UiO : Universitetet i Oslo

UHMX – en epostfiltertjeneste for sektoren

Presentasjon for førstelinjeforum
25. oktober 2017

marte.svalastoga@usit.uio.no

Plan for presentasjonen

- Intro til e-post
- UHMX
- Demonstrasjon av webgrensesnitt
- Spørsmål?

Hvor passer UHMX inn?

INTRO TIL E-POST

Gammel teknologi, tillitsbasert

- E-post er eldre enn internett
- SMTP RFC 5321 (bygger på RFC 821 fra 1982)
- Ulike systemer lover å ta ansvar for melding
- Mangler verifisering av avsender

Hva er en epostadresse?

marte.svalastoga@**usit.uio.no**

- Består av **localpart** + **domene**
- Domenet må slås opp i DNS for å finne ut hvor meldingen skal leveres

```
;; ANSWER SECTION:
usit.uio.no.            43200   IN      MX      10 smtp.uio.no.
```

Konvoluttadresser og fritekstadresser

```
Received: from mail-uhmx11.uio.no ([129.240.1.45])
        by mail-uhmx01.uio.no with smtp (Exim
4.82_1-5b7a7c0-XX)
        (envelope-from <svala@usit.uio.no>)
        id 1e6tFY-000BzG-1u
        for martesv@uia.no; Tue, 24 Oct 2017
09:05:13 +0200
From: Presidenten <trump@whitehouse.gov>
To: Marte <svalastoga@whitehouse.gov>
Date: Tue, 24 Oct 2017 09:04:00 +0100
Subject: Dette er en falsk melding
```

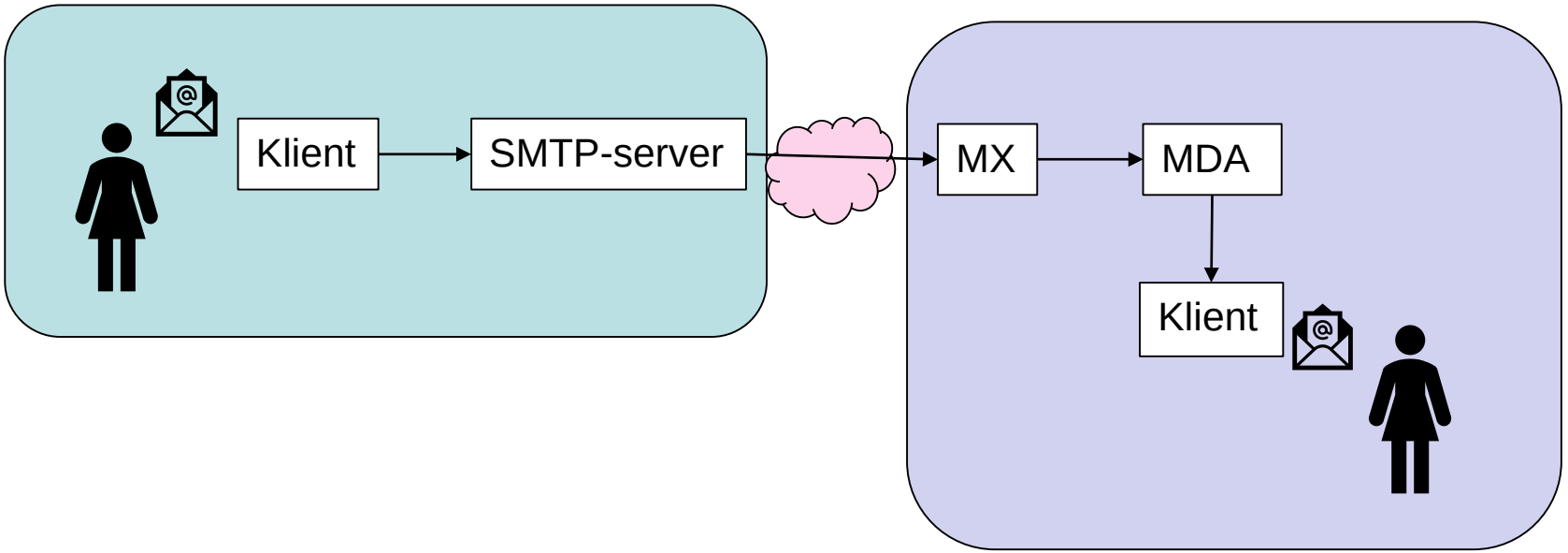
```
HELO mail-uhmx11.uio.no
250 mail-uhmx01.uio.no Hello mail-uhmx11.uio.no [129.240.1.45]
MAIL FROM:<svala@usit.uio.no>
250 OK
RCPT TO:<martesv@uia.no>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: "Presidenten" <trump@whitehouse.gov>
To: "Marte" <svalastoga@whitehouse.gov>
Date: Tue, 24 October 2017 09:04:00 +0100
Subject: Dette er en falsk melding

Jeg later som om jeg er USAs president, og sender deg e-post.

På forhånd takk
.
250 OK id=1e6tFY-000BzG-1u
QUIT
221 mail-uhmx01.uio.no closing connection
```

