PCP-PANA Implementation Report

Pedro Moreno Sánchez and Rafa Marin Lopez
(University of Murcia)
Ricardo V Martija and Subir Das
(Applied Communication Sciences)
Yoshihiro Ohba
(Toshiba)

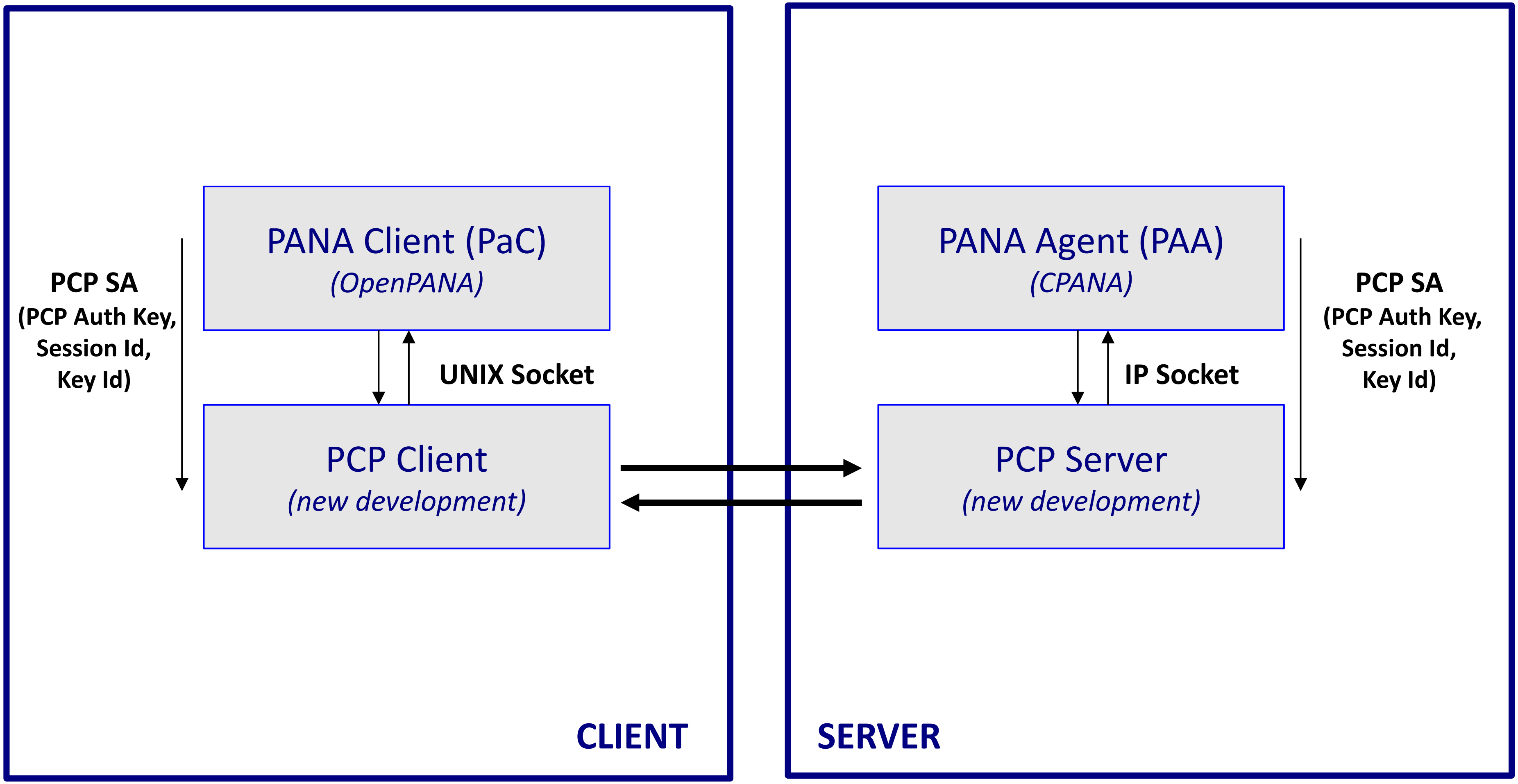
Objective

- To report PANA-based PCP authentication running code
  - based on draft <draft-ohba-pcp-pana-03>
  - Using two available open source implementations of PANA
    - OpenPANA (Client) and CPANA (Server)

