DIME

— Dark Internet Mail Environment —

Jan Lenk

Free and Open Source Software AG
Fakultät für Informatik
March 10, 2017

Inhaltsverzeichnis

Inhaltsverzeichnis

Motivation - Warum?
Oh man, nicht noch ein Mail-Standard

- Verschlüsselung (z.B. PGP) ist guter Schutz
  - leider noch nicht sehr verbreitet
- Großes Problem sind Metadaten
  - Empfänger
  - Sender
  - IP-Adressen
  - ...

Motivation - Geschichte
Who the fudge is Ladar Levison?

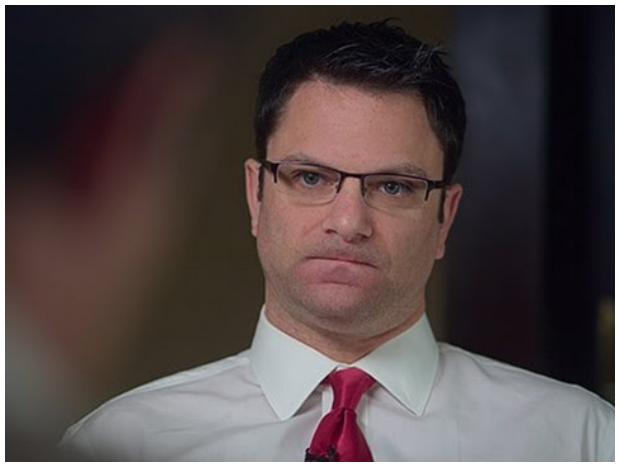


Figure: Ladar Levison

Figure: Princess

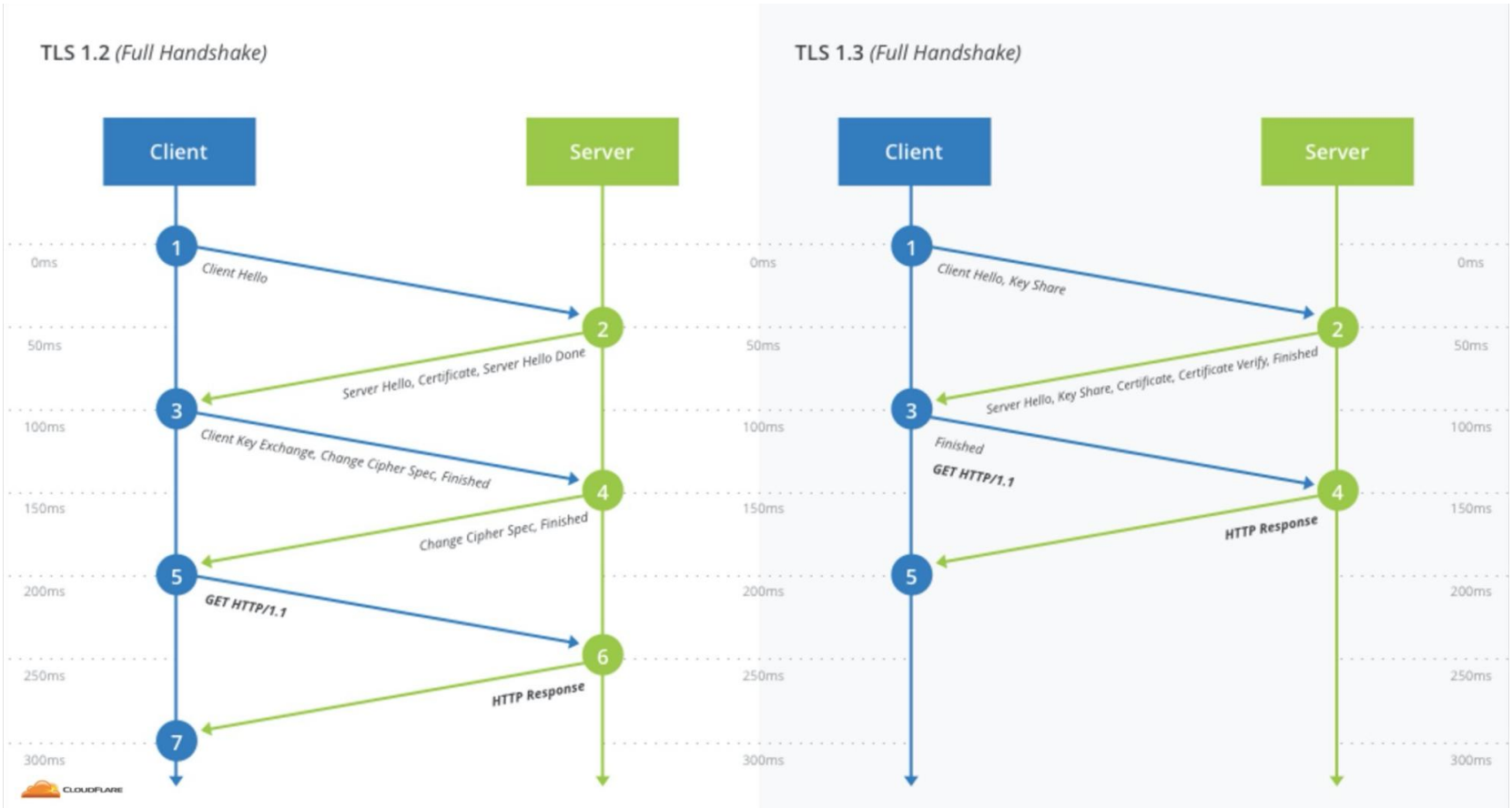
- Lavabit: anonymer Mail-Dienst
- August 2013 wurde Ladar vor Gericht geladen
  - NSA wollte alle privaten Schlüssel und Mails

