AGITOS WEBSOLUTIONS

DKIM: Technik und Anwendungsszenarien

Florian Sager
Agitos Websolutions

Werbung

Agitos, München (1998-)

- Softwareentwicklung für's Web,
  bezogen auf DKIM nachfolgend zu finden unter (agitos.de)
- Managed Hosting (Linux only)
- Consulting

eco-Arbeitskreis „E-Mail“ (2007-)

- Teilnehmer: eco-Mitglieder, große dt. Provider und RZ,
  Leitung: Florian Sager
- Ziel: Austausch auf techn. Ebene zur gemeinsamen
  Fortentwicklung in Sachen „E-Mail“ in Deutschland

AGITOS WEBSOLUTIONS

Erwartungen an die DKIM-Signatur?

AGITOS WEBSOLUTIONS

DKIM-Historie

2004:

- Yahoo! entwickelt Domain Keys (crypto-based), Licence-Grant-Pat.
- Cisco entwickelt Identified Mail (crypto-based)

2005:

- Neuorganisation: gemeinsame Entwicklung eines offenen Standards
- Zusammenführung zu **D**omain **K**eys **I**dentified **M**ail
- Unterstützt von u.a. Alt-N Technologies, AOL, Cisco, EarthLink, IBM, Microsoft, PGP Corporation, Sendmail, StrongMail Systems, VeriSign and Yahoo!

05/2007: RFC 4871, Basisdokument

2009: Errata Document, Update zur Klarstellung

AGITOS WEBSOLUTIONS

DKIM Charter: aktueller Stand

- RFCs
  - Analysis of Threats Motivating DomainKeys Identified Mail (DKIM) (RFC 4686)
  - **DomainKeys Identified Mail (DKIM) Signatures (RFC 4871)**
  - Requirements for a DomainKeys Identified Mail (DKIM) Signing Practices Protocol (RFC 5016)
- Drafts
  - **DKIM Author Domain Signing Practices (ADSP)**
  - DomainKeys Identified Mail (DKIM) Service Overview
  - DomainKeys Identified Mail (DKIM) Development, Deployment and Operations
  - RFC 4871 -- Update

AGITOS WEBSOLUTIONS

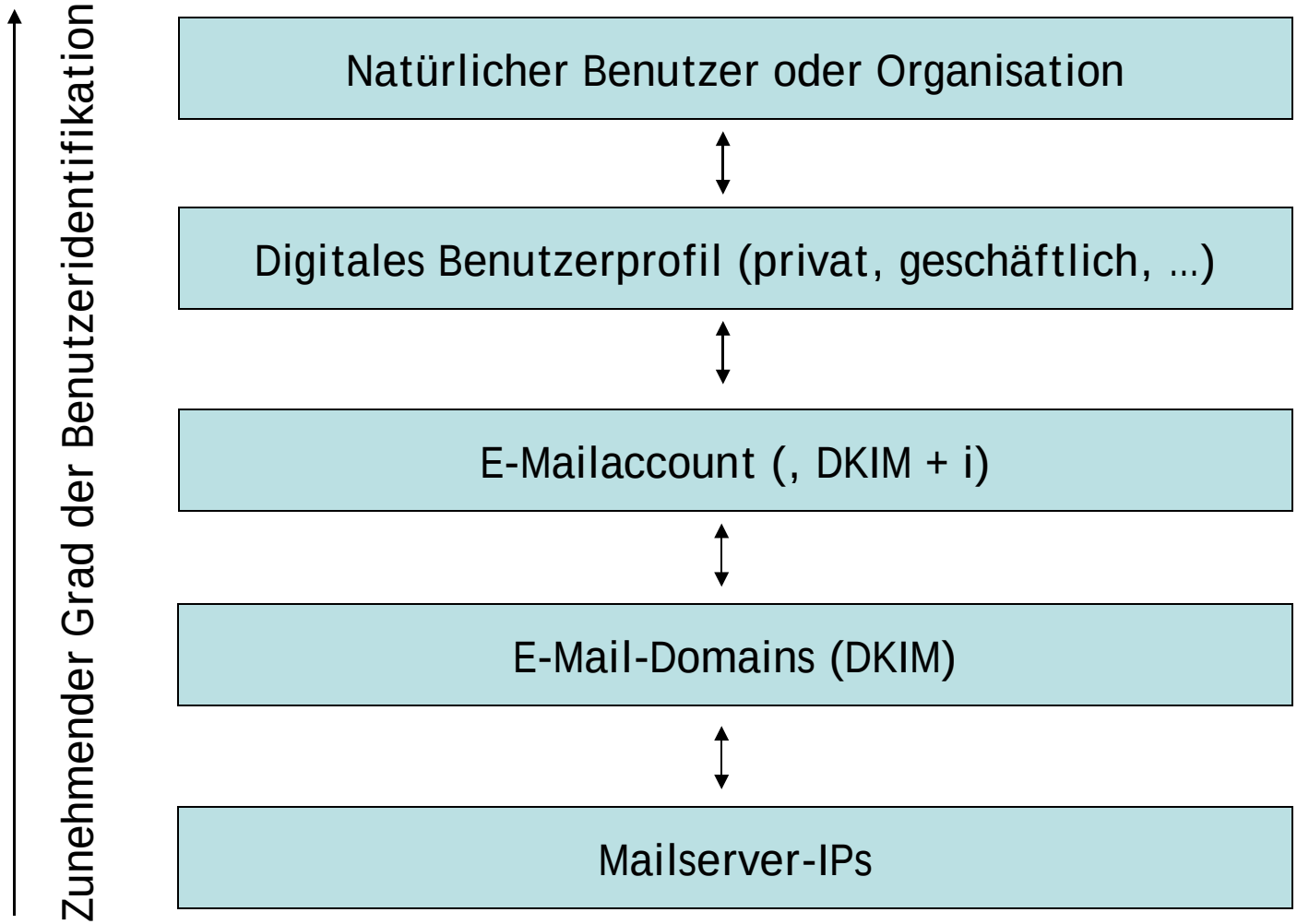
Oft gehörte Irrtümer …

DKIM-Signaturen sind vorteilhaft, denn sie sagen aus, dass **Sender „gut“ sind**.

DKIM-Signaturen sind unnütz, denn auch Spammails werden signiert.

Man bedenke:

DKIM bietet Sender-Identifikation auf technischer Ebene; Vorteile der DKIM-Signatur bestehen nicht durch die Signatur selbst, sondern können sich erst durch aufsetzende Anwendungen ergeben.


Zunehmender Grad der Benutzeridentifikation
Natürlicher Benutzer oder Organisation
Digitales Benutzerprofil (privat, geschäftlich, …)
E-Mailaccount (, DKIM + i)
E-Mail-Domains (DKIM)
Mailserver-IPs

AGITOS WEBSOLUTIONS

DKIM-Zweck (aus RFC 4871+Errata)

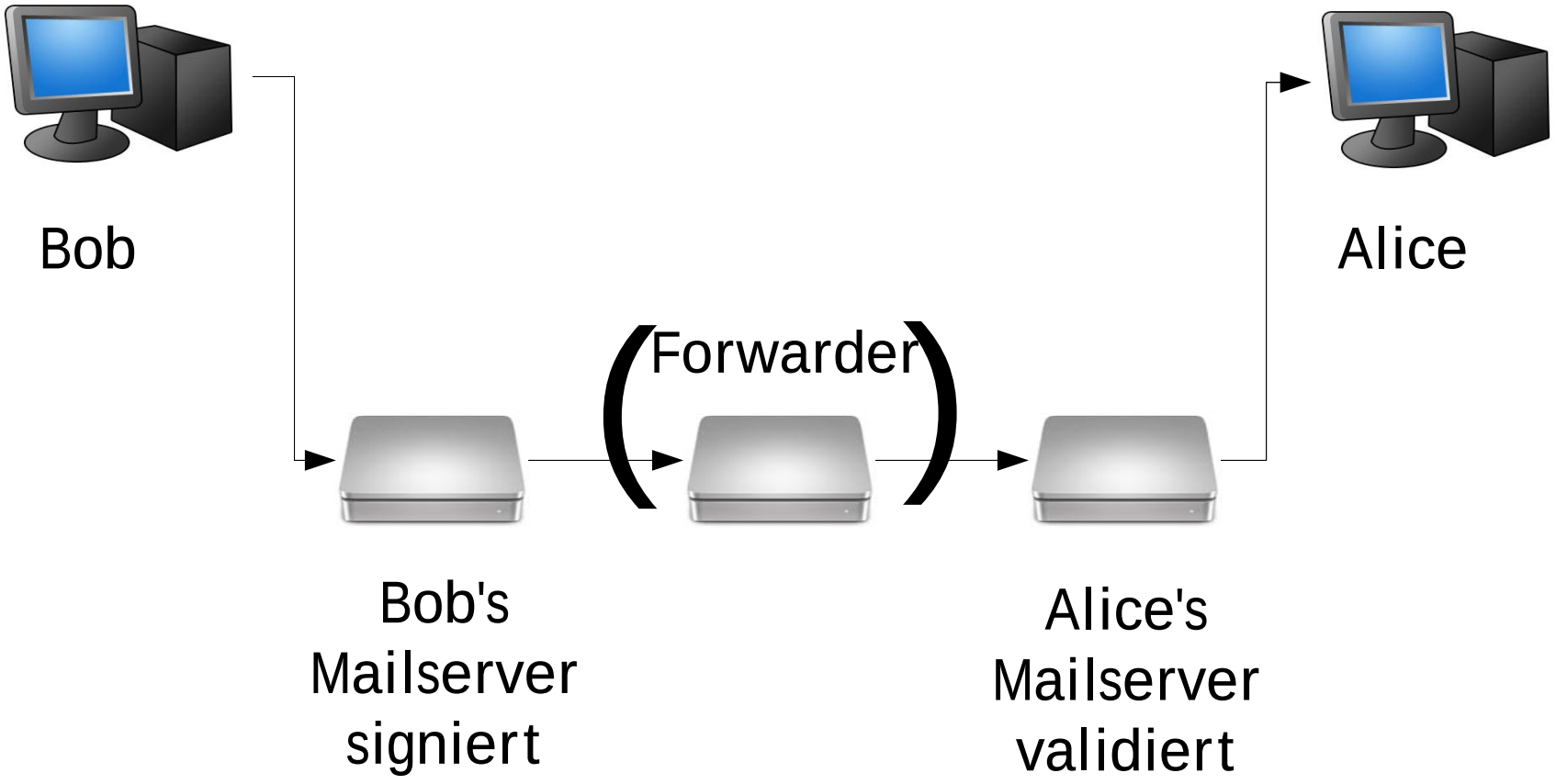
„The ultimate goal of this framework is to permit a person, role or organization that owns the signing domain to assert responsibility for a message, thus protecting message signer identity and the integrity of the messages they convey while retaining the functionality of Internet email as it is known today.“