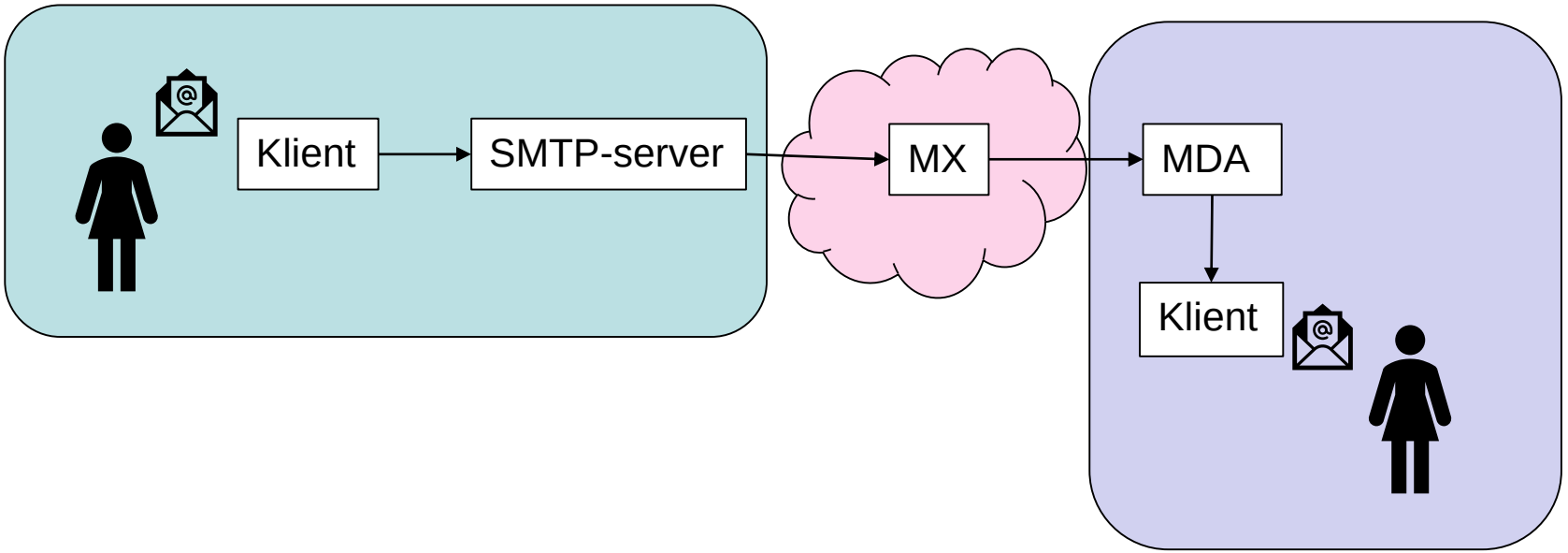
Hva er en MX

- Kort for Mail eXchanger
- Innkommende e-post – ikke utgående.



Hva er en MX

- Kort for Mail eXchanger
- Innkommende e-post – ikke utgående.



Typer uønsket e-post

- Spam
  - Lettere å definere for en bank enn for en forsknings- og utdanningsinstitusjon
- Malware / ransomware
  - Kryptovirus
- Phishing
  - Målrettet vs generell
- Spearphishing
  - Direktørsvindel

Hvordan stoppe uønsket e-post?

- Stadig vanskeligere, spam har utviklet seg
- Grålisting
- SPF og DKIM
- Regelsett fra internett tildeler poeng
- Svartelistetjenester

