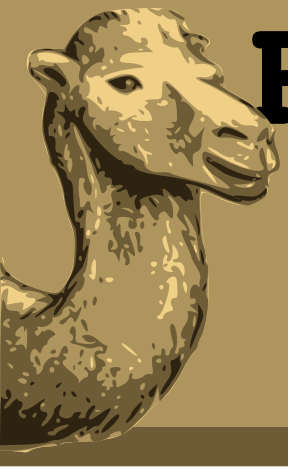
Perl Mongers im Ruhrgebiet



Ruhr.pm

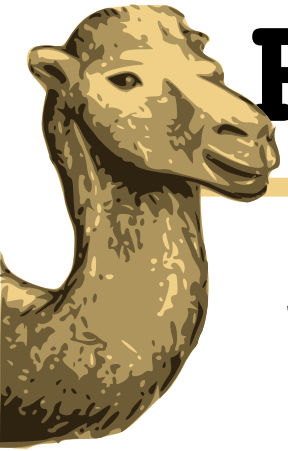
Spam-Filterung auf SMTP-Protokollebene mit Hermes Antispam Proxy

Autor: Veit Wahlich

EMail: veit AT ruhr.pm.org

Datum: 16. November 2007

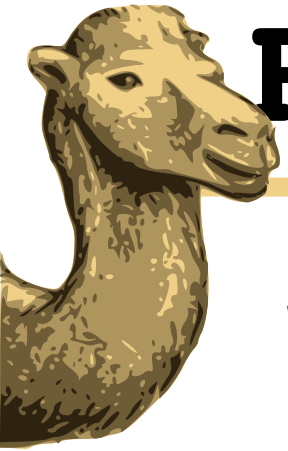
http://ruhr.pm.org/



Ruhr.pm

Was ist Hermes?

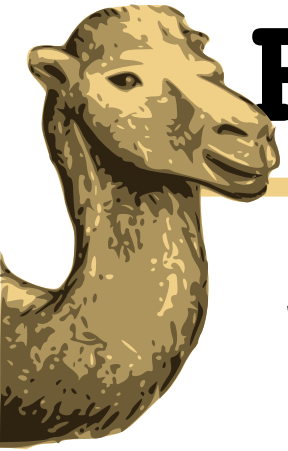
- transparenter SMTP-Proxy
  - wird vor dem “echten” SMTP-Server/MTA platziert
  - Durchleitung in Echtzeit, beobachtet Kommunikation
  - minimale Auswirkungen auf die Kommunikation
    - generiert nur Verweigerungen und deaktiviert Pipelining
    - erkennt und verarbeitet TLS-Verschlüsselung
    - deaktiviert sich bei erfolgreicher SMTP-Authentisierung
    - fügt Verarbeitungsinformationen in EMail-Header ein



Ruhr.pm

Was ist Hermes?

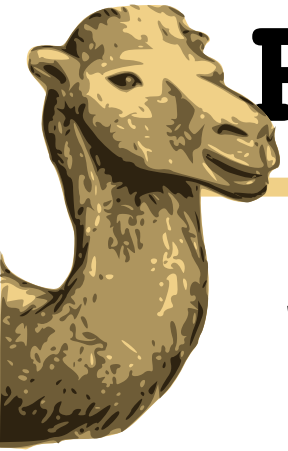
- implementiert viele Anti-Spam-Techniken
  - passive Techniken (Protocol Enforcement)
    - aktives Banner Delay
    - Throttling
    - Greylisting
    - Rejection Penalty



Ruhr.pm

Was ist Hermes?

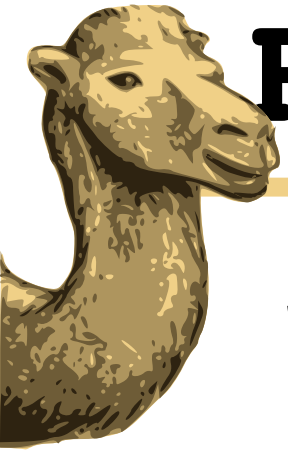
- implementiert viele Anti-Spam-Techniken
  - aktive Techniken
    - DNS-based Blackhole Lists und White Lists
    - Sender Policy Framework
    - Reverse Hostname Check



Ruhr.pm

Was ist Hermes?

- sehr effizient
  - geringe Ressourcennutzung
    - niedriger Speicher- und Rechenzeitverbrauch
  - entlastet eventuell nachgeschaltete Filter deutlich
    - z.B. SpamAssassin, DSPAM, Virenscanner, ...
- sehr effektiv
  - in der Praxis >98% Minderung des Spamaufkommens allein durch Hermes



Ruhr.pm

Was ist Hermes?

- mehr Fakten zu Hermes:
  - implementiert in C++, SQLite 3 als Backend-DBMS
  - entwickelt von ITEISA, S.C. (El Astillero, Spanien)
  - junges, aktives Projekt; seit April 2007 unter GPL
  - Pakete für viele Plattformen direkt von den Entwicklern
    - generische i386-RPMs für Linux
    - SRPMs für RPM-basierte Linux-Distributionen, Darwin
    - Win32-Binärdistribution für Microsoft Windows

Ruhr.pm

Prämissen für Hermes

- um profitabel zu sein, müssen Spammer so viele Spam-EMails so schnell wie möglich zustellen
- die Anzahl simultaner Verbindungen pro Host ist begrenzt
- der Anzahl von Hosts unter der Kontrolle von Spammern ist begrenzt
- das Verfolgen von Zustell-Statusinformationen ist aufwändig und für Spammer unattraktiv

Aktives Banner Delay

- Idee:
  - Nach IETF RFC 821/2821 darf der einliefernde Host erst Daten übermitteln, nachdem er vom SMTP-Server mit einer 220-Meldung begrüßt wurde.
  - Spammer haben es eilig und begrenzte simultane Verbindungen.

Aktives Banner Delay

- Funktion/Implementierung:
  - einige Sekunden Pause vor Begrüßung
  - Spammern werden Ressourcen blockiert
    - belegte Ressourcen (Verbindung, RAM, etc) reduzieren die Anzahl von Spam-EMails, die der Spammer während dieser Zeit an andere Server übermittelt
  - eilige Spammer übertragen trotzdem oder geben auf
    - vorzeitige Übermittlung von Daten beendet die Verbindung (Protokollverletzung)

Aktives Banner Delay

- Vor- und Nachteile
  - reduziert das Spam-Aufkommen bereits deutlich
  - Blockade von Ressourcen bremst Massmailer
    - betrifft Spammer, Newsletter-Versender und Mailinglists
    - reguläre EMail-Server nur minimal beeinträchtigt
  - keine Ablehnung der EMails von regulären Servern
  - stört eventuell Relay-Benutzer
    - falls SMTP-MX auch als SMTP-Relay verwendet wird

Ruhr.pm

Throttling

- Idee:
  - Nach IETF RFC 821/2821 wird ein SMTP-Befehl erst dann verarbeitet, wenn der vorhergehende bestätigt wurde.
  - Spammer haben es eilig und begrenzte simultane Verbindungen.