1

[1] http://www.newyorker.com/tech/elements/how-the-government-killed-a-secure-e-mail-company

Inhaltsverzeichnis

SSL/TLS - 1


TLS 1.2 (Full Handshake)
Client
Server
0ms
50ms
100ms
150ms
200ms
250ms
300ms
1
Client Hello
2
Server Hello, Certificate, Server Hello Done
3
Client Key Exchange, Change Cipher Spec, Finished
4
Change Cipher Spec, Finished
5
GET HTTP/1.1
6
HTTP Response
7
CLOUDFLARE
TLS 1.3 (Full Handshake)
Client
Server
0ms
50ms
100ms
150ms
200ms
250ms
300ms
1
Client Hello, Key Share
2
Server Hello, Key Share, Certificate, Certificate Verify, Finished
3
Finished
GET HTTP/1.1
4
HTTP Response
5

SSL/TLS - 2
Secure Socket Layer/Transport Layer Security

- setzt direkt auf TCP auf
- Beobachter kann nur sehen:
  - Verbindungsendknoten
  - Typ der Verschlüsselung
  - Frequenz der Datenübertragung
  - annähernde Menge der Daten
- Ablauf:
  1. Client sendet Spezifikationen in Klartext
  2. Server sendet Spezifikationen + Zertifikat
  3a. Client überprüft Zertifikat
  3b. Client initiiert Schlüsselaustausch (RSA/DH)
  4. Verifizierung des Schlüssels

DNSSEC

- alle DNS-Antworten sind signiert (Authentizität)
- Chain of Trust:
  - Parentdomain verifiziert Subdomain
  - Startpunkte sind Trust Anchors (authoritative Nameserver)
- ca. 15% der Nameserver weltweit nutzen DNSSEC (Stand: 19.02.2017) [2]

