

SIP issues

Jan Růžička
CESNET
email,sip:janru@cesnet.cz

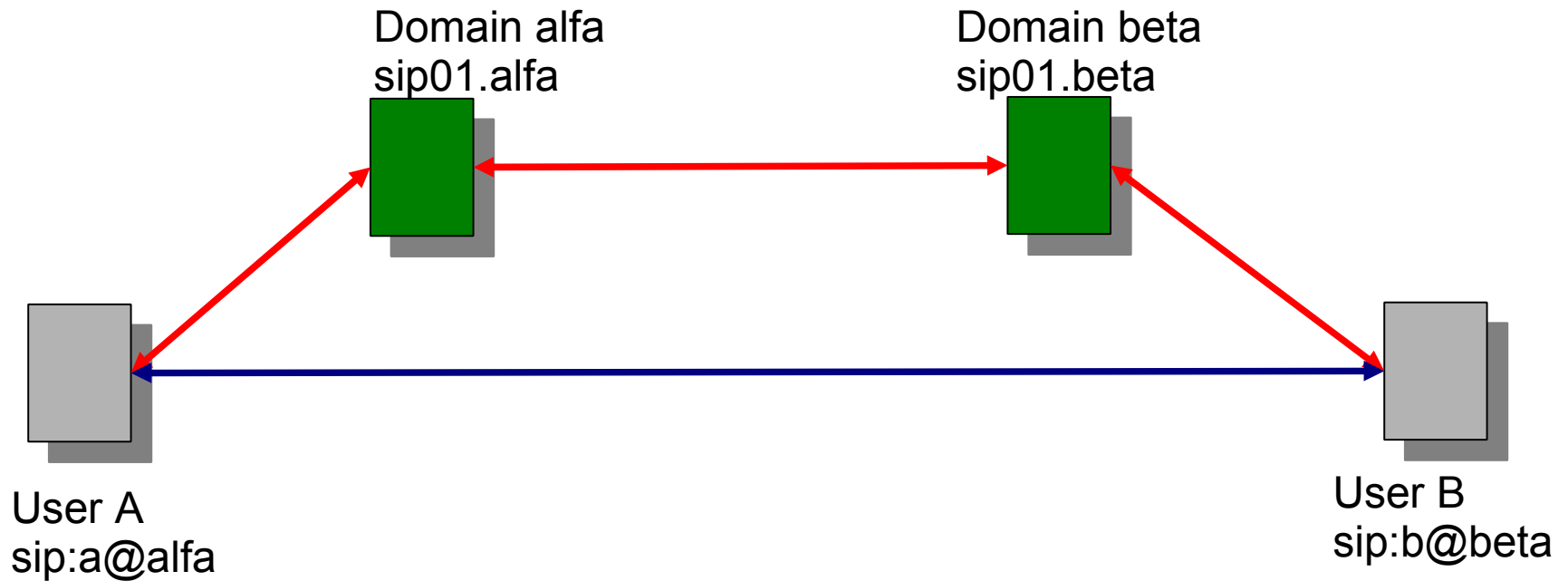
Architecture

- **User Agent**
- Server
 - registrar
 - redirect
 - **proxy**
 - stateless
 - statefull
- B2BUA
- Gateway (UA)
- MCU (UA)
- Outbound proxy
- ***SIP enabled firewall***
with NAT functionality – not transparent
- *SBC*
- *Services (click-to-dial, conf. Reservation and dial out)*

Border elements

- one point definition for peering ->
 - SBE signalling
 - DBE data
- Firewall piercing
- Topology hiding
- Defend IP PBX – more functions, less cpm

