5G网络能力开放安全架构和流程研究

Research on Security Architecture and Procedure of 5G Network Capability Exposure

彭 健,李文彬,陈 丰(中国联通广东分公司,广东 广州 510627)
Peng Jian,Li Wenbin,Chen Feng(China Unicom Guangdong Branch,Guangzhou 510627,China)

摘 要:
5G网络能力开放的业务需求随着5G网络的规模商用正不断涌现,对网络能力开放的安全保障也逐渐成为运营商重点关注的问题,基于此,对5G网络能力开放的安全架构和流程进行了研究。首先,介绍了3GPP定义的网络能力开放框架CAPIF的相关功能实体和架构;其次,分析了CAPIF安全架构中各个接口的安全策略和流程,并对运营商针对各个接口的安全策略进行了建议;最后,对CAPIF安全架构的发展进行了展望。

关键词:
5G;能力开放;CAPIF;安全
doi:10.12045/j.issn.1007-3043.2023.04.003
文章编号:1007-3043(2023)04-0010-07
中图分类号:TN915.08
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
The business requirements of 5G network capability exposure are emerging with the scale commercialization of 5G networks, and the security of network capability exposure is becoming a key concern for operators. Based on this, the security architecture and procedure of 5G network capability exposure is studied. Firstly, the relevant functional entities and architecture of CAPIF which is a network capability exposure framework defined by 3GPP are introduced. Secondly, the security policies and procedures of interfaces in the CAPIF security architecture are analyzed, and the security policies of operators for interfaces are suggested. Finally, the development of the CAPIF security architecture is prospected.

Keywords:
5G;Network capability exposure;CAPIF;Security

引用格式:彭健,李文彬,陈丰. 5G网络能力开放安全架构和流程研究[J]. 邮电设计技术,2023(4):10-16.

1 概述

网络能力开放一直是移动通信网络的重要研究课题,也是实现5G网络即服务(Network as a Service,NaaS)目标的关键技术。为解决业内进行网络能力开放时缺乏权威标准的问题,避免各个运营商网络能力开放方法的不一致,并降低第三方业务提供商的应用开发难度,3GPP在R15标准中定义了通用API框架(Common API Framework,CAPIF)架构,对5G SA网络中的能力开放架构和流程进行了规定,并在R16的eCAPIF课题中对网络能力开放架构进行了加强。

随着5G业务的快速发展,5G与千行百业的结合正不断深入,网络能力开放的业务场景也不断涌现,随之而来的网络安全挑战也日益凸显,如何在开展网络能力开放的过程中充分保障网络侧和第三方应用侧的安全,已成为运营商重点关注的问题。因此,需要结合运营商网络的特点,对CAPIF的安全架构和安全策略流程进行研究,以便在实际部署中更好地实现

收稿日期:2023-03-02

其安全防护能力。

2 CAPIF架构

CAPIF是3GPP定义的标准能力开放架构，可以视为5G网络能力开放的基石，其架构如图1所示。

CAPIF架构的主要功能实体包括以下几项。

a）CAPIF核心功能（CAPIF Core Function），主要功能包括：

（a）对API使用者进行认证、授权。

（b）发布、存储和支持服务API信息的发现。

（c）配置/存储策略信息，从而控制服务API访问。

（d）存储服务API调用日志，向授权实体提供服务API调用日志。

（e）根据服务API调用日志进行收费。

（f）监控服务API调用。

（g）支持对访问日志进行审计。

b）API使用者（API Invoker）：需要调用5G网络能力的第三方应用程序，可以在PLMN可信域域内，也可以在域外。

c）API开放功能（API Exposing Function）：服务API的提供者，API Invoker到服务API通信的入口。

d）API发布功能（API Publishing Function）：进行服务API发布。

e）API管理功能（API Management Function）：监控、查询服务API的调用情况。

其中，属于5G核心网内部功能实体的包括CAPIF核心功能、API开放功能、API发布功能和API管理功能这4个功能实体。在实际部署时，这4个功能实体可以根据网络情况和实际需求进行合设或者分设，例如可以选择将这4个功能实体合设并体现为网络开放功能（Network Exposure Function，NEF），也可以将CAPIF核心功能单独设置，并将其他3个功能实体合设为NEF。