Throttling

- Funktion/Implementierung:
  - nach jedem SMTP-Befehl wird eine oder mehrere Sekunden Pause eingeschoben
  - Spammern werden Ressourcen blockiert
  - eilige Spammer geben evtl. auf
  - Throttling wird beendet, wenn:
    - der Benutzer sich authentifiziert hat (SMTP-Auth)
    - der DATA-Befehl den Transfer des EMail-Inhalts einleitet

Throttling

- Vor- und Nachteile
  - reduziert Spam etwas
  - Blockade von Ressourcen bremst Massmailer
  - keine Ablehnung der EMails von regulären Servern

Deaktivierung von Pipelining

- Idee:
  - IETF RFC 1854/2920 definiert die SMTP-Erweiterung “Pipelining”.
    - erlaubt das Zusammenfassen und die Übermittlung mehrerer SMTP-Befehle auf einmal
    - implementiert von den meisten MTAs, teilweise nicht per Konfiguration zu deaktivieren
    - beschleunigt regulären EMail-Verkehr nur minimal
    - Hauptprofiteure sind Massmailer

Deaktivierung von Pipelining

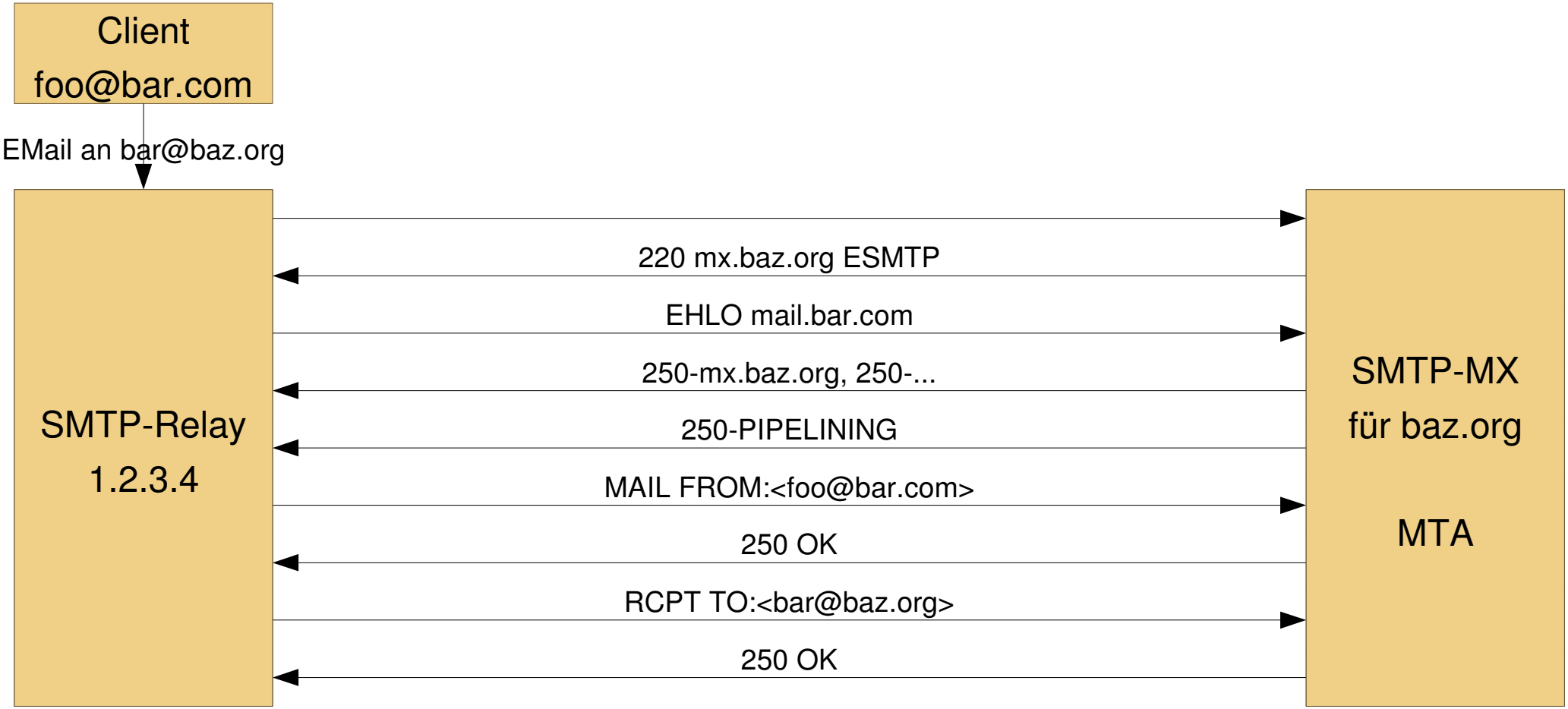
- Funktion/Implementierung:
  - die Optionszeile “250-PIPELINING” wird unterdrückt, sofern vom MTA übermittelt
  - Pipelining wird nicht akzeptiert

