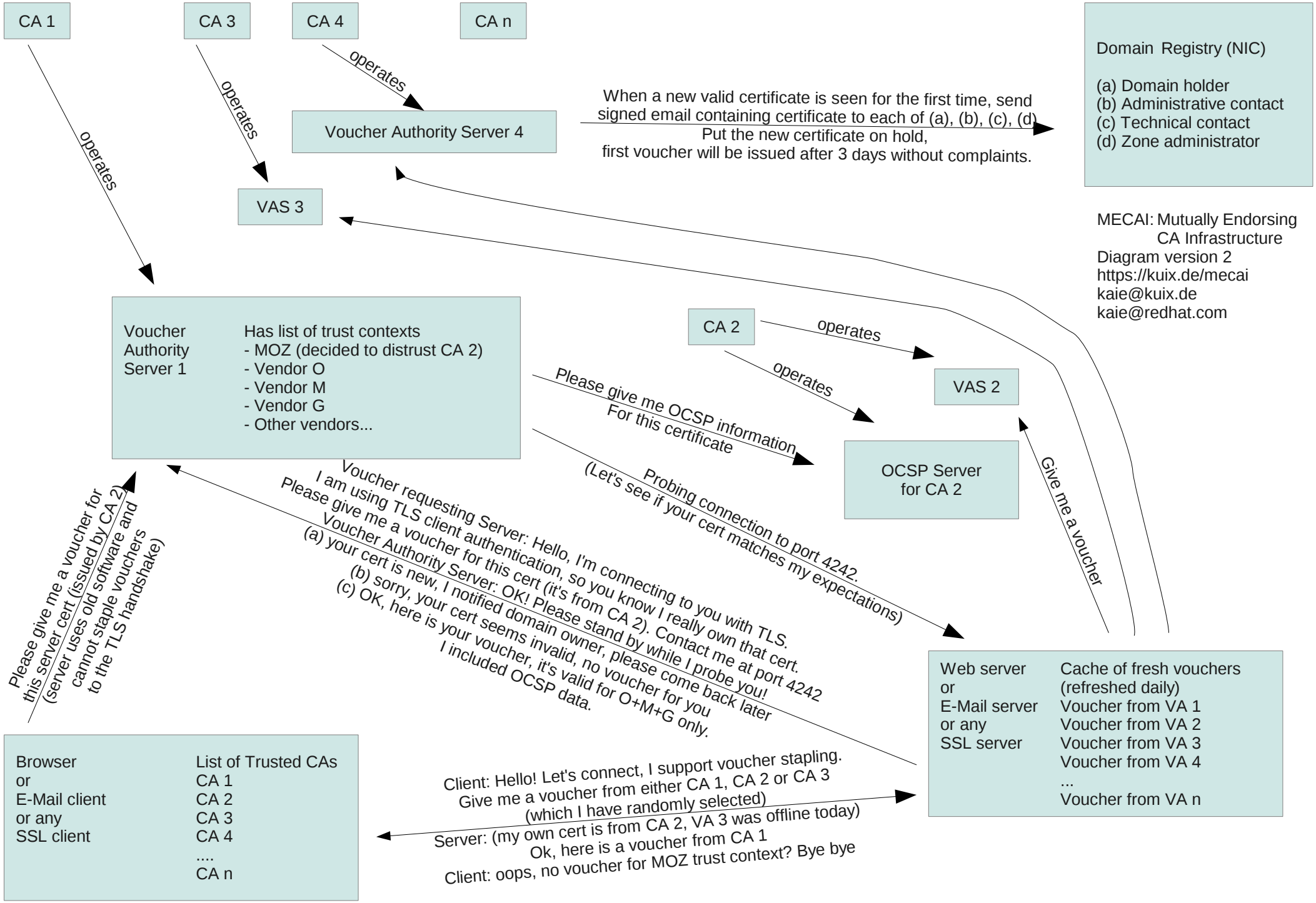
CA 1
CA 3
CA 4
CA n
operates
operates
operates
Voucher Authority Server 4
When a new valid certificate is seen for the first time, send signed email containing certificate to each of (a), (b), (c), (d)
Put the new certificate on hold,
first voucher will be issued after 3 days without complaints.
Domain Registry (NIC)
(a) Domain holder
(b) Administrative contact
(c) Technical contact
(d) Zone administrator
VAS 3
MECAI: Mutually Endorsing CA Infrastructure
Diagram version 2
https://kuix.de/mecai
kaie@kuix.de
kaie@redhat.com
Voucher Authority Server 1
Has list of trust contexts
- MOZ (decided to distrust CA 2)
- Vendor O
- Vendor M
- Vendor G
- Other vendors...
CA 2
operates
operates
VAS 2
Please give me OCSP information
For this certificate
OCSP Server for CA 2
Probing connection to port 4242.
(Let's see if your cert matches my expectations)
Give me a voucher
Voucher requesting Server: Hello, I'm connecting to you with TLS.
I am using TLS client authentication, so you know I really own that cert.
Please give me a voucher for this cert (it's from CA 2). Contact me at port 4242
Voucher Authority Server: OK! Please stand by while I probe you!
(a) your cert is new, I notified domain owner, please come back later
(b) sorry, your cert seems invalid, no voucher for you
(c) OK, here is your voucher, it's valid for O+M+G only.
I included OCSP data.
Please give me a voucher for this server cert (issued by CA 2)
(server uses old software and cannot staple vouchers to the TLS handshake)
Web server or E-Mail server or any SSL server
Cache of fresh vouchers (refreshed daily)
Voucher from VA 1
Voucher from VA 2
Voucher from VA 3
Voucher from VA 4
...
Voucher from VA n
Browser or E-Mail client or any SSL client
List of Trusted CAs
CA 1
CA 2
CA 3
CA 4
....
CA n
Client: Hello! Let's connect, I support voucher stapling.
Give me a voucher from either CA 1, CA 2 or CA 3
(which I have randomly selected)
Server: (my own cert is from CA 2, VA 3 was offline today)
Ok, here is a voucher from CA 1
Client: oops, no voucher for MOZ trust context? Bye bye