AGITOS WEBSOLUTIONS

Wie wird eine DKIM-Signatur generiert?

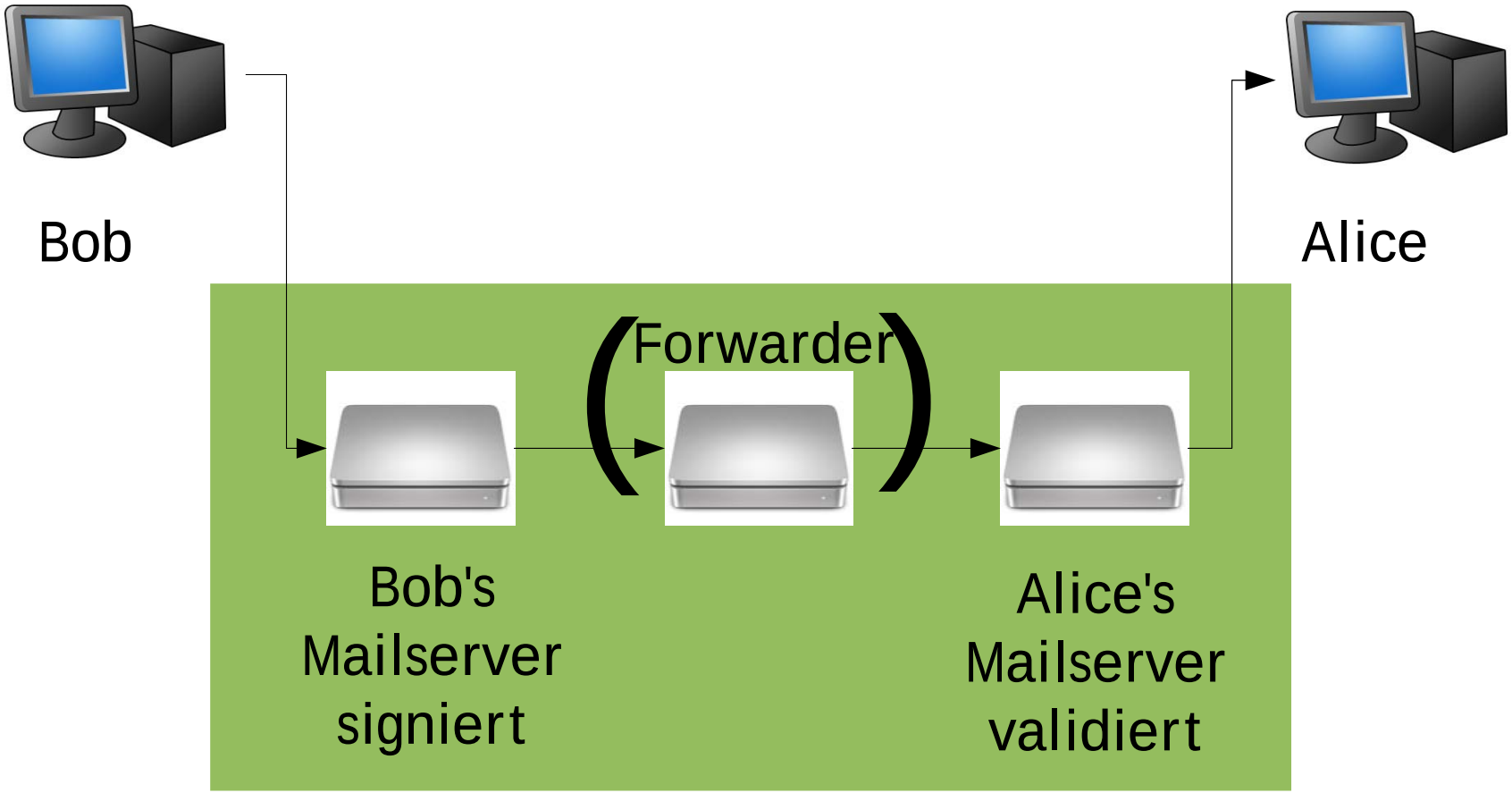
AGITOS WEBSOLUTIONS

DKIM: Klassisches Anwendungsszenario



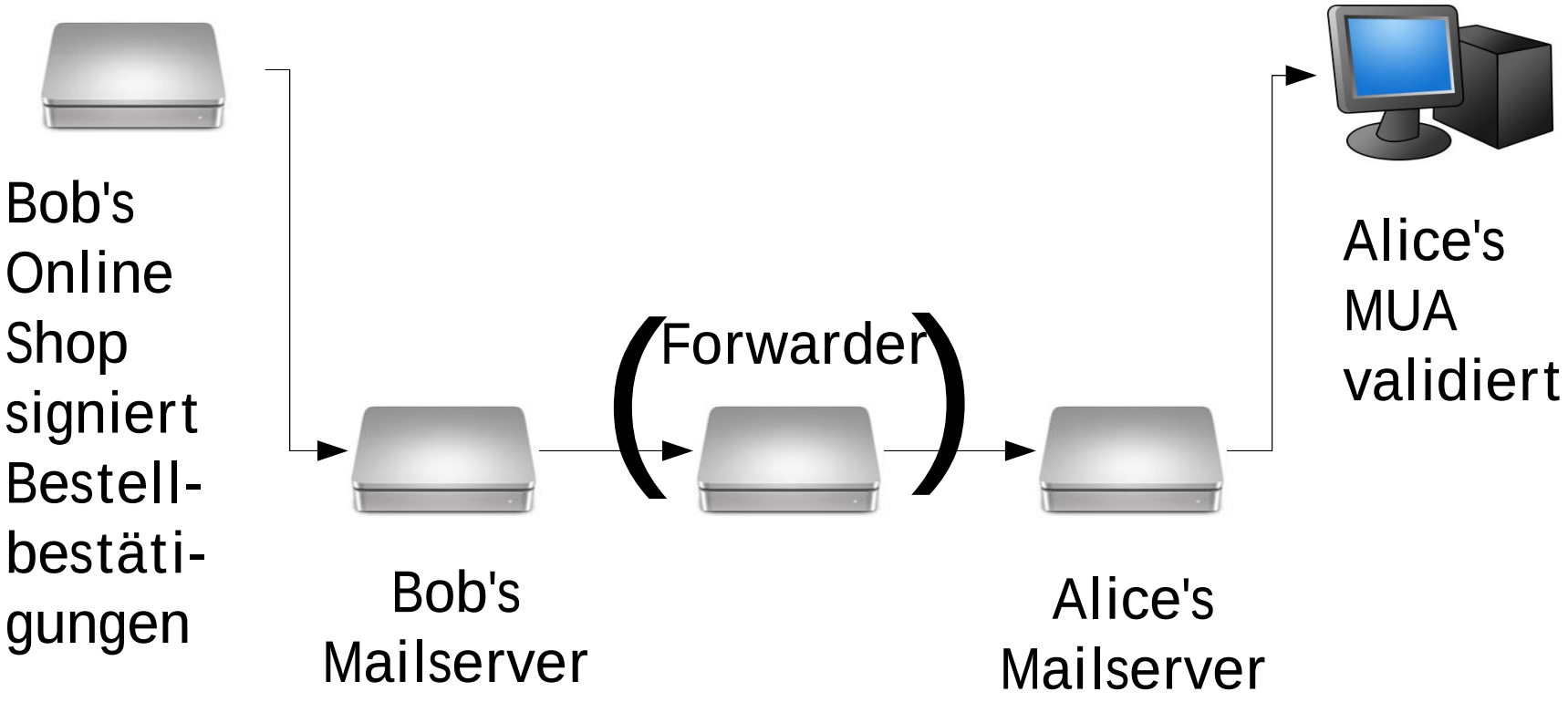
AGITOS WEBSOLUTIONS

DKIM: Klassisches Anwendungsszenario



AGITOS WEBSOLUTIONS

Denkbares Szenario mit Signatur und Validierung an Endpunkten



Signature-Example

```
DKIM-Signature: v=1; t=1191504983; d=agitos.de;
   s=testselector; i=webmaster@agitos.de; h=Message-
   ID:From:To:Subject:Date:MIME-Version:Content-Type:X-
   Priority:X-MSMail-Priority:X-Mailer:X-MimeOLE;
   c=relaxed/simple; a=rsa-sha256;
   bh=vCa+kQywfD0xOneQUkrXgJyJlZAupLeGiR+jTz7ZyFs=;
   b=Fs0YRhPFdSNI8EUT25CRd8rHXzI8Od57rL0W7rNJvvuKdSuEv77ChHCY
   YxCf79ZB7ZoaQ6x3ZyEdfqxyOSK3kihCZGTz22jFRRQc8r7lKtUXsHugz8
   ViTF3PLRz4Z0U6BKOV+SpF2bOlL9jvIALFOOoireTN5LulIO4pb91vO6Y=
```

bh = base64(sha256(canon(body))) // Body Hash

b = base64(rsa(sha256(
canon(h-konkateniert) + CRLF + DKIM-Signature mit b=,‘))))

