

OpenLI

INTERCEPT INTERNET TRAFFIC BASED ON OPEN SOURCE

PIM VAN STAM - S3GROUP

Contents

- Recap Lawful interception in The Netherlands
- OpenLI software
- Steps for implementation in The Netherlands

Non-technology abbreviations

CIOT: Centraal Informatiepunt Opsporing Telecommunicatie

ETSI: European Telecommunication Standardisation Institute

HI: Handover Interface

LEA: Law Enforcement Agency

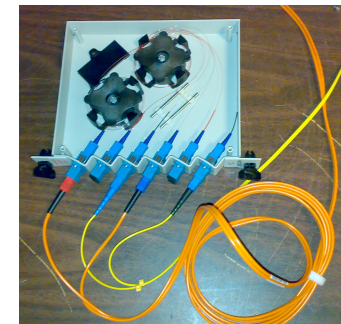
LEMF: Law Enforcement Monitoring Facility

LI: Lawful Intercept

NDA: Non-Disclosure Agreement

VOG: Verklaring Omtrent Gedrag (certificate of conduct)

WMS: Warrant Management System



Recap Lawful interception

Lawful interception in The Netherlands

Telecommunicatiewet (TW) artikel 13.1, lid 1:

“Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten stellen hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar aan gebruikers indien deze aftapbaar zijn.”

Artikel 13.2, lid 2:

“Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevel op grond van het [Wetboek van Strafvordering](#) dan wel een toestemming op grond van de [Wet op de inlichtingen- en veiligheidsdiensten 2017](#) tot het aftappen of opnemen van door hen verzorgde telecommunicatie.”