Implemented Features

- PCP-PANA side-by-side approach <draft-ohba-pcp-pana-03>
  - Capability discovery using ANNOUNCE with AUTH_CAPABILITY option
  - Result Code = AUTHENITICATION_REQUIRED when PCP SA is needed and unauthenticated PCP request is received
  - Server-initiated re-authentication for re-key
  - Server-initiated PANA authentication when PCP server reboots
  - Explicit PCP SA termination using PANA termination phase
- MAP and PEER opcodes <draft-ietf-pcp-base-29>
  - Use of AUTHENTICATION_TAG option for authenticated PCP exchange <draft-ietf-pcp-authentication-01>
  - Protected unsolicited responses
  - Silent discard of unauthenticated messages once PCP SA is established
  - Dynamic firewall settings based on MAP/PEER state
  - Use of examples described in <draft-boucadair-pcp-flow-examples-00>

Software Architecture (Single Client)



PCP SA
(PCP Auth Key,
Session Id,
Key Id)

PANA Client (PaC)
(OpenPANA)

UNIX Socket

PCP Client
(new development)

CLIENT

PANA Agent (PAA)
(CPANA)

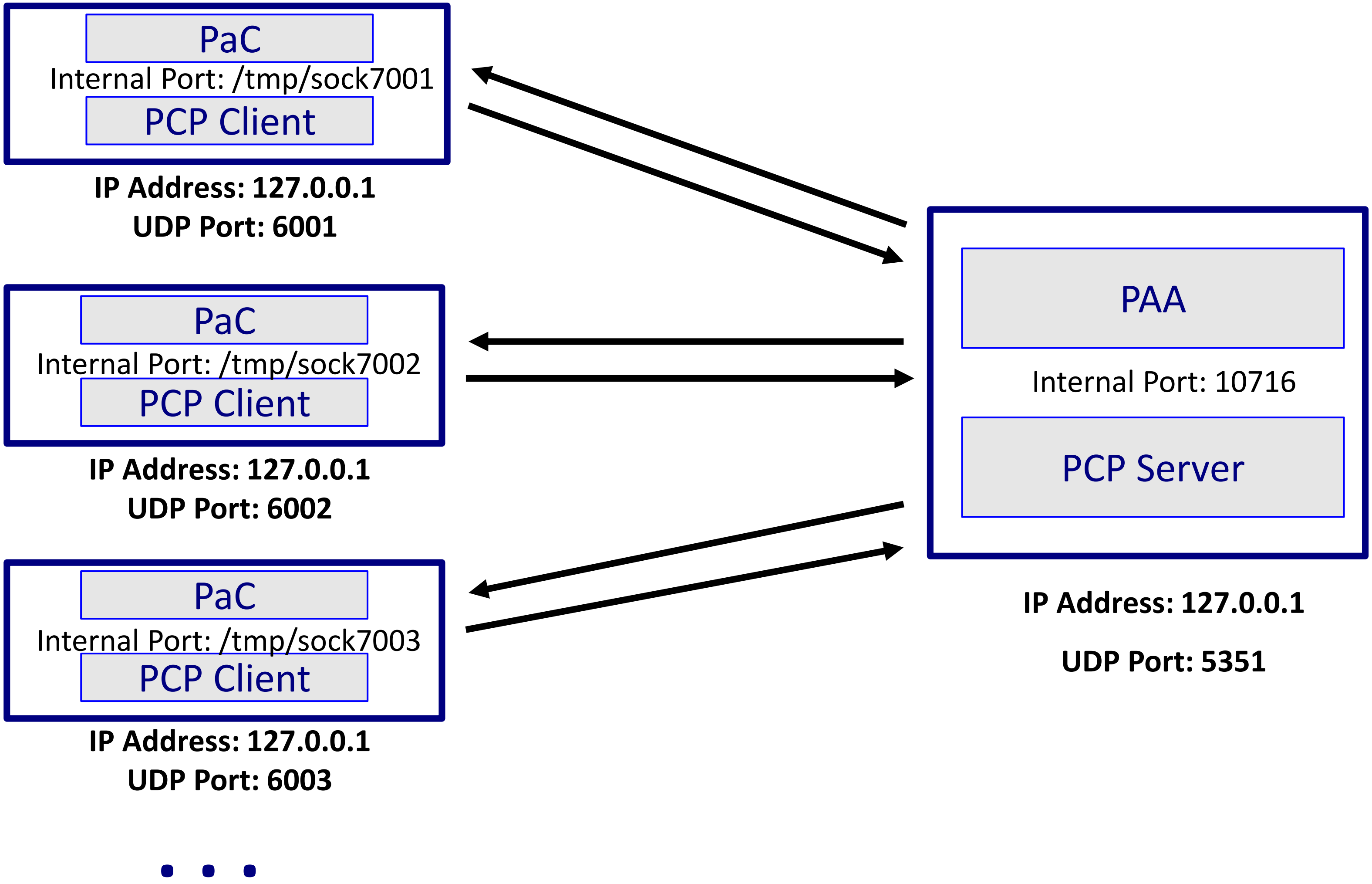
IP Socket

PCP Server
(new development)