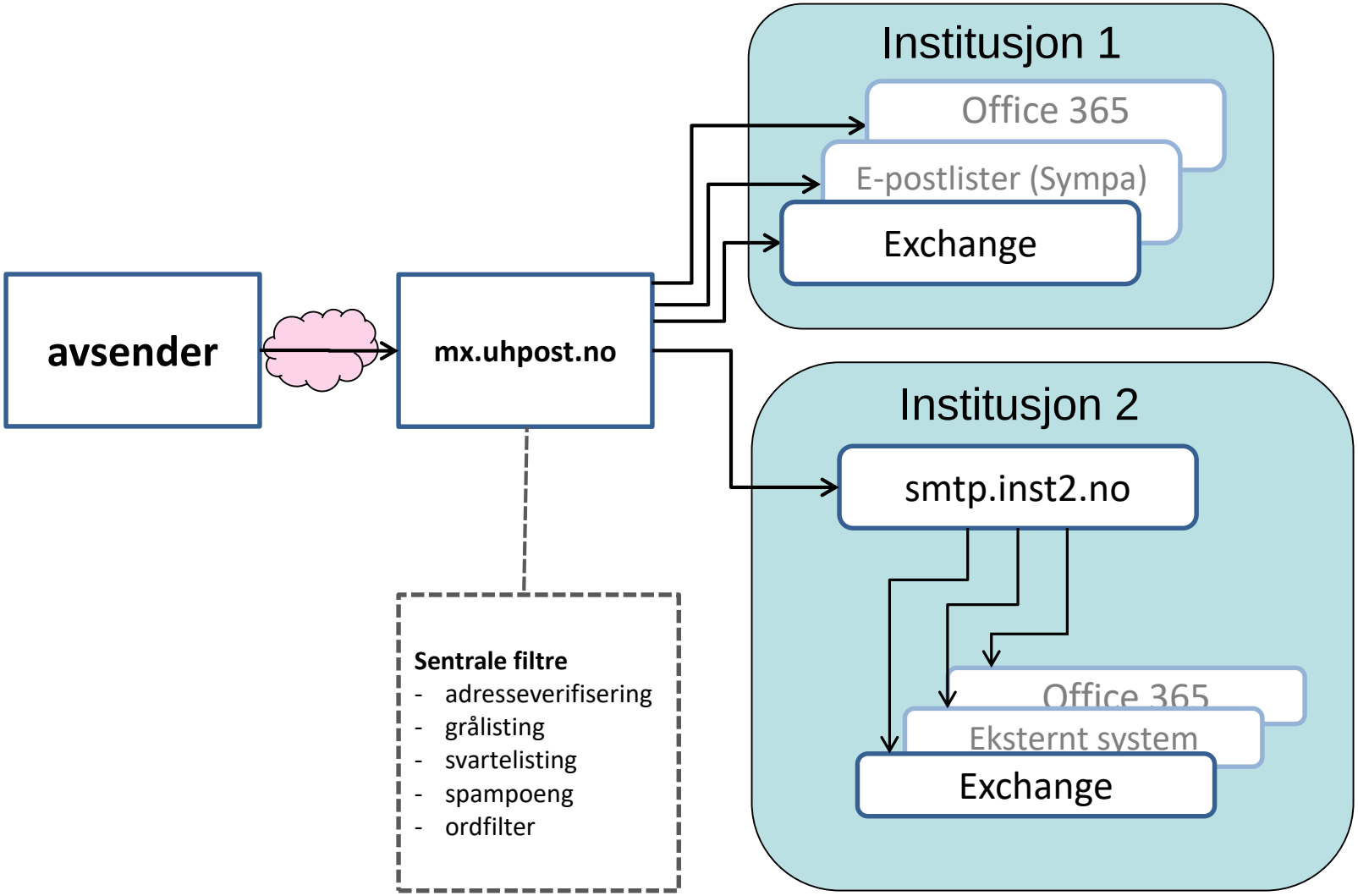
SPF og DKIM

- Sender Policy Framework – definerer hvilke maskiner som får sende fra hvilke domener
- Lar domeneeier indikere ønsket reaksjon

```
"v=spf1 ip4:129.240.10.0/25 -all"
```

- DomainKeys Identified Mail
- Lar avsendersystem signere deler av e-post, offentlig nøkkel i DNS

HVA ER UHMX?


Institusjon 1
Office 365
E-postlister (Sympa)
Exchange
avsender
mx.uhpost.no
Institusjon 2
smtp.inst2.no
Office 365
Eksternt system
Exchange
Sentrale filtre
- adresseverifisering
- grålisting
- svartelisting
- spampoeng
- ordfilter

Tanken bak UHMX

- Samarbeid for å redusere spam og phishing i UH-sektoren
- MX-tjeneste satt opp og driftet av oss
- Webgrensesnitt for kundene

Felles for alle

- Abonnerer på:
  - Regler for spamgjenkjenning