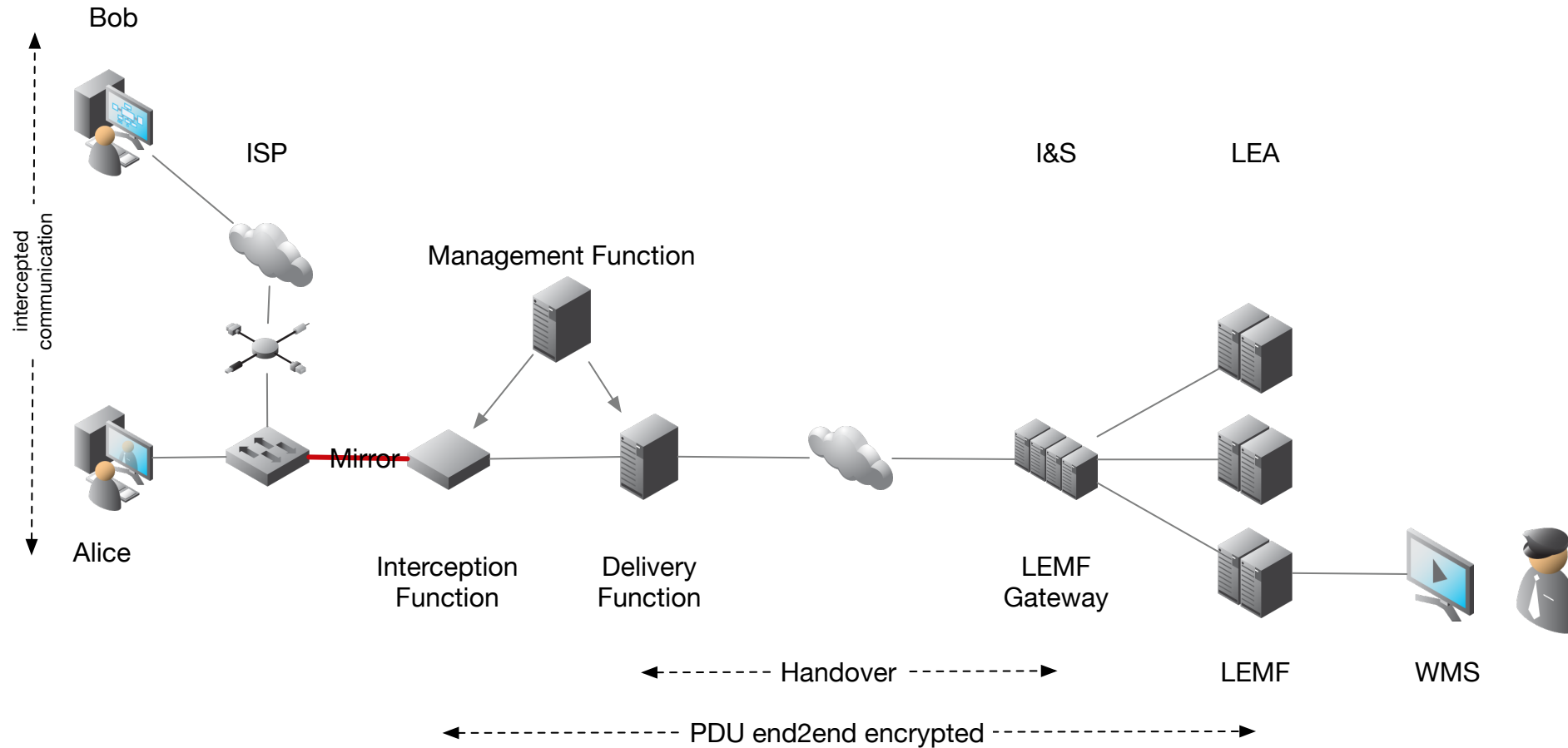


Lawful interception in The Netherlands

What you need to do as provider:

- Tappable (TW art 13.1 lid 1)
- Security measures - BBGT (TW art 13.2 lid 3, Besluit Beveiliging Gegevens Telecommunicatie)
- CIOT connection (TW 13.4, lid 2 en 4, Besluit Verstrekking Gegevens Telecommunicatie)
- VOG en NDA employers (BBGT art 4.2 en bijlage IIb)
- Security plan en continuity plan (BBGT art 3.1, TW11, source?)

Lawful interception in The Netherlands



Lawful interception in The Netherlands

Specifications:

- ETSI TS 102 232
 - part 1 - Handover specification for IP delivery
 - part 2 - Messaging Services
 - part 3 - Internet Access Services
 - part 4 - L2 Services
 - part 5 - IP Multimedia Services
 - part 6 - PSTN / ISDN Services
 - part 7 - Mobile Services
- ETSI-IP.nl: Implementatie details for Dutch situation

Lawful interception in The Netherlands

Specifications:

