ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29828—2013

信息安全技术　可信计算规范
可信连接架构

Information security technology—Trusted computing specification—Trusted connect architecture

2013-11-12 发布　　2014-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位:北京工业大学、西安西电捷通无线网络通信股份有限公司、瑞达信息安全产业股份有限公司、西安电子科技大学、北京理工大学、武汉大学、北京天融信科技有限公司、北京电子科技学院、北京金奥博数码信息技术有限责任公司、中国电子科技集团公司第三十研究所、国家无线电监测中心、北京网贝合创科技有限公司、中国航天科工集团二院七 O 六所、郑州信大捷安信息技术有限公司、上海格尔软件股份有限公司、西安邮电大学、江南计算机技术研究所、国家广播电影电视总局广播科学研究院、中国电子技术标准化研究院、华为技术有限公司、深圳长城电脑有限公司、中安科技集团有限公司、长春吉大正元信息技术股份有限公司、北京鼎普科技股份有限公司、成都卫士通信息产业股份有限公司、北京密安网络技术股份有限公司、中国电力科学研究院、无线网络安全技术国家工程实验室。

本标准主要起草人:沈昌祥、肖跃雷、曹军、张立强、张兴、韩永飞、方娟、李海鹏、黄振海、陈曦、祝烈煌、李兆斌、刘彤、冷冰、宋起柱、陈志浩、张焕国、秦志强、段丽娟、李晖、张龙、铁满霞、赖晓龙、常超稳、谭武征、韩勇桥、刘智君、姚琦、裴庆祺、张子剑、葛莉、鞠磊、赵桂芳、朱林、朱志祥、蒋炎河、王磊、邹冰玉、赖英旭、马卓、张变玲、杜志强、胡亚楠、刘卫国、池亚平、吴素研、苑克龙、王晓程、于昇、李兴华、王轲、张国强、李琴、刘贤刚、位继伟、尹瀚、秦晰、魏占祯、李瑛、刘了、梁晋春、公备、邵存金、李大东、何长龙、万俊、贾科、张世雄、王明坤、高昆仑、许胜伟、姚金利、王勇、侯亚荣、任兴田、杨宇光、赵国磊、韩培胜、曹慧渊、郭沛宇、郎风华。

引　言

随着信息化的逐渐发展，网络安全面临严峻的考验，各种计算机网络遭受的攻击和破坏80%是来自于内部。目前业内的安全解决方案往往侧重于先防外后防内，先防服务设施后防终端设施。而可信计算技术则逆其道而行之，首先保证所有终端的可信赖性，通过可信赖的组件来组建更大的可信系统。可信计算平台在底层进行防护，通过可信硬件对上层进行保护，为用户提供更强的安全防护。可信网络连接本质上包含两个方面的内容：第一方面需要创建一套在网络内部系统运行状况的策略；第二方面，只有遵守网络设定的策略的终端才能访问网络，网络将隔离和定位那些不遵守策略的设备。

本标准的主要目标是提出一个实现终端连接到网络的双向用户身份鉴别和平台鉴别，进而实现可信网络连接的可信连接架构，并定义其层次、实体、组件、接口、实现流程、评估、隔离和修补以及各个接口的具体实现。

本标准主要内容是：

——可信连接架构，实现终端连接到网络的双向用户身份鉴别和平台鉴别。

——定义可信连接架构中各个接口的具体实现。

本标准的使用者是可信计算的生产企业、检测机构和科研机构。

本标准的发布机构提请注意，声明符合本标准时，可能涉及第5章与“一种基于三元对等鉴别的可信网络连接方法”、“一种基于三元对等鉴别的可信网络连接系统”等相关的专利的使用。

本标准的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本标准的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本标准发布机构备案。相关信息可通过以下联系方式获得：

专利权人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路68号 西安软件园秦风阁A201

联系人：刘长春

邮政编码：710075

电子邮件：ipri@iwncomm.com

电　　话：029-87607836

传　　真：029-87607829

网　　址：http://www.iwncomm.com

请注意除了上述专利外，本标准的某些内容仍可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

信息安全技术　可信计算规范
可信连接架构

1　范围

本标准规定了可信连接架构的层次、实体、组件、接口、实现流程、评估、隔离和修补以及各个接口的具体实现，解决终端连接到网络的双向用户身份鉴别和平台鉴别问题，实现终端连接到网络的可信网络连接。

本标准适用于具有可信平台控制模块的终端与网络的可信网络连接。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 15629.11—2003　信息技术　系统间远程通信和信息交换局域网和城域网　特定要求　第11部分：无线局域网媒体访问控制和物理层规范

GB 15629.11—2003/XG1—2006　信息技术　系统间远程通信和信息交换　局域网和城域网　特定要求　第11部分：无线局域网媒体访问控制和物理层规范　第1号修改单

GB/T 28455—2012　信息安全技术　引入可信第三方的实体鉴别及接入架构规范

ISO/IEC 9798-3：1998/Amd.1：2010　信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制　第1号修改单：引入在线可信第三方的机制(Information technology—Security techniques—Entity authentication—Part 3：Mechanisms using digital signature techniques—Amendment 1：Mechanisms involving an on-line trusted third party)

ISO/IEC 18028-5：2006　信息技术　安全技术　IT网络安全　第5部分：使用虚拟专用网的跨网通信安全保护(Information technology—Security techniques—IT network security—Part 5：Securing communications across networks using virtual private networks)

IETF RFC 2138　远程认证拨入用户服务(Remote Authentication Dial In User Service)

IETF RFC 2246　TLS协议1.0版本(The TLS Protocol Version 1.0)

IETF RFC 2547　边界网关协议/多协议标签交换 虚拟专用网(BGP/MPLS VPNs)

IETF RFC 2675　Ipv6 巨型包(IPv6 Jumbograms)

IETF RFC 2865　远程认证拨入用户服务(Remote Authentication Dial In User Service)

IETF RFC 2866　远程认证拨入用户服务的计费(RADIUS Accounting)

IETF RFC 3280　X.509公钥基础设施证书和证书撤销列表轮廓(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile)

IETF RFC 3539　认证、授权和计费传输轮廓(Authentication Authorization and Accounting Transport Profile)

IETF RFC 3588　Diameter基础协议(Diameter Base Protocol)

IETF RFC 3589　3GPP的Diameter命令代码(Diameter Command Codes for Third Generation Partnership Project Release 5)

IETF RFC 4346　TLS协议1.1版本(The TLS Protocol Version 1.1)

IETF RFC 4675　RADIUS VLAN 与优先级(RADIUS Attributes for Virtual LAN and Priority Support)

IETF RFC 5246　TLS 协议 1.2 版本(The TLS Protocol Version 1.2)

3　术语和定义

下列术语和定义适用于本文件。

3.1

组件　component

计算系统中可被度量的软件、固件和硬件模块。

3.2

完整性度量　integrity measurement

使用杂凑算法对被度量对象计算其杂凑值的过程。

3.3

完整性度量值　integrity measurement value

组件被杂凑算法计算后得到的杂凑值。

3.4

完整性报告　integrity report

包含快照和 Quote 数据的信息集合。

3.5

完整性基准值　predefined integrity value

组件在发布时或在可信状态下被度量得到的杂凑值,作为完整性校验的参考基准。

3.6

平台鉴别　platform authentication

实现平台身份鉴别和平台完整性评估的过程。

3.7

平台配置寄存器　platform configuration register

可信平台控制模块内部用于存储完整性度量值的存储单元。

3.8

平台身份鉴别　platform identity authentication

对平台身份进行验证的过程。

3.9

平台身份密钥　platform identity key

可信平台控制模块的身份密钥。

3.10

信任链　trusted chain

在计算系统启动和运行过程中,使用完整性度量方法在组件之间所建立的信任传递关系。

3.11

可信计算平台　trusted computing platform

通过可信平台控制模块在计算系统中建立的支撑系统,用于实现可信计算功能的,对计算系统实施保护和管理。

3.12

可信基础支撑软件　trusted basic supporting software

可信计算平台支撑体系中的基础软件部分，用于保障信任链在软件系统的传递，保证系统软件的可信性，为应用开发提供必要的标准编程接口，管理可信计算平台的可信资源。

3.13

三元对等架构　tri-element peer architecture

引入在线第三方的安全架构，实现实体之间的双向鉴别。

3.14

基于三元对等架构的访问控制技术 TePA-based access control

一种基于端口控制的访问控制方法，通信双方在三元对等架构下依据鉴别协议的结果进行端口控制。

3.15

三元可扩展鉴别协议　tri-element authentication extensible protocol

满足基于三元对等鉴别的访问控制技术的可扩展鉴别协议，采用了复用模型，即鉴别协议的传输需经两次封装过程。

3.16

可信网络连接　trusted network connection

终端连接到受保护网络的过程，包括用户身份鉴别、平台身份鉴别和平台完整性评估三个步骤。

3.17

可信连接架构　trusted connect architecture

一种基于三元对等鉴别的可信网络连接架构，实现双向用户身份鉴别和平台鉴别。

3.18

可信平台控制模块　trusted platform control module

可信平台控制模块是一种集成在可信计算平台中，用于建立和保障信任源点的硬件核心模块，为可信计算提供完整性度量、安全存储、可信报告以及密码服务等功能。

3.19

可信第三方　trusted third party

一个安全的权威方，它为其他安全相关实体所信任。

3.20

用户身份鉴别　user identity authentication

对用户身份进行验证的过程。

4　缩略语

下列缩略语适用于本文件。

AC　访问控制器(Access Controller)
AE　鉴别器实体(Authenticator Entity)
AP　接入点(Access Point)
APS　鉴别策略服务者(Authentication Policy Server)
ASN　抽象语法标记(Abstract Syntax Notation)
ASE　鉴别服务实体(Authentication Service Entity)
ASU　鉴别服务单元(Authentication Service Unit)
ASUE　鉴别请求者实体(Authentication Supplicant Entity)

AR	访问请求者(Access Requestor)
BK	基密钥(Base Key)
BIOS	基本输入输出系统(Basic Input Output System)
CBC-MAC	密码块链接消息鉴别编码(Cipher Block Chaining Message Authentication Code)
DER	可辨别编码规则(Distinguish Encoding Rule)
EAP	可扩展鉴别协议(Extensible Authentication Protocol)
ECC	椭圆曲线密码学(Elliptic Curve Cryptography)
ECDH	椭圆曲线密码体制的 Diffie-Hellman 交换(Elliptic Curve Diffie-Hellman)
ECDSA	椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm)
EPS	评估策略服务者(Evaluation Policy Server)
ETLS	增强型 TLS 协议(Enhanced TLS)
EWAI	增强型 WAI 协议(Enhanced WAI)
IF-APS	鉴别策略服务接口(Authentication Policy Service Interface)
IF-EPS	评估策略服务接口(Evaluation Policy Server Interface)
IF-IM	完整性度量接口(Integrity Measurement Interface)
IF-IMC	完整性度量收集接口(Integrity Measurement Collector Interface)
IF-IMV	完整性度量校验接口(Integrity Measurement Verifier Interface)
IF-TNCCAP	TNC 客户端-TNC 接入点接口(TNC Client-Server Interface)
IF-TNT	可信网络传输接口(Trusted Network Transport Interface)
IMC	完整性度量收集者(Integrity Measurement Collector)
IMV	完整性度量校验者(Integrity Measurement Verifier)
IP	因特网协议(Internet Protocol)
IPL	初始程序装载(Initial Program Laoder)
LAN	局域网(Local Area Network)
MAC	媒体访问控制(Medium Access Control)
MAK	消息鉴别密钥(Message Authentication Key)
NAC	网络访问控制者(Network Access Controller)
NAR	网络访问请求者 (Network Access Requestor)
OFB	输出反馈(Output Feed Back)
OID	客体标识符(Object Identifier)
PAI	平台鉴别基础设施(Platform Authentication Infrastucture)
PCR	平台配置寄存器(Platform Configuration Register)
PIK	平台身份密钥(Platform Identity Key)
PM	策略管理器(Policy Manager)
RADIUS	远程认证拨入用户服务(Remote Authentication Dial In User Service)
ROM	只读内存(Read-Only Memory)
STA	站点(Station)
SML	度量存储日志(Stored Measurement Log)
TCA	可信连接架构(Trusted Connect Authentication)
TAEP	三元可扩展鉴别协议(Tri-element Extensible Authentication Protocol)
TePA	三元对等架构(Tri-element Peer Authentication)
TePA-AC	基于三元对等架构的访问控制技术(TePA-based Access Control)
TLS	传输层安全(Transport Layer Security)

TNC	可信网络连接(Trusted Network Connect)
TNCC	TNC 客户端(TNC Client)
TNCAP	TNC 接入点(TNC Access Point)
TPCM	可信平台控制模块(Trusted Platform Control Module)
TTP	可信第三方(Trusted Third Party)
UCK	单播完整性校验密钥(Unicast Integrity Check Key)
UEK	单播加密密钥(Unicast Encryption Key)
VLAN	虚拟局域网(Virtual LAN)
VPN	虚拟专用网(Virtual Private Network)
WAI	无线局域网鉴别基础结构(WLAN Authentication Infrastucture)
WAPI	无线局域网鉴别与保密基础结构(WLAN Authentication and Privacy Infrastucture)
WIE	WAPI 信息元素(WAPI Information Element)
WLAN	无线局域网(Wireless LAN)

5 总体描述

5.1 概述

可信连接架构(TCA)规定了具有可信平台控制模块(TPCM)的终端接入网络的可信网络连接(TNC),如图 1 所示。TCA 是一种基于三元对等实体鉴别(见 ISO/IEC 9798-3:1998/Amd.1:2010)的可信网络连接架构,实现双向用户身份鉴别和平台鉴别。

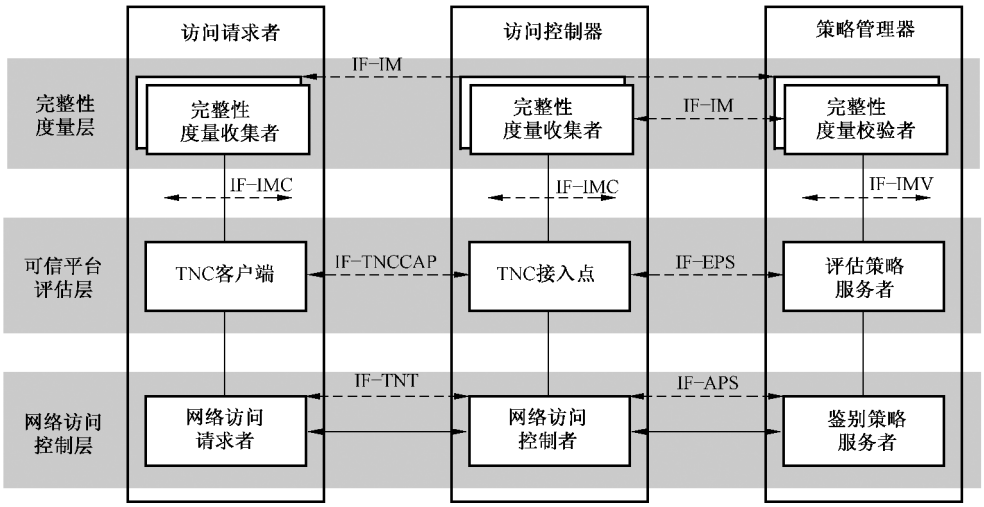

图 1 可信连接架构(TCA)

在图 1 所示的 TCA 中,存在 3 个实体:访问请求者(AR)、访问控制器(AC)和策略管理器(PM),从上至下分为 3 个抽象层:完整性度量层、可信平台评估层和网络访问控制层。在每个实体中,矩形方框表示实体中的组件。组件之间存在相应的接口,用带名称的双向虚线箭头表示。

AR 和 AC 都具有 TPCM,AR 请求访问受保护网络,AC 控制 AR 对受保护网络的访问。PM 对 AR 和 AC 进行集中管理。AR 和 AC 基于 PM 来实现 AR 和 AC 之间的双向用户身份鉴别和平台鉴别,其中平台鉴别包括平台身份鉴别和平台完整性评估,PM 在用户身份鉴别和平台鉴别过程中充当可

信第三方。平台完整性评估包含两个阶段：第一阶段，校验平台完整性度量值是否被篡改；第二阶段，评估平台完整性度量值是否与相应的基准完整性度量值相同。

5.2 实体

5.2.1 访问请求者

AR 是请求接入受保护网络的实体，包含的组件为：网络访问请求者（NAR）、TNC 客户端（TNCC）和完整性度量收集者（IMC），其中 TNCC 和 IMC 之间的接口为完整性度量收集接口（IF-IMC）。AR 的功能为：向 AC 发送访问请求，基于 PM 实现与 AC 之间的双向用户身份鉴别和平台鉴别，依据本地所做出的访问决策执行访问控制。

5.2.2 访问控制器

AC 是控制 AR 访问受保护网络的实体，包含的组件为：网络访问控制者（NAC）、TNC 接入点（TNCAP）和 IMC，其中 TNCAP 和 IMC 之间接口为 IF-IMC。AC 的功能为：基于 PM 实现与 AR 之间双向用户身份鉴别和平台鉴别，依据本地所做出的访问决策执行访问控制。

5.2.3 策略管理器

PM 是 AR 和 AC 的集中管理方，包含的组件为：鉴别策略服务者（APS）、评估策略服务者（EPS）和完整性度量校验者（IMV），其中 EPS 和 IMV 之间的接口为完整性度量校验接口（IF-IMV）。PM 的功能为：协助 AR 和 AC 实现它们之间的双向用户身份鉴别和平台鉴别。在用户身份鉴别和平台鉴别过程中，PM 充当 AR 和 AC 的可信第三方。

5.3 层次

5.3.1 网络访问控制层

网络访问控制层包含的组件为：NAR、NAC 和 APS，其中 NAR 和 NAC 之间的接口为可信网络传输接口（IF-TNT），NAC 和 APS 之间的接口为鉴别策略服务接口（IF-APS）。网络访问控制层中的 IF-TNT 和 IF-APS 定义了网络传输机制和访问控制机制，用于实现网络访问控制层的用户身份鉴别功能、网络传输功能和访问控制功能，具体见第 6 章。

5.3.2 可信平台评估层

可信平台评估层包含的组件为：TNCC、TNCAP 和 EPS，其中 TNCC 和 TNCAP 之间的接口为 TNC 客户端-TNC 接入点接口（IF-TNCCAP），TNCAP 和 EPS 之间的接口为评估策略服务接口（IF-EPS）。可信平台评估层中的 IF-TNCCAP 和 IF-EPS 定义了平台鉴别基础设备（PAI），用于实现可信平台评估层的平台鉴别功能，具体见第 7 章。

5.3.3 完整性度量层

完整性度量层包含的组件为：IMC 和 IMV，其中 IMC 和 IMV 之间的接口为完整性度量接口（IF-IM）。完整性度量层中 IF-IM 定义了 IMC 和 IMV 之间的消息交互（见第 8 章）。

5.4 组件

5.4.1 网络访问请求者

NAR 是 AR 中的一个组件，其功能为：负责向 AC 发起访问请求，与 NAC 和 APS 执行用户身份鉴

别协议来实现 AR 和 AC 之间的双向用户身份鉴别，传送和接收用户身份鉴别协议和平台鉴别协议数据，向 TNCC 发送平台鉴别请求，从 TNCC 接收它所做出的访问决策，依据 NAR 所做出的访问决策或从 TNCC 接收到的访问决策执行访问控制。

5.4.2 网络访问控制者

NAC 是 AC 中的一个组件，其功能为：负责启动用户身份鉴别协议，与 NAR 和 APS 执行用户身份鉴别协议来实现 AR 和 AC 之间的双向用户身份鉴别，传送和接收用户身份鉴别协议和平台鉴别协议数据，向 TNCAP 发送平台鉴别请求，从 TNCAP 接收它所做出的访问决策，依据 NAC 所做出的访问决策或从 TNCAP 接收到的访问决策执行访问控制。

5.4.3 鉴别策略服务者

APS 是 PM 中的一个组件，其功能为：作为可信第三方与 NAR 和 NAC 执行用户身份鉴别协议来实现 AR 和 AC 之间的双向用户身份鉴别，传送和接收用户身份鉴别协议和平台鉴别协议数据。值得注意的是，APS 可以不参与用户身份鉴别协议。

5.4.4 TNC 客户端

TNCC 的功能为：执行网络连接管理，通过 IF-IMC（见 5.5.6）接口与它上端的各个 IMC 进行信息交互，与 TNCAP 和 EPS 执行一轮或多轮平台鉴别协议，实现 AR 和 AC 之间的双向平台鉴别，其中 EPS 充当可信第三方。

平台鉴别过程完成时，TNCC 生成它的访问决策并发送给网络访问控制层中的 NAR。

5.4.5 TNC 接入点

TNCAP 的功能为：执行网络连接管理，通过 IF-IMC（见 5.5.6）接口与它上端的各个 IMC 进行信息交互，与 TNCC 和 EPS 执行一轮或多轮平台鉴别协议，实现 AR 和 AC 之间的双向平台鉴别，其中 EPS 充当可信第三方。

平台鉴别过程完成时，TNCAP 生成它的访问决策并发送给网络访问控制层中的 NAC。

5.4.6 评估策略服务者

EPS 的功能为：不参与 TNCC 与 TNCAP 之间的网络连接管理，通过 IF-IMV（见 5.5.7）接口与它上端的各个 IMV 进行信息交互，作为可信第三方与 TNCC 和 TNCAP 执行平台鉴别协议，实现 AR 和 AC 之间的双向平台鉴别。在平台鉴别协议中，EPS 验证 AR 和 AC 的 PIK 证书的有效性，以及评估 AR 和 AC 的平台完整性。

5.4.7 完整性度量收集者

IMC 是运行在 AR 和 AC 上的组件，它收集 AR 和 AC 的平台完整性度量值，并发送给相应的 IMV。

5.4.8 完整性度量校验者

IMV 是运行在 PM 上的组件，它校验和评估所接收到的 AR 和 AC 的平台完整性度量值。

5.5 接口

5.5.1 可信网络传输接口

IF-TNT 是 NAR 和 NAC 之间的接口，负责完成网络访问控制层的用户身份鉴别功能、网络传输

功能和访问控制功能，具体见第 6 章。

5.5.2 鉴别策略服务接口

IF-APS 是 NAC 和 APS 之间的接口，负责完成网络访问控制层的用户身份鉴别功能和网络传输功能，具体见 6.2。

5.5.3 TNC 客户端-TNC 接入点接口

IF-TNCCAP 是 TNCC 和 TNCAP 之间的接口，负责完成可信平台评估层的平台鉴别功能，具体见第 7 章。

5.5.4 评估策略服务接口

IF-EPS 是 TNCAP 和 EPS 之间的接口，负责完成可信平台评估层的平台鉴别功能，具体见第 7章。

5.5.5 完整性度量接口

IF-IM 是 IMC 和 IMV 之间的接口，定义 IMC 和 IMV 之间交换的特定厂商的组件信息，具体见第 8 章。

5.5.6 完整性度量收集接口

IF-IMC 是 TNCC 与它上端的各个 IMC 之间的接口，负责完成 TNCC 与它上端的各个 IMC 之间的信息交互，用于实现平台鉴别功能(见 9.2)。IF-IMC 是 TNCAP 与它上端的各个 IMC 之间的接口，负责完成 TNCAP 与它上端的各个 IMC 之间的信息交互，用于实现平台鉴别功能(见 9.2)

5.5.7 完整性度量校验接口

IF-IMV 是 EPS 与它上端的各个 IMV 之间的接口，负责完成 EPS 与它上端的各个 IMV 之间的信息交互，用于完成平台鉴别功能(见 9.3)。

5.6 实现过程

TCA 的实现过程如图 2 所示。

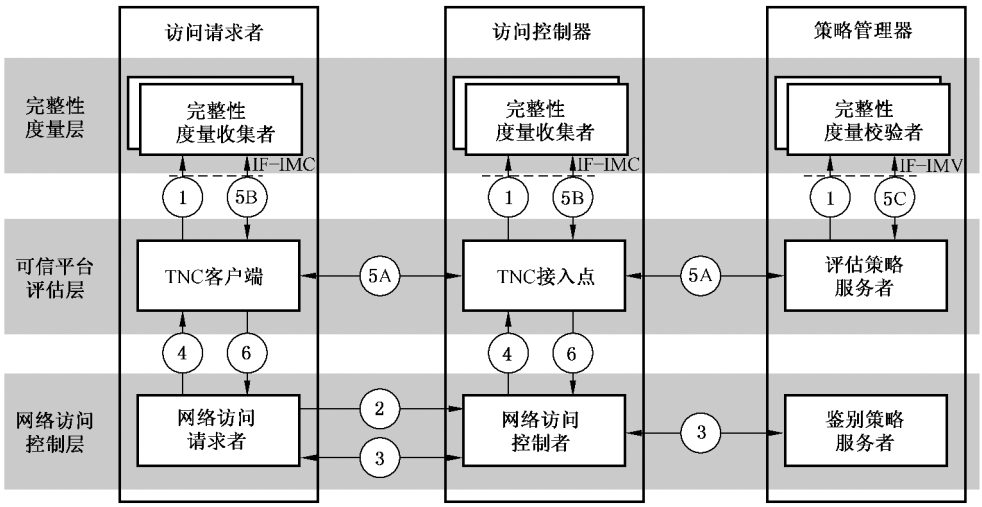

图 2 TCA 的实现过程

在图 2 中，TCA 的实现过程的具体步骤为：

1） 在建立可信网络连接之前，TNCC 和 TNCAP 必须分别根据特定平台绑定函数来加载它们上端的各个 IMC，而 EPS 必须根据特定平台绑定函数加载它上端的各个 IMV，其中特定平台绑定函数不在本标准中规定。

2） NAR 向 NAC 发起网络访问请求。

3） NAC 收到 NAR 的网络访问请求后，与 NAR 和 APS 执行用户身份鉴别协议来实现 AR 和 AC 之间的双向用户身份鉴别，其中 APS 可以不参与用户身份鉴别协议。若 APS 参与该用户身份鉴别协议，则 APS 在该用户身份鉴别协议中充当可信第三方。在用户身份鉴别协议中，NAR 和 NAC 协商出 AR 和 AC 之间的主密钥或会话密钥。若用户身份鉴别完成后要求立即做出访问决策，则 NAR 和 NAC 分别依据用户身份鉴别结果生成访问决策，然后跳至步骤 7）。

4） 若 NAR 需要执行平台鉴别过程，则 NAR 向 TNCC 发送平台鉴别请求，若 NAC 需要执行平台鉴别过程，则 NAC 向 TNCAP 发送平台鉴别请求。

5A） 当 TNCAP 收到平台鉴别请求信息时，启动平台鉴别过程，与 TNCC 和 EPS 执行一轮或多轮平台鉴别协议来实现 AR 和 AC 之间的平台鉴别。当 TNCC 收到 NAR 的平台鉴别请求信息，或一轮平台鉴别协议结束后还没完成对 AC 的平台鉴别时，TNCC 等待 TNCAP 发起的一轮平台鉴别协议。

