

free5GCのSignalingを end-to-endで解析してみた

2021年4月13日

Open Mobile Network Infra
Community Japan #2

Muneaki Ogawa (@nickel0)

自己紹介、発表背景、内容

■ 自己紹介

- 小川 宗晃 (Muneaki Ogawa)
- NTT NS研 → 楽天モバイル → ソラコム (SWE)
- 3GPPのArchitectureやSignaling (C-Plane)周りが好きです

■ 発表背景

- 前回OMNI#1に参加してfree5GCやmagmaなどのパケットコアのOSSがあることを知り自分でも動かしてみたくなった（なので全くの初心者ですw）
- 3GPPの5GS仕様※は過去にそれなりに読み込んだ経験があるので、仕様まわりでこのコミュニティに貢献できればいいなと思い発表してみることにした

※ TS 23.501~TS 23.503、TS 24.501、TS 33.501、TS 29.50xあたり

■ 話す内容

- free5GCとUERANSIMの環境構築からパケットキャプチャ、解析の始め方
- パケットの解析と3GPP仕様を元にしたend-to-end Signalingの解説
(今回はRegistrationが中心)

■ 対象者

- free5GC初心者でパケットキャプチャしてみたい人
- 5GSはなんとなく知っているが理解を深めたい人

free5GCのセットアップとパケットキャプチャ

■ セットアップ

- EC2インスタンスを2台準備
- [free5GC Stage 3 Installation Guide](#)に従いfree5GCとUERANSIMをセットアップ

■ パケットキャプチャ

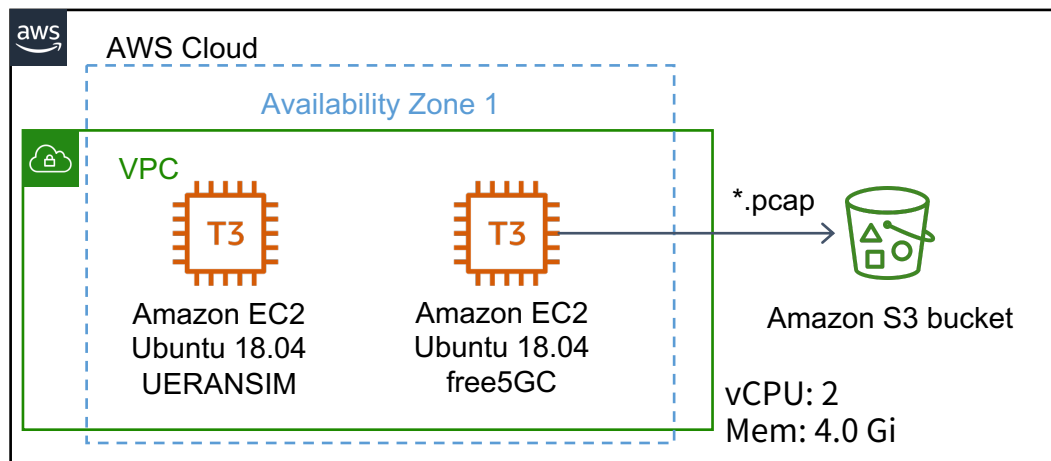
- free5GC側のインスタンスで取得（UERANSIMからのパケットと5GC内のSBIのパケットの両方が取得できるため）

```
sudo tcpdump -U -w "/var/tmp/${hostname}-${Y%m%d}-${H%M%S}.pcap" -n -i any
```

- 取得したパケットはS3バケットに貯めてダウンロード

```
aws s3 sync /var/tmp/ s3://free5gc-dev-tcpdump/ --include '*.pcap'
github.com/nickel0/5gs-call-flow
```

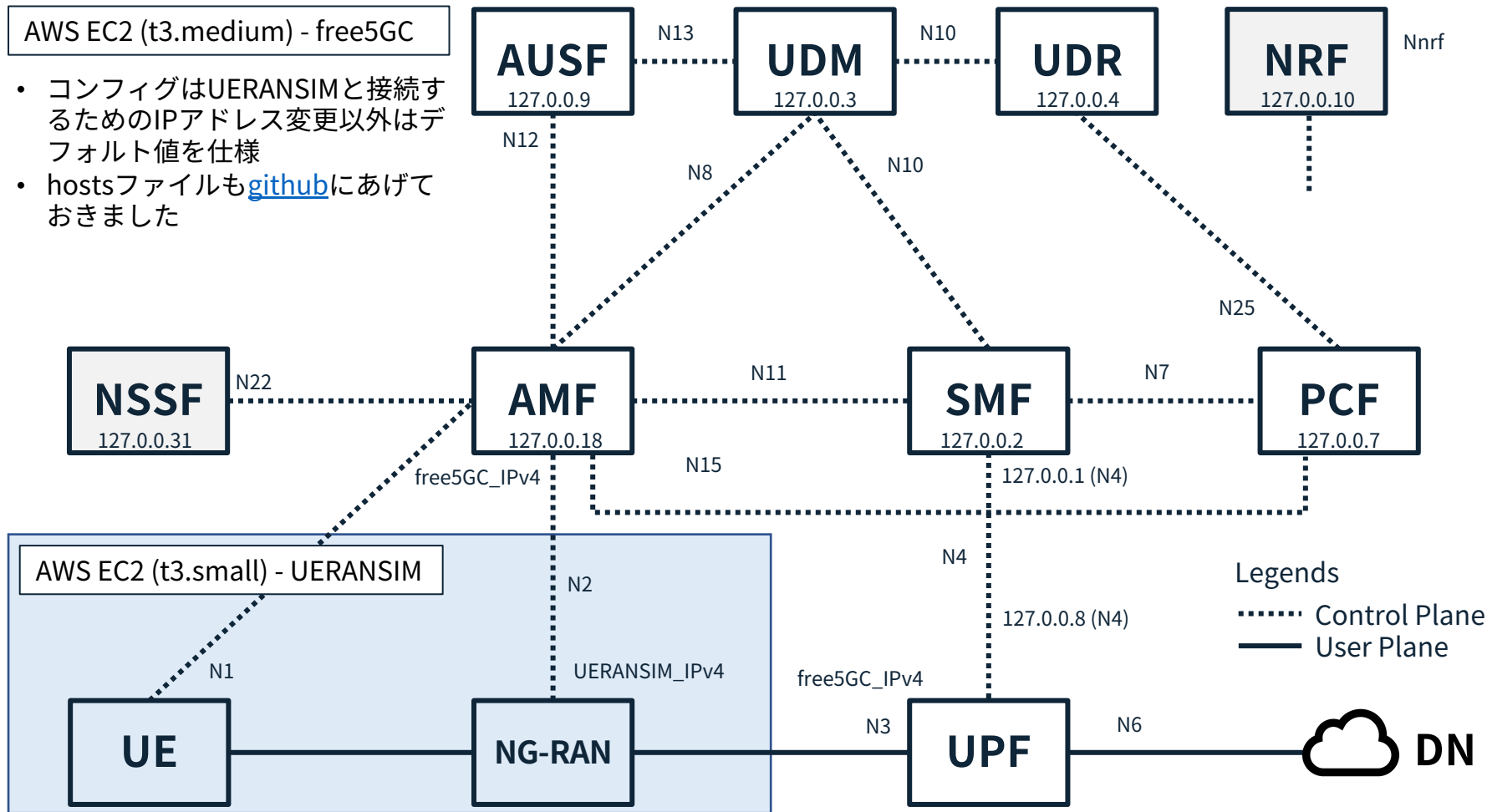
「自分で直ぐにpcapを見たい！」という方のために[こちら](#)においておきました。