PCP SA
(PCP Auth Key,
Session Id,
Key Id)

SERVER

Software Architecture (Multiple Clients)



PaC

Internal Port: /tmp/sock7001

PCP Client

IP Address: 127.0.0.1
UDP Port: 6001

PaC

Internal Port: /tmp/sock7002

PCP Client

IP Address: 127.0.0.1
UDP Port: 6002

PaC

Internal Port: /tmp/sock7003

PCP Client

IP Address: 127.0.0.1
UDP Port: 6003

. . .

PAA

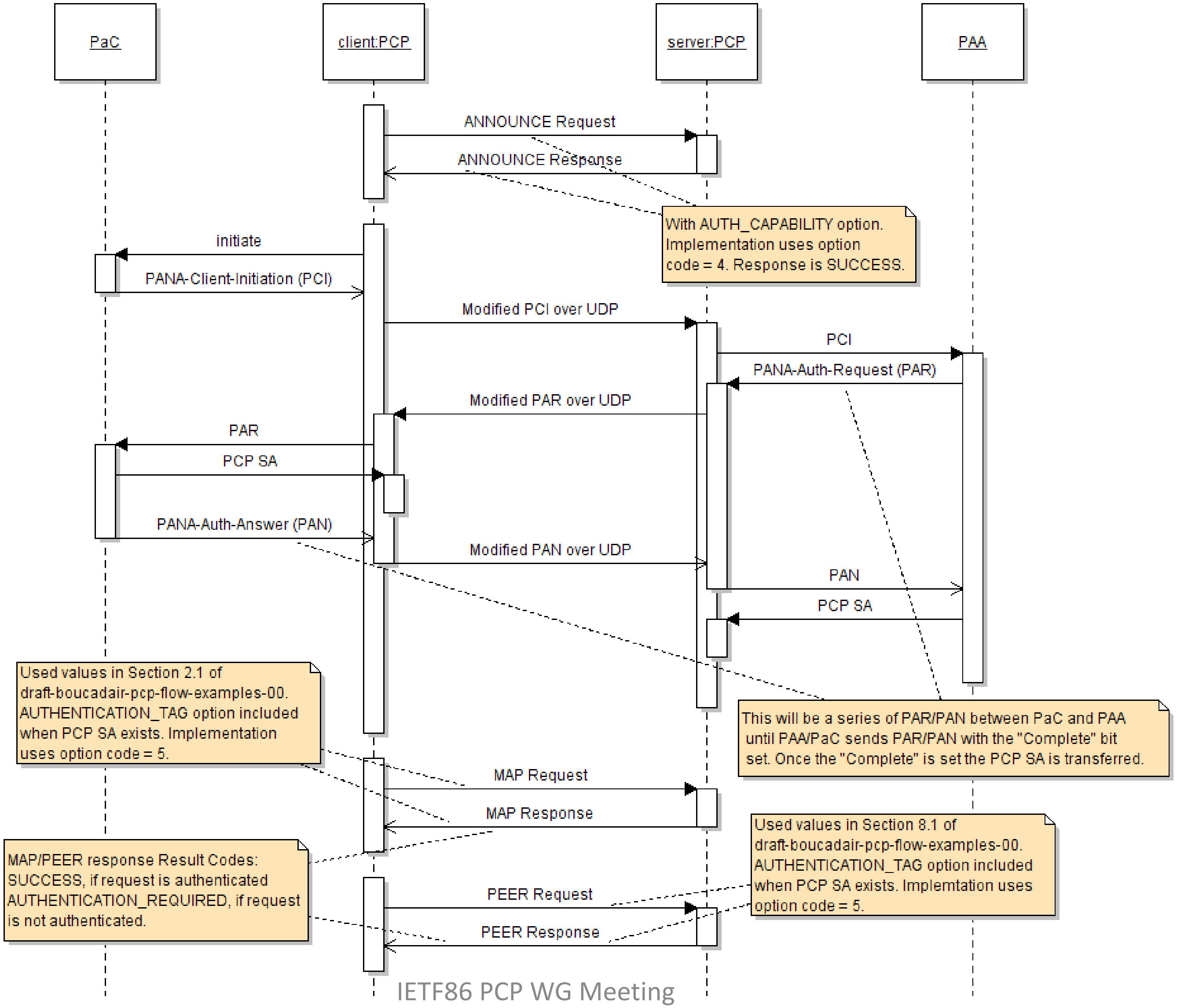
Internal Port: 10716

PCP Server

IP Address: 127.0.0.1

UDP Port: 5351

Implemented Call Flow
(Start with ANNOUNCE)



With AUTH_CAPABILITY option. Implementation uses option code = 4. Response is SUCCESS.