5B） 在平台鉴别过程中，TNCC 通过 IF-IMC（见 5.5.6）与它上端的各个 IMC 进行信息交互。TNCAP 通过 IF-IMC（见 5.5.6）与它上端的各个 IMC 进行信息交互。

5C） EPS 负责验证 AR 和 AC 的 PIK 证书，并通过 IF-IMV（见 5.5.7）调用它上端的各个 IMV 来校验和评估 AR 和 AC 的平台完整性度量值。EPS 依据平台完整性评估策略生成 AR 和 AC 的平台完整性评估结果，最后将 PIK 证书验证结果和平台完整性评估结果发送给 TNCC 和 TNCAP。

6） 当 AR 和 AC 的平台鉴别完成时，TNCC 和 TNCAP 分别依据 EPS 生成 AR 和 AC 的 PIK 证书验证结果和平台完整性评估结果生成访问决策（允许/禁止/隔离），并分别发送给 NAR 和 NAC。

7） NAR 依据它所生成的访问决策或从 TNCC 接收到的访问决策执行访问控制，NAC 依据它所生成的访问决策或从 TNCAP 接收到的访问决策执行访问控制，从而实现可信网络连接，即 AC 依据访问决策控制 AR 对受保护网络的访问，AR 依据访问决策判定是否连接至该受保护网络，其中过程中所涉及的算法均以套件形式存在，需符合国家对于密码管理的有关规定。

5.7 评估、隔离和修补

5.7.1 具有隔离修补层的 TCA

隔离和修补功能是 TCA 中的重要组成部分。若平台身份未被成功鉴别，则断开连接；否则，校验和评估平台完整性。若平台完整性校验和评估未成功通过，则接入隔离域对平台进行修补，通过平台修补后可重新执行平台鉴别过程。具有隔离和修补功能的 TCA 如图 3 所示。

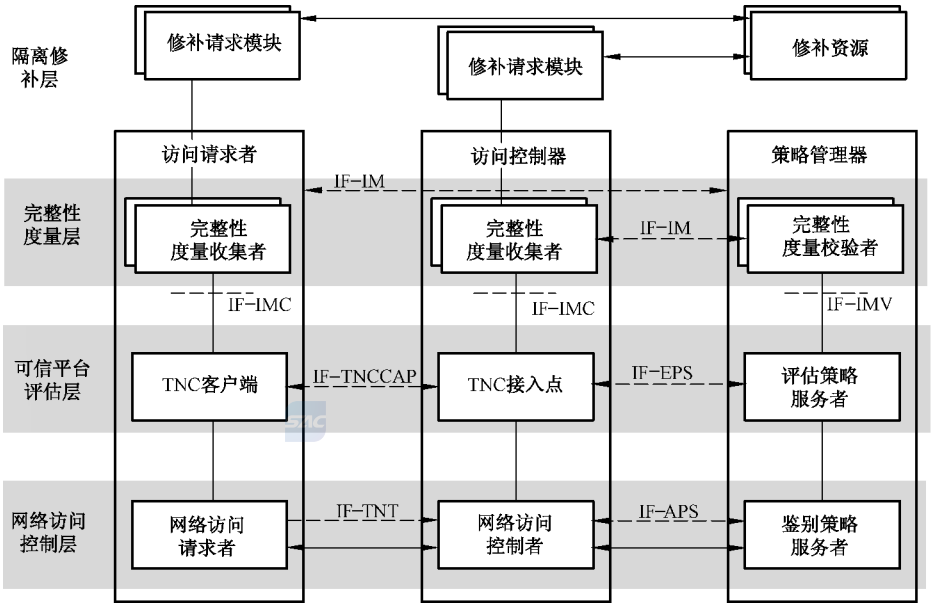

图 3　具有隔离修补层的可信连接架构

在图 3 中的隔离修补层，驻留在 AR 和 AC 的修补请求模块可向 PM 所提供的修补资源请求修补。当 AR 的平台需要进行修补时，AR 的各个 IMC 调用驻留在 AR 的修补请求模块向 PM 所提供的修补资源请求修补并完成自身平台修补；当 AC 的平台需要进行修补时，AC 的各个 IMC 调用驻留在 AC 的修补请求者模块向 PM 所提供的修补资源请求修补并完成自身平台修补。

5.7.2　评估

平台鉴别包括平台身份鉴别和平台完整性评估。这里，评估是依据 AR 和 AC 的平台完整性度量值进行的，其中完整性管理框架参见附录 A。

TCA 中的 TNCC 和 TNCAP 分别将 AR 和 AC 的平台完整性度量值发送给 EPS(平台完整性度量值通过平台 PIK 私钥签名确保平台完整性度量值来源的抗抵赖性)，EPS 调用它上端的各个 IMV 对 AR 和 AC 的平台完整性度量值进行校验和评估，生成平台完整性评估结果，并发送给 TNCC 和 TNCAP。

当 TNCC 和 TNCAP 收到平台完整性评估结果后，若 AR 和 AC 的平台需要修补，则分别通知 NAR 和 NAC 进行隔离，NAR 和 NAC 将访问隔离域并依照 EPS 传输过来的平台修补信息进行修补。平台修补完成后，TNCC 和 TNCAP 将平台修补部分的平台完整性度量值发送给 EPS(平台完整性度量值通过平台 PIK 私钥签名确保平台完整性度量值来源的抗抵赖性)，执行下一个平台鉴别过程。

5.7.3　隔离

对实体进行隔离的技术有：VLAN 隔离、IP 过滤和基于端口的控制。

5.7.3.1　VLAN 隔离

VLAN 隔离(见 RFC 2675)是使 AR 和 AC 接入一个虚拟局域网，该虚拟局域网为 AR 和 AC 提供了平台修补资源(如软件补丁、病毒更新文件等)。

5.7.3.2　IP 过滤

IP 过滤是使用 AC 配置 IP 的过滤集，通过这些 IP 过滤集来实现隔离(见 RFC 2865)。

5.7.3.3 基于端口的控制

基于端口的控制是指定义两种逻辑端口：非受控端口和受控端口，通过对受控端口进行控制来实现隔离（见 6.3.1）。

5.7.4 修补

修补是使 AR 和 AC 的平台安全状态符合对方定义的平台完整性评估策略所指定的平台安全状态，这可通过对平台组件进行更新或升级的方式来实现。当 AR 和 AC 的平台不能通过平台完整性评估时，证明它们的平台安全状态未达到对方定义的平台完整性评估策略所指定的平台安全状态，则 AR 和 AC 将被接入隔离域并进行平台修补。

6 网络访问控制层

6.1 概述

在网络访问控制层，NAR、NAC 和 APS 采用三元可扩展鉴别协议（TAEP）来实现 TCA 的网络传输，其中 TCA 的 TAEP 实现方式包括：序列 TAEP 鉴别方式和隧道 TAEP 鉴别方式。

在网络访问控制层，NAR 和 NAC 采用基于三元对等架构的访问控制技术（TePA-AC）来实现 TCA 的访问控制，其中 TCA 的 TePA-AC 实现方式包括：全端口控制实现方式和部分端口控制方式。

TAEP 和 TePA-AC 的定义见 GB/T 28455—2012。

6.2 网络传输机制

6.2.1 序列 TAEP 鉴别方式

6.2.1.1 概述

序列 TAEP 鉴别方式是指采用一序列 TAEP 鉴别方法来实现 TCA 的双向用户身份鉴别和平台鉴别。本标准规定了两种适用于 TCA 的序列 TAEP 鉴别实现（见 6.2.1.2 和 6.2.1.3），前者适用于 AR 和 AC 在用户身份鉴别过程中生成会话密钥的情况，后者适用于 AR 和 AC 在用户身份鉴别过程中生成主密钥的情况，也可以适用于 AR 和 AC 在用户身份鉴别过程中生成会话密钥的情况。

6.2.1.2 TCA 的序列 TAEP 鉴别实现一

6.2.1.2.1 层次模型

图 4 为 TCA 的序列 TAEP 鉴别实现一的层次模型。

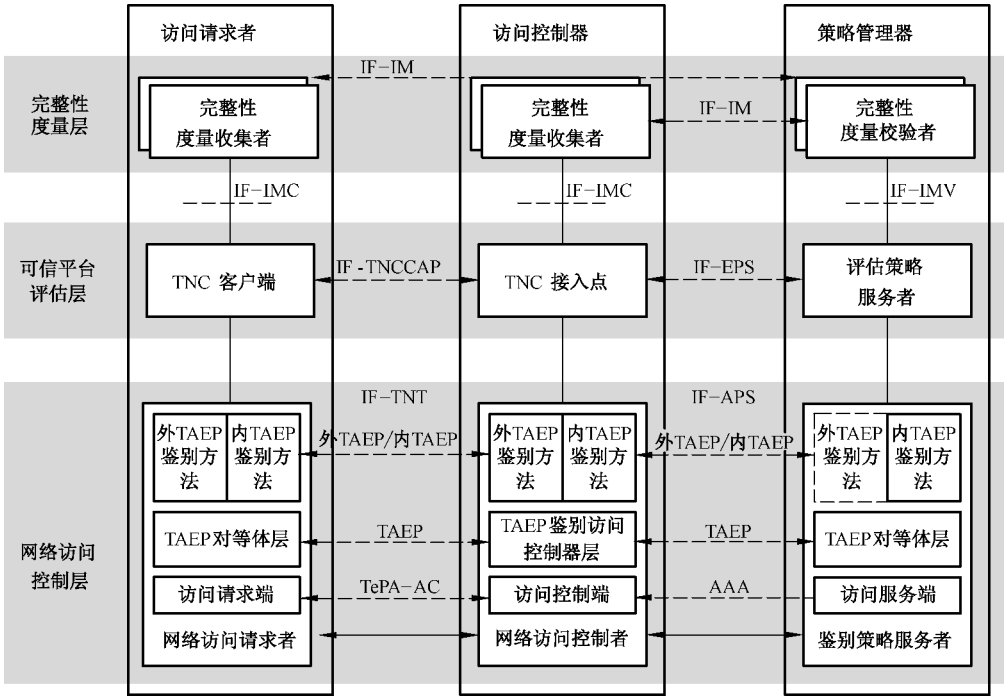

图 4　TCA 的序列 TAEP 鉴别实现一的层次模型

在图 4 中，NAR、NAC 和 APS 先执行一个外 TAEP 鉴别方法，然后再执行一个内 TAEP 鉴别方法，其中 AR 和 AC 之间的内 TAEP 鉴别方法中的数据字段被外 TAEP 鉴别方法协商的 AR 和 AC 之间的会话密钥所保护。保护机制中的密码算法采用 SM4。TAEP 对等体层和 TAEP 鉴别访问控制器层为 TAEP 层次模型(见 GB/T 28455—2012)中的两种角色。访问请求端和访问控制端利用 TePA-AC 来实现 TCA 的访问控制(见 6.3)，其中 TAEP 包承载在 TePA-AC 上。访问控制端和访问服务端可以利用 AAA 协议(见 RFC 3539)来承载 TAEP 包，例如：RADIUS 和 Diameter(见 RFC 2138、RFC 2865、RFC 2866、RFC 4675、RFC 3588 和 RFC 3589)。

APS 中的外 TAEP 鉴别方法为虚线框，表示 APS 可以不参与外 TAEP 鉴别方法。

对于 TCA 的这种序列 TAEP 鉴别实现，内 TAEP 包中的 PIK 签名必须密码绑定外 TAEP 鉴别方法为 AR 和 AC 之间建立的会话密钥，密码绑定方法是将该会话密钥作为 PIK 签名的外部数据输入。

6.2.1.2.2　外 TAEP 鉴别方法

外 TAEP 鉴别方法用于实现 AR 和 AC 之间的双向用户身份鉴别，以及协商 AR 和 AC 之间的会话密钥。外 TAEP 鉴别方法用于封装传输用户身份鉴别协议，它可以封装各种用户身份鉴别协议。

外 TAEP 包可以封装基于预共享密钥的 WAI 协议单播密钥协商过程(见 GB 15629.11—2003 和 GB 15629.11—2003/XG1—2006)。当外 TAEP 包封装 WAI 协议单播密钥协商过程时，本标准规定相应的外 TAEP 鉴别方法的 Type 字段为 TAEP-WAI(值为 200)。

外 TAEP 包封装的双向用户身份鉴别协议也可以根据不同的网络环境选用。

6.2.1.2.3　内 TAEP 鉴别方法

内 TAEP 鉴别方法用于实现 AR 和 AC 之间的平台鉴别。

当内 TAEP 包封装 PAI 协议(见 7.2.2)时,本标准规定相应的内 TAEP 鉴别方法的 Type 字段为 TAEP-PAI(值为 201)。

6.2.1.2.4 TAEP 交互过程

TCA 的 TAEP 交互过程如下:

a) NAC 向 NAR 发送 TAEP 的 Request 分组,其中 Type 字段的值为 Identity。

b) NAR 向 NAC 发送 TAEP 的 Response 分组,其中 Type 字段的值为 Identity,Type-Data 字段的值包含 AR 的身份。

c) NAC 向 APS 发送 TAEP 的 Request 分组,其中 Type 字段的值为 TP Authentication,Type-Data 字段的值包含 AR 和 AC 的身份。

d) APS 向 NAC 发送 TAEP 的 Response 分组,其中 Type 字段的值为 TP Authentication,Type-Data 字段的值包含 PM 所支持的各种 TAEP 鉴别方法类型。

e) NAC 选取一种外 TAEP 鉴别方法与 NAR、APS 执行外 TAEP 鉴别方法过程,即 NAC 与 NAR 之间、NAC 与 APS 之间交互一系列 TAEP 的 Request 分组和 Response 分组,直至外 TAEP 鉴别方法过程完成,其中 Type 字段的值为 NAC 选取的外 TAEP 鉴别方法类型,Type-Data 字段的值包含该外 TAEP 鉴别方法类型对应的外 TAEP 鉴别方法消息。

f) 若步骤 e)完成后 NAC 还需要执行平台鉴别过程,则执行步骤 g);否则利用 TAEP 的 Success 分组或 Failure 分组结束鉴别过程,即若在步骤 e)中的外 TAEP 鉴别方法过程中 NAC 成功鉴别 AR 的用户身份,则向 NAR 发送 TAEP 的 Success 分组;若在步骤 e)中的外 TAEP 鉴别方法过程中 NAC 不能成功鉴别 AR 的用户身份,则向 NAR 发送 TAEP 的 Failure 分组。

g) NAC 选取一种内 TAEP 鉴别方法与 NAR、APS 执行内 TAEP 鉴别方法过程,即 NAC 与 NAR 之间、NAC 和 APS 之间交互一系列 TAEP 的 Request 分组和 Response 分组,直到内 TAEP 鉴别方法过程完成,其中 Type 字段的值为 NAC 选取的内 TAEP 鉴别方法类型,Type-Data 字段的值为 NAC 选取的内 TAEP 鉴别方法类型对应的内 TAEP 鉴别方法消息。内 TAEP 鉴别方法消息由可信平台评估层中的 TNCC、TNCAP 和 EPS 进行相应处理。

h) NAC 利用 TAEP 的 Success 分组或 Failure 分组结束鉴别过程,即:若在步骤 g)中的内 TAEP 鉴别方法过程中 TNCAP 成功鉴别 AR 的平台(包括平台身份鉴别和平台完整性评估),则向 NAR 发送 TAEP 的 Success 分组。若在步骤 g)中的内 TAEP 鉴别方法过程中 TNCAP 不能成功鉴别 AR 的平台,则向 NAR 发送 TAEP 的 Failure 分组。

以上步骤描述了 TCA 的序 TAEP 鉴别实现一的典型 TAEP 交互过程,但根据鉴别方法的不同,步骤过程会有不同。

当外 TAEP 鉴别方法的 Type 字段为 TAEP-WAI 且封装基于预共享密钥的 WAI 协议单播密钥协商过程,内 TAEP 鉴别方法的 Type 字段为 TAEP-PAI 时且封装 PAI 协议(见 7.2.2)时,TCA 的序列 TAEP 鉴别实现一的一个完整的 TAEP 交互过程如图 5 所示。

图 5　序列 TAEP 鉴别实现一的 TAEP 交互过程

在图 5 中，根据 PAI 协议的特点，与 TAEP-PAI 相关的消息 1～消息 6 的 TAEP 交互可能执行多轮次。

在一轮 PAI 协议中，当消息 5 未被生成时，消息 5 和消息 6 的 TAEP 交互不存在。

在一轮 PAI 协议中，当消息 5 被生成，但消息 6 未被生成时，消息 6 的 TAEP 交互存在，其 Data 值为 NULL。

6.2.1.3　TCA 的序列 TAEP 鉴别实现二

6.2.1.3.1　层次模型

图 6 为 TCA 的序列 TAEP 鉴别实现二的层次模型。

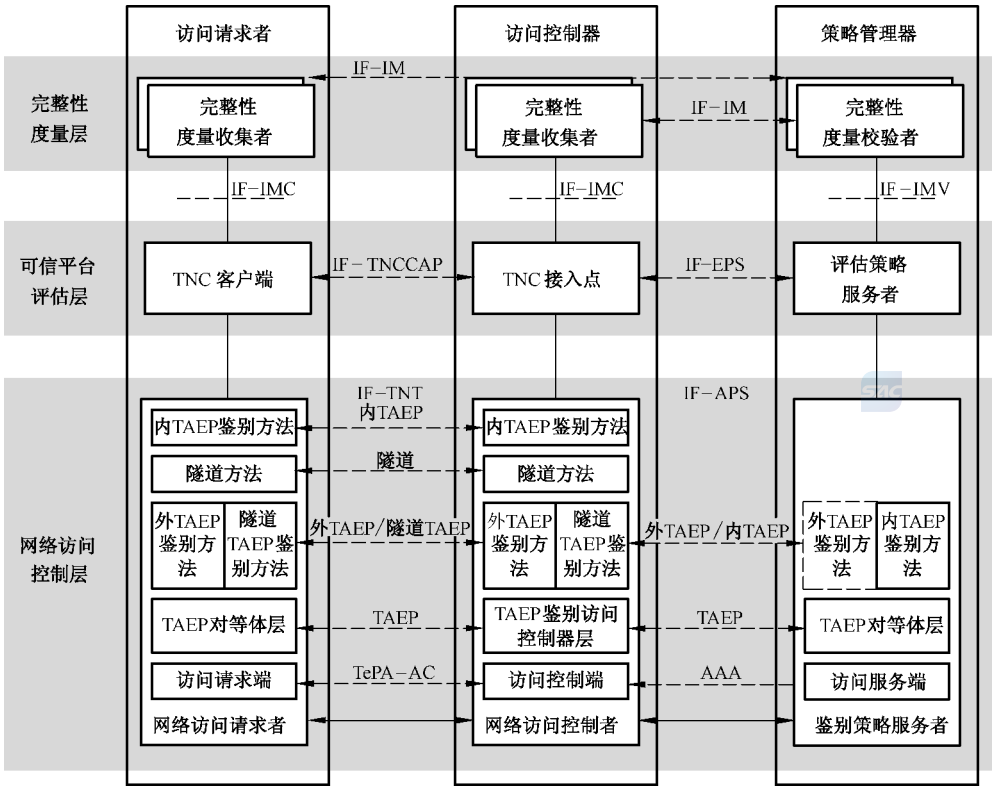

图 6　TCA 的序列 TAEP 鉴别实现二的层次模型

在图 6 中，NAR、NAC 和 APS 先执行一个外 TAEP 鉴别方法，然后再执行一个隧道 TAEP 鉴别方法，其中隧道 TAEP 鉴别方法包含两个阶段：隧道方法和内 TAEP 鉴别方法。TAEP 对等体层和 TAEP 鉴别访问控制器层是 TAEP 层次模型（见 GB/T 28455—2012）中的两种角色。访问请求端和访问控制端利用 TePA-AC 来实现 TCA 的访问控制（见 6.3），其中 TAEP 包承载在 TePA-AC 上。访问控制端和访问服务端可以利用 AAA 协议（见 RFC 3539）来承载 TAEP 包，例如，RADIUS 和 Diameter（见 RFC 2138、RFC 2865、RFC 2866、RFC 4675、RFC 3588 和 RFC 3589）。外 TAEP 鉴别方法建立 AR 和 AC 之间的主密钥或会话密钥。外 TAEP 鉴别方法还可以建立 AR 和 PM 之间的会话密钥，以及 AC 和 PM 之间的会话密钥。隧道 TAEP 鉴别方法中的隧道方法建立 AR 和 AC 之间的隧道密钥。

APS 中的外 TAEP 鉴别方法为虚线框，表示 APS 可以不参与外 TAEP 鉴别方法。

对于 TCA 的这种序列 TAEP 鉴别实现，内 TAEP 包中的 PIK 签名必须密码绑定外 TAEP 鉴别方法为 AR 和 AC 之间建立的主密钥或会话密钥、隧道 TAEP 鉴别方法中隧道方法所建立的隧道密钥，密码绑定方法是将这两阶段密钥作为 PIK 签名的外部数据输入。

6.2.1.3.2　外 TAEP 鉴别方法

外 TAEP 鉴别方法用于实现 AR 和 AC 之间的双向用户身份鉴别，以及协商 AR 和 AC 之间的主密钥或会话密钥。外 TAEP 鉴别方法用于还可以用于协商 AR 和 PM 之间的会话密钥，以及 AC 和 PM 之间的会话密钥。外 TAEP 鉴别方法用于封装传输用户身份鉴别协议，它可以封装各种用户身份鉴别协议。

当采用公钥证书时，外 TAEP 包可以封装基于证书的 WAI 协议（见 GB 15629.11—2003 和 GB 15629.11—2003/XG1—2006）及增强型 WAI 协议（见 6.2.1.3.5）的证书鉴别过程、三元对等鉴别协议（见 ISO/IEC 9798-3:1998/Amd.1:2010）。当采用预共享密钥时，外 TAEP 包可以封装基于预共享密钥的 WAI 协议单播密钥协商过程（见 GB 15629.11—2003 和 GB 15629.11—2003/XG1—2006）。当

外 TAEP 包封装 WAI 协议及增强型 WAI 协议时，本标准规定相应的外 TAEP 鉴别方法的 Type 字段为 TAEP-WAI。

外 TAEP 包封装的双向用户身份鉴别协议也可以根据不同的网络环境选用。

6.2.1.3.3 隧道 TAEP 鉴别方法

隧道 TAEP 鉴别方法用于封装传输平台鉴别协议，如 PAI 协议(见 7.2.2)，它包含以下两个阶段：

第一阶段，NAR 和 NAC 利用隧道方法建立 AR 和 AC 之间的安全隧道。

第二阶段：NAR、NAC 和 APS 交互内 TAEP 鉴别方法的内 TAEP 包，其中 AR 和 AC 之间的内 TAEP 包是利用隧道方法所建立的安全隧道进行保护的。

对于隧道方法，本标准推荐采用 TLS 协议(见 RFC 2246、4346 和 5246)的全匿名模式，其中 ECDH 交换参数采用国家密码管理局批准的 ECC 域参数，杂凑算法采用国家密码管理局批准的 KD-HMAC-SHA256、HMAC-SHA256 和 SHA256 算法，分组算法采用国家密码管理局批准的 SM4 算法，加密工作模式采用 OFB 模式，完整性校验工作模式采用 CBC-MAC 模式，从而本标准将相应的 TLS 密码套件规定为 TLS_ECDH_anon_WITH_SM4_OFB_CBC_MAC_SHA256，其值为{0x00，0xfe}。

当采用 TLS 协议的完全匿名模式作为隧道方法时，本标准规定相应的隧道 TAEP 鉴别方法的 Type 字段为 TAEP-TTLS(值为 202)。

内 TAEP 鉴别方法用于实现 AR 和 AC 之间的平台鉴别。当内 TAEP 包封装 PAI 协议(见7.2.2)时，本标准规定相应的内 TAEP 鉴别方法的 Type 字段为 TAEP-PAI。

6.2.1.3.4 TAEP 交互过程

TCA 的 TAEP 交互过程如下：

a) NAC 向 NAR 发送 TAEP 的 Request 分组，其中 Type 字段的值为 Identity。

b) NAR 向 NAC 发送 TAEP 的 Response 分组，其中 Type 字段的值为 Identity，Type-Data 字段的值包含 AR 的身份。

c) NAC 向 APS 发送 TAEP 的 Request 分组，其中 Type 字段的值为 TP Authentication，Type-Data 字段的值包含 AR 和 AC 的身份。

d) APS 向 NAC 发送 TAEP 的 Response 分组，其中 Type 字段的值为 TP Authentication，Type-Data 字段的值包含 PM 所支持的各种 TAEP 鉴别方法类型。

e) NAC 选取一种外 TAEP 鉴别方法与 NAR、APS 执行外 TAEP 鉴别方法过程，即 NAC 与 NAR 之间、NAC 与 APS 之间交互一系列 TAEP 的 Request 分组和 Response 分组，直至外 TAEP 鉴别方法过程完成，其中 Type 字段的值为 NAC 选取的外 TAEP 鉴别方法类型，Type-Data 字段的值包含该外 TAEP 鉴别方法类型对应的外 TAEP 鉴别方法消息。

f) 若步骤 e)完成后 NAC 还需要执行平台鉴别过程，则执行步骤 g)，否则利用 TAEP 的 Success 分组或 Failure 分组结束鉴别过程，即若在步骤 e)中的外 TAEP 鉴别方法过程中 NAC 成功鉴别 AR 的用户身份，则向 NAR 发送 TAEP 的 Success 分组；若在步骤 e)中的外 TAEP 鉴别方法过程中 NAC 不能成功鉴别 AR 的用户身份，则向 NAR 发送 TAEP 的 Failure 分组。

g) NAC 选取一种隧道 TAEP 鉴别方法与 NAR 执行隧道方法过程建立 AR 和 AC 之间的安全隧道，即 AR 和 AC 之间交互一系列 TAEP 的 Request 分组和 Response 分组，直至隧道方法过程完成，其中 Type 字段的值为隧道 TAEP 鉴别方法类型，Type-Data 字段的值为隧道方法消息。

h) NAC 向 NAR 发送 TAEP 的 Request 分组，其中 Type 字段的值为步骤 g)中的隧道 TAEP 鉴别方法类型，Type-Data 字段的值为利用步骤 g)建立的安全隧道进行保护的内 TAEP 包。内 TAEP 包的 Code 字段的值为 Request，Type 字段的值为 Identity。当 TNCAP 需要请求用于