[2] https://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=1&r=1&w=7&g=0

Inhaltsverzeichnis

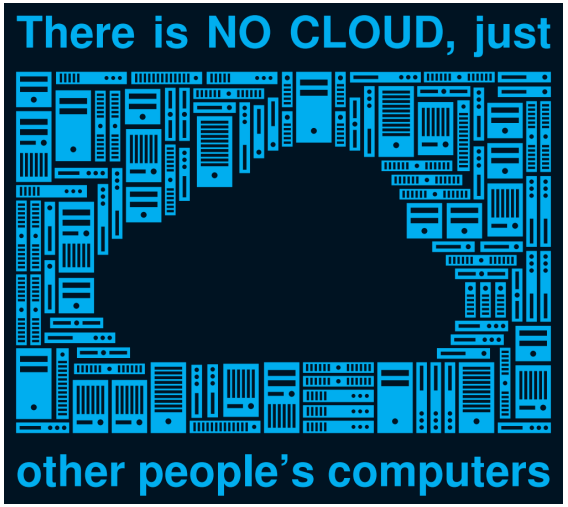
SMTP - Simple Mail Transfer Protocol

- erweiterbar mit TLS
- Auflösen von Mail-Adresse um an SMTP-Server zu kommen
- Probleme:
  - Einspielen und Umleiten von Mails
  - Manipulieren von Sender und Empfänger Zeile
  - Beeinträchtigung von Verkehr durch DDoS

IMAP - Internet Message Access Protocol

- Nachrichten bleiben auf Server gespeichert
- mehrere Benutzer sind parallel online
- ungünstig: langes aufrechthalten der Verbindung

POP - Post Office Protocol



- Nachrichten werden lokal gespeichert
- kurzes aufrechthalten der Verbindung
- nur ein Benutzer darf online sein
- ungünstig: veraltetes Protokoll

MIME - Multipurpose Internet Mail Extension

- alle Mails werden im MIME-Format verschickt
- erweitert das Mail-Format auf:
  - Zeichen außerhalb des ASCII-Zeichensatzes
  - nicht Textanhänge (z.B. Bilder und Videos)
  - Header Informationen nicht im ASCII-Format
  - Body mit mehreren Teilen