3 CAPIF安全架构

因为CAPIF架构肩负着对可信域外的第三方应用开放网络功能的职责，其安全防护的重要性也格外突出。针对CAPIF功能架构，3GPP定义的安全架构如图2所示。

CAPIF安全架构涉及的接口众多，总体上可以分为2类：可信域内通信接口和可信域外通信接口，前者包括CAPIF-1/2/3/4/5/7接口，后者包括CAPIF-1e/2e/3e/4e/5e/7e接口。针对这些接口，其总体安全要求包括以下几点。

a）支持双向认证。

b）消息传递需保证完整性和保密性，并能抵御重

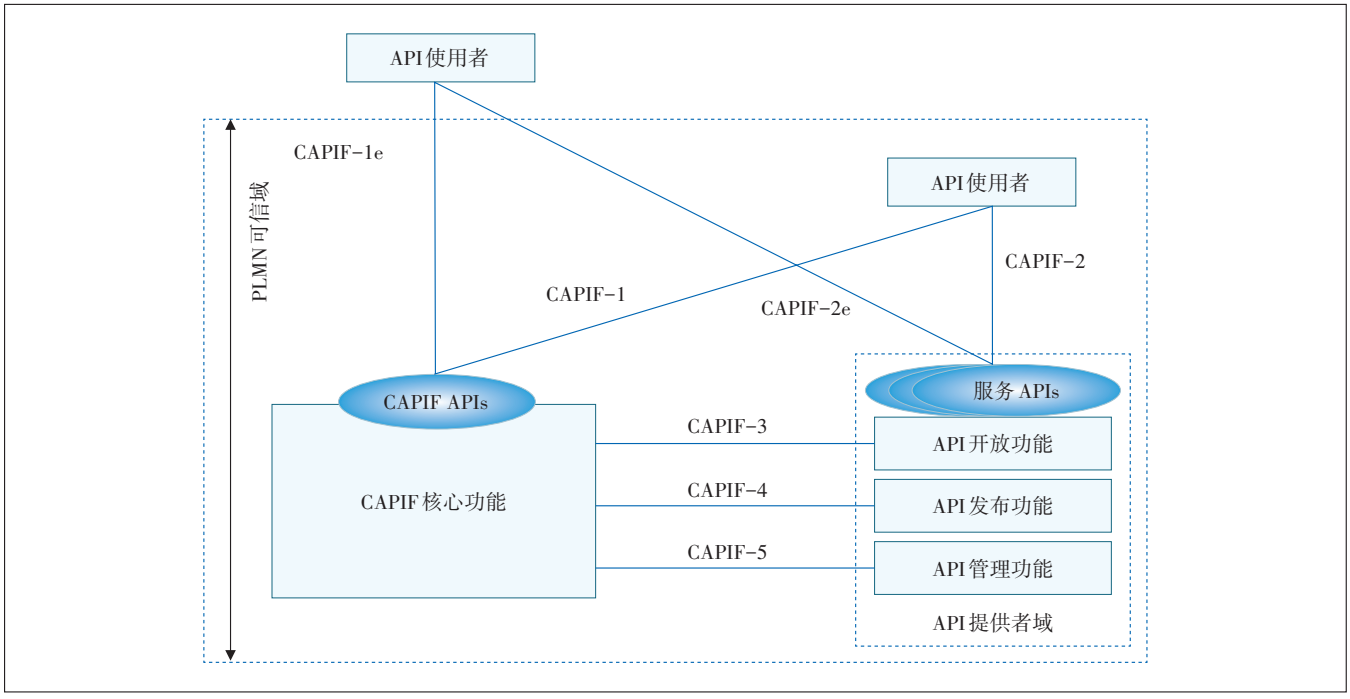

图1　CAPIF功能架构

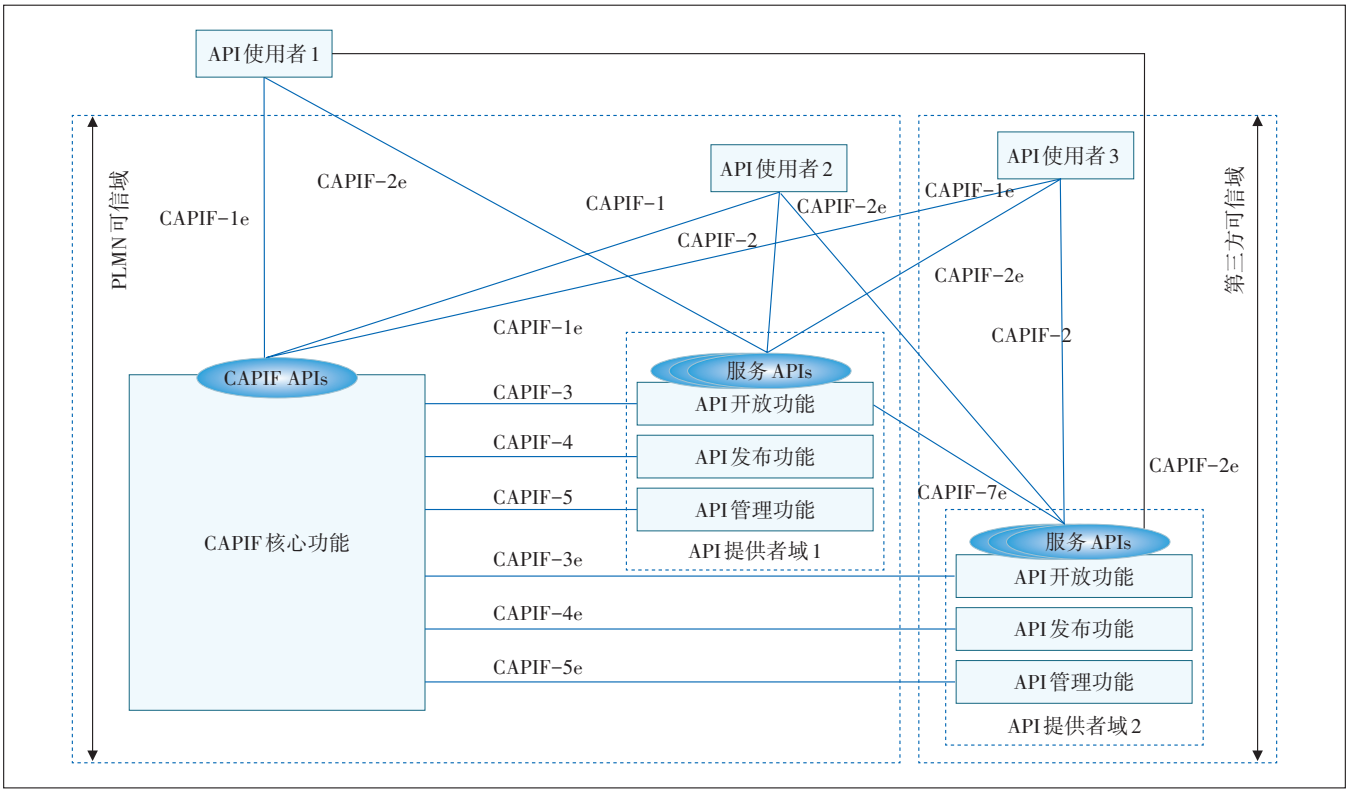

图2 CAPIF安全架构

放攻击。

c)需保证通信中的用户隐私。

这些接口采用的协议都是HTTPS/HTTP,因此,为满足上述安全要求,3GPP参考了互联网通信领域最为成熟的安全防护策略,要求CAPIF中所有接口都强制支持传输层安全性协议(Transport Layer Security,TLS)。

TLS对信息的安全传递主要基于3类算法:哈希函数、对称加密算法和非对称加密算法,其中,非对称加密算法用于身份认证和密钥协商,对称加密算法根据协商的密钥对数据进行加密,哈希函数用于验证信息的完整性。TLS中这3类算法的组合一般也被称为加密套件。

TLS协议采用Server-Client式架构模型,即通信的双方中,一方作为TLS服务端(TLS Server),另一方作为TLS客户端(TLS Client)。完成TLS通道建立后,TLS服务端和TLS客户端之间可以通过IP网络创建起安全的连接。TLS协议与上层的应用层协议(如HTTP、FTP、Telnet等)完全解耦,应用层协议能透明地运行在TLS协议之上,在TLS完成加密通道建立之后,所有应用层数据在通过加密通道发往对端时都会被加密,从而保证双方在通信时的数据完整性和保密性,并抵御重放攻击。

