

Kamailio

Topology Hiding

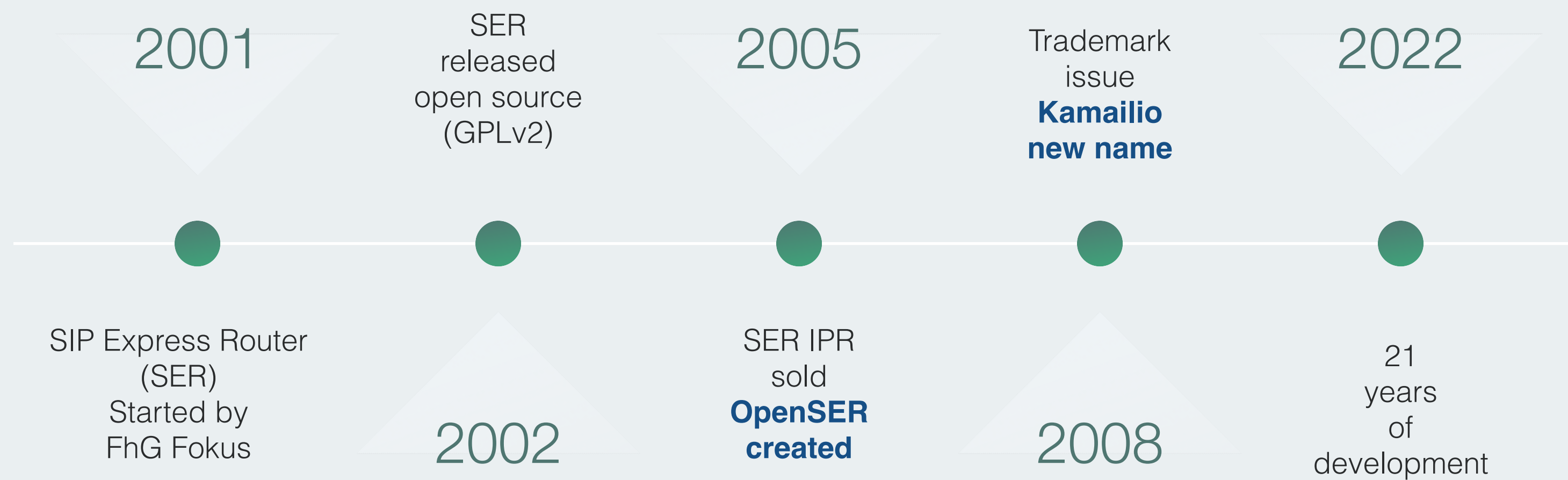
protect the network architecture

Daniel-Constantin Mierla  Co-Founder Kamailio Project  daniel@asipto.com



- ▶ Originally from Romania, living in Berlin, Germany
- ▶ Computer science software engineer - Polytechnics University Bucharest (2001)
- ▶ Researcher in RTC at Fraunhofer Fokus Institute, Berlin, Germany (2002-2005)
- ▶ Co-founder, main coordinator and lead developer of Kamailio, an open source SIP Server
- ▶ Professional consultancy for SIP, VoIP, Kamailio and all RTC at asipto.com
- ▶ Involved in open source real time communications since 2002
- ▶ Working with open standard protocols, mainly from IETF, GSMA/3GPP/ITU
- ▶ C software developer - mainly VoIP server side infrastructure
- ▶ Co-organizer of Kamailio World Conference, FOSDEM RTC DevRoom
- ▶ Speaking and promoting OSS RTC at world wide events





nowadays

- over 50 yearly active developers
- used by large rtc companies (millions of subscribers, billions of minutes per month)
-