Zugehöriger DNS Record

Public Key für einen 1024-bit Private Key: 1024 Bit werden empfohlen

```
testselector._domainkey.agitos.de IN TXT ("v=DKIM1;"
   "p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQ"
   "KBgQDwIRP/UC3SBsEmGqZ9ZJW3/DkMoGeLnQg1fWn7/zYt"
   "IxN2SnFCjxOCKG9v3b4jYfcTNh5ijSsq631uBItLa7od+v"
   "/RtdC2UzJ1lWT947qR+Rcac2gbto/NMqJ0fzfVjH4OuKhi"
   "tdY9tf6mcwGjaNBcWToIMmPSPDdQPNUYckcQ2QIDAQAB")
```

AGITOS WEBSOLUTIONS

Header in der DKIM Signatur

Die folgenden Header SOLLTEN in der Signatur enthalten sein, falls sie in der zu signierenden E-Mail vorhanden sind:

- From (erforderlich in allen Signaturen)
- Sender, Reply-To
- Subject
- Date, Message-ID
- To, Cc
- MIME-Version
- Content-Type, Content-Transfer-Encoding, Content-ID, Content-Description
- Resent-Date, Resent-From, Resent-Sender, Resent-To, Resent-Cc, Resent-Message-ID
- In-Reply-To, References
- List-Id, List-Help, List-Unsubscribe, List-Subscribe, List-Post
- List-Owner, List-Archive

Die folgenden Header SOLLTEN NICHT in der Signatur enthalten sein:

- Return-Path
- Comments, Keywords
- Bcc, Resent-Bcc
- DKIM-Signature
- Authentication-Results

AGITOS WEBSOLUTIONS

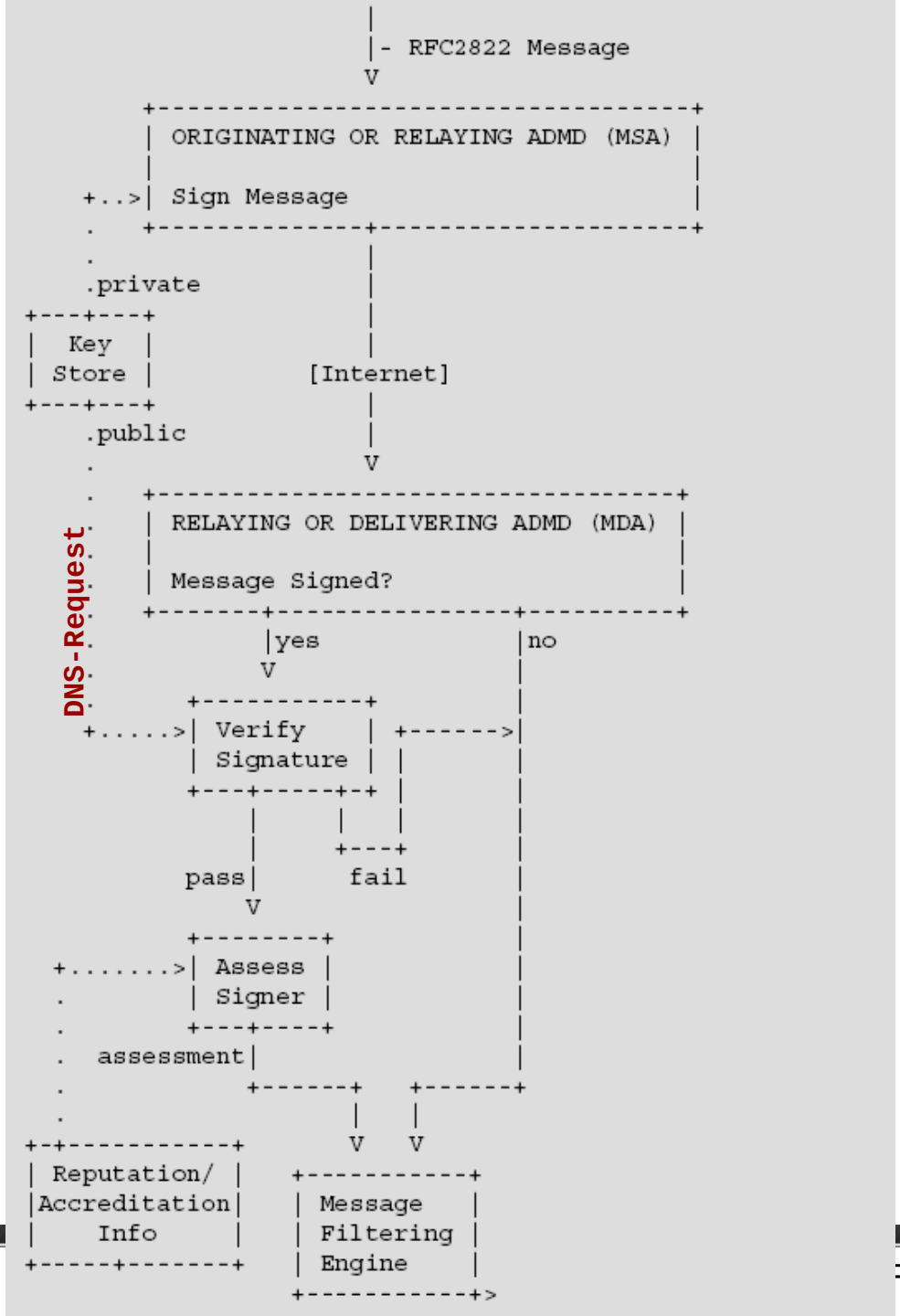
Spezielle, optionale Parameter der DKIM-Signatur:

- l-Parameter: Body Length Limit (Byte-Count) → Stabilität über Mailinglist-Server vs. Abuse

- z-Parameter: Kopierte Header, wie vorhanden zum Zeitpunkt der Einbringung der Signatur, mit Feldnamen und Feldinhalt

- x-Parameter: Signaturverfallszeit

Service Architecture (w/o Author Domain Signing Practices)



Allg. Authentication-Results Header (M. Kucherawy)

- http://tools.ietf.org/html/rfc5451
- Unterstützte Authentifizierungsmethoden:
  - auth
  - dkim
  - dkim-adsp
  - domainkeys
  - iprev
  - senderid
  - spf
- Beispiel:

```
Authentication-Results: <server-id>; dkim=pass
header.i=@enews.1up.com; dkim=pass header.i=FileFront@enews.1up.com
```

- WICHTIG: Authentication-Results Header in eingehenden Mails sollten entfernt werden, sofern nicht vertrauenswürdig