Deaktivierung von Pipelining

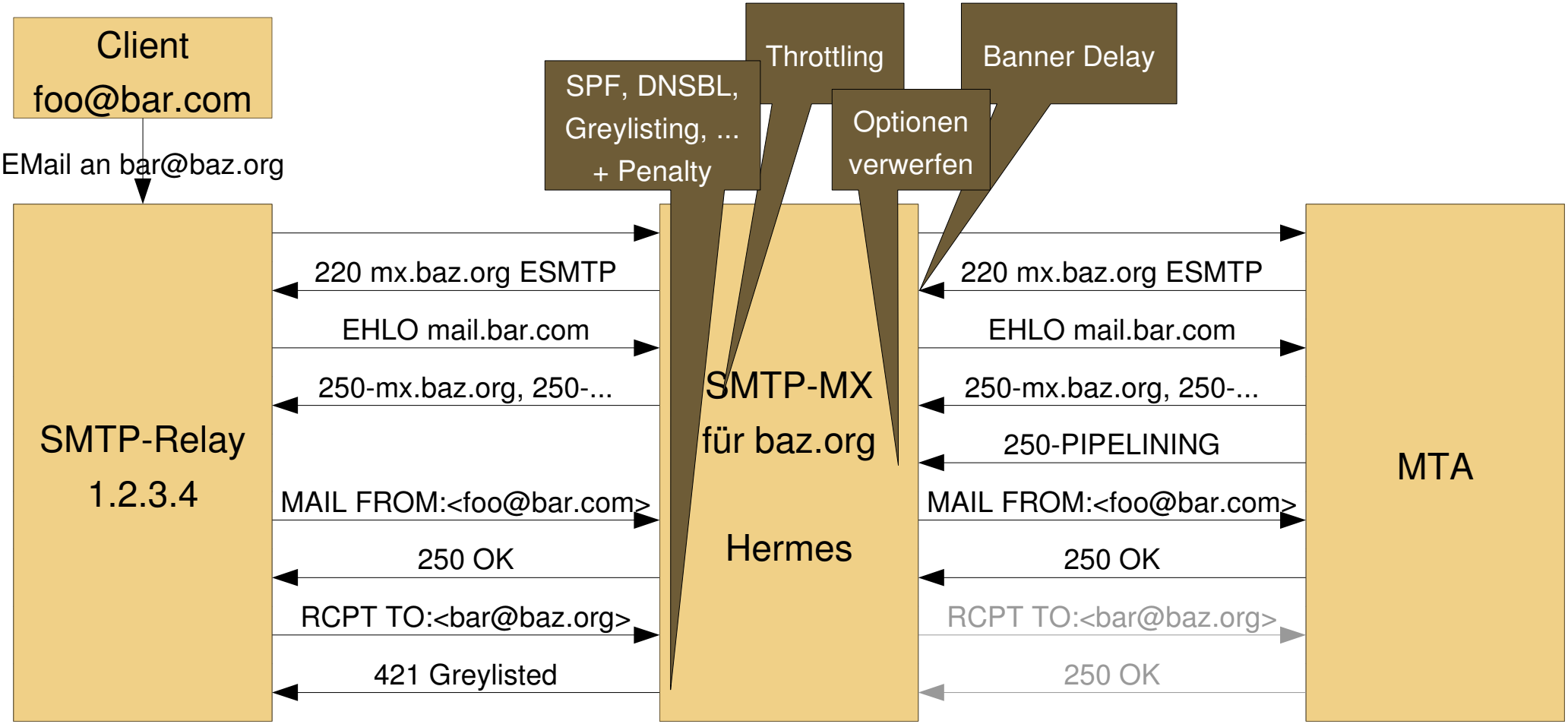
- Vor- und Nachteile
  - verhindert Ersparnis durch Pipelining bei notwendigen Betriebsressourcen der Massmailer
  - keine Ablehnung der EMails von regulären Servern

Ruhr.pm

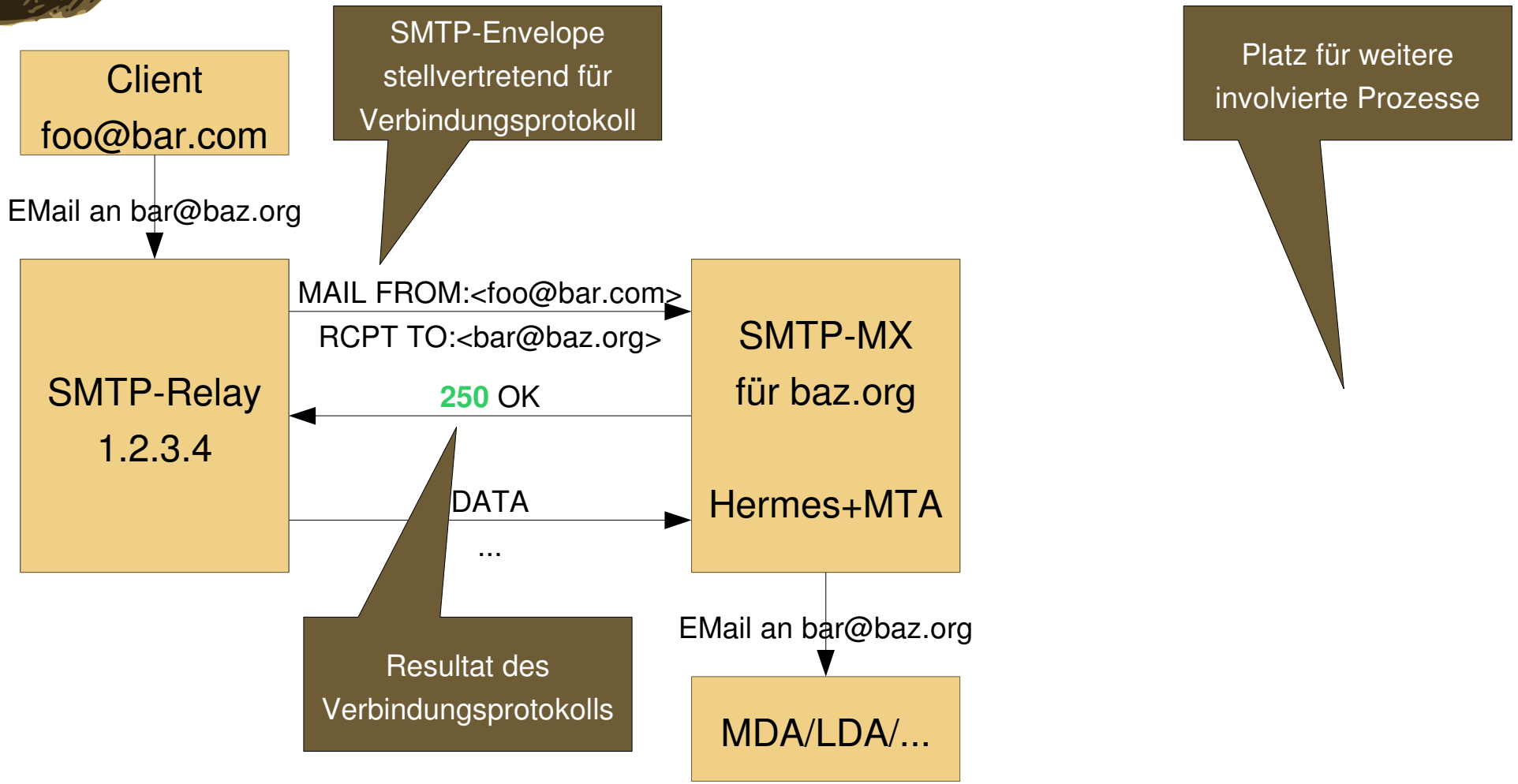
Reguläre EMail-Zustellung



EMail-Zustellung mit Hermes



Vereinfachte Darstellung



Ruhr.pm

Greylisting

- Idee:
  - Das Verfolgen von Zustellinformationen ist aufwändig (Zeit, Bandbreite, Speicher, zusätzliche Verbindungen) und für Spammer damit eher unattraktiv.
  - Nach IETF RFC 821/2821 akzeptiert jeder korrekt implementierte SMTP-Server “Soft Rejects” und unternimmt in diesem Fall erneute Zustellversuche.
  - Ablehnen nur des ersten Zustellversuchs aus bislang unbekannter Quelle mit einem “Soft Reject”.