www.kamailio.org
@kamailio

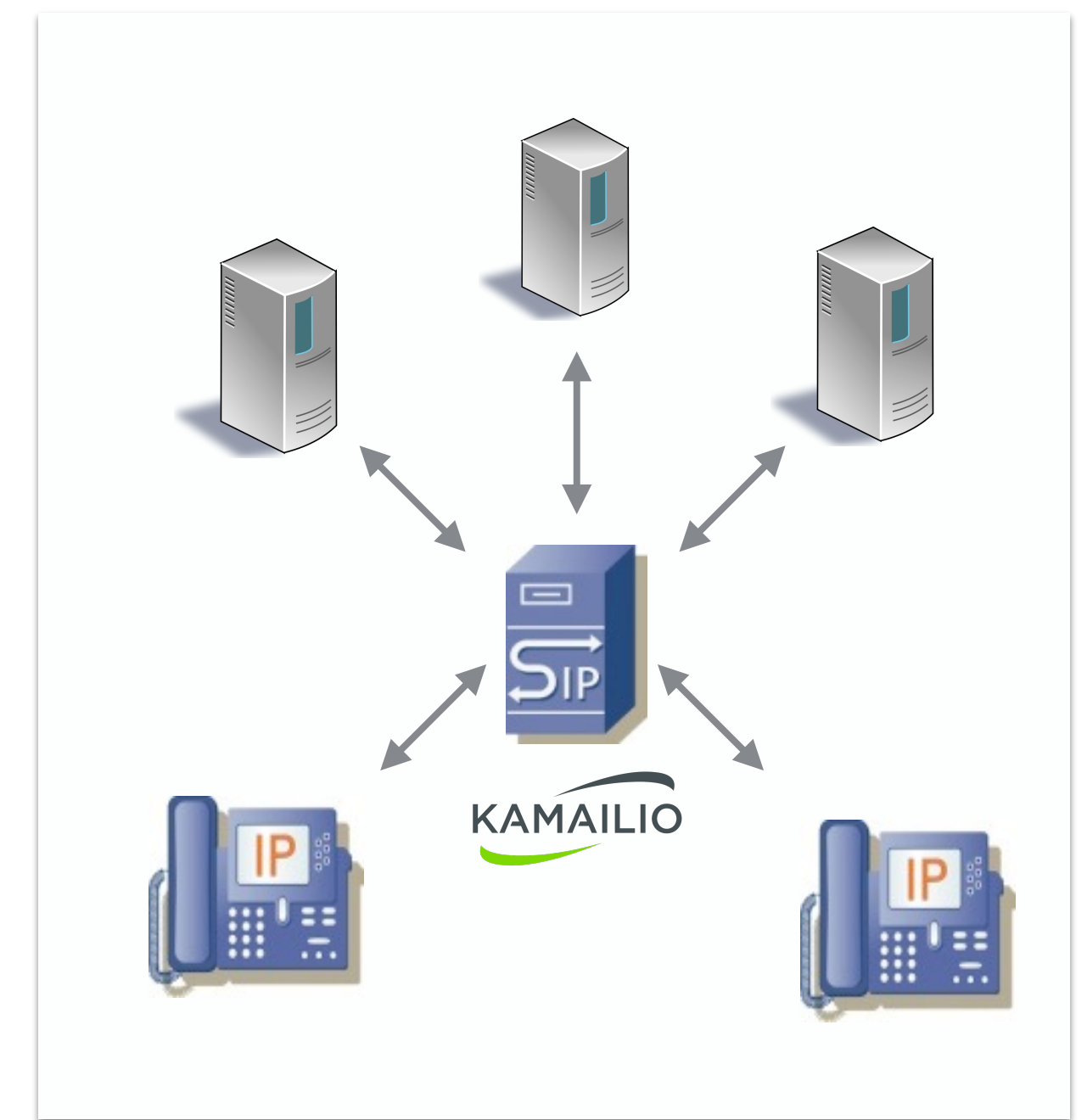


www.kamailioworld.com
@kamailioworld

KAMAILIO SIP SERVER IN ONE SLIDE



- * Open Source SIP (IETF RFC3261) Signaling Server implementation, developed since 2001
- * Can be used for VoIP (Voice, Video, VoLTE/IMS, SIP-I/SIP-T), Instant Messaging, Presence, WebRTC, IoT, Diameter, SQL and NoSQL backends, load balancing, least cost routing, security, ...
- * Designed for modularity, flexibility and scalability
 - * used by large telecoms, mobile operators and OTT services world wide
 - * thousands of call setups per second,
 - * hundred thousands of connected phones per instance
- * IPv6/IPv4 - UDP/TCP/TLS/SCTP/WebSocket - asynchronous routing
- * Classic SIP - WebRTC gateway using Kamailio + RTPEngine
- * Embedded interpreters: Lua, Python, JavaScript, Ruby, Squirrel, Perl, .Net, Java
- * About 250 modules (extensions) - <https://www.kamailio.org/docs/modules/stable/>
- * Over 80 active developers each year
- * Runs its own conference - Kamailio World
 - * in Berlin, Germany: <https://www.kamailioworld.com>





<https://www.kamailio.org/w/kamailio-v5-6-0-release-notes/>

<https://www.kamailio.org/w/kamailio-v5-5-0-release-notes/>

* jwt

* STIR/SHAKEN

* nats

* websocket client

* ruxc - http client

* posops

* sworker - siprepo

* slack

wait no longer

Kamailio is now available at half price





SIP Proxy Router

configuration file

KAMAILIO CONFIGURATION FILE STRUCTURE

- * **Three major parts**

- * **Global parameters**

- * Application parameters — ex: debug level, sockets, tcp tunings, worker processes, ...
 - * Custom (script specific) parameters — ex: groupid.name

- * **Modules settings**

- * Loading modules and modules parameters

- * **Routing blocks**

- * Rules for routing SIP traffic
 - * Blocks for handling requests, responses, branches, failures, ...

- * **The routing blocks**

- * Similar concept with functions/procedures
 - * Predefined identifiers: request_route, route, branch_route, failure_route, onreply_route, event_route, ...
 - * Contain actions: statements, conditions, loops
 - * Basic arithmetic and string operations
 - * Good support for regular expressions from core and modules
 - * Script variables with scope per process (private), global (shared), transaction or dialog

```
# global settings
#!define FLT_ACC 1
debug=3
fork=no
listen=192.168.1.34:5060
...
pstn.gw = 1.2.3.4" desc "pstn gateway ip"
...
```

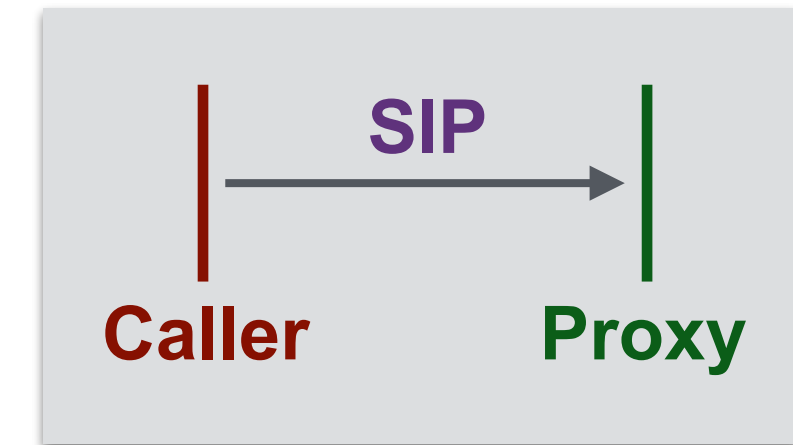
```
# module settings
mpath="/usr/local/lib/kamailio/modules/"
loadmodule="tm.so"
...
modparam("tm", "fr_inv_timer", 30000)
.....
```

```
# routing blocks
request_route {
    xlog("request received from $si\n");
    if($si=="10.1.2.10") {
        route(REDIRECT);
    } else {
        $rd = "10.1.2.5";
    }
    t_on_reply("LOGRPL");
    t_relay();
}
route[REDIRECT] {
    $rd = "10.1.2.3";
    send_reply("302", "Redirected");
    exit;
}
onreply_route[LOGRPL] {
    xlog("response received from $si\n");
}
...
```


SIP PROXY ROUTER - RECEIVED INVITE

INVITE sip:1002@asipto.lab;user=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.178.62:1024;branch=z9hG4bK-ampxo9rfducs;rport
From: "1001" <sip:1001@asipto.lab>;tag=6ehxxq7ebj
To: <sip:1002@asipto.lab;user=phone>
Call-ID: 313534373435383130393132333431-3xurg8bzzlop
CSeq: 1 INVITE
Max-Forwards: 70
User-Agent: snom370/8.7.5.35
Contact: <sip:1001@192.168.178.62:1024;line=vuw36p4a>;reg-id=1
X-Serialnumber: 0004132672E3
P-Key-Flags: resolution="31x13", keys="4"
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO, UPDATE
Allow-Events: talk, hold, refer, call-info
Supported: timer, replaces, from-change
Session-Expires: 3600
Min-SE: 90
Content-Type: application/sdp
Content-Length: 405

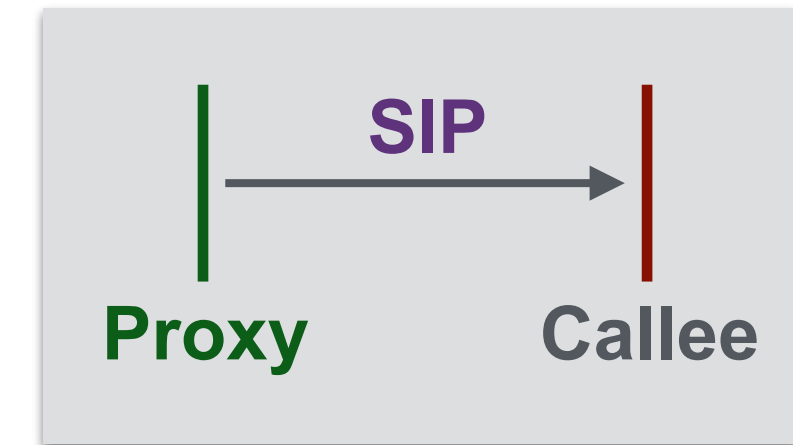
v=0
o=root 904410018 904410018 IN IP4 192.168.178.62
s=call
c=IN IP4 192.168.178.62
t=0 0
m=audio 62556 RTP/AVP 9 0 8 3 99 112 18 101
a=rtpmap:9 G722/8000
...