Author Domain Signing Practices

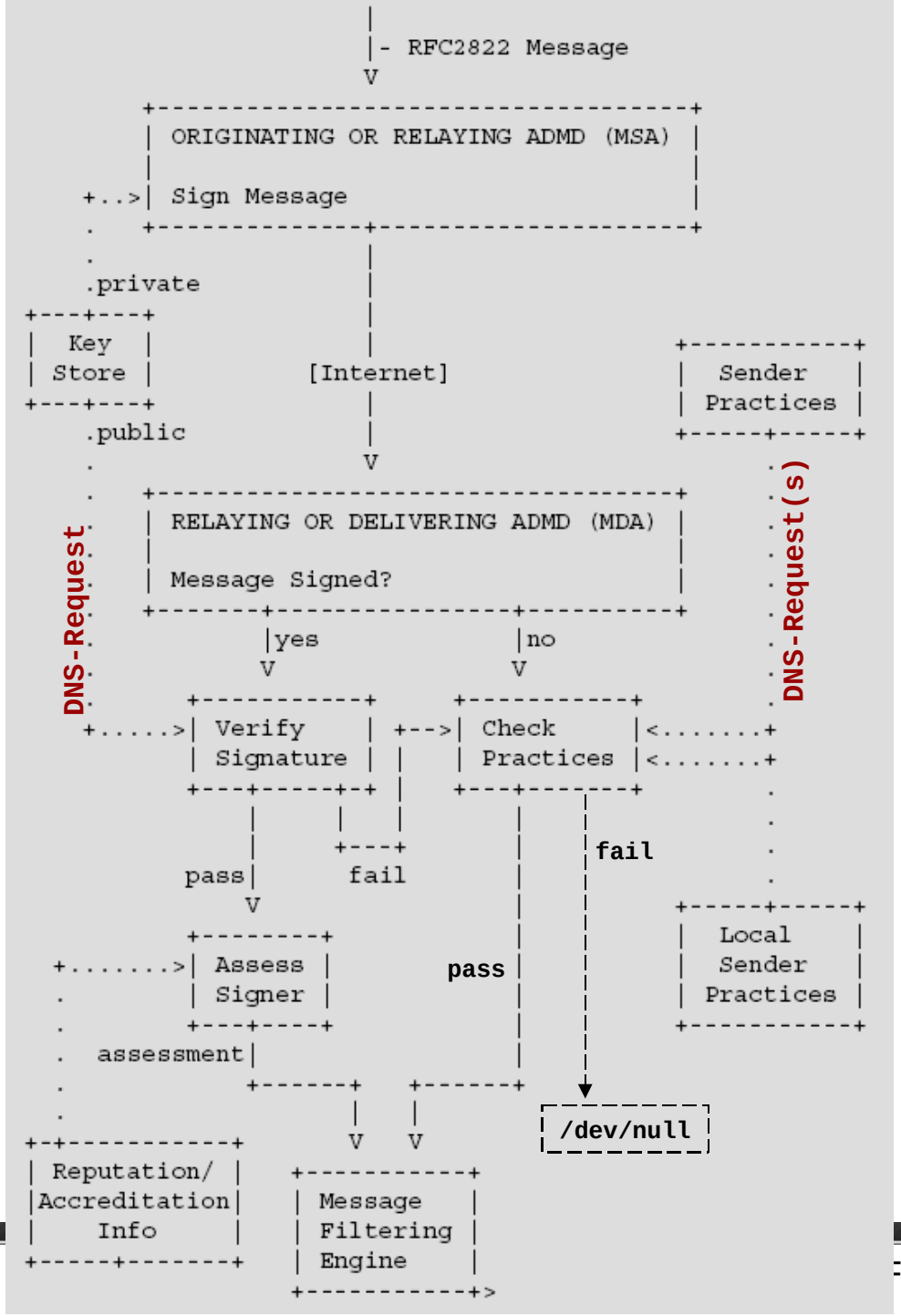
- Ziel: Hilfsmittel gegen Mailheader Spoofing über die Deklaration der „Verpflichtung“ zur Signatur (Originator Domain)
- Verifier können diese Policy über die Domain Zone abrufen, bspw. **`_adsp._domainkey IN TXT „dkim=all“`**
- Mit **`dkim=all`** muss eine gültige Signatur vorhanden sein

  Was passiert in Fehlerfällen wie a) DNS Timeout bei Public Key Requests b) Transit System invalidiert Signatur?

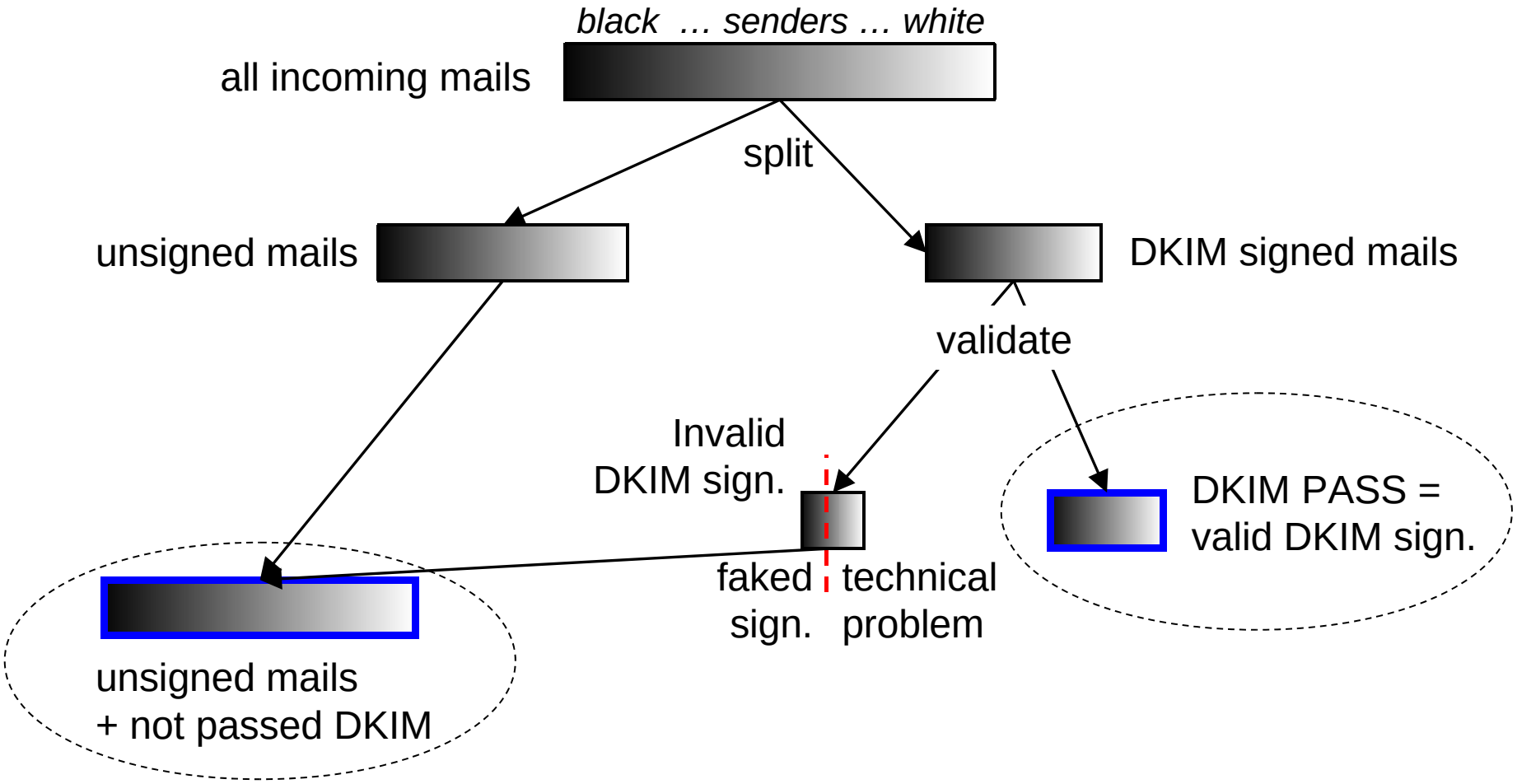
  → http://www.sendmail.org/dkim/wizard

AGITOS WEBSOLUTIONS

Service Architecture with ADSP



Email Partitionen unter Auth-Infos



AGITOS WEBSOLUTIONS

DKIM-Nutzung

- Agitos-Mailserver, Zeitraum Mitte April bis Mitte Juni:
  - E-Mails ohne DKIM-Signaturen: 93%
  - E-Mails mit validen DKIM-Signaturen: 6,5%
  - E-Mails mit invaliden DKIM-Signaturen: 0,5%
    → Fehlerrate bei 7,7 % (!) bei gewöhnlichem DKIM-Mailtraffic
    → Vgl. DKIM-Spam-Fehlerrate bei dkim-reputation.org: 23%
- Tendenz: anfänglich intensivere Nutzung durch Spammer
- inzwischen: weniger Spam seitens Google und Yahoo!
- DKIM-Domain-Checks in dkim-reputation.org auf knapp 9 Mio. Domains ergeben ~6% Domains mit _domainkey Records (Heuristik)

AGITOS WEBSOLUTIONS

Warum treten invalide DKIM-Signaturen auf?

- Public Keys können nicht angefordert werden
  - DNS Timeouts
  - DKIM Check nach Enfernung eines Public Keys aus der Domain Zone im DNS
- Transitsysteme schreiben Header/Body um
- Mißbrauch, kopierte Signaturen werden in Mails mit beliebig anderem Content verwendet

DKIM error rates

Figures from a mailinglist posting from Mark Martinec:

DKIM-Results except PASS: 11%

- failed mails that were NOT sent through mailinglist servers: 1,7%
- failed mails that were sent through mailinglist servers only: 71%

→ Who in the room wants to reject DKIM signed mails that don‘t validate?

BUT: the long-term-goal is email rejection based on signature validation failures → check your email infrastructure for DKIM non-destruction

AGITOS WEBSOLUTIONS

Vermeidung von Signatur-Invalidierung

- **Tipp:** Mailinglistserver sollten DKIM-Signaturen in eingehenden Mails löschen und eigene einbringen
- **Tipp:** Mails in 7-Bit-Encoding versenden
- **Tipp:** Canonicalization relaxed --> weitergehende Canonicalization in v=2 nötig?
- **Tipp:** Signaturen sollten möglichst weit „außen“ geprüft werden: Authentication-Results-Header intern verwenden + Key-Expiry vermeiden
- **(Tipp:** length-Parameter aufnehmen zur Reduktion des Mailinglistproblems)

AGITOS WEBSOLUTIONS

DKIM und Performance

- Problematik Rechenzeit für DKIM: eher in Empfangssystemen (da 7% des Traffics), weniger in Versandsystemen (hier dauert der Versand schlichtweg minimal länger)
- DKIM bietet eine Möglichkeit mehr für DDOS Attacken
- Public Key Lookup-Performance „Problem“ → keine async-Verarbeitung bspw. in SA möglich
- Daumenregel: bei 100% DKIM-Traffic ist für die Validierung Rechenleistung nötig, die etwas unter derjenigen für Virenscanning liegt.

