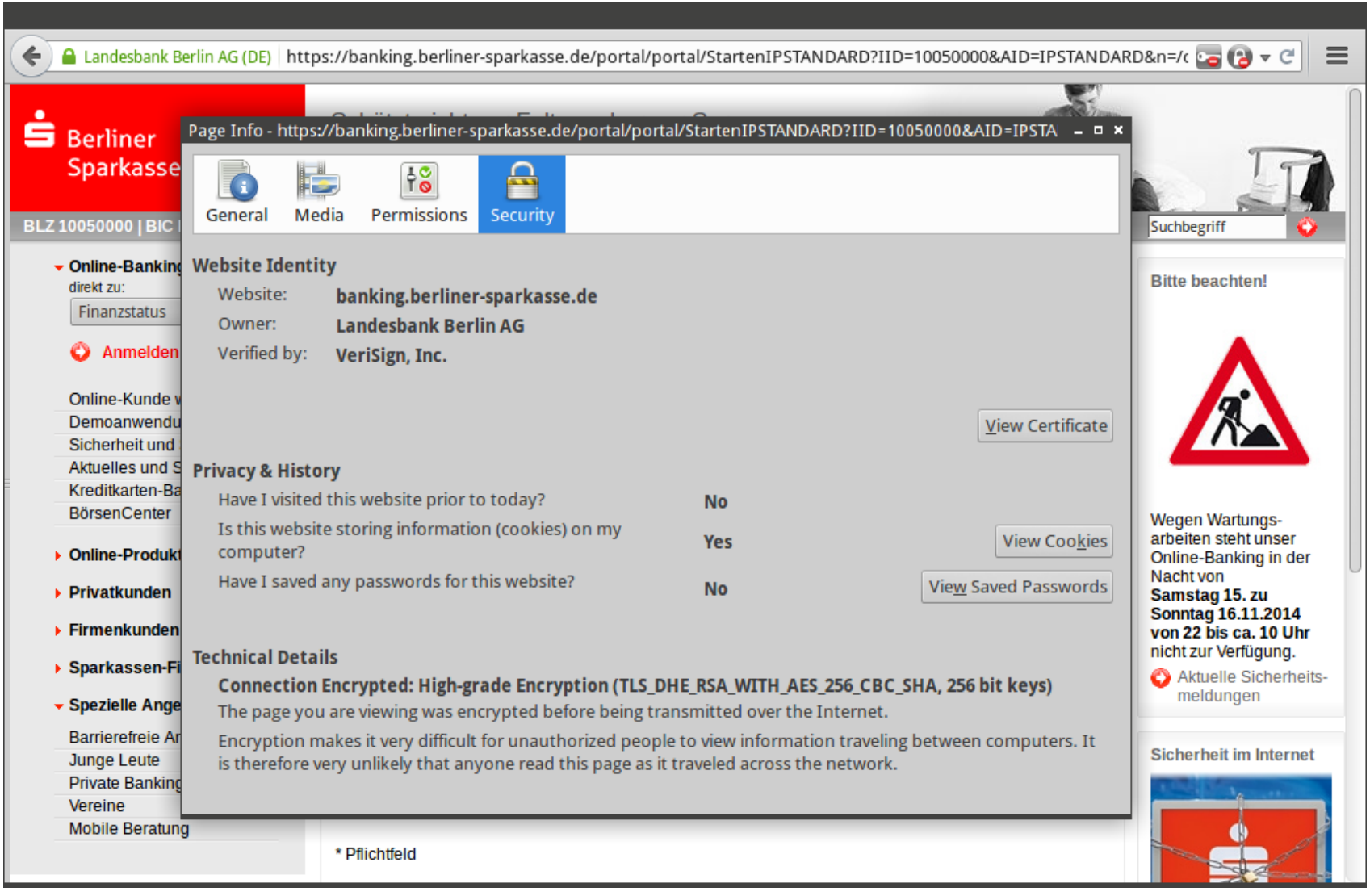

https://www.google.com/#q=berliner+sparkasse+online+banking
Google
berliner sparkasse online banking
Sign in
Web
Shopping
Videos
News
Images
More
Search tools
About 60,600 results (0.18 seconds)
Online-Banking - Berliner Sparkasse (10050000) - Online ...
https://banking.berliner-sparkasse.de/.../portal/?...%2F... Translate this page
Die Internet-Filiale der Berliner Sparkasse: Online-Banking, ...
Online-Banking - Berliner Sparkasse
https://www.berliner-sparkasse.de/.../banking/online-b... Translate this page
Das Online-Banking Ihrer Sparkasse ist einfach und bequem. Unabhängig von ...
Berliner Sparkasse (10050000) - Mach's direkt! Einfach ...
https://www.berliner-sparkasse.de/ Translate this page
Die Internetfiliale der Berliner Sparkasse mit Online-Banking, Girokonten,
bedürfnisorientierte Beratung. Mach's online!
Berliner Sparkasse (10050000) - Online-Banking ...
https://www.berliner-sparkasse.de/.../banking/.../index.... Translate this page
Lesen Sie, welche Aufträge Sie grundsätzlich per Online-Banking durchführen ...
Berliner Sparkasse (10050000) - Online-Produkte
https://www.berliner-sparkasse.de/online.../index.php?... Translate this page
Die Internet-Filiale der Berliner Sparkasse: Online-Banking, Rente, Aktien,
ng, Immobilienangebote.
https://www.berliner-sparkasse.de

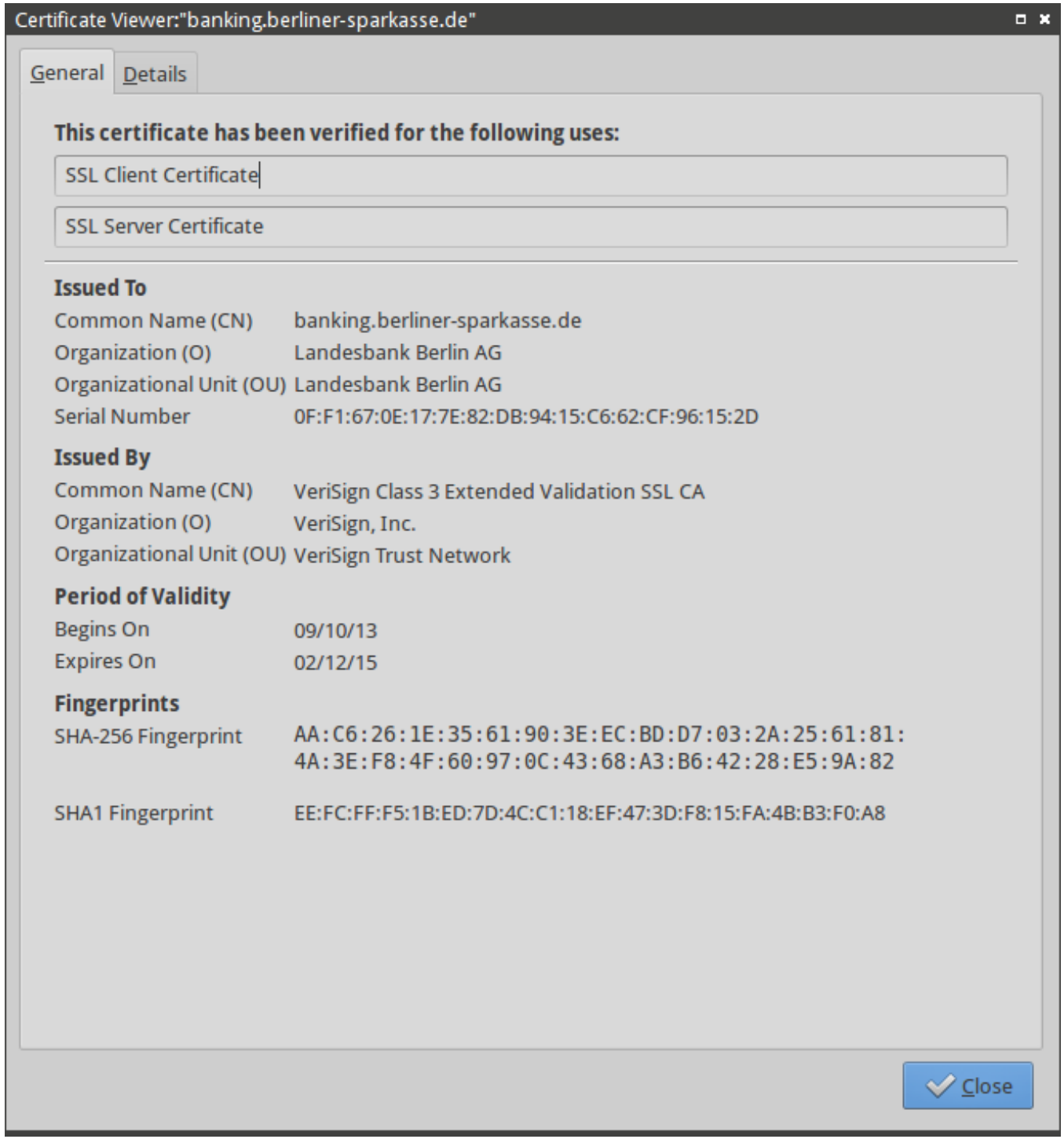

Berliner Sparkasse (10050000) - Mach's direkt! Einfach, schnell und sicher. Keine Bank ist näher! Ihr Finanzpartner in allen Lebenslagen! - Mozilla Firefox
Landesbank Berlin AG (DE)
https://www.berliner-sparkasse.de/privatkunden/index.php?n=%2Fprivatkunden%2F
Berliner Sparkasse
Schützt nicht vor Falten, aber vor Sorgen:
Ihre Altersvorsorge.
Jetzt informieren
BLZ 10050000 | BIC BELADEBEXXX
Über uns
Standorte
Kontakt
Karriere
Shop
Videos
FAQ
Suchbegriff
Online-Banking
direkt zu:
Finanzstatus
Anmelden
Online-Kunde werden
Demoanwendung
Sicherheit und Sperren
Aktuelles und Service
Kreditkarten-Banking
BörsenCenter
Online-Produkte
Privatkunden
Betreuungskonzept
Konten und Karten
Online und Telefon
Sparen und Anlegen
Altersvorsorge
Versicherungen
Kredite und Finanzierungen
Wertpapiere und Börse
Immobilien und Wohnen
Erben und Vererben
Firmenkunden
Machen Sie mehr aus Ihrem Geld!
Sichern Sie sich Zinsen ab dem ersten Cent! Und das Beste: Ihr Guthaben ist jederzeit verfügbar.
Jetzt Tagesgeldkonto eröffnen
VisaCard
Immobilien
Realzinsfalle
Plussparen
Tagesgeld
Mietkaution
Zeit für eine Veränderung!
Ein Wechsel kann sich für Sie auszahlen und bietet oft mehr Leistung zu günstigeren Konditionen.
Jetzt wechseln
Online-Shopping ist perfekt für Sie
Mit unserer Visa Card können Sie bequem im Internet einkaufen - weltweit.
Jetzt informieren
Sparen, gewinnen und Gutes tun
Kaufvertrag statt Mietvertrag
Telefon
030 869 869 69
Termin vereinbaren
Öffnungszeiten
Wichtige Rufnummern
Newsletter
Social Media
Auf einen Blick
SEPA-Check
IBAN-Rechner
Produkt-Center
Konditionen & Preise
PresseCenter
Kundenmagazin
DAX
TecDAX
Dow
Vortagesschluss