Inhaltsverzeichnis

Anforderungen - 1

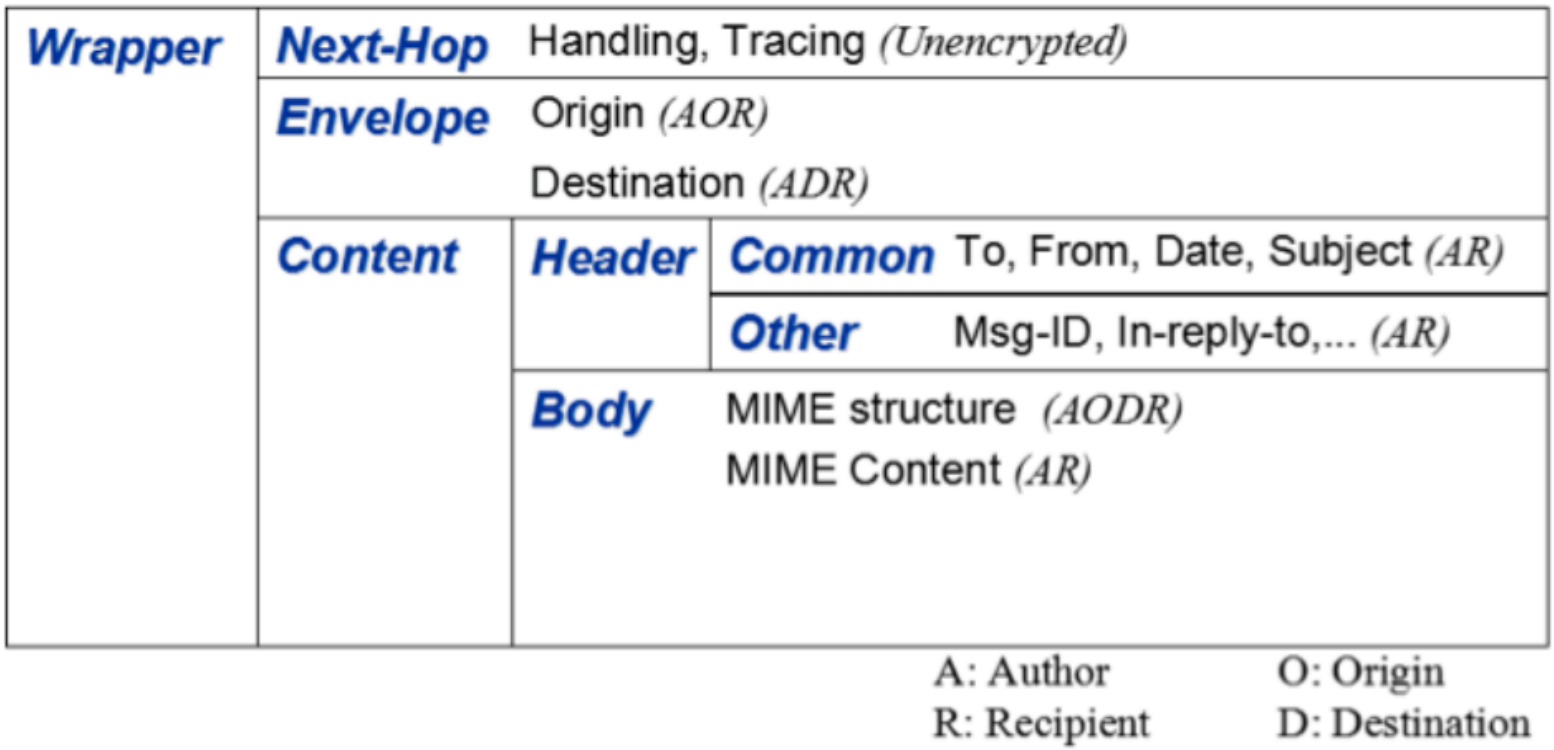


Figure 5 - DIME Message Object

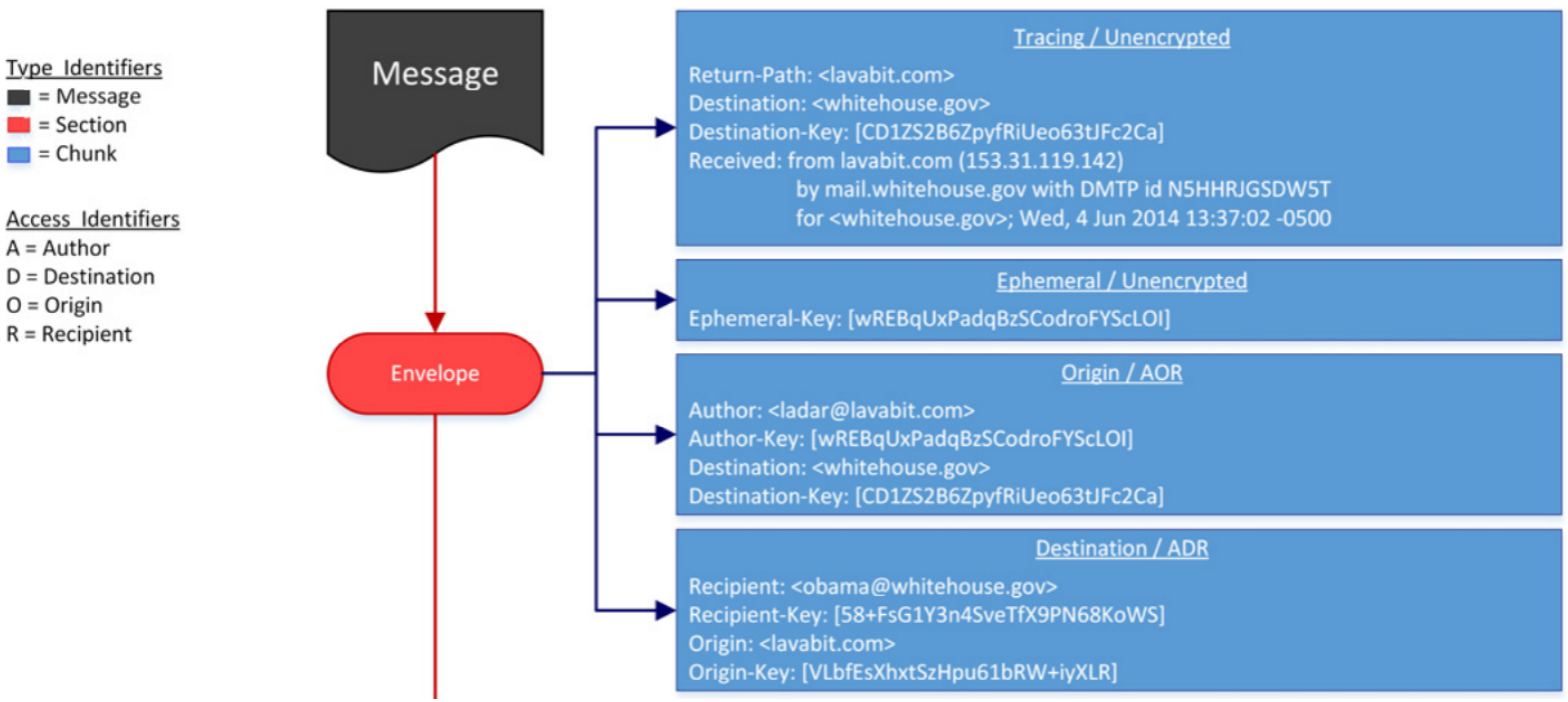
Anforderungen - 2

- Sender- und Empfängeradressen sind verschlüsselt und eingebettet
- nur Sender und Empfänger können ganze Nachricht entschlüsseln
- Nachricht wird in Baumstruktur umgewandelt