内 TAEP 鉴别方法的 AR 的身份时，TNCAP 通知 NAC 发送该内 TAEP 包。当 NAR 收到该内 TAEP 包时，NAR 向 TNCC 请求用于内 TAEP 鉴别方法的 AR 的身份。

i) NAR 向 NAC 发送 TAEP 的 Response 分组，其中 Type 字段对应步骤 h)中 TAEP 的 Request 分组中的 Type 字段，Type-Data 字段的值为利用步骤 g)建立的安全隧道进行保护的内 TAEP 包。内 TAEP 包的 Code 字段的值为 Response，Type 字段对应步骤 h)中内 TAEP 包的 Request 分组中的 Type 字段，Type-Data 字段中包含用于内 TAEP 鉴别方法的 AR 的身份。当 NAR 从 TNCC 接收到用于内 TAEP 鉴别方法的 AR 的身份时，NAR 向 NAC 发送该内 TAEP 包。当 NAC 收到该内 TAEP 包时，NAC 向 TNCAP 发送用于内 TAEP 鉴别方法的 AR 的身份。

j) NAC 向 APS 发送 TAEP 的 Request 分组，其中 Type 字段的值为 TP Authentication，Type-Data 字段中 Subtype 字段的值为 FF-FF-FE(用于标识 TCA 中内 TAEP 包的 TP Authentication 类型分组)，Subdata 字段的值包含用于内 TAEP 鉴别方法的 AR 和 AC 身份。Subdata 字段的值还可以包含对 AR 的平台鉴别策略请求信息，具体值不在本标准中规定。当 TNCAP 需要向 EPS 请求内 TAEP 鉴别方法类型或对 AR 的平台鉴别策略时，TNCAP 通知 NAC 发送该内 TAEP 包。当 APS 收到该内 TAEP 包时，APS 向 EPS 发送用于内 TAEP 鉴别方法的 AR 和 AC 身份或对 AR 的平台鉴别策略请求信息。

k) APS 向 NAC 发送 TAEP 的 Response 分组，其中 Type 字段对应步骤 j)中 TAEP 的 Request 分组中的 Type 字段，Type-Data 字段中 Subtype 的值为 FF-FF-FE，Subdata 字段的值包含各个内 TAEP 鉴别方法类型。Subdata 字段的值还可以包含 EPS 分发给 TNCAP 的对 AR 的平台鉴别策略。当 APS 从 EPS 接收到各个内鉴别方法类型或对 AR 的平台鉴别策略时，APS 向 NAC 发送该内 TAEP 包，NAC 收到该内 TAEP 包后将其 Subdata 字段的值发送给 TNCAP，然后 TNCAP 选取一种内 TAEP 鉴别方法发起内 TAEP 鉴别过程。对 AR 的平台鉴别策略的管理参见附录 B。

l) NAC 根据 TNCAP 选取的一种内 TAEP 鉴别方法与 NAR、APS 交互一系列 TAEP 的 Request 分组和 Response 分组，直到内 TAEP 鉴别方法过程完成。对于 NAC 与 NAR 之间交互的一系列 TAEP 的 Request 分组和 Response 分组，其中 Type 字段的值为步骤 g)中的隧道 TAEP 鉴别方法类型，Type-Data 字段的值为利用步骤 g)建立的安全隧道进行保护的内 TAEP 包。内 TAEP 包的 Type 字段的值为 TNCAP 选取的内 TAEP 鉴别方法类型，Type-Data 字段的值为 TNCAP 选取的内 TAEP 鉴别方法类型对应的内 TAEP 鉴别方法消息。对于 NAC 与 APS 之间交互的一系列 TAEP 的 Request 分组和 Response 分组，其中 Type 字段的值为 TNCAP 选取的内 TAEP 鉴别方法类型，Type-Data 字段的值为 TNCAP 选取的内 TAEP 鉴别方法类型对应的内 TAEP 鉴别方法消息。内 TAEP 鉴别方法消息由可信平台评估层中的 TNCC、TNCAP 和 EPS 进行相应处理。

m) NAC 利用 TAEP 的 Success 分组或 Failure 分组结束鉴别过程，即：若在步骤 l)中的内 TAEP 鉴别方法过程中 TNCAP 成功鉴别 AR 的平台(包括平台身份鉴别和平台完整性评估)，则向 NAR 发送 TAEP 的 Success 分组。若在步骤 l)中的内 TAEP 鉴别方法过程中 TNCAP 不能成功鉴别 AR 的平台，则向 NAR 发送 TAEP 的 Failure 分组。

以上步骤描述了 TCA 的序 TAEP 鉴别实现二的典型 TAEP 交互过程，但根据鉴别方法的不同，步骤过程会有不同。

当外 TAEP 鉴别方法的 Type 字段为 TAEP-WAI 且封装基于证书的 WAI 协议的证书鉴别过程，隧道 TAEP 鉴别方法的 Type 字段为 TAEP-TTLS 且隧道方法为全匿名模式 TLS 协议，内 TAEP 鉴别方法的 Type 字段为 TAEP-PAI 且封装 PAI 协议(7.2.2)时，TCA 的序 TAEP 鉴别实现二的一个完整的 TAEP 交互过程如图 7 所示。

图 7　序列 TAEP 鉴别实现二的 TAEP 交互过程一

在图 7 中，根据 PAI 协议的特点，与 TAEP-PAI 相关的消息 1～消息 6 的 TAEP 交互可能执行多轮次。

在一轮 PAI 协议中，当消息 5 未被生成时，消息 5 和消息 6 的 TAEP 交互不存在。

在一轮 PAI 协议中，当消息 5 被生成，但消息 6 未被生成时，消息 6 的 TAEP 交互存在，其 Data 值为 NULL。

当外 TAEP 鉴别方法的 Type 字段为 TAEP-WAI 且封装基于证书的增强型 WAI 协议（见 6.2.1.3.5）的证书鉴别过程，隧道 TAEP 鉴别方法的 Type 字段为 TAEP-TTLS 且隧道方法为全匿名模

式 TLS 协议，内 TAEP 鉴别方法的 Type 字段为 TAEP-PAI 且封装 PAI 协议(7.2.2)时，TCA 的序 TAEP 鉴别实现二的一个完整的 TAEP 交互过程如图 8 所示。

图 8　序列 TAEP 鉴别实现二的 TAEP 交互过程二

在图 8 中，根据 PAI 协议的特点，与 TAEP-PAI 相关的消息 1～消息 6 的 TAEP 交互可能执行多轮次。

在一轮 PAI 协议中，当消息 5 未被生成时，消息 5 和消息 6 的 TAEP 交互不存在。

在一轮 PAI 协议中，当消息 5 被生成，但消息 6 未被生成时，消息 6 的 TAEP 交互存在，其 Data 值为 NULL。

6.2.1.3.5 增强型 WAI 协议

6.2.1.3.5.1 概述

WAI 协议（见 GB 15629.11—2003 和 GB 15629.11—2003/XG1—2006）中的 STA、AP 和 ASU 分别对应于本标准中的 AR、AC 和 PM。ASUE 驻留在 STA 中，AE 驻留在 AP 或 STA 中，ASE 驻留在 ASU 中。相对于 WAI 协议，增强型 WAI（EWAI）协议增加了 ASUE 与 ASU 之间、AE 和 ASU 之间的密钥协商，使得其证书鉴别过程与 WAI 协议的证书鉴别过程不相同。本标准规定 EWAI 协议中的 STA 和 AP 都信任同一个 ASU。EWAI 协议中未明确规定部分参见 WAI 协议，包括单播密钥协商过程、组播密钥/站间密钥通告过程等。

在执行 EWAI 协议之前，ASUE 和 AE 利用 WAPI 信息元素（见 GB 15629.11—2003 和 GB 15629.11—2003/XG1—2006）协商鉴别和密钥管理套件以及 ASUE 是否需要建立与 ASU 之间的会话密钥及密码套件，具体协商过程不在本标准中规定。

6.2.1.3.5.2 增强型 WAI 协议分组格式

EWAI 协议分组格式与 WAI 协议相同，其中类型字段的值如下：

1 WAI 协议分组；

2 EWAI 协议分组；

其他值保留。

子类型字段的值如下：

1 消息 1；

2 消息 2；

3 消息 3；

4 消息 4；

5 消息 5；

6 消息 6；

7 消息 7；

8 消息 8；

9 消息 9；

其他值保留。

EWAI 协议分组中其他字段的定义与 WAI 协议相同。

6.2.1.3.5.2.1 增强型 WAI 协议分组数据字段的固定内容

a） 标识 FLAG

标识 FLAG 字段中比特 7 表示密钥协商请求标识。若比特 7 的值为 1，表示 ASUE 需要与 ASU 协商它们之间的会话密钥及密码套件，否则不需要。

标识 FLAG 字段中其他比特的定义与 WAI 协议相同。

b） FLAG

长度为 1 个八位位组，格式如图 9 所示。

B0	B1	B2	B3～B7
证书验证请求标识	ASUE与ASU之间密钥协商请求标识	AE与ASU之间密钥协商请求标识	保留

图 9　FLAG

其中：

——证书验证请求标识比特：1 表示需要验证 ASUE 和 AE 的证书；0 表示不需要验证。

——ASUE 和 ASU 之间密钥协商请求标识比特：1 表示需要协商 ASUE 和 ASU 之间的会话密钥及密码套件；0 表示不需要协商。

——AE 与 ASU 之间密钥协商请求标识比特：1 表示需要协商 AE 和 ASU 之间的会话密钥及密码套件；0 表示不需要协商。

EWAI 协议分组数据字段中的其他固定内容定义与 WAI 协议相同。

6.2.1.3.5.2.2　增强型 WAI 协议分组数据字段的属性内容

EWAI 协议分组数据字段的属性内容定义与 WAI 协议相同。

6.2.1.3.5.3　增强型 WAI 协议的证书鉴别过程

EWAI 协议的证书鉴别过程如图 10 所示。

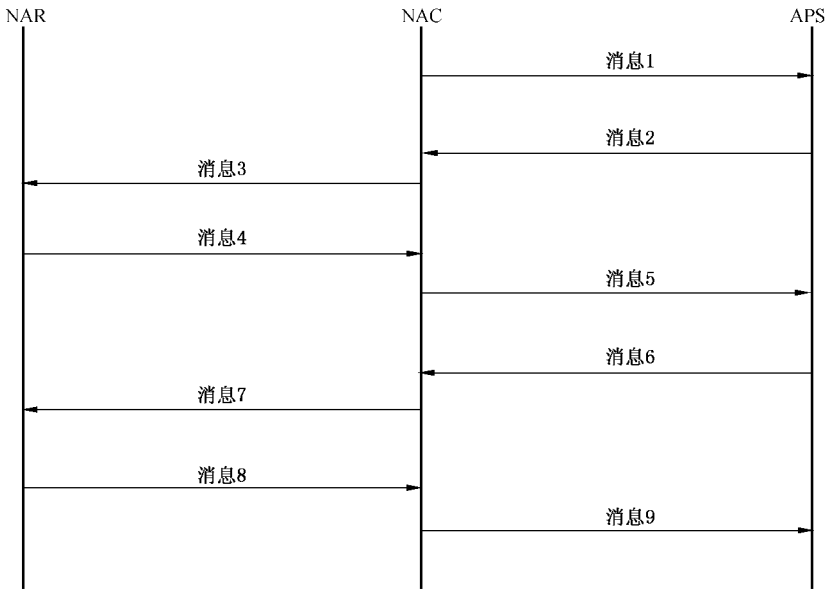

图 10　EWAI 协议的证书鉴别过程

6.2.1.3.5.3.1　消息 1

消息 1 的数据字段格式如图 11 所示。

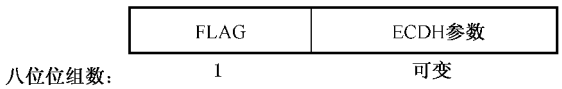

图 11　消息 1 的数据字段格式

其中：

——FLAG 字段长度为 1 个八位组，定义如前，比特 1 和 2 有意义。比特 1 和 2 的值不能同时为 0。

——ECDH 参数字段由参数标识和参数长度和参数内容组成，参数标识字段长度为 1 个八位位组，参数长度字段为 2 个八位位组，表示参数内容字段的八位位组数。参数字段的值定义如下：

- 参数标识为 1 时，参数内容以 OID 方式表示，参数长度字段表示 OID 标识的八位位组数，参数内容为 OID 编码。本规范采用值为 1.2.156.11235.1.1.2.1 的 OID 表示国家密码管理局批准的 ECC 域参数，OID 编码采用 ASN.1/DER。
- 参数标识其他值保留。

当 STA 关联或重新关联至 AP/STA，ASUE 和 AE 选择采用证书鉴别及密钥管理方法，或 AE 收到 ASUE 的预鉴别开始分组时，若 ASUE 需要协商与 ASU 之间的会话密钥及密码套件、或 AE 需要协商与 ASU 之间的会话密钥及密码套件，则 AE 向 ASU 发送消息 1。

ASU 收到消息 1 后，执行如下处理：

a)　利用随机数产生器生成 ASU 询问。

b)　选择 WAPI 信息元素，包含单播密码套件列表、当前使用的鉴别和密钥管理套件，构成 WIE_{ASU}。

c)　依据 FLAG、ECDH 参数、ASU 询问和 WIE_{ASU} 构成消息 2，并发送给 AE。

6.2.1.3.5.3.2　消息 2

消息 2 的数据字段格式如图 12 所示。

图 12　消息 2 的数据字段格式

其中：

——FLAG 字段长度为 1 个八位组，定义如前，比特 1 和 2 有意义。FLAG 字段的值与消息 1 中的 FLAG 字段的值相同。

——ECDH 参数字段长度为可变，其值与消息 1 中的 ECDH 参数字段的值相同。

——ASU 询问字段长度为 32 个八位位组，由 ASU 采用随机数生成算法生成，记作 N_{ASU}。

——WIE_{ASU} 字段长度为可变，是 ASU 选择的 WAPI 信息元素，包含单播密码套件列表、当前鉴别和密钥管理套件。

当 ASU 收到 AE 发送的消息 1 时，ASU 向 AE 发送消息 2。

AE 收到消息 2 后，执行如下处理：

a)　检查 FLAG 字段中比特 1 的值，若值为 0，则执行步骤 b)；否则执行步骤 c)。

b)　检查 FLAG 字段中比特 2 的值，若值为 0，则丢弃消息 1；否则执行步骤 d)。

c)　检查 FLAG 字段中比特 2 的值，若值为 0，则执行步骤 e)；否则执行步骤 f)。

d) 首先生成标识 FLAG 和鉴别标识，然后依据标识 FLAG、鉴别标识、本地 ASU 的身份、STA_{AE} 的证书、ECDH 参数、ASU 询问和 WIE_{ASU} 构成消息 3，并发送给 ASUE。

e) 首先从 WIE_{ASU} 中选择一种用于 AE 与 ASU 之间的单播密码套件，然后生成标识 FLAG 和鉴别标识，最后依据标识 FLAG、鉴别标识、本地 ASU 的身份、STA_{AE} 的证书、ECDH 参数构成消息 3，并发送给 ASUE。

f) 首先从 WIE_{ASU} 中选择一种用于 AE 与 ASU 之间的单播密码套件，然后生成标识 FLAG 和鉴别标识，最后依据标识 FLAG、鉴别标识、本地 ASU 的身份、STA_{AE} 的证书、ECDH 参数、ASU 询问和 WIE_{ASU} 构成消息 3，并发送给 ASUE。

6.2.1.3.5.3.3 消息 3

消息 3 的数据字段格式如图 13 所示。

	标识FLAG	鉴别标识	本地ASU的身份	STA_{AE}的证书	ECDH参数	ASU询问	WIE_{ASU}
八位位组数：	1	32	可变	可变	可变	32	可变

图 13 消息 3 的数据字段格式

其中：

——标识 FLAG 字段长度为 1 个八位位组，定义如前，比特 0、1 和 7 有意义。当 STA 关联或重新关联至 AP 时进行证书鉴别过程，比特 0(BK 更新标识)的值为 0；当证书鉴别过程进行 BK 更新时，比特 0(BK 更新标识)的值为 1。如果不是预鉴别过程，比特 1(预鉴别标识)的值为 0；如果是预鉴别过程，比特 1(预鉴别标识)的值为 1。若标识 FLAG 字段中比特 7 的值为 1，ASU 询问字段和 WIE_{ASU} 字段存在；否则不存在。当比特 0 的值为 1 时，ASUE 不需要与 ASU 协商它们之间的会话密钥及密码套件，AE 也不需要与 ASU 协商它们之间的会话密钥及密码套件。

——鉴别标识字段长度为 32 个八位位组。若标识字段比特 0(BK 更新标识)的值为 0，则鉴别标识字段的值由 AE 采用随机数生成算法生成；若标识字段比特 0(BK 更新标识)的值为 1，则鉴别标识字段的值为上一次证书鉴别过程所协商的鉴别标识。

——本地 ASU 的身份字段标识 AE 信任的 ASU，采用 GB 15629.11—2003/XG1—2006 的 8.1.4.1.1中的定义。

——STA_{AE}(作为 AE 实体的站)的证书字段表示作为 AE 实体的站的证书，采用 GB 15629.11—2003/XG1—2006 的 8.1.4.1.1 的定义。

——ECDH 参数字段长度为可变。若 ASUE 需要协商与 ASU 之间的会话密钥及密码套件、或 AE 需要协商与 ASU 之间的会话密钥及密码套件，则 ECDH 参数字段的值与消息 1 中 ECDH 参数字段的值相同；否则 ECDH 参数字段的值由参数标识和参数长度和参数内容组成，参数标识字段长度为 1 个八位位组，参数长度字段为 2 个八位位组，表示参数内容字段的八位位组数。参数字段的值定义如下：

- 参数标识为 1 时，参数内容以 OID 方式表示，参数长度字段表示 OID 标识的八位位组数，参数内容为 OID 编码。本规范采用值为 1.2.156.11235.1.1.2.1 的 OID 表示国家密码管理局批准的 ECC 域参数，OID 编码采用 ASN.1/DER。
- 参数标识其他值保留。

——ASU 询问字段长度为 32 个八位位组，由 ASU 采用随机数生成算法生成。

——WIE_{ASU} 字段长度为可变，是 ASU 选择的 WAPI 信息元素，包含单播密码套件列表、当前鉴别

和密钥管理套件。

当 STA 关联或重新关联至 AP/STA，ASUE 和 AE 选择采用证书鉴别及密钥管理方法，或 AE 收到 ASUE 的预鉴别开始分组时，若 ASUE 不需要协商与 ASU 之间的会话密钥及密码套件、且 AE 不需要协商与 ASU 之间的会话密钥及密码套件，则 AE 首先生成标识 FLAG 和鉴别标识，然后依据标识 FLAG、鉴别标识、本地 ASU 的身份、STA_{AE}的证书、ECDH 参数构成消息 3，并发送给 ASUE；当 AE 的本地策略要求重新进行证书鉴别过程时，AE 首先生成标识 FLAG 和鉴别标识，然后依据标识 FLAG、鉴别标识、本地 ASU 的身份、STA_{AE}的证书、ECDH 参数构成消息 3，并发送给 ASUE；当 AE 收到 ASU 发送的消息 2 时，AE 向 ASUE 发送消息 3。

ASUE 接收到由 AE 发送的消息 3 后，进行如下处理：

a) ASUE 检查消息 3 中标识字段的比特 0(BK 更新标识)的值，当值为 1 时执行步骤 b)；当值为 0 时执行步骤 c)。

b) ASUE 检查消息 3 中鉴别标识字段与上一次证书鉴别过程中保存的鉴别标识是否一致，若不一致，则丢弃该消息 3；否则执行步骤 c)。

c) 检查标识 FLAG 字段中比特 7 的值，若值为 0，则执行步骤 d)；否则执行步骤 e)。

d) ASUE 根据消息 3 中的 AE 信任的 ASU 身份选择由该 ASU 颁发的证书或者根据本地策略选择证书，产生用于 ECDH 交换的临时私钥 x、临时公钥 x·P 和 32 个八位位组的 ASUE 询问 N_{ASUE}(随机数)，然后依据标识 FLAG、鉴别标识、ASUE 询问、ASUE 密钥数据、STA_{AE}的身份、STA_{ASUE}的证书、ECDH 参数、ASUE 信任的 ASU 列表、ASUE 的签名构成消息 4，并发送给 AE。

e) 首先从 WIE_{ASU}中选择一种用于 ASUE 与 ASU 之间的单播密码套件，然后根据消息 3 中的 AE 信任的 ASU 身份选择由该 ASU 颁发的证书或者根据本地策略选择证书，产生用于 ECDH 交换的临时私钥 x、临时公钥 x·P 和 32 个八位位组的 ASUE 询问 N_{ASUE}(随机数)，最后依据标识 FLAG、鉴别标识、ASUE 询问、ASUE 密钥数据、STA_{AE}的身份、STA_{ASUE}的证书、ECDH 参数、ASUE 信任的 ASU 列表、$WIE_{ASUE\text{-}ASU}$、对 ASUE 密钥数据的签名、ASUE 的签名构成消息 4，并发送给 AE。

6.2.1.3.5.3.4 消息 4

消息 4 的数据字段格式如图 14 所示。

	标识 FLAG	鉴别标识	ASUE 询问	ASUE 密钥数据	STA_{AE} 的身份	STA_{ASUE} 的证书	ECDH 参数	ASUE信任的ASU列表	$WIE_{ASUE\text{-}ASU}$	对ASUE密钥数据的签名	ASUE 的签名
八位位组数：	1	32	32	可变	可变	可变	可变	可变	可变	可变	可变

图 14 消息 4 的数据字段格式

其中：

——标识 FLAG 字段长度为 1 个八位位组，定义如前，比特 0、1、2、3 和 7 有意义。本字段除比特 2(证书验证请求标识)、比特 3(可选字段标识)以外的其他比特，应与 AE 发送的消息 3 中标识字段对应比特相同。比特 2(证书验证请求标识)为 1 表示 ASUE 要求验证 AE 证书的有效性，为 0 表示不需要验证 AE 证书的有效性。当在比特 0(BK 更新标识)为 0 时，比特 2 必须为 1，即不是进行 BK 更新时，必须验证 AE 证书的有效性。比特 3(可选字段标识)为 1 表示分组中有可选字段，为 0 表示没有。若标识 FLAG 字段中比特 7 的值为 1，WIE_{ASU}字段和对

ASUE 密钥数据的签名字段存在;否则不存在。当比特 0 的值为 1 时,ASUE 不需要与 ASU 协商它们之间的会话密钥及密码套件,AE 也不需要与 ASU 协商它们之间的会话密钥及密码套件。

——鉴别标识字段长度为 32 个八位位组。若 ASUE 发起 BK 更新,则鉴别标识字段的值为上一次证书鉴别过程所协商的鉴别标识;否则本字段值应与 AE 发送的消息 3 中鉴别标识字段值相同。

——ASUE 询问字段长度为 32 个八位位组,由 ASUE 采用随机数生成算法生成,记作 N_{ASUE}。

——ECDH 参数字段长度为可变。若 ASUE 发起 BK 更新,则本字段的值与上一次证书鉴别过程的消息 3 中的 ECDH 参数字段的值相同;否则本字段的值应与消息 3 中的 ECDH 参数字段相同。

——ASUE 密钥数据格式如前定义,内容是 ASUE 生成的用于 ECDH 交换的临时公钥。

——STA_{AE}的身份字段,采用 GB 15629.11—2003/XG1—2006 的 8.1.4.1.1 中的定义。

——STA_{ASUE}(作为 ASUE 实体的站)的证书字段表示作为 ASUE 实体的站的证书,采用 GB 15629.11—2003/XG1—2006 的 8.1.4.1.1 的定义。

——STA_{ASUE}信任的服务器列表字段,该字段为可选字段,采用身份列表属性表示,其定义如前。内容包含 STA_{ASUE}信任的服务器,但不包含 STA_{ASUE}的证书颁发者。若 ASUE 除了信任他的证书颁发者以外,还信任其他的某些实体,可以通过该字段通知鉴别服务器。当标识 FLAG 字段中比特 7 的值为 1 时,STA_{ASUE}信任的服务器列表字段的值为消息 3 中本地 ASU 的身份字段的值。

——$WIE_{ASUE\text{-}ASU}$字段长度为可变,是 ASUE 选择的 WAPI 信息元素,包含当前鉴别和密钥管理套件、ASUE 选择的用于 ASUE 与 ASU 之间的单播密码套件。

——对 ASUE 密钥数据的签名字段采用签名属性表示,其定义如前,它是 ASUE 生成的对 ASUE 密钥数据字段的签名。

——ASUE 的签名字段采用签名属性表示,其定义如前,它是对本分组中除本字段之外所有数据字段的签名。

当 ASUE 收到 AE 的消息 3 或 ASUE 要求进行 BK 更新时,ASUE 发送消息 4 给 AE。

AE 收到 ASUE 发来的消息 4 后,进行如下处理:

a) 如果 AE 没有发送消息 3,则检查鉴别标识字段值和上一次证书鉴别过程中保存的鉴别标识是否相同,若相同,执行步骤 b);否则丢弃该分组。如果 AE 发送了消息 3,则比较鉴别标识字段值及标识字段的比特 0、比特 1 与 AE 发送的消息 3 中相应字段的值是否相同,若不同,则丢弃该分组;否则,执行步骤 b)。

b) 检查 STA_{AE}的身份字段是否与自己的身份一致,以及 ECDH 参数字段是否与自己在消息 3 中的 ECDH 参数一致,若不一致,则丢弃该分组;否则验证 ASUE 签名,若验证不通过,则丢弃该分组;若标识字段的比特 2 为 1 或 AE 的本地策略要求使用 ASU 鉴别 STA_{ASUE}的证书,则设置 FLAG 字段中比特 0 的值为 1,然后执行步骤 c);否则执行步骤 h)。

c) 若消息 4 中比特 7 的值为 0 且 AE 不需要与 ASU 协商它们之间的会话密钥及密码套件,则执行步骤 d);若消息 4 中比特 7 的值为 1 且消息 1 中比特 2 的值为 0,则执行步骤 e);若消息 4 中比特 7 的值为 0 且消息 1 中比特 2 的值为 1,则执行步骤 f);若消息 4 中比特 7 的值为 1 且消息 1 中比特 2 的值为 1,则执行步骤 g)。

d) 依据 FLAG、ADDID、AE 询问、ASUE 询问、STA_{ASUE}的证书、STA_{AE}的证书、ASUE 信任的 ASU 列表构成消息 5,并发送给 ASU。

e) 依据 FLAG、ADDID、AE 询问、ASUE 询问、STA_{ASUE}的证书、STA_{AE}的证书、ASUE 信任的 ASU 列表、$WIE_{ASUE\text{-}ASU}$、ASUE 密钥数据、对 ASUE 密钥数据的签名构成消息 5,并发送

