Renewal of the Email Services
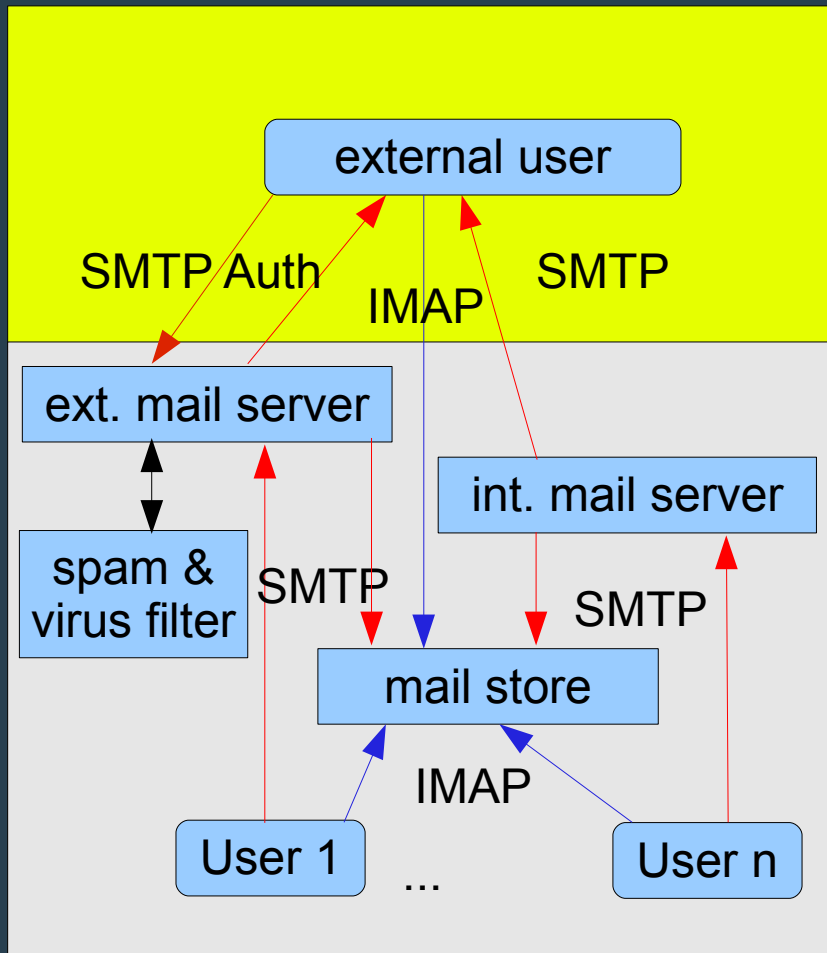
IMAP, SMTP & Co.

Wolfgang Friebel

Technical Seminar Zeuthen, 6.10.2009

Outline of the talk

- Schematic view of the mail flow in Zeuthen

- What will when be changed

- Receiving email and configuration of mail clients

- Sending email

- Spam and mail filtering
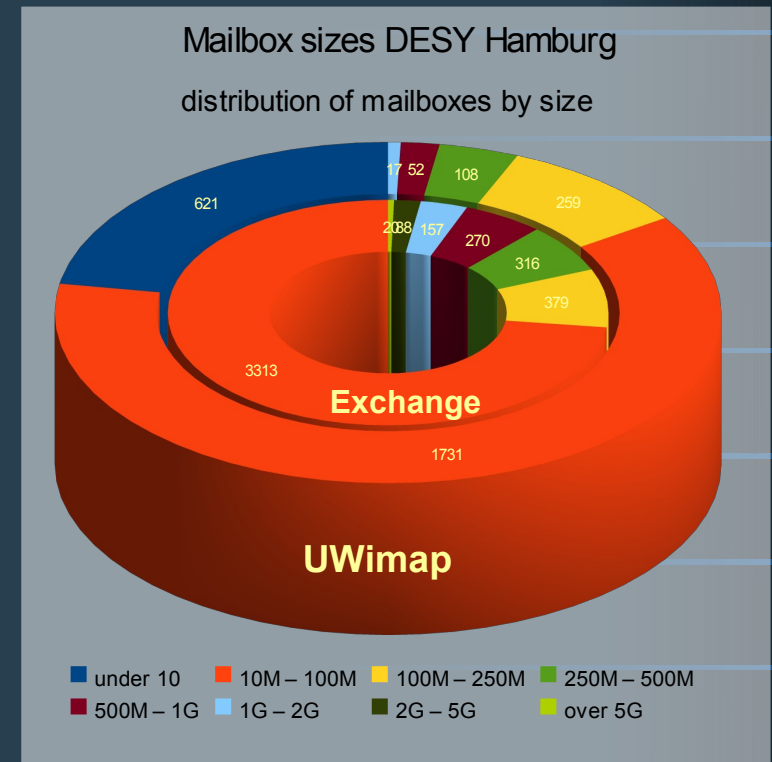
- Frequently asked questions