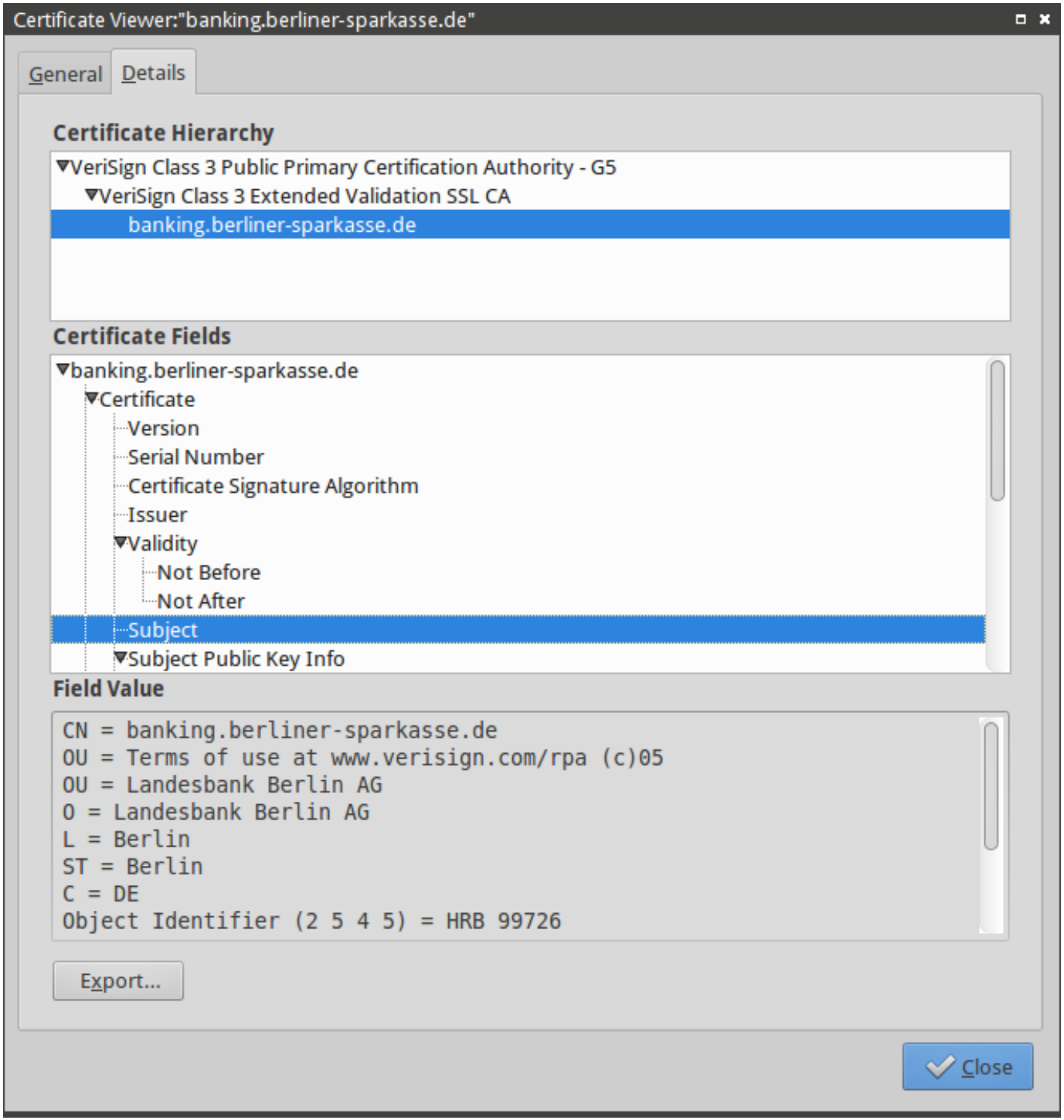

Berliner Sparkasse (10050000) - Mach's direkt! Einfach, schnell und sicher. Keine Bank ist näher! Ihr Finanzpartner in allen Lebenslagen! - Mozilla Firefox
Landesbank Berlin AG (DE)
https://www.berliner-sparkasse.de/privatkunden/index.php?n=%2Fprivatkunden%2F
Berliner Sparkasse
Schützt nicht vor Falten, aber vor Sorgen:
Ihre Altersvorsorge.
Jetzt informieren
BLZ 10050000 | BIC BELADEBEXXX
Über uns
Standorte
Kontakt
Karriere
Shop
Videos
FAQ
Suchbegriff
Online-Banking
direkt zu:
Finanzstatus
Anmelden
Demoanwendung
Sicherheit und Sperren
Aktuelles und Service
Kreditkarten-Banking
BörsenCenter
Online-Produkte
Privatkunden
Betreuungskonzept
Konten und Karten
Online und Telefon
Sparen und Anlegen
Altersvorsorge
Versicherungen
Kredite und Finanzierungen
Wertpapiere und Börse
Immobilien und Wohnen
Erben und Vererben
Firmenkunden
Visa Card 1 Jahr kostenlos.
Bei Beantragung eines Girokontos
mit Visa Card bis zum 30.11.2014.
Eine unschlagbare Kombi
Unser Girokonto mit Visa Card -
In Deutschland und weltweit immer
kostenlos Bargeld abheben!
Jetzt Kombi testen
VisaCard
Immobilien
Realzinsfalle
Plussparen
Tagesgeld
Mietkaution
Zeit für eine Veränderung!
Ein Wechsel kann sich für
Sie auszahlen und bietet oft
mehr Leistung zu
günstigeren Konditionen.
Jetzt wechseln
Online-Shopping ist perfekt für Sie
Mit unserer Visa Card
können Sie bequem im
Internet einkaufen - weltweit.
Jetzt informieren
Sparen, gewinnen und Gutes tun
Kaufvertrag statt Mietvertrag
Telefon
030 869 869 69
Termin vereinbaren
Öffnungszeiten
Wichtige
Rufnummern
Newsletter
Social Media
Auf einen Blick
SEPA-Check
IBAN-Rechner
Produkt-Center
Konditionen & Preise
PresseCenter
Kundenmagazin
DAX
TecDAX
Dow
Vortagesschluss

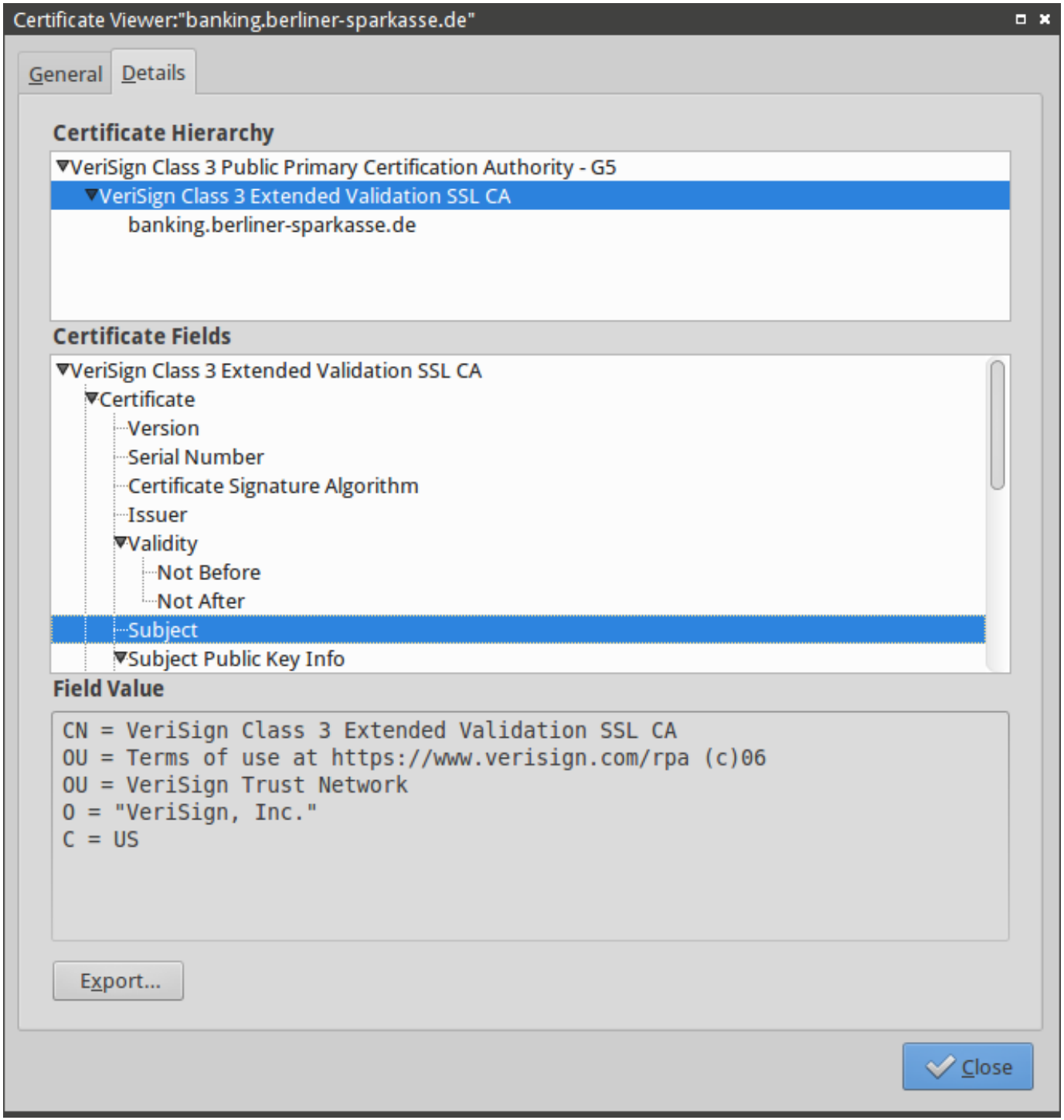

Berliner Sparkasse (10050000) - Online-Banking: Anmelden - Mozilla Firefox
Landesbank Berlin AG (DE) https://banking.berliner-sparkasse.de/portal/portal/StartenIPSTANDARD?IID=10050000&AID=IPSTANDARD&n=/c
Berliner Sparkasse
Schützt nicht vor Falten, aber vor Sorgen:
Ihre Altersvorsorge.
Jetzt informieren
BLZ 10050000 | BIC BELADEBEXXX
Über uns
Standorte
Kontakt
Karriere
Shop
Videos
FAQ
A
A
A
Suchbegriff
Online-Banking
direkt zu:
Finanzstatus
Anmelden
Online-Kunde werden
Demoanwendung
Sicherheit und Sperren
Aktuelles und Service
Kreditkarten-Banking
BörsenCenter
Online-Produkte
Privatkunden
Firmenkunden
Sparkassen-Finanzkonzept
Spezielle Angebote
Barrierefreie Angebote
Junge Leute
Private Banking
Vereine
Mobile Beratung
Online-Banking: Anmelden
Wichtiger Hinweis:
Die Berliner Sparkasse wird Sie unter keinen Umständen - weder per E-Mail, telefonisch oder auf andere Weise - auffordern, eine TAN für eine Test-, Rücküberweisung oder zur Bestätigung einer Sicherheitsüberprüfung einzugeben.
Wenden Sie sich im Zweifelsfall bitte an unsere Hotline unter Telefon 030 869 869 57.
Aktuelles:
Neu: Kontowecker und iTunes Gutscheincodes
Aktuelle Sicherheitsmeldungen
Anmeldename oder Legitimations-ID*:
PIN*:
Mit dem Absenden Ihrer Anmeldedaten erkennen Sie die Sicherheitshinweise an.
* Pflichtfeld
Bitte beachten!
Wegen Wartungs-arbeiten steht unser Online-Banking in der Nacht von Samstag 15. zu Sonntag 16.11.2014 von 22 bis ca. 10 Uhr nicht zur Verfügung.
Aktuelle Sicherheits-meldungen
Sicherheit im Internet