This will be a series of PAR/PAN between PaC and PAA until PAA/PaC sends PAR/PAN with the "Complete" bit set. Once the "Complete" is set the PCP SA is transferred.

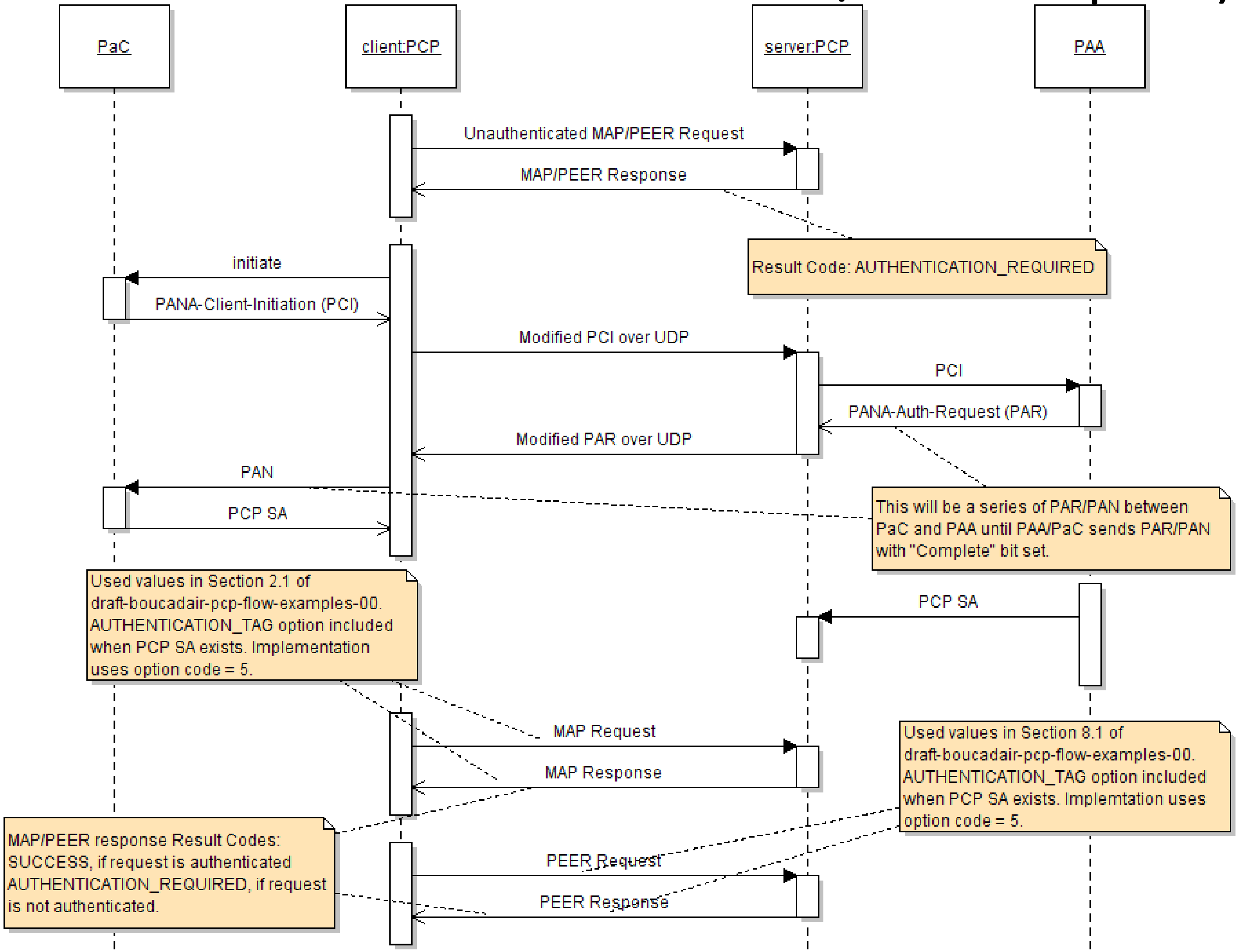
Used values in Section 2.1 of draft-boucadair-pcp-flow-examples-00. AUTHENTICATION_TAG option included when PCP SA exists. Implementation uses option code = 5.

MAP/PEER response Result Codes:
SUCCESS, if request is authenticated
AUTHENTICATION_REQUIRED, if request is not authenticated.