AGITOS WEBSOLUTIONS

DKIM für Mail-Filtering?

- Rejects und DKIM in der SMTP-Kommunikation: DATA muss abgewartet werden, danach erfolgt der DKIM-Check (DNS-Lookup ist auf aufwändigsten, dann noch Einholung von Bewertungen) --> derzeitige Implementierungen setzen nach Entgegennahme der Mail an (soweit mir bekannt)

- DKIM-Checks sind also nachrangig nach groben IP-Checks, sie stellen eine verfeinerte Filterung dar

DKIM Deployment

Deployment-Planung I

- Regelmäßige Key-Rotationen?
  - Generierung eines neuen Schlüsselpaars
  - Veröffentlichung des Public-Keys im DNS unter einem unbenutzten Selector
  - Kopieren des Private-Keys in DKIM-Signer-Installationen
  - Konfiguration der DKIM-Signer auf neuen Private-Key/Selector
  - Nach Wartezeit: Entfernung des alten Public-Keys aus dem DNS

    → Automatismus ist ratenswert, evtl. Rotations-Policy nötig
- Verwendung mehrerer Signaturdomains/Selektoren?
  - Abwägung Verwaltungsaufwand vs. Security
  - Selektoren pro Monat? Pro Abteilung? Pro E-Mail Kampagne?

Deployment-Planung II

- Verwendung von signierenden SMTP-Relays für jeglichen Outbound-Mail-Traffic?
  - Konzentration des Traffics auf weniger Smarthosts als derzeit?
  - Wie mit Roaming-Usern verfahren?

  → Kann die Signaturdomain den Mailtraffic verantworten? Auswirkungen auf Domain-Reputation bedenken.

Deployment-Planung III

- Schlüssel-Delegation: bei Versand von Mails durch eine 3rd-Party mit Signatur der 1st-Party:
  - eigenes Schlüsselpaar generieren, Public-Key in der Signaturdomain veröffentlichen und Private-Key an 3rd-Party geben
  - Public-Key von 3rd-Party generieren lassen und im DNS eintragen
  - DNS-Delegation vornehmen:

    abc._domainkey IN CNAME def._domainkey.third-party.tld.

    … also NICHT eigenes Schlüsselpaar an Dritte weitergeben ;)

Generierung eines Schlüsselpaars

- Private Key, etwa mit OpenSSL:

  `openssl genrsa -out priv.key <bitsize>`

  Generierung eines RSA Private Keys, bitsize ist per Default 512, für DKIM empfehlen sich 1024 Bit (→ Performancefrage)

- Public Key:

  `openssl rsa -in priv.key –pubout -out pub.pem -outform PEM`

  Generierung eines Public Keys aus dem Private Key im PEM-Format (=Base64 encoded)

Veröffentlichung des Public-Key im DNS

- **Ergebnis, Beispiel:**

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6PUokFAZ/oJplFyPgFoSdVUhP
sLIETGH8hyTk/AecqwTUSLewcpDmBG/xmOjJSjnvaukX527MEa75wsJrzge3Qlpp
4JKwbjtQTfcH3WG5ExdkhFuMlEbM2KtgwAHpbK8VpbQPGwRoW1gm8AqsQBJKTlFG
qta5p1xa3iEzdLkH4wIDAQAB
-----END PUBLIC KEY-----
```

- **Eintragung in der Zone der Signaturdomain:**

```
someselector._domainkey IN TXT ("v=DKIM1; g=*; k=rsa;"
    "p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6PUokFAZ/oJplFyPgFoSdVUhP"
    "sLIETGH8hyTk/AecqwTUSLewcpDmBG/xmOjJSjnvaukX527MEa75wsJrzge3Qlpp"
    "4JKwbjtQTfcH3WG5ExdkhFuMlEbM2KtgwAHpbK8VpbQPGwRoW1gm8AqsQBJKTlFG"
    "qta5p1xa3iEzdLkH4wIDAQAB")
```

- **Reload DNS**

Attribute in DKIM TXT Record (auszugsweise)

Attribute stellen Forderungen an Signaturen dar:

- Version: `v=DKIM1`
- Key für Verschlüsselungsverfahren: `k=rsa`
- Beschränkung auf Localparts? `g=*` (alle), `g=a*` (Einschr.)
- Unterstützte Hash-Algorithmen für Signatur: `h=sha256`
- …
- TTL für Record: eher gering (2 Stunden?), falls Keys kurzfristig rotiert werden müssen

DKIM Implementierungen

AGITOS WEBSOLUTIONS

Implementierungen: http://www.dkim.org/deploy/

- Spez. Hinweis auf Open Source Daemons:
  - DKIMproxy: http://dkimproxy.sourceforge.net/
  - dkim-milter: http://sourceforge.net/projects/dkim-milter/
  - Spamassassin: DKIM.pm Modul, Verifikation, konfigurierbare Auswirkung auf Scores
  - Amavis: Signatur und Validierung → nächster Vortrag
- Libraries:
  - Libdkim (C++): http://libdkim.sourceforge.net/
  - Mail-DKIM Perl module: http://dkimproxy.sourceforge.net
  - pydkim (Python): http://hewgill.com/pydkim/
  - PHP (alpha release): http://php-dkim.sourceforge.net/
  - DKIM for JavaMail: http://dkim-javamail.sourceforge.net (agitos.de)

Beispiel: dkim-milter (Signing)

- Package Installation
- Listening/Relay-Socket für milter festlegen
- Private-Keys sicher speichern, chown <milteruser>, chmod 400
- Config-File schreiben inkl. Zuordnung von Signaturdomains zu Keys (nächste Folie)
- Milter start
- MTA auf milter-Sockets anpassen, reload
- Ggf. Testversand an Reflector:

  http://testing.dkim.org/reflector.html

AGITOS WEBSOLUTIONS

dkim-filter.conf für Signatur

```
Mode                s
Canonicalization    relaxed/relaxed
SignatureAlgorithm  rsa-sha256
Socket              inet:10035@127.0.0.1
Domain              /etc/dkim-filter/domains.file
KeyList             /etc/dkim-filter/keylist.file
SenderHeaders       X-Sender, Resent-Sender, Resent-From, Sender, From
OmitHeaders         Content-Transfer-Encoding
AlwaysSignHeaders   Subject
AutoRestart         True
Background          True
Diagnostics         Yes
InternalHosts       /etc/dkim-filter/internal-hosts.file
Syslog              yes
LogWhy              true
```

AGITOS WEBSOLUTIONS

DKIMproxy, Config für Validierung

```
# specify what address/port DKIMproxy should listen on
listen    127.0.0.1:10045