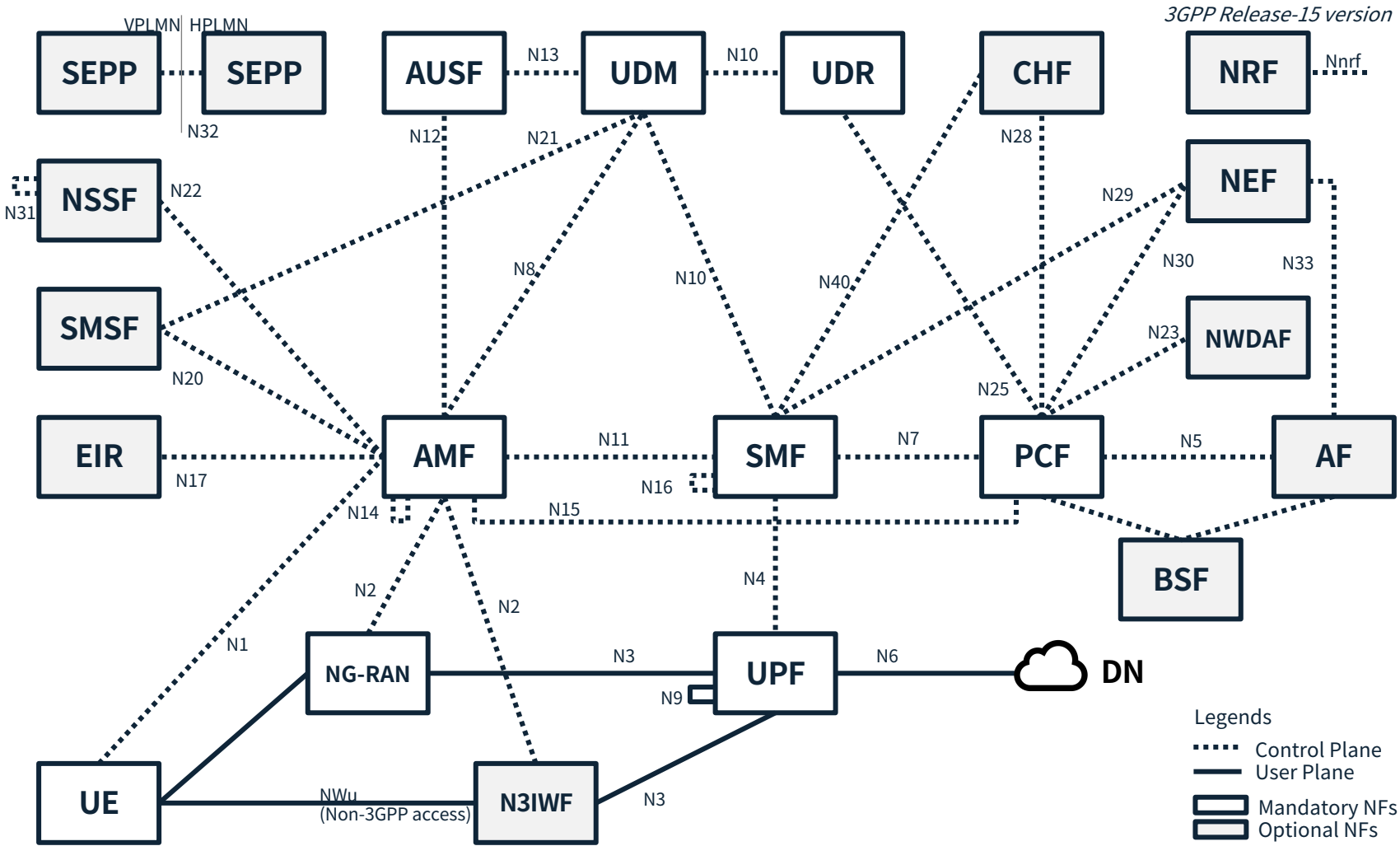
5GSアーキテクチャと今回の環境との対応

AWS EC2 (t3.medium) - free5GC

- コンフィグはUERANSIMと接続するためのIPアドレス変更以外はデフォルト値を仕様
- hostsファイルも[github](#)にあげておきました



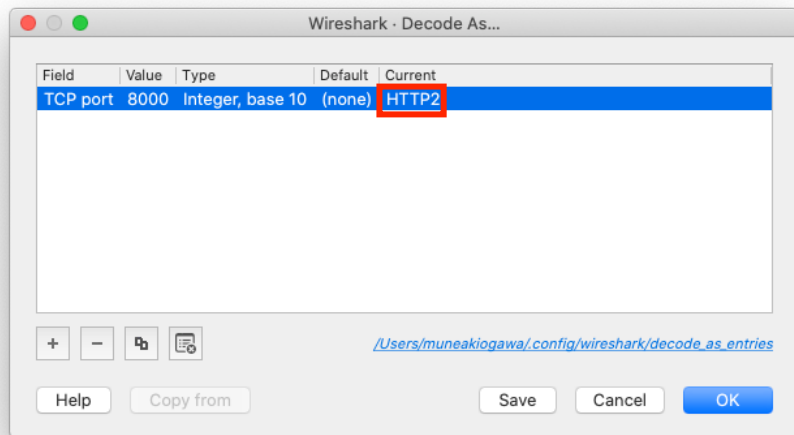
3GPP Release-15 5GS Reference Architecture



[事前準備] HTTP/2のデコード

- Wiresharkでhttp2でフィルタをかけて何も表示されない場合は、デコードの設定を確認。TCP port 8000をHTTP2としてデコードするように設定する。
- free5GCはデフォルトではHTTPSは使用しないコンフィグになっている。HTTPSを使う場合、keylogファイルをWireshark側への設定が必要。
 - free5GCが生成するkeylogファイルは[こちら](#)を参照

SMFのコンフィグファイル例

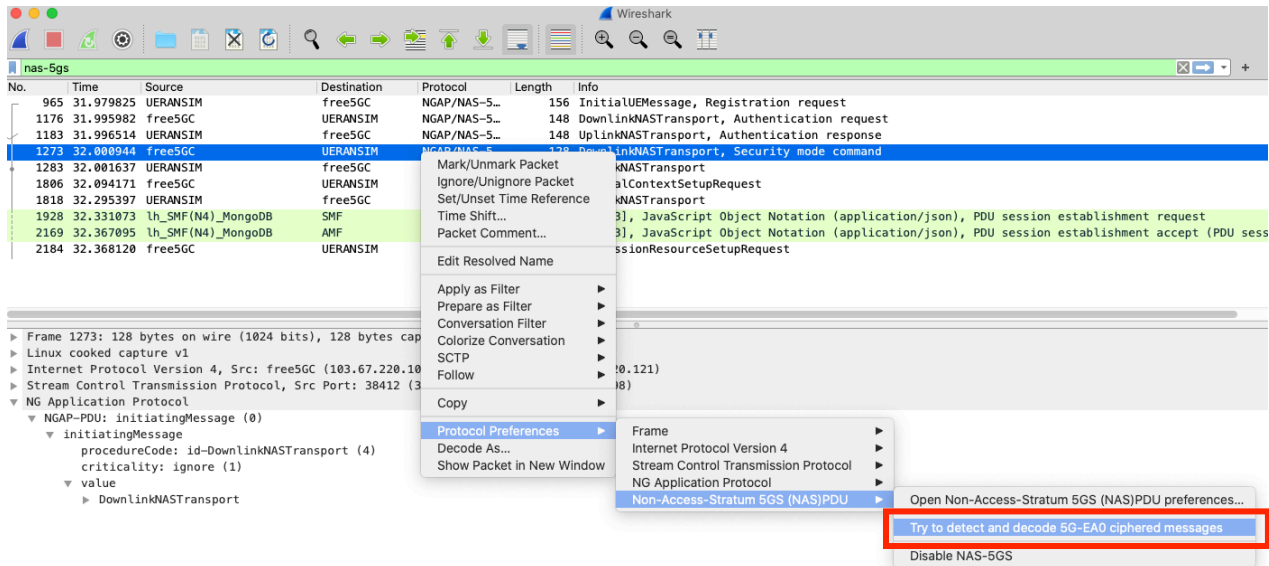


```
ubuntu@ip-103-67-220-102:~/free5gc/config$ cat smfcfg.yaml
info:
  version: 1.0.0
  description: SMF initial local configuration

configuration:
  smfName: SMF # the name of this SMF
  sbi: # Service-based interface information
    scheme: http # the protocol for sbi (http or https)
    registerIPv4: 127.0.0.2 # IP used to register to NRF
    bindingIPv4: 127.0.0.2 # IP used to bind the service
    port: 8000 # Port used to bind the service
  tls: # the local path of TLS key
    key: free5gc/support/TLS/smf.key # SMF TLS Certificate
    pem: free5gc/support/TLS/smf.pem # SMF TLS Private key
  ...
```