SIP PROXY ROUTER - FORWARDED INVITE

INVITE sip:1002@192.168.178.79:5061 SIP/2.0
Record-Route: <sip:192.168.178.75;lr>
Via: SIP/2.0/UDP 192.168.178.75;branch=z9hG4bK413a.b38be0298e62d68af96ff08fe8acf7ec.0
Via: SIP/2.0/UDP 192.168.178.62:1024;received=192.168.178.62;branch=z9hG4bK-ampxo9rfducs;rport=1024
From: "1001" <sip:1001@asipto.lab>;tag=6ehxxq7ebj
To: <sip:1002@asipto.lab;user=phone>
Call-ID: 313534373435383130393132333431-3xurg8bzzlop
CSeq: 1 INVITE
Max-Forwards: 69
User-Agent: snom370/8.7.5.35
Contact: <sip:1001@192.168.178.62:1024;line=vuw36p4a>;reg-id=1
X-Serialnumber: 0004132672E3
P-Key-Flags: resolution="31x13", keys="4"
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO, UPDATE
Allow-Events: talk, hold, refer, call-info
Supported: timer, replaces, from-change
Session-Expires: 3600
Min-SE: 90
Content-Type: application/sdp
Content-Length: 405

v=0
o=root 904410018 904410018 IN IP4 192.168.178.62
s=call
c=IN IP4 192.168.178.62
t=0 0
m=audio 62556 RTP/AVP 9 0 8 3 99 112 18 101
a=rtpmap:9 G722/8000
...





Topology Hiding

masking headers

topoh module

TOPOH MODULE

□ module: topoh

□ goals

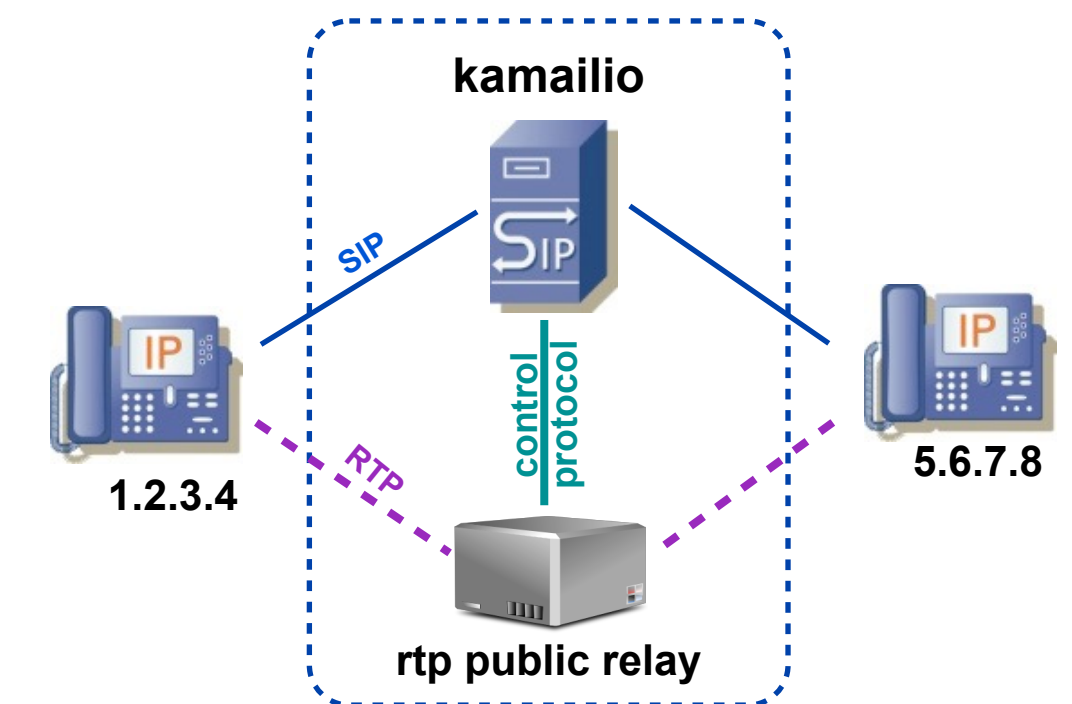
- hide sensitive IP addresses
 - contact header
 - Via stack
 - Record-Route and Route stacks

□ design

- stateless processing
 - no track of transactions or dialogs
- distributed processing
 - encoding/decoding can be done by different servers
- transparent processing
 - config writer should not care about topology hiding
 - everything is in clear while config processing
- event routes to control topology masking
 - skip it based on various conditions

- secret key to encode/decode
- encoded fields are SIP grammar valid
- encoding IP and prefixes can be set via parameters
- survive restarts
- no functions to be called in config file
 - everything is done automatically
 - hooks in core after receiving and before sending
 - just load the module and adjust parameters

- *use it with a media relay to hide the source of media traffic*

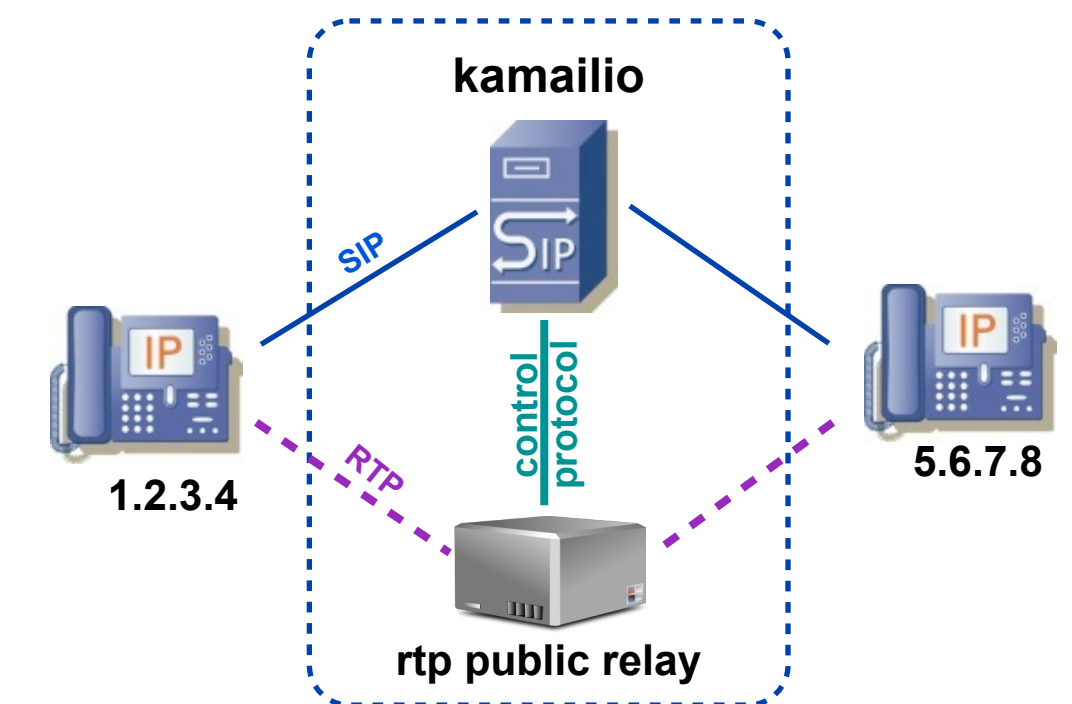


TOPOH MODULE

```
...
loadmodule "topoh.so"
...
# ----- topoh params -----
modparam("topoh", "mask_key", "my secret here")
modparam("topoh", "mask_ip", "10.1.1.10")
...
```

```
event_route[topoh:msg-outgoing] {
    if($sndto(ip)== "10.1.1.10") {
        drop;
    }
}
```

```
event_route[topoh:msg-sending] {
    if(is_request() && $tU=="bob") {
        drop;
    }
}
```



TOPOH MODULE

server.com == 192.168.178.10
alice == 192.168.178.27
bob == 192.168.178.22

U 192.168.178.27:40416 -> 192.168.178.10:5060

INVITE sip:bob@server.com SIP/2.0.

Via: SIP/2.0/UDP 192.168.178.27:40416;branch=z9hG4bK321149767.