给 ASU。

f) 首先产生用于 ECDH 交换的临时私钥 y、临时公钥 y·P 和 32 个八位位组的 AE 询问 N_{AE}(随机数),然后依据 FLAG、ADDID、AE 询问、ASUE 询问、STA_{ASUE} 的证书、STA_{AE} 的证书、ASUE 信任的 ASU 列表、$WIE_{AE\text{-}ASU}$、AE 密钥数据、对 AE 密钥数据的签名构成消息 5,并发送给 ASU。

g) 首先产生用于 ECDH 交换的临时私钥 y、临时公钥 y·P 和 32 个八位位组的 AE 询问 N_{AE}(随机数),然后依据 FLAG、ADDID、AE 询问、ASUE 询问、STA_{ASUE} 的证书、STA_{AE} 的证书、ASUE 信任的 ASU 列表、$WIE_{ASUE\text{-}ASU}$、ASUE 密钥数据、对 ASUE 密钥数据的签名、$WIE_{AE\text{-}ASU}$、AE 密钥数据、对 AE 密钥数据的签名构成消息 5,并发送给 ASU。

h) 若消息 4 中比特 7 的值为 0 且 AE 不需要与 ASU 协商它们之间的会话密钥及密码套件,则执行步骤 i);若消息 4 中比特 7 的值为 1 且比特 2 的值为 0,则执行步骤 j);若消息 4 中比特 7 的值为 0 且比特 2 的值为 1,则执行步骤 k);若消息 4 中比特 7 的值为 1 且比特 2 的值为 1,则执行步骤 1)。

i) AE 本地鉴别 STA_{ASUE} 的证书,即根据本地缓存的 STA_{ASUE} 证书的验证结果及其根据本地策略所定义的时效性确定 STA_{ASUE} 证书的验证结果。若 STA_{ASUE} 证书为有效,则 AE 首先设定接入结果为成功,然后本地生成用于 ECDH 交换的临时私钥 y、临时公钥 y·P 和 32 个八位位组的 AE 询问 N_{AE}(随机数),使用自己的临时私钥 y 和消息 4 中 ASUE 的临时公钥 x·P 进行 ECDH 计算,得到主密钥种子$(x\cdot y\cdot P)_{abscissa}$,对其进行扩展 KD-HMAC-SHA256$((x\cdot y\cdot P)_{abscissa}, N_{AE}||N_{ASUE}||$"base key expansion for key and additional nonce"),生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子,接着对该鉴别标识种子进行 SHA-256 运算,得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识,接着将标识字段的比特 3(可选字段标识)置为 0,表示没有可选字段,最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、AE 的签名构成消息 7,并发送给 ASUE。若 STA_{ASUE} 证书为无效,则 AE 首先设定接入结果为不成功,然后设置 AE 的询问 N_{AE} 和 AE 的密钥数据(AE 的临时公钥)为任意值,接着将标识字段的比特 3(可选字段标识)置为 0,表示没有可选字段,最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、AE 的签名构成消息 7,并发送给 ASUE。

j) AE 本地鉴别 STA_{ASUE} 的证书,即根据本地缓存的 STA_{ASUE} 证书的验证结果及其根据本地策略所定义的时效性确定 STA_{ASUE} 证书的验证结果。若 STA_{ASUE} 证书为有效,则依据 FLAG、ADDID、ASUE 询问、STA_{ASUE} 的证书、$WIE_{ASUE\text{-}ASU}$、ASUE 密钥数据、对 ASUE 密钥数据的签名构成消息 5,并发送给 ASU。若 STA_{ASUE} 证书为无效,则 AE 首先设定接入结果为不成功,然后设置 AE 的询问 N_{AE}、AE 的密钥数据(AE 的临时公钥)、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码为任意值,接着将标识字段的比特 3(可选字段标识)置为 0,表示没有可选字段,最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、AE 的签名构成消息 7,并发送给 ASUE。

k) AE 本地鉴别 STA_{ASUE} 的证书,即根据本地缓存的 STA_{ASUE} 证书的验证结果及其根据本地策略所定义的时效性确定 STA_{ASUE} 证书的验证结果。若 STA_{ASUE} 证书为有效,则首先产生用于 ECDH 交换的临时私钥 y、临时公钥 y·P 和 32 个八位位组的 AE 询问 N_{AE}(随机数),然后依据 FLAG、ADDID、AE 询问、STA_{AE} 的证书、$WIE_{AE\text{-}ASU}$、AE 密钥数据、对 AE 密钥数据的签名构成消息 5,并发送给 ASU。若 STA_{ASUE} 证书为无效,则 AE 首先设定接入结果为不成功,然后设置 AE 的询问 N_{AE} 和 AE 的密钥数据(AE 的临时公钥)为任意值,接着将标识字段的比特

3(可选字段标识)置为0,表示没有可选字段,最后依据标识FLAG、ASUE询问、AE询问、接入结果、ASUE密钥数据、AE密钥数据、STA_{AE}的身份、STA_{ASUE}的身份、AE的签名构成消息7,并发送给ASUE。

l) AE本地鉴别STA_{ASUE}的证书,即根据本地缓存的STA_{ASUE}证书的验证结果及其根据本地策略所定义的时效性确定STA_{ASUE}证书的验证结果。若STA_{ASUE}证书为有效,则首先产生用于ECDH交换的临时私钥y、临时公钥y·P和32个八位位组的AE询问N_{AE}(随机数),然后依据FLAG、ADDID、AE询问、ASUE询问、STA_{ASUE}的证书、STA_{AE}的证书、$WIE_{ASUE-ASU}$、ASUE密钥数据、对ASUE密钥数据的签名、WIE_{AE-ASU}、AE密钥数据、对AE密钥数据的签名构成消息5,并发送给ASU。若STA_{ASUE}证书为无效,则AE首先设定接入结果为不成功,然后设置AE的询问N_{AE}、AE的密钥数据(AE的临时公钥)、ASU密钥数据、对ASU密钥数据的签名、ASU-ASUE消息鉴别码为任意值,接着将标识字段的比特3(可选字段标识)置为0,表示没有可选字段,最后依据标识FLAG、ASUE询问、AE询问、接入结果、ASUE密钥数据、AE密钥数据、STA_{AE}的身份、STA_{ASUE}的身份、ASU密钥数据、对ASU密钥数据的签名、ASU-ASUE消息鉴别码、AE的签名构成消息7,并发送给ASUE。

6.2.1.3.5.3.5 消息5

消息5的数据字段格式如图15所示。

	FLAG	ADDID	AE询问	ASUE询问	STA_{ASUE}的证书	STA_{AE}的证书	ASUE信任的ASU列表	$WIE_{ASUE-ASU}$	ASUE密钥数据	对ASUE密钥数据的签名	WIE_{AE-ASU}	AE密钥数据	对AE密钥数据的签名
八位位组数:	1	12	32	32	可变	可变	可变	可变	可变	可变	可变	可变	可变

图15 消息5的数据字段格式

其中:

——FLAG字段长度为1个八位位组,定义如前,比特0、1和2有意义。若标识FLAG字段的比特2为1或AE的本地策略要求使用ASU鉴别STA_{ASUE}的证书,则设置FLAG字段中比特0的值为1;否则设置为0。若ASUE需要与ASU协商它们之间的会话密钥及密码套件,则设置FLAG字段中比特1的值为1;否则设置为0。若AE需要与ASU协商它们之间的会话密钥及密码套件,则设置FLAG字段中比特2的值为1;否则设置为0。

——ADDID字段长度为12个八位位组,由$MAC_{AE}||MAC_{ASUE}$组成。当FLAG字段中比特0的值为1时,本字段存在。

——AE询问字段长度为32个八位位组。由AE采用随机数生成算法生成,记作N_{AE}。当FLAG字段中比特0或比特1的值为1时,本字段存在。

——ASUE询问字段长度为32个八位位组。本字段值应与ASUE发送的消息4中ASUE询问字段值相同。当FLAG字段中比特0或比特2的值为1时,本字段存在。

——STA_{ASUE}的证书字段,定义如前。该字段和消息4中STA_{ASUE}的证书字段相同。当FLAG字段中比特0或比特2的值为1时,本字段存在。

——STA_{AE}的证书字段,定义如前。内容包含STA_{AE}的证书。当FLAG字段中比特0或比特1的值为1时,本字段存在。

——ASUE信任的服务器列表字段,该字段为可选字段,采用身份列表属性表示,其定义如前。本字段值应与ASUE发送的消息4中的ASUE信任的服务器列表字段相同。当FLAG字段中

比特 0 的值为 1 时，本字段存在。

——$WIE_{ASUE\text{-}ASU}$字段长度为可变，其值与消息 4 中 $WIE_{ASUE\text{-}ASU}$字段的值相同。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——ASUE 密钥数据字段长度为可变，其值与消息 4 中 ASUE 密钥数据字段的值相同。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——对 ASUE 密钥数据字段长度为可变，其值与消息 4 中对 ASUE 密钥数据字段的值相同。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——$WIE_{AE\text{-}ASU}$字段长度为可变，是 AE 选择的 WAPI 信息元素，包含当前鉴别和密钥管理套件、AE 选择的用于 AE 与 ASU 之间的单播密码套件。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

——AE 密钥数据格式如前定义，内容是 AE 生成的用于 ECDH 交换的临时公钥。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

——对 AE 密钥数据的签名字段采用签名属性表示，其定义如前，它是 AE 生成的对 AE 密钥数据字段的签名。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

当消息 4 中标识 FLAG 指示要进行证书验证或 AE 自己需要进行证书验证，或 ASUE 需要与 ASU 协商它们之间的会话密钥及密码套件，或 AE 需要与 ASU 协商它们之间的会话密钥及密码套件时，AE 向 ASU 发送消息 5。

AE 接收到 ASUE 发送的消息 4 后，向 ASU 发送消息 5。在消息 5 超时时间内 AE 不对 ASUE 发送的消息 4 进行处理。

ASU 收到消息 5 后，进行如下处理：

a) 检查 FLAG 字段中的比特 0 的值，若值为 0，则执行步骤 b)；否则执行步骤 f)。

b) 检查消息 1 中 FLAG 字段中比特 1 和 2 的值，若比特 1 的值为 0 且比特 2 的值为 0，则丢弃消息 5；若比特 1 的值为 1 且比特 2 的值为 0，则执行步骤 c)；若比特 1 的值为 0 且比特 2 的值为 1，则执行步骤 d)；若比特 1 的值为 1 且比特 2 的值为 1，则执行步骤 e)。

c) 首先生成用于 ECDH 交换的临时私钥 z 和临时公钥 z · P，然后计算 KD-HMAC-SHA256 ($(x \cdot z \cdot P)_{abscissa}$，ADDID|| N_{ASU} ||N_{ASUE} ||“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU}为 ASU 询问，N_{ASUE}为 ASUE 询问，生成 48 个八位位组为 ASU 与 ASUE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，最后依据 FLAG、ADDID、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码构成消息 6，并发送给 AE。

d) 首先生成用于 ECDH 交换的临时私钥 z 和临时公钥 z · P，然后计算 KD-HMAC-SHA256 ($(y \cdot z \cdot P)_{abscissa}$，ADDID|| N_{ASU} ||N_{AE} ||“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU}为 ASU 询问，N_{AE}为 AE 询问，生成 48 个八位位组为 ASU 与 AE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，最后依据 FLAG、ADDID、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-AE 消息鉴别码构成消息 6，并发送给 AE。

e) 首先生成用于 ECDH 交换的临时私钥 z 和临时公钥 z · P，然后计算 KD-HMAC-SHA256 ($(x \cdot z \cdot P)_{abscissa}$，ADDID|| N_{ASU} ||N_{ASUE} ||“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU}为 ASU 询问，N_{ASUE}为 ASUE 询问，生成 48 个八位位组为 ASU 与 ASUE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，接着计算

KD-HMAC-SHA256 ((y · z · P)$_{abscissa}$，ADDID|| N_{ASU} ||N_{AE} ||“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU} 为 ASU 询问，N_{AE} 为 AE 询问，生成 48 个八位位组为 ASU 与 AE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，最后依据 FLAG、ADDID、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、ASU-AE 消息鉴别码构成消息 6，并发送给 AE。

f) 检查消息 1 中 FLAG 字段中比特 1 和 2 的值，若比特 1 的值为 0 且比特 2 的值为 0，则执行步骤 g)；若比特 1 的值为 1 且比特 2 的值为 0，则执行步骤 h)；若比特 1 的值为 0 且比特 2 的值为 1，则执行步骤 i)；若比特 1 的值为 1 且比特 2 的值为 1，则执行步骤 j)。

g) 首先 ASU 参照 RFC3280 验证 STA_{AE}证书和 STA_{ASUE}证书，并生成 STA_{AE}证书和 STA_{ASUE}证书的验证结果及签名，然后依据 FLAG、ADDID、证书的验证结果、ASU 的签名构成消息 6，并发送给 AE。

h) 首先 ASU 参照 RFC 3280 验证 STA_{AE}证书和 STA_{ASUE}证书，并生成 STA_{AE}证书和 STA_{ASUE}证书的验证结果及签名，然后生成用于 ECDH 交换的临时私钥 z 和临时公钥 z · P，接着计算 KD-HMAC-SHA256 ((x · z · P)$_{abscissa}$，ADDID|| N_{ASU} ||N_{ASUE} ||“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU} 为 ASU 询问，N_{ASUE} 为 ASUE 询问，生成 48 个八位位组为 ASU 与 ASUE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，最后依据 FLAG、ADDID、证书的验证结果、ASU 的签名、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码构成消息 6，并发送给 AE。

i) 首先 ASU 参照 RFC 3280 验证 STA_{AE}证书和 STA_{ASUE}证书，并生成 STA_{AE}证书和 STA_{ASUE}证书的验证结果及签名，然后生成用于 ECDH 交换的临时私钥 z 和临时公钥 z · P，接着计算 KD-HMAC-SHA256 ((y · z · P)$_{abscissa}$，ADDID|| N_{ASU} ||N_{AE} ||“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU} 为 ASU 询问，N_{AE} 为 AE 询问，生成 48 个八位位组为 ASU 与 AE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，最后依据 FLAG、ADDID、证书的验证结果、ASU 的签名、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-AE 消息鉴别码构成消息 6，并发送给 AE。

j) 首先 ASU 参照 RFC 3280 验证 STA_{AE}证书和 STA_{ASUE}证书，并生成 STA_{AE}证书和 STA_{ASUE}证书的验证结果及签名，然后生成用于 ECDH 交换的临时私钥 z 和临时公钥 z · P，接着计算 KD-HMAC-SHA256 ((x · z · P)$_{abscissa}$，ADDID|| N_{ASU} ||N_{ASUE} ||“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU} 为 ASU 询问，N_{ASUE} 为 ASUE 询问，生成 48 个八位位组为 ASU 与 AE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，接着计算 KD-HMAC-SHA256 ((y · z · P)$_{abscissa}$，ADDID|| N_{ASU} ||N_{AE} ||“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU} 为 ASU 询问，N_{AE} 为 AE 询问，生成 48 个八位位组为 ASU 与 ASUE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，最后依据 FLAG、ADDID、证书的验证结果、ASU 的签名、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、ASU-AE 消息鉴别码构成消息 6，并发送给 AE。

6.2.1.3.5.3.6 消息 6

消息 6 的数据字段格式如图 16 所示。

	FLAG	ADDID	证书的验证结果	ASU的签名	ASU密钥数据	对ASU密钥数据的签名	ASU-ASUE消息鉴别码	ASU-AE消息鉴别码
八位位组数：	1	12	可变	可变	可变	可变	20	20

图 16　消息 6 的数据字段格式

其中：

——FLAG 字段长度为 1 个八位位组，定义如前，比特 0、1 和 2 有意义。比特 0、1 和 2 的值分别与消息 5 中比特 0、1 和 2 的值相同。

——ADDID 字段长度为 12 个八位位组。该字段值和消息 5 中的 ADDID 字段的值相同。

——证书的验证结果字段采用证书验证结果属性表示，其格式定义如前。字段中的第一个一次性随机数值和消息 5 中的 AE 询问值相同，第二个一次性随机数值和消息 5 中的 ASUE 询问值相同。字段中的第一个证书及结果对应于消息 5 中的 STA_{ASUE} 证书，第二个证书及结果对应于消息 5 中的 STA_{AE} 证书。当 FLAG 字段中比特 0 的值为 1 时，本字段存在。验证结果定义如下：

0　表示证书有效；

1　表示证书的颁发者不明确；

2　表示证书基于不可信任的根证书；

3　表示证书未到生效期或已过期；

4　表示签名错误；

5　表示证书已吊销；

6　表示证书未按规定用途使用；

7　表示证书吊销状态未知；

8　表示证书错误原因未知；

其他值保留。

——ASU 的签名字段采用签名属性表示，其定义如前。它对证书的验证结果字段的签名。当 FLAG 字段中比特 0 的值为 1 时，本字段存在。

——ASU 密钥数据格式如前定义，内容是 ASU 生成的用于 ECDH 交换的临时公钥。当 FLAG 字段中比特 1 或 2 的值为 1 时，本字段存在。

——对 ASU 密钥数据的签名字段采用签名属性表示，其定义如前，它是 ASU 生成的对 ASU 密钥数据字段的签名。当 FLAG 字段中比特 0 或 1 的值为 1 时，本字段存在。

——ASU-ASUE 消息鉴别码字段长度为 20 个八位位组，其值为 ASU 利用最新协商的 ASU 与 ASUE 之间的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对消息 2 中的 WIE_{ASU} 和 ASU 询问，消息 5 中的 $WIE_{ASUE-ASU}$、ASUE 询问、STA_{ASUE} 的证书、ASUE 密钥数据和对 ASUE 密钥数据的签名，消息 6 中 ASU 密钥数据和对 ASU 密钥数据的签名计算得到。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——ASU-AE 消息鉴别码字段长度为 20 个八位位组，其值为 ASU 利用最新协商的 ASU 与 AE 之间的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对消息 1、消息 2、消息 5 和消息 6 本字段之前的所有字段计算得到，不包含各个消息的分组头。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

ASU 收到消息 5 后，向 AE 发送消息 6。

AE 收到消息 6 后，进行如下处理：

a) 检查 FLAG 字段中的比特 0 的值，若值为 0，则执行步骤 b)；否则执行步骤 f)。

b) 检查消息 1 中 FLAG 字段中比特 1 和 2 的值，若比特 1 的值为 0 且比特 2 的值为 0，则丢弃消息 5；若比特 1 的值为 1 且比特 2 的值为 0，则执行步骤 c)；若比特 1 的值为 0 且比特 2 的值为 1，则执行步骤 d)；若比特 1 的值为 1 且比特 2 的值为 1，则执行步骤 e)。

c) 首先本地生成用于 ECDH 交换的临时私钥 y、临时公钥 y·P 和 32 个八位位组的 AE 询问 N_{AE}（随机数），使用自己的临时私钥 y 和消息 4 中 ASUE 的临时公钥 x·P 进行 ECDH 计算，得到主密钥种子$(x\cdot y\cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256[$(x\cdot y\cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”]，生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，然后对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识，接着设定接入结果为成功，接着将标识字段的比特 3（可选字段标识）置为 0，表示没有可选字段，最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、AE 的签名构成消息 7，并发送给 ASUE。

d) 首先验证对 ASU 密钥数据的签名，若验证不通过，则丢弃消息 6；否则计算 KD-HMAC-SHA256（$(y\cdot z\cdot P)_{abscissa}$，ADDID$||N_{ASU}||N_{AE}||$“pairwise key expansion for unicast and additional keys and nonce”），其中 N_{ASU} 为 ASU 询问，N_{AE} 为 AE 询问，生成 48 个八位位组为 ASU 与 AE 之间的单播会话密钥（第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK），然后验证 ASU-AE 消息鉴别码，若验证不通过，则丢弃消息 6；否则使用自己的临时私钥 y 和消息 4 中 ASUE 的临时公钥 x·P 进行 ECDH 计算，得到主密钥种子$(x\cdot y\cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256（$(x\cdot y\cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”），生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，接着对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识，接着设定接入结果为成功，接着将标识字段的比特 3（可选字段标识）置为 0，表示没有可选字段，最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、AE 的签名构成消息 7，并发送给 ASUE。

e) 首先验证对 ASU 密钥数据的签名，若验证不通过，则丢弃消息 6；否则计算 KD-HMAC-SHA256（$(y\cdot z\cdot P)_{abscissa}$，ADDID$||N_{ASU}||N_{AE}||$“pairwise key expansion for unicast and additional keys and nonce”），其中 N_{ASU} 为 ASU 询问，N_{AE} 为 AE 询问，生成 48 个八位位组为 ASU 与 AE 之间的单播会话密钥（第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK），然后验证 ASU-AE 消息鉴别码，若验证不通过，则丢弃消息 6；否则使用自己的临时私钥 y 和消息 4 中 ASUE 的临时公钥 x·P 进行 ECDH 计算，得到主密钥种子$(x\cdot y\cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256（$(x\cdot y\cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”），生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，接着对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识，接着设定接入结果为成功，接着将标识字段的比特 3（可选字段标识）置为 0，表示没有可选字段，最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、AE 的签名构成消息 7，并发送给 ASUE。

f) 检查消息 1 中 FLAG 字段中比特 1 和 2 的值，若比特 1 的值为 0 且比特 2 的值为 0，则执行步骤 g)；若比特 1 的值为 1 且比特 2 的值为 0，则执行步骤 h)；若比特 1 的值为 0 且比特 2 的值为 1，则执行步骤 i)；若比特 1 的值为 1 且比特 2 的值为 1，则执行步骤 j)。

g) 首先根据 ADDID 确定对应的消息 6，检查证书的验证结果字段中的第一个一次性随机数值与自己在消息 5 中的 AE 的询问是否相同，若不相同，则丢弃消息 6；否则验证 ASU 的签名，若不正确，则丢弃消息 6；否则：若 STA_{ASUE} 证书为有效，则首先设定接入结果为成功，然后本地生成用于 ECDH 交换的临时私钥 y 和临时公钥 y · P，使用自己的临时私钥 y 和 ASUE 的临时公钥 x · P 进行 ECDH 计算，得到密钥种子 $(x \cdot y \cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256 ($(x \cdot y \cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”)，生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，然后对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识并保存，最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、复合的证书验证结果、AE 的签名构成消息 7(若标识 FLAG 字段的比特 2 为 0，则消息 7 不包含复合的证书验证结果)，并发送给 ASUE；若 STA_{ASUE} 证书为无效，则首先 AE 设定接入结果为不成功，AE 的询问 N_{AE} 和 AE 的密钥数据(AE 的临时公钥)设置为任意值，然后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、复合的证书验证结果、AE 的签名构成消息 7(若标识 FLAG 字段的比特 2 为 0，则消息 7 不包含复合的证书验证结果)，并发送给 ASUE。

h) 首先根据 ADDID 确定对应的消息 6，检查证书的验证结果字段中的第一个一次性随机数值与自己在消息 5 中的 AE 的询问是否相同，若不相同，则丢弃消息 6；否则验证 ASU 的签名，若不正确，则丢弃消息 6；否则：若 STA_{ASUE} 证书为有效，则首先设定接入结果为成功，然后本地生成用于 ECDH 交换的临时私钥 y 和临时公钥 y · P，使用自己的临时私钥 y 和 ASUE 的临时公钥 x · P 进行 ECDH 计算，得到密钥种子 $(x \cdot y \cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256 ($(x \cdot y \cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”)，生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，然后对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识并保存，最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、复合的证书验证结果、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、AE 的签名构成消息 7(若标识 FLAG 字段的比特 2 为 0，则消息 7 不包含复合的证书验证结果)，并发送给 ASUE；若 STA_{ASUE} 证书为无效，则 AE 首先设定接入结果为不成功，AE 的询问 N_{AE} 和 AE 的密钥数据(AE 的临时公钥)可设置任意值，然后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE} 的身份、STA_{ASUE} 的身份、复合的证书验证结果、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、AE 的签名构成消息 7(若标识 FLAG 字段的比特 2 为 0，则消息 7 不包含复合的证书验证结果)，并发送给 ASUE。

i) 首先验证对 ASU 密钥数据的签名，若验证不通过，则丢弃消息 6；否则计算 KD-HMAC-SHA256 ($(y \cdot z \cdot P)_{abscissa}$，ADDID$||$ $N_{ASU}||N_{AE}||$“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU} 为 ASU 询问，N_{AE} 为 AE 询问，生成 48 个八位位组为 ASU 与 AE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，然后验证 ASU-AE 消息鉴别码，若验证不通过，则丢弃消息 6；否则根据 ADDID 确定对应的消息 6，检查证书的验证结果字段中的第一个一次性随机数值与自己在消息 5 中的 AE 的询问是否相

同，若不相同，则丢弃消息 6；否则验证 ASU 的签名，若不正确，则丢弃消息 6；否则若 STA_{ASUE} 证书为有效，则首先设定接入结果为成功，然后使用自己的临时私钥 y 和 ASUE 的临时公钥 x·P 进行 ECDH 计算，得到密钥种子$(x \cdot y \cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256 ($(x \cdot y \cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”)，生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，然后对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识并保存，最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE}的身份、STA_{ASUE}的身份、复合的证书验证结果、AE 的签名构成消息 7(若标识 FLAG 字段的比特 2 为 0，则消息 7 不包含复合的证书验证结果)，并发送给 ASUE；若 STA_{ASUE}证书为无效，AE 首先设定接入结果为不成功，然后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE}的身份、STA_{ASUE}的身份、复合的证书验证结果、AE 的签名构成消息 7(若标识 FLAG 字段的比特 2 为 0，则消息 7 不包含复合的证书验证结果)，并发送给 ASUE。

j) 首先验证对 ASU 密钥数据的签名，若验证不通过，则丢弃消息 6；否则计算 KD-HMAC-SHA256 ($(y \cdot z \cdot P)_{abscissa}$，ADDID|| $N_{ASU}||N_{AE}||$“pairwise key expansion for unicast and additional keys and nonce”)，其中 N_{ASU}为 ASU 询问，N_{AE}为 AE 询问，生成 48 个八位位组为 ASU 与 AE 之间的单播会话密钥(第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK)，然后验证 ASU-AE 消息鉴别码，若验证不通过，则丢弃消息 6；否则根据 ADDID 确定对应的消息 6，检查证书的验证结果字段中的第一个一次性随机数值与自己在消息 5 中的 AE 的询问是否相同，若不相同，则丢弃消息 6；否则验证 ASU 的签名，若不正确，则丢弃消息 6；否则若 STA_{ASUE} 证书为有效，则首先设定接入结果为成功，然后使用自己的临时私钥 y 和 ASUE 的临时公钥 x·P进行 ECDH 计算，得到密钥种子$(x \cdot y \cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256 ($(x \cdot y \cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”)，生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，接着对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识并保存，最后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE}的身份、STA_{ASUE}的身份、复合的证书验证结果、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、AE 的签名构成消息 7(若标识 FLAG 字段的比特 2 为 0，则消息 7 不包含复合的证书验证结果)，并发送给 ASUE；若 STA_{ASUE}证书为无效，AE 首先设定接入结果为不成功，然后依据标识 FLAG、ASUE 询问、AE 询问、接入结果、ASUE 密钥数据、AE 密钥数据、STA_{AE}的身份、STA_{ASUE}的身份、复合的证书验证结果、ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码、AE 的签名构成消息 7(若标识 FLAG 字段的比特 2 为 0，则消息 7 不包含复合的证书验证结果)，并发送给 ASUE。

6.2.1.3.5.3.7 消息 7

消息 7 的数据字段格式如图 17 所示。

	标识 FLAG	ASUE 询问	AE 询问	接入结果	ASUE 密钥数据	AE密钥数据	STA_{AE} 的身份	STA_{ASUE} 身份	复合的证书验证结果	ASU 密钥数据	对ASU密钥数据的签名	ASU-ASUE消息鉴别码	AE 的签名
八位位组数：	1	32	32	1	可变	可变	可变	可变	可变	可变	可变	20	可变