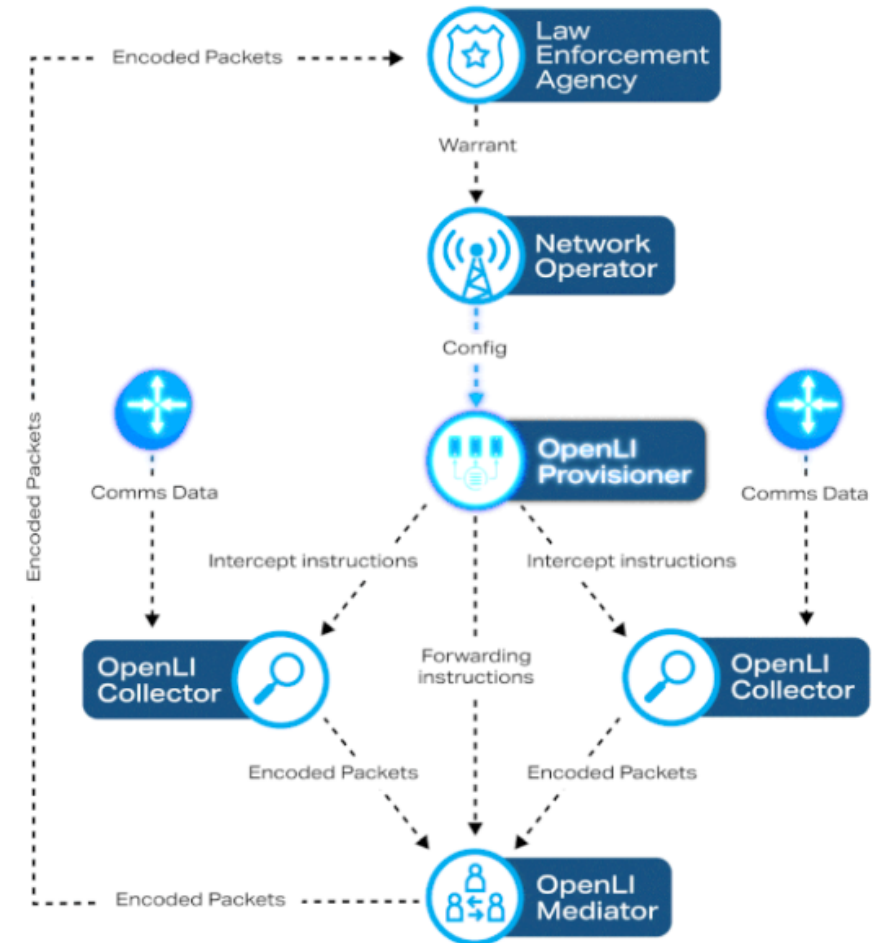
- Handover interfaces
 - HI1: Warrant handling in XML format
 - E-mail: e-sub-HI1 Lite
 - Message Broker: e-sub-HI1
 - HI2: IRI - Intercept Related Information
 - HI3: CC - Content of Communication
- HI2/HI2 transport
 - Transport encrypted
 - Header in ASN.1 format
 - Payload encrypted

OpenLI software

OpenLI software

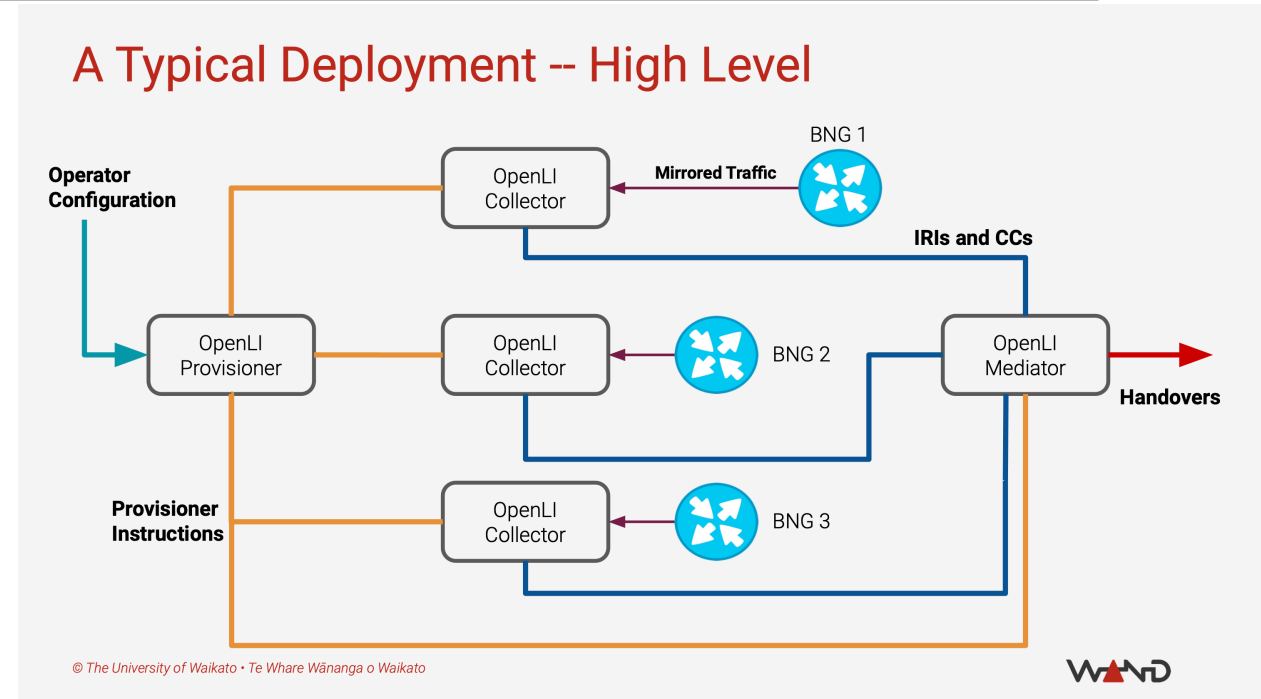
- Initiative from NZNOG community
- WAND research group from University of Waikato developed software
- 13 organisations contribute money to fund the project
- Open source
- Conforms ETSI standards (TS 101 671 and TS 102 232 (p1, p3, p5, p7))
- Development and support transferred to Searchlight
- Funding with support contracts