  - Kommersielle svartelister
  - Registre over kjente virussignaturer
  - Sperring av enkelte filtyper
- Svartelister på adresse- og domenenivå
- Egenutviklet ordfilter som tildeler spampoeng
- **Drar fordel av å være flere om jobben**

Styres per institusjon

- Egne utvidelser til svartelister og ordfilter
- Hvilke filtyper som skal sperres
- Grense for spam-markering av e-post
- Størrelsesbegrensning på mottak av e-post
- Adresseverifisering
- Hvor skal e-post leveres (smarthost / basere på LDAP-oppslag)

Hva skal til?

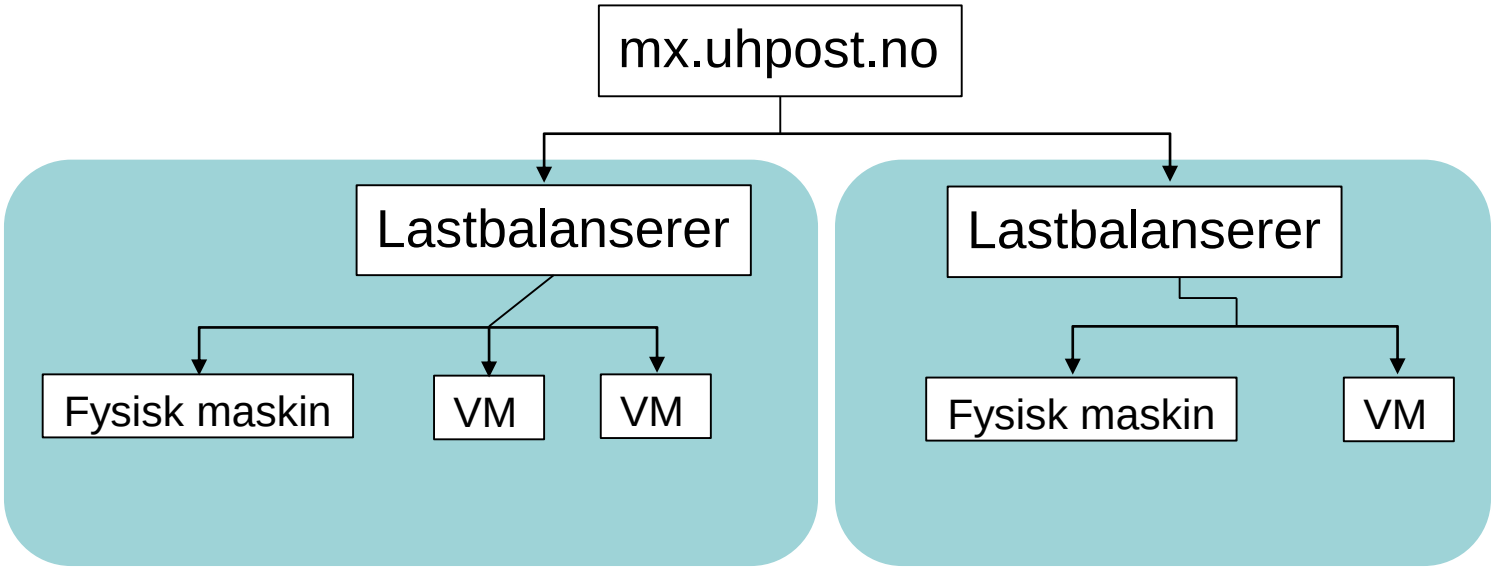
- Ta kontakt på uhmx-merkantilt@usit.no prisoverslag, bli kunde
- Sette MX-oppføring til mx.uhpost.no
  - Settes per domene, ikke alle må være i UHMX
- Tilgang til admingrensesnitt
- Gi oss LDAP-tilgang for adresseverifisering