Used values in Section 8.1 of draft-boucadair-pcp-flow-examples-00. AUTHENTICATION_TAG option included when PCP SA exists. Implemtation uses option code = 5.

Implemented Call Flow

(Start with unauthenticated MAP/PEER request)



Result Code: AUTHENTICATION_REQUIRED

This will be a series of PAR/PAN between PaC and PAA until PAA/PaC sends PAR/PAN with "Complete" bit set.

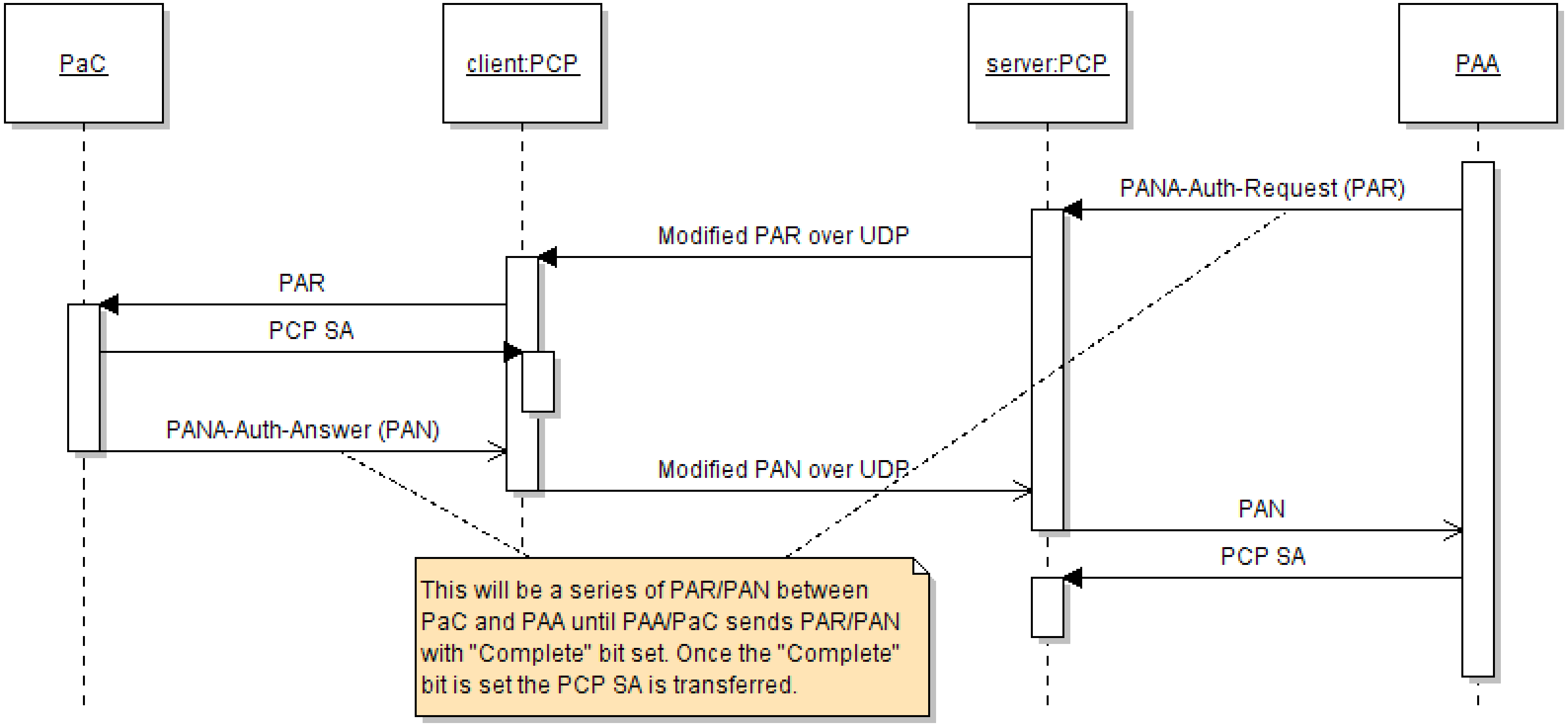
Used values in Section 2.1 of draft-boucadair-pcp-flow-examples-00. AUTHENTICATION_TAG option included when PCP SA exists. Implementation uses option code = 5.

Used values in Section 8.1 of draft-boucadair-pcp-flow-examples-00. AUTHENTICATION_TAG option included when PCP SA exists. Implemtation uses option code = 5.

MAP/PEER response Result Codes:
SUCCESS, if request is authenticated
AUTHENTICATION_REQUIRED, if request is not authenticated.