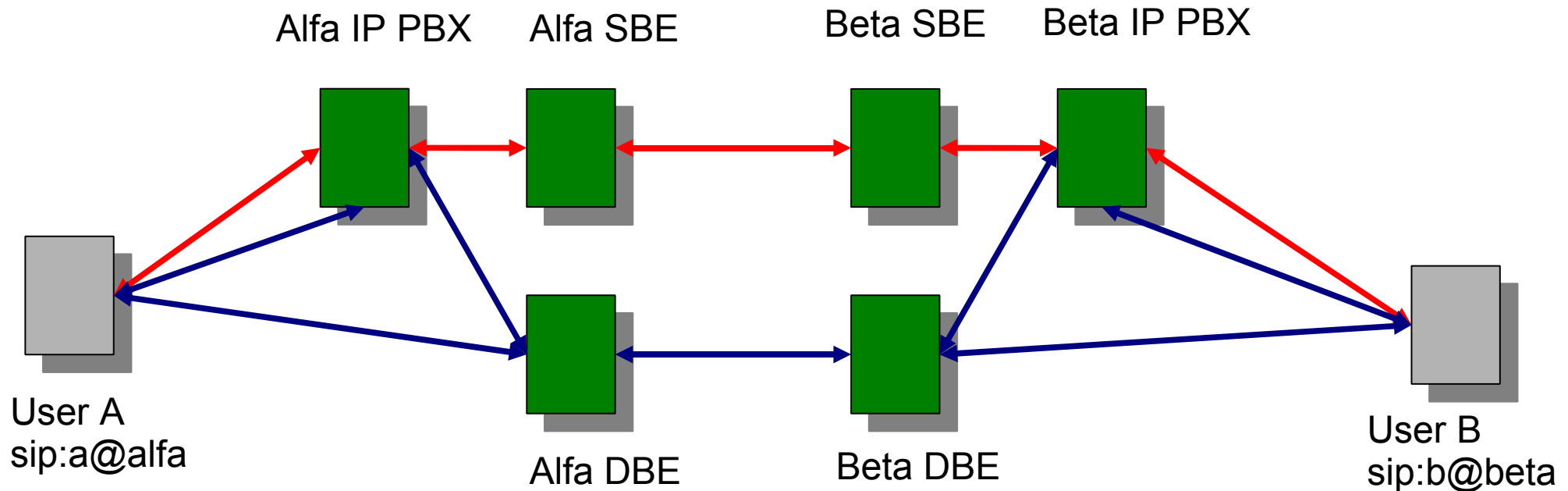
SIP „trapeziod“ direct peering



↔ DATA
↔ SIP

SIP „trapeziod“ II

firewalled sites and telco peers



Even more complicated if there is a „peering“ element or telco operator in between

Authentication II - local

- Vendor enhancements - closed
 - Microsoft Messenger- LCS – AD (NTLM)
- “OPEN” extensions to enhance authn
 - H.350 – LDAP schema with password and config. Client has to implement LDAP.
 - HTTP part – SSO
 - System wide (HTTP) Authentication client for i.e. browsers and sip clients
 - Directly in SIP?
 - Server side has to be enhanced too (amount of (vendors) clients vs servers)
 - Hardware clients are more difficult to extend - UI