From: "alice" <sip:alice@server.com>;tag=166646806.

To: <sip:bob@server.com>.

Call-ID: 989804978-40416-6@BJC.BGI.BHI.CH.

CSeq: 50 INVITE.

Contact: "alice" <sip:alice@192.168.178.27:40416>.

Max-Forwards: 70.

User-Agent: Grandstream GXV3140 1.0.7.3.

Privacy: none.

P-Preferred-Identity: "alice" <sip:alice@server.com>.

Supported: replaces, path, timer.

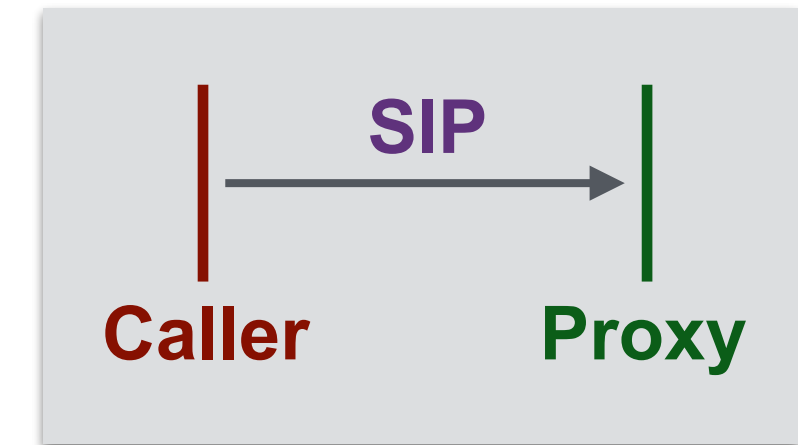
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE.

Content-Type: application/sdp.

Accept: application/sdp, application/dtmf-relay.

Content-Length: 483.

.



TOPOH MODULE

U 192.168.178.10:5060 -> 192.168.178.22:1056

INVITE sip:bob@192.168.178.22:1056;line=mu3z2i1j SIP/2.0.

Record-Route: <sip:192.168.178.10;lr=on>.

Via: SIP/2.0/UDP 192.168.178.10;branch=z9hG4bK8d21.062561f6.0.

Via: SIP/2.0/UDP 10.1.1.10;branch=z9hG4bKsr-JfymiMenCtp4urS5CX1ZiHvRItc.TM5nCHOBT6SfCXN94v5pswyRIRDZN80HU6gBI8LqTwDiCMe.CXm0TMNP.

From: "alice" <sip:alice@server.com>;tag=166646806.

To: <sip:bob@server.com>.

Call-ID: 989804978-40416-6@BJC.BGI.BHI.CH.

CSeq: 50 INVITE.

Contact: "alice" <sip:10.1.1.10;line=sr-ORyIIHvITJS.IXenCXNciHvPItcZTMWfC6m.T5**>.

Max-Forwards: 69.

User-Agent: Grandstream GXV3140 1.0.7.3.

Privacy: none.

P-Preferred-Identity: "alice" <sip:alice@server.com>.

Supported: replaces, path, timer.

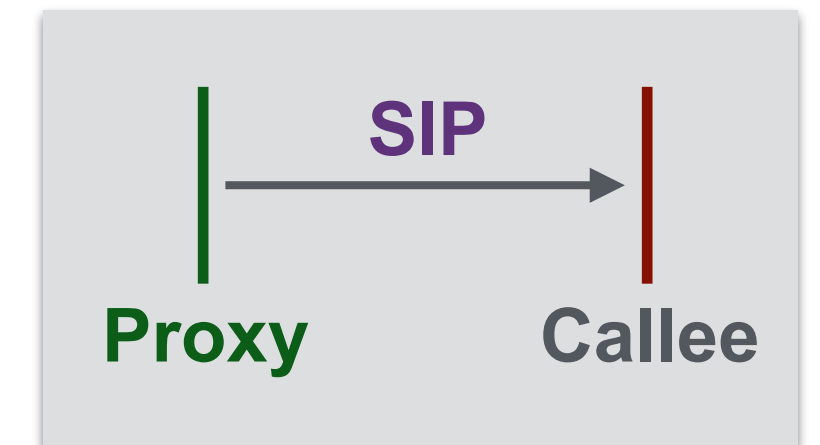
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE.

Content-Type: application/sdp.

Accept: application/sdp, application/dtmf-relay.

Content-Length: 483.

.



TOPOH MODULE

U 192.168.178.22:1056 -> 192.168.178.10:5060

SIP/2.0 200 Ok.

Via: SIP/2.0/UDP 192.168.178.10;branch=z9hG4bK8d21.062561f6.0.

Via: SIP/2.0/UDP 10.1.1.10;branch=z9hG4bKsr-

JfymiMenCtp4urS5CX1ZiHvRItc.TM5nCHOBT6SfCXN94v5pswyRIRDZN80HU6gBI8LqTwDiCMe.CXm0TMNP.

Record-Route: <sip:192.168.178.10;lr=on>.

From: "alice" <sip:alice@server.com>;tag=166646806.

To: <sip:bob@server.com>;tag=o3ybqqof1s.

Call-ID: 989804978-40416-6@BJC.BGI.BHI.CH.

CSeq: 50 INVITE.

Contact: <sip:bob@192.168.178.22:1056;line=mu3z2i1j>;reg-id=1.

User-Agent: snom370/8.4.18.

Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO, UPDATE.

Allow-Events: talk, hold, refer, call-info.

Supported: timer, 100rel, replaces, from-change.

Content-Type: application/sdp.

Content-Length: 496.

.

U 192.168.178.10:5060 -> 192.168.178.27:40416

SIP/2.0 200 Ok.

Via: SIP/2.0/UDP 192.168.178.27:40416;branch=z9hG4bK321149767.

Record-Route: <sip:192.168.178.10;lr=on>.

From: "alice" <sip:alice@server.com>;tag=166646806.

To: <sip:bob@server.com>;tag=o3ybqqof1s.

Call-ID: 989804978-40416-6@BJC.BGI.BHI.CH.

CSeq: 50 INVITE.

Contact: <sip:10.1.1.10;line=sr-ORyIIHvlCJS.IXenCXNciHvPItcZCHW.C6JRIR.o3-Jp3dJMGHDoC8W*>;reg-id=1.

User-Agent: snom370/8.4.18.

Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO, UPDATE.