Våre kunder i dag

- UiO
  - Ca 2.5M e-post levert per uke
- UiA
  - Pilot
  - Ca 230k e-post levert per uke
- AHO
  - Ca 17k e-post levert per uke
- NB
  - Ca 33k e-post levert per uke
- UNINETT - kun i test

Design

- mx.uhpost.no lastbalansert over to bygg
- Fem tjenere i bakkant
- Blanding av fysiske og virtuelle maskiner



Merkantil informasjon

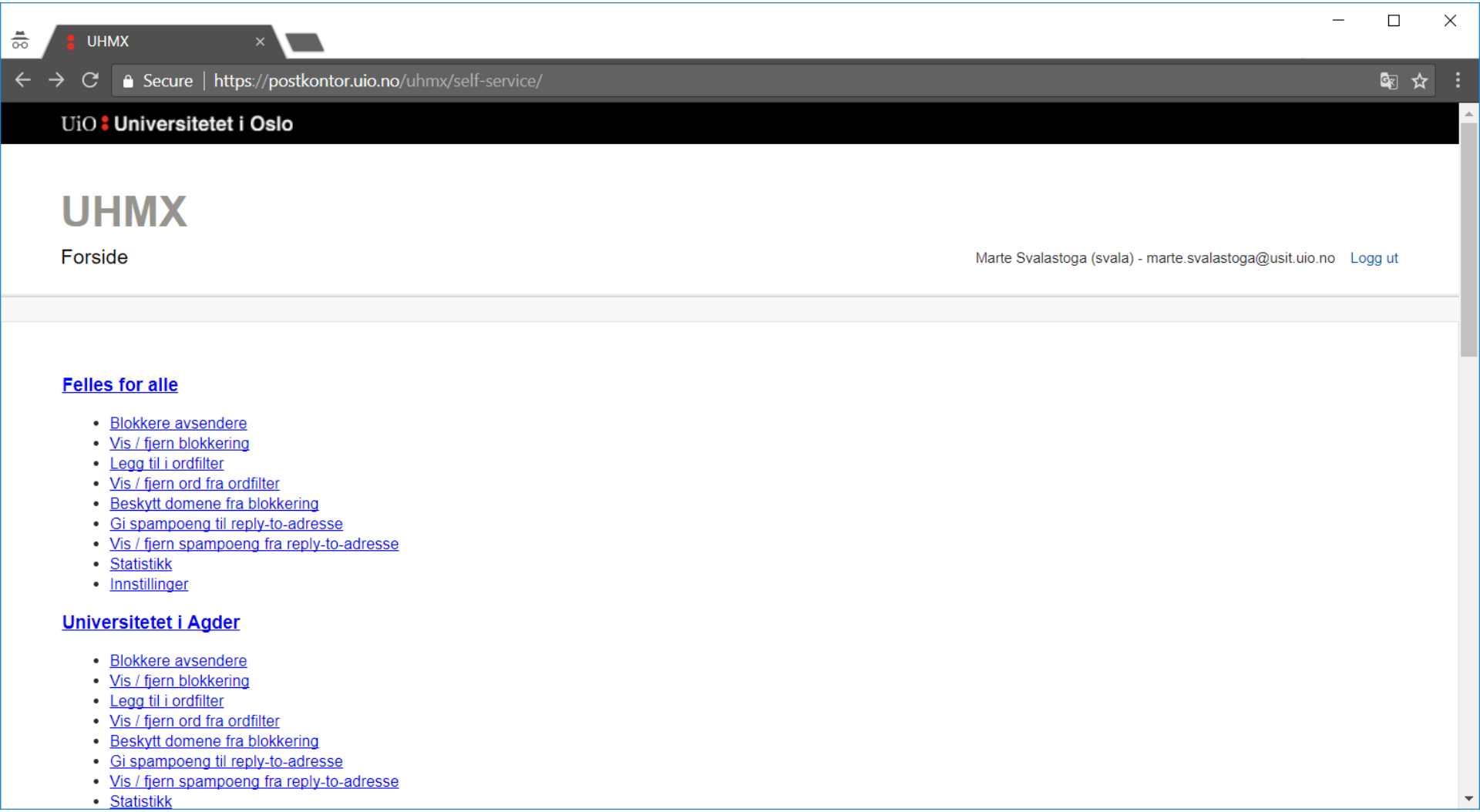
- Prismodell i dag basert på størrelse på institusjon – ta kontakt for estimat
- Tjenesten er forankret i BOTT og UH-sky
- Kanskje gjennom det nye forvaltningsorganet på sikt