- Next steps

The mail flow in Zeuthen

- SMTP for sending mail
- SMTP Auth to send from outside
- IMAP for reading mail
- external mail server currently also mail store
- external server performs spam tagging and virus scanning on a separate machine
- Users can send/receive emails using Hamburg servers as well

Why a new IMAP Server

- dovecot can handle 1000 active users on a single computer
- UW-IMAP (with mbox format) allows no concurrent access
    - Concurrent access to mails can cause locking or loss of emails
- Mbox format limit 2GB reached soon
- Slow access with mbox format
- Flexibility of dovecot
    - ACL's for folders
    - compressed folders
    - quota
- Situation with developers

Mailbox sizes DESY Hamburg

distribution of mailboxes by size

Exchange

UWimap

|			
■ under 10	■ 10M – 100M	■ 100M – 250M	■ 250M – 500M
■ 500M – 1G	■ 1G – 2G	■ 2G – 5G	■ over 5G

New IMAP Server

- UW-IMAP gets replaced by dovecot
- Server supports additional folders besides INBOX (quota of 1 GB in addition to AFS home directory quota)
  - mail quota can get displayed using check_inbox (Linux)
- no more locking problems (AFS!!!)
- Much higher speed of email access
- central mail filtering (sieve scripts on imap server)
  - central mail filter by default moves spam mails into the junk folder
- Use of own filters possible
  - but no login on imap, hence upload using mail client

Configuration changes for users

- separate servers for sending (mail) and reading (imap) of mail

- INBOX of all users will be on imap instead on mail

  - more than 50 users already moved, others will follow until end of Oct
- new internal server for sending (mail1) is operational

  - now on a virtual machine

- no more access to folders in AFS space using the IMAP server
  - folders in AFS accessible as local folders only
  - folders on IMAP server are not in AFS space