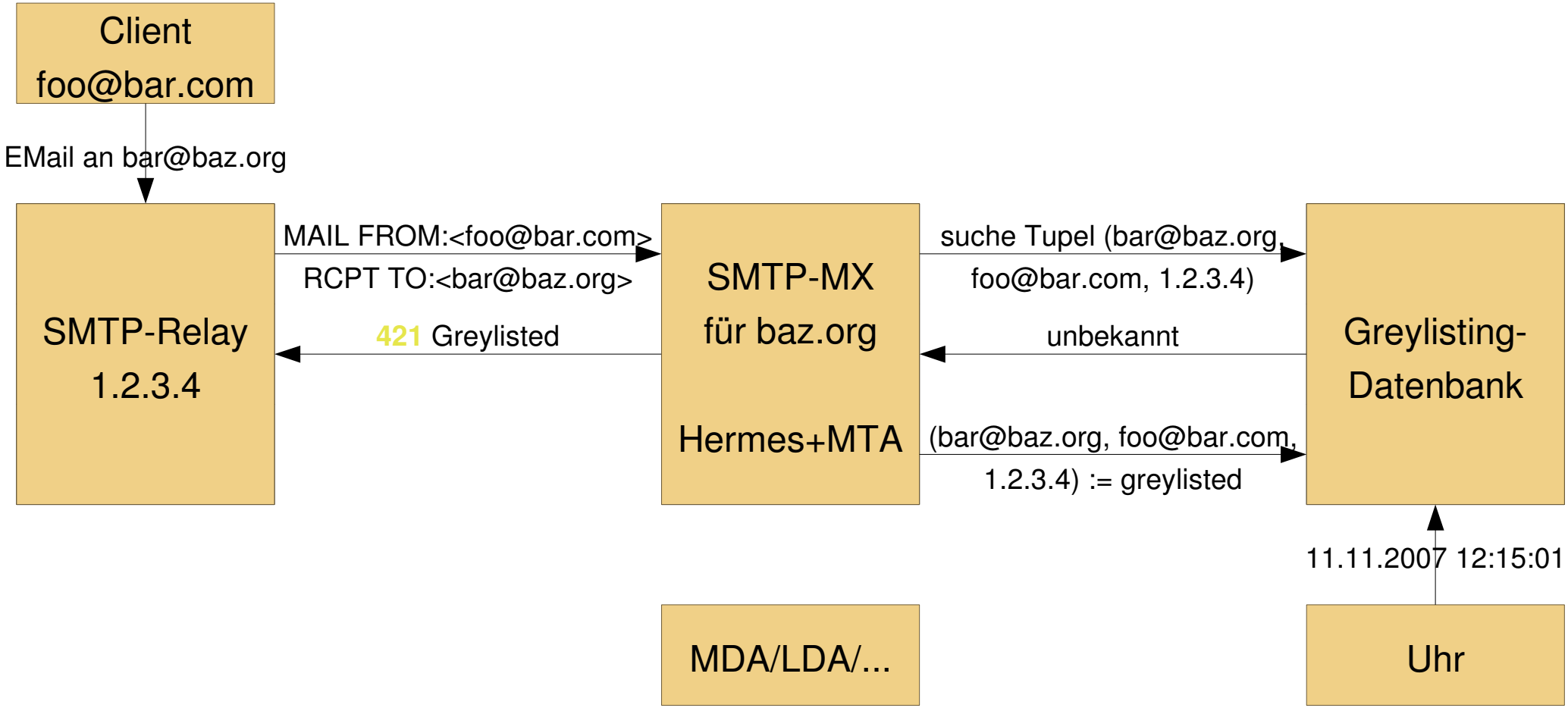
Greylisting

- Funktionsweise/Implementierung:
  - erster Zustellversuch eines Tupels aus Absender, Empfänger und SMTP-Client wird abgelehnt
  - weitere Zustellversuche werden akzeptiert und das Tupel für die Zukunft gespeichert/aktualisiert
  - Whitelists erlauben Ausnahmen vom Greylisting
    - Host (IP-Adresse)
    - Reverse-Hostname
    - Empfänger-Adresse oder -Domain