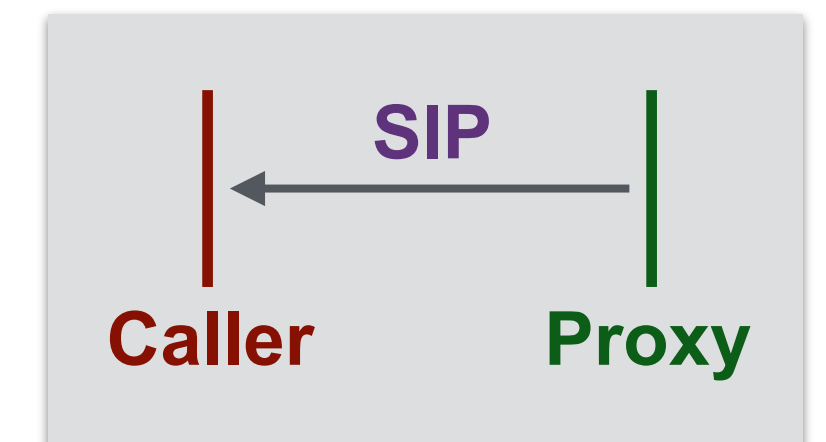
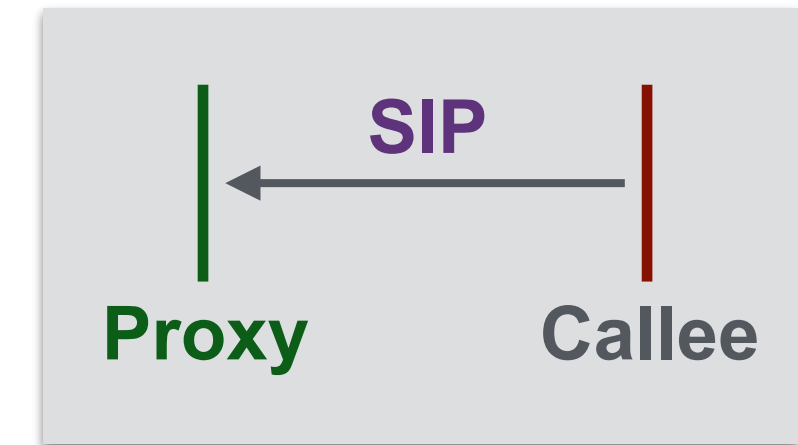
Allow-Events: talk, hold, refer, call-info.

Supported: timer, 100rel, replaces, from-change.

Content-Type: application/sdp.

Content-Length: 496.

.



TOPOH MODULE

U 192.168.178.27:40416 -> 192.168.178.10:5060

BYE sip:10.1.1.10;line=sr-ORyIIHvICJS.IXenCXNciHvPItcZCHW.C6JRIR.o3-Jp3dJMGHDoC8W* SIP/2.0.

Via: SIP/2.0/UDP 192.168.178.27:40416;branch=z9hG4bK271415657;rport.

Route: <sip:192.168.178.10;lr=on>.

From: "alice" <sip:alice@server.com>;tag=166646806.

To: <sip:bob@server.com>;tag=o3ybqqof1s.

Call-ID: 989804978-40416-6@BJC.BGI.BHI.CH.

CSeq: 51 BYE.

Contact: <sip:alice@192.168.178.27:40416>.

Max-Forwards: 70.

Supported: replaces, path, timer.

User-Agent: Grandstream GXV3140 1.0.7.3.

Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE.

Content-Length: 0.

U 192.168.178.10:5060 -> 192.168.178.22:1056

BYE sip:bob@192.168.178.22:1056;line=mu3z2i1j SIP/2.0.

Via: SIP/2.0/UDP 192.168.178.10;branch=z9hG4bK9d21.d62bd214.0.

Via: SIP/2.0/UDP 10.1.1.10;branch=z9hG4bKsr-

JfymiMenCtp4urS5CX1ZiHvRItc.TM5nCHOBT6SfCXN94v5pswTRIRDZN80HU6gBI8LqTwDiCHO.T6vgTHJPIPD13PDfhXmlT6vR.

From: "alice" <sip:alice@server.com>;tag=166646806.

To: <sip:bob@server.com>;tag=o3ybqqof1s.

Call-ID: 989804978-40416-6@BJC.BGI.BHI.CH.

CSeq: 51 BYE.

Contact: <sip:10.1.1.10;line=sr-ORyIIHvITJS.IXenCXNciHvPItcZTMWfC6m.T5**>.

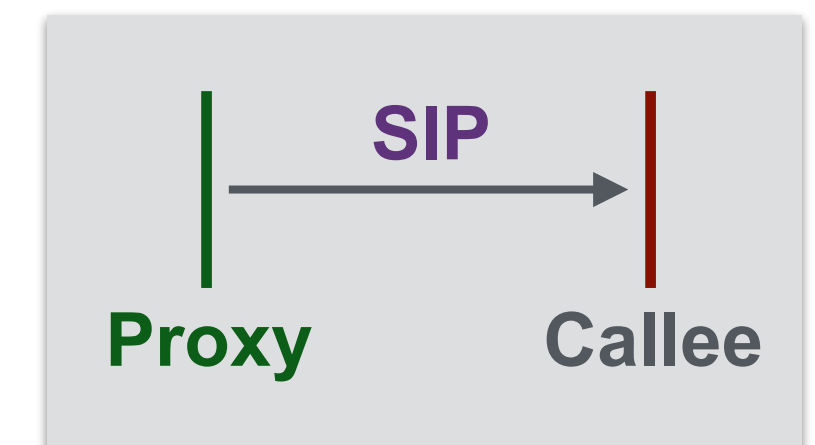
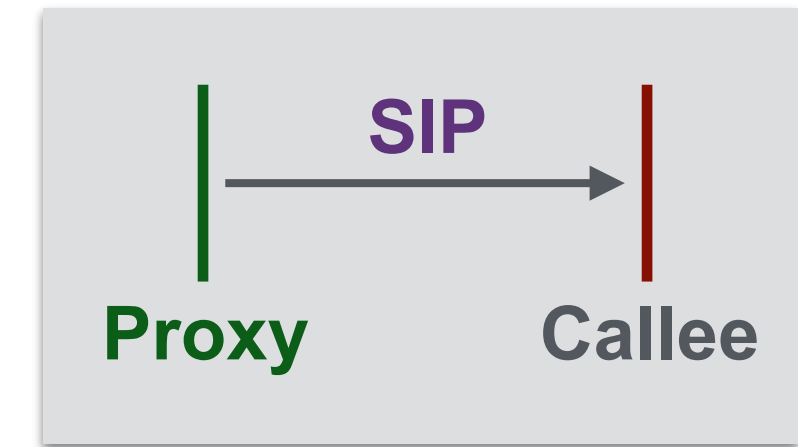
Max-Forwards: 69.

Supported: replaces, path, timer.

User-Agent: Grandstream GXV3140 1.0.7.3.

Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE.

Content-Length: 0.