[事前準備] 暗号化NAS(5G-EA0)のデコード

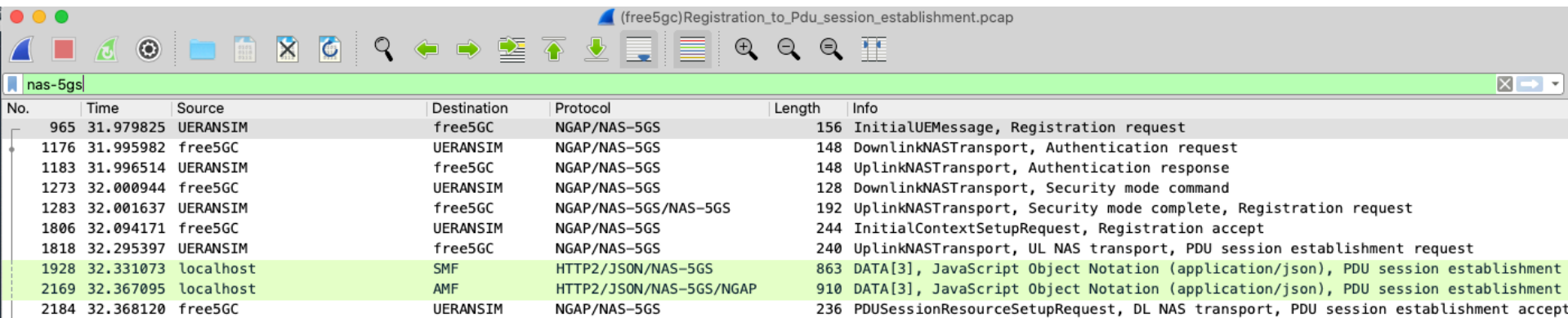
- UERANSIMとfree5GC間ではデフォルトではNASの暗号化アルゴリズムに5G-EA0 (NEA0)を適用。
 - 5G-EA0はNull Ciphering Algorithmで、値が全て"0"のKEYSTREAM（長さはinput parameter と等しい）を生成する。暗号化していないのと同様。(see TS 33.501 Annex D)
- Wiresharkはデフォルトでは暗号化NAS(5G-EA0)のデコードはdisableなため、enableにする。



(注) 試験環境は5G-EA0でもいいですが、商用環境では使わないことをお勧めします。

UERANSIM-free5GC間のNASのパケット

- 先ずはNASのパケットを確認してみる
- "nas-5gs"でフィルタリングすると

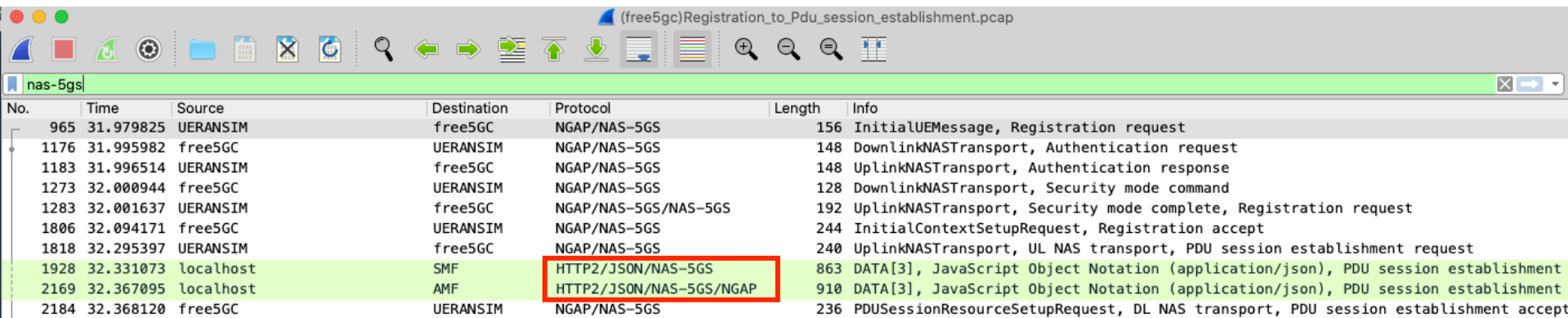


The image shows a Wireshark packet capture window titled "(free5gc)Registration_to_Pdu_session_establishment.pcap". The filter bar contains "nas-5gs". The packet list table below shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
965	31.979825	UERANSIM	free5GC	NGAP/NAS-5GS	156	InitialUEMessage, Registration request
1176	31.995982	free5GC	UERANSIM	NGAP/NAS-5GS	148	DownlinkNASTransport, Authentication request
1183	31.996514	UERANSIM	free5GC	NGAP/NAS-5GS	148	UplinkNASTransport, Authentication response
1273	32.000944	free5GC	UERANSIM	NGAP/NAS-5GS	128	DownlinkNASTransport, Security mode command
1283	32.001637	UERANSIM	free5GC	NGAP/NAS-5GS/NAS-5GS	192	UplinkNASTransport, Security mode complete, Registration request
1806	32.094171	free5GC	UERANSIM	NGAP/NAS-5GS	244	InitialContextSetupRequest, Registration accept
1818	32.295397	UERANSIM	free5GC	NGAP/NAS-5GS	240	UplinkNASTransport, UL NAS transport, PDU session establishment request
1928	32.331073	localhost	SMF	HTTP2/JSON/NAS-5GS	863	DATA[3], JavaScript Object Notation (application/json), PDU session establishment
2169	32.367095	localhost	AMF	HTTP2/JSON/NAS-5GS/NGAP	910	DATA[3], JavaScript Object Notation (application/json), PDU session establishment
2184	32.368120	free5GC	UERANSIM	NGAP/NAS-5GS	236	PDUResourceSetupRequest, DL NAS transport, PDU session establishment accept

UERANSIM-free5GC間のNASのパケット

- 先ずはNASのパケットを確認してみる
- "nas-5gs"でフィルタリングすると



(free5gc)Registration_to_Pdu_session_establishment.pcap

nas-5gs

No.	Time	Source	Destination	Protocol	Length	Info
965	31.979825	UERANSIM	free5GC	NGAP/NAS-5GS	156	InitialUEMessage, Registration request
1176	31.995982	free5GC	UERANSIM	NGAP/NAS-5GS	148	DownlinkNASTransport, Authentication request
1183	31.996514	UERANSIM	free5GC	NGAP/NAS-5GS	148	UplinkNASTransport, Authentication response
1273	32.000944	free5GC	UERANSIM	NGAP/NAS-5GS	128	DownlinkNASTransport, Security mode command
1283	32.001637	UERANSIM	free5GC	NGAP/NAS-5GS/NAS-5GS	192	UplinkNASTransport, Security mode complete, Registration request
1806	32.094171	free5GC	UERANSIM	NGAP/NAS-5GS	244	InitialContextSetupRequest, Registration accept
1818	32.295397	UERANSIM	free5GC	NGAP/NAS-5GS	240	UplinkNASTransport, UL NAS transport, PDU session establishment request
1928	32.331073	localhost	SMF	HTTP2/JSON/NAS-5GS	863	DATA[3], JavaScript Object Notation (application/json), PDU session establishment
2169	32.367095	localhost	AMF	HTTP2/JSON/NAS-5GS/NGAP	910	DATA[3], JavaScript Object Notation (application/json), PDU session establishment
2184	32.368120	free5GC	UERANSIM	NGAP/NAS-5GS	236	PDUSessionResourceSetupRequest, DL NAS transport, PDU session establishment accept

???