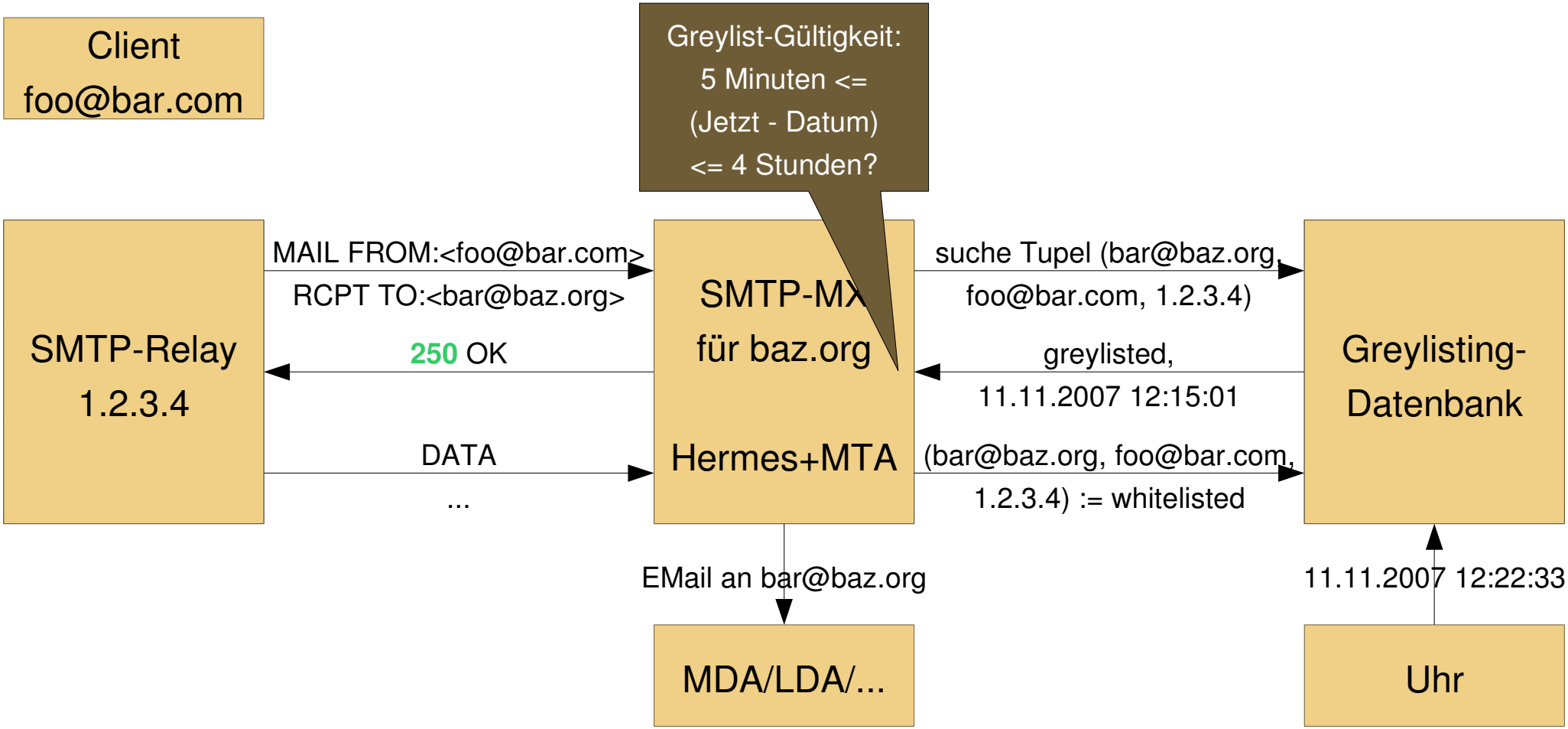
Greylisting

- Vor- und Nachteile:
  - sehr effektiv gegen den meisten Spam
    - außer Spam von regulären MTAs (meist gehackte Hosts)
  - Zustellverzögerungen bei EMails von neuen oder sehr seltenen Kontakten von mehreren Minuten
  - die Annahme, dass alle Zustellversuche vom selben Host ausgehen, ist nicht zwingend korrekt
    - Probleme mit Google Mail bekannt, Workaround

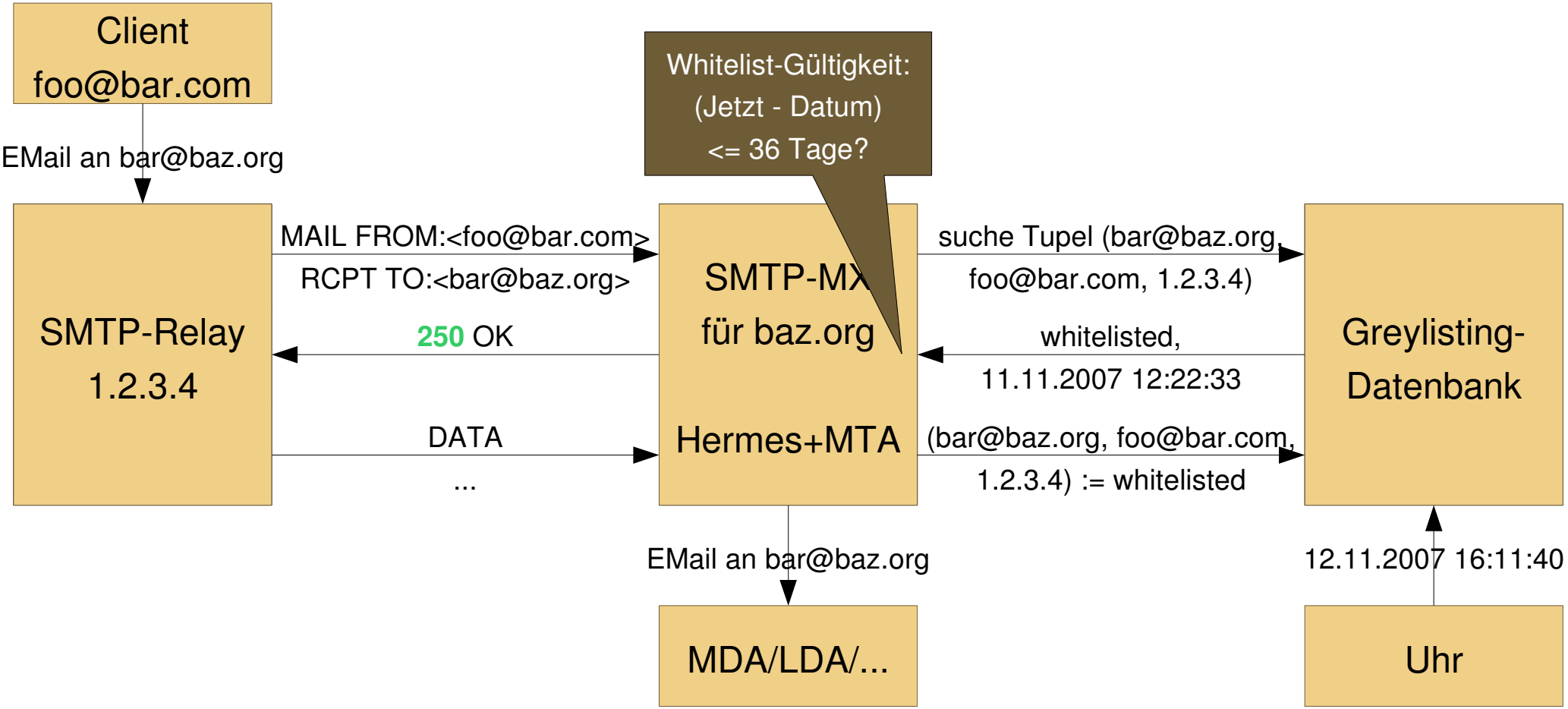
Greylisting: erster Versuch



Greylisting: zweiter Versuch



Greylisting: weitere EMail



Sender Policy Framework

- Idee:
  - Ein Domain-Besitzer kann und darf entscheiden, wer EMails mit seiner Domain als Absender verschickt.
- Geschichte:
  - seit April 2006 spezifiziert unter IETF RFC 4408
  - vor Februar 2004: “Sender Permitted From”
  - geht zurück bis auf Paul Vixies “An idea: SMTP MAIL FROM verification” von Dezember 1997