Comparison of UW-IMAP and dovecot
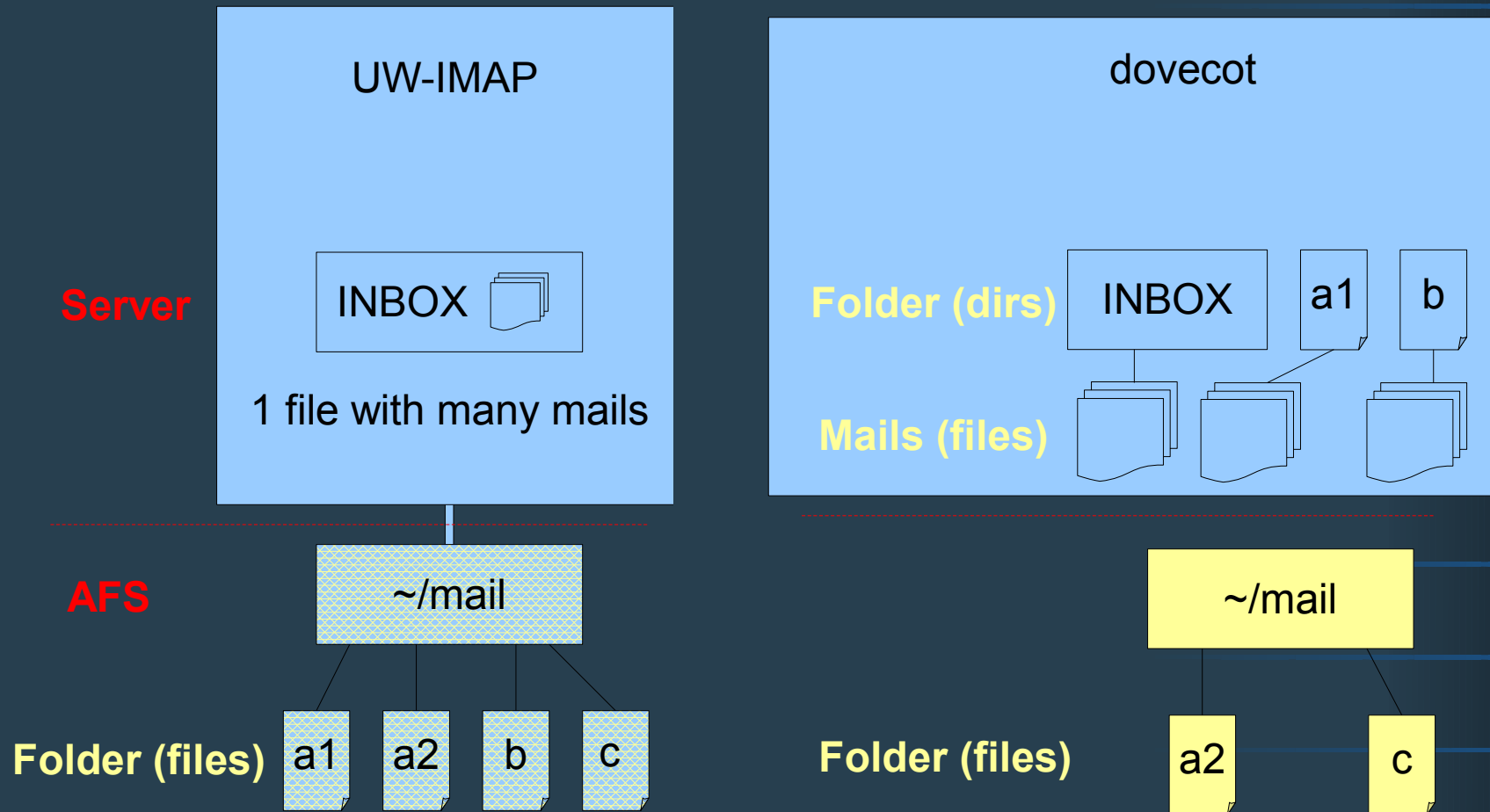
Move from mail to imap (1)

- before October 15:
  - move is voluntary, user is sending an email to postmaster@ifh.de when move should take place. On request **all** folders in ~/mail in AFS space can be copied to the IMAP server (max. 500 MB)
  - folder names containing certain chars (space, .) can cause problems
  - user gets confirmation mail saying that the INBOX and optionally folders have been copied and email is received on mail and imap
  - user can send email to stop mail reception on mail
  - After at most 48 hours mail reception on mail is stopped finally
- then the mail client has to be reconfigured (see later)
- No further configuration changes required (e.g. registry) !

Move from mail to imap (2)

- after October 15:
    - user gets informed by email that his INBOX has been copied to imap and new email is received on mail and imap
    - user can send mail to stop mail reception on mail
    - After at most 48 hours mail reception on mail is stopped finally
- user has to reconfigure the mail client
    - detailed information on the following slides
- There is no change in the preferred address when sending mail: firstame.lastname@desy.de, the real address of the INBOX in the registry stays unchanged (account@mail.ifh.de)

Configuration of mail clients

- mail clients
  - alpine (successor of pine, text based)
  - thunderbird
  - mulberry (very powerful, MacOS look and feel, on Linux buggy)
  - others, e.g. evolution, outlook, ...
- configuration described on https://dvinfo.ifh.de/IMAPServer
- important parameters:
  - server name imap.ifh.de, protocol IMAP, port 143 (TLS), 993 (SSL)
  - mail directory on server: keep empty (or maybe ~)
  - correct installation of CA Certificates is crucial for proper functionality!