UERANSIM-free5GC間のNASのパケット

(free5gc)Registration_to_Pdu_session_establishment.pcap

nas-5gs

No.	Time	Source	Destination	Protocol	Length	Info
965	31.979825	UERANSIM	free5GC	NGAP/NAS-5GS	156	InitialUEMessage, Registration request
1176	31.995982	free5GC	UERANSIM	NGAP/NAS-5GS	148	DownlinkNASTransport, Authentication request
1183	31.996514	UERANSIM	free5GC	NGAP/NAS-5GS	148	UplinkNASTransport, Authentication response
1273	32.000944	free5GC	UERANSIM	NGAP/NAS-5GS	128	DownlinkNASTransport, Security mode command
1283	32.001637	UERANSIM	free5GC	NGAP/NAS-5GS/NAS-5GS	192	UplinkNASTransport, Security mode complete, Registration request
1806	32.094171	free5GC	UERANSIM	NGAP/NAS-5GS	244	InitialContextSetupRequest, Registration accept
1818	32.295397	free5GC	free5GC	NGAP/NAS-5GS	240	UplinkNASTransport, UL NAS transport, PDU session establishment request
1928	32.331073	localhost	SMF	HTTP2/JSON/NAS-5GS	863	DATA[3], JavaScript Object Notation (application/json), PDU session establishment
2169	32.367095	localhost	AMF	HTTP2/JSON/NAS-5GS/NGAP	910	DATA[3], JavaScript Object Notation (application/json), PDU session establishment
2184	32.368120	free5GC	UERANSIM	NGAP/NAS-5GS	236	PDU Session Resource Setup Request, DL NAS transport, PDU session establishment accept

- NAS-MMはAMFで終端
→ モビリティ管理を担当
- NAS-SMはSMFで終端
→ セッション管理を担当
- EPCではMMEで両方も終端されていたが5GCでは機能分担された

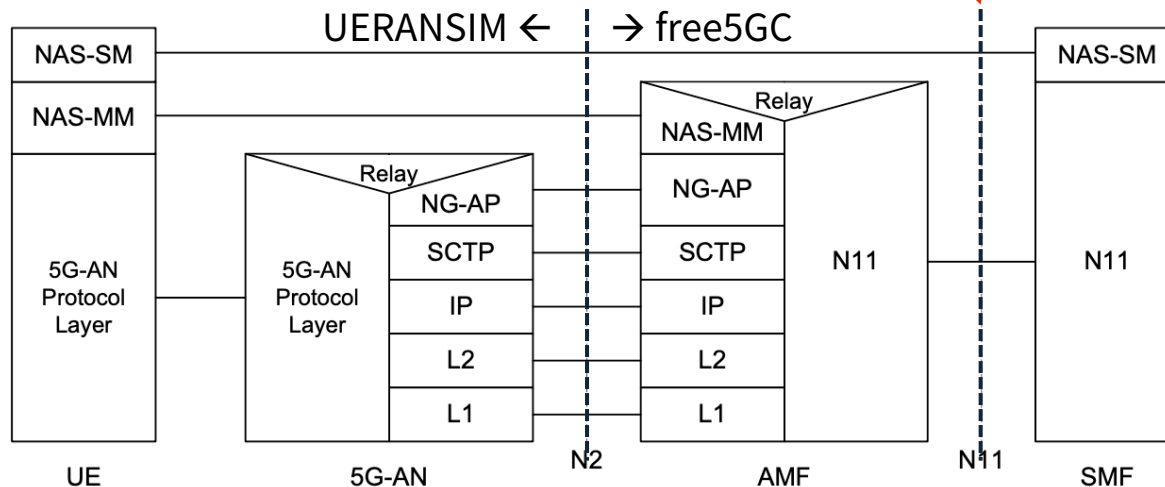


Figure 8.2.2.3-1: Control Plane protocol stack between the UE and the SMF

UERANSIM-free5GC間のNASのパケット

- SMFからのNAS-5GC, NGAPはMIME multipartでカプセル化されている

free5GC	UERANSIM	NGAP/NAS-5GS	244	IN
UERANSIM	free5GC	NGAP/NAS-5GS	240	Up
localhost	SMF	HTTP2/JSON/NAS-5GS	863	DA
localhost	AMF	HTTP2/JSON/NAS-5GS/NGAP	910	DA
free5GC	UERANSIM	NGAP/NAS-5GS	236	PD

▼ MIME Multipart Media Encapsulation, Type: multipart/related, Boundary: "54b2374a4b868c99680f447ca070c2dabc2ac94065b071a1851fe196e6bc"

[Type: multipart/related]

First boundary: --54b2374a4b868c99680f447ca070c2dabc2ac94065b071a1851fe196e6bc\r\n

▼ Encapsulated multipart part: (application/json)

Content-Type: application/json\r\n\r\n

▶ JavaScript Object Notation: application/json

Boundary: \r\n--54b2374a4b868c99680f447ca070c2dabc2ac94065b071a1851fe196e6bc\r\n

▼ Encapsulated multipart part: (application/vnd.3gpp.5gnas)

Content-Id: GSM_NAS\r\n

Content-Type: application/vnd.3gpp.5gnas\r\n\r\n

▶ Non-Access-Stratum 5GS (NAS)PDU

Boundary: \r\n--54b2374a4b868c99680f447ca070c2dabc2ac94065b071a1851fe196e6bc\r\n

▼ Encapsulated multipart part: (application/vnd.3gpp.ngap)

Content-Id: N2SmInformation\r\n

Content-Type: application/vnd.3gpp.ngap\r\n\r\n

▶ NG Application Protocol

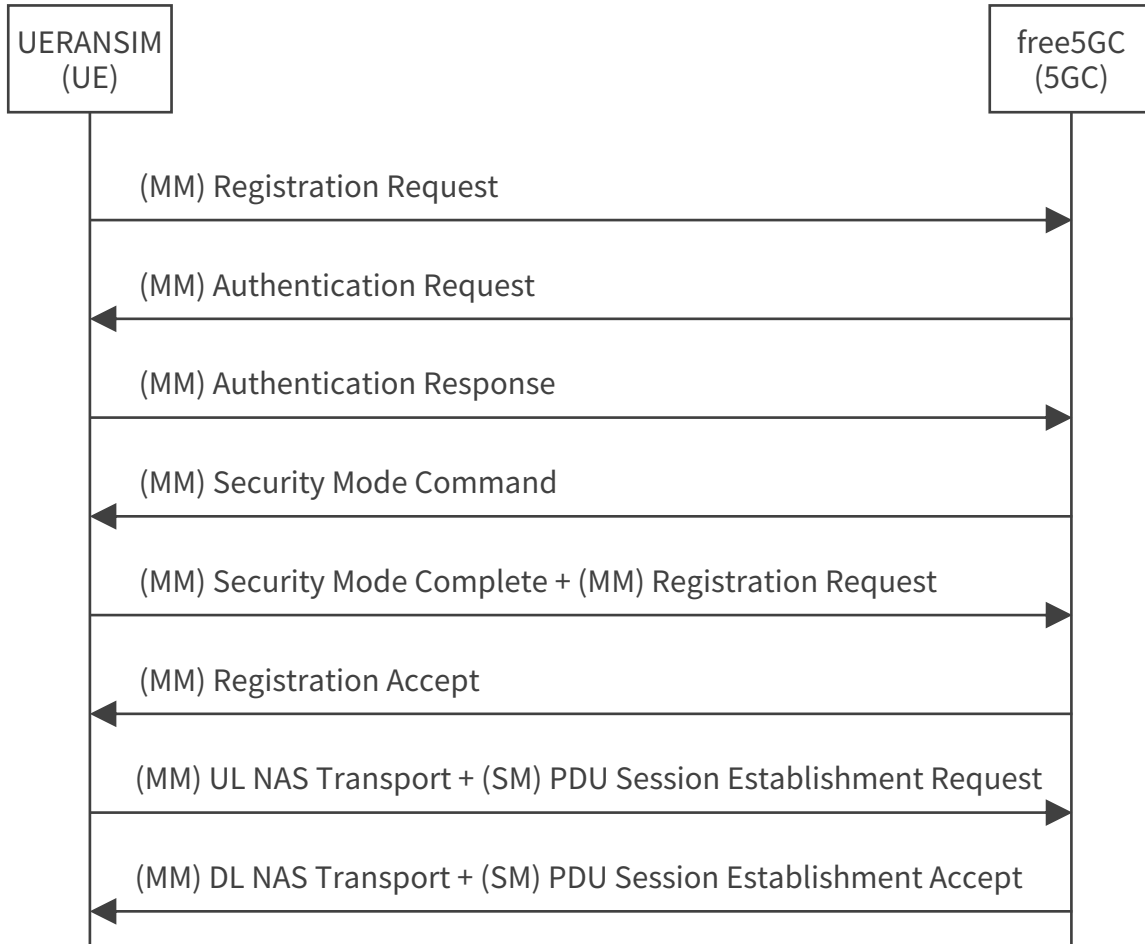
Last boundary: \r\n--54b2374a4b868c99680f447ca070c2dabc2ac94065b071a1851fe196e6bc--\r\n