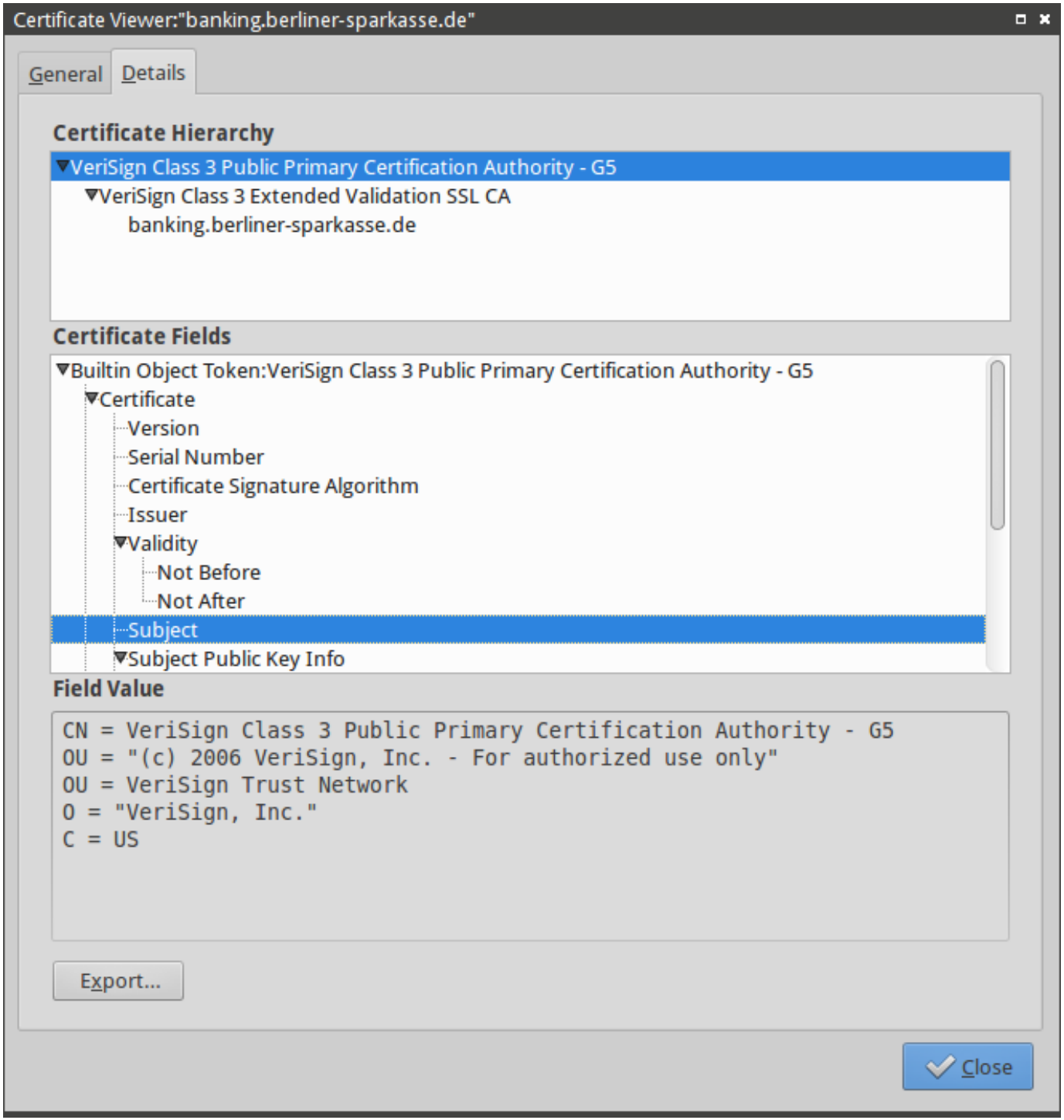

Berliner Sparkasse (10050000) - Online-Banking: Anmelden - Mozilla Firefox
Landesbank Berlin AG (DE)
https://banking.berliner-sparkasse.de/portal/portal/StartenIPSTANDARD?IID=10050000&AID=IPSTANDARD&n=/c
You are connected to
berliner-sparkasse.de
which is run by
Landesbank Berlin AG
Berlin
Berlin, DE
Verified by: VeriSign, Inc.
The connection to this website is secure.
More Information...
r Falten, aber vor Sorgen:
rge.
eren
Kontakt
Karriere
Shop
Videos
FAQ
Suchbegriff
king: Anmelden
inweis:
se wird Sie unter keinen Umständen - weder per
er auf andere Weise - auffordern, eine TAN für eine
ng oder zur Bestätigung einer
Sicherheitsüberprüfung einzugeben.
Wenden Sie sich im Zweifelsfall bitte an unsere Hotline unter Telefon 030 869 869 57.
Aktuelles:
Neu: Kontowecker und iTunes Gutscheincodes
Aktuelle Sicherheitsmeldungen
Anmeldename oder Legitimations-ID*:
PIN*:
Mit dem Absenden Ihrer Anmeldedaten erkennen Sie die Sicherheitshinweise an.
* Pflichtfeld
Sicherheit und Sperren
Aktuelles und Service
Kreditkarten-Banking
BörsenCenter
Online-Produkte
Privatkunden
Firmenkunden
Sparkassen-Finanzkonzept
Spezielle Angebote
Barrierefreie Angebote
Junge Leute
Private Banking
Vereine
Mobile Beratung
Bitte beachten!
Wegen Wartungs-arbeiten steht unser Online-Banking in der Nacht von Samstag 15. zu Sonntag 16.11.2014 von 22 bis ca. 10 Uhr nicht zur Verfügung.
Aktuelle Sicherheits-meldungen
Sicherheit im Internet

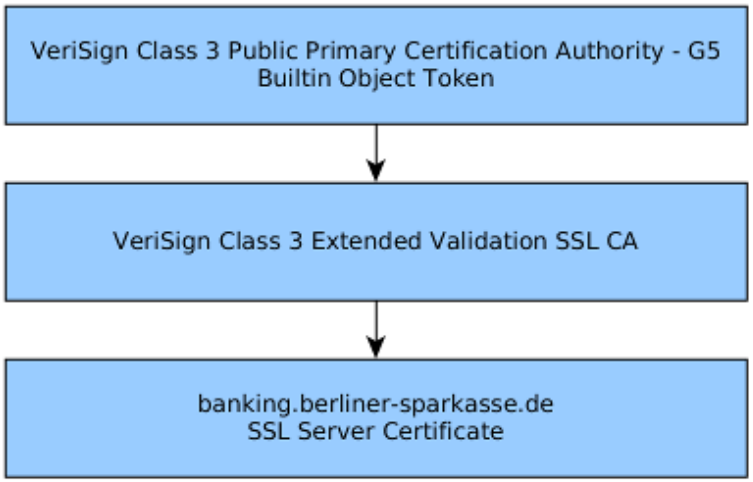

Landesbank Berlin AG (DE)
https://banking.berliner-sparkasse.de/portal/portal/StartenIPSTANDARD?IID=10050000&AID=IPSTANDARD&n=/c
Berliner Sparkasse
BLZ 10050000 | BIC
Online-Banking
direkt zu:
Finanzstatus
Anmelden
Online-Kunde w
Demoanwendu
Sicherheit und
Aktuelles und S
Kreditkarten-Ba
BörsenCenter
Online-Produkt
Privatkunden
Firmenkunden
Sparkassen-Fi
Spezielle Ange
Barrierefreie Ar
Junge Leute
Private Banking
Vereine
Mobile Beratung
* Pflichtfeld
Page Info - https://banking.berliner-sparkasse.de/portal/portal/StartenIPSTANDARD?IID=10050000&AID=IPSTA
General
Media
Permissions
Security
Website Identity
Website: banking.berliner-sparkasse.de
Owner: Landesbank Berlin AG
Verified by: VeriSign, Inc.
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted: High-grade Encryption (TLS_DHE_RSA_WITH_AES_256_CBC_SHA, 256 bit keys)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.
Suchbegriff
Bitte beachten!
Wegen Wartungs-arbeiten steht unser Online-Banking in der Nacht von Samstag 15. zu Sonntag 16.11.2014 von 22 bis ca. 10 Uhr nicht zur Verfügung.
Aktuelle Sicherheits-meldungen
Sicherheit im Internet

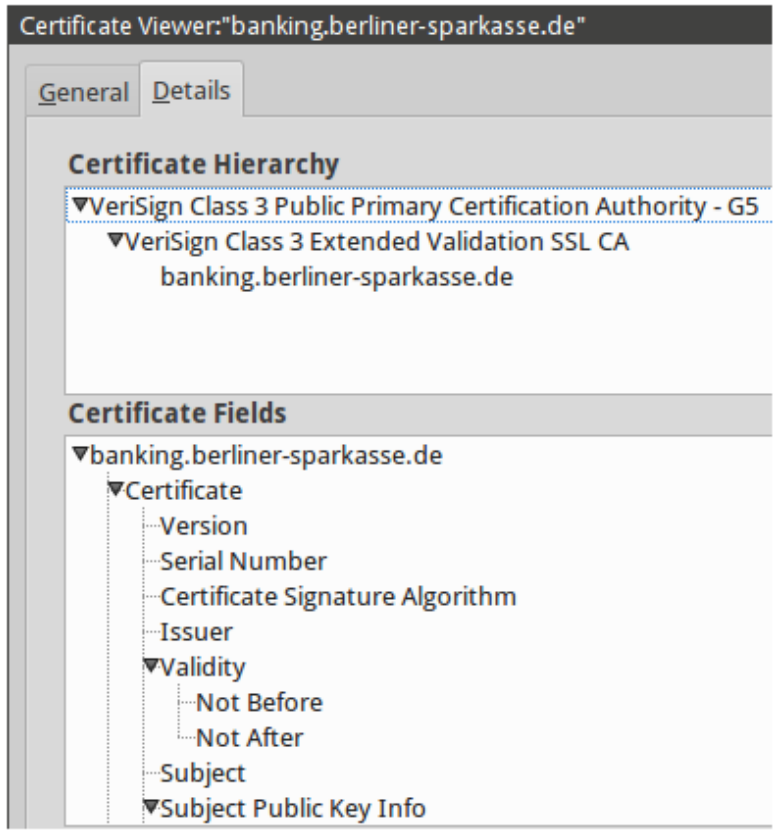

Certificate Viewer:"banking.berliner-sparkasse.de"
General
Details
This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate
Issued To
Common Name (CN) banking.berliner-sparkasse.de
Organization (O) Landesbank Berlin AG
Organizational Unit (OU) Landesbank Berlin AG
Serial Number 0F:F1:67:0E:17:7E:82:DB:94:15:C6:62:CF:96:15:2D
Issued By
Common Name (CN) VeriSign Class 3 Extended Validation SSL CA
Organization (O) VeriSign, Inc.
Organizational Unit (OU) VeriSign Trust Network
Period of Validity
Begins On 09/10/13
Expires On 02/12/15
Fingerprints
SHA-256 Fingerprint AA:C6:26:1E:35:61:90:3E:EC:BD:D7:03:2A:25:61:81:
4A:3E:F8:4F:60:97:0C:43:68:A3:B6:42:28:E5:9A:82
SHA1 Fingerprint EE:FC:FF:F5:1B:ED:7D:4C:C1:18:EF:47:3D:F8:15:FA:4B:B3:F0:A8
Close


Certificate Viewer:"banking.berliner-sparkasse.de"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
banking.berliner-sparkasse.de
Certificate Fields
banking.berliner-sparkasse.de
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Field Value
CN = banking.berliner-sparkasse.de
OU = Terms of use at www.verisign.com/rpa (c)05
OU = Landesbank Berlin AG
O = Landesbank Berlin AG
L = Berlin
ST = Berlin
C = DE
Object Identifier (2 5 4 5) = HRB 99726
Export...
Close


Certificate Viewer:"banking.berliner-sparkasse.de"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
banking.berliner-sparkasse.de
Certificate Fields
VeriSign Class 3 Extended Validation SSL CA
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Field Value
CN = VeriSign Class 3 Extended Validation SSL CA
OU = Terms of use at https://www.verisign.com/rpa (c)06
OU = VeriSign Trust Network
O = "VeriSign, Inc."
C = US
Export...
Close


Certificate Viewer:"banking.berliner-sparkasse.de"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
banking.berliner-sparkasse.de
Certificate Fields
Builtin Object Token:VeriSign Class 3 Public Primary Certification Authority - G5
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Field Value
CN = VeriSign Class 3 Public Primary Certification Authority - G5
OU = "(c) 2006 VeriSign, Inc. - For authorized use only"
OU = VeriSign Trust Network
O = "VeriSign, Inc."
C = US
Export...
Close


VeriSign Class 3 Public Primary Certification Authority - G5
Builtin Object Token
VeriSign Class 3 Extended Validation SSL CA
banking.berliner-sparkasse.de
SSL Server Certificate


Certificate Viewer:"banking.berliner-sparkasse.de"
General
Details
Certificate Hierarchy
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Extended Validation SSL CA
banking.berliner-sparkasse.de
Certificate Fields
banking.berliner-sparkasse.de
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info

DANE

DNS-based Authentication of Named Entities

Was ist DANE?