- Validierung der Schlüssel immer über 2 Quellen

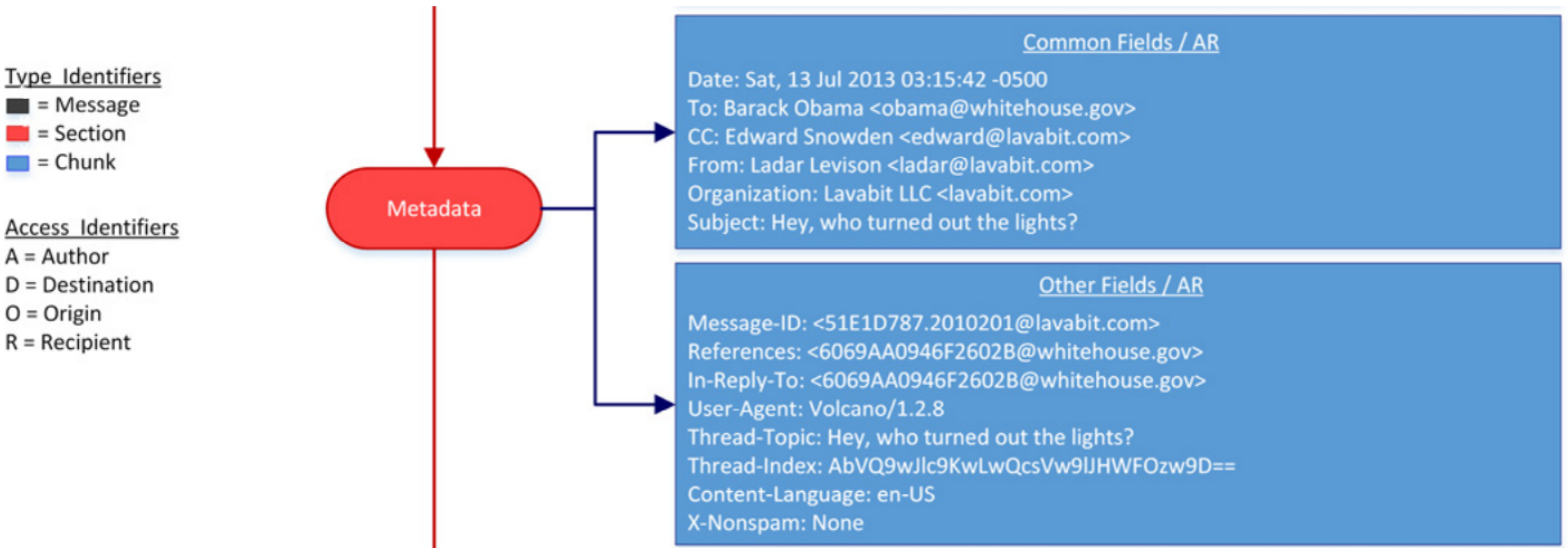
Nachricht - Aufbau 1

- jede Nachricht verschlüsselt mit kurzlebigem Schlüssel
- Aufteilen der Nachricht in Chunks
  - seperate Verarbeitung
  - jeder mit individuellem, kurzlebigem und symmetrischen Schlüssel verschlüsselt
  - mehrere Schlüsselslots (für jeden Teilnehmer)