图 17 消息 7 的数据字段格式

其中：

——标识 FLAG 字段长度为 1 个八位位组，定义如前，比特 0、1、3 和 7 有意义。本字段比特 0、比特 1 应与 ASUE 发送的消息 4 中标识字段值相同。比特 3(可选字段标识)由 ASUE 根据上下文环境设置。比特 3(可选字段标识)为 1 表示分组中有可选字段(复合的证书验证结果)，为 0 表示没有。若本字段中比特 7 的值为 1，则 ASU 密钥数据字段、对 ASU 密钥数据的签名字段和 ASU-ASUE 消息鉴别码字段存在；否则不存在。

——ASUE 询问字段长度为 32 个八位位组。本字段值应与 ASUE 发送的消息 4 中 ASUE 的询问字段值相同。

——AE 询问字段长度为 32 个八位位组。字段值应与 AE 发送的消息 5 中 AE 的询问字段值相同。

——ASUE 密钥数据格式如前定义，内容是 ASUE 生成的用于 ECDH 交换的临时公钥，本字段值应与 ASUE 发送的消息 4 中 ASUE 密钥数据字段值相同。

——AE 密钥数据格式如前定义，内容是 AE 生成的用于 ECDH 交换的临时公钥。

——STA_{AE}的身份字段，定义如前。

——STA_{ASUE}的身份字段，定义如前。

——接入结果字段的长度为 1 个八位位组，其定义如前。具体意义如下：

0　表示接入成功，对应证书验证结果值为 0；

1　表示无法验证证书，对应证书验证结果值为 1；

2　表示证书错误，对应证书验证结果除 0 和 1 之外的其他值；

3　表示本地策略禁止。

其他值保留。

——复合的证书验证结果字段是可选的，若存在，则由消息 6 中证书的验证结果和 ASU 的签名两个字段组成，并且内容和它们相同。

——ASU 密钥数据格式如前定义，其值与消息 6 中的 ASU 密钥数据字段相同。

——对 ASU 密钥数据的签名字段采用签名属性表示，其定义如前，其值与消息 6 中对 ASU 密钥数据的签名字段相同。

——ASU-ASUE 消息鉴别码字段长度为 20 个八位位组，其值与消息 6 中 ASU-ASUE 消息鉴别码字段相同。

——AE 的签名字段采用签名属性表示，其定义如前。它是对本分组中除本字段之外所有数据字段的签名。

AE 收到消息 6，或收到消息 4 后，发送消息 7。

ASUE 收到消息 7 后，进行如下处理：

a) 根据 STA_{AE}的身份和 STA_{ASUE}的身份判断是否为对应当前消息 4 的消息 7，若不是，则丢弃消息 7；否则，执行步骤 b)。

b) 检查标识字段的比特 0、比特 1 与自己发送的消息 4 中相应字段的值是否相同，若不相同，则丢弃消息 7；否则执行步骤 c)。

c) 比较 ASUE 的询问与自己在消息 4 中发送的 ASUE 询问是否相同、比较 ASUE 密钥数据与 ASUE 发送的消息 4 中 ASUE 密钥数据是否相同，若不相同，则丢弃消息 7；否则执行步骤 d)。

d) 验证 AE 的签名是否正确，若不正确，则丢弃消息 7；否则若消息 7 中的接入结果为不成功，则解除与该 STA_{AE}的链路验证；否则执行步骤 e)。

e) 若 ASUE 在消息 4 中不要求进行证书验证，则执行步骤 f)；否则执行步骤 i)。

f) 检查标识 FLAG 字段中比特 7 的值，若值为 0，则执行步骤 g)；否则执行步骤 h)。

g) 本地鉴别 STA_{AE} 的证书，即根据本地缓存的 STA_{AE} 证书的验证结果及其根据本地策略所定义的时效性确定 STA_{AE} 证书的验证结果。若 STA_{AE} 证书为无效，则解除与该 STA_{AE} 的链路验证；若 STA_{AE} 证书为有效，则 ASUE 使用自己的临时私钥 x 和 AE 的临时公钥 y·P 进行 ECDH 计算，得到密钥种子 $(x \cdot y \cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256（$(x \cdot y \cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”），生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，然后对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识。

h) 首先验证对 ASU 密钥数据的签名，若验证不通过，则丢弃消息 7；否则计算 KD-HMAC-SHA256（$(x \cdot z \cdot P)_{abscissa}$，ADDID$||N_{ASU}||N_{ASUE}||$“pairwise key expansion for unicast and additional keys and nonce”），其中 N_{ASU} 为 ASU 询问，N_{ASUE} 为 ASUE 询问，生成 48 个八位位组为 ASU 与 ASUE 之间的单播会话密钥（第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK），然后验证 ASU-ASUE 消息鉴别码，若验证不通过，则丢弃消息 7；否则：本地鉴别 STA_{AE} 的证书，即根据本地缓存的 STA_{AE} 证书的验证结果及其根据本地策略所定义的时效性确定 STA_{AE} 证书的验证结果。若 STA_{AE} 证书为无效，则解除与该 STA_{AE} 的链路验证；若 STA_{AE} 证书为有效，则 ASUE 使用自己的临时私钥 x 和 AE 的临时公钥 y·P 进行 ECDH 计算，得到密钥种子 $(x \cdot y \cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256（$(x \cdot y \cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”），生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，然后对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识。最后依据标识 FLAG、ASUE-ASU 消息鉴别码构成消息 8，并发送给 AE。

i) 检查标识 FLAG 字段中比特 7 的值，若值为 0，则执行步骤 j）；否则执行步骤 k）。

j) ASUE 检查证书的验证结果字段中的第二个一次性随机数值与自己在消息 4 中的 ASUE 询问是否相同，若不相同，则丢弃消息 7；否则验证 ASU 签名，若不正确，则丢弃消息 7；否则检查 AE 证书的鉴别结果，若 STA_{AE} 证书为无效，解除与该 STA_{AE} 的链路验证；若 STA_{AE} 证书为有效，则 ASUE 使用自己的临时私钥 x 和 AE 的临时公钥 y·P 进行 ECDH 计算，得到密钥种子 $(x \cdot y \cdot P)_{abscissa}$，对其进行扩展 KD-HMAC-SHA256（$(x \cdot y \cdot P)_{abscissa}$，$N_{AE}||N_{ASUE}||$“base key expansion for key and additional nonce”），生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，然后对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识。

k) 首先验证对 ASU 密钥数据的签名，若验证不通过，则丢弃消息 7；否则计算 KD-HMAC-SHA256（$(x \cdot z \cdot P)_{abscissa}$，ADDID$||N_{ASU}||N_{ASUE}||$“pairwise key expansion for unicast and additional keys and nonce”），其中 N_{ASU} 为 ASU 询问，N_{ASUE} 为 ASUE 询问，生成 48 个八位位组为 ASU 与 ASUE 之间的单播会话密钥（第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK），然后验证 ASU-ASUE 消息鉴别码，若验证不通过，则丢弃消息 7；否则检查证书的验证结果字段中的第二个一次性随机数值与自己在消息 4 中的 ASUE 询问是否相同，若不相同，则丢弃消息 7；否则验证 ASU 签名，若不正确，则丢弃消息 7；否则检查 AE 证书的鉴别结果是否为有效，若 STA_{AE} 证书为无效，解除与该 STA_{AE} 的链路验证；若 STA_{AE} 证书为有效，则 ASUE 使用自己的临时私钥 x 和 AE 的临时公钥 y·P 进行 ECDH 计算，得到密钥种子（x·y

·P)$_{abscissa}$，对其进行扩展 KD-HMAC-SHA256 ((x·y·P)$_{abscissa}$，N_{AE}||N_{ASUE}||“base key expansion for key and additional nonce”)，生成长度为 16 个八位位组的基密钥 BK 和长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识种子，然后对该鉴别标识种子进行 SHA-256 运算，得到长度为 32 个八位位组的下一次证书鉴别过程的鉴别标识。最后依据标识 FLAG、ASUE-ASU 消息鉴别码构成消息 8，并发送给 AE。

6.2.1.3.5.3.8 消息 8

消息 8 的数据字段格式如图 18 所示。

	标识FLAG	ASUE-ASU消息鉴别码
八位位组数：	1	20

图 18 消息 8 的数据字段格式

其中：

——标识 FLAG 字段长度为 1 个八位组，定义如前，比特 7 有意义。本字段比特 7 的值与消息 7 中本字段比特 7 的值相同。

——ASUE-ASU 消息鉴别码字段长度为 20 个八位位组，其值为 ASUE 利用最新协商的 ASU 与 ASUE 之间的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对消息 3 中的 WIE_{ASU} 和 ASU 询问，消息 4 中的 $WIE_{ASUE-ASU}$、ASUE 询问、STA_{ASUE} 的证书、ASUE 密钥数据和对 ASUE 密钥数据的签名，消息 7 中 ASU 密钥数据、对 ASU 密钥数据的签名、ASU-ASUE 消息鉴别码计算得到。

当 ASUE 收到消息 7，且消息 7 的标识 FLAG 字段中比特 7 的值为 1 时，ASUE 向 AE 发送消息 8。

AE 收到消息 8 后，进行如下处理：

a) 若消息 6 的 FLAG 字段中比特 1 的值为 1，则执行步骤 b)；否则执行步骤 c)。

b) 若消息 6 的 FLAG 字段中比特 2 的值为 0，则依据 FLAG、ASUE-ASU 消息鉴别码构成消息 9，并发送给 ASU；否则依据 FLAG、ASUE-ASU 消息鉴别码、AE-ASU 消息鉴别码构成消息 9，并发送给 ASU。

c) 若消息 6 的 FLAG 字段中比特 2 的值为 1，依据 FLAG、AE-ASU 消息鉴别码构成消息 9，并发送给 ASU。

6.2.1.3.5.3.9 消息 9

消息 9 的数据字段格式如图 19 所示。

	FLAG	ASUE-ASU消息鉴别码	AE-ASU消息鉴别码
八位位组数：	1	20	20

图 19 消息 9 的数据字段格式

其中：

——FLAG 字段长度为 1 个八位组，定义如前，比特 1 和 2 有意义。本字段的值与消息 6 中 FLAG 字段的值相同。

——ASUE-ASU 消息鉴别码字段长度为 20 个八位位组，其值与消息 8 中的 ASUE-ASU 消息鉴别码字段的值相同。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——AE-ASU 消息鉴别码字段长度为 20 个八位位组，其值为 AE 利用最新协商的 ASU 与 AE 之间的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对消息 1、消息 2、消息 5、消息 6、消息 9 本字段之前的所有字段计算得到，不包含各个消息的分组头。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

当消息 6 的 FLAG 字段中比特 1 的值为 1，或消息 6 的 FLAG 字段中比特 2 的值为 1 时，AE 向 ASU 发送消息 9。

ASU 收到消息 9，进行如下处理：

a) 检查 FLAG 字段中比特 1 的值，若值为 1，执行步骤 b)；否则执行步骤 e)。

b) 检查 FLAG 字段中比特 2 的值，若值为 0，则执行步骤 c)；否则执行步骤 d)。

c) 验证 ASUE-ASU 消息鉴别码，若验证不通过，则丢弃消息 9；否则成功协商了 ASUE 与 ASU 之间的会话密钥及密码套件。

d) 验证 ASUE-ASU 消息鉴别码，若验证不通过，则丢弃消息 9；否则继续验证 AE-ASU 消息鉴别码，若验证不通过，则丢弃消息 9；否则成功协商了 ASUE 与 ASU 之间的会话密钥及密码套件，以及 AE 与 ASU 之间的会话密钥及密码套件。

e) 检查 FLAG 字段中比特 2 的值，若值为 1，则验证 AE-ASU 消息鉴别码，若验证不通过，则丢弃消息 9；否则成功协商了 AE 与 ASU 之间的会话密钥及密码套件。

在证书鉴别过程中，对于 ASUE 与 ASU 之间、AE 与 ASU 之间协商的密码套件，其密码算法采用 SM4。

在证书鉴别过程中，要进行 ECDH 协商出基密钥，或要进行 ECDH 协商出 ASUE 与 ASU 之间的会话密钥，或要进行 ECDH 协商出 AE 与 ASU 之间的会话密钥。对于 ECDH 算法，做以下说明：

1) 临时私钥 x、y、z 是在[1..n−1]间的整数，n 是椭圆曲线域参数中基点 P 的阶。

2) 临时公钥 x·P、y·P、z·P 是椭圆曲线域参数定义的椭圆曲线上的点。

3) ECDH 协商出来密钥种子$(x\cdot y\cdot P)_{abscissa}$是 x·y·P 的坐标，x·y·P 不能是无穷远点；ECDH 协商出来密钥种子$(x\cdot z\cdot P)_{abscissa}$是 x·z·P 的坐标，x·z·P 不能是无穷远点；ECDH 协商出来密钥种子$(x\cdot y\cdot P)_{abscissa}$是 y·z·P 的坐标，y·z·P 不能是无穷远点。

6.2.2 隧道 TAEP 鉴别方式

6.2.2.1 概述

隧道 TAEP 鉴别方式是指采用一个隧道 TAEP 鉴别方法来实现 TCA 的双向用户身份鉴别和平台鉴别，其中 AR 和 AC 之间的平台鉴别数据是利用隧道方法所建立的安全隧道进行保护的。隧道方法可以采用 TLS 协议和增强型 TLS 协议(见 6.2.2.2.4)来建立。

6.2.2.2 隧道 TAEP 鉴别实现

6.2.2.2.1 层次模型

图 20 为 TCA 的一种隧道 TAEP 鉴别实现的层次模型。

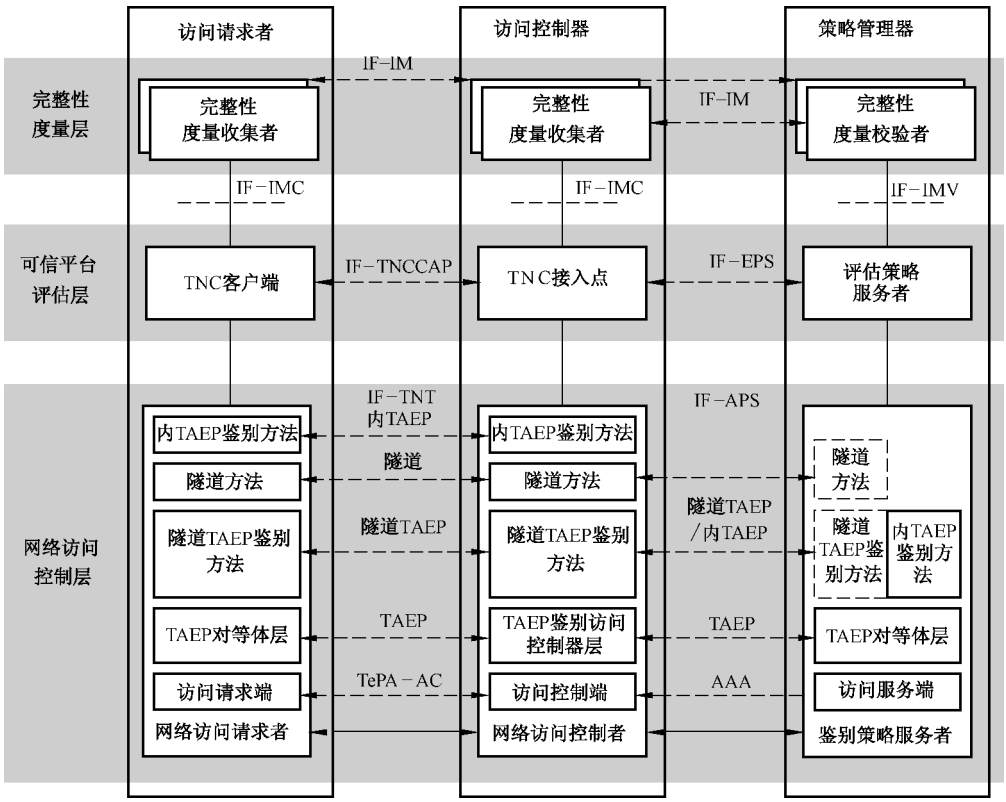

图 20　TCA 的隧道 TAEP 鉴别方式层次模型

在图 20 中，NAR、NAC 和 APS 执行一个隧道 TAEP 鉴别方法，其中隧道 TAEP 鉴别方法包含两个阶段：隧道方法和内 TAEP 鉴别方法。TAEP 对等体层和 TAEP 鉴别访问控制器层是 TAEP 层次模型（见 GB/T 28455—2012）中的两种角色。访问请求端和访问控制端利用 TePA-AC 来实现 TCA 的访问控制（见 6.3），其中 TAEP 包承载在 TePA-AC 上。访问控制端和访问服务端可以利用 AAA 协议（见 RFC 3539）来承载 TAEP 包，例如：RADIUS 和 Diameter（见 RFC 2138、RFC 2865、RFC 2866、RFC 4675、RFC 3588 和 RFC 3589）。

APS 中的隧道 TAEP 鉴别方法和隧道方法为虚线框，表示 APS 可以不参与隧道方法。

对于 TCA 的隧道 TAEP 鉴别方式，内 TAEP 包中的 PIK 签名必须密码绑定隧道 TAEP 鉴别方法中隧道方法所建立的隧道密钥，密码绑定方法是将该隧道密钥作为 PIK 签名的外部数据输入。

6.2.2.2.2　隧道 TAEP 鉴别方法

隧道 TAEP 鉴别方法用于封装传输用户身份鉴别协议和平台鉴别协议，它包含以下两个阶段：

第一阶段，NAR 和 NAC 利用隧道方法建立 AR 和 AC 之间的安全隧道，其中 APS 可以参与该安全隧道的建立过程，也可以不参与该安全隧道的建立过程。

第二阶段：NAR、NAC 和 APS 交互内 TAEP 鉴别方法的内 TAEP 包，其中 AR 和 AC 之间的内 TAEP 包是利用隧道方法所建立的安全隧道进行保护的。

对于隧道方法，本标准推荐采用 TLS 协议（见 RFC 2246、RFC 4346、RFC 5246）及增强型 TLS 协议的完全模式，其中 ECDH 交换参数应采用国家密码管理局批准的 ECC 域参数，签名算法应采用国家密码管理局批准的 ECDSA 算法，杂凑算法应采用国家密码管理局批准的 KD-HMAC-SHA256、

HMAC-SHA256 和 SHA256 算法，分组算法应采用国家密码管理局批准的 SM4 算法，加密工作模式应采用 OFB 模式，完整性校验工作模式应采用 CBC-MAC 模式，从而本标准将相应的 TLS 密码套件规定为 TLS_ECDH_ECDSA_WITH_SM4_OFB_CBC_MAC_SHA256，其值为{0x00，0xfd}。

当采用 TLS 协议及增强型 TLS 协议的完全模式作为隧道方法时，本标准规定相应的隧道 TAEP 鉴别方法的 Type 字段为 TAEP-TTLS。

内 TAEP 鉴别方法用于实现 AR 和 AC 之间的平台鉴别。当内 TAEP 包封装 PAI 协议（见 7.2.2）时，本标准规定相应的内 TAEP 鉴别方法的 Type 字段为 TAEP-PAI。

6.2.2.2.3 TAEP 交互过程

TCA 的 TAEP 交互过程如下：

a) NAC 向 NAR 发送 TAEP 的 Request 分组，其中 Type 字段的值为 Identity。

b) NAR 向 NAC 发送 TAEP 的 Response 分组，其中 Type 字段的值为 Identity，Type-Data 字段的值包含 AR 的身份。

c) NAC 向 APS 发送 TAEP 的 Request 分组，其中 Type 字段的值为 TP Authentication，Type-Data 字段的值包含 AR 和 AC 的身份。

d) APS 向 NAC 发送 TAEP 的 Response 分组，其中 Type 字段的值为 TP Authentication，Type-Data 字段的值包含 PM 所支持的各种 TAEP 鉴别方法类型。

e) NAC 选取一种隧道 TAEP 鉴别方法与 NAR、APS 执行隧道方法过程建立 AR 和 AC 之间的安全隧道，即 AR 和 AC 之间交互一系列 TAEP 的 Request 分组和 Response 分组，以及 AC 和 PM 之间交互一系列 TAEP 的 Request 分组和 Response 分组（APS 参与隧道方法的情况），直至隧道方法过程完成，其中 Type 字段的值为隧道 TAEP 鉴别方法类型，Type-Data 字段的值为隧道方法消息。

f) NAC 向 NAR 发送 TAEP 的 Request 分组，其中 Type 字段的值为步骤 e）中的隧道 TAEP 鉴别方法类型，Type-Data 字段的值为利用步骤 e）建立的安全隧道进行保护的内 TAEP 包。内 TAEP 包的 Code 字段的值为 Request，Type 字段的值为 Identity。当 TNCAP 需要请求用于内 TAEP 鉴别方法的 AR 的身份时，TNCAP 通知 NAC 发送该内 TAEP 包。当 NAR 收到该内 TAEP 包时，NAR 向 TNCC 请求用于内 TAEP 鉴别方法的 AR 的身份。

g) NAR 向 NAC 发送 TAEP 的 Response 分组，其中 Type 字段对应步骤 f）中 TAEP 的 Request 分组中的 Type 字段，Type-Data 字段的值为利用步骤 e）建立的安全隧道进行保护的内 TAEP 包。内 TAEP 包的 Code 字段的值为 Response，Type 字段对应步骤 f）中内 TAEP 包的 Request 分组中的 Type 字段，Type-Data 字段中包含用于内 TAEP 鉴别方法的 AR 的身份。当 NAR 从 TNCC 接收到用于内 TAEP 鉴别方法的 AR 的身份时，NAR 向 NAC 发送该内 TAEP 包。当 NAC 收到该内 TAEP 包时，NAC 向 TNCAP 发送用于内 TAEP 鉴别方法的 AR 的身份。

h) NAC 向 APS 发送 TAEP 的 Request 分组，其中 Type 字段的值为 TP Authentication，Type-Data 字段中 Subtype 字段的值为 FF-FF-FE（用于标识 TCA 中内 TAEP 包的 TP Authentication 类型分组），Subdata 字段的值包含用于内 TAEP 鉴别方法的 AR 和 AC 身份。Subdata 字段的值还可以包含对 AR 的平台鉴别策略请求信息，具体值不在本标准中规定。当 TNCAP 需要向 EPS 请求内 TAEP 鉴别方法类型或对 AR 的平台鉴别策略时，TNCAP 通知 NAC 发送该内 TAEP 包。当 APS 收到该内 TAEP 包时，APS 向 EPS 发送用于内 TAEP 鉴

别方法的 AR 和 AC 身份或对 AR 的平台鉴别策略请求信息。

i) APS 向 NAC 发送 TAEP 的 Response 分组，其中 Type 字段对应步骤(h)中 TAEP 的 Request 分组中的 Type 字段，Type-Data 字段中 Subtype 的值为 FF-FF-FE，Subdata 字段的值包含各个内 TAEP 鉴别方法类型。Subdata 字段的值还可以包含 EPS 分发给 TNCAP 的对 AR 的平台鉴别策略。当 APS 从 EPS 接收到各个内鉴别方法类型或对 AR 的平台鉴别策略时，APS 向 NAC 发送该内 TAEP 包，NAC 收到该内 TAEP 包后将其 Subdata 字段的值发送给 TNCAP，然后 TNCAP 选取一种内 TAEP 鉴别方法发起内 TAEP 鉴别过程。对 AR 的平台鉴别策略的管理参见附录 B。

j) NAC 根据 TNCAP 选取的一种内 TAEP 鉴别方法与 NAR、APS 交互一系列 TAEP 的 Request 分组和 Response 分组，直到内 TAEP 鉴别方法过程完成。对于 NAC 与 NAR 之间交互的一系列 TAEP 的 Request 分组和 Response 分组，其中 Type 字段的值为步骤 e)中的隧道 TAEP 鉴别方法类型，Type-Data 字段的值为利用步骤 e)建立的安全隧道进行保护的内 TAEP 包。内 TAEP 包的 Type 字段的值为 TNCAP 选取的内 TAEP 鉴别方法类型，Type-Data 字段的值为 TNCAP 选取的内 TAEP 鉴别方法类型对应的内 TAEP 鉴别方法消息。对于 NAC 与 APS 之间交互的一系列 TAEP 的 Request 分组和 Response 分组，其中 Type 字段的值为 TNCAP 选取的内 TAEP 鉴别方法类型，Type-Data 字段的值为 TNCAP 选取的内 TAEP 鉴别方法类型对应的内 TAEP 鉴别方法消息。内 TAEP 鉴别方法消息由可信平台评估层中的 TNCC、TNCAP 和 EPS 进行相应处理。

k) NAC 利用 TAEP 的 Success 分组或 Failure 分组结束鉴别过程，即：若在步骤 j)中的内 TAEP 鉴别方法过程中 TNCAP 成功鉴别 AR 的平台(包括平台身份鉴别和平台完整性评估)，则向 NAR 发送 TAEP 的 Success 分组。若在步骤 j)中的内 TAEP 鉴别方法过程中 TNCAP 不能成功鉴别 AR 的平台，则向 NAR 发送 TAEP 的 Failure 分组。

以上步骤描述了 TCA 的隧道 TAEP 鉴别实现的典型 TAEP 交互过程，但根据鉴别方法的不同，步骤过程会有不同。

当隧道 TAEP 鉴别方法的 Type 字段为 TAEP-TTLS 且隧道方法为完全模式 TLS 协议，内 TAEP 鉴别方法的 Type 字段为 TAEP-PAI 且封装 PAI 协议(7.2.2)时，TCA 的隧道 TAEP 鉴别实现的一个完整的 TAEP 交互过程如图 21 所示。