Implemented Call Flow

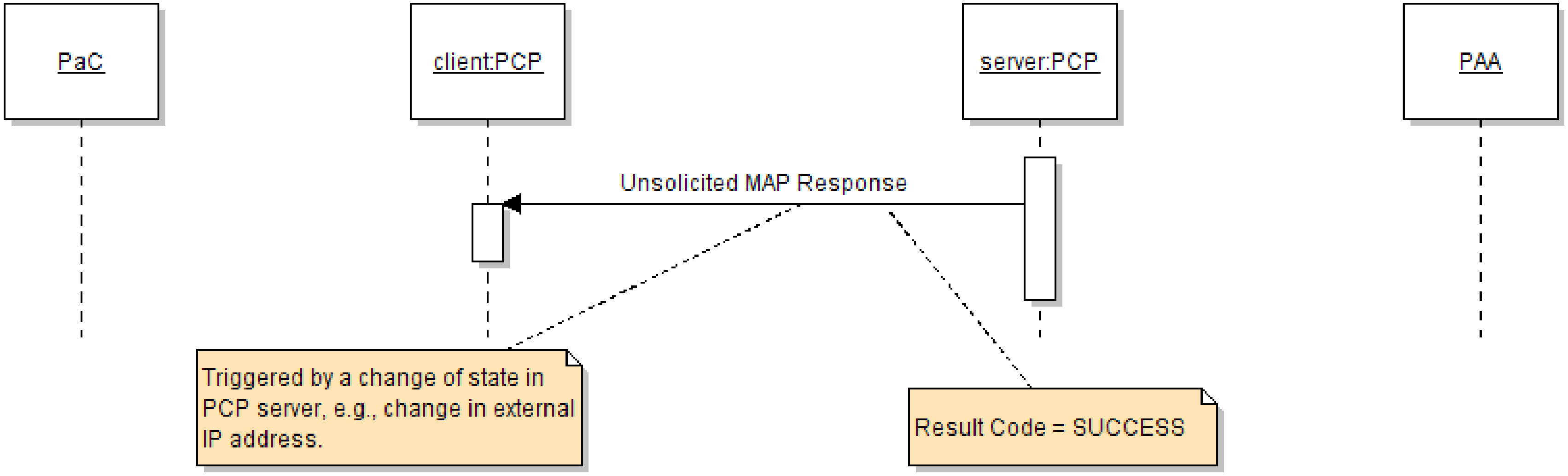
(PAA-Initiated Re-authentication)



This will be a series of PAR/PAN between PaC and PAA until PAA/PaC sends PAR/PAN with "Complete" bit set. Once the "Complete" bit is set the PCP SA is transferred.

Implemented Call Flow

(Unsolicited MAP Response)