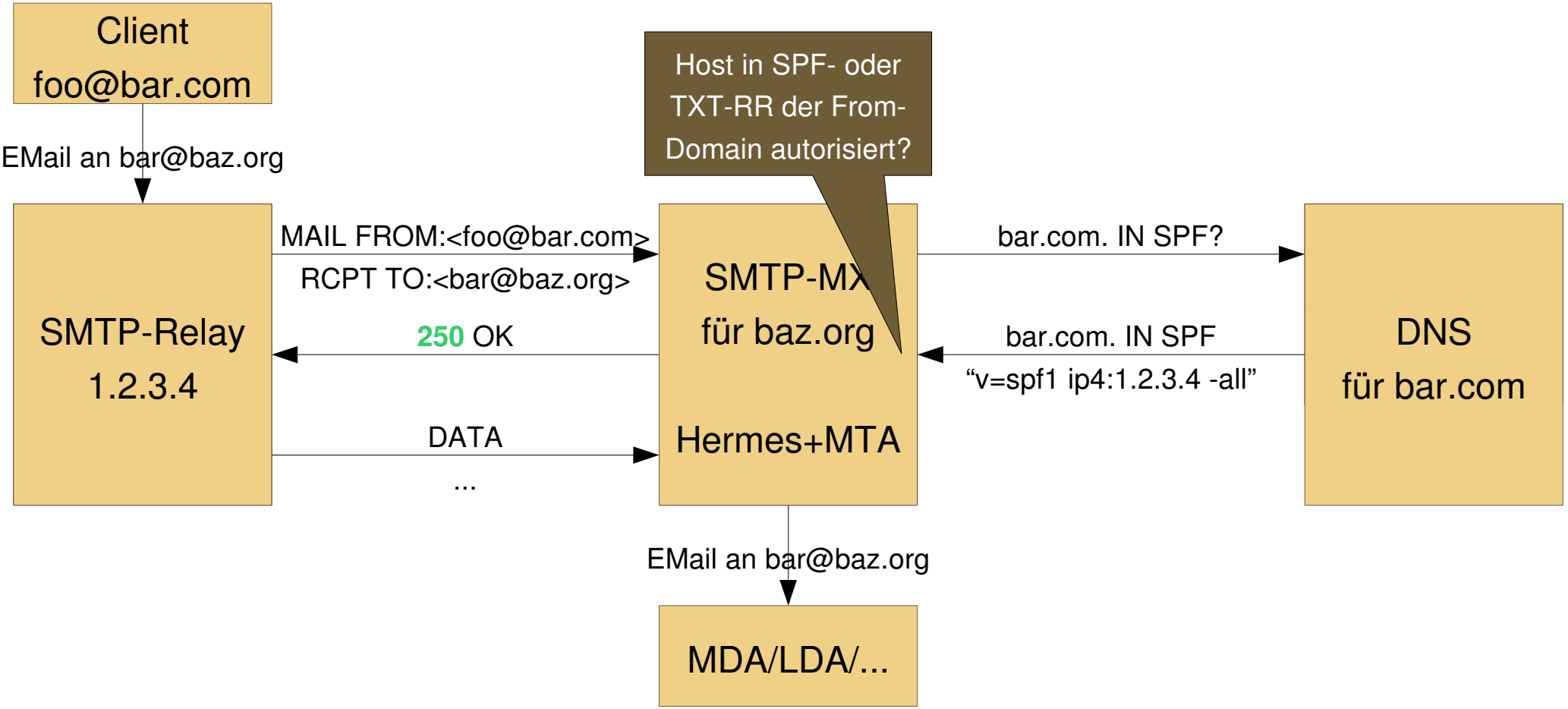
Sender Policy Framework

- Funktionsweise:
  - Veröffentlichung von Autorisierungsinformationen als SPF-Direktiven im DNS in SPF- oder TXT-RRs
  - flexible Mechanismen definieren Hosts
    - IPv4-/IPv6-Adresse, PTR-/A-/MX-RRs, “alle anderen”
    - Netz-Option: “auch Hosts unterhalb dieser Netmask”
    - Ererben der Direktiven anderer Domains
  - Qualifikatoren legen Schicksal fest
    - pass, fail, soft fail (Empfänger entscheidet) und neutral