4 TLS通道建立流程

3GPP R16版本中,要求CAPIF安全架构涉及的接口必须支持目前主流的TLS 1.2和TLS 1.3版本,下面以基于TLS 1.2版本进行双向认证的TLS通道建立流程为例,说明TLS如何保证双方通信的安全性。TLS 1.2版本中,TLS客户端和TLS服务端需进行4次交互完成TLS通道建立,其流程如图3所示。

a)TLS客户端发起请求,TLS客户端向TLS服务端发送“Client Hello”消息,其中包含了本端TLS版本号、支持的加密套件和随机数1等信息。

b)TLS服务端回应请求,在双向认证的场景中,此部分包括5条消息。

(a)“Server Hello”消息:从“Client Hello”内的加密套件中选定一组用于后续密钥协商,并发送随机数2。

(b)“Certificate”消息:将自己的公钥证书发给客户端。

(c)“Server Key Exchange”消息:发送密钥协商算法的参数(也就是公钥)并包含签名认证。

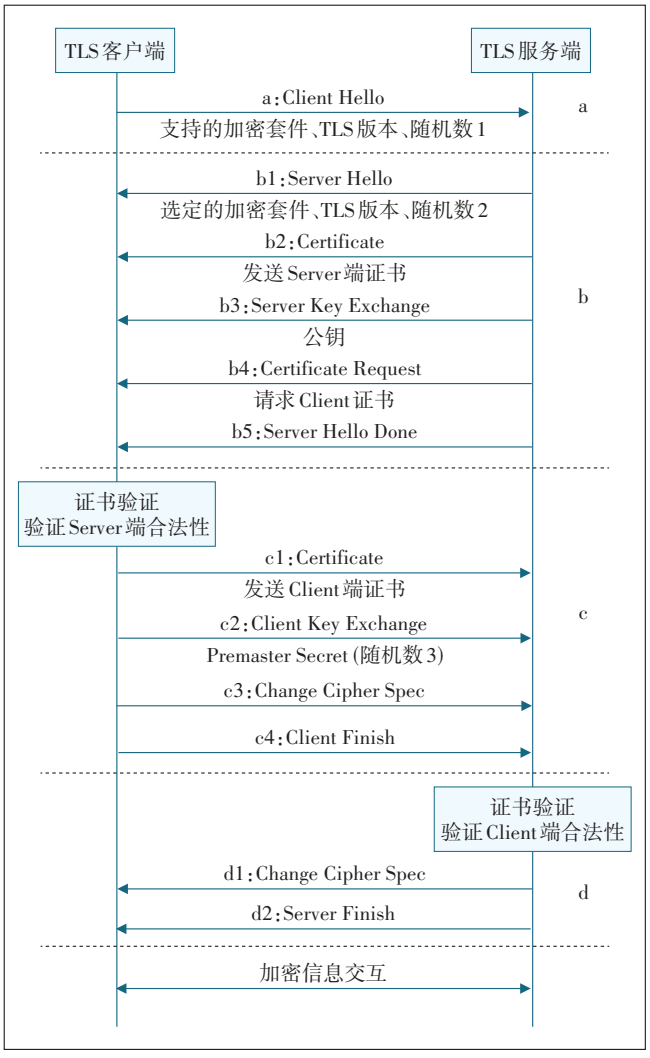

图3　TLS通道建立流程（1.2版本，双向认证）

（d）“Certificate Request”消息：向客户端请求证书进行验证。

（e）“Server Hello Done”消息：向客户端表示回应消息结束。

c）TLS客户端对接收到的服务端证书进行验证，验证通过后发送下列4条消息。

（a）“Certificate”消息：将自己的证书发给服务端。

（b）“Client Key Exchange”消息：客户端基于前面生成的随机数1和随机数2，生成随机数3，并使用Server发送的公钥对随机数3进行加密，加密后的随机数3即为预主密钥（Premaster Key），然后传送给服务端。

（c）“Change Cipher Spec”消息：基于随机数1、随机数2和随机数3，客户端侧已经能计算得到主密钥（Master Secrect），客户端通知服务端，后续消息都会使用主密钥进行加密。

（d）“Client Finish”消息：客户端将前面的协商消息生成摘要，再用主密钥进行加密，服务端接收后需要用自己生成的主密钥解密，若能正常解密，则表示协商成功。

d）TLS服务端对接收到的客户端证书进行验证，并完成通道建立，包含2条消息。

（a）“Change Cipher Spec”消息：服务端使用自己的私钥对接收到的预主密钥进行解密，得到随机数3，此时服务端也已可以基于随机数1，随机数2和随机数3计算得到主密钥，服务端通知客户端，后续消息都用主密钥进行加密。

（b）“Server Finish”消息：服务端将前面的协商消息生成摘要，再用主密钥进行加密，客户端接收后需要用自己生成的主密钥解密，若能正常解密，则表示协商成功。