# specify what address/port DKIMproxy forwards mail to
relay     127.0.0.1:10046
```

Beispiel-Ergebnis der Validierung:

Authentication-Results: <servid>; domainkeys=pass header.from=service@1800petmeds.com;
dkim=pass header.i=@1800petmeds.com

Deployment Tools


Photocase: Bratscher

Key-Generierung und DNS-Record Formatierung

- Aus Sendmail's Open Source milter Packet:

  `dkim-genkey` : generiert ein Schlüsselpaar und gibt DNS TXT Record aus

  http://sourceforge.net/projects/dkim-milter/

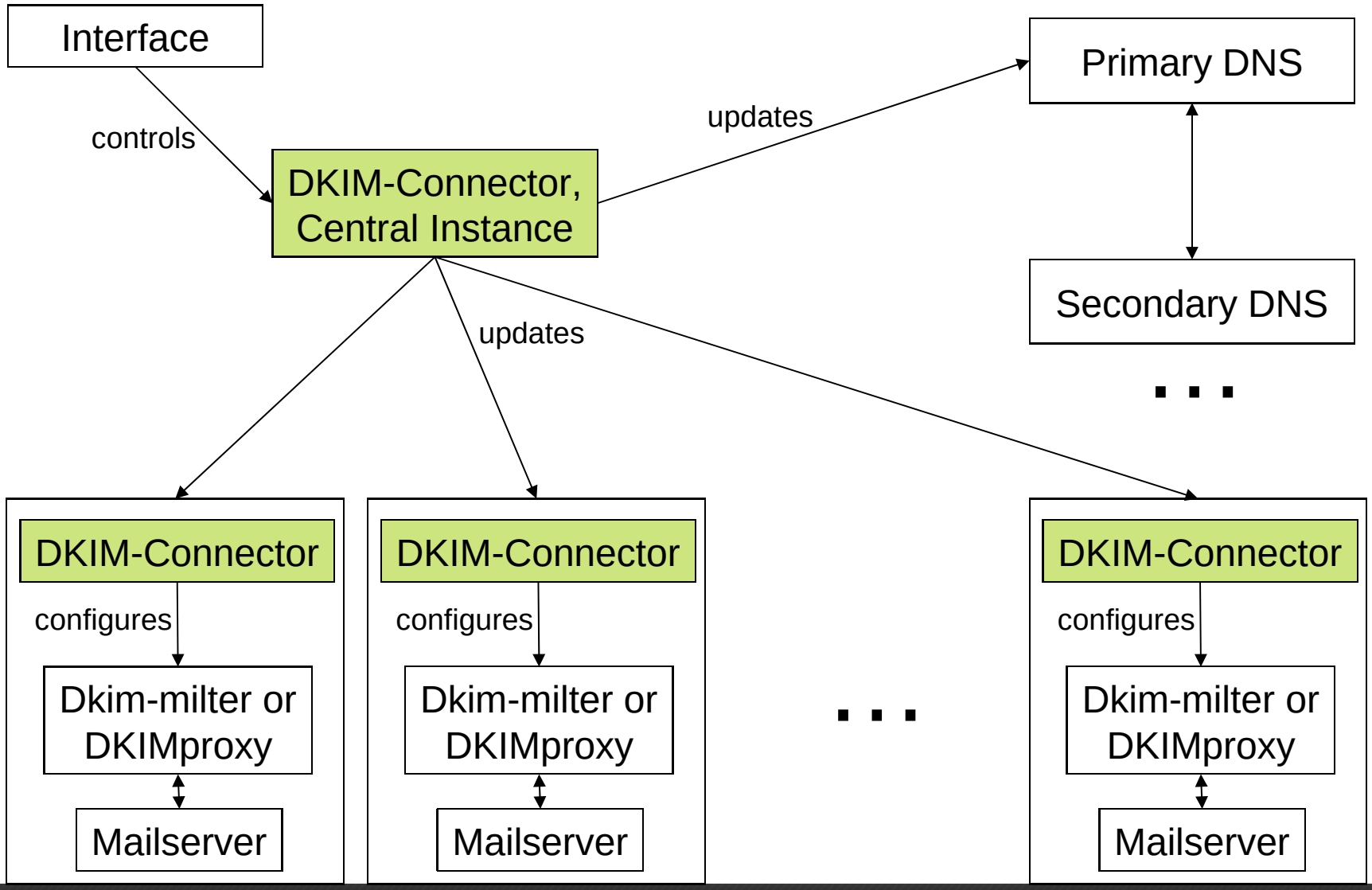
- Empfehlung: **DKIM DNS Wizard**
  http://www.dnswatch.info/dkim/create-dns-record

AGITOS WEBSOLUTIONS

DKIM Connector (agitos.de)

DKIM Connector Open Source Project

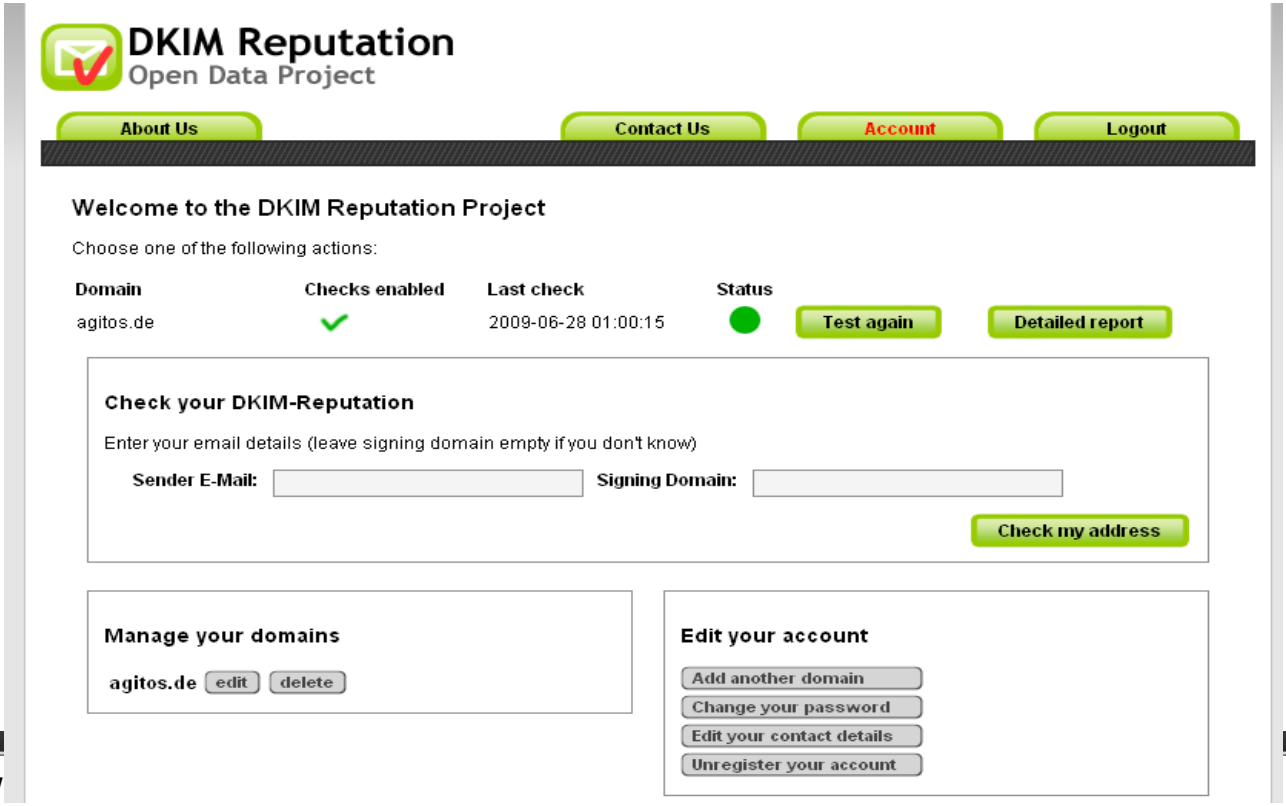
- Vereinfacht die Konfiguration verteilter DKIM-Signer:
  - Administriert eine oder mehrere DKIM-milter or DKIMproxy Instanzen
  - Updates für Primary DNS (nsupdate, optional TSIG)
  - Geplant: transaktionssicherer Reload aller Instanzen nach einem Update
- Insbesondere empfehlenswert bei Multi-Domain-Hosting und 1st-Party-Signaturen
- Perl Implementierung
- Status: Redevelopment im Mai 2009 abgeschlossen, jetzt v0.9
- Rückmeldung seitens der Community dürfte noch umfangreicher sein
- http://dkim-connector.agitos.de


Interface
controls