Source: openli.nz website



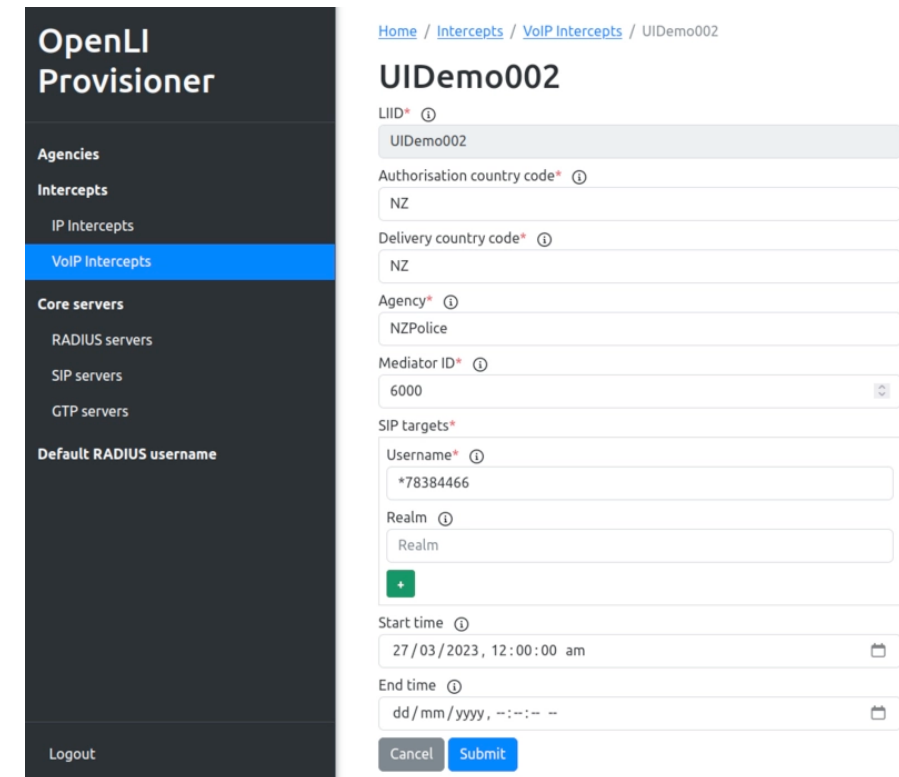
OpenLI software

- Elements:
 - Provisioner: Management function
 - Collector: Interception function
 - Captures traffic
 - Filtering
 - Encode to ETSI format
 - Mediator: Delivery function
 - Mapping intercepts to LEA's
 - Handover to LEA's