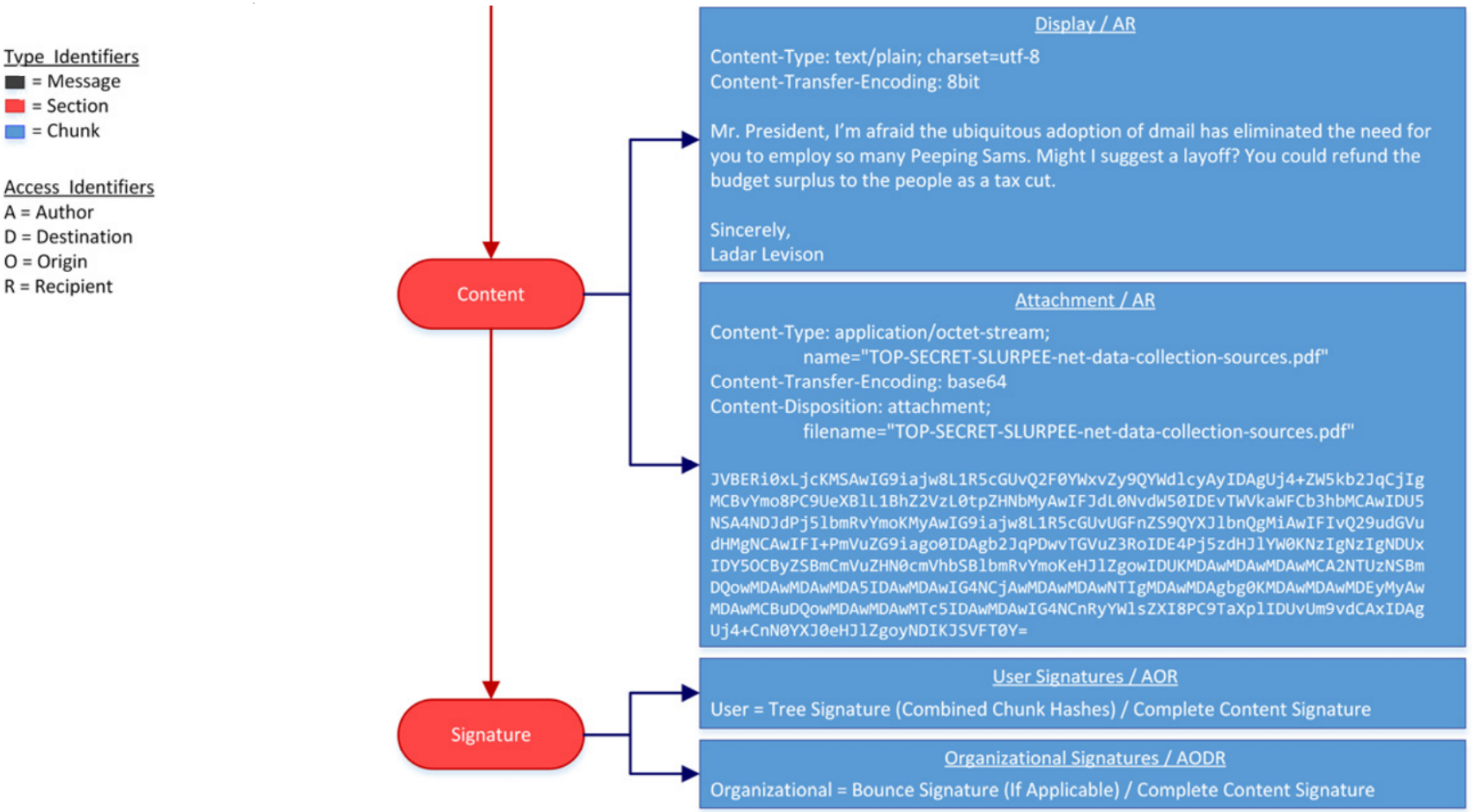
Nachricht - Aufbau 2



Nachricht - Aufbau 3



Nachricht - Aufbau 4



Signet Data Format

- versenden von kryptografischen Informationen
- trägt Signaturen zur Validierung von Benutzer und Organisation
- Felder:
  - cryptographic (öffentliche Schlüssel und Signaturen)
  - informational (ermöglicht Verwendung von verschiedenen Feldern)
  - undefined (willkürlicher Name, Daten Werte)
- Klassen:
  - organisation signet: assoziiert mit Domain Name
  - user signet: assoziiert mit Mail-Adresse