JSON

NAS-5GS

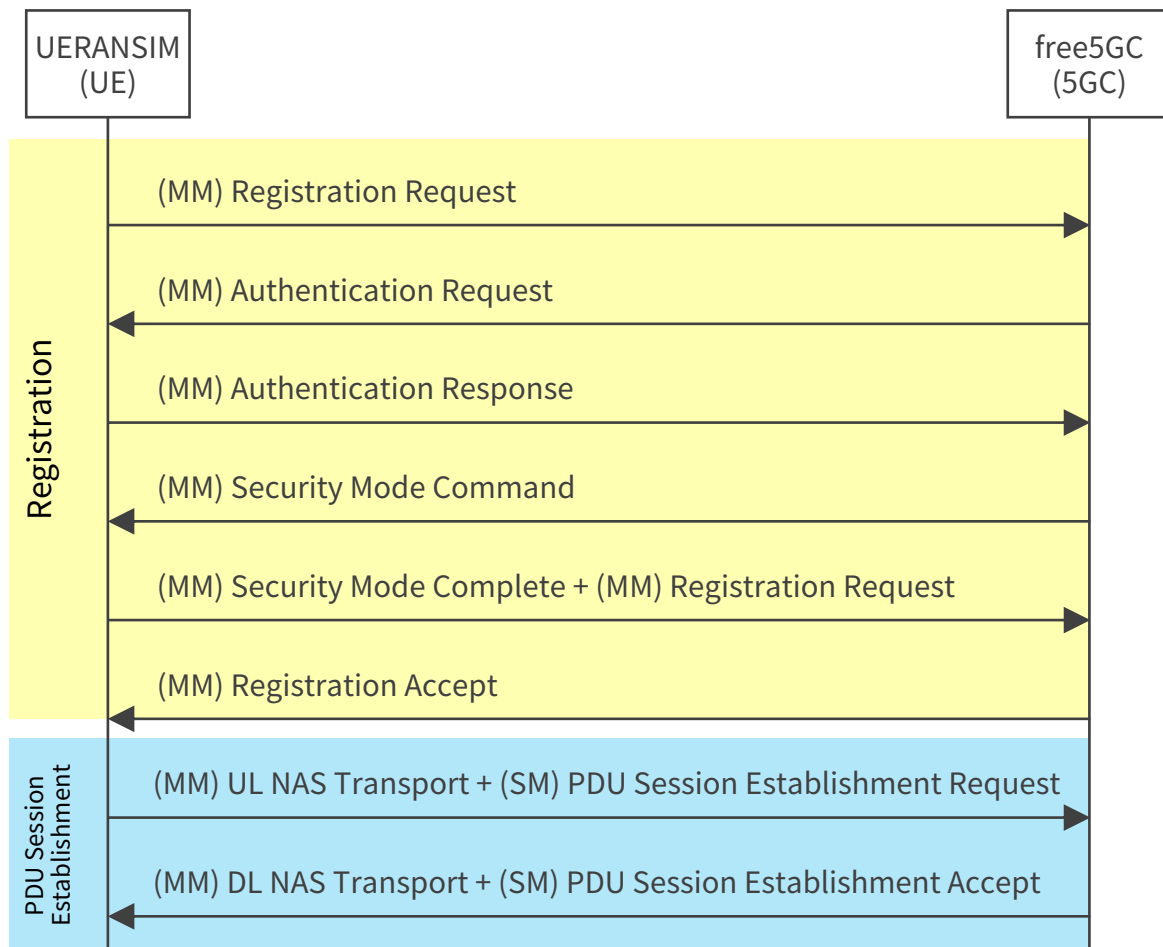
NGAP

UERANSIM-free5GC間のNASのコールフロー



HTTP2/JSON/NAS-5Gが何者かわかった。次に、UE - 5GC間のNASのコールフローに着目してみる

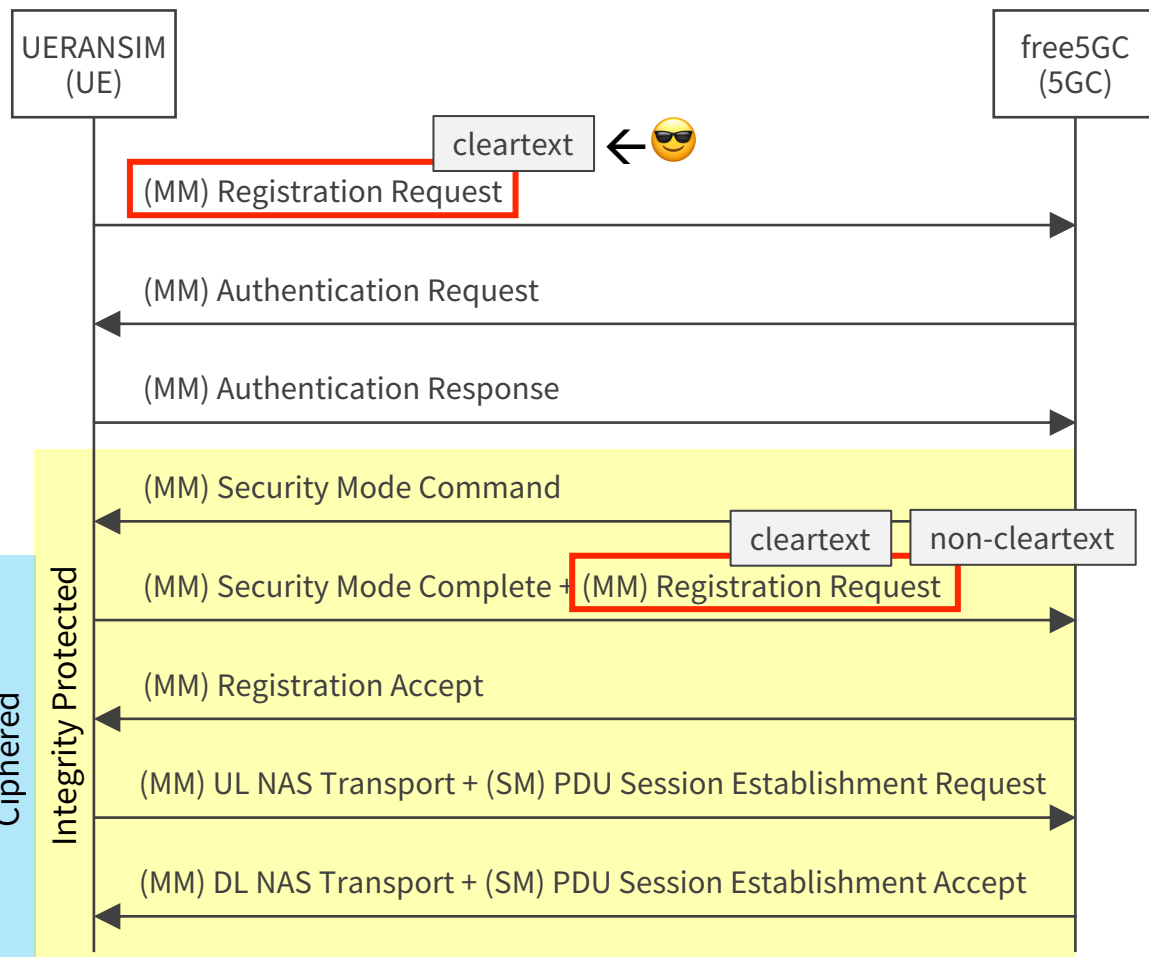
UERANSIM-free5GC間のNASのコールフロー



EPSからの大きな変更①

- EPSでは、認証/位置登録の手順とセッション確立を同時にリクエストすることができていた。
- 5GSでは、認証/位置登録の手順とセッション確立の手順が分離された。
- (IoT端末のような認証/位置登録はするがセッション確立は必要ないというケースを考慮)
- 確立したいPDUセッション毎にリクエストを送る。(InternetとIMSの2つのセッション確立するなら2回PDUセッション確立手順を行う)

UERANSIM-free5GC間のNASのコールフロー



EPSからの大きな変更②

- NASのRegistration Requestが2回送られている！？
- 1回目は暗号化されていないので中間者🕶️に盗み見られても構わない情報(cleartextという)しか送らない
→ Initial NAS Protection
- 2回目は暗号化されてから送る。ユーザ固有の情報など(non-cleartextという)も含めて送れる。
- Man in the middle attackされてもかまわないデザインになっている。
- EPSではIMSIを盗み見られるリスクがあったが5GSではそれを克服している。