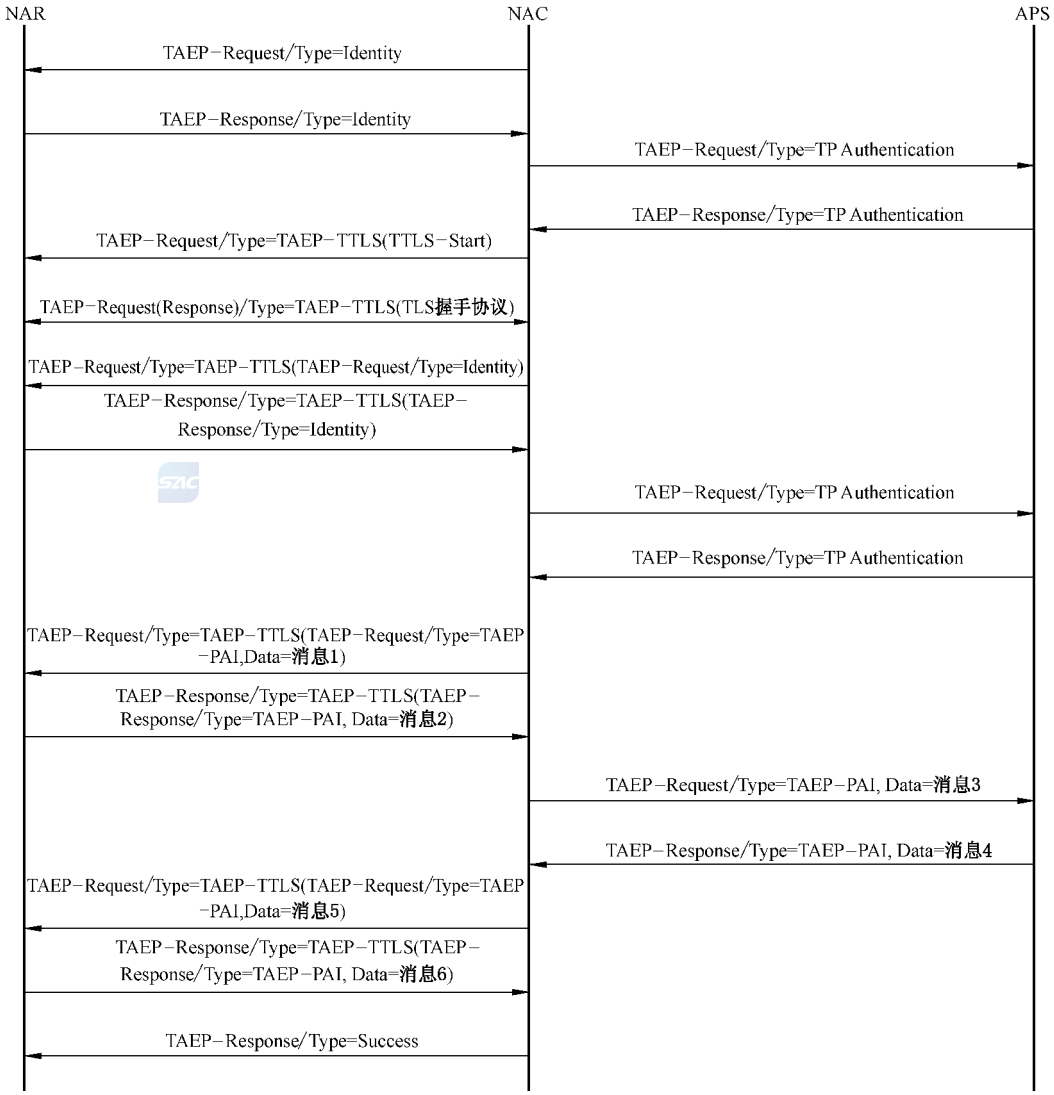

图 21　隧道 TAEP 鉴别实现的 TAEP 交互过程一

在图 21 中，根据 PAI 协议的特点，与 TAEP-PAI 相关的消息 1～消息 6 的 TAEP 交互可能执行多轮次。

在一轮 PAI 协议中，当消息 5 未被生成时，消息 5 和消息 6 的 TAEP 交互不存在。

在一轮 PAI 协议中，当消息 5 被生成，但消息 6 未被生成时，消息 6 的 TAEP 交互存在，其 Data 值为 NULL。

当隧道 TAEP 鉴别方法的 Type 字段为 TAEP-TTLS 且隧道方法为完全模式增强型 TLS 协议，内 TAEP 鉴别方法的 Type 字段为 TAEP-PAI 且封装 PAI 协议(7.2.2)时，TCA 的隧道 TAEP 鉴别实现的一个完整的 TAEP 交互过程如图 22 所示。

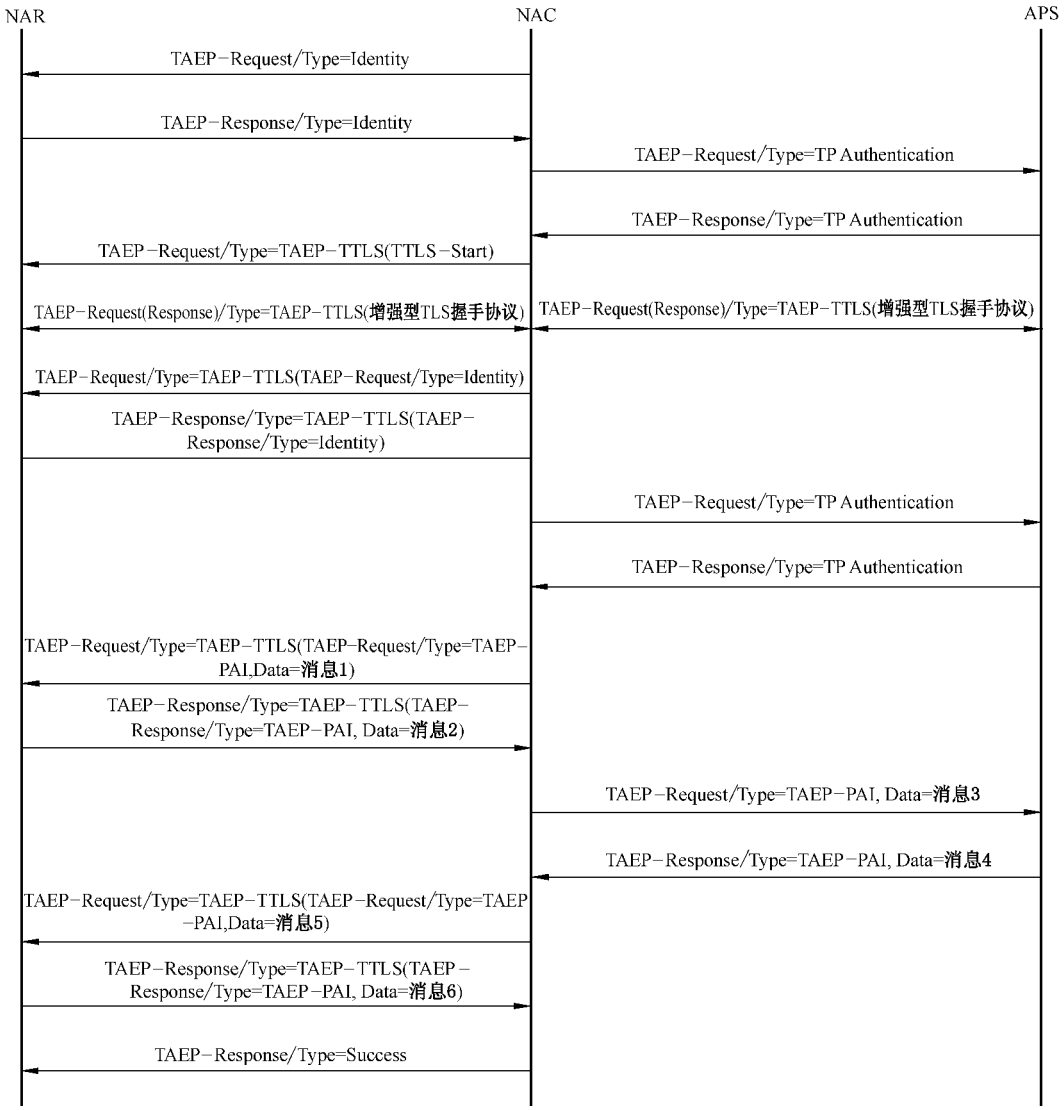

图 22　隧道 TAEP 鉴别实现的 TAEP 交互过程二

在图 22 中，根据 PAI 协议的特点，与 TAEP-PAI 相关的消息 1～消息 6 的 TAEP 交互可能执行多轮次。

在一轮 PAI 协议中，当消息 5 未被生成时，消息 5 和消息 6 的 TAEP 交互不存在。

在一轮 PAI 协议中，当消息 5 被生成，但消息 6 未被生成时，消息 6 的 TAEP 交互存在，其 Data 值为 NULL。

6.2.2.2.4　增强型 TLS 协议

6.2.2.2.4.1　概述

增强型 TLS（ETLS）协议是可信第三方（TTP）在线的 TLS 协议。ETLS 协议中的客户端（Client）、服务端（Server）和 TTP 分别对应于本标准中的 AR、AC 和 PM。相对于 TLS 协议，ETLS 协议增加了 Client 证书和 Server 证书的集中验证，增加了 Client 与 TTP 之间、Server 与 TTP 之间的会话密钥及密码套件的协商。

Client 与 TTP 之间、Server 与 TTP 之间的会话密钥生成方法与 Client 与 Server 之间的会话密钥

生成方法相同，都是采用 KD-HMAC-SHA256 算法，其中输入参数与输出参数与 TLS 协议相同。

ETLS 协议中未明确规定部分参见 TLS 协议。

6.2.2.2.4.2 增强型 TLS 协议的记录协议

ETLS 记录协议仅使用于 Client 与 Server 之间，其中版本号为 3.4(对应 ETLS 协议)，其他与 TLS 记录协议相同。

6.2.2.2.4.3 增强型 TLS 协议的握手协议

6.2.2.2.4.3.1 封装方法

6.2.2.2.4.3.1.1 Client 与 Server 之间

采用 TLS 协议的封装方法。

6.2.2.2.4.3.1.2 Server 与 TTP 之间

ETLS 协议的握手协议分组格式如图 23 所示。

	版本	类型	子类型	保留	长度	分组序号	分片序号	标识	数据
八位位组数：	2	1	1	2	2	2	1	1	可变

图 23 ETLS 协议的握手协议分组格式

其中：

——版本字段长度为 2 个八位位组，表示 ETLS 协议的版本号。当前版本为 1；

——类型字段长度为 1 个八位位组，表示协议类型，定义如下：

1 ETLS 协议分组；

其他值保留。

——子类型字段的长度为 1 个八位位组，当类型字段的值为 1 时，子类型字段值定义如下；当类型字段为其他值时，子类型字段值保留。

1 消息 1；

2 消息 2；

3 消息 3；

4 消息 4；

其他值保留。

——保留字段长度为 2 个八位位组，默认值为 0。

——长度字段长度为 2 个八位位组，其值表示 ETLS 协议分组所有字段的八位位组数。

——分组序号字段长度为 2 个八位位组，其值表示协议分组序号。第一个分组序号为 1，后序分组依次按 1 递增。

——分片序号字段长度为 1 个八位位组，其值表示分片的顺序编号，每一个分组的第一个分片序号为 0，后序分片依次按 1 递增。

——标识字段长度为 1 个八位位组，比特 0 表示后续是否有分片，值为 0 表示没有，值为 1 表示有。比特 1 至比特 7 保留。

——数据字段的内容根据类型和子类型的值而定，它除了包含固定的内容，还可以包含可选的属性。

6.2.2.2.4.3.2 握手过程

ETLS 协议的握手过程如图 24。

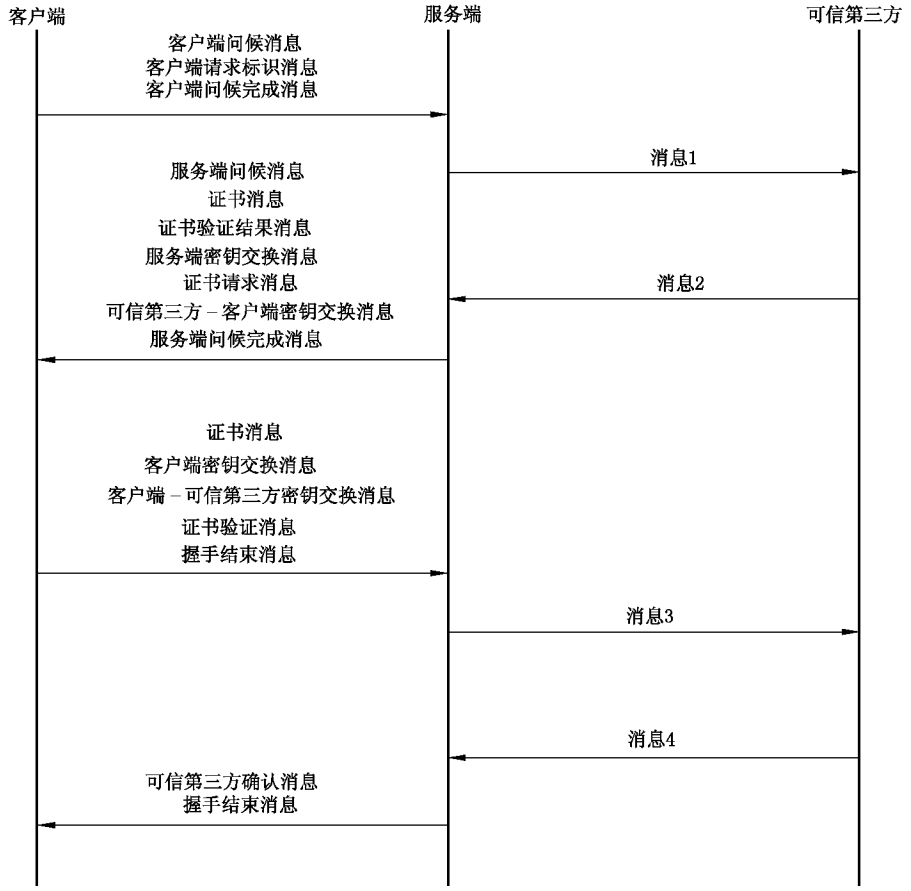

图 24 ETLS 协议的握手过程

在图 24 中，客户端问候消息(ClientHello)、服务端问候消息(ServerHello)、证书消息(Certificate)、服务端密钥交换消息(ServerKeyExchange)、证书请求消息(CertificateRequest)、服务端问候完成消息(ServerHelloDone)、客户端密钥交换消息(ClientKeyExchange)、证书验证消息(CertificateVerify)和握手结束消息(Finished)与 TLS 协议中所定义的握手消息相同。客户端请求标识消息(ClientRequestFlag)、客户端问候完成消息(ClientHelloDone)、证书验证结果消息(CertificateValidationResult)、可信第三方－客户端密钥交换消息(TTPClientKeyExchange)、客户端－可信第三方密钥交换消息(ClientTTPKeyExchange)和可信第三方确认消息(TTPConfirmed)为新增加的 6 种握手消息。

6.2.2.2.4.3.2.1 消息 1

消息 1 的数据字段格式如图 25 所示。

	FLAG	Client 询问	Server 证书	Client 密码套件计数	Client 密码套件	Server 询问	Server 密码套件计数	Server 密码套件
八位位组数：	1	32	可变	2	2×m	32	2	2×n

图 25 消息 1 的数据字段格式

其中：

——FLAG 字段长度为 1 个八位组，定义如图 26 所示。

B0	B1	B2	B3	B4～B7
Client证书验证请求标识	Server证书验证请求标识	Client与TTP之间密钥协商请求标识	Server与TTP之间密钥协商请求标识	保留

图 26　FLAG

其中：

——Client 证书验证请求标识比特：1 表示需要验证 Client 证书的有效性；0 表示不需要验证。

——Server 证书验证请求标识比特：1 表示需要验证 Server 证书的有效性；0 表示不需要验证。

——Client 与 TTP 之间密钥协商请求标识比特：1 表示需要协商 Client 与 TTP 之间的会话密钥及密码套件；0 表示不需要协商。

——Server 与 TTP 之间密钥协商请求标识比特：1 表示需要协商 Server 与 TTP 之间的会话密钥及密码套件；0 表示不需要协商。

比特 1、2 和 3 有意义。

——Client 询问字段长度为 32 个八位位组，其格式定义参见 TLS 协议中的 Random，其值为 ClientHello. random。当 FLAG 字段中比特 1 或 2 的值为 1 时，本字段存在。

——Server 证书字段长度为可变，其格式定义见 TLS 协议中的 Certificate，其值为 Server 发送的 Certificate。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

——Client 密码套件计数字段长度为 2 个八位位组，其值为 ClientHello. cipher_suites 的计数。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——Client 密码套件字段长度为 2×m，其中 m 为 Client 密码套件计数。Client 密码套件的值为 ClientHello. cipher_suites。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——Server 询问字段长度为 32 个八位位组，其格式定义参见 TLS 协议中的 Random，其值为 ServerHello. random。当 FLAG 字段中比特 3 的值为 1 时，本字段存在。

——Server 密码套件计数字段长度为 2 个八位位组，其值为 ServerHello. cipher_suites 的计数。当 FLAG 字段中比特 3 的值为 1 时，本字段存在。

——Server 密码套件字段长度为 2×n，其中 n 为 Server 密码套件计数。Server 密码套件的值为 ServerHello. cipher_suites。当 FLAG 字段中比特 3 的值为 1 时，本字段存在。

当 Server 收到 ClientHelloDone 时，若 Client 需要验证 Server 证书的有效性，或 Client 需要协商与 TTP 之间的会话密钥及密码套件，或 Server 需要协商与 TTP 之间的会话密钥及密码套件，则 Server 向 TTP 发送消息 1。值得注意的是：若 Server 支持的最高版本低于 3.4，则 Server 丢弃 Client 发送的 ClientRequestFlag 和 ClientHelloDone。

TTP 收到消息 1 后，进行如下处理：

a）　检查 FLAG 字段中比特 1 的值，若值为 0，执行步骤 b）；否则执行步骤 f）。

b）　检查 FLAG 字段中比特 2 和 3 的值，若比特 2 的值为 0 且比特 3 的值为 0，则丢弃消息 1；若比特 2 的值为 0 且比特 3 的值为 1，则执行步骤 c）；若比特 2 的值为 1 且比特 3 的值为 0，则执行步骤 d）；若比特 2 的值为 1 且比特 3 的值为 1，则执行步骤 e）。

c）　首先选取一种用于 TTP 与 Server 之间的密码套件，然后依据 FLAG、TTP 询问、TTP-Server 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名构成消息 2，并发送给 Server。

d）　首先选取一种用于 TTP 与 Client 之间的密码套件，然后依据 FLAG、TTP 询问、TTP-Client 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名构成消息 2，并发送给 Server。

e) 首先选取一种用于 TTP 与 Server 之间的密码套件，以及选取一种用于 TTP 与 Client 之间的密码套件，然后依据 FLAG、TTP 询问、TTP-Client 密码套件、TTP-Server 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名构成消息 2，并发送给 Server。

f) 检查 FLAG 字段中比特 2 和 3 的值，若比特 2 的值为 0 且比特 3 的值为 0，则执行步骤 g)；若比特 2 的值为 0 且比特 3 的值为 1，则执行步骤 h)；若比特 2 的值为 1 且比特 3 的值为 0，则执行步骤 i)；若比特 2 的值为 1 且比特 3 的值为 1，则执行步骤 j)。

g) 首先生成 Server 证书的验证结果及相应的签名，然后依据 FLAG、Client 询问、Server 证书、Server 证书的验证结果、对 Server 证书验证结果的签名构成消息 2，并发送给 Server。

h) 首先生成 Server 证书的验证结果及相应的签名，然后选取一种用于 TTP 与 Server 之间的密码套件，最后依据 FLAG、Client 询问、Server 证书、Server 证书的验证结果、对 Server 证书验证结果的签名、TTP 询问、TTP-Server 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名构成消息 2，并发送给 Server。

i) 首先生成 Server 证书的验证结果及相应的签名，然后选取一种用于 TTP 与 Client 之间的密码套件，最后依据 FLAG、Client 询问、Server 证书、Server 证书的验证结果、对 Server 证书验证结果的签名、TTP 询问、TTP-Client 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名构成消息 2，并发送给 Server。

j) 首先生成 Server 证书的验证结果及相应的签名，然后选取一种用于 TTP 与 Server 之间的密码套件，以及选取一种用于 TTP 与 Client 之间的密码套件，最后依据 FLAG、Client 询问、Server 证书、Server 证书的验证结果、对 Server 证书验证结果的签名、TTP 询问、TTP-Client 密码套件、TTP-Server 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名构成消息 2，并发送给 Server。

6.2.2.2.4.3.2.2 消息 2

消息 2 的数据字段格式如图 27 所示。

	FLAG	Client 询问	Server 证书	Server 证书的验证结果	对Server证书验证结果的签名	TTP 询问	TTP-Client 密码套件	TTP-Server 密码套件	TTP 密钥数据	对TTP密钥数据的签名
八位位组数：	1	32	可变	1	可变	32	2	2	可变	可变

图 27 消息 2 的数据字段格式

其中：

——FLAG 字段长度为 1 个八位组，定义如前，比特 1、2 和 3 有意义。

——Client 询问字段长度为 32 个八位位组，其值为 ClientHello. random。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

——Server 证书字段长度为可变，其值为 Server 发送的 Certificate。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

——Server 证书的验证结果字段为 1 个八位位组，验证结果的定义如前。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

——对 Server 证书验证结果的签名字段长度为可变，采用签名属性格式定义，它是 TTP 生成的对 Client 询问、Server 证书、Server 证书的验证结果的签名。当 FLAG 字段中比特 1 的值为 1 时，本字段存在。

——TTP 询问字段长度为 32 个八位位组，其格式定义见 TLS 协议中的 Random，它是 TTP 生成

的。当 FLAG 字段中比特 2 或 3 的值为 1 时，本字段存在。

——TTP-Client 密码套件字段长度为 2 个八位位组，其格式定义见 TLS 协议中的 CipherSuite，其值是 TTP 选择的一种用于 TTP 与 Client 之间的密码套件。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——TTP-Server 密码套件字段长度为 2 个八位位组，其格式定义见 TLS 协议中的 CipherSuite，其值是 TTP 选择的一种用于 TTP 与 Server 之间的密码套件。当 FLAG 字段中比特 3 的值为 1 时，本字段存在。

——TTP 密钥数据字段为可变，其格式定义如前，它是 TTP 生成的用于 ECDH 交换的临时公钥。当 FLAG 字段中比特 2 或 3 的值为 1 时，本字段存在。

——对 TTP 密钥数据的签名字段长度为可变，采用签名属性格式定义，它是 TTP 生成的对 TTP 密钥数据的签名。当 FLAG 字段中比特 2 或 3 的值为 1 时，本字段存在。

当 TTP 收到 Server 的消息 1 时，TTP 向 Server 发送消息 2。

Server 收到消息 2 后，进行如下处理：

a) 检查 FLAG 字段中比特 1 的值，若值为 0，执行步骤 b)；否则执行步骤 f)。

b) 检查 FLAG 字段中比特 2 和 3 的值，若比特 2 的值为 0 且比特 3 的值为 0，则丢弃消息 1；若比特 2 的值为 0 且比特 3 的值为 1，则执行步骤 c)；若比特 2 的值为 1 且比特 3 的值为 0，则执行步骤 d)；若比特 2 的值为 1 且比特 3 的值为 1，则执行步骤 e)。

c) 验证对 TTP 密钥数据的签名，若验证不通过，则丢弃消息 2；否则依次向 Client 发送 ServerHello、Certificate、ServerKeyExchange、CertificateRequest 和 ServerHelloDone。

d) 依次向 Client 发送 ServerHello、Certificate、ServerKeyExchange、CertificateRequest、TTPClientKeyExchange、ServerHelloDone。

e) 验证对 TTP 密钥数据的签名，若验证不通过，则丢弃消息 2；否则依次向 Client 发送 ServerHello、Certificate、ServerKeyExchange、CertificateRequest、TTPClientKeyExchange、ServerHelloDone。

f) 检查 FLAG 字段中比特 2 和 3 的值，若比特 2 的值为 0 且比特 3 的值为 0，则执行步骤 g)；若比特 2 的值为 0 且比特 3 的值为 1，则执行步骤 h)；若比特 2 的值为 1 且比特 3 的值为 0，则执行步骤 i)；若比特 2 的值为 1 且比特 3 的值为 1，则执行步骤 j)。

g) 依次向 Client 发送 ServerHello、Certificate、CertificateValidationResult、ServerKeyExchange、CertificateRequest、ServerHelloDone。

h) 验证对 TTP 密钥数据的签名，若验证不通过，则丢弃消息 3；否则依次向 Client 发送 ServerHello、Certificate、CertificateValidationResult、ServerKeyExchange、CertificateRequest、ServerHelloDone。

i) 依次向 Client 发送 ServerHello、Certificate、CertificateValidationResult、ServerKeyExchange、CertificateRequest、TTPClientKeyExchange、ServerHelloDone。

j) 验证对 TTP 密钥数据的签名，若验证不通过，则丢弃消息 3；否则依次向 Client 发送 ServerHello、Certificate、CertificateValidationResult、ServerKeyExchange、CertificateRequest、TTPClientKeyExchange、ServerHelloDone。

6.2.2.2.4.3.2.3 消息 3

消息 3 的数据字段格式如图 28 所示。

	FLAG	Server 询问	Client 证书	Client 密钥数据	对Client 密钥数据的签名	Client-TTP消息鉴别码	Server 证书	Server 密钥数据	对Server 密钥数据的签名	Server-TTP消息鉴别码
八位位组数：	1	32	可变	可变	可变	20	可变	可变	可变	可变

图 28　消息 3 的数据字段格式

其中：

——FLAG 字段长度为 1 个八位组，定义如前，比特 0、1、2 和 3 有意义。

——Server 询问字段长度为 32 个八位位组，其值为 ServerHello. random。当 FLAG 字段中比特 0 的值为 1 时，本字段存在。

——Client 证书字段长度为可变，其值为 Client 发送的 Certificate。当 FLAG 字段中比特 0 或 2 的值为 1 时，本字段存在。

——Client 密钥数据字段为可变，其格式定义如前，它是 Client 生成的用于 ECDH 交换的临时公钥。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——对 Client 密钥数据的签名字段长度为可变，采用签名属性格式定义，它是 Client 生成的对 Client 密钥数据的签名。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——Client-TTP 消息鉴别码长度为 20 个八位位组，其值为 Client 利用最新协商的 Client 与 TTP 之间的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对 Client 询问、Client 密码套件计数、Client 密码套件、TTP 询问、TTP-Server 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名、Client 证书、Client 密钥数据、对 Client 密钥数据的签名计算得到。当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——Server 证书字段长度为可变，其值为 Server 发送的 Certificate。当 FLAG 字段中比特 3 的值为 1 且比特 1 的值为 0 时，本字段存在。

——Server 密钥数据字段为可变，其格式定义如前，它是 Server 生成的用于 ECDH 交换的临时公钥。当 FLAG 字段中比特 3 的值为 1 时，本字段存在。

——对 Server 密钥数据的签名字段长度为可变，采用签名属性格式定义，它是 Server 生成的对 Server 密钥数据的签名。当 FLAG 字段中比特 3 的值为 1 时，本字段存在。

——Server-TTP 消息鉴别码长度为 20 个八位位组，其值为 Server 利用最新协商的 Server 与 TTP 之间的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对消息 1、消息 2 和消息 3 中本字段之前的所有字段计算得到。当 FLAG 字段中比特 3 的值为 1 时，本字段存在。

当 Server 收到 Client 发送的 Finished 时，若 Server 需要验证 Client 证书的有效性，或 Client 需要协商与 TTP 之间的会话密钥及密码套件，或 Server 需要协商与 TTP 之间的会话密钥及密码套件，则 Server 向 TTP 发送消息 3。