Privacy Processing Agent - 1
Organisation Privacy Agent

- Schnittstelle zwischen E-Mail Client und Internet
- erleichtert Schlüsselverwaltung
- erzeugt Domain-Name basiertes Paket um komplette Nachricht

1. Signierung:
   - Authentität von Benutzer Signet bzw. beliebiger Nachricht
   - mittels krypt. Signatur von Organisation Server
2. Verschlüsselung:
   - packt und entpackt User Mailadresse
3. Channel: TLS
   - Nachrichtstruktur nur bei kompromitierten Kanal sichtbar

Privacy Processing Agent - 2
User Privacy Agent

- bietet kryptographische Funktionen von User
- ermöglicht:
  - Schlüsselmanagement
  - Rückgewinnung von Signet
  - Ausgabe von Warnungen an User
  - automatische Verschlüsselung

Signet Retrieval Service
I want my signet and I want it now!!

- Benutzer stellt Anfrage an lokalen Signet Resolver
- Signet Resolver sucht Key Service via DNS Resolver
- Signet Resolver empfängt und validiert Signet

1. Organisation verifiziert Benutzer
2. Key Service verifiziert Organisation

Fingerprints

- holen von spezifischem Signet (Identifizierung)
- Verifizierung der Gültigkeit von gespeichertem Signet
- erzeugt durch SHA2-512 von kryptographischem Signet
- wird in verschlüsseltem Umschlag mitgesendet