alpine

- in Zeuthen already preconfigured (server mail instead of imap)
- configuration change to use the new server
    - inbox-path={imap.ifh.de}inbox in .pinerc or
    - change Inbox Path in alpine (Setup -> Config Screen) or
    - export IMAPSERVER=imap.ifh.de in .zshenv (Zeuthen only) or
    - setenv IMAPSERVER imap.ifh.de in .cshrc (Zeuthen only)
- configure alpine to display additional folders on server
    - setup -> collectionLists -> add collection
        - arbitrary nickname, server Name: imap.ifh.de, remaining fields empty
        - in this collection the folder junk wil get displayed
        - new folders in this collection are visible on all mail clients talking IMAP

Reply address in alpine

- settings that are identical for all users are written to the global alpine configuration file
  - From: address is different for all users, the built in default will construct it from domain (ifh.de) and accountname. This should be changed !
  - only a problem of (al)pine, other mail readers will usually ask for the email address to be used in the From: header
- Even worse on computers not managed by DESY
  - default is a From: according to the template account@host.domain
  - at DESY this regularly causes reply mails to bounce
- therefore important: change From: in setup -> configure
  - recommended to modify as well: alt-addresses (Alternate Adresses)

alpine and Multimedia Attachments

- handled properly (graphics, URL display in browser, sound, ...)
  - requires correct MIME settings in alpine
- all attachments do have a MIME type
  - characterizes type of documents, e.g. Image/JPEG
  - mapping of an application to a MIME type in /etc/mailcap
    - example: image/*; gthumb %s
    - own rules in ~/.mailcap can enhance or replace global rules
    - example: postscript files:application/pdf; acroread %s
    - some programs put rules in ~/.mailcap on installation, please check!!!
  - generic type: Application/OCTET-STREAM
    - No rule does apply, last resort: assignment of apps to file extensions
  - mapping of file extensions to MIME type in /etc/mime.types
    - own rules in .mime.types can enhance or replace global rules

Thunderbird Certificates

- download required Certificate Authority (CA) Certificates
    - (see also https://dvinfo.ifh.de/IMAPServer#Thunderbird)
    - https://pki.pca.dfn.de/desy-ca/pub/cacert/g_rootcert.crt
    - https://pki.pca.dfn.de/desy-ca/pub/cacert/g_intermediatecacert.crt
    - https://pki.pca.dfn.de/desy-ca/pub/cacert/g_cacert.crt
- in the Edit menu: Preferences: Advanced: View Certificates (Windows: in the Tools menu under Options)
    - select the Authorities tab
    - import all three certificates and select the checkbox "use for email"
- configure other mail clients accordingly !!!

Thunderbird and Kerberos (Windows)

- configure Kerberos authentication
  - install Kerberos for Windows (kfW) http://web.mit.edu/Kerberos/dist/
  - start and configure the Network Identity Manager
    - realm IFH.DE, no Kerberos4 Ticket, DESY account name
  - request ticket (need to type your password)
- configure thunderbird for Kerberos (Tools menu)
  - use secure Authentication (Account settings: Server Settings)
  - switch off SSPI (Options: Advanced: General: Config Editor)
    - set auth.use-sspi to false
- test
  - ilf it works:
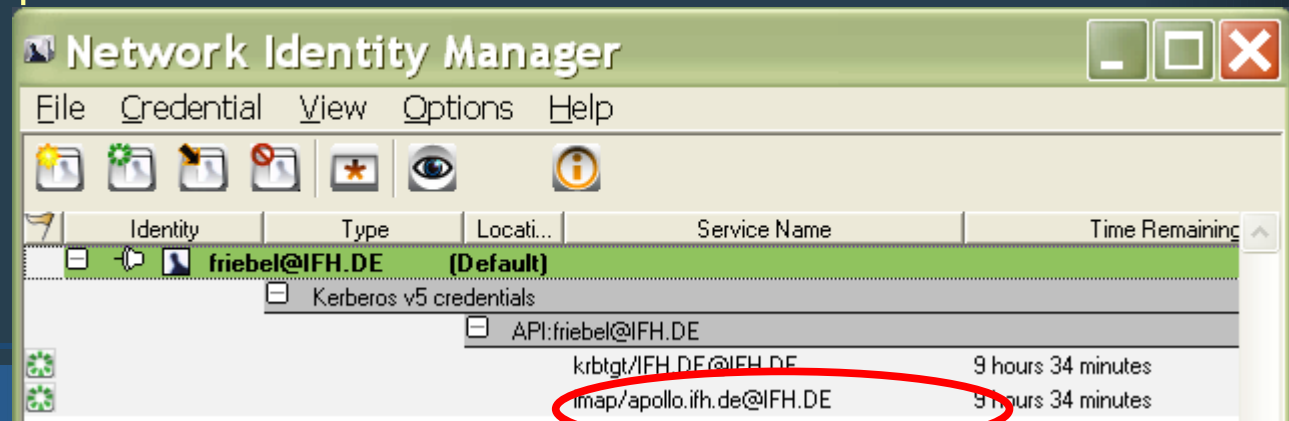
Name spaces