至此，TLS客户端和TLS服务端间的加密通道建立完成，后续通信内容都将使用主密钥进行加密。因为公钥加密的数据只能通过私钥解密，在双方私钥安全的前提下，预主密钥和主密钥都具有极高的安全性，基本上不可能被第三方获得。因此，基于TLS通道的消息交互可以满足CAPIF架构的安全需求。

5 CAPIF安全架构相关接口的安全流程

5.1 CAPIF-1e和CAPIF-1接口安全流程

CAPIF-1e接口处于域外API使用者与CAPIF核心功能之间，在双方经过双向认证完成TLS通道建立之后，API使用者需要向CAPIF核心功能协商一个在后续的业务流程中用于CAPIF-2e接口认证和保护的策略。CAPIF-2e接口安全策略选择流程如图4所示。

a）API使用者使用在注册流程中获得的Client证书，完成TLS的通道建立。

b）API使用者在安全策略请求消息中向CAPIF核心功能发送自身支持的安全策略列表及其他辅助选择信息。

c）CAPIF核心功能基于API使用提供的信息、访问场景和AEF能力，选定CAPIF-2e接口使用的安全策略。

d）CAPIF核心功能向API使用者发送安全策略响应消息，明确选定的安全策略以及相应的安全策略信息，以便API使用者在后续CAPIF-2e接口的业务流程中使用。

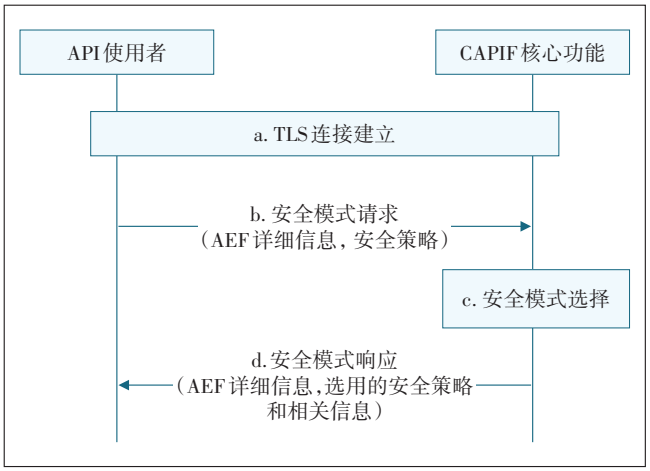

图4 CAPIF-2e接口安全策略选择流程

CAPIF-1e接口因为涉及与域外通信，其安全策略要求是强制性的。CAPIF-1接口处于域内API使用者与CAPIF核心功能之间，其安全要求和流程与CAPIF-1e一致，但是运营商可以决定是否启用相应的安全流程。

5.2 CAPIF-2e和CAPIF-2接口安全流程

CAPIF-2e接口处于域外API使用者与API开放功能(API Exposing Function，AEF)之间，在API使用者完成CAPIF-1e接口的安全认证后，需要与AEF建立TLS连接以保证业务流程的安全性。

基于CAPIF-1e业务流程中CAPIF核心功能选定的安全策略，此TLS连接可以通过3种方式建立，分别是TLS-PSK方式、TLS-PKI方式和TLS-OAuth token方式。

5.2.1 TLS-PSK方式

使用TLS-PSK方式进行CAPIF-2e接口安全认证的流程如图5所示。

a) CAPIF-1e认证和安全会话按照前文流程建立，CAPIF核心功能选定TLS-PSK策略并且同时提供密钥AEF_{PSK}的有效定时器值。

b) API使用者和CAPIF核心功能获取到与AEF一一对应的密钥AEF_{PSK}，并启动AEF_{PSK}的有效计时。

c) API使用者向AEF发送认证请求，里面应包含由CAPIF核心功能分配的API使用者ID。

d) AEF向CAPIF核心功能请求安全信息以执行认证。

e) CAPIF核心功能通过CAPIF-3接口向AEF提供与所选安全策略(TLS-PSK)有关的安全信息。此时，CAPIF核心功能应同时指示AEF_{PSK}的剩余有效计时。