OpenLI software

- Linux
- Built in C
- Can use DPDK, hopefully XDP in near future
- Project on github: <https://github.com/OpenLI-NZ/openli>
- REST API as basis
- Configuration files as starting point
- Has a (basic) web interface, openli-provisioner-web (not tried yet)



The screenshot displays the OpenLI Provisioner web interface. On the left is a dark sidebar with a menu containing 'Agencies', 'Intercepts' (with sub-items 'IP Intercepts' and 'VoIP Intercepts'), 'Core servers' (with sub-items 'RADIUS servers', 'SIP servers', and 'GTP servers'), and 'Default RADIUS username'. The 'VoIP Intercepts' item is highlighted in blue. At the bottom of the sidebar is a 'Logout' link. The main content area on the right shows the configuration for 'UIDemo002'. At the top of this area are navigation links: 'Home / Intercepts / VoIP Intercepts / UIDemo002'. The configuration form includes fields for 'LIID*' (set to 'UIDemo002'), 'Authorisation country code*' (set to 'NZ'), 'Delivery country code*' (set to 'NZ'), 'Agency*' (set to 'NZPolice'), 'Mediator ID*' (set to '6000'), and 'SIP targets*'. The 'SIP targets*' section has a '+' button and fields for 'Username*' (set to '*78384466') and 'Realm' (set to 'Realm'). At the bottom of the form are 'Start time' (set to '27/03/2023, 12:00:00 am') and 'End time' (set to 'dd/mm/yyyy, --:--:--') fields, each with a calendar icon. At the very bottom are 'Cancel' and 'Submit' buttons.

OpenLI software - config files

collector-config.yaml

provisioneraddr: 192.168.1.10
provisionerport: 9001
operatorid: S3LI
networkelementid: IF-DC
interceptpointid: if-01-01
seqtrackerthreads: 1
encoderthreads: 2
forwardingthreads: 1
sipallowfromident: no
logstatfrequency: 5
RMQenabled: false
RMQname: "rmquser"
RMQpass: "rmqpassword"

inputs:
- uri: eth1
 threads: 2

mediator-config.yaml

operatorid: S3LI
altoperatorid: 12345
mediatorid: 6001
provisioneraddr: 192.168.1.10
provisionerport: 12001
listenaddr: 192.168.1.10
listenport: 8888
pcapdirectory: /data/openlipcaps/
pcaprotatefreq: 30
pcapfilename: example-%L-%d%m%y-%H%M%S
pcapcompress: 1
RMQenabled: false
RMQname: "rmquser"
RMQpass: "rmqpassword"
RMQSSL: true
RMQheartbeatfreq: 30



OpenLI software - config files

provisioner-config.yaml

clientaddr: 192.168.1.10
clientport: 9001
mediationaddr: 192.168.1.10
mediationport: 12001
updateaddr: 12.13.14.15
updateport: 9009
intercept-config-file: /etc/openli/running-intercept-config.yaml
voip-ignorecomfort: no
restauthdb: /var/lib/openli/provauth.db
restauthkey: verysecret

running-intercept-config.yaml

sipservers: []
radiusservers: []
gtpservers: []
smtpservers: []
imapservers: []
pop3servers: []
agencies:
- hi3address: 21.22.23.24
 hi3port: 3004
 hi2address: 21.22.23.24
 hi2port: 3004
 agencyid: lenS
 keepalivefreq: 300
 keepalivewait: 30
voipintercepts: []
ipintercepts: []
emailintercepts: []



OpenLI software - REST API

REST-API

Creating an API key:

```
/usr/sbin/openli-prov-adduser.sh 'restauthkey' 'user' 'apikey' 'database'
```

Bijv:

```
/usr/sbin/openli-prov-adduser.sh abcdefghij testapi VENc0xGGzdqHWPvZLxoq /var/lib/openli/provauth.db
```