Initial NAS Protection

1st NAS Registration Request

```
▼ NAS-PDU: 7e00417900d0102f8390000000000000000000000301001002e04f0f0f02f05040101020353...
▼ Non-Access-Stratum 5GS (NAS)PDU
  ▼ Plain NAS 5GS Message
    Extended protocol discriminator: 5G mobility management messages (126)
    0000 .... = Spare Half Octet: 0
    ... 0000 = Security header type: Plain NAS message, not security protected (0)
    Message type: Registration request (0x41)
  ▶ 5GS registration type
  ▶ NAS key set identifier
  ▶ 5GS mobile identity
  ▶ 5GMM capability
  ▶ UE security capability
  ▶ NSSAI - Requested NSSAI
  ▶ 5GS update type
```

TS 24.501 4.4.6 でRegistration Requestでのcleartext IEが定義されている。
それ以外のIEはnon-cleartext IEで、暗号化して送らなければならない。

- Extended protocol discriminator
- Security header type
- Spare half octet
- Registration request message identity
- 5GS registration type
- ngKSI
- 5GS mobile identity
- UE security capability
- Additional GUTI
- UE status
- EPS NAS message container.

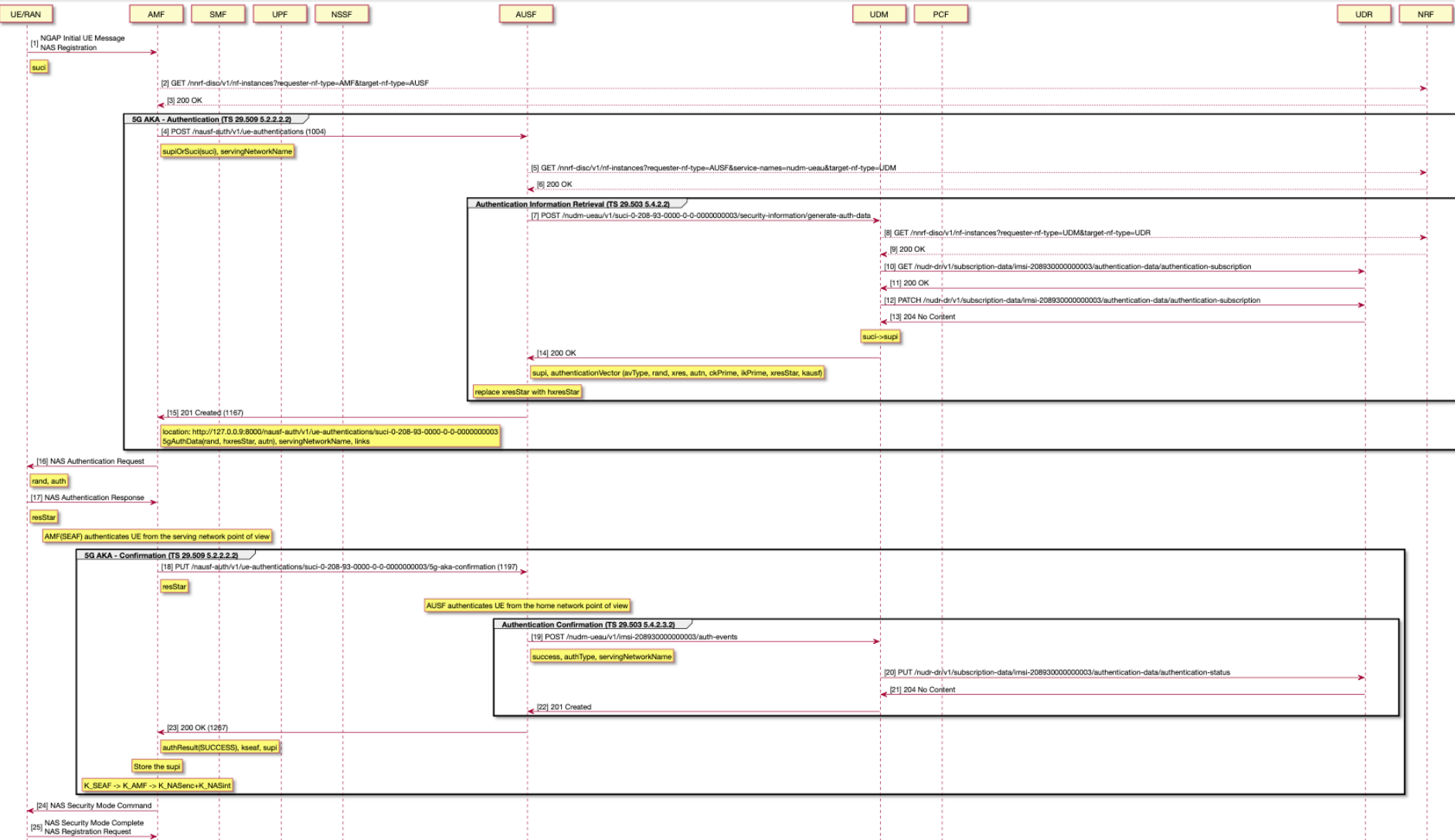
UERANSIMからの1st NAS Registration Requestにはnon-cleartextである5GMM capabilityとNSSAI - Requested NSSAIが含まれているが、これは3GPP標準違反

2nd NAS Registration Request

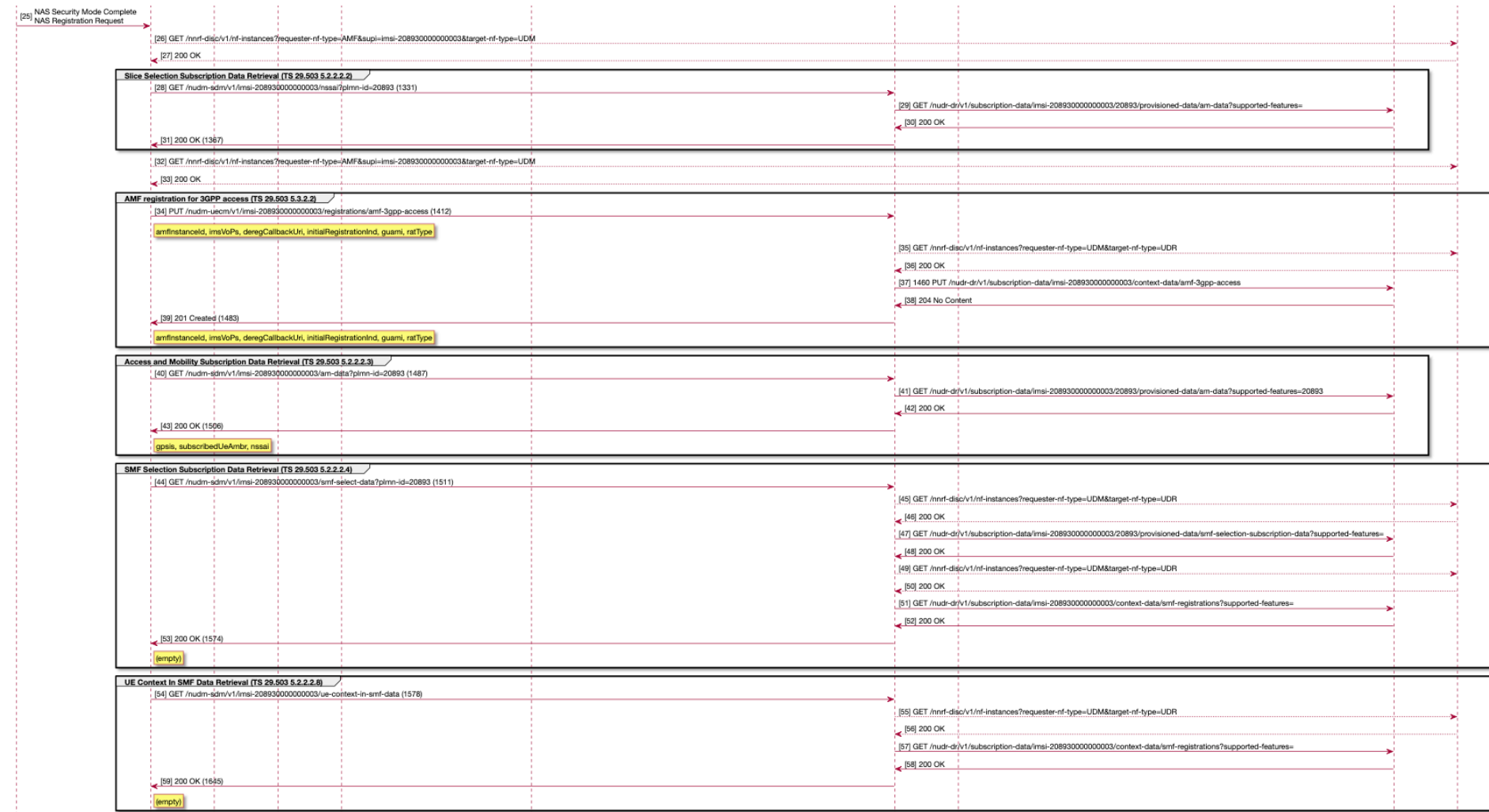
```
▼ NAS-PDU: 7e04dbfec568007e005e7700094573806121856151f17100267e00417900d0102f83900...
▼ Non-Access-Stratum 5GS (NAS)PDU
  ▼ Security protected NAS 5GS message
    Extended protocol discriminator: 5G mobility management messages (126)
    0000 .... = Spare Half Octet: 0
    ... 0100 = Security header type: Integrity protected and ciphered with new 5GS security co
    Message authentication code: 0xdbfec568
    Sequence number: 0
  ▼ Plain NAS 5GS Message
    Extended protocol discriminator: 5G mobility management messages (126)
    0000 .... = Spare Half Octet: 0
    ... 0000 = Security header type: Plain NAS message, not security protected (0)
    Message type: Security mode complete (0x5e)
  ▶ 5GS mobile identity
  ▼ NAS message container
    Element ID: 0x71
    Length: 38
  ▼ Non-Access-Stratum 5GS (NAS)PDU
    ▼ Plain NAS 5GS Message
      Extended protocol discriminator: 5G mobility management messages (126)
      0000 .... = Spare Half Octet: 0
      ... 0000 = Security header type: Plain NAS message, not security protected (0)
      Message type: Registration request (0x41)
    ▶ 5GS registration type
    ▶ NAS key set identifier
    ▶ 5GS mobile identity
    ▶ 5GMM capability
    ▶ UE security capability
    ▶ NSSAI - Requested NSSAI
    ▶ 5GS update type
```