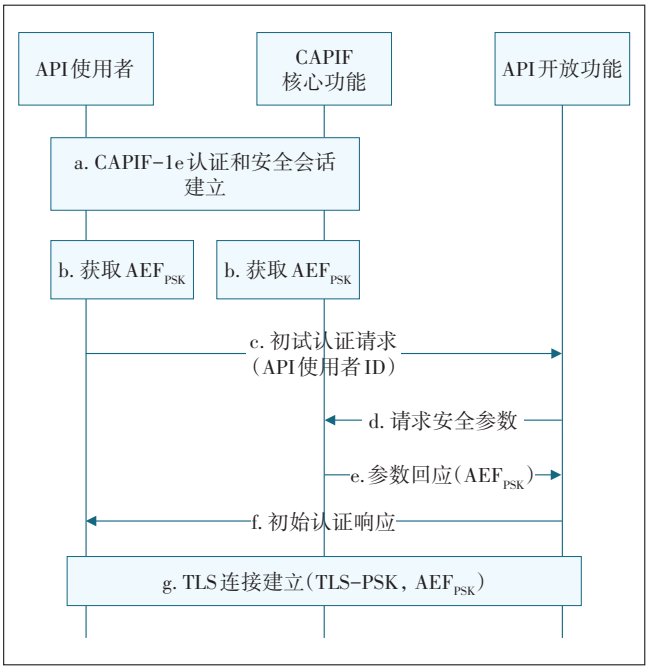

图5 CAPIF-2e接口安全认证流程(TLS-PSK方式)

f) 在获取相关安全信息(即AEF_{PSK})后，AEF回复认证请求响应消息，并启动TLS会话建立流程。AEF根据CAPIF核心功能指示的值，启动AEF_{PSK}的有效定时。

g) API使用者和AEF使用AEF_{PSK}进行相互认证，并建立CAPIF-2e接口的TLS会话。

5.2.2 TLS-PKI方式

使用PKI方式进行CAPIF-2e接口安全认证的流程如图6所示。

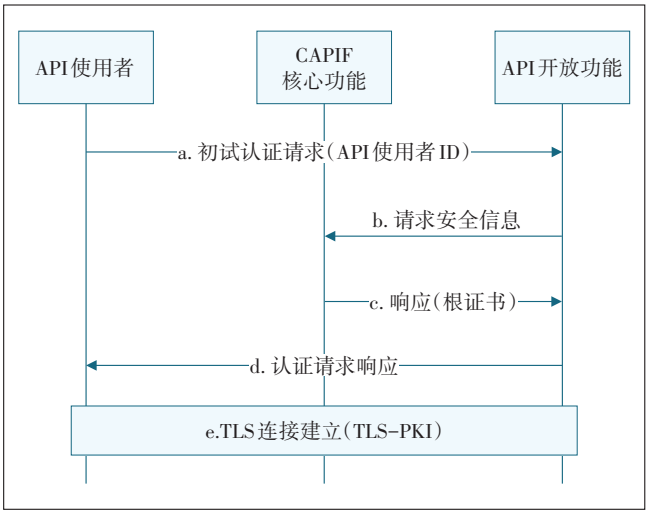

图6 CAPIF-2e接口安全认证流程(PKI方式)