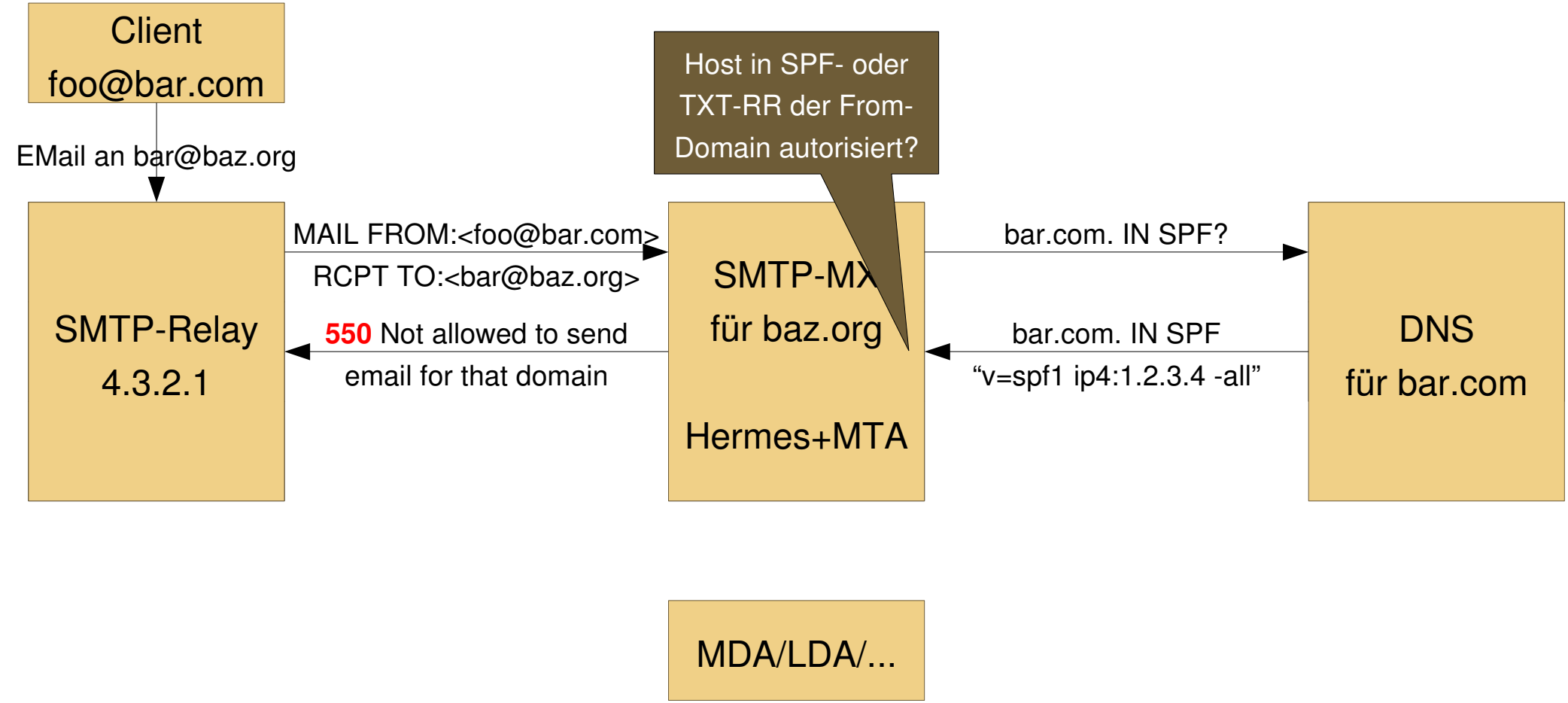
Sender Policy Framework

- Vor- und Nachteile:
  - effektiv gegen Phishing-Mails und Domain-Missbrauch
  - nicht effektiv gegen Spam-Mails
    - Spammer registrieren einfach eigene Domains oder suchen gezielt nach Domains ohne SPF
  - keine Ablehnungen falls DNS nicht verfügbar
  - evtl. Ablehnung weitergeleiteter EMails (Forwarder)
    - ändern des Absenders im SMTP Envelope per SRS
    - Patch für Ausnahme einzelner Empfänger von SPF

Sender Policy Framework: legitim



Sender Policy Framework: Spam



Ruhr.pm

DNS-based Blackhole List

- Idee:
  - ein Host, der einmal Spam-EMails verschickt, verschickt weiterhin Spam-EMails
  - Blacklists können automatisch generiert werden
    - Dial-In-Netze, z.B. aus der RIPE-DB
    - Honey Pot (versteckt veröffentlichte EMail-Adressen)
    - Scans nach Open Relays
  - Blacklists können handverlesen sein
    - aufwändig, i.d.R. nur gegen Gebühr nutzbar

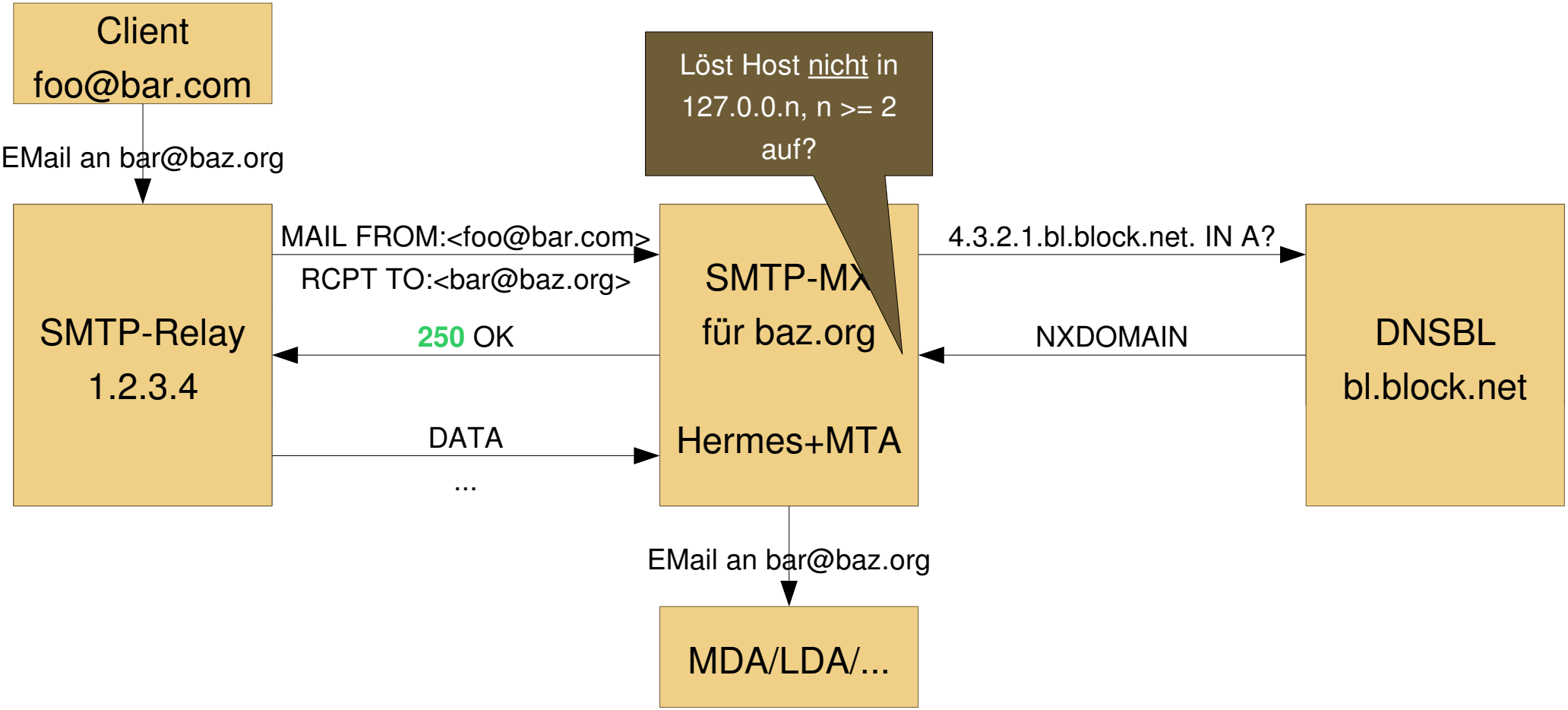
DNS-based Blackhole List

- Funktionsweise/Implementierung:
  - EMail-Zustellung wird abgelehnt, wenn der einliefernde Host in DNSBLs gelistet ist
    - z.B. Spamcop.net, NJABL, Spamhaus, blackholes.us, ...
  - die Anzahl der für eine Ablehnung notwendigen Treffer ist konfigurierbar
  - Whitelists erlauben Ausnahmen von DNSBLs
    - gemeinsame Whitelists mit Greylisting