Information for experienced users

- are collection of rules how mails will be treated on server
  - storage format, access rights, visibility etc.
- default name space
  - currently storage of mails in Maildir++ format, 2010 in dbox format
- #mbox name space
  - hidden from users, storing of mails in mbox format
  - folders can get compressed, then read only
  - well suited for e.g. old sent-mail folders

Sending of email

- sending of email without restrictions only within DESY

- internal server is faster, no extra load by spammers

- DESY mail servers do only accept mail from
  - mail servers
  - arbitrary machines within DESY
  - authenticated users with DESY cccount (world wide)

- authentication against mail server only using TLS (or SSL)
  - by username/password (always working, but not very convenient)
  - By using Kerberos (recommended if offered by client, not Outlook)

- certificate chain has to be intact and complete
  - can be achieved by installing the certificates as described above

Mail filtering

- client side mail filtering
  - filter will be working with all mail servers, filtering at client start
  - needs to be configured separately for each mail client
- server side mail filtering
  - filter gets engaged when email is received
  - each mail client does see the same effects of the filter(s) on email
  - configuration depends on mail server used
  - procmail was used on mail, now on imap sieve has to be used
  - managesieve needs to be used to manipulate sieve scripts (usually built into the clients)

Mail filtering on server

- we have to use a non standard managesieve configuration
  - port 2009 instead of 2000, Host imap.ifh.de, TLS must be used
  - configuration currently only within DESY (port blocked from outside)
- several graphical interfaces available
  - thunderbird: sieve addon http://sieve.mozdev.org/ (script editing)
  - https://www-zeuthen.desy.de/dv-bin/imap/manage.pl (standalone)
  - https://imap.ifh.de/webmail (squirrelmail)
  - mulberry mail client comes with integrated interface (IMAP use ok)
- each interface with separate script management mechanisms
  - user has to select **a single** interface
  - Own script replaces global script (spam filter) unconditionally

Mailfilter GUI examples

DESY homepage [LOGOUT] [HELP]

[View/Edit Rules] [Add Rule] [Folders and ACL's] [Advanced Options]

Server:	Userid:	Used Quota: [128314 kB / 512000 kB (25.06%	Script:
imap.ifh.de	friebel@IFH.DE	usage)]	[default]

Save Changes   Refresh   Reset Values

New Rule Entry for user: friebel@IFH.DE

Rule#: [1] **Priority:** 2   **Status:** ENABLED

☐ **Continue checking other rules after applying this rule**
☐ **Keep a copy in your Inbox**
☐ **Use regular expressions**

IF all of ▼ **field(s):**   'from' contains
                                 'to' contains
                                 'subject' contains
                 Msg size less ▼ than   (K)ilobytes
              Field name   contains

THEN   ○ File Into   ▼ (Mail Folder)
                ○ Forward To
                ○ Reject

                                                          (Text Messa

                ○ Discard

Hint: Use * or ? for wildcards
To invert a rule use ! as the first character of your search string

Save Rule   Clear

Server-Side Mail Filtering - Editing Mail Filtering Rule #1

Condition

The condition for the following rules is: AND (Every item must match) ▼

- Header ▼ | From ▼ | contains ▼ | my_favorite_spammer
- Header ▼ | From ▼ | contains ▼ | other_spammer
- Header ▼ | X-Spam-Flag ▼ | contains ▼ | YES

Less...   More...