DANE ist eine Sammlung von Internet Standards.

- RFC 6394 Use Cases and Requirements for DANE
- **RFC 6698** The DANE TLS Protocol: TLSA
  - RFC 7218 Adding Acronyms to Simplify Conversations about DANE

DANE bescreibt, wie „Named Entities“ in DNS und DNSSEC

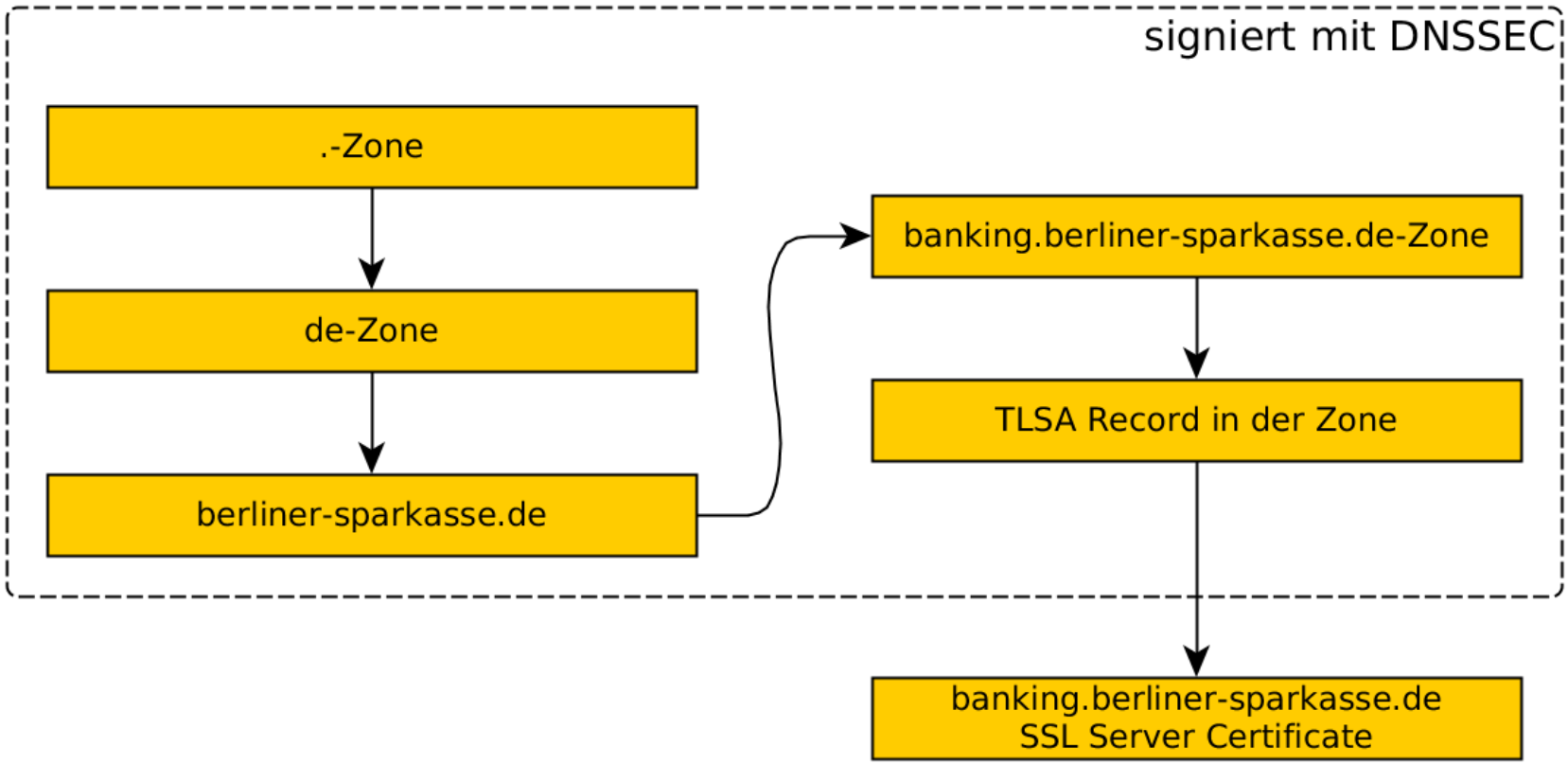
- **repräsentiert** und
- **authentifiziert** werden.

„Named Entities“ sind

- Webseiten und Server,
- E-Mail-Adressen,
- Jabber/Chat IDs usw.

Internet Drafts für OpenPGP, S/MIME, **SMTP**, IPsec, OTR, STUN, SIP.

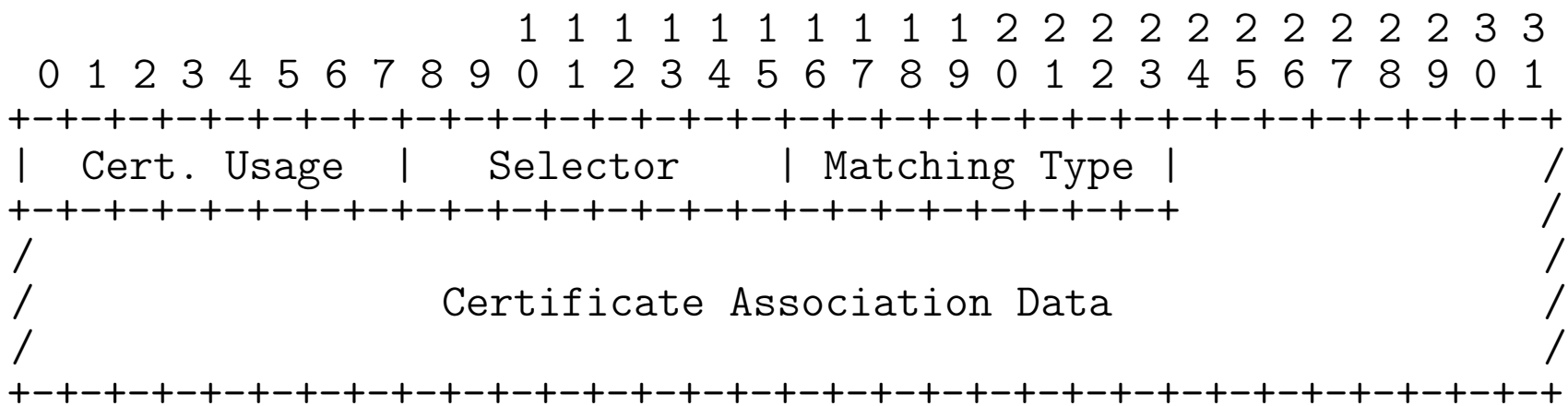
Wie funktioniert DANE?



TLSA Record Namen

- Ähnlich wie bei SRV Records.
- Port und Protokoll als Präfix.
- z.B.: TLSA Record für `https://mitakas.com`
  - `_443._tcp.mitakas.com.`
- z.B.: TLSA Record für SMTP
  - `_587._tcp.mitakas.com.`

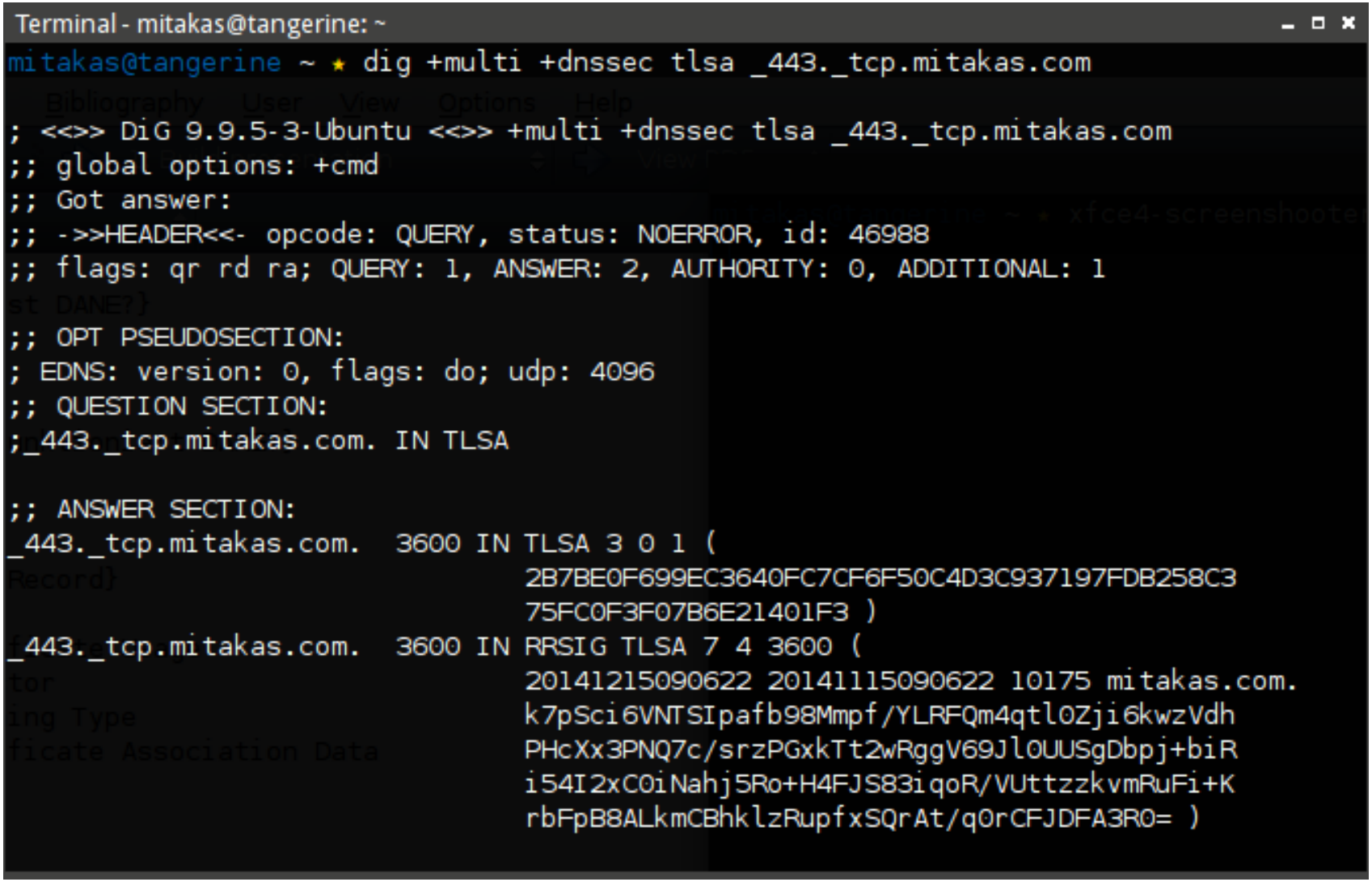
TLSA RDATA Wire Format



TLSA Record Felder

- Certificate Usage
  - 0 CA constraint
  - 1 Service certificate constraint
  - 2 Trust anchor assertion
  - 3 Domain-issued certificate
- Selector
  - 0 Full certificate
  - 1 SubjectPublicKeyInfo
- Matching Type
  - 0 No hash used
  - 1 SHA-256
  - 2 SHA-512
- Certificate Association Data