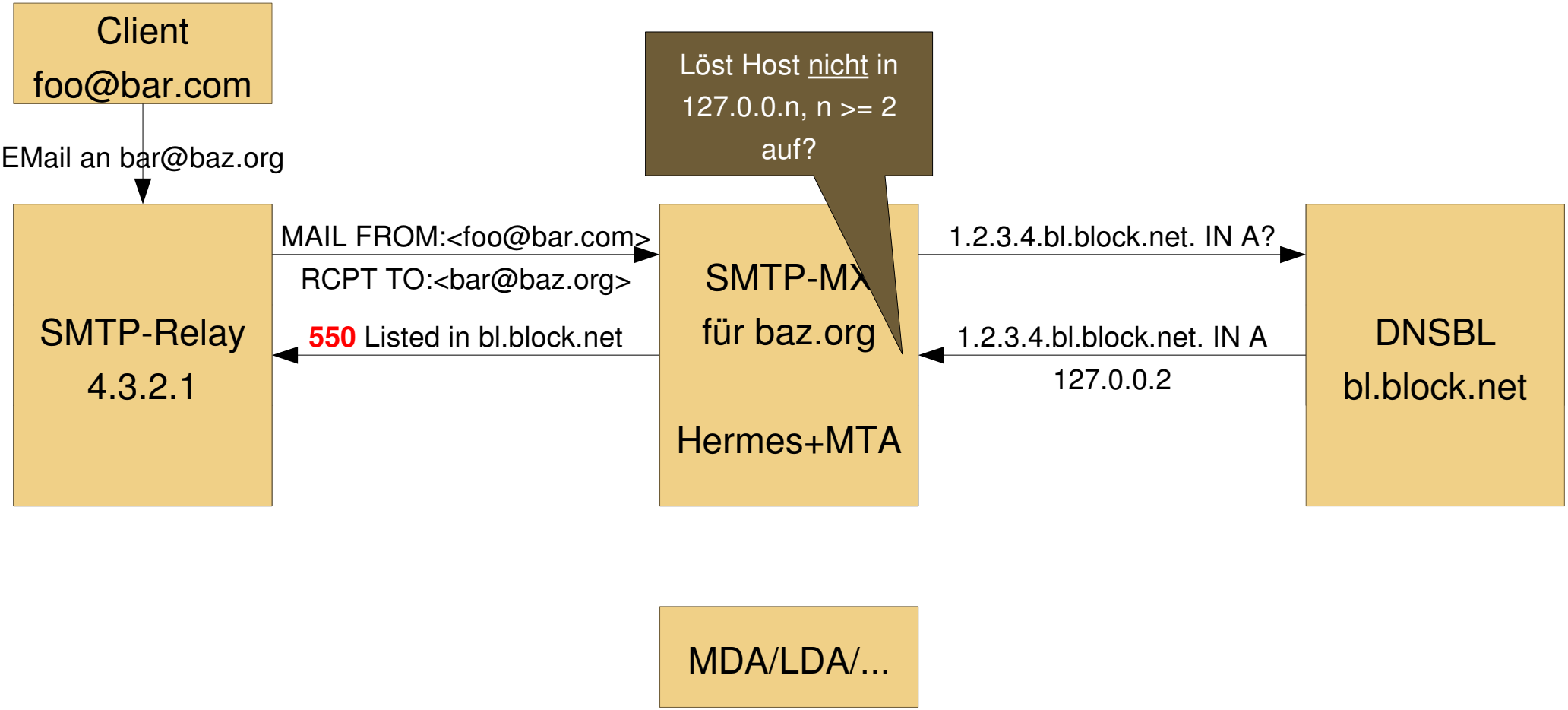
DNS-based Blackhole List

- Vor- und Nachteile:
  - effektiv – aber fehleranfällig
    - oft fehlerhafte Zuordnungen (z.B. ganzer ISP als Dial-In)
    - ISPs/Mailserver/Webserver werden unschuldig gelistet
      - einzelne Kunden verschicken Spam-Mails
      - Newsletter werden als Spam gemeldet
    - Entfernung von DNSBLs oft nicht/nur schwer möglich oder nur gegen Gebühr
  - keine Ablehnungen falls DNS nicht verfügbar

DNS-based Blackhole List: legitim



DNS-based Blackhole List: Spam



DNS-based White List

- identisch mit DNSBLs, enthalten aber Hosts, die bekannt sind, keinen Spam zu verschicken
  - Eintrag i.d.R. nur gegen Gebühr, Zertifikat oder Vertrag mit Strafe
- Listing in ausreichend vielen DNSWLs setzt ablehnende Tests aus

Reverse Hostname Check

- Idee:
  - Reguläre Server besitzen einen PTR-RR bzw. es ist zumutbar, PTR-RRs für Server einzurichten.
    - Kein Standard oder RFC setzt voraus, dass EMail-Server PTR-RRs besitzen müssen!
- Funktion/Implementierung:
  - löst die IP-Adresse eines einliefernden Hosts nicht auf einen Hostname auf, wird die Übermittlung abgelehnt
  - Whitelists erlauben Ausnahmen von PTR-RR-Check

Reverse Hostname Check

- Vor- und Nachteile:
  - bedingt effektiv gegen Zombie-Hosts
  - false positives möglich
    - allerdings inzwischen weit verbreitet und akzeptiert
  - kein Standard oder RFC setzt PTR-RRs für Server voraus

Ruhr.pm

Rejection Penalty

- Idee:
  - Nach IETF RFC 821/2821 muss ein einliefernder Host warten, bis ein Server Erfolg oder Misserfolg des letzten Befehls meldet.
    - sonst gilt eine EMail nicht als zugestellt
  - Spammer haben es eilig und begrenzte simultane Verbindungen.

Rejection Penalty

- Funktion/Implementierung:
  - wird die Übermittling einer EMail abgelehnt, wird die Statusmeldung mehrere Sekunden verzögert
    - sowohl Soft Rejects als auch Final Rejects

Ruhr.pm

Rejection Penalty

- Vor- und Nachteile:
  - Spammern werden Ressourcen blockiert
    - trifft auch die SMTP-Relays und unbekannten/ unregelmäßigen Absendern im Greylisting
    - legitime Massmailer (z.B. Newsletter) i.d.R. nicht/kaum betroffen

Ruhr.pm

Vielen Dank
für Ihre Aufmerksamkeit

Ruhr.pm

Links

- Hermes Anti-Spam Proxy
  - http://www.hermes-project.com/
- Präsentation, Patches, RHEL-/CentOS-RPMs
  - http://ruhr.pm.org/treffen/artikel.psp?id=52
  - http://ruhr.pm.org/material.psp