Plain NAS messageとなっているが、暗号化されたNASの中のcontainerとして格納されているため暗号する必要がない。

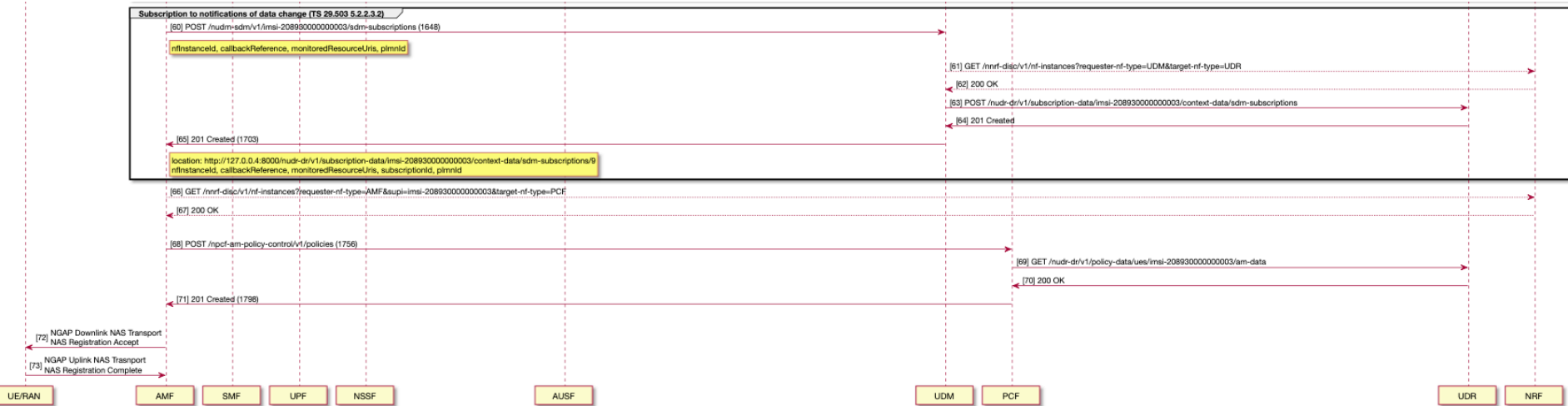
(参考) 5GS Registrationのend-to-end call flow(詳細版)



(参考) 5GS Registrationのend-to-end call flow(詳細版)



(参考) 5GS Registrationのend-to-end call flow(詳細版)



5GS Registrationのend-to-end call flow(簡略版)

- UERANSIM/free5GCのキャプチャを参考に作成
- 簡単にするためNRF、UDR、PCF、一部の信号などかなりいろいろ省略して大事なことだけ描いています。

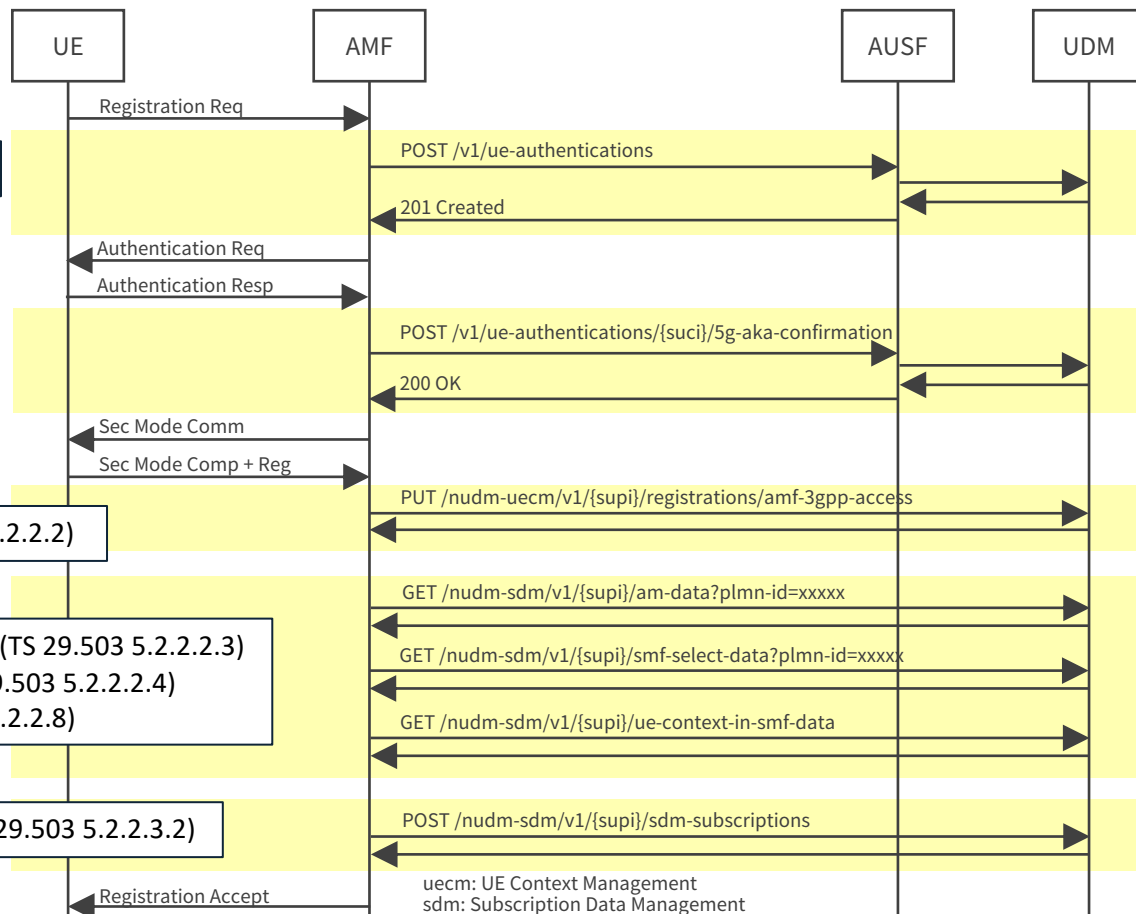
5G AKA - Authentication (TS 29.509 5.2.2.2.2)