a）API使用者向AEF发送认证请求，包括API使用者ID。

b）AEF向CAPIF核心功能请求安全信息以执行认证。

c）CAPIF核心功能通过CAPIF-3接口向AEF提供与所选安全策略（TLS-PKI）有关的安全信息和API使用者的根CA证书，以便AEF验证。

d）获取安全信息后，AEF向API调用者发送认证请求响应消息，以启动TLS会话建立流程。

e）API使用者和AEF基于证书进行相互认证，并通过CAPIF-2e建立TLS会话。

5.2.3　TLS-OAuth token

使用TLS-OAuth token方式进行CAPIF-2e接口安全认证的流程如图7所示。

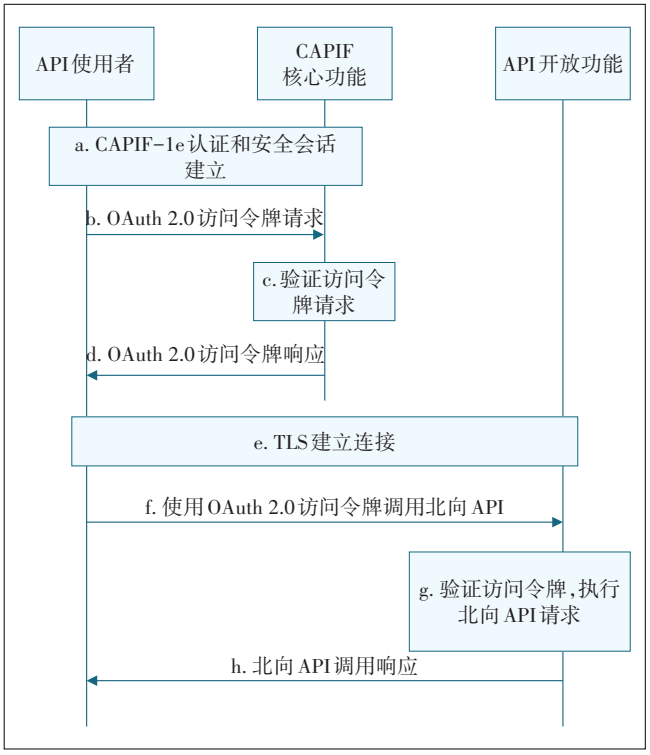

图7　CAPIF-2e接口安全认证流程（TLS-OAuth token方式）

a）CAPIF-1e认证和安全会话按照前文流程建立。

b）API使用者应按照OAuth 2.0规范向CAPIF核心功能发送访问令牌请求。

c）CAPIF核心功能应根据OAuth 2.0规范验证访问令牌请求。

d）如果访问令牌请求消息被成功验证，则CAPIF核心功能应生成API使用者专用的访问令牌，并在访问令牌响应消息中返回。

e）API使用者根据CAPIF核心功能指示的认证和授权方法，通过与AEF建立TLS会话来认证AEF。

f）对AEF认证成功后，API使用者应向AEF发起3GPP北向API的调用。根据OAuth 2.0协议，从CAPIF核心功能收到的访问令牌应与北向API调用请求一起发送。

g）AEF通过验证CAPIF核心功能的签名来验证访问令牌的完整性。如果访问令牌验证成功，AEF应根据访问令牌中的授权要求来验证API使用者的北向API调用请求，确保API使用者对请求的API具有访问权限。

h）在成功验证访问令牌和API使用者的授权要求后，应调用所请求的北向API，并向API使用者返回适当的响应。

CAPIF-2e接口因为涉及与域外通信，其安全策略要求是强制性的。CAPIF-2接口处于域内API使用者与AEF之间，其安全要求和流程与CAPIF-2e一致，但是运营商可以决定是否启用相应的安全流程。

5.3　CAPIF-3e/4e/5e和CAPIF-3/4/5接口安全流程

CAPIF-3e/4e/5e接口分别处于CAPIF核心功能与域外API开放功能、域外API发布功能和域外API管理功能之间。由于涉及与域外通信，其业务流程必须基于TLS建立的安全通道进行，通道建立流程遵循TLS 1.2和TLS 1.3的协议规定，其安全策略要求是强制性的。

CAPIF-3/4/5接口处分别于CAPIF核心功能与域内API开放功能、域内API发布功能和域内API管理功能之间。

对应的业务流程应支持基于TLS建立的安全通道进行，通道建立流程遵循TLS 1.2和TLS 1.3的协议规定。但是，因为不涉及域外通信，运营商可以决定是否启用相应的安全流程。

5.4　CAPIF-7e和CAPIF-7接口安全流程

CAPIF-7e接口处于域内AEF与域外AEF之间，其安全要求和流程与CAPIF-2e一致，因为涉及与域外通信，其安全策略要求是强制性的。

CAPIF-7接口处于域内AEF之间，其安全要求和流程与CAPIF-2一致，因为不涉及域外通信，运营商可以决定是否启用相应的安全流程。

5.5　实际部署时的安全策略选择建议

国内运营商在进行5G网络能力开放部署时，一般

会选择将CAPIF中的API开放功能、API发布功能和API管理功能合设为NEF,作为5G核心网对外提供开放API的统一入口。同时,部署5G网络能力开放平台,作为运营商向外部第三方应用开放网络能力的统一门户。CAPIF核心功能对API调用者的鉴权、授权、认证等功能由能力开放平台实现,图8给出了其组网示意。