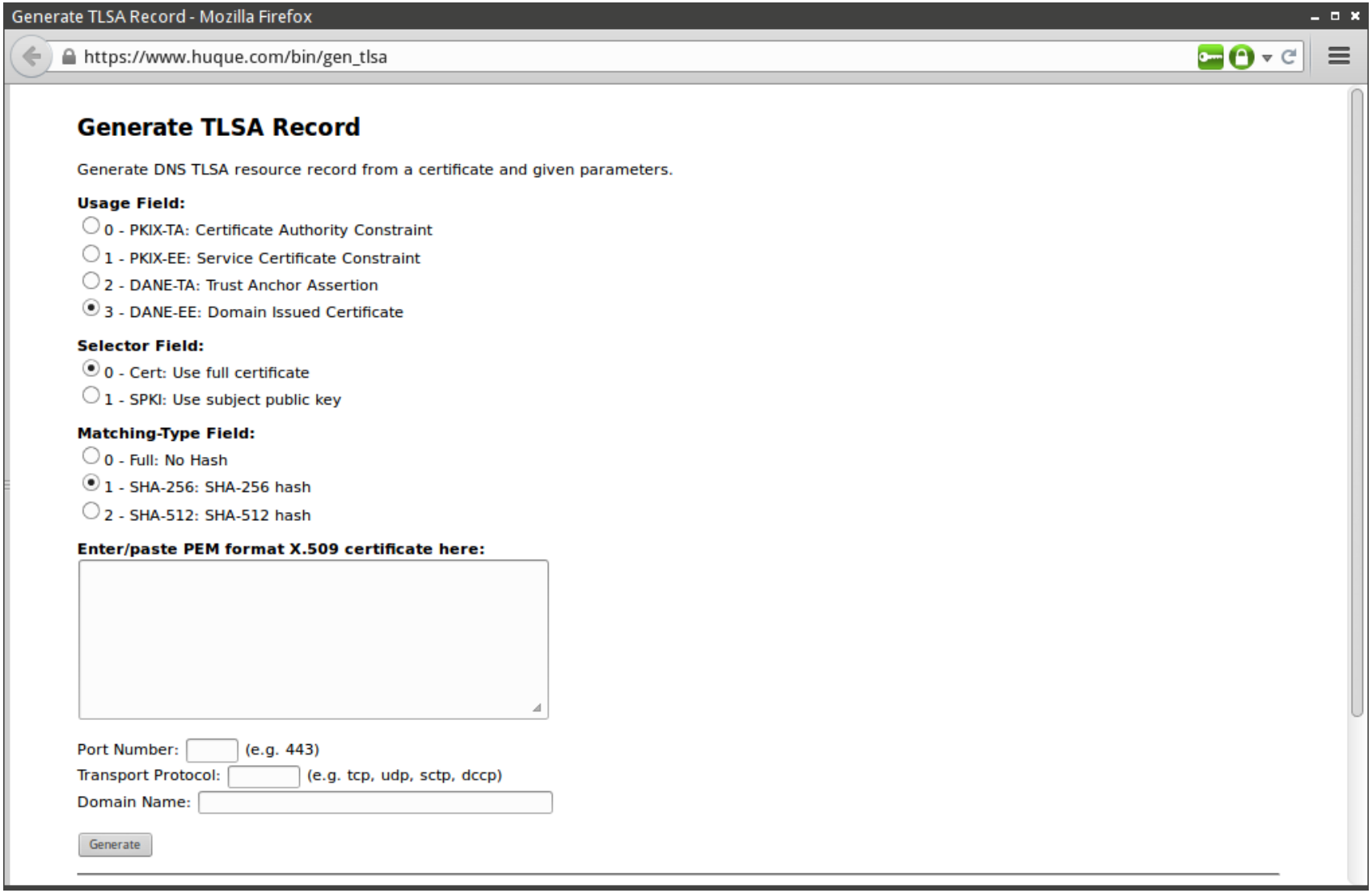
Beispiele


Terminal - mitakas@tangerine: ~
mitakas@tangerine ~ ★ dig +multi +dnssec tlsa _443._tcp.mitakas.com
; <<>> DiG 9.9.5-3-Ubuntu <<>> +multi +dnssec tlsa _443._tcp.mitakas.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46988
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;_443._tcp.mitakas.com. IN TLSA
;; ANSWER SECTION:
_443._tcp.mitakas.com. 3600 IN TLSA 3 0 1 (
2B7BE0F699EC3640FC7CF6F50C4D3C937197FDB258C3
75FC0F3F07B6E21401F3)
_443._tcp.mitakas.com. 3600 IN RRSIG TLSA 7 4 3600 (
20141215090622 20141115090622 10175 mitakas.com.
k7pSci6VNTSIpafb98Mmpf/YLRFQm4qtl0Zji6kwzVdh
PHcXx3PNQ7c/srzPGxkTt2wRggV69Jl0UUSgDbpj+biR
i54I2xC0iNahj5Ro+H4FJS83iqoR/VUttzzkvmRuFi+K
rbFpB8ALkmCBhklzRupfxSQrAt/q0rCFJDFA3R0=)

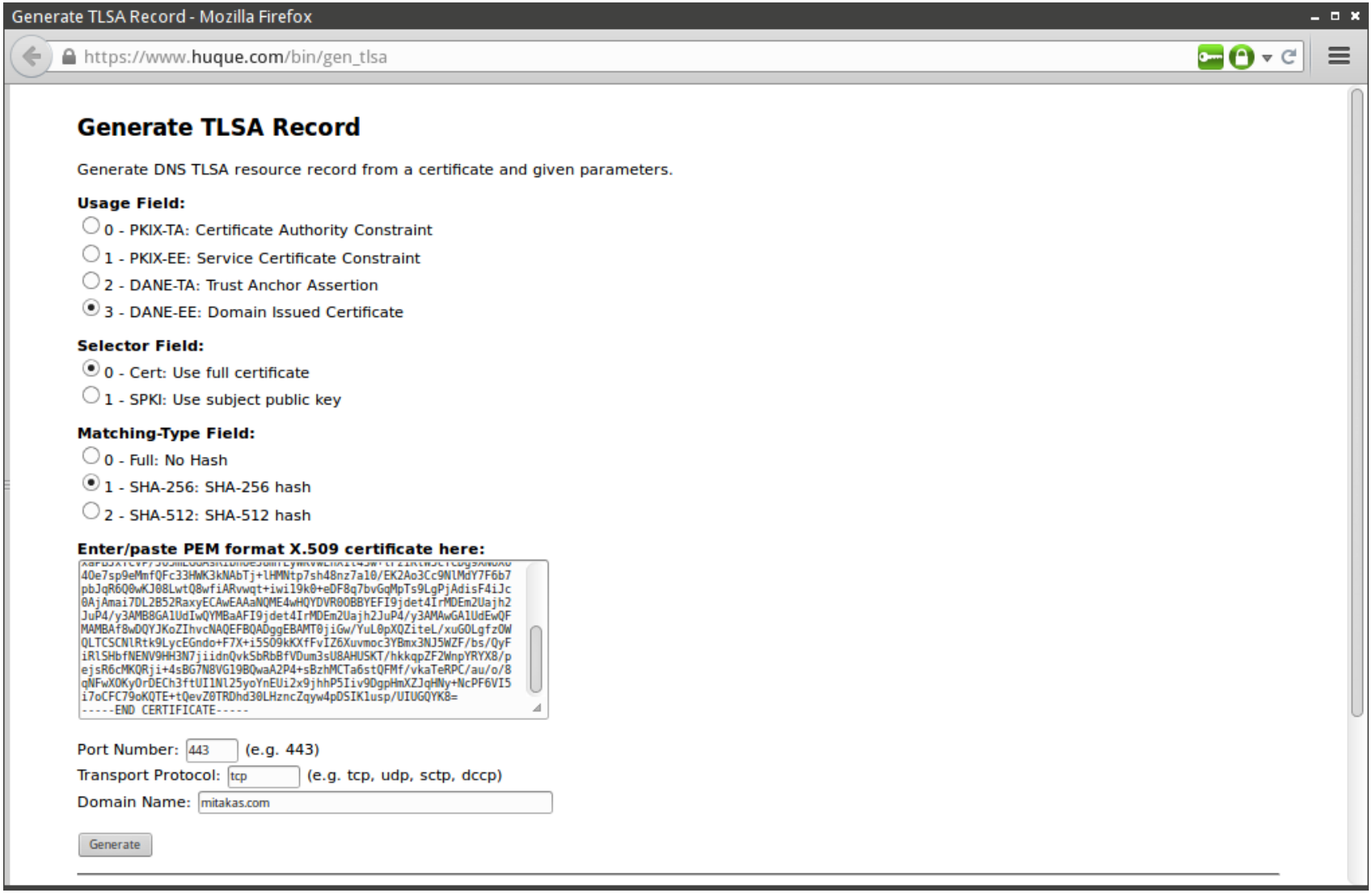
Beispiele

```
▼ Queries
  ▼ _443._tcp.mitakas.com: type TLSA, class IN
      Name: _443._tcp.mitakas.com
      Type: TLSA (TLSA)
      Class: IN (0x0001)
▼ Answers
  ▼ _443._tcp.mitakas.com: type TLSA, class IN
      Name: _443._tcp.mitakas.com
      Type: TLSA (TLSA)
      Class: IN (0x0001)
      Time to live: 1 hour
      Data length: 35
      Certificate Usage: Domain-issued certificate (3)
      Selector: Full certificate (0)
      Matching Type: SHA-256 (1)
      Certificate Association Data: 2b7be0f699ec3640fc7cf6f50c4d3c937197fdb258c375fc...
  ▶ _443._tcp.mitakas.com: type RRSIG, class IN
```