Action

Choose what to do when this rule triggers, from one of the following:

○ ✔ **Keep Message**
◉ 📤 **Move to Folder** – junk ▼

    Or specify a new folder: to be created under
    [None] ▼

○ 🔀 **Redirect**
○ ↩ **Reject**
○ ✖ **Discard**
○ 🏖 **Vacation**

Additional Actions

☐ 🔴 **STOP**
☐ ✉ **Notify**
☐ 📨 **Also keep copy in INBOX, marked as deleted.**
☐ 🔧 **Disable**

Apply Changes   Cancel

6. Okt.   techn. Semi

Spam tagging and filtering

- Global spam filter installed on imap
  - can be modified, replaced by own filter or get deactivated
  - default filter rule:

```
require "fileinto";
if header :contains "X-Spam-Level" "*****" {
    fileinto "junk";
}
```

- for spam filtering use X-Spam-Level, not Subject: header
  - also valid for client side filtering (german only, with pictures):
    - http://adweb.desy.de/~gut/SpamFilterOutlook2000.htm
    - http://dv-zeuthen.desy.de/services/mail/spamfiltereinstellungen_windows_xp/

Spam filtering using alpine

- use global filter rules

- or enhance default rule to move spam to /dev/null if score > 10

- use Indexcolor rules

  - e.g. "spam" rule: display a line in the index in grey, if score > 0

- select possible spam by entering ; r spam ↵

Frequently asked questions

- maximal allowed size of emails to send
  - all central DESY mail servers do accept up to 50MB mails
  - binary files < 30 MB only (get encoded, grow because of that)
  - accepted maximum size on many other machines 10MB
  - If an email exceeds the size limit, the sending user does get a bounce with the name of the complaining mail server, please read carefully
  - better option: put file in ~/public/www/<filename> and send URL http://www-zeuthen.desy.de/~<username>/<filename> by email
- what is my quota on the mail server
  - is shown in some mail clients (in Thunderbird above 75%)
  - on Linux computers in Zeuthen: check_inbox

Frequently asked questions (2)

- why obvious SPAM mails with a regular pattern are not tagged
  - our first aim is to minimize the amount of good emails in spam, not minimizing the number of spam emails in the INBOX
  - There is no adaption of spam rules to the patterns seen at DESY. This would cause extra work and could badly influence the scoring rules
  - Seemingly efficient rules will work only for a few weeks before spammers use new methods (example: spam als JPEG picture)
- I do get spam email with my address in the From: header
  - all sender and recipient addresses can easily be spoofed
  - only the address on the envelope has to be correct, envelope information is never displayed. The email seen corresponds to the content of an ordinary mail, info there can be different from envelope
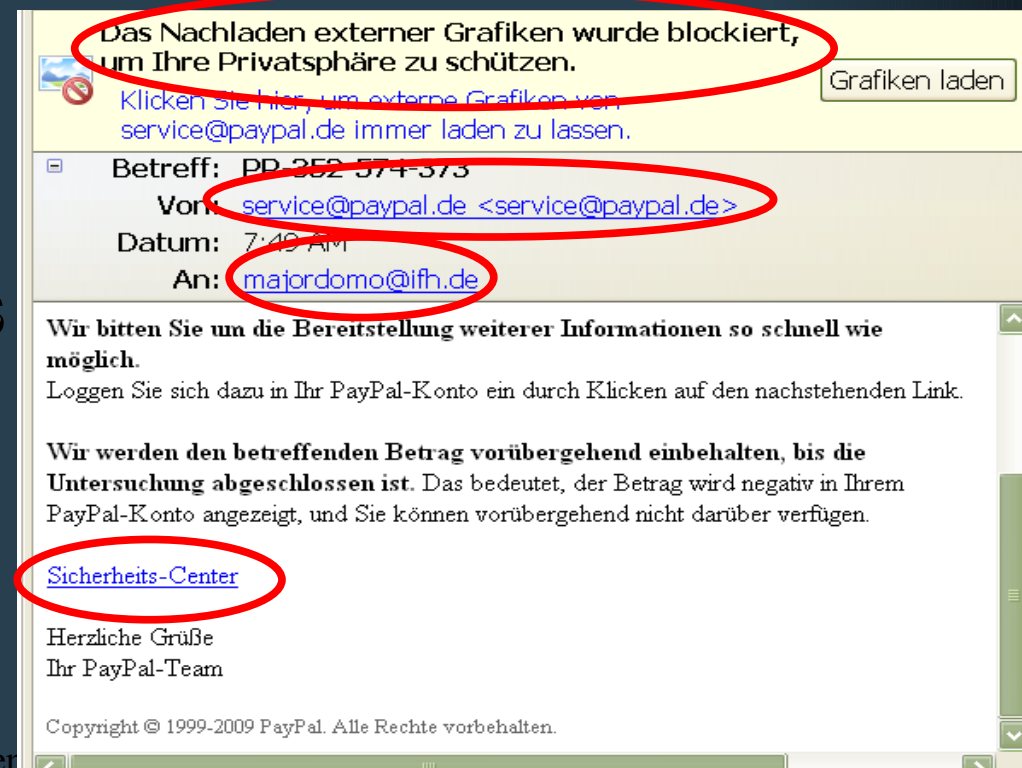
Frequently asked questions (3)