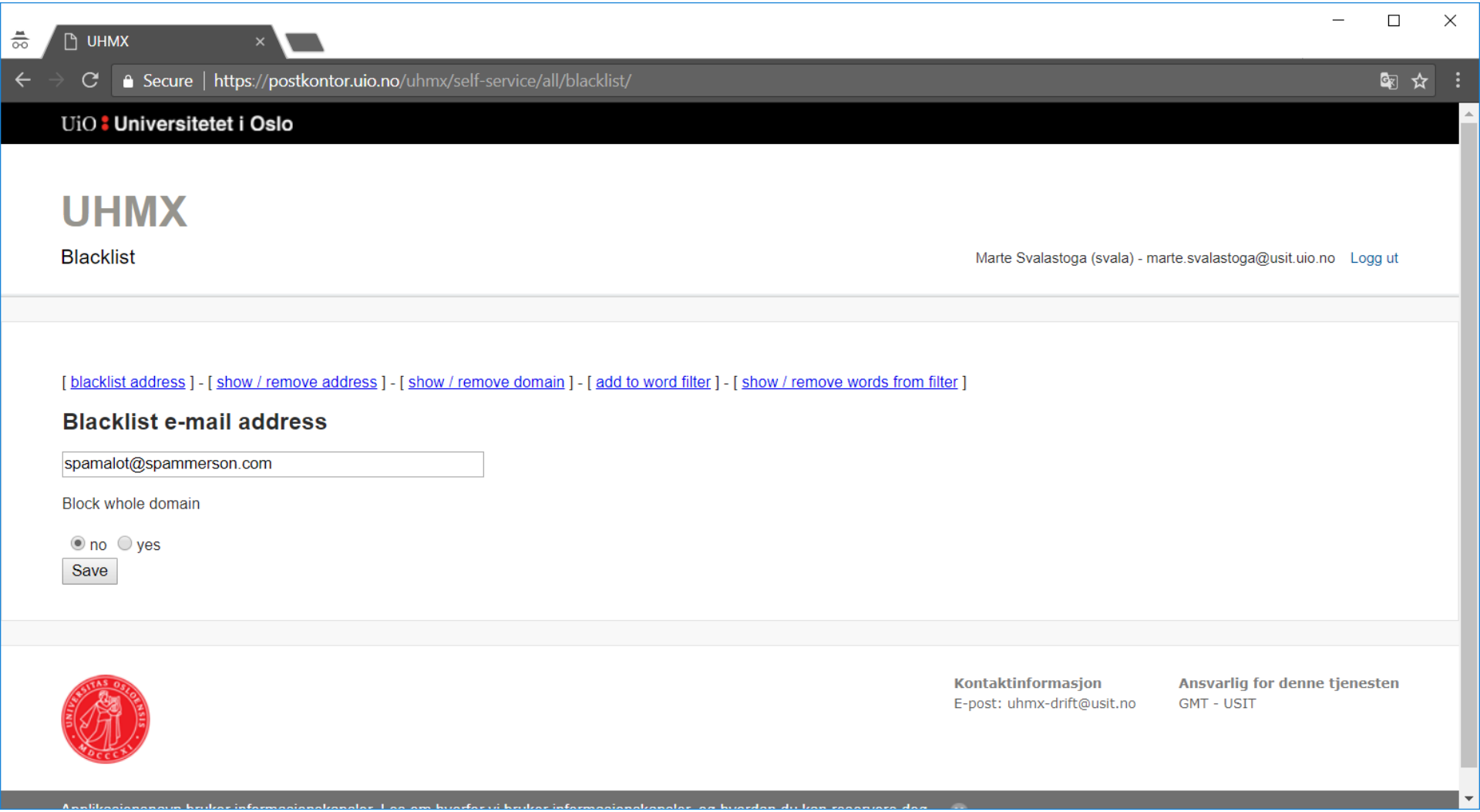
Sympa - epostlister

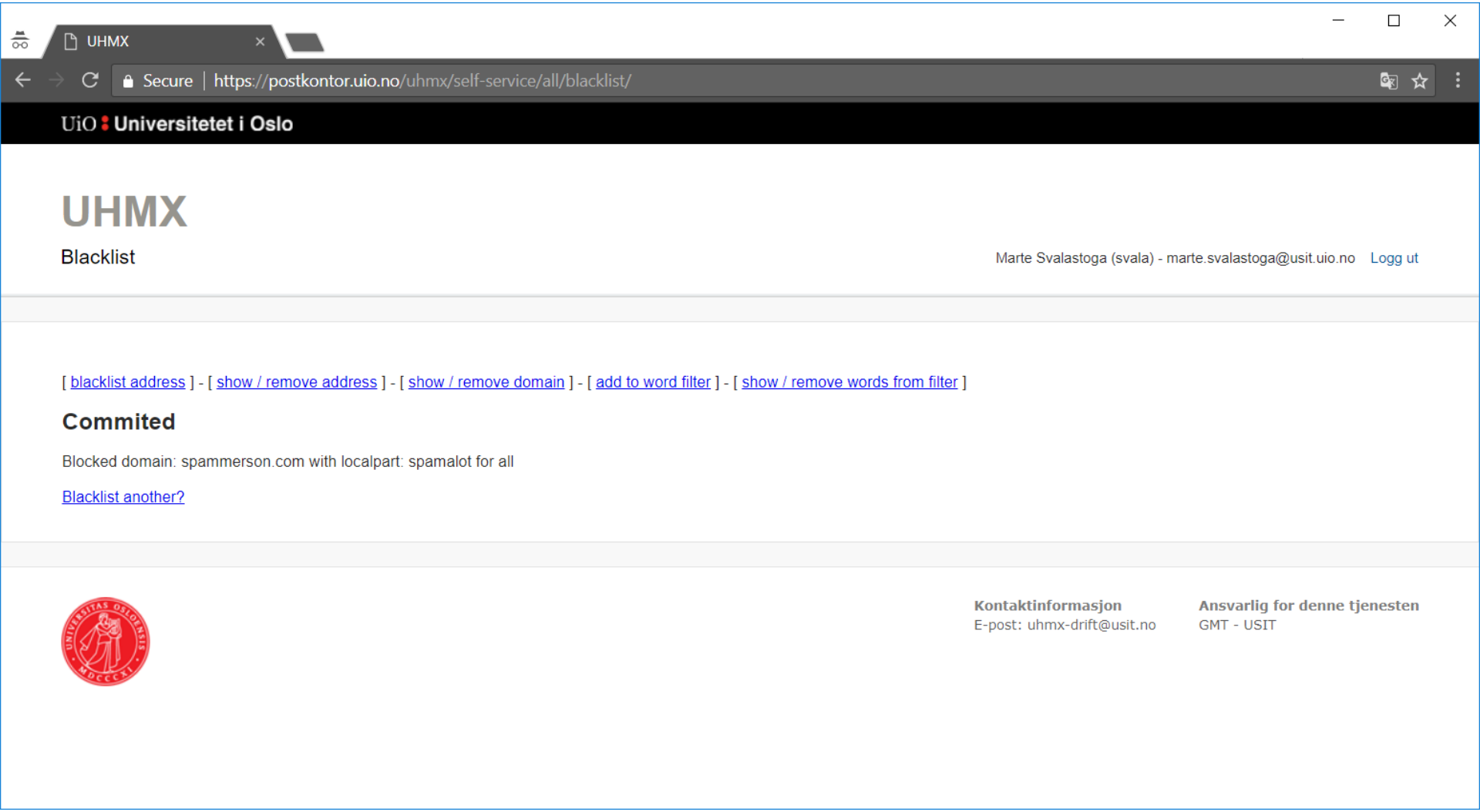
- Selges som tjeneste av USIT
- Open Source-prosjekt med lang historie
- Funksjonalitet:
  - Støtter **store** lister (700k+ medlemmer)
  - Automatisk synkronisering fra grupper
  - Arkivmuligheter