5G AKA - Confirmation (TS 29.509 5.2.2.2.2)

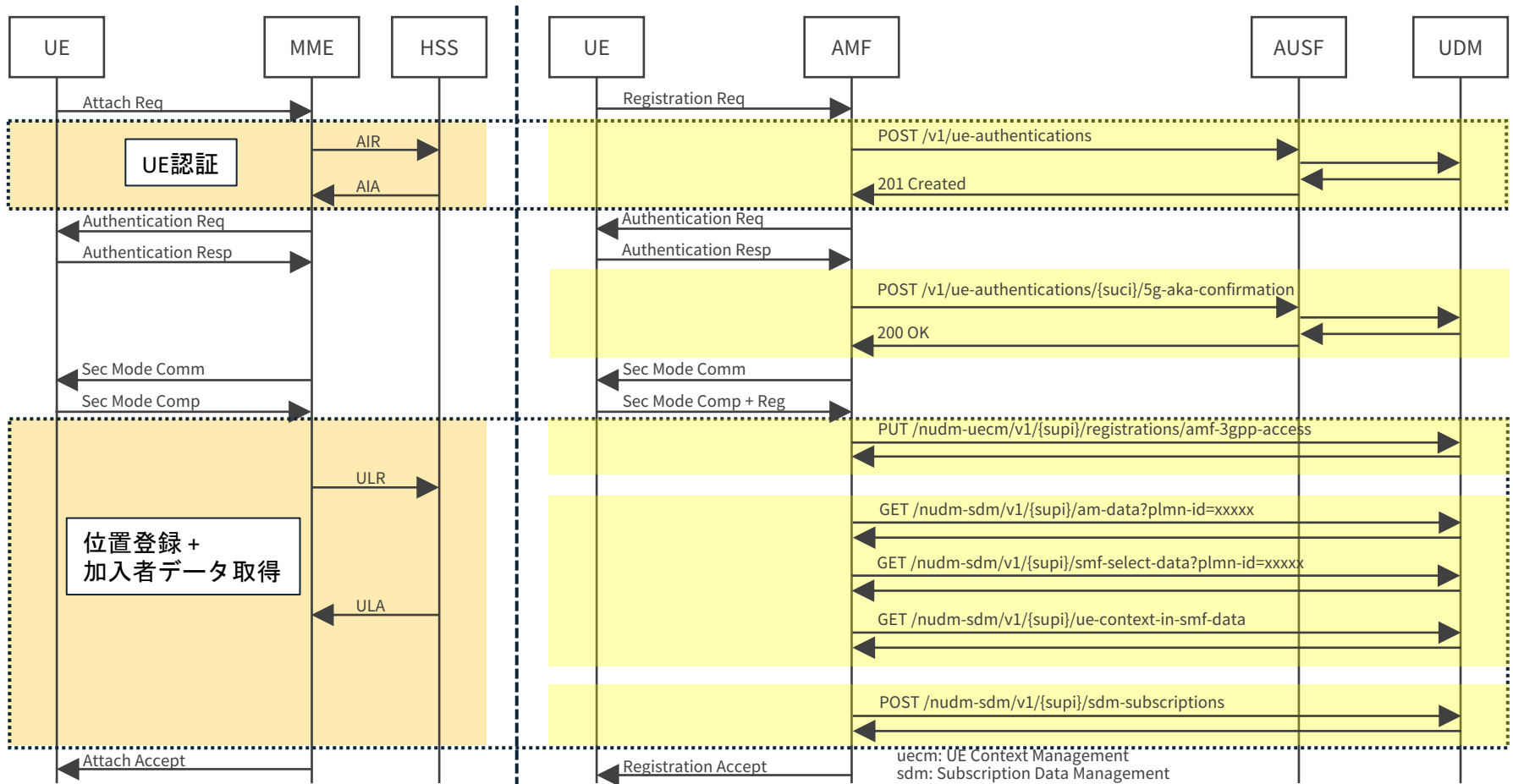
AMF registration for 3GPP access (TS 29.503 5.3.2.2.2)

Access and Mobility Subscription Data Retrieval (TS 29.503 5.2.2.2.3)
SMF Selection Subscription Data Retrieval (TS 29.503 5.2.2.2.4)
UE Context In SMF Data Retrieval (TS 29.503 5.2.2.2.8)

Subscription to notifications of data change (TS 29.503 5.2.2.3.2)



EPS Attachと5GS Registrationの比較



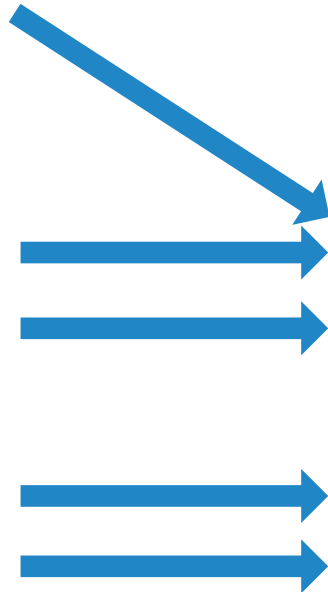
(参考) EPS NASと5GS NASのマッピング (一部)

TS 24.301 EPS NAS

- EMM common procedures
 - GUTI reallocation
- EMM specific procedures
 - Attach
 - Non-Emergency
 - Emergency
 - Tracking area updating
 - Mobility Update
 - Periodic Update

TS 24.501 5GS NAS

- 5GMM specific procedure
 - Registration 今回見たRegistration
 - Initial Registration
 - Emergency Registration
 - Mobility Update
 - Mobility Update
 - Periodic Update



Mastering 5GC Spec (仕様に強くなる！おすすめの勉強法)

5GCに詳しい人はまだ少ない気がします。以下は、おすすめの勉強の仕方です。

■ ステップ0

- 日本語の入門書(e.g. 5G教科書)や解説記事(e.g. ドコモのテクニカルジャーナル)等を見て雰囲気をつかむ。ここで新機能やコンセプトを理解しておくこと次のステップが楽になる。なお、ググって出てくる一般向けの情報は不正確な情報が多いのであまり見ないほうがよい。

■ ステップ1

- 3GPPのアーキテクチャ、動作仕様(Stage 2仕様)であるTS 23.501 ~ TS 23.503、TS 33.501を読む。Optionalな機能はひとまず読み飛ばしてOK。

■ ステップ3

- free5GCなど実際に動かしてキャプチャをしてみる。キャプチャとTS 23.502を平行して見てコールフローの大まかな流れと信号の役割を理解する。

■ ステップ4

- プロトコル仕様(Stage3仕様)であるTS 24.501やTS 29.5xx等を読む。ステップ3で取得したパケットをより詳細に解析したり、興味のある機能を深掘りしたりしてみる。

■ ステップ5

- ここまできたら、3GPPの最新のリリースや動向を追ってみたり、最近追加された機能を実装してOSS活動に貢献したり、いろいろできるようになると思います！

まとめ

■ 主な内容

- free5GCとUERANSIMの環境構築からパケットキャプチャ、解析の始め方
 - HTTP/2と暗号化NASのデコードの設定を忘れないように
- パケットキャプチャと3GPP仕様を元にしたend-to-end Signalingの解説(Registrationが中心)
 - Initial NAS Protectionと、RegistrationとPDU Session Establishmentの分離が特徴
 - Registrationを見た限りfree5GCの完成度は高そう

■ 今後も機会があれば話してみたいこと

- Registrationを中心に話したので次はPDU Session Establishmentを話したい。free5GC Stage3でサポートしれたULCLも試したい。
- 5G-AKAやSUCIなどセキュリティ周りも詳しく話したい。(個人的にはSEPPも気になる)
- まだfree5GC以外は動かしていないが他のも(magmaとか)比較してみたい。

■ さいごに

- コミュニティを通じて5GCに詳しい人とつながりたいです！
質問や議論したいことがあったらOMNIのSlackやtwitterで話しかけてくれると嬉しいです！