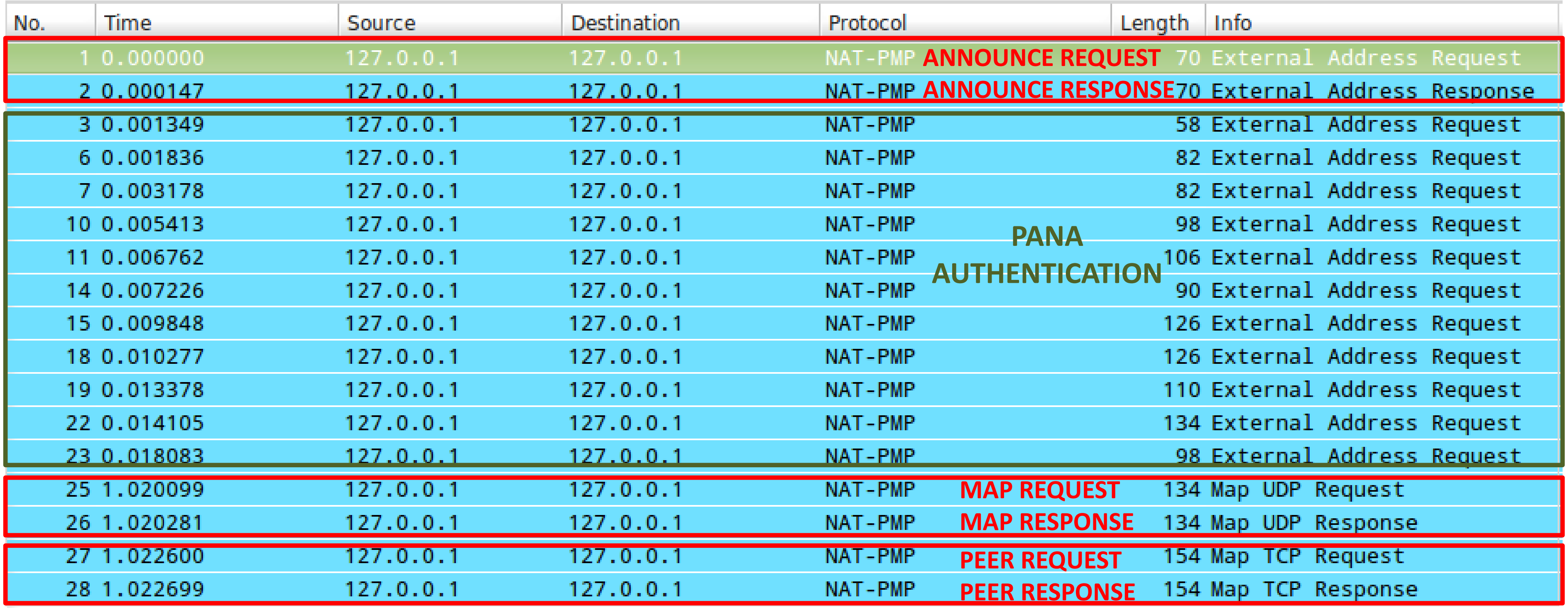


Triggered by a change of state in PCP server, e.g., change in external IP address.

Result Code = SUCCESS

Packet Capture

(PCP SA establishment – Authenticated MAP/PEER messages)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	NAT-PMP	70	External Address Request
2	0.000147	127.0.0.1	127.0.0.1	NAT-PMP	70	External Address Response
3	0.001349	127.0.0.1	127.0.0.1	NAT-PMP	58	External Address Request
6	0.001836	127.0.0.1	127.0.0.1	NAT-PMP	82	External Address Request
7	0.003178	127.0.0.1	127.0.0.1	NAT-PMP	82	External Address Request
10	0.005413	127.0.0.1	127.0.0.1	NAT-PMP	98	External Address Request
11	0.006762	127.0.0.1	127.0.0.1	NAT-PMP	106	External Address Request
14	0.007226	127.0.0.1	127.0.0.1	NAT-PMP	90	External Address Request
15	0.009848	127.0.0.1	127.0.0.1	NAT-PMP	126	External Address Request
18	0.010277	127.0.0.1	127.0.0.1	NAT-PMP	126	External Address Request
19	0.013378	127.0.0.1	127.0.0.1	NAT-PMP	110	External Address Request
22	0.014105	127.0.0.1	127.0.0.1	NAT-PMP	134	External Address Request
23	0.018083	127.0.0.1	127.0.0.1	NAT-PMP	98	External Address Request
25	1.020099	127.0.0.1	127.0.0.1	NAT-PMP	134	Map UDP Request
26	1.020281	127.0.0.1	127.0.0.1	NAT-PMP	134	Map UDP Response
27	1.022600	127.0.0.1	127.0.0.1	NAT-PMP	154	Map TCP Request
28	1.022699	127.0.0.1	127.0.0.1	NAT-PMP	154	Map TCP Response