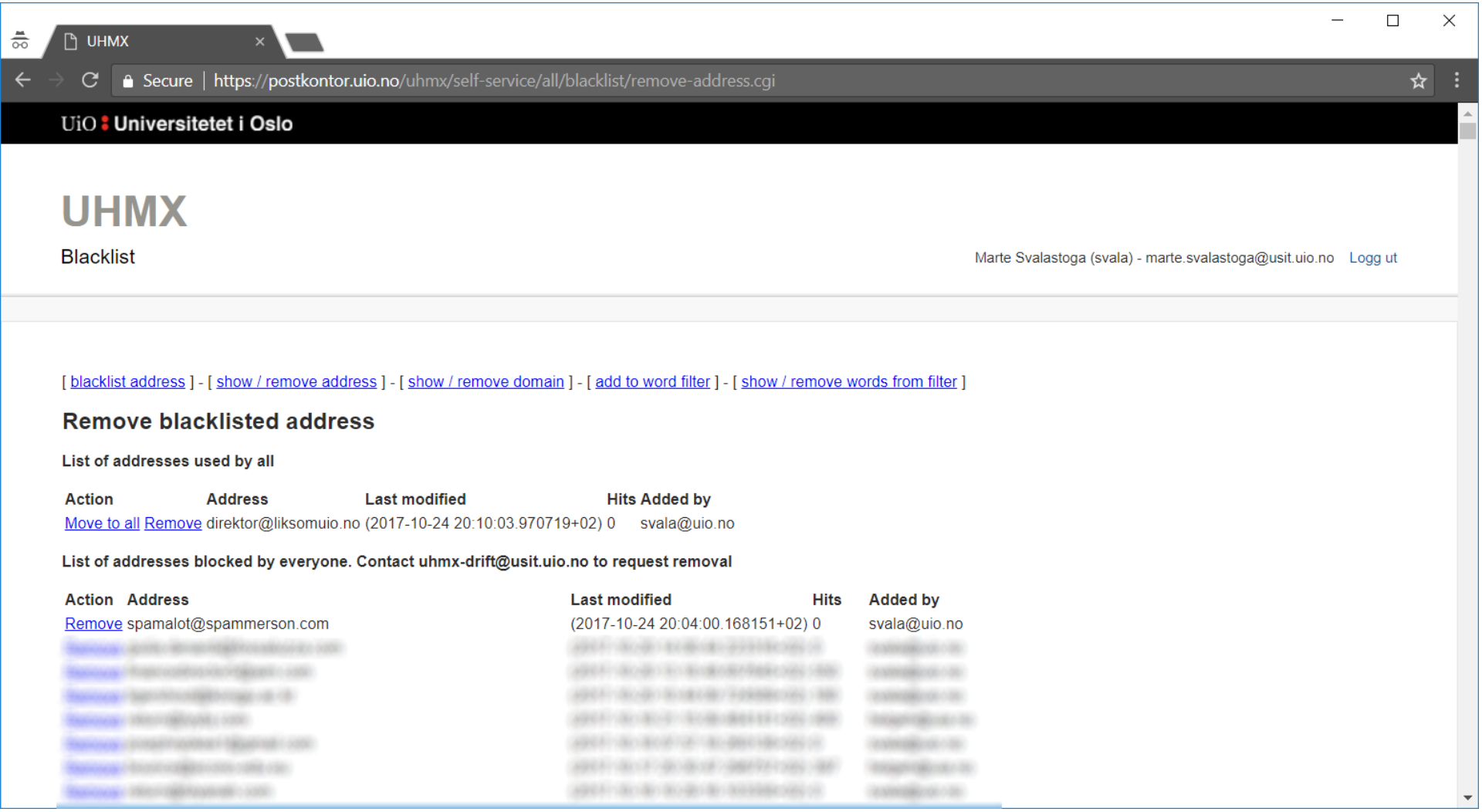
sympa-merkantilt@usit.uio.no

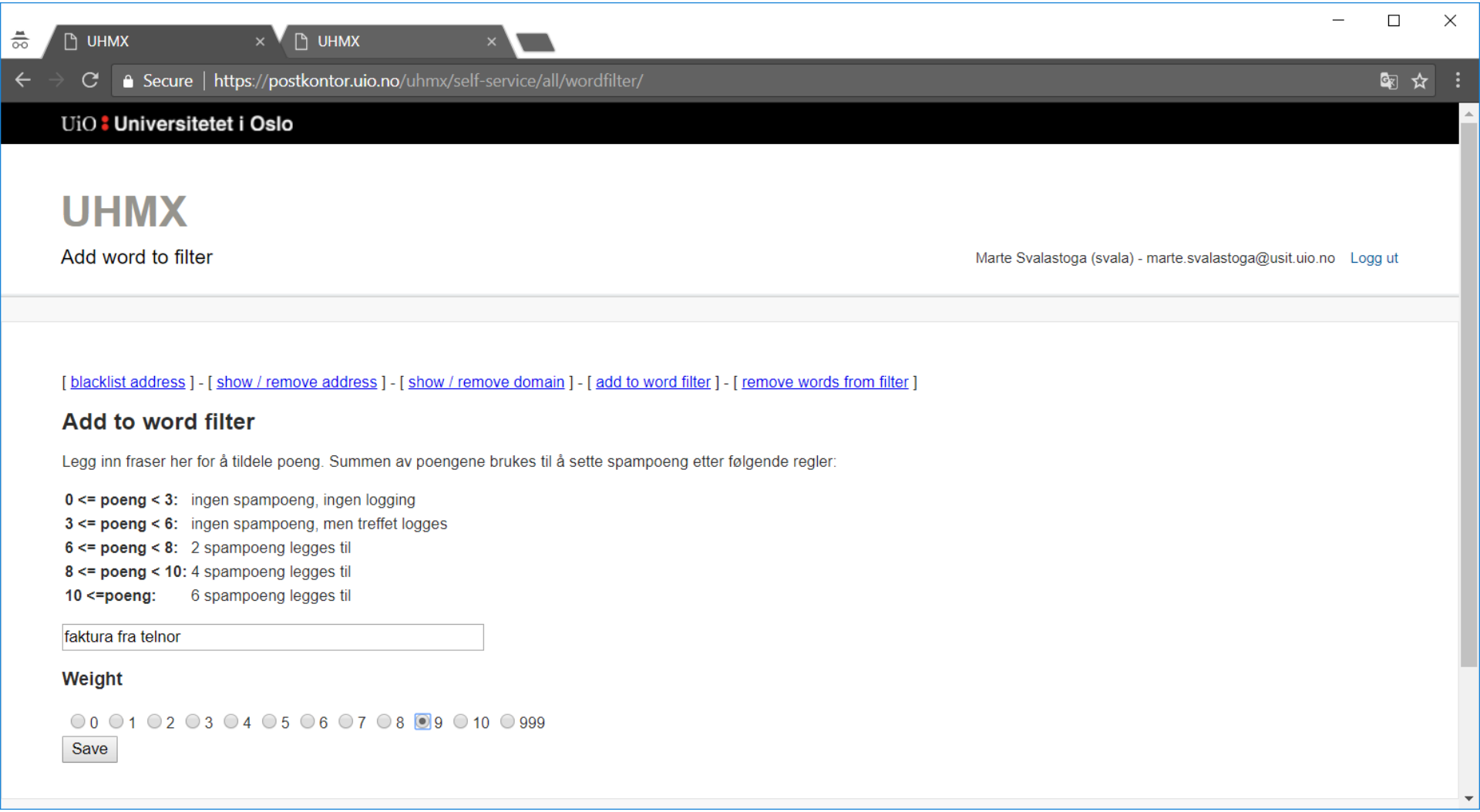
ADMINGRENSESNITT – DEMO


UHMX
Secure
https://postkontor.uio.no/uhmx/self-service/
UiO : Universitetet i Oslo
UHMX
Forside
Marte Svalastoga (svala) - marte.svalastoga@usit.uio.no
Logg ut
Felles for alle
Blokkere avsendere
Vis / fjern blokkering
Legg til i ordfilter
Vis / fjern ord fra ordfilter
Beskytt domene fra blokkering
Gi spampoeng til reply-to-adresse
Vis / fjern spampoeng fra reply-to-adresse
Statistikk
Innstillinger
Universitetet i Agder
Blokkere avsendere
Vis / fjern blokkering
Legg til i ordfilter
Vis / fjern ord fra ordfilter
Beskytt domene fra blokkering
Gi spampoeng til reply-to-adresse
Vis / fjern spampoeng fra reply-to-adresse
Statistikk


UHMX
Secure | https://postkontor.uio.no/uhmx/self-service/all/blacklist/
UiO : Universitetet i Oslo
UHMX
Blacklist
Marte Svalastoga (svala) - marte.svalastoga@usit.uio.no Logg ut
[blacklist address] - [show / remove address] - [show / remove domain] - [add to word filter] - [show / remove words from filter]
Blacklist e-mail address
spamalot@spammerson.com
Block whole domain
no yes
Save
Kontaktinformasjon
E-post: uhmx-drift@usit.no
Ansvarlig for denne tjenesten
GMT - USIT


UHMX
Secure | https://postkontor.uio.no/uhmx/self-service/all/blacklist/
UiO : Universitetet i Oslo
UHMX
Blacklist
Marte Svalastoga (svala) - marte.svalastoga@usit.uio.no Logg ut
[blacklist address] - [show / remove address] - [show / remove domain] - [add to word filter] - [show / remove words from filter]
Commited
Blocked domain: spammerson.com with localpart: spamalot for all
Blacklist another?
Kontaktinformasjon
E-post: uhmx-drift@usit.no
Ansvarlig for denne tjenesten
GMT - USIT


UHMX
Secure | https://postkontor.uio.no/uhmx/self-service/all/blacklist/remove-address.cgi