DKIM-Connector, Central Instance
updates
Primary DNS
Secondary DNS
updates
DKIM-Connector
configures
Dkim-milter or DKIMproxy
Mailserver
DKIM-Connector
configures
Dkim-milter or DKIMproxy
Mailserver
DKIM-Connector
configures
Dkim-milter or DKIMproxy
Mailserver

AGITOS WEBSOLUTIONS

DKIM-Monitoring: Funktionieren Ihre Signaturen?

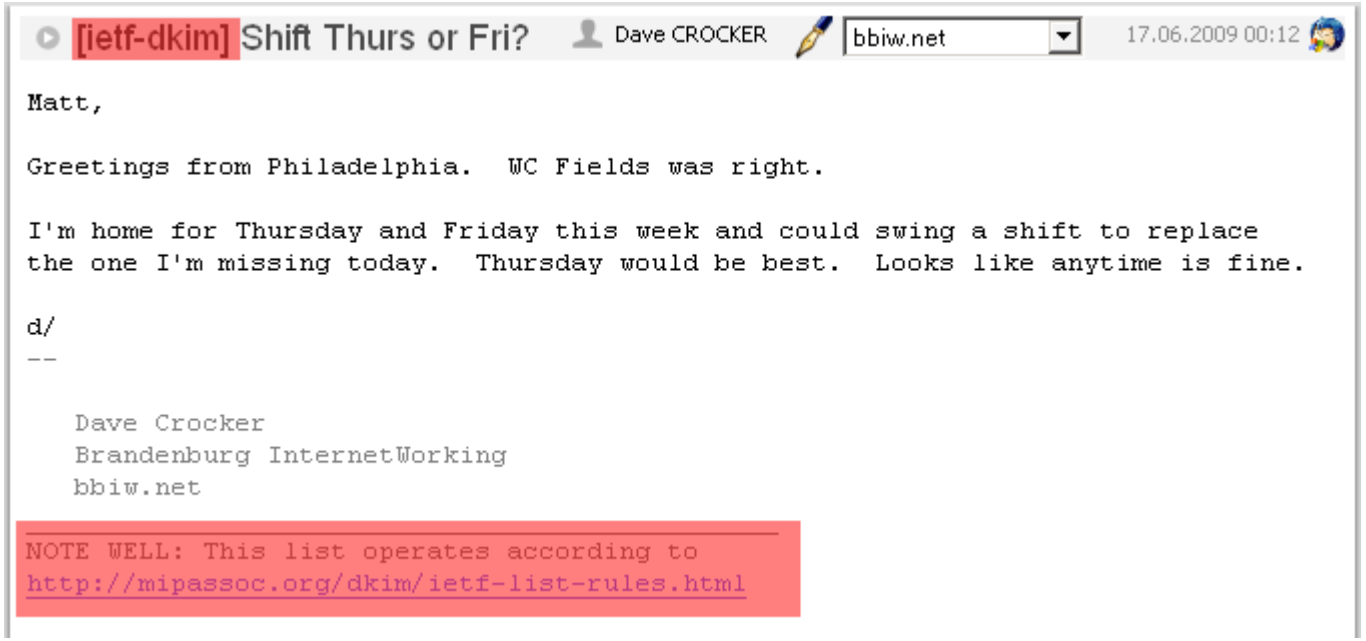
- http://www.dkim-reputation.org → Login/Register (frei)
- Anmeldung für regelmäßige, automatische DKIM-Checks auf eigenen Accounts (agitos.de)



AGITOS WEBSOLUTIONS

DKIM: Anwendungs-szenarien

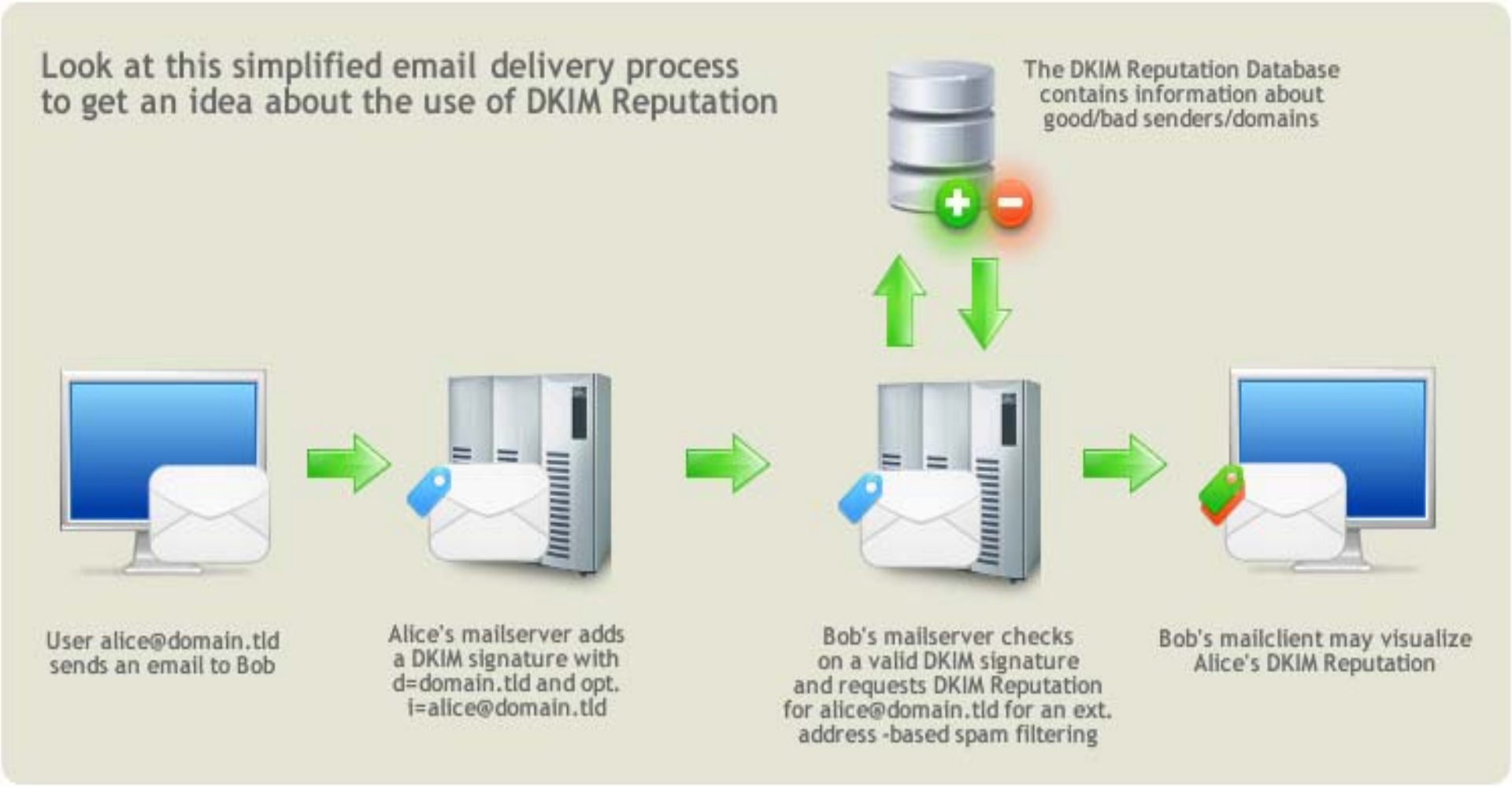
(1) „DKIM-Visualisierung“ im MUA



Denkbar über Authentication-Results Header oder Validierung im Client

- Aber: von Anwendern gewünscht?
- Für Anwender verwendbare Information?
- Nur verwendbar in Verbindung mit Reputationsinformation?
- Zukünftig denkbar: default server-id über die Zone des Mailserver-MX veröffentlichen

(2) dkim-reputation.org (agitos.de) Reduktion von False-Positives



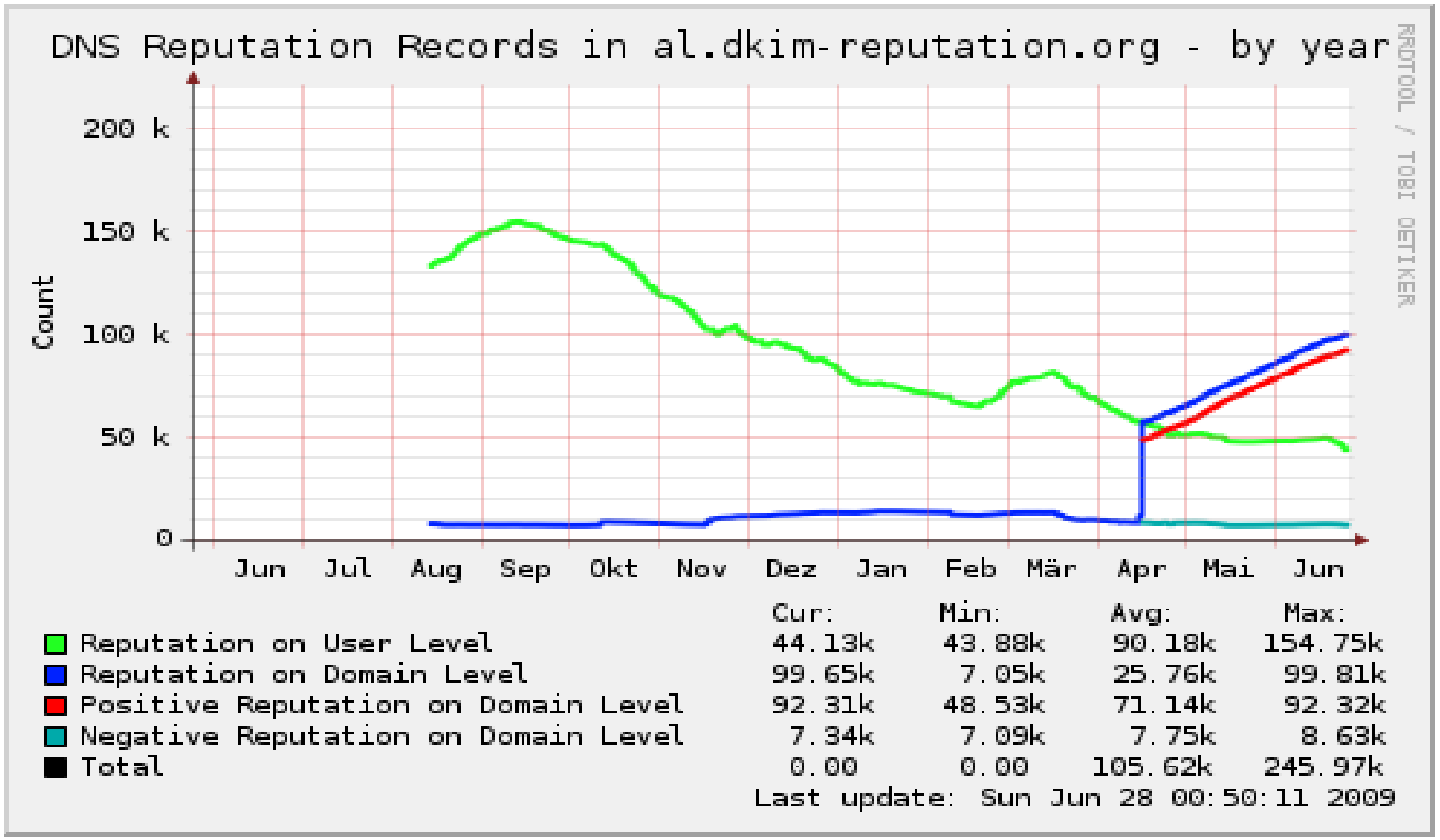
AGITOS WEBSOLUTIONS

DKIM Reputation Open Data Project

dkim-reputation.org: Eckdaten

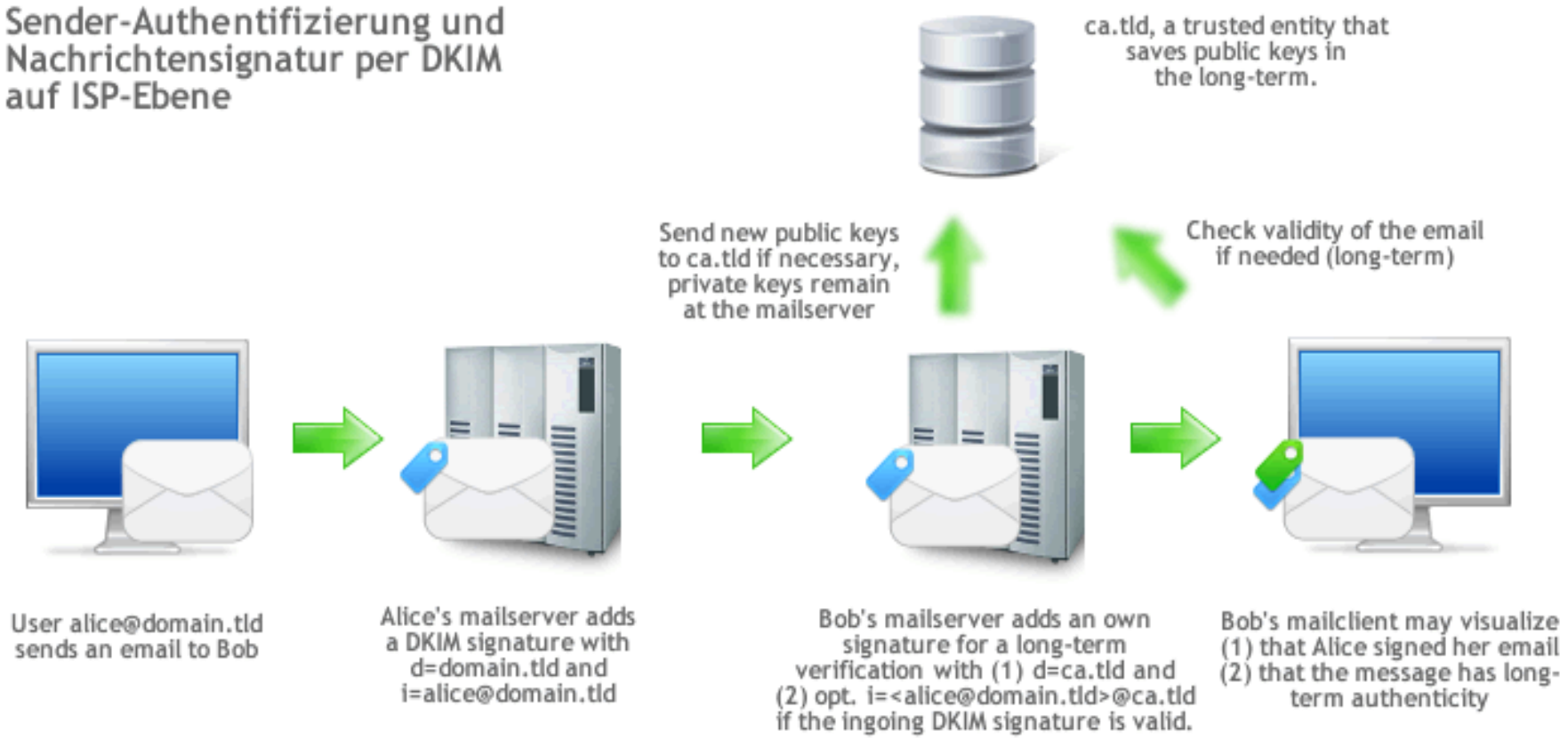
- Begonnen im Frühjahr 2008
- Erhält Spam aus dem nixSpam-Projekt, verarbeitet lediglich Spam mit validen Signaturen
- Sammelt Positiv-Domains seit Frühjahr 2009