TTP 收到消息 3 后，进行如下处理：

a)　检查 FLAG 字段中比特 0 的值，若值为 0，执行步骤 b)；否则执行步骤 f)。

b)　检查 FLAG 字段中比特 2 和 3 的值，若比特 2 的值为 0 且比特 3 的值为 0，则丢弃消息 3；若比特 2 的值为 0 且比特 3 的值为 1，则执行步骤 c)；若比特 2 的值为 1 且比特 3 的值为 0，则执行步骤 d)；若比特 2 的值为 1 且比特 3 的值为 1，则执行步骤 e)。

c)　首先验证 Server-TTP 消息鉴别码，若验证不通过，则丢弃消息 3；否则依据 FLAG、TTP-Server 消息鉴别码构成消息 4，并发送给 Server。

d)　首先验证 Client-TTP 消息鉴别码，若验证不通过，则丢弃消息 3；否则依据 FLAG、TTP-Client 消息鉴别码构成消息 4，并发送给 Server。

e) 首先验证 Server-TTP 消息鉴别码，若验证不通过，则丢弃消息 3，否则验证 Client-TTP 消息鉴别码，若验证不通过，则丢弃消息 3；否则依据 FLAG、TTP-Client 消息鉴别码、TTP-Server 消息鉴别码构成消息 4，并发送给 Server。

f) 检查 FLAG 字段中比特 2 和 3 的值，若比特 2 的值为 0 且比特 3 的值为 0，则执行步骤 g)；若比特 2 的值为 0 且比特 3 的值为 1，则执行步骤 h)；若比特 2 的值为 1 且比特 3 的值为 0，则执行步骤 i)；若比特 2 的值为 1 且比特 3 的值为 1，则执行步骤 j)。

g) 首先生成 Client 证书的验证结果及相应的签名，然后依据 FLAG、Server 询问、Client 证书、Client 证书的验证结果、对 Client 证书验证结果的签名构成消息 4，并发送给 Server。

h) 首先验证 Server-TTP 消息鉴别码，若验证不通过，则丢弃消息 3；否则生成 Client 证书的验证结果及相应的签名，然后依据 FLAG、Server 询问、Client 证书、Client 证书的验证结果、对 Client 证书验证结果的签名、TTP-Server 消息鉴别码构成消息 4，并发送给 Server。

i) 首先验证 Client-TTP 消息鉴别码，若验证不通过，则丢弃消息 3；否则生成 Client 证书的验证结果及相应的签名，然后依据 FLAG、Server 询问、Client 证书、Client 证书的验证结果、对 Client 证书验证结果的签名、TTP-Client 消息鉴别码构成消息 4，并发送给 Server。

j) 首先验证 Server-TTP 消息鉴别码，若验证不通过，则丢弃消息 3；否则验证 Client-TTP 消息鉴别码，若验证不通过，则丢弃消息 3；否则生成 Client 证书的验证结果及相应的签名，然后依据 FLAG、Server 询问、Client 证书、Client 证书的验证结果、对 Client 证书验证结果的签名、TTP-Client 消息鉴别码、TTP-Server 消息鉴别码构成消息 4，并发送给 Server。

6.2.2.2.4.3.2.4 消息 4

消息 4 的数据字段格式如图 29 所示。

	FLAG	Server 询问	Client 证书	Client证书的验证结果	对Client证书验证结果的签名	TTP-Client消息鉴别码	TTP-Server消息鉴别码
八位位组数：	1	32	可变	1	可变	20	20

图 29 消息 4 的数据字段格式

其中：

——FLAG 字段长度为 1 个八位组，定义如前，比特 0、2 和 3 有意义。

——Server 询问字段长度为 32 个八位位组，其值为 ServerHello. random。当 FLAG 字段中比特 0 的值为 1 时，本字段存在。

——Client 证书字段长度为可变，其值为 Client 发送的 Certificate。当 FLAG 字段中比特 0 的值为 1 时，本字段存在。

——Client 证书的验证结果字段为 1 个八位位组，验证结果的定义如前。当 FLAG 字段中比特 0 的值为 1 时，本字段存在。

——对 Client 证书验证结果的签名字段长度为可变，采用签名属性格式定义，它是 TTP 生成的对 Server 询问、Client 证书、Client 证书的验证结果的签名，当 FLAG 字段中比特 0 的值为 1 时，本字段存在。

——TTP-Client 消息鉴别码长度为 20 个八位位组，其值为 TTP 利用最新协商的 TTP 与 Client 之间的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对 Client 询问、Client 密码套件计数、Client 密码套件、TTP 询问、TTP-Client 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名、Client 证书、Client 密钥数据、对 Client 密钥数据的签名、Client-TTP 消息鉴别码计算得到。

当 FLAG 字段中比特 2 的值为 1 时，本字段存在。

——TTP-Server 消息鉴别码长度为 20 个八位位组，其值为 TTP 利用最新协商的 TTP 与 Server 之间的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对消息 1、消息 2、消息 3、消息 4 中本字段之前的所有字段计算得到。当 FLAG 字段中比特 3 的值为 1 时，本字段存在。

当 TTP 收到消息 3 时，TTP 向 Server 发送消息 4。

Server 收到消息 4 后，进行如下处理：

进行如下处理：

a) 检查 FLAG 字段中比特 0 的值，若值为 0，执行步骤 b)；否则执行步骤 f)。

b) 检查 FLAG 字段中比特 2 和 3 的值，若比特 2 的值为 0 且比特 3 的值为 0，则丢弃消息 3；若比特 2 的值为 0 且比特 3 的值为 1，则执行步骤 c)；若比特 2 的值为 1 且比特 3 的值为 0，则执行步骤 d)；若比特 2 的值为 1 且比特 3 的值为 1，则执行步骤 e)。

c) 首先验证 TTP-Server 消息鉴别码，若验证不通过，则丢弃消息 4；否则向 Client 发送 Finished。

d) 依次向 Client 发送 TTPConformed、Finished。

e) 首先验证 TTP-Server 消息鉴别码，若验证不通过，则丢弃消息 4；否则依次向 Client 发送 TTPConformed、Finished。

f) 检查 FLAG 字段中比特 2 和 3 的值，若比特 2 的值为 0 且比特 3 的值为 0，则执行步骤 g)；若比特 2 的值为 0 且比特 3 的值为 1，则执行步骤 h)；若比特 2 的值为 1 且比特 3 的值为 0，则执行步骤 i)；若比特 2 的值为 1 且比特 3 的值为 1，则执行步骤 j)。

g) 首先验证对 Client 证书验证结果的签名，若验证不通过，则丢弃消息 4；否则向 Client 发送 Finished。

h) 首先验证对 Client 证书验证结果的签名，若验证不通过，则丢弃消息 4；否则验证 TTP-Server 消息鉴别码，若验证不通过，则丢弃消息 4；否则向 Client 发送 Finished。

i) 首先验证对 Client 证书验证结果的签名，若验证不通过，则丢弃消息 4；否则向 Client 发送 TTPConformed、Finished。

j) 首先验证对 Client 证书验证结果的签名，若验证不通过，则丢弃消息 4；否则验证 TTP-Server 消息鉴别码，若验证不通过，则丢弃消息 4；否则向 Client 发送 TTPConformed、Finished。

当 FLAG 字段中比特 0 的值为 0 时，Server 验证 Client 所发送的 Certificate，若 Client 所发送的 Certificate 为无效，则 Server 丢弃 Client 所发送的 Certificate 或向 Client 发送警告消息。当 FLAG 字段中比特 0 的值为 1 时，Server 依据消息 4 中 Client 证书的验证结果字段的值来验证 Client 所发送的 Certificate，若 Client 所发送的 Certificate 为无效，则 Server 中止该握手过程或向 Client 发送警告消息。

6.2.2.2.4.3.2.5 ClientRequestFlag

ClientReuestFlag 的握手协议类型值为 40。

Client 在发送 ClientHello 后发送 ClientReuestFlag。

ClientReuestFlag 消息结构包含 1 个八位位组的 flag，其比特 0 和 1 有意义。当比特 0 的值为 1 时，表示 Client 需要验证 Server 证书的有效性。当比特 1 的值为 1 时，表示 Client 需要与 TTP 协商它们之间的会话密钥及密码套件。

6.2.2.2.4.3.2.6 ClientHelloDone

ClientHelloDone 的握手协议类型值为 41。

Client 发送此消息指明 ClientHello 和相关消息的完成。发送此消息之后，Client 等待 Server 的响应。收到 Client 的 ClientHelloDone 消息后，Server 便可以向 TTP 发送消息 1，或向 Client 发送

ServerHello 消息。

ClientHelloDone 消息结构为空结构。

6.2.2.2.4.3.2.7 CertificateValidationResult

CertificateValidationResult 的握手协议类型值为 42。

Server 在发送 Certificate 后发送 CertificateValidationResult，用于向 Client 提供 Server 的证书验证结果。CertificateValidationResult 消息是可选的。当 ClientReuestFlag 中 flag 字段中比特 0 的值为 1 时，CertificateValidationResult 消息存在。

当 CertificateValidationResult 消息不存在时，Client 验证 Server 所发送的 Certificate，若 Server 所发送的 Certificate 为无效，则 Client 丢弃 Server 所发送的 Certificate 或向 Server 发送警告消息。当 CertificateValidationResult 消息存在时，Client 依据 CertificateValidationResult 来验证 Server 所发送的 Certificate，若 Server 所发送的 Certificate 为无效，则 Client 丢弃 Server 所发送的 Certificate 或向 Server 发送警告消息。

CertificateValidationResult 的消息结构包含消息 2 中的 Client 询问、Server 证书、Server 证书的验证结果、对 Server 证书验证结果的签名。

6.2.2.2.4.3.2.8 TTPClientKeyExchange

TTPClientKeyExchange 的握手协议类型值为 43。

Server 在发送 CertificateRequest 后发送 TTPClientKeyExchange，用于 TTP 与 Client 协商它们之间的会话密钥。TTPClientKeyExchange 消息是可选的。当 ClientReuestFlag 中 flag 字段中比特 1 的值为 1 时，TTPClientKeyExchange 消息存在。

TTPClientKeyExchange 的消息结构包含消息 2 中的 TTP 询问、TTP-Client 密码套件、TTP 密钥数据、对 TTP 密钥数据的签名。

6.2.2.2.4.3.2.9 ClientTTPKeyExchange

ClientTTPKeyExchange 的握手协议类型值为 44。

Client 在发送 ClientKeyExchange 后发送 ClientTTPKeyExchange，用于 Client 与 TTP 协商它们之间的会话密钥。ClientTTPKeyExchange 消息是可选的。当 ClientReuestFlag 中 flag 字段中比特 1 的值为 1 时，ClientTTPKeyExchange 消息存在。

ClientTTPKeyExchange 的消息结构包含消息 3 中的对 Client 密钥数据的签名、Client-TTP 消息鉴别码。

6.2.2.2.4.3.2.10 TTPKeyConformed

TTPKeyConformed 的握手协议类型值为 45。

当 Server 收到消息 4 时，Server 向 Client 发送 TTPKeyConformed，用于确认 Client 与 TTP 之间协商的会话密钥。TTPKeyConformed 消息是可选的。当 ClientReuestFlag 中 flag 字段中比特 1 的值为 1 时，TTPKeyConformed 消息存在。

TTPKeyConformed 的消息结构包含消息 4 中的 TTP-Client 消息鉴别码。

6.3 访问控制机制

6.3.1 全端口控制实现方式

全端口控制实现方式是指完全采用端口控制来实现 TCA 的允许、禁止和隔离，其端口控制系统结

构如图 30 所示。

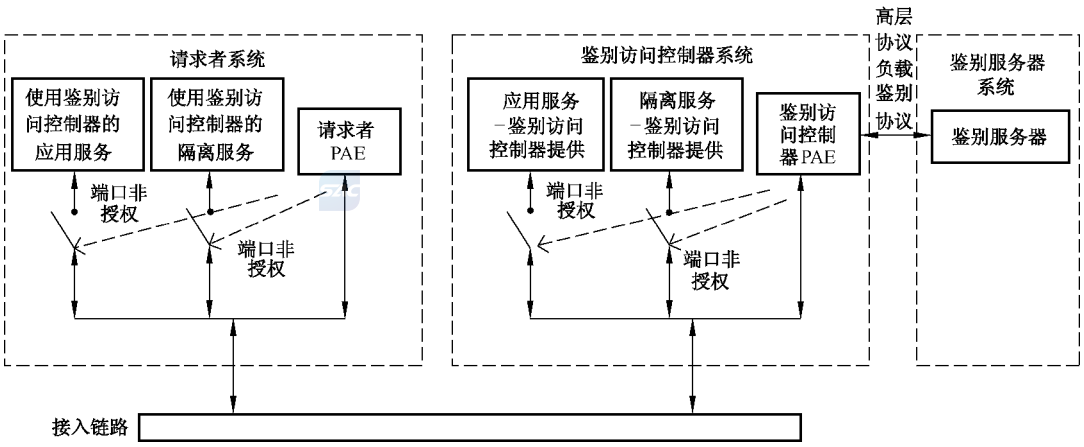

图 30　全端口控制实现方式下的端口控制系统结构

TCA 的 AR、AC 和 PM 分别对应图 30 中请求者系统、鉴别访问控制器系统和鉴别服务器系统。在图 30 中，请求者系统和鉴别访问控制器系统的左边受控端口为应用服务受控端口，而右边受控端口为隔离服务受控端口。非受控端口只能传输 TAEP 数据包，应用服务受控端口能传输应用服务数据包，而隔离服务受控端口能传输隔离服务数据包。

当受控端口为强制授权时，请求者系统和鉴别访问控制器系统的应用服务受控端口无条件设置为授权，而请求者系统和鉴别访问控制器系统的隔离服务受控端口无条件设置为非授权。

当受控端口为强制非授权时，请求者系统和鉴别访问控制器系统的应用服务受控端口和隔离服务受控端口无条件设置为非授权。

当受控端口为自动时，则请求者系统和鉴别访问控制器系统的应用服务受控端口和隔离服务受控端口根据请求者、鉴别访问控制器和鉴别服务器之间的鉴别结果来设置。请求者、鉴别访问控制器和鉴别服务器首先执行用户身份鉴别协议，用户身份鉴别完成后若要求立即做出访问决策，则请求者和鉴别访问控制器依据所做出的访问决策设置应用服务受控端口，即访问决策为允许时设置为授权，访问决策为禁止时不设置并断开链接；否则执行平台鉴别协议，平台鉴别完成后，若访问决策为允许，则请求者和鉴别访问控制器设置应用服务受控端口为授权，若访问决策为隔离，则请求者和鉴别访问控制器设置隔离服务受控端口为授权，若访问决策为禁止时不设置并断开链接。平台修补完成后，请求者和鉴别访问控制器的隔离服务受控端口设置为非授权，然后请求者、鉴别访问控制器和鉴别访问控制器重新执行平台鉴别。访问请求者中的应用服务受控端口和隔离服务受控端口处于互斥状态，即仅一个受控端口处于授权状态。访问控制器中的应用服务受控端口和隔离服务受控端口处于互斥状态，即仅一个受控端口处于授权状态。

6.3.2　部分端口控制实现方式

部分端口控制实现方式是指采用端口控制来实现允许和禁止，而采用其他应用层技术（见 5.7.3）来实现隔离，其端口控制系统结构见 GB/T 28455—2012。

在 GB/T 28455—2012 中，非受控端口传输 TAEP 数据包，受控端口传输应用服务数据包。

7　可信平台评估层

7.1　概述

在一次可信网络连接过程中，可信平台评估层的 TNCC、TNCAP 和 EPS 执行一个或多个平台鉴

别过程来实现 AR 和 AC 之间的平台鉴别，其中每个平台鉴别过程包含一轮或多轮平台鉴别协议，EPS 在平台鉴别协议中充当可信第三方。

可信平台评估层的平台鉴别实现见 7.2 定义的 PAI，相应的平台鉴别协议为 PAI 协议（见 7.2.2）。

7.2 平台鉴别基础设施

PAI 包含以下部分：

——PAI 管理；

——PAI 协议。

7.2.1 PAI 管理

7.2.1.1 网络连接管理

TNCC 和 TNCAP 参与网络连接管理，而 EPS 不参与网络连接管理。

在一次可信网络连接过程的首个平台鉴别过程中，当 TNCAP 收到 NAC 发送的平台鉴别请求（表示 NAC 在完成用户身份鉴别后不立即生成访问决策）时，TNCAP 本地创建一个网络连接标识，记为 connectionID，它为长度为 4 个八位位组的整型数据。

在一次可信网络连接过程的首个平台鉴别过程中，当 TNCC 收到 NAR 发送的平台鉴别请求（表示 NAR 在完成用户身份鉴别后不立即生成访问决策）且收到 TNCAP 发送的首个平台鉴别过程中的首轮 PAI 协议的消息 1 时，TNCC 本地创建一个 connectionID，它为长度为 4 个八位位组的整型数据。

TNCC 和 TNCAP 本地创建的 connectionID 将持续至 AR 和 AC 断开网络连接。若 AR 和 AC 断开网络连接，则 TNCC 和 TNCAP 分别删除本地创建的 connectionID。

7.2.1.2 平台鉴别过程管理

一次可信网络连接过程包含一个或多个平台鉴别过程，其中平台鉴别过程按平台鉴别需求可分为以下 3 种平台鉴别过程：双向平台鉴别过程、对 AR 的单向平台鉴别过程和对 AC 的单向平台鉴别过程。在一个平台鉴别过程中，TNCAP 生成的 AC 的访问决策或 TNCC 生成的 AR 的访问决策的值为允许、隔离或禁止。

一次可信网络连接过程中的平台鉴别过程管理如下：

步骤 1）当 TNCAP 收到 NAC 发送的平台鉴别请求时，TNCAP 执行如下步骤：

步骤 1.1）若 TNCC、TNCAP 和 EPS 需要执行一个双向平台鉴别过程，则执行步骤 2）；

步骤 1.2）若 TNCC、TNCAP 和 EPS 需要执行一个对 AR 的单向平台鉴别过程，则执行步骤 3）；

步骤 1.3）若 TNCC、TNCAP 和 EPS 需要执行一个对 AC 的单向平台鉴别过程，则执行步骤 4）。

步骤 2）当本平台鉴别过程完成时，若 TNCAP 生成的 AC 的访问决策为允许且 TNCC 生成的 AR 的访问决策为允许，则表示可信网络连接成功；若 TNCAP 生成的 AC 的访问决策为允许且 TNCC 生成的 AR 的访问决策为隔离，则 TNCC、TNCAP 和 EPS 在 AC 的平台修补完成后跳至步骤 1.3）执行一个对 AC 的单向平台鉴别过程；若 TNCAP 生成的 AC 的访问决策为隔离且 TNCC 生成的 AR 的访问决策为允许，则 TNCC、TNCAP 和 EPS 在 AR 的平台修补完成后跳至步骤 1.2）执行一个对 AR 的单向平台鉴别过程；若 TNCAP 生成的 AC 的访问决策为隔离且 TNCC 生成的 AR 的访问决策为隔离，则 TNCC、TNCAP 和 EPS 在 AR 的平台修补及 AC 的平台修补完成后跳至步骤 1.1）执行一个双向平台鉴别过程；若 TNCAP 生成的 AC 的访问决策为禁止，则 TNCAP 通知 NAC 断开与 AR 的连接，而 TNCC 收到 AC 的访问决策后通知 NAR 断开与 AC 的连接；若 TNCC 生成的 AR 的访问决策为禁止，则 TNCC 通知 NAR 断开与 AC 的连接，而 TNCAP 收到 AR 的访问决策后通知 NAC 断开与 AR 的连接。

步骤 3)当本平台鉴别过程完成时,若 TNCAP 生成的 AC 的访问决策为允许,则表示可信网络连接成功;若 TNCAP 生成的 AC 的访问决策为隔离,则 TNCC、TNCAP 和 EPS 在 AR 的平台修补完成后跳至步骤 1.2)执行一个对 AR 的单向平台鉴别过程;若 TNCAP 生成的 AC 的访问决策为禁止,则 TNCAP 通知 NAC 断开与 AR 的连接,而 TNCC 收到 AC 的访问决策后通知 NAR 断开与 AC 的连接。

步骤 4)当本平台鉴别过程完成时,若 TNCC 生成的 AR 的访问决策为允许,则表示可信网络连接成功;若 TNCC 生成的 AR 的访问决策为隔离,则 TNCC、TNCAP 和 EPS 在 AC 的平台修补完成后跳至步骤 1.3)执行一个对 AC 的单向平台鉴别过程;若 TNCC 生成的 AR 的访问决策为禁止,则 TNCC 通知 NAR 断开与 AC 的连接,而 TNCAP 收到 AR 的访问决策后通知 NAC 断开与 AR 的连接。

7.2.1.3 PAI 协议管理

7.2.1.3.1 PAI 协议基本流程

PAI 协议是由 TNCAP 发起的,其基本流程如图 31 所示。

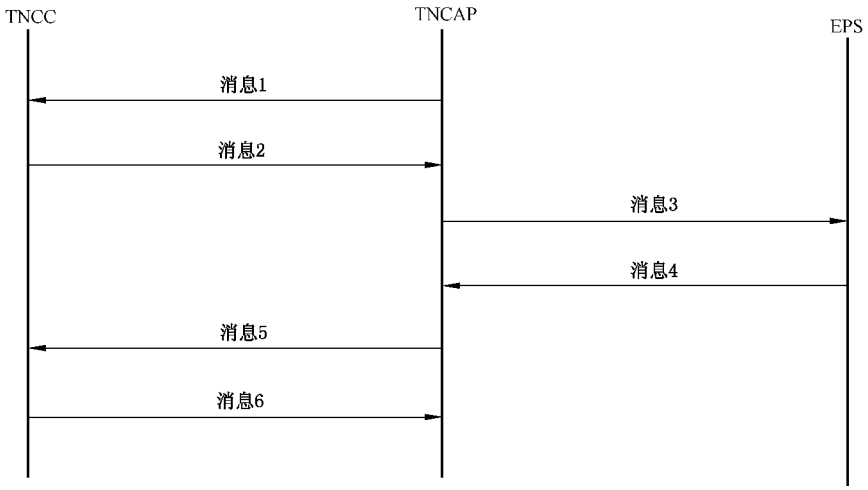

图 31 PAI 协议基本流程

在图 31 中,当 TNCC 生成 AR 的访问决策时才会向 TNCAP 发送消息 6。

7.2.1.3.2 PAI 协议与平台鉴别过程的关系

一个平台鉴别过程包含一轮或多轮 PAI 协议。在一次可信网络连接过程中,平台鉴别过程按执行顺序可分为以下 2 种平台鉴别过程:首个平台鉴别过程和非首个平台鉴别过程,其中首个平台鉴别过程可以为双向平台鉴别过程、对 AR 的单向平台鉴别过程或对 AC 的单向平台鉴别过程,非首个平台鉴别过程也可以为双向平台鉴别过程、对 AR 的单向平台鉴别过程或对 AC 的单向平台鉴别过程。

在一个平台鉴别过程中,PAI 协议按执行顺序可分为以下 2 种 PAI 协议:首轮 PAI 协议和非首轮 PAI 协议。在一个双向平台鉴别过程中,首轮 PAI 协议必然为一轮双向 PAI 协议,而非首轮 PAI 协议可以为双向 PAI 协议、对 AR 的单向 PAI 协议或对 AC 的单 PAI 协议。在一个对 AR 的单向平台鉴别过程中,首轮 PAI 协议和非首轮 PAI 协议都为一轮对 AR 的单向 PAI 协议。在一个对 AC 的单向平台鉴别过程中,首轮 PAI 协议和非首轮 PAI 协议都为一轮对 AC 的单向 PAI 协议。

7.2.1.3.3 双向平台鉴别过程中的 PAI 协议管理

双向平台鉴别过程中的 PAI 协议管理如下:

步骤 1)TNCC、TNCAP 和 EPS 执行一轮双向 PAI 协议,若 TNCAP 在本轮 PAI 协议中生成 AC

的访问决策，则执行步骤 1.1)；否则步骤 1.2)。

步骤 1.1)若 AC 的访问决策为禁止，则 TNCAP 向 TNCC 发送本轮 PAI 协议的消息 5 后通知 NAC 断开与 AR 的连接，其中本轮 PAI 协议的消息 5 包含 AC 的访问决策；TNCC 收到本轮 PAI 协议的消息 5 后通知 NAR 断开与 AC 的连接。若 AC 的访问决策不为禁止，则 TNCAP 向 TNCC 发送本轮 PAI 协议的消息 5；TNCC 收到本轮 PAI 协议的消息 5 后，若 TNCC 生成 AR 的访问决策，则执行步骤 1.1.1)；否则执行步骤 1.1.2)。

步骤 1.1.1)若 AR 的访问决策为禁止，则 TNCC 向 TNCAP 发送本轮 PAI 协议的消息 6 后通知 NAR 断开与 AC 的连接，其中本轮 PAI 协议的消息 6 包含 AR 的访问决策；TNCAP 收到本轮 PAI 协议的消息 6 后通知 NAC 断开与 AR 的连接。若 AR 的访问决策不为禁止，则 TNCC 向 TNCAP 发送本轮 PAI 协议的消息 6；TNCAP 收到本轮 PAI 协议的消息 6 后，本双向平台鉴别过程成功完成。

步骤 1.1.2)TNCC、TNCAP 和 EPS 执行一轮对 AC 的单向 PAI 协议，若 TNCC 在本轮 PAI 协议中生成 AR 的访问决策，则执行步骤 1.1.2.1)；否则执行步骤 1.1.2.2)。

步骤 1.1.2.1)若 AR 的访问决策为禁止，则 TNCC 向 TNCAP 发送本轮 PAI 协议的消息 6 后通知 NAR 断开与 AC 的连接，其中本轮 PAI 协议的消息 6 包含 AR 的访问决策；TNCAP 收到本轮 PAI 协议的消息 6 后通知 NAC 断开与 AR 的连接。若 AR 的访问决策不为禁止，则 TNCC 向 TNCAP 发送本轮 PAI 协议的消息 6；TNCAP 收到本轮 PAI 协议的消息 6 后，本双向平台鉴别过程成功完成。

步骤 1.1.2.2)TNCC、TNCAP 和 EPS 跳至步骤 1.1.2)执行一轮对 AC 的单向 PAI 协议。

步骤 1.2)TNCAP 向 TNCC 发送本轮 PAI 协议的消息 5，其中本轮 PAI 协议的消息 5 中不包含 AC 的访问决策；TNCC 收到本轮 PAI 协议的消息 5 后，若 TNCC 生成 AR 的访问决策，则执行步骤 1.2.1)；否则执行步骤 1.2.2)。

步骤 1.2.1)若 AR 的访问决策为禁止，则 TNCC 向 TNCAP 发送本轮 PAI 协议的消息 6 后通知 NAR 断开与 AC 的连接，其中本轮 PAI 协议的消息 6 包含 AR 的访问决策；TNCAP 收到本轮 PAI 协议的消息 6 后通知 NAC 断开与 AR 的连接。若 AR 的访问决策不为禁止，则执行步骤 1.2.1.1)。

步骤 1.2.1.1)TNCC、TNCAP 和 EPS 执行一轮对 AR 的单向 PAI 协议，若 TNCAP 在本轮 PAI 协议中生成 AC 的访问决策，则执行步骤 1.2.1.1.1)；否则执行步骤 1.2.1.1.2)。