Topology Hiding

stripping headers

topos module

TOPOS MODULE

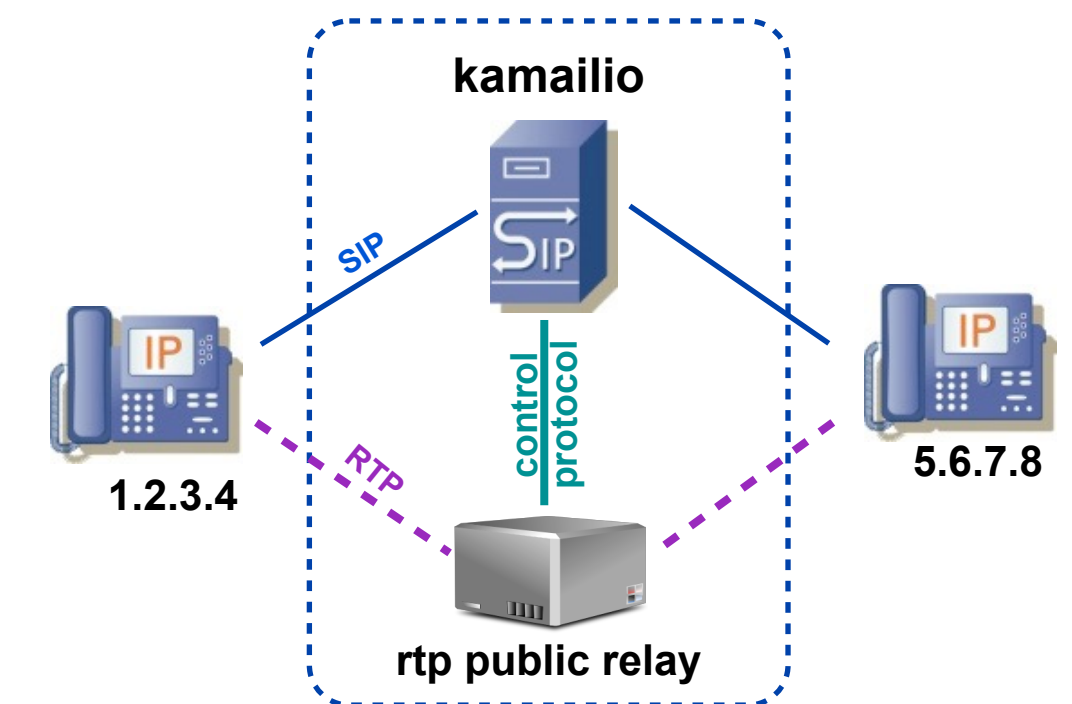
□ module: topos

□ goals

- remove or replace sensitive headers
 - contact header
 - Via stack
 - Record-Route and Route stacks

□ design

- database storage
 - track of sip traffic
- alternative redis storage (topoh_redis)
- distributed processing
 - shared database
- transparent processing
 - config writer should not care about topology stripping
 - full sip packet while config processing
- event routes to control topology stripping
- context grouping for spiralling
- ack-to-back user agent **like** signalling
- use with a RTP relay for full privacy



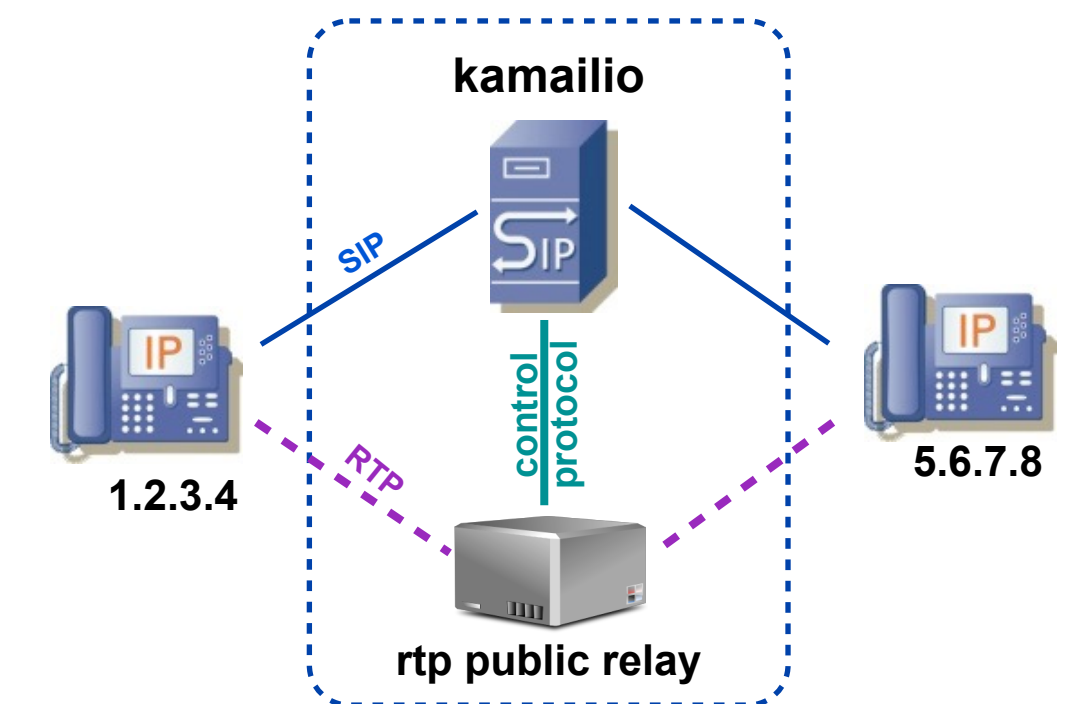
<https://kamailio.org/docs/modules/stable/modules/topos.html>

TOPOS MODULE

```
...
loadmodule "topos.so"
...
# ----- topos params -----
modparam("topos", "storage", "db")
modparam("topoh", "db_url", "mysql://kamailio:kamailio@localhost/kamailio")
...
```

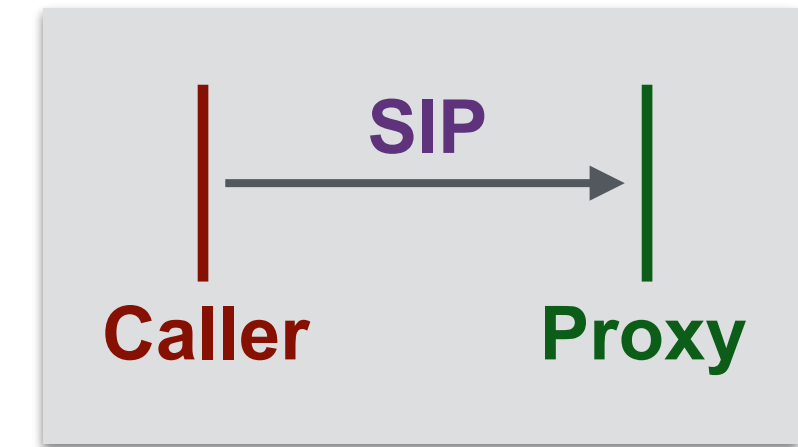
```
event_route[topos:msg-outgoing] {
    if($sndto(ip)=="10.1.1.10") {
        drop;
    }
}
```

```
event_route[topos:msg-sending] {
    if(is_request() && $tU=="bob") {
        drop;
    }
}
```



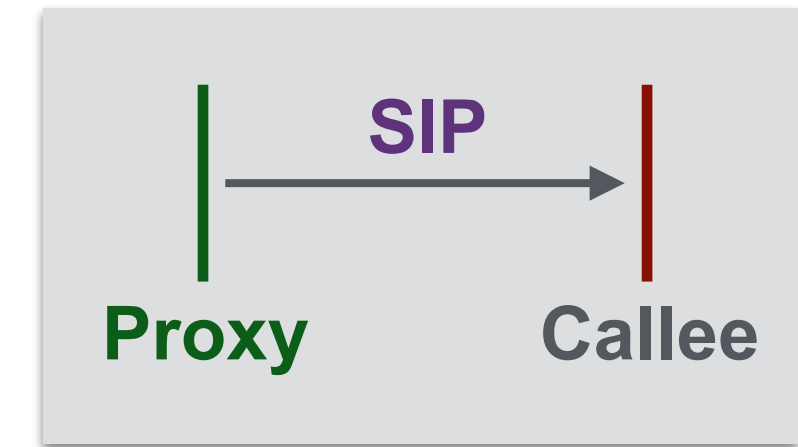
TOPOS MODULE

INVITE sip:alice@siplab01z.asipto.com SIP/2.0.
Via: SIP/2.0/UDP 10.99.0.164:60218;branch=z9hG4bKefc06c860482aea5;rport
Contact: <sip:bob-0xb400007bf5eedf20@10.99.0.164:60218>
Max-Forwards: 70
Route: <sip:siplab01z.asipto.com;lr>
To: <sip:alice@siplab01z.asipto.com>
From: "bob" <sip:bob@siplab01z.asipto.com>;tag=97a7ab7f2d090489
Call-ID: 3de048a6508f6906
CSeq: 11792 INVITE
User-Agent: baresip v2.7.0
Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,NOTIFY,SUBSCRIBE,INFO,MESSAGE,UPDATE,REFER
Supported: gruu,path,outbound,replaces,norefersub
Content-Type: application/sdp
Content-Length: 751
.