Peer Authentication

Interdomain – opening of closed islands and interconnecting of them, anti-spit

- HTTP digest -weak and uncomfortable
- TLS
- assertions

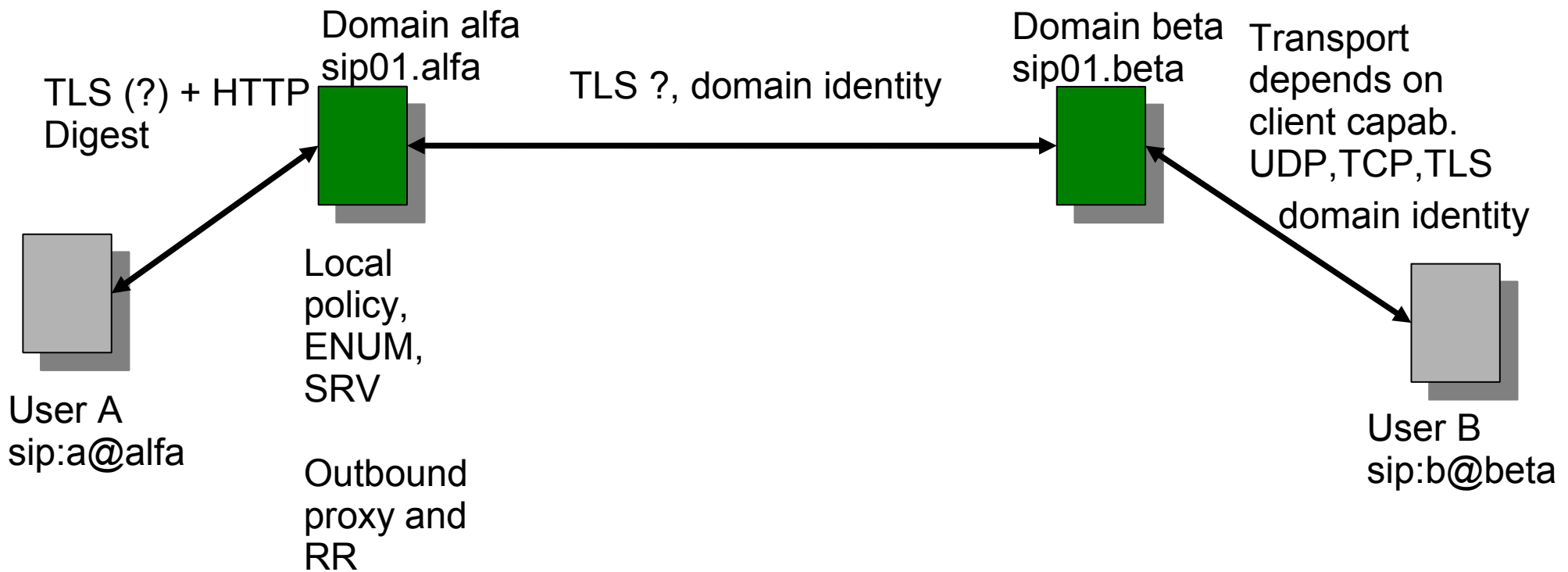
Peer Authentication II TLS

- Necessity
 - Hop-by-hop transitive trust
 - Express service in cert (also needed for sip identity)
 - Subjaltname: SIP domain in DNS or URI and id-kp-sipDomain EKU (draft-gurbani-sip-domain-certs-06)
 - RFC4985: SRVName _sip.domain (matching _sip.*.domain)
- Options
 - Trusted CA, set of CA (root issue in openssl)
 - Multiple TLS ports – Clients, Separate peers
 - NAPTR and SRV issue
 - Speermint NAPTR peering advertisement
 - Is TLS enough to do authz – need something in SIP

Peer Authentication III

- Identity assertions
 - signed headers SIP-identity RFC4474, only requests
 - SAML rich authz, XML over HTTP
 - Who should/can add identity
 - SignballingBE,DataBE issue
- SIP identity implementations
 - SER - initial version, problems with TLS module
 - OpenSER - master thesis work, untested, unofficial
 - repro – „untested“

SIP „trapeziod“ II



Handling trusted peers

- What to do with trusted or untrusted connections?
- change of ring tone - standardized? Alert-Info: tlsmelody, Alert-Info:<<http://mediaserver/tls.wav>>
- untrusted -> ?/dev/null? only during attack or outage
-

SIP identity RFC4474

INVITE sip:bob@biloxi.example.org SIP/2.0

Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8

To: Bob <sip:bob@biloxi.example.org>

From: Alice <sip:alice@atlanta.example.com>;tag=1928301774

Call-ID: a84b4c76e66710

CSeq: 314159 INVITE

Max-Forwards: 70

Date: Thu, 21 Feb 2002 13:02:03 GMT

Contact: <sip:alice@pc33.atlanta.example.com>

Content-Type: application/sdp

Content-Length: 147

v=0

o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com

s=Session SDP

c=IN IP4 pc33.atlanta.example.com

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

SIP identity II

- Interesting headers

```
sip:alice@atlanta.example.com|sip:bob@biloxi.example.org|
a84b4c76e66710|314159 INVITE|Thu, 21 Feb 2002 13:02:03 GMT|
alice@pc33.atlanta.example.com|v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
s=Session SDP
c=IN IP4 pc33.atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- Identity signature

```
Identity:"kjOP4YVZXmF0X3/4RUfAG6ffwbVQepNGRBz58b3dJq3prEV4h5Gn
S4F6udDRCI4/rSK9cl+TFv45nu0Qu2d/0WPP0vvc3JWwuUmHrCwG
wC+tW7fOWnC07QKgQn40uwg57WaXixQev5N0JfoLXnO3UDoum
89JRhXPAIp2vffJbD4="
Identity-Info: <https://atlanta.example.com/atlanta.cer>;alg=rsa-sha1
```