ANNOUNCE REQUEST

ANNOUNCE RESPONSE

PANA AUTHENTICATION

MAP REQUEST

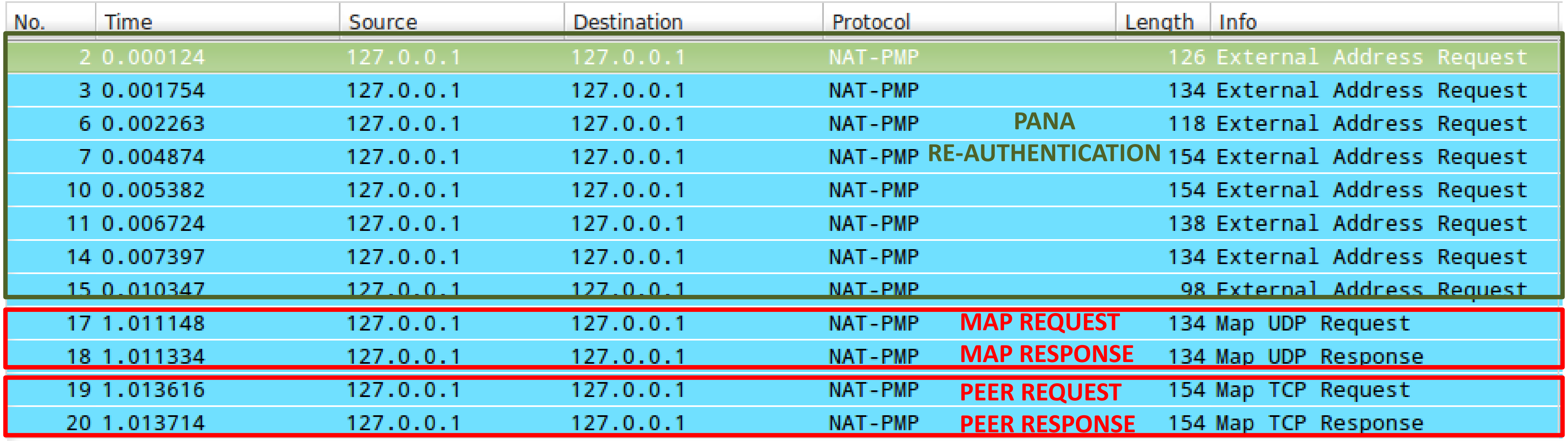
MAP RESPONSE

PEER REQUEST

PEER RESPONSE

Packet Capture

(PCP SA reestablishment – PANA re-auth initiated by PAA)



No.	Time	Source	Destination	Protocol	Length	Info
2	0.000124	127.0.0.1	127.0.0.1	NAT-PMP	126	External Address Request
3	0.001754	127.0.0.1	127.0.0.1	NAT-PMP	134	External Address Request
6	0.002263	127.0.0.1	127.0.0.1	NAT-PMP	118	External Address Request
7	0.004874	127.0.0.1	127.0.0.1	NAT-PMP	154	External Address Request
10	0.005382	127.0.0.1	127.0.0.1	NAT-PMP	154	External Address Request
11	0.006724	127.0.0.1	127.0.0.1	NAT-PMP	138	External Address Request
14	0.007397	127.0.0.1	127.0.0.1	NAT-PMP	134	External Address Request
15	0.010347	127.0.0.1	127.0.0.1	NAT-PMP	98	External Address Request
17	1.011148	127.0.0.1	127.0.0.1	NAT-PMP	134	Map UDP Request
18	1.011334	127.0.0.1	127.0.0.1	NAT-PMP	134	Map UDP Response
19	1.013616	127.0.0.1	127.0.0.1	NAT-PMP	154	Map TCP Request
20	1.013714	127.0.0.1	127.0.0.1	NAT-PMP	154	Map TCP Response

PANA RE-AUTHENTICATION

MAP REQUEST

MAP RESPONSE

PEER REQUEST

PEER RESPONSE

Additional Overhead

	Additional lines of code to support PCP	Note
Openpana	100	PCP Key derivation and export. Unix Sockets.
Cpana (libcpana)	200	PCP Key derivation and export.

How Close Are We with the PCP authentication requirements?

REQ #	Description (draft-reddy-pcp-auth-req-00)	pcp-{base,pana} specifications	Our prototype
1	Client authentication (PCP Client = host or proxy)	✔	✔
2	PCP server to indicate the need for authentication	✔	✔
3	PCP client must be able to verify authenticated unsolicited response	✔	✔
4	PCP server sends unsolicited authenticated response	✔	✔
5	Server-initiated re-authentication after PCP SA has expired	✔	✔
6	Authenticated PCP client must verify all authenticated unsolicited response	✔	✔
7	No trust of unauthenticated message	✔	✔
8	Identity confidentiality	✔	To be implemented
9	Optional PCP message confidentiality (*)	-	-
10	Immune to passive dictionary attacks	✔	✔
11	No guessable SA	✔	✔
12	Multiplexing authentication and PCP messages over the same port	✔	✔
13	Accommodating authentication between administrative domains	✔	✔ (not tested)
14	Functional across NAT	✔	✔ (not tested)
15	Proxy to validate PCP message	✔	To be implemented
16	Proxy to ensure PCP message integrity	✔	To be implemented
17	SA sharing among multiple PCP clients on the same host (*)	-	-
18	Choose a widely deployed authentication technique	✔	✔
19	Minimal change to PCP	✔	✔

*) New functionality introduced after draft-ohba-pcp-pana-03 was published

Future Plan

- PCP Proxy support
- Identity confidentiality support
- Support for new functionalities (e.g.,REQ-9,17) once defined
- Address missing functionalities (such as group SA for multicast ANNOUNCE response)

Conclusion

- PANA-based PCP authentication solution is simple and it is inter-operable
  - With minimal changes to PCP
- PCP authentication support requires only minimal change (100 to 200 LoC) to existing open-source PANA implementations
- PANA-based PCP authentication solution can easily meet all proposed PCP authentication requirements

Acknowledgment

The authors gratefully acknowledge the support of

- Prof. Antonio F. Skarmeta (Univ. of Murcia)
- Yasuyuki Tanaka (Toshiba)
- Alper Yegin (Samsung)