UiO : Universitetet i Oslo
UHMX
Blacklist
Marte Svalastoga (svala) - marte.svalastoga@usit.uio.no Logg ut
[blacklist address] - [show / remove address] - [show / remove domain] - [add to word filter] - [show / remove words from filter]
Remove blacklisted address
List of addresses used by all
Action Address Last modified Hits Added by
Move to all Remove direktor@liksomuio.no (2017-10-24 20:10:03.970719+02) 0 svala@uio.no
List of addresses blocked by everyone. Contact uhmx-drift@usit.uio.no to request removal
Action Address Last modified Hits Added by
Remove spamalot@spammerson.com (2017-10-24 20:04:00.168151+02) 0 svala@uio.no


UHMX
UHMX
Secure | https://postkontor.uio.no/uhmx/self-service/all/wordfilter/
UiO : Universitetet i Oslo
UHMX
Add word to filter
Marte Svalastoga (svala) - marte.svalastoga@usit.uio.no Logg ut
[blacklist address] - [show / remove address] - [show / remove domain] - [add to word filter] - [remove words from filter]
Add to word filter
Legg inn fraser her for å tildele poeng. Summen av poengene brukes til å sette spampoeng etter følgende regler:
0 <= poeng < 3: ingen spampoeng, ingen logging
3 <= poeng < 6: ingen spampoeng, men treffet logges
6 <= poeng < 8: 2 spampoeng legges til
8 <= poeng < 10: 4 spampoeng legges til
10 <=poeng: 6 spampoeng legges til
faktura fra telnor
Weight
0 1 2 3 4 5 6 7 8 9 10 999
Save

Spørsmål?

uhmx-merkantilt@usit.uio.no

Administrasjonsgrensesnitt

- Blokkere avsenderadresser/domener
- Ord/fraser legges til ordfilter
- Beskytt domene fra svartelisting
- Gi spampoeng til to/from/reply-to-adresse
- Vis statistikk for institusjon
- Endre innstillinger*

Software

- Exim
- DNSBL
  - Med utvidelse via webgrensesnitt
- ClamAV
  - Sanesecurity
  - Filtypeblokkering
- SpamAssassin
  - Med utvidelse via webgrensesnitt