TOPOS MODULE

INVITE sip:alice@204.14.38.189:61316;transport=UDP;rinstance=d95ecbd2fc1acdc2 SIP/2.0
Via: SIP/2.0/UDP 200.10.10.100;branch=z9hG4bKc684.5d4a99f065208dd826e33f8dd3aa4551.0
Max-Forwards: 69
To: <sip:alice@siplab01z.asipto.com>
From: "bob" <sip:bob@siplab01z.asipto.com>;tag=97a7ab7f2d090489
Call-ID: 3de048a6508f6906
CSeq: 11792 INVITE
User-Agent: baresip v2.7.0
Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,NOTIFY,SUBSCRIBE,INFO,MESSAGE,UPDATE,REFER
Supported: gruu,path,outbound,replaces,norefersub
Content-Type: application/sdp
Content-Length: 751
Contact: <sip:btpsh-634da825-e9d-3@200.10.10.100>



.

TOPOS MODULE

SIP/2.0 200 OK

Via: SIP/2.0/UDP 200.10.10.100;branch=z9hG4bKc684.5d4a99f065208dd826e33f8dd3aa4551.0

Contact: <sip:alice@204.14.38.189:61316;transport=UDP>

To: <sip:alice@siplab01z.asipto.com>;tag=03e88a26

From: "bob" <sip:bob@siplab01z.asipto.com>;tag=97a7ab7f2d090489

Call-ID: 3de048a6508f6906

CSeq: 11792 INVITE

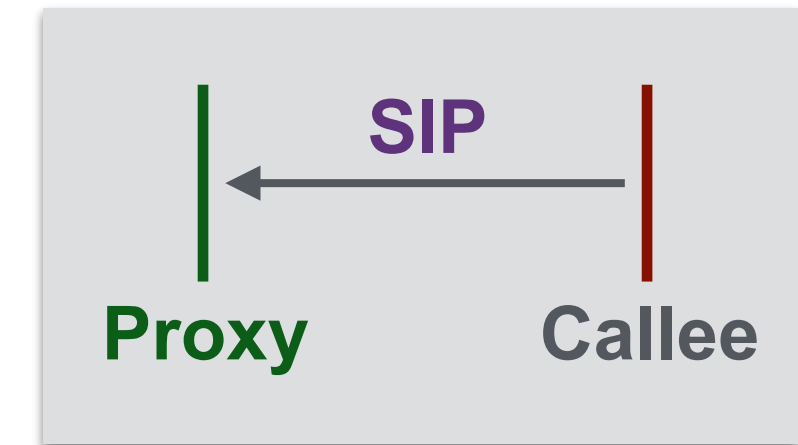
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE

Content-Type: application/sdp

User-Agent: Z 5.5.13 v2.10.18.3

Allow-Events: presence, kpml, talk

Content-Length: 327



SIP/2.0 200 OK

To: <sip:alice@siplab01z.asipto.com>;tag=03e88a26

From: "bob" <sip:bob@siplab01z.asipto.com>;tag=97a7ab7f2d090489

Call-ID: 3de048a6508f6906

CSeq: 11792 INVITE

Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE

Content-Type: application/sdp

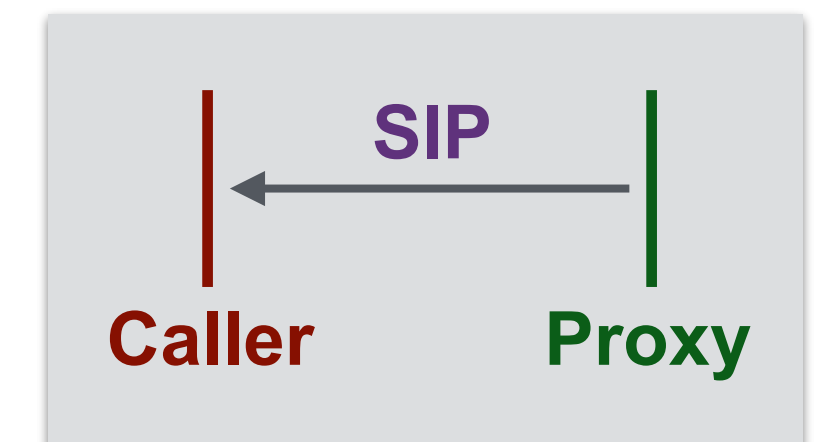
User-Agent: Z 5.5.13 v2.10.18.3

Allow-Events: presence, kpml, talk

Content-Length: 327

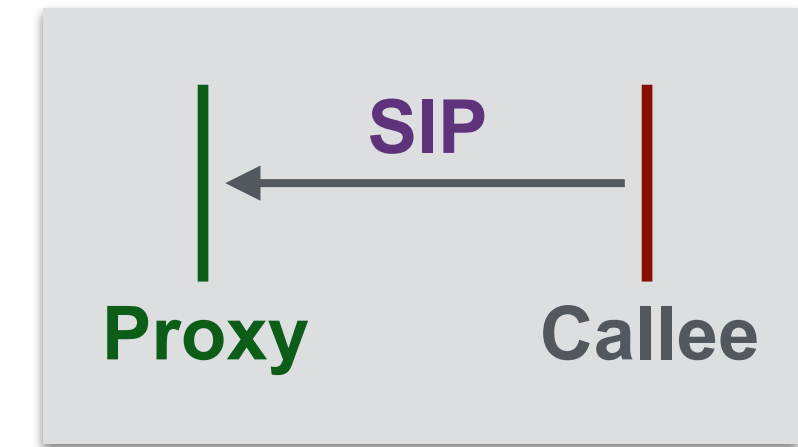
Via: SIP/2.0/UDP 10.99.0.164:60218;received=204.14.38.189;branch=z9hG4bKefc06c860482aea5;rport=60218

Contact: <sip:atpsh-634da825-e9d-3@200.10.10.100>

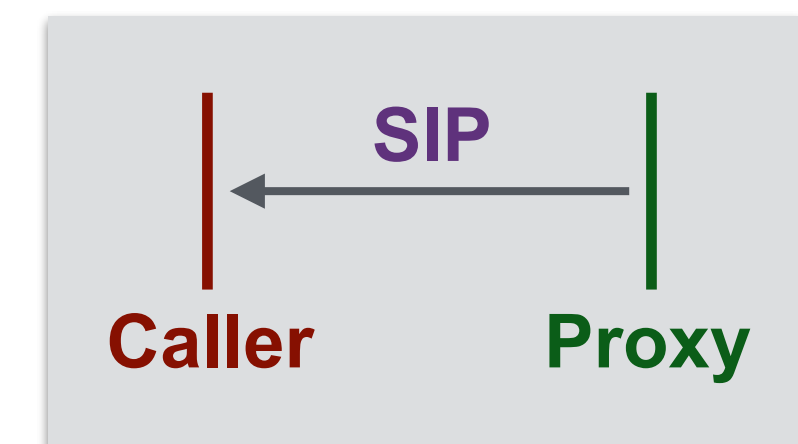


TOPOS MODULE

BYE sip:btpsh-634da825-e9d-3@200.10.10.100 SIP/2.0
Via: SIP/2.0/UDP 10.99.0.150:61316;branch=z9hG4bK-524287-1---714779474df296db;rport
Max-Forwards: 70
To: "bob" <sip:bob@siplab01z.asipto.com>;tag=97a7ab7f2d090489
From: <sip:alice@siplab01z.asipto.com>;tag=03e88a26
Call-ID: 3de048a6508f6906
CSeq: 2 BYE
User-Agent: Z 5.5.13 v2.10.18.3
Content-Length: 0