Example API call, here the list of agencies and creating one. These are the delivery points

```
curl -X GET http://192.168.1.10:9009/agency
```

```
curl -H "X-API-KEY:VENc0xGGzdqHWPvZLxoq" -X GET http://192.168.1.10:9009/agency
```

```
curl -X PUT -H "Content-Type: application/json" -d @locallea.json http://192.168.1.10:9009/agency
```

locallea.json

```
{  
  "agencyid": "LocalLEA",  
  "hi2address": "127.0.0.1",  
  "hi2port": "41002",  
  "hi3address": "127.0.0.1",  
  "hi3port": "41003",  
  "keepalivefreq": "300",  
  "keepalivewait": "30"  
}
```

OpenLI software - Testing with local LEA

Create a (local) delivery agency. See example previous slide (locallea)

tracepktdump tool is in libtrace4-tools. With this tool you can decode ETSI packets of a live stream or from a captured file.

Examples:

```
$ tracepktdump etsilive:21.22.23.24:3004
```

Or

```
$ tracepktdump etsilive:127.0.0.1:41002 (for IRI only)
```

With a captured file:

```
$ tracepktdump etsifile:test.dump
```

Create an etsifile with i.e. tcpdump. In Wireshark 'follow tcp session' and store payload in binary file.

Capture: Packet Length: 174/174 Direction Value: -1

ETSILI: 0x56264e45d163 (94722521944419): pS-PDU:

ETSILI: 0x56264e45d165 (2): PSHeader:

ETSILI: 0x56264e45d16e (9): li-psDomainId: 0.4.0.2.2.5.1.30

ETSILI: 0x56264e45d189 (27): lawfulInterceptionIdentifier: gi_|+=y!s

ETSILI: 0x56264e45d18d (4): authorizationCountryCode: NL

ETSILI: 0x56264e45d18f (2): communicationIdentifier:

ETSILI: 0x56264e45d191 (2): networkIdentifier:

ETSILI: 0x56264e45d19b (10): operatorIdentifier: 12345

ETSILI: 0x56264e45d19f (4): networkElementIdentifier:

ETSILI: 0x56264e45d1a2 (3): sequenceNumber: 0

ETSILI: 0x56264e45d1a4 (2): microSecondTimeStamp:

ETSILI: 0x56264e45d1aa (6): seconds: 1679415246

ETSILI: 0x56264e45d1af (5): microseconds: 439119

ETSILI: 0x56264e45d1b2 (3): timeStampQualifier: timeOfMediation

ETSILI: 0x56264e45d1b4 (2): Payload:

ETSILI: 0x56264e45d1b6 (2): encryptionContainer:

ETSILI: 0x56264e45d1b9 (3): encryptionType: None

ETSILI: 0x56264e45d20b (82): encryptedPayload:

ETSILI: 0x56264e45d20b (0): byteCounter: 7213033549383860897

ETSILI: 0x56264e45d20b (0): payload:

ETSILI: 0x56264e45d20b (0): tRIPayload:

ETSILI: 0x56264e45d20b (0): integrityCheck:

ETSILI: 0x56264e45d20b (0): includedSequenceNumbers: 0

ETSILI: 0x56264e45d20b (0): checkType: Hash

ETSILI: 0x56264e45d20b (0): dataType: IRI

ETSILI: 0x56264e45d20b (0): checkValue: 0x6e0eb51086c2b9bd0b4e2c0

ETSILI: 0x56264e45d20b (0): hashAlgorithm: SHA-256

ETSILI: 0x56264e45d20e (3): encryptedPayloadType: part1

Implementation in NL

Implementation in NL

- Connection on peering vlan AMS-IX or NL-ix
- Direct peering with police on one of the IXP's
- Warrants by e-mail + PGP or Message Broker
- Operator ID deposit is RDI (Rijksinspectie voor Digitale Infrastructuur)
- Encrypted payload: necessary because there is one connection point for all agencies
- Testing with police is mandatory. We are planning to test OpenLI with the government. Internal tests by S3group are positive.

Questions?