- **Is a given email spam?**
  - visible From: and To: header easily spoofable
  - download of pictures can yield information about your computer
  - Visible links (URLs) frequently point to spammer sites

- **inspecting all headers helps**

Received: from dhcp-077-211-218-116.chello.nl

(user-5433e1d5.lns6-c13.telh.dsl.pol.co.uk...)

- **carefully looking at URL's helps**

<A href=3D"htTP://www.paypal.com.de.cgi-bin.

webscr.cmd.GRiWgwheUnNOGoMgKIK=

OmyE.armartshop.com/...

Das Nachladen externer Grafiken wurde blockiert, um Ihre Privatsphäre zu schützen.

Klicken Sie hier, um externe Grafiken von service@paypal.de immer laden zu lassen.

Grafiken laden

Betreff: PP-352-574-373
Von: service@paypal.de <service@paypal.de>
Datum: 7:49 AM
An: majordomo@ifh.de

Wir bitten Sie um die Bereitstellung weiterer Informationen so schnell wie möglich.

Loggen Sie sich dazu in Ihr PayPal-Konto ein durch Klicken auf den nachstehenden Link.

Wir werden den betreffenden Betrag vorübergehend einbehalten, bis die Untersuchung abgeschlossen ist. Das bedeutet, der Betrag wird negativ in Ihrem PayPal-Konto angezeigt, und Sie können vorübergehend nicht darüber verfügen.

Sicherheits-Center

Herzliche Grüße
Ihr PayPal-Team

Copyright © 1999-2009 PayPal. Alle Rechte vorbehalten.

What is next?

- until end of October move of all Zeuthen INBOXes to imap
- spamassassin upgrade for improved spam tagging
  - new version 3.3 should be ready soon
- beginning 2010 new more efficient format for storing mail
  - important for backup, few large files instead of many small ones
  - gets implemented in dovecot 2.0
- improving documentation, optimizing the mail server and client configuration (feedback from users welcome)
- UNIX mail store in Hamburg (mail.desy.de) will be based on dovecot as well (currently in testing phase)

Useful links

- **DESY specific links**
    - **http://dv-zeuthen.desy.de/services/mail/** (general info)
    - **https://dvinfo.ifh.de/IMAPServer** (general info for IMAP server)
    - **https://dvinfo.ifh.de/MailReaderConfiguration** (mail configuration)
    - **https://dvinfo.ifh.de/MailFilter** (general info on mail filtering)
    - **https://imap.ifh.de/webmail** (squirrelmail for configuring own mail filter)
    - **https://www-zeuthen.desy.de/dv-bin/imap/manage.pl** (dito)
    - **https://pki.pca.dfn.de/desy-ca/pub/** (Certificates for DESY)
- **General links**
    - **http://wiki.dovecot.org/** (dovecot wiki)
    - **http://sieve.info/** (sieve filter resources)
    - **http://pigeonhole.dovecot.org/** (currently used sieve implementation)

Questions and comments ?

● dovecot

Webster:

Main Entry: dove·cote

Pronunciation: \'dəv-,kōt, -,kät\

Variant(s): also dove·cot \-,kät\

Function: noun

Date: 15th century

1 : a small compartmented raised house or box for domestic pigeons

2 : a settled or harmonious group or organization