BYE sip:bob-0xb400007bf5eedf20@10.99.0.164:60218 SIP/2.0
Via: SIP/2.0/UDP 200.10.10.100;branch=z9hG4bK68c9.785d869648797f7c4a22521599212934.0
Max-Forwards: 69
To: "bob" <sip:bob@siplab01z.asipto.com>;tag=97a7ab7f2d090489
From: <sip:alice@siplab01z.asipto.com>;tag=03e88a26
Call-ID: 3de048a6508f6906
CSeq: 2 BYE
User-Agent: Z 5.5.13 v2.10.18.3
Content-Length: 0



Is it now a B2BUA?



IT IS NOT





...

• **Website:** <https://www.kamailio.org>

• Development project: <https://github.com/kamailio/kamailio>

• Documentation page: <https://www.kamailio.org/w/documentation/>

• Wiki tutorials: <https://www.kamailio.org/wiki/>

• Bug tracker: <https://github.com/kamailio/kamailio/issues>

• Users mailing list: <https://lists.kamailio.org/cgi-bin/mailman/listinfo/sr-users>

• Realtime chat channels: Matrix: #kamailio (kamailio.dev)

• Business directory: <https://www.kamailio.org/w/business-directory/>

• Download: <https://www.kamailio.org/w/download/> (or OS distro repos)

Resources



SecSIPIDx Project - STIR/SHAKEN

<https://github.com/asipto/secsipidx>

Components:

- `secsipid`: Go library - common functions
- `csecsipid`: C library - wrapper code to build dynamic or static library and .h include files
- `secsipidx`: `main.go` - CLI tool and HTTP API server for checking or building SIP identity

Secure SIP Identity Extensions - IETF STIR and SHAKEN

41 commits 1 branch 0 packages 0 releases 1 contributor GPL-2.0

Branch: master New pull request Find file Clone or download

File/Folder	Description	Last Commit
miconda	README.md: updated to-do list - the https server mode implemented	Latest commit 18500a4 26 days ago
csecsipid	csecsipid: include local file to get rid of cgo warning	last month
secsipid	secsipid: propagate origid via parameter	last month
.gitignore	.gitignore: skip binary app	2 months ago
LICENSE	Initial commit	2 months ago
README.md	README.md: updated to-do list - the https server mode implemented	25 days ago
main.go	secsipidx: coherent naming for command line parameters	last month

secsipidx

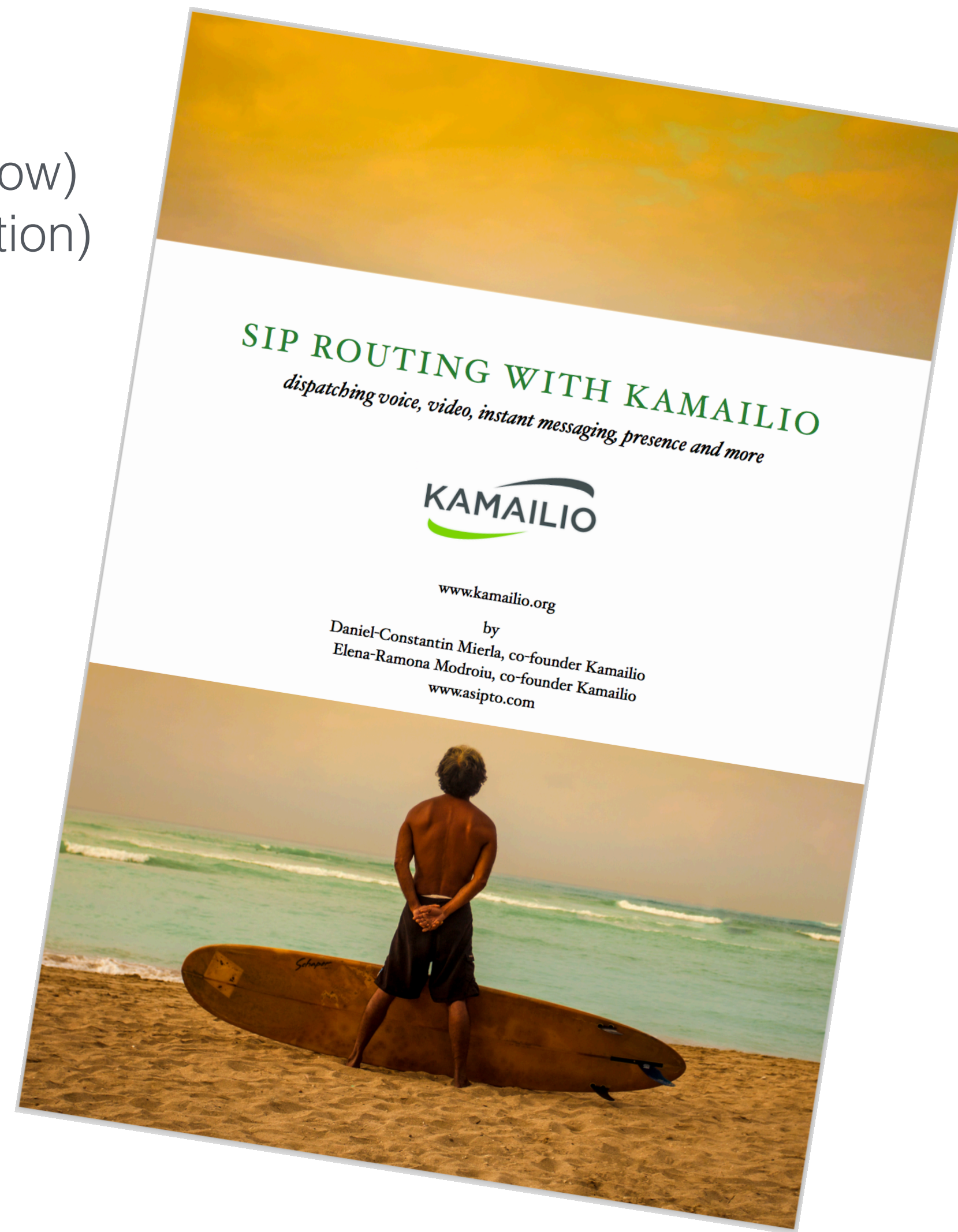
Secure SIP/Telephony Identity Extensions

Overview

Applications and libraries implementing STIR and SHAKEN (RFC8224, RFC8588), used in SIP/VoIP services:

- RFC8224 - <https://tools.ietf.org/html/rfc8224>
- RFC8588 - <https://tools.ietf.org/html/rfc8588>

- content update for v5.3.x (selling now)
- new chapters under work (new edition)



<https://www.asipto.com/sw/kamailio-admin-book/>



THANK YOU!

Daniel-Constantin Mierla

Co-Founder Kamilio Project

@miconda

asipto.com



Aiming For A Berlin Edition In 2023
(late May - early June)

www.kamailioworld.com