- Dient zur Reduktion von False-Positives, ggf. Zukunftsthema
- Positive Reputation kann bspw. über Web-of-Trust gebildet werden
- (Feedbackloops + DKIM-Services)
- Spamassassin-Plugin verfügbar
- dkim-milter enthält Test-Implementierung zur Nutzung

Reputationsdaten auf User-/Domainlevel

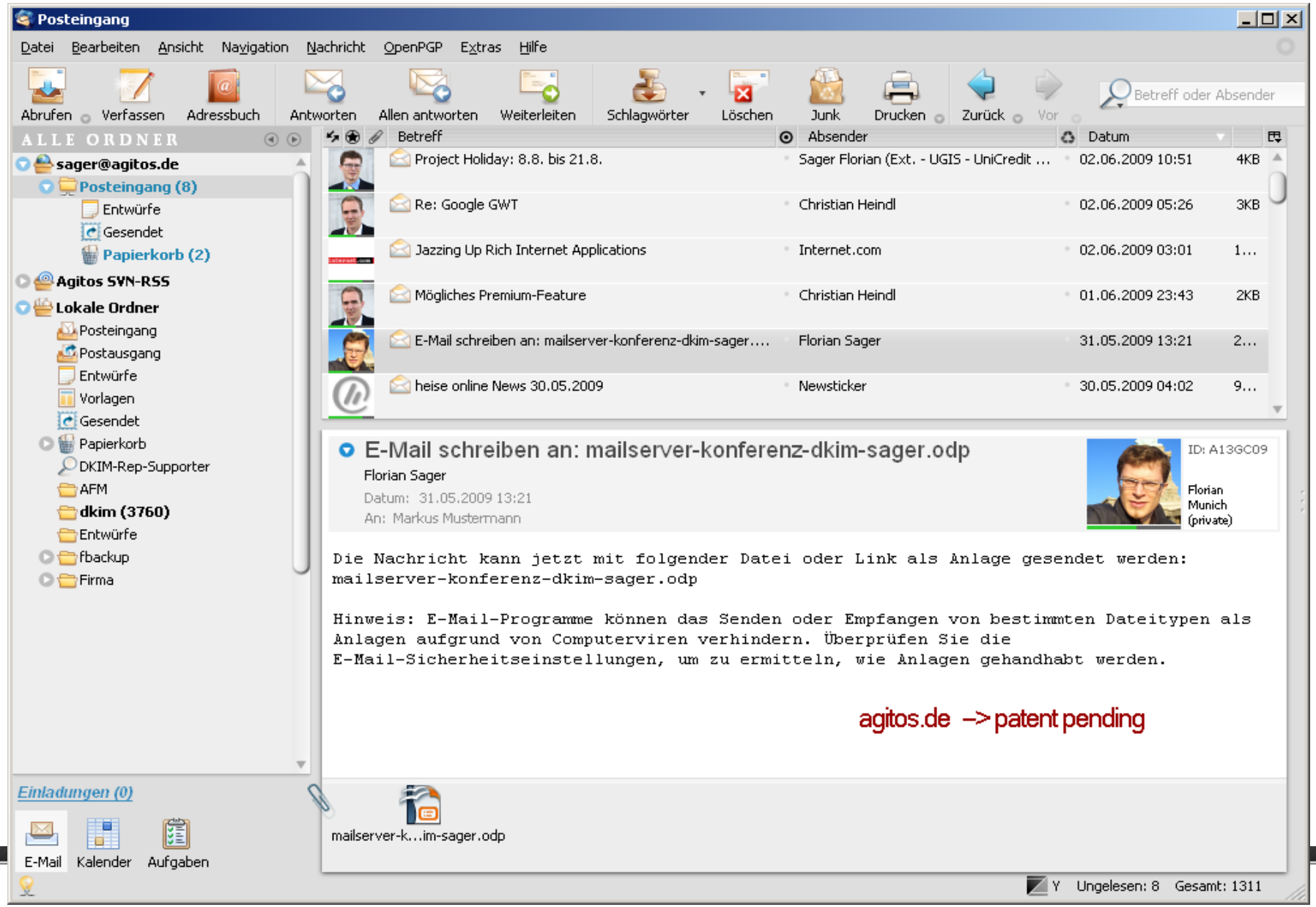


AGITOS WEBSOLUTIONS

(3) Gesteigerte Beweiskraft durch E-Mail-Signatur? (agitos.de)



(4) User-Profile in Mailclients (agitos.de)



AGITOS WEBSOLUTIONS

Vertrauenswürdige Sender sollten ihre Mails mit DKIM signieren.

www.dkim-reputation.org

DKIM wird eingesetzt von:

alice-dsl.de amazon.de bankofamerica.com bluewin.ch charite.de commerzbank.com dell.com doubleclick.com ebay.com facebook.com fh-trier.de flickr.com fotolia.com geocities.com gmail.com googlemail.com gwdg.de harrisbank.com hff-potsdam.de ip-exchange.de jpmorgan.com last.fm linkedin.com loewe.de malteser.at meinvz.net messe-muenchen.de orkut.de payback.de php.net postbank.de rtl2.de schuelervz.net skype.com sovereignbank.com spb.de spreadshirt.net tommyhilfiger.de tu-hamburg.de tu-harburg.de twitter.com uni-bremen.de uni-hohenheim.de uni-tuebingen.de usbank.com verbrauchernews.de vodafone.de vu-wien.ac.at westfaelischer-anzeiger.de wu-wien.ac.at yahoo.com youtube.com ...