步骤 1.2.1.1.1)若 AC 的访问决策为禁止，则 TNCAP 向 TNCC 发送本轮 PAI 协议的消息 5 后通知 NAC 断开与 AR 的连接，其中本轮 PAI 协议的消息 5 包含 AC 的访问决策；TNCC 收到本轮 PAI 协议的消息 5 后通知 NAR 断开与 AC 的连接。若 AC 的访问决策不为禁止，则本双向平台鉴别过程成功完成。

步骤 1.2.1.1.2)TNCC、TNCAP 和 EPS 跳至步骤 1.2.1.1)执行一轮对 AR 的单向 PAI 协议。

步骤 1.2.2)TNCC、TNCAP 和 EPS 跳至步骤 1)执行一轮双向 PAI 协议。

7.2.1.3.4 对 AR 的单向平台鉴别过程中的 PAI 协议管理

对 AR 的单向平台鉴别过程中的 PAI 协议管理如下：

步骤 1)TNCC、TNCAP 和 EPS 执行一轮对 AR 的单向 PAI 协议，若 TNCAP 在本轮 PAI 协议中生成 AC 的访问决策，则执行步骤 1.1)；否则执行步骤 1.2)。

步骤 1.1)若 AC 的访问决策为禁止，则 TNCAP 向 TNCC 发送本轮 PAI 协议的消息 5 后通知 NAC 断开与 AR 的连接，其中本轮 PAI 协议的消息 5 包含 AC 的访问决策；TNCC 收到本轮 PAI 协议的消息 5 后通知 NAR 断开与 AC 的连接。若 AC 的访问决策不为禁止，则本对 AR 的单向平台鉴别过程成功完成。

步骤 1.2)TNCC、TNCAP 和 EPS 跳至步骤 1)执行一轮对 AR 的单向 PAI 协议。

7.2.1.3.5 对 AC 的单向平台鉴别过程中的 PAI 协议管理

对 AC 的单向平台鉴别过程中的 PAI 协议管理如下：

步骤 1)TNCC、TNCAP 和 EPS 执行一轮对 AC 的单向 PAI 协议，若 TNCC 在本轮 PAI 协议中生成 AR 的访问决策，则执行步骤 1.1)；否则执行步骤 1.2)。

步骤 1.1)若 AR 的访问决策为禁止，则 TNCC 向 TNCAP 发送本轮 PAI 协议的消息 6 后通知 NAR 断开与 AC 的连接，其中本轮 PAI 协议的消息 6 包含 AR 的访问决策；TNCAP 收到本轮 PAI 协议的消息 6 后通知 NAC 断开与 AR 的连接。若 AR 的访问决策不为禁止，则本对 AC 的单向平台鉴别过程成功完成。

步骤 1.2)TNCC、TNCAP 和 EPS 跳至步骤 1)执行一轮对 AR 的单向 PAI 协议。

7.2.2 PAI 协议

7.2.2.1 PAI 协议分组格式

PAI 协议分组格式如图 32 所示。

版本 (2)	类型 (1)	消息序号 (1)	保留 (2)	长度 (4)	分组序号 (2)	分片序号 (1)	标识 (1)	数据 (可变)

图 32 PAI 协议分组格式

其中：

——版本字段长度为 2 个八位位组，表示 PAI 的版本号。当前版本为 1。

——类型字段长度为 1 个八位位组，表示 PAI 协议类型，其值如下：

1 PAI-1 协议；

2 PAI-2 协议；

其他值保留。

——消息序号字段长度为 1 个八位位组，其值如下：

1 消息 1；

2 消息 2；

3 消息 3；

4 消息 4；

5 消息 5；

6 消息 6；

其他值保留。

——保留字段长度为 2 个八位位组，默认值为 0。

——长度字段长度为 4 个八位位组，其值为 PAI 协议分组所有字段的八位位组数。

——分组序号字段为 2 个八位位组，表示 PAI 协议分组序号。第一个分组序号为 1，后序分组依次按 1 递增。

——分片序号字段为 1 个八位位组，表示分片的顺序编号。每一个分组的第一个分片序号为 0，后序分片依次按 1 递增。

——标识字段长度为 1 个八位位组，比特 0 表示后续是否有分片，值为 0 表示没有，值为 1 表示有。比特 1 至比特 7 保留。

——数据字段长度为可变，其内容根据版本、类型和消息序号的值而定，它可以包含固定内容，还可以包含属性内容。

7.2.2.1.1 PAI 协议分组数据字段的固定内容

a) 标识 FLAG

长度为 2 个八位位组。格式如图 33 所示。

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14～B15
对 AR 的平台鉴别需求	AR的平台鉴别错误指示	AR的平台配置保护需求	是否包含AR的PIK证书	对AC的平台鉴别需求	AC的平台鉴别错误指示	AC的平台配置保护需求	是否包含AC的PIK证书	AC的PIK证书验证需求	是否包含AR的访问决策	是否包含AC的访问决策	是否包含AR的Quote数据（值）	是否包含AC的Quote数据（值）	是否包含复合PIK证书验证和平台完整性评估结果	保留

图 33　标识 FLAG 格式

其中：

——对 AR 的平台鉴别需求比特：1 表示 TNCAP 需要对 AR 进行平台鉴别；0 表示 TNCAP 不需要对 AR 进行平台鉴别。

——AR 的平台鉴别错误指示比特：1 表示 AR 的平台鉴别错误指示存在；0 表示 AR 的平台鉴别错误指示不存在。

——AR 的平台配置保护需求比特：1 表示 TNCC 需要对 AR 的平台配置进行保护；0 表示 TNCC 不需要对 AR 的平台配置进行保护。

——是否包含 AR 的 PIK 证书比特：1 表示包含 AR 的 PIK 证书；0 表示不包含 AR 的 PIK 证书。

——对 AC 的平台鉴别需求比特：1 表示 TNCC 需要对 AC 进行平台鉴别；0 表示 TNCC 不需要对 AC 进行平台鉴别。

——AC 的平台鉴别错误指示比特：1 表示 AC 的平台鉴别错误指示存在；0 表示 AC 的平台鉴别错误指示不存在。

——AC 的平台配置保护需求比特：1 表示 TNCAP 需要对 AC 的平台配置进行保护；0 表示 TNCAP 不需要对 AC 的平台配置进行保护。

——是否包含 AC 的 PIK 证书比特：1 表示包含 AC 的 PIK 证书；0 表示不包含 AC 的 PIK 证书。

——AC 的 PIK 证书验证需求比特：1 表示需要验证 AC 的 PIK 证书有效性；0 表示不需要验证 AC 的 PIK 证书有效性。

——是否包含 AR 的访问决策比特：1 表示包含 AR 的访问决策；0 表示不包含 AR 的访问决策。

——是否包含 AC 的访问决策比特：1 表示包含 AC 的访问决策；0 表示不包含 AC 的访问决策。

——是否包含 AR 的 Quote 数据(值)比特：1 表示包含 AR 的 Quote 数据值或 AR 的 Quote 数据；0 表示不包含 AR 的 Quote 数据值或 AR 的 Quote 数据。

——是否包含 AC 的 Quote 数据(值)比特：1 表示包含 AC 的 Quote 数据值或 AC 的 Quote 数据；0 表示不包含 AC 的 Quote 数据值或 AC 的 Quote 数据。

——是否包含复合 PIK 证书验证和平台完整性评估结果比特：1 表示包含复合 PIK 证书验证和平台完整性评估结果；0 表示不包含复合 PIK 证书验证和平台完整性评估结果。

b)　一次性随机数

长度为 32 个八位位组。

c)　组件类型级平台完整性度量请求参数条目

组件类型级平台完整性度量请求参数条目如图 34 所示。

FLAG(1)	组件类型厂家 ID(3)
组件类型(4)	组件属性级平台完整性度量请求参数条目数(2)
组件属性级平台完整性度量请求参数条目 1(8)	
组件属性级平台完整性度量请求参数条目 2(8)	
…	

图 34　组件类型级平台完整性度量请求参数

其中：

——FLAG 字段长度为 1 个八位位组，比特 0 有意义。若比特 0 的值为 0，则该组件类型级平台完整性度量请求参数条目可跳过。若比特 0 的值为 1，则该组件类型级平台完整性度量请求参数条目不可跳过。

——组件类型厂家 ID 字段长度为 3 个八位位组，其定义见 8.2.2。

——组件类型字段长度为 4 个八位位组，其定义见 8.2.2。

——组件属性级平台完整性度量请求参数条目数字段长度为 2 个八位位组，其值为组件属性级平台完整性度量请求参数条目数的个数。

——组件属性级平台完整性度量请求参数条目 1、组件属性级平台完整性度量请求参数条目 2、…为本条中 d)定义的组件属性级平台完整性度量请求参数条目。

d)　组件属性级平台完整性度量请求参数条目

组件属性级平台完整性度量请求参数条目如图 35 所示。

保留 (1)	组件属性类型厂家 ID (3)	组件属性类型 (4)

图 35　组件属性级平台完整性度量请求参数条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件属性类型厂家 ID 字段长度为 3 个八位位组，其值如下：

0　表示该组件属性类型是本标准定义的；

其他值保留。

——组件属性类型字段长度为 4 个八位位组，其值如下：

1　产品信息；

2　数字版本；

3　字符串版本；

4　操作状态；

5　完整性信息；

其他值保留。

e)　组件类型级平台完整性评估策略条目

组件类型级平台完整性评估策略条目如图 36 所示。

FLAG(1)	组件类型厂家 ID(3)
组件类型(4)	组件产品级平台完整性评估策略条目数(2)
条目序号 1(2)	组件产品级平台完整性评估策略条目 1(可变)
条目序号 2(2)	组件产品级平台完整性评估策略条目 2(可变)
…	…
组件产品级汇聚平台完整性评估策略(可变)	

图 36　组件类型级平台完整性评估策略条目

其中：

——FLAG 字段长度为 1 个八位位组，比特 0 有意义。若比特 0 的值为 0，则组件产品级汇聚平台完整性评估策略字段不存在。若比特 0 的值为 1，则组件产品级汇聚平台完整性评估策略字段存在。当组件产品级平台完整性评估策略条目数字段的值为 1 时，组件产品级汇聚平台完整性评估策略字段不存在。

——组件类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件类型字段长度为 4 个八位位组，其定义如前。

——组件产品级平台完整性评估策略条目数字段长度为 2 个八位位组，其值为组件产品级平台完整性评估策略条目数的个数。

——条目序号 1、条目序号 2、…分别对应各自后续字段中的组件产品级平台完整性评估策略条目 1、组件产品级平台完整性评估策略条目 2、…，其值为 2 个八位位组的整型数据。

——组件产品级平台完整性评估策略条目 1、组件产品级平台完整性评估策略条目 2、…为本节中 f)定义的组件产品级平台完整性评估策略条目。

——组件产品级汇聚平台完整性评估策略字段长度为可变，其格式为 7.2.2.1.2 中 j)定义的汇聚平台完整性评估策略。当组件产品级汇聚平台完整性评估策略字段中的汇聚平台完整性评估策略类型字段的值为 1 时，组件产品级汇聚平台完整性评估策略字段中的汇聚平台完整性评估策略值字段的值为条目序号 1、条目序号 2、…的或与表达式。

f)　组件产品级平台完整性评估策略条目

组件产品级平台完整性评估策略条目如图 37 所示。

FLAG(1)	组件产品序号(1)
组件属性级平台完整性评估策略条目数(2)	
条目序号 1(2)	组件属性级平台完整性评估策略条目 1(可变)
条目序号 2(2)	组件属性级平台完整性评估策略条目 2(可变)
…	…
组件属性级汇聚平台完整性评估策略(可变)	

图 37　组件产品级平台完整性评估策略条目

其中：

——FLAG 字段长度为 1 个八位位组，比特 0 有意义。若比特 0 的值为 0，则组件属性级汇聚平台完整性评估策略字段不存在。若比特 0 的值为 1，则组件属性级汇聚平台完整性评估策略字段存在。当组件属性级平台完整性评估策略条目数字段的值为 1 时，组件属性级汇聚平台完

整性评估策略字段不存在。

——组件产品序号字段长度为 1 个八位位组，其值为 1、2、…，依次递增。当组件产品序号字段的值为 0xff 时，表示该组件产品级平台完整性评估策略条目不限定于某个组件产品，这时组件属性级平台完整性评估策略条目数字段的值为 1。

——组件属性级平台完整性评估策略条目数字段长度为 2 个八位位组，其值为组件属性级平台完整性评估策略条目数的个数。

——条目序号 1、条目序号 2、…分别对应各自后续字段中的组件属性级平台完整性评估策略条目 1、组件属性级平台完整性评估策略条目 2、…，其值为 2 个八位位组的整型数据。

——组件属性级平台完整性评估策略条目 1、组件属性级平台完整性评估策略条目 2、…为本节中 g)定义的组件属性级平台完整性评估策略条目。

——组件属性级汇聚平台完整性评估策略字段长度为可变，其格式为 7.2.2.1.2 中 j)定义的汇聚平台完整性评估策略。当组件属性级汇聚平台完整性评估策略字段中的汇聚平台完整性评估策略属性字段的值为 1 时，组件属性级汇聚平台完整性评估策略字段中的汇聚平台完整性评估策略值字段的值为条目序号 1、条目序号 2、…的或与表达式。

g) 组件属性级平台完整性评估策略条目

组件属性级平台完整性评估策略条目如图 38 所示。

保留 (1)	组件属性类型厂家 ID (3)	组件属性类型 (4)	组件属性级平台完整性评估策略 (可变)

图 38 组件属性级平台完整性评估策略条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件属性类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件属性类型字段长度为 4 个八位位组，其定义如前。

——组件属性级平台完整性评估策略字段长度为可变，其定义不在本标准中规定。

h) 组件类型级平台完整性度量值条目

组件类型级平台完整性度量值条目如图 39 所示。

<table>
<tr><td colspan="2">保留(1)</td><td colspan="2">组件类型厂家 ID(3)</td></tr>
<tr><td colspan="2">组件类型(4)</td><td>状态码(1)</td><td>IF-IM 级平台完整性度量值条目数(2)</td></tr>
<tr><td colspan="4">IF-IM 级平台完整性度量值条目 1(可变)</td></tr>
<tr><td colspan="4">IF-IM 级平台完整性度量值条目 2(可变)</td></tr>
<tr><td colspan="4">……</td></tr>
</table>

图 39 组件类型级平台完整性度量值条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件类型字段长度为 4 个八位位组，其定义如前。

——状态码字段长度为 1 个八位位组，其值如下：

1 支持；

2　不支持；

其他值保留。

若状态码字段的值为 2，则状态码字段的后续字段不存在。

——IF-IM 级平台完整性度量值条目数字段长度为 2 个八位位组，其值为 IF-IM 级平台完整性度量值条目数的个数。

——IF-IM 级平台完整性度量值条目 1、IF-IM 级平台完整性度量值条目 2、…为本节中 i)定义的 IF-IM 级平台完整性度量值条目。

i)　IF-IM 级平台完整性度量值条目

IF-IM 级平台完整性度量值条目如图 40 所示。

IMC 标识(2)	IF-IM 消息(可变)

图 40　IF-IM 级平台完整性度量值条目

其中：

——IMC 标识字段长度为 2 个八位位组，其定义见 9.2.2.1.1。

——IF-IM 消息字段长度为可变，其定义见 8.2。这里，IF-IM 消息用于封装平台完整性度量值。当 IF-IM 级平台完整性度量值条目用于 PAI-1 协议时，IF-IM 消息中包含完整性报告的 IF-IM 属性。当 IF-IM 级平台完整性度量值条目用于 PAI-2 协议时，IF-IM 消息中包含完整性报告索引信息的 IF-IM 属性。

j)　组件类型级 Quote 数据值条目

组件类型级 Quote 数据值条目如图 41 所示。

保留(1)	组件类型厂家 ID(3)
组件类型(4)	IF-IM 级 Quote 数据值条目数(2)
IF-IM 级 Quote 数据值条目 1(可变)	
IF-IM 级 Quote 数据值条目 2(可变)	
……	

图 41　组件类型级 Quote 数据值条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件类型字段长度为 4 个八位位组，其定义如前。

——IF-IM 级 Quote 数据值条目数字段长度为 2 个八位位组，其值为 IF-IM 级 Quote 数据值条目数的个数。

——IF-IM 级 Quote 数据值条目 1、IF-IM 级 Quote 数据值条目 2、…为本节中 k)定义的 IF-IM 级 Quote 数据值条目。

k)　IF-IM 级 Quote 数据值条目

IF-IM 级 Quote 数据值条目如图 42 所示。

IMC 标识(2)	Quote 数据(可变)

图 42　IF-IM 级 Quote 数据值条目

其中：

——IMC 标识字段长度为 2 个八位位组，其定义见 9.2.2.1.1。

——Quote 数据字段长度为可变，其定义不在本标准中规定。

l) 组件类型级平台配置保护策略条目

组件类型级平台配置保护策略条目如图 43 所示。

保留(1)	组件类型厂家 ID(3)
组件类型(4)	组件产品级平台配置保护策略条目数(2)
组件产品级平台配置保护策略条目 1(可变)	
组件产品级平台配置保护策略条目 2(可变)	
……	

图 43 组件类型级平台配置保护策略条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件类型字段长度为 4 个八位位组，其定义如前。

——组件产品级平台配置保护策略条目数字段长度为 2 个八位位组，其值为组件产品级平台配置保护策略条目数的个数。

——组件产品级平台配置保护策略条目 1、组件产品级平台配置保护策略条目 2、…为本节中 m)定义的组件产品级平台配置保护策略条目。

m) 组件产品级平台配置保护策略条目

组件产品级平台配置保护策略条目如图 44 所示。

保留(1)	组件产品序号(1)
组件属性级平台配置保护策略条目数(2)	
组件属性级平台配置保护策略条目 1(可变)	
组件属性级平台配置保护策略条目 2(可变)	
……	

图 44 组件产品级平台配置保护策略条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件产品序号字段长度为 1 个八位位组，其值为 1、2、…，依次递增。当组件产品序号字段的值为 0xff 时，表示该组件产品级平台配置保护策略条目不限定于某个组件产品。

——组件属性级平台配置保护策略条目数字段长度为 2 个八位位组，其值为组件属性级平台配置保护策略条目数的个数。

——组件属性级平台配置保护策略条目 1、组件属性级平台配置保护策略条目 2、…为本节中 n)定义的组件属性级平台配置保护策略条目。

n) 组件属性级平台配置保护策略条目

组件属性级平台配置保护策略条目如图 45 所示。

保留 (1)	组件属性类型厂家 ID (3)	组件属性类型 (4)	组件属性级平台配置保护策略 (可变)

图 45　组件属性级平台配置保护策略条目

其中：

——保留字段长度为 1 个八位位组，值默认为 0。

——组件属性类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件属性类型字段长度为 4 个八位位组，其定义如前。

——组件属性级平台配置保护策略字段长度为可变，其定义不在本标准中规定。

o)　组件类型级平台修补信息条目

组件类型级平台修补信息条目如图 46 所示。

保留(1)	组件类型厂家 ID(3)
组件类型(4)	IF-IM 级平台修补信息条目数(2)
IF-IM 级平台修补信息条目 1(8)	
IF-IM 级平台修补信息条目 2(8)	
……	

图 46　组件类型级平台修补信息条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件类型字段长度为 4 个八位位组，其定义如前。

——IF-IM 级平台修补信息条目数字段长度为 2 个八位位组，其值为 IF-IM 级平台修补信息条目数的个数。

——IF-IM 级平台修补信息条目 1、IF-IM 级平台修补信息条目 2、…为本节中 p)定义的 IF-IM 级平台修补信息条目。

p)　IF-IM 级平台修补信息条目

IF-IM 级平台修补信息条目如图 47 所示。

IMC 标识(2)	IF-IM 消息(可变)

图 47　IF-IM 级平台修补信息条目

其中：

——IMC 标识字段长度为 2 个八位位组，其定义如前。

——IF-IM 消息字段长度为可变，其定义如前。这里，IF-IM 消息用于封装平台修补信息。

q)　组件类型级错误原因信息条目

组件类型级错误原因信息条目如图 48 所示。

保留(1)	组件类型厂家 ID(3)
组件类型(4)	组件类型级错误原因信息码(2)
组件产品级错误原因信息条目数(2)	
组件产品级错误原因信息条目 1(可变)	
组件产品级错误原因信息条目 2(可变)	
……	

图 48　组件类型级错误原因信息条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件类型字段长度为 4 个八位位组，其定义如前。

——组件类型级错误原因信息码字段长度为 2 个八位位组，其值如下：

1　各个 IMVs 不支持该消息类型(组件类型厂家 ID 及组件类型)；

2　各个 IMCs 不支持该消息类型(组件类型厂家 ID 及组件类型)；

3　生成各个组件产品级错误原因信息条目；

其他值保留。

当组件类型级错误原因信息码字段的值为 3 时，组件类型级错误原因信息码字段的后续字段才存在。

——组件产品级错误原因信息条目数字段长度为 2 个八位位组，其值为组件产品级错误原因信息条目数的个数。

——组件产品级错误原因信息条目 1、组件产品级错误原因信息条目 2、…为本节中 r)定义的组件产品级错误原因信息条目。

r)　组件产品级错误原因信息条目

组件产品级错误原因信息条目如图 49 所示。

保留(1)	条目序号(2)
组件产品级错误原因信息码(2)	组件属性级错误原因信息条目数(2)
组件属性级错误原因信息条目 1(可变)	
组件属性级错误原因信息条目 2(可变)	
……	

图 49　组件产品级错误原因信息条目

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——条目序号字段长度为 2 个八位位组，其值为相应组件产品级平台完整性评估策略条目对应的条目序号。

——组件产品级错误原因信息码字段长度为 2 个八位位组，其值如下：

1　IMV 不支持该组件产品级平台完整性评估策略条目所对应的组件产品序号及组件产品；

2　IMV 不支持该组件产品级平台完整性评估策略条目所对应的组件产品序号、组件属性类

型厂家 ID 及组件属性类型；

3 IMC 不支持该组件产品级平台完整性评估策略条目所对应的组件产品；

4 IMC 不支持该组件产品级平台完整性评估策略条目所对应的组件属性类型厂家 ID 及组件属性类型；

5 生成各个组件属性级错误原因信息条目；

其他值保留。

当组件产品级错误原因信息码字段的值为 5 时，组件产品级错误原因信息码字段的后续字段才存在。

——组件属性级错误原因信息条目数字段长度为 2 个八位位组，其值为组件属性级错误原因信息条目数的个数。

——组件属性级错误原因信息条目 1、组件属性级错误原因信息条目 2、…为本节中 s)定义的组件属性级错误原因信息条目。

s) 组件属性级错误原因信息条目

组件属性级错误原因信息条目如图 50 所示。

保留 (1)	组件属性类型厂家 ID (3)	组件属性类型 (4)	组件属性级错误原因信息码 (2)

图 50 组件属性级错误原因信息条目

其中：

——保留字段长度为 1 个八位位组，值默认为 0。

——组件属性类型厂家 ID 字段长度为 3 个八位位组，其定义如前。

——组件属性类型字段长度为 4 个八位位组，其定义如前。

——组件属性级错误原因信息码字段长度为 2 个八位位组，其值如下：

1 组件属性级平台完整性评估策略和组件属性级平台配置保护策略冲突；

2 IMV 不支持该组件属性类型厂家 ID 及组件属性类型；

3 IMC 不支持该组件属性类型厂家 ID 及组件属性类型；

4 该组件属性类型厂家 ID 及组件属性类型对应的组件属性修补失败；

其他值保留。

7.2.2.1.2 PAI 协议分组数据字段的属性内容

属性采用类型-长度-值(TLV)的格式构成，格式如图 51 所示。

类型 (1)	长度 (4)	值 (可变)

图 51 类型-长度-值(TLV)的格式

其中：

——类型字段长度为 1 个八位位组，其值如下：

1 签名属性；

2　平台完整性度量请求参数；

3　平台完整性评估策略；

4　平台完整性度量值；

5　Quote 数据值；

6　平台配置保护策略；

7　PIK 证书验证和平台完整性评估结果；

8　平台修补信息；

9　错误原因信息；

10 汇聚平台完整性评估策略；

其他值保留。

——长度字段长度为 4 个八位位组，其值是值字段的八位位组数。

——值字段长度为可变，表示属性的内容。

a)　签名属性

签名属性如图 52 所示。

	类型	长度	身份	签名算法	签名值
八位位组数：	1	2	可变	可变	可变

图 52　签名属性

其中身份为 PM 的用户身份证书的身份，或者为 PIK 证书的身份。

签名算法包含长度和内容两个子字段。其长度字段为 2 个八位位组，表示内容字段的八位位组数。内容字段由 1 个八位位组的杂凑算法标识、1 个八位位组的签名算法标识和参数字段组成：

——杂凑算法标识定义如下：

1　表示 SHA-256 杂凑算法；

其他值保留。

——签名算法标识定义如下：

1　表示 ECDSA-192；

2　表示 ECDSA-256；

其他值保留。

——参数字段表示签名算法的参数，由参数标识、参数长度和参数内容组成。参数标识字段长度为 1 个八位位组；参数长度字段为 2 个八位位组，表示参数内容字段的八位位组数；当签名算法标识字段值为 1 时，参数字段的值定义如下：

- 参数标识为 1 时，标识参数以 OID 方式表示，参数长度字段表示 OID 标识的八位位组数，参数内容为 OID 编码，本标准采用的 ECC 参数的 OID 为 1.2.156.11235.1.1.2.1，OID 编码采用 ASN.1/DER。
- 参数标识其他值保留。

——签名值字段包含长度和内容，长度子字段为 2 个八位位组，表示内容子字段的八位位组数。内容子字段为签名的值。

b)　平台完整性度量请求参数

平台完整性度量请求参数如图 53 所示。

类型(1)	长度(4)
保留(1)	组件类型级平台完整性度量请求参数条目数(2)
组件类型级平台完整性度量请求参数条目 1(可变)	
组件类型级平台完整性度量请求参数条目 2(可变)	
……	

图 53　平台完整性度量请求参数

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型级平台完整性度量请求参数条目数字段长度为 2 个八位位组，其值为组件类型级平台完整性度量请求参数条目的个数。

——组件类型级平台完整性度量请求参数条目 1、组件类型级平台完整性度量请求参数条目 2、…为 7.2.2.1.1 中 c)定义的组件类型级平台完整性度量请求参数条目。

c)　平台完整性评估策略

平台完整性评估策略如图 54 所示。

类型(1)	长度(4)
FLAG(1)	组件类型级平台完整性评估策略条目数(2)
条目序号 1(2)	组件类型级平台完整性评估策略条目 1(可变)
条目序号 2(2)	组件类型级平台完整性评估策略条目 1(可变)
……	……
组件类型级汇聚平台完整性评估策略(可变)	

图 54　平台完整性评估策略

其中：

——FLAG 字段长度为 1 个八