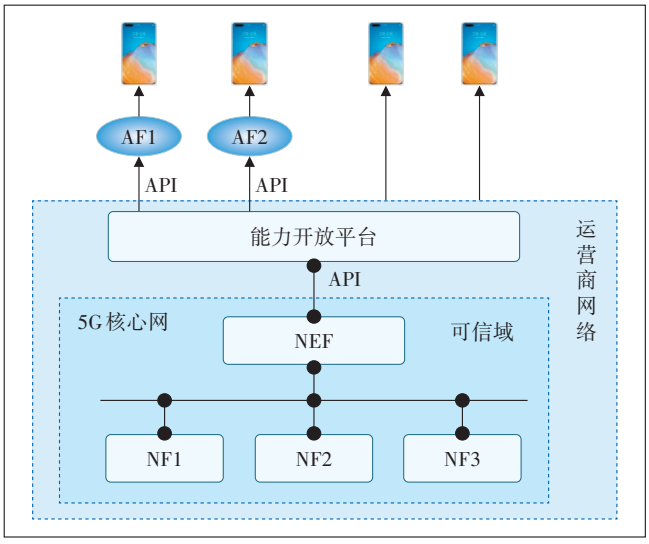

图8 能力开放平台部署示意

此部署方案下,NEF只需要与运营商网络内的能力开放平台进行对接,实现API开放。CAPIF的众多接口被收敛为NEF与能力开放平台之间的一个接口,因为该接口同处于运营商内部网络,接口安全可控度更高,通过前述TLS策略和流程即能充分保证安全。而API使用者也是与能力开放平台对接,完成5G网络能力的调用。能力开放平台作为IT平台,在向外部API调用者开放能力时,一方面可以更灵活地采用目前最先进的安全防护方案,例如在3GPP定义的安全策略之外叠加零信任网关等更多防护设备,实现更全面和完善的安全防护能力,另一方面,部署能力开放平台在运营方面也有利于运营商对网络开放的原子能力进行更灵活的编排和组合,提升能力销售时的价值。

6 结束语

3GPP对CAPIF安全架构的设计可以说已经比较完善,但是随着标准的推进以及5G网络能力开放业务的不断发展,新的接口和业务流程也将不断出现,随之而来的是新的安全挑战和防护需求,CAPIF安全架构需要不断演进,以满足各种场景下的防护需求。

运营商在3GPP的安全体系之外,可以视自己实际情况灵活地引入更多的安全防护手段,保障网络和业务安全,例如,中国联通定义了信令安全网关,用于5G专用网元等安全域外功能实体和5GC大网网元之间的信令面安全通信等业务场景,在能力开放场景中,第三方应用将API调用请求发送到NEF时,将通过信令安全网关接口拦截消息并进行安全筛选和策略应用,进一步提高了安全防护能力。

另外,随着国家对国密的推广,在CAPIF安全架构业务流程中引入国密,例如使用国密SSL对TLS进行替代,进一步加强其安全防护能力,也是未来的研究课题之一。

参考文献:

[1] 3GPP. System architecture for the 5G System(5GS):3GPP TS 23.501[S/OL].[2022-12-26]. ftp://ftp.3gpp.org/Specs/.
[2] 3GPP. Common API framework for 3GPP northbound APIs:3GPP TS 23.222[S/OL].[2022-12-26]. ftp://ftp.3gpp.org/Specs/.
[3] 3GPP. Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs: 3GPP TS 33.122[S/OL].[2022-12-26]. ftp://ftp.3gpp.org/Specs/.
[4] 3GPP. Network Domain Security(NDS); Authentication Framework(AF):3GPP TS 33.310[S/OL].[2022-12-26]. ftp://ftp.3gpp.org/Specs/.
[5] 3GPP. Network Domain Security(NDS); IP network layer security: 3GPP TS 33.210[S/OL].[2022-12-26]. ftp://ftp.3gpp.org/Specs/.
[6] 朱斌,林琳,胡悦,等.面向行业的5G网络能力开放发展策略研究[J].邮电设计技术,2020(7):1-6.
[7] 胡悦,李善诗,朱斌.浅析运营商通信网络能力开放门户架构设计[J].邮电设计技术,2019(5):14-18.
[8] 张卓筠,贺晓博,高功应,等.5G网络能力开放需求和解决方案研究[J].邮电设计技术,2016(7):9-11.
[9] 杨红梅,林美玉.5G网络及安全能力开放技术研究[J].移动通信,2020,44(4):65-68.
[10] 陶伟宜,陈云.基于5G SA网络的能力开放平台网络能力验证研究[J].邮电设计技术,2022(6):65-70.
[11] 林奕琳,何宇锋,刘玉芹,等.5G网络能力开放部署及关键技术方案[J].移动通信,2021,45(6):81-87.

作者简介:
彭健,工程师,学士,主要从事移动通信技术研究、新技术跟踪及创新业务产品研究工作;李文彬,工程师,学士,主要从事移动通信技术研究、新技术跟踪及创新业务产品研究工作;陈丰,工程师,硕士,主要从事移动通信技术研究、5G专网应用研究及创新业务产品研究工作。