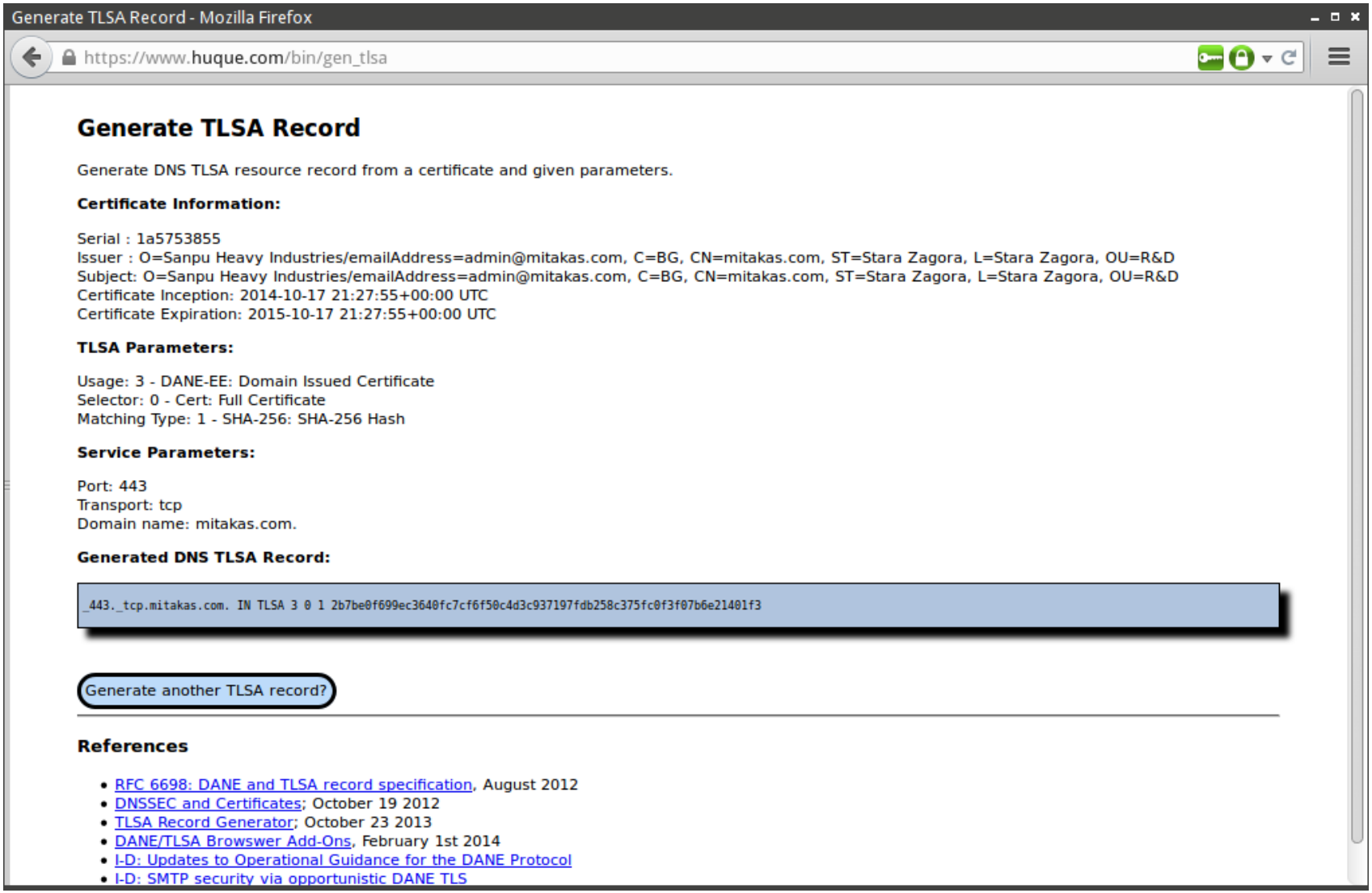
TLSA Records erzeugen



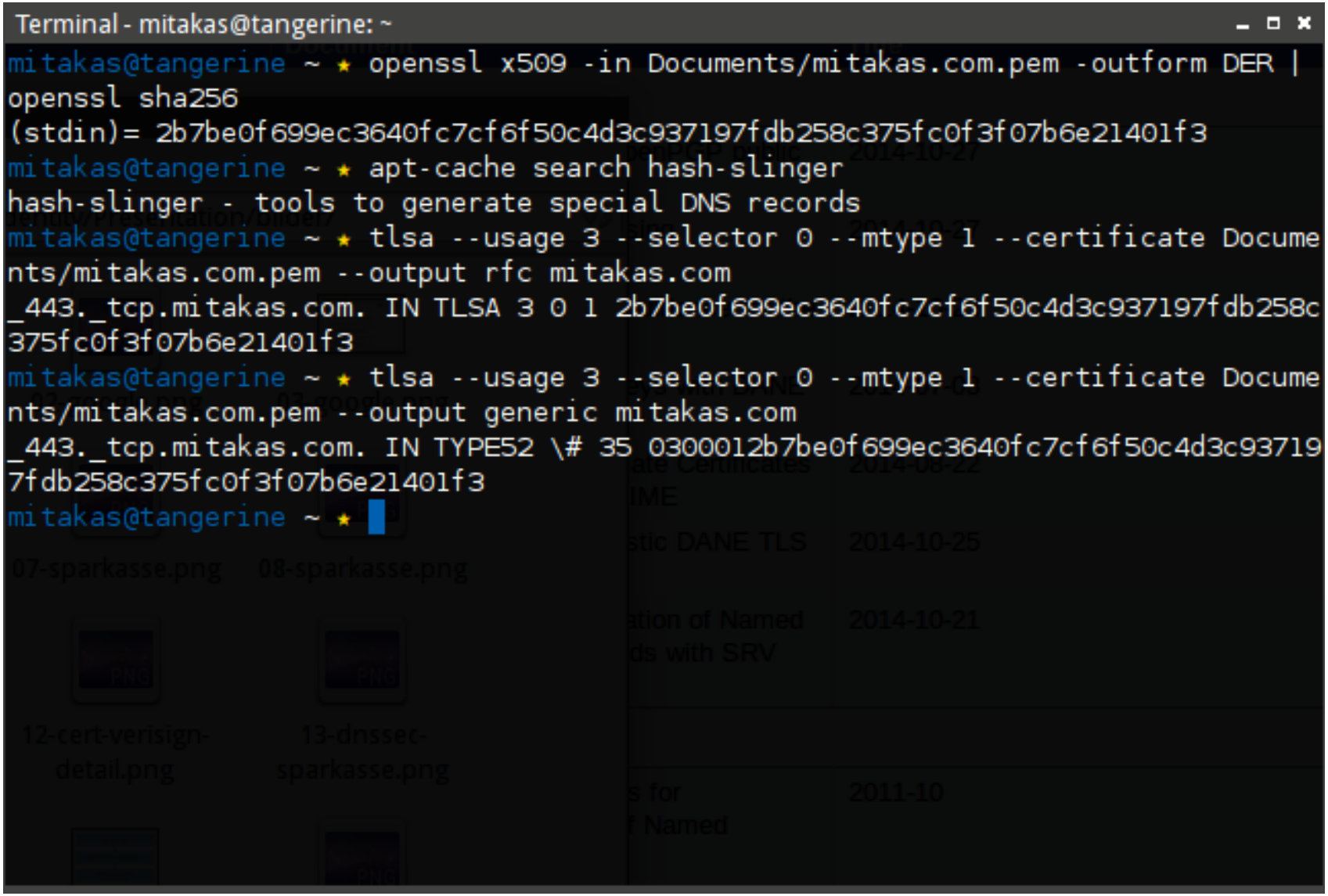
TLSA Records erzeugen



TLSA Records erzeugen



TLSA Records erzeugen



Welche Probleme hat DANE?

DANE Deployment Observations (Internet Draft)

- Awareness of DANE
- Creation of TLSA records
- Inability to enter TLSA records at DNS hosting operators
- Availability of developer libraries
- Perception that DANE is only for self-signed certificates
- Performance
- Cryptographic concerns