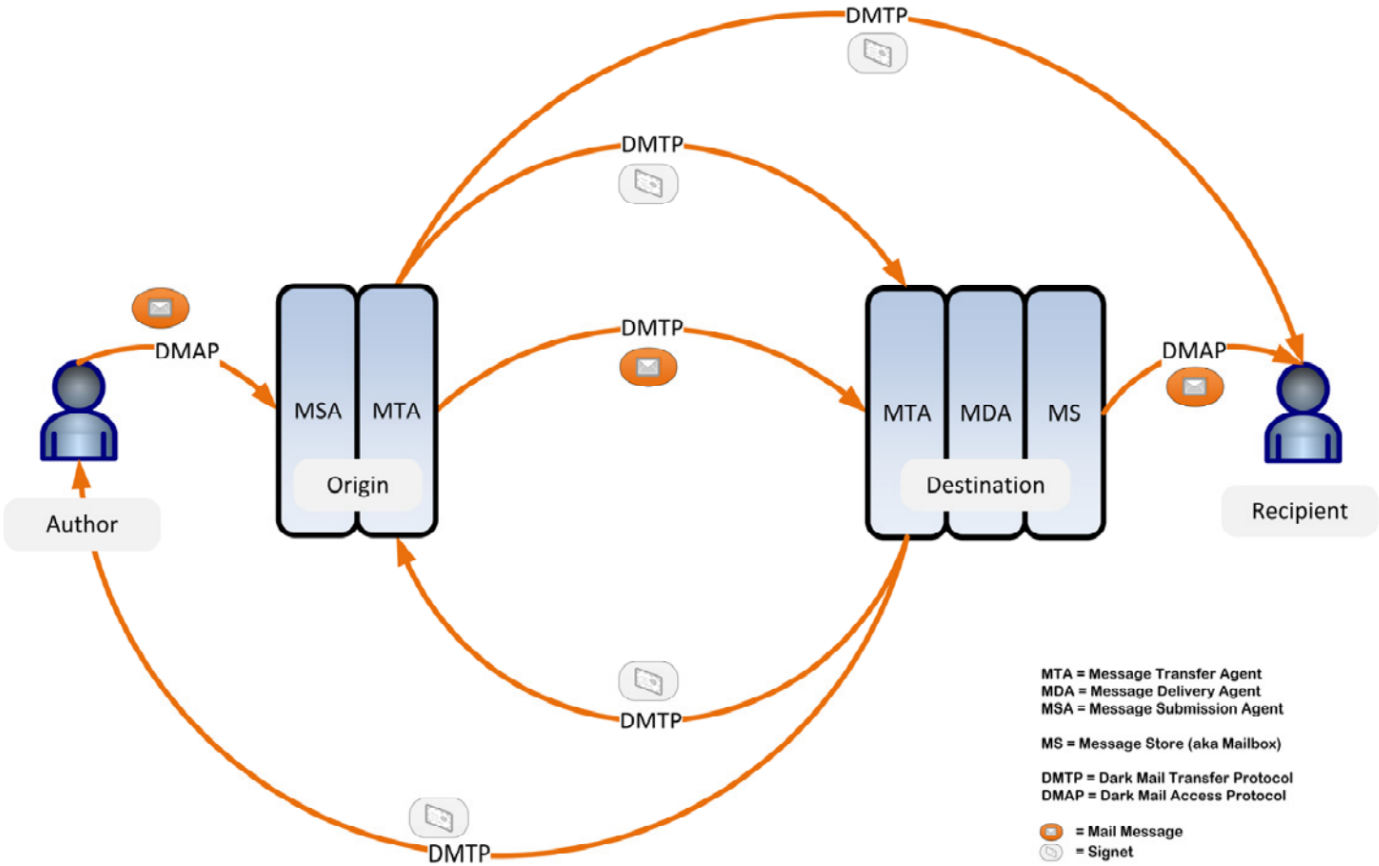
Management Record

- im DNS-System bereit gestellt
- verbreitet Vorschriften und Hostname Informationen
- kryptographischer Vertrauensanker von DIME
- finden von organisations Key Service
- verbreiten von public organisation Keys

D/MIME
Message Data Format

- Aufgaben:
  - Kopf und Körper werden in Chunks zerlegt
  - individueller, kurzlebiger und symmetrischer Schlüssel für Chunks
- Domain Keys Identified Mail (DKIM):
  - Nachrichten müssen von Author und organisatorischer Domain signiert werden
- benutzte krytographische Algorithmen:
  1. Elliptical Curve und Diffie-Hellman für Schlüssel generierung
  2. AES für Nachricht und Keyslots
  3. Verifizieren der Nachricht via Edwards-Curve Signatur

Anforderungen - 1



DMTP - Dark Mail Transfer Protocol

- Mail Transfer:
  - Aufbau TCP/TLS Verbindung
- Signet Resolver:
  - Holen von Signets
  - Überprüfen der stabilität von gecacheten Signets
- Unterschied zu SMTP:
  1. Mailbox Namen von protokoll Verkehr entfernt
  2. neue Kommandos für Signet Handhabung
  3. TLS Unterstützung nicht mehr optional

DMAP - Dark Mail Access Protocol

- Authentifizierung
- Kommunikation zwischen Benutzer und Organisations Server
- Zeigen der Kenntnis über Passwort ohne dieses zu senden

Inhaltsverzeichnis

Funktionsumfang - Account Modes

How paranoid are you?

1. Trustful:
   - Server erzeugt und speichert Signet und verschlüsselten privaten Schlüssel
2. Cautious:
   - User erstellt Schlüssel und Signet
   - Server speichert privaten verschlüsselten Schlüssel
3. Paranoid:
   - Benutzer erzeugt Schlüssel und Signet lokal
   - Server bekommt keine Kopie von Schlüssel, jedoch Signet

Inhaltsverzeichnis

Zusammenfassung

- Header und Body sind verschlüsselt
- trotz zentraler Instanzen, komplette Kontrolle
- Metadaten sind geschützt
- easy to use
- Bald werden Accounts frei geschaltet
- modifizierter Client nötig (soon to be released)

Noch Fragen?

- DIME:
  - https://darkmail.info/
  - https://lavabit.com/
  - https://darkmail.info/downloads/dark-internet-mail-environment-march-2015.pdf [Spezifikation]
  - https://github.com/lavabit/ [code]
  - https://lavabit.com/explain-lavabit.html [kurze Erklärung]
- FOSS-AG: https://foss-ag.de
- Jan:
  - Riot: @ThiefOfTime
  - Telegram: @ThiefOfTime
  - Mail: thiefoftime@protonmail.ch