DANE und SMTP

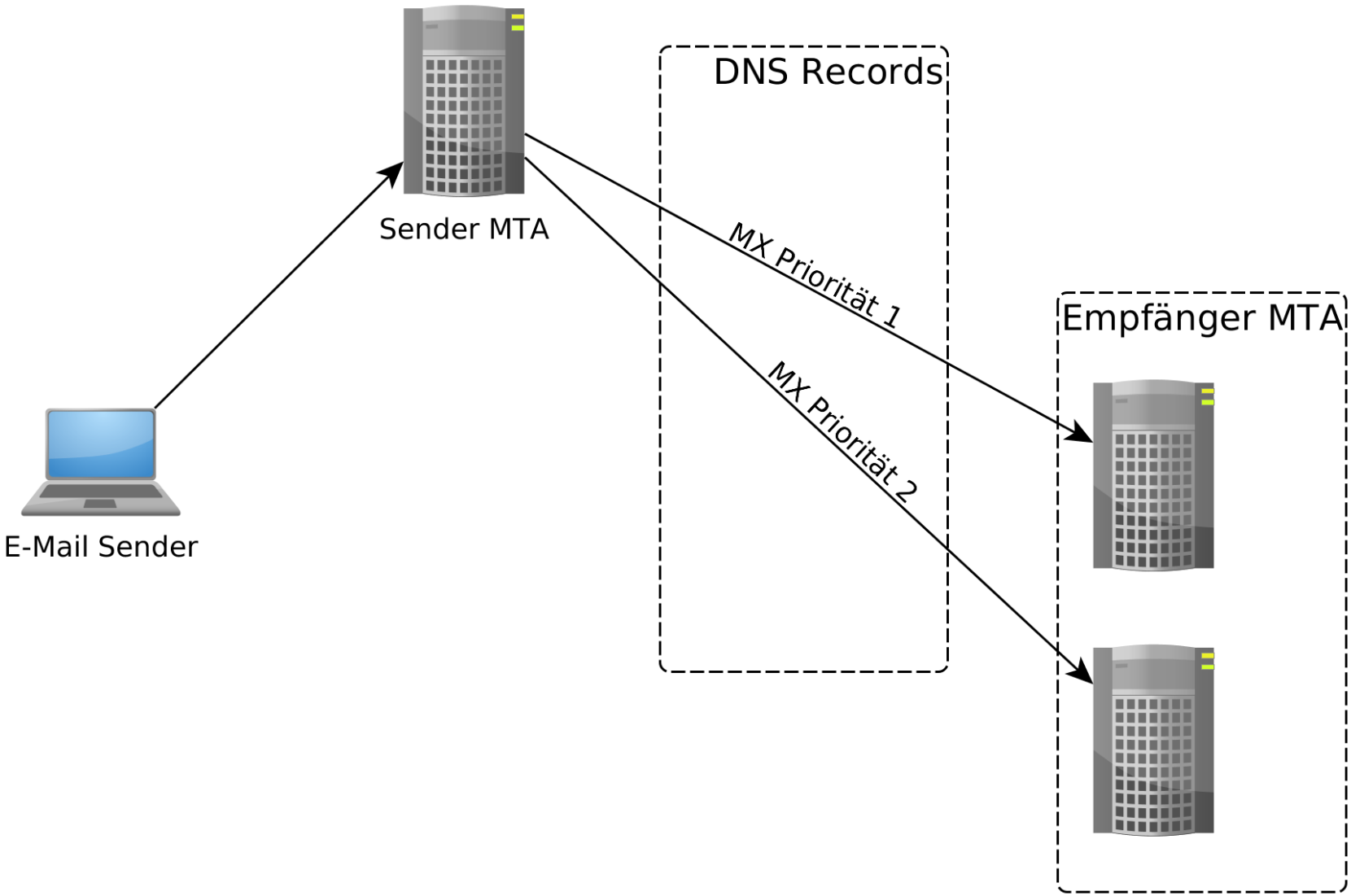


Abbildung: Typisches Szenario

DANE und SMTP

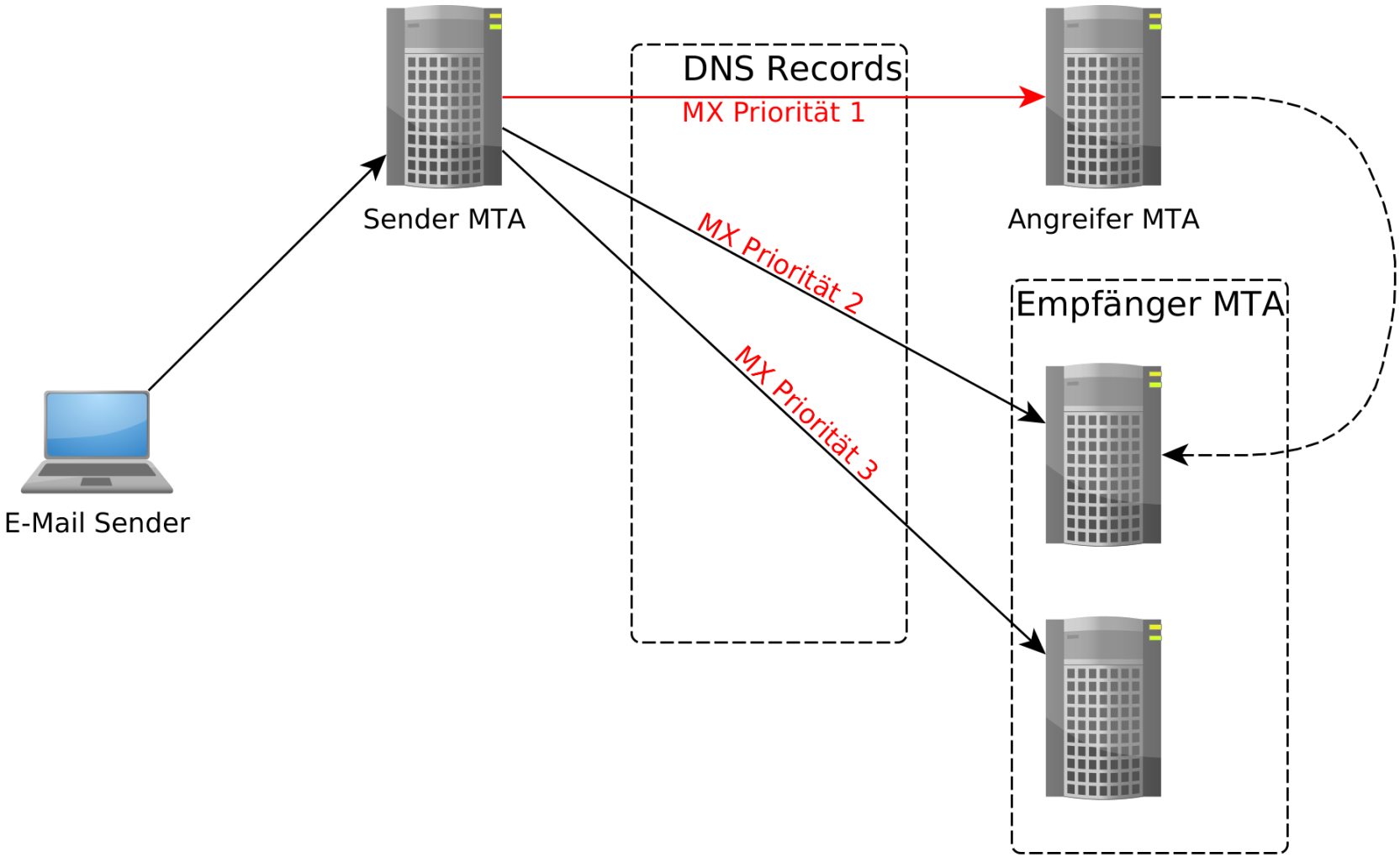


Abbildung: Falscher MX Record

DANE und SMTP

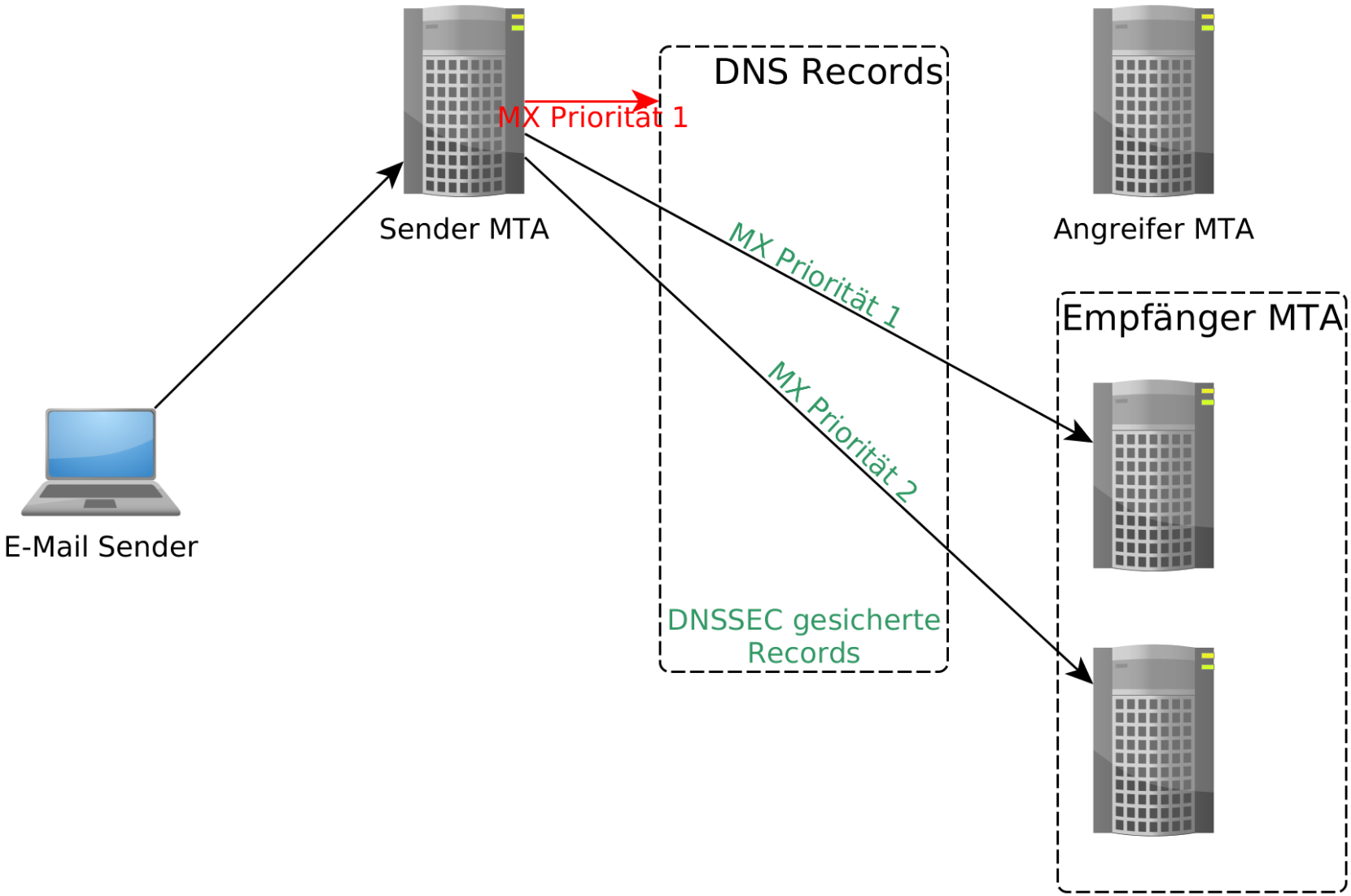


Abbildung: Lösung mit DNSSEC

DANE und SMTP

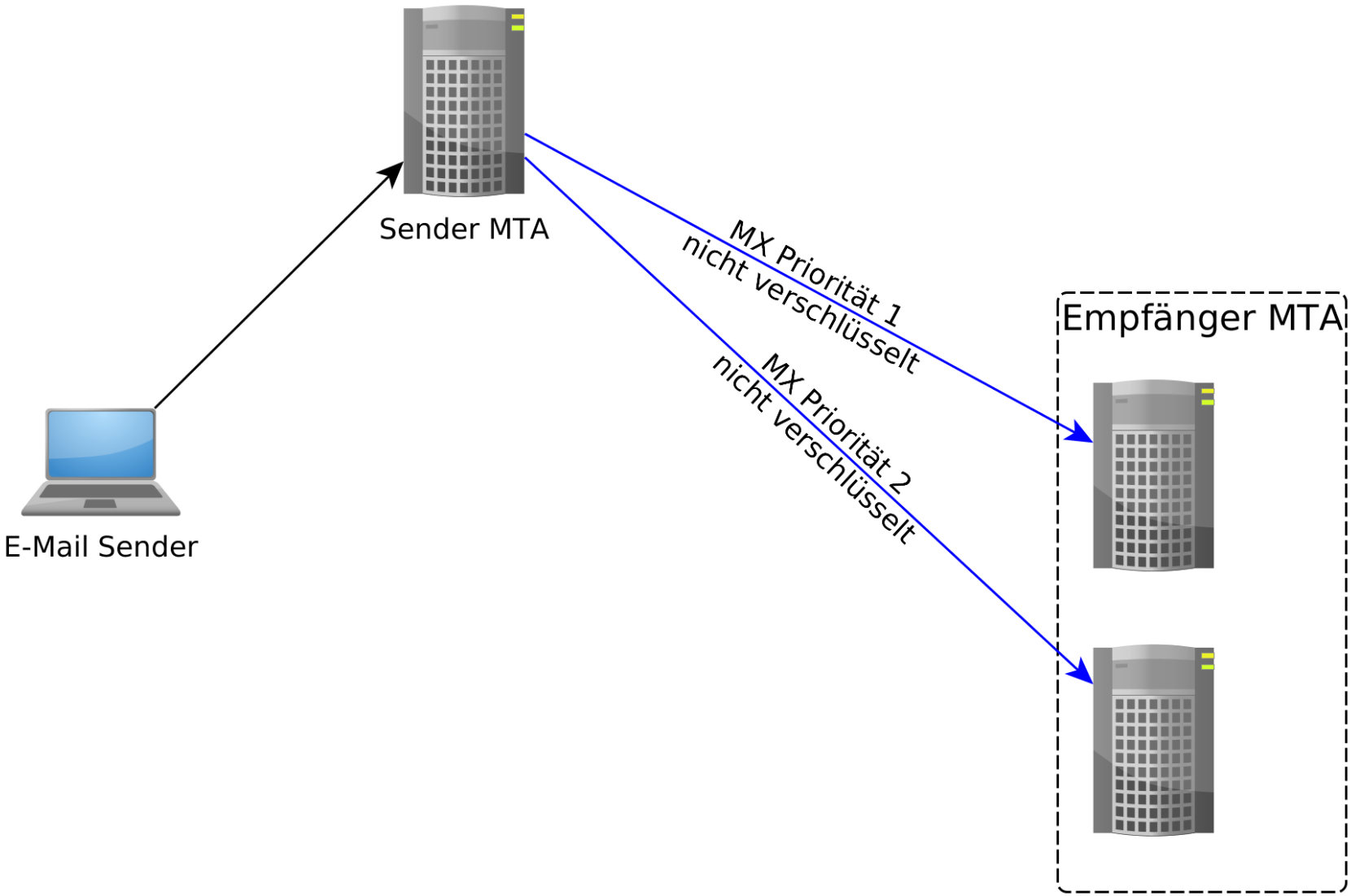


Abbildung: SMTP zwischen MTAs nicht veschlüsselt

DANE und SMTP

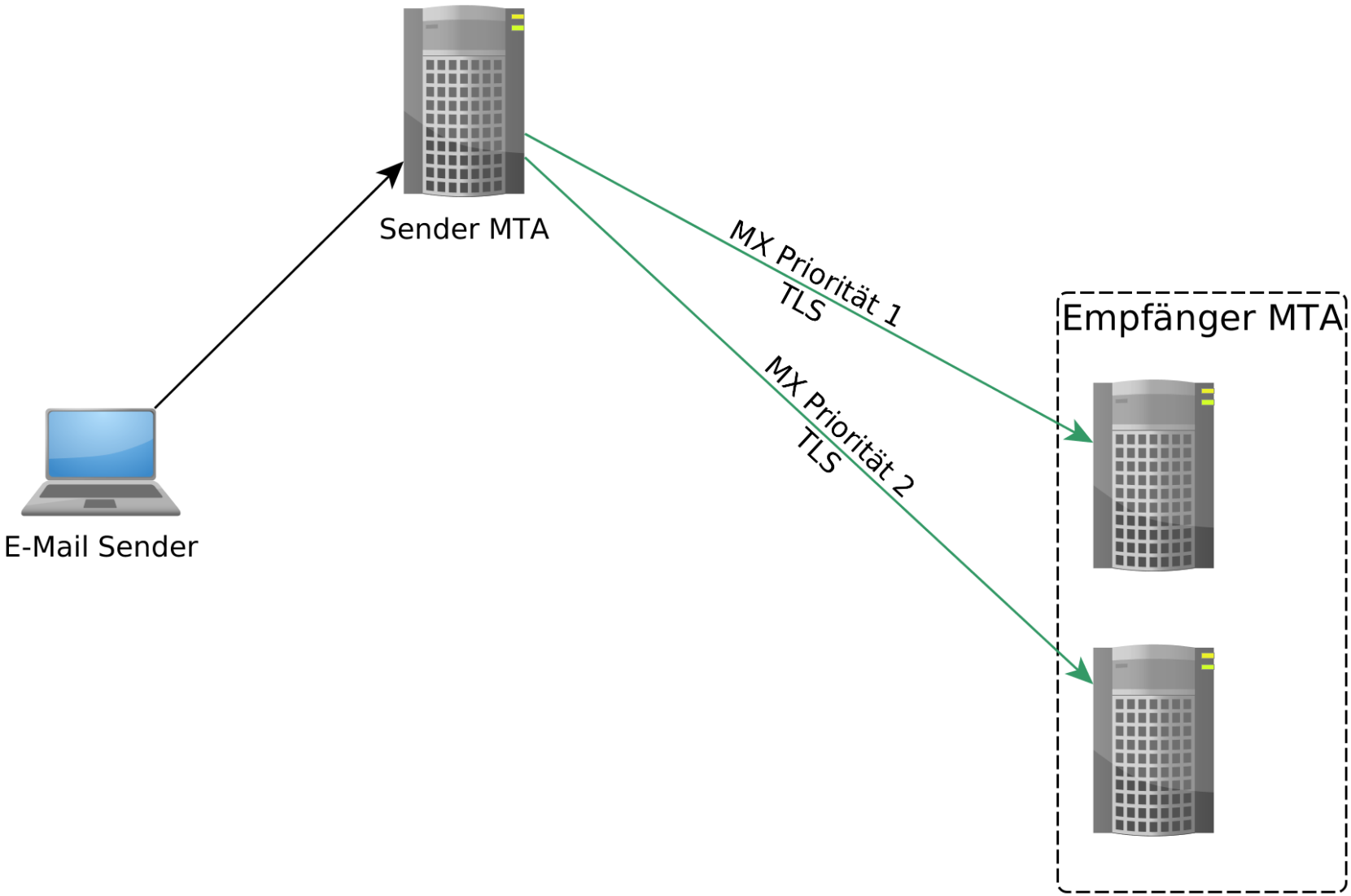


Abbildung: Lösung mit TLS

DANE und SMTP

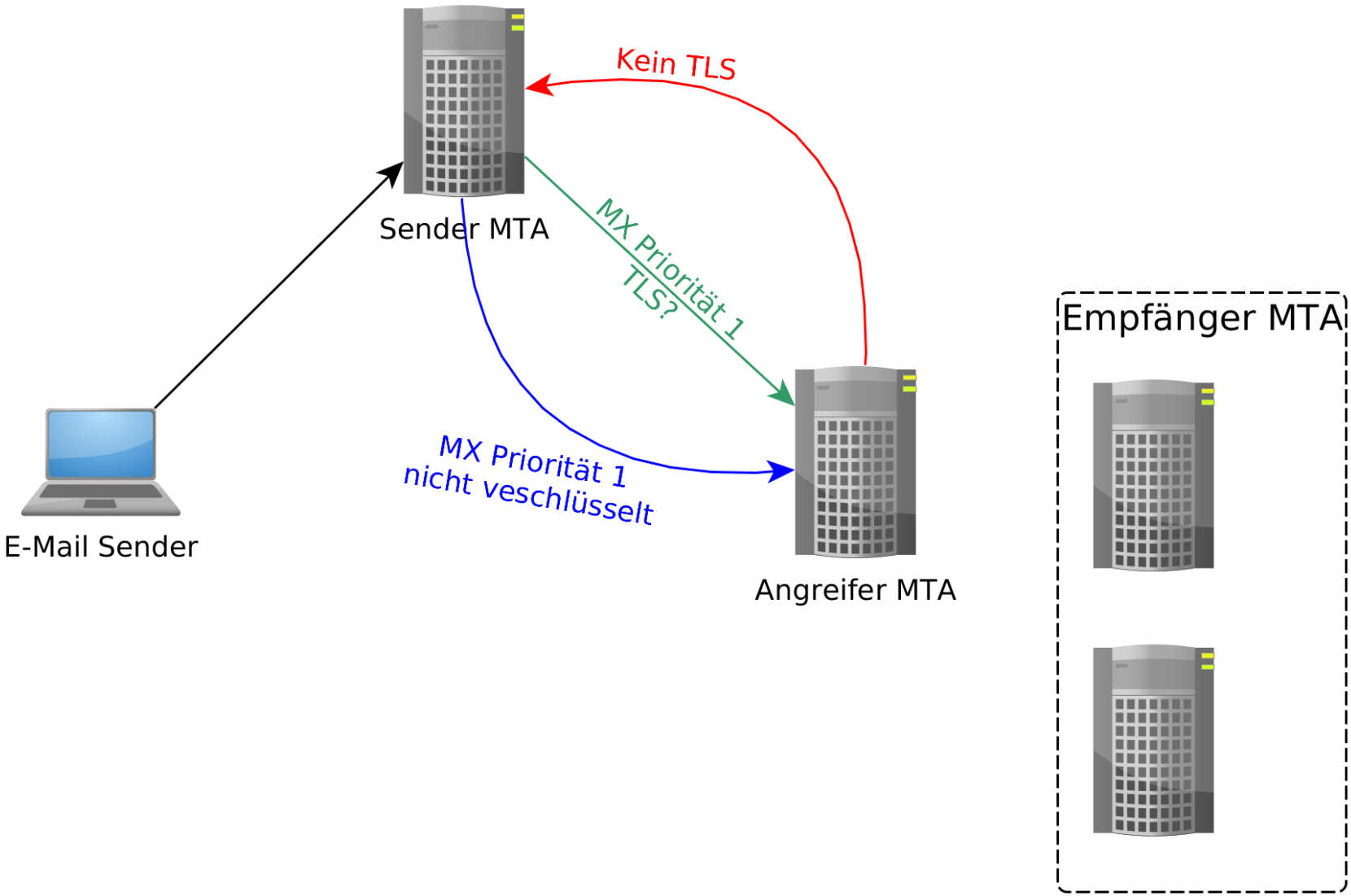


Abbildung: STARTTLS „downgrade“-Angriff

DANE und SMTP

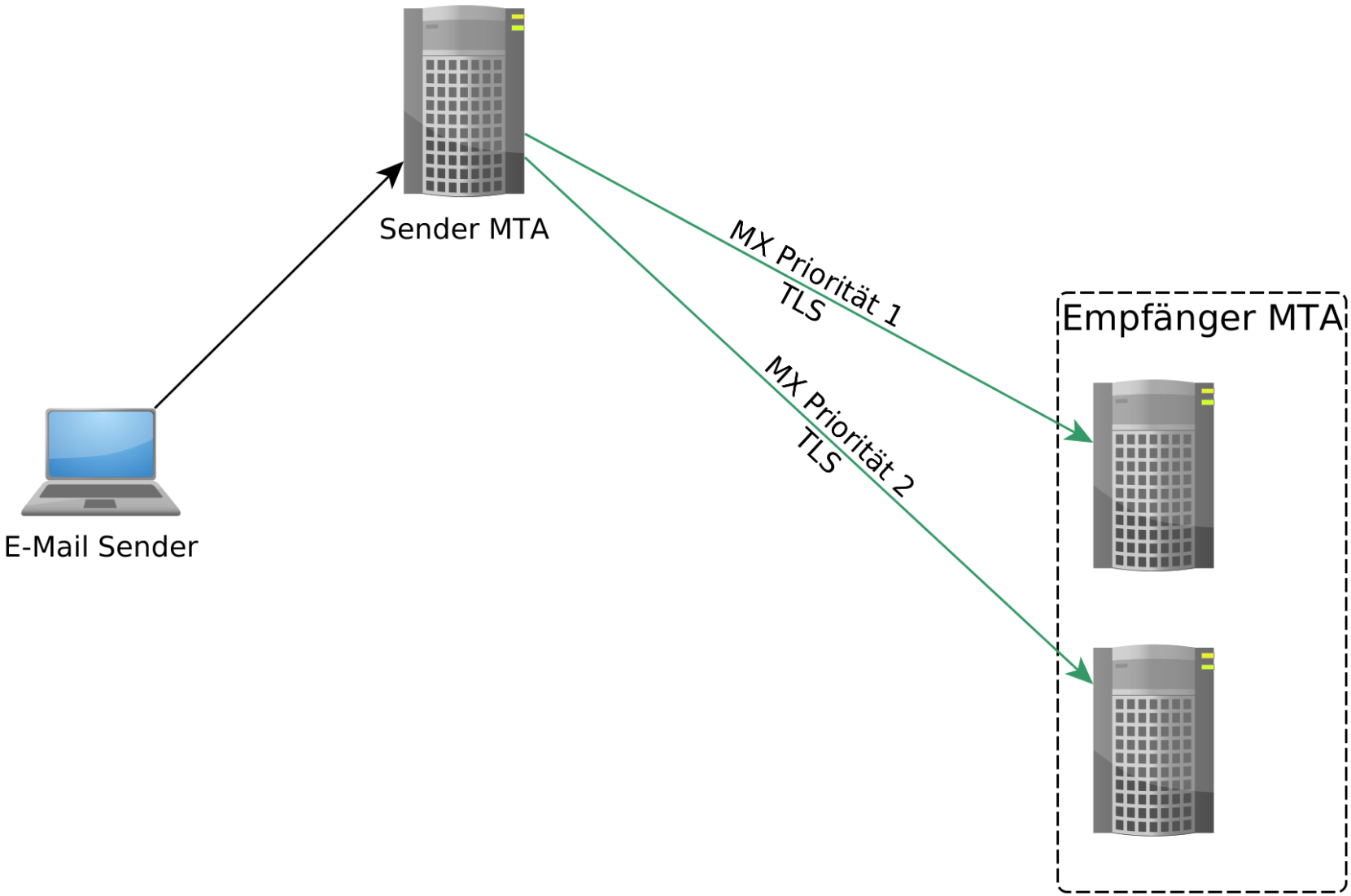


Abbildung: Lösung mit DANE

Vorteile von DANE

- MX-Abfragen werden sicherer (durch DNSSEC)
- TLS wird „downgrade“-fest
- Sicherung gegen falsche TLS/SSL-Zertifikate
- Zertifikat-Widerruf wird einfacher

Ausblick

- DNS
- DNSSEC
- DANE

Literatur


Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. (2005a).
DNS Security Introduction and Requirements.
RFC 4033.


Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. (2005b).
Protocol Modifications for the DNS Security Extensions.
RFC 4035.


Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. (2005c).
Resource Records for the DNS Security Extensions.
RFC 4034.


Davies, M., Walnut, M., and Jackman, B. (1993).
Proceedings of the Twenty-Sixth Internet Engineering Task Force.
Corporation for National Research Initiatives.


Friedl, S. (2008).
An Illustrated Guide to the Kaminsky DNS Vulnerability.
`http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html`.
Zulezt besucht am: 2014-11-11.


Hoffman, P. and Schlyter, J. (2012).
The DNS-Based Authentication of Named Entities (DANE). Transport Layer Security (TLS) Protocol: TLSA.
RFC 6698.


Mockapetris, P. (1987).
Domain names - concepts and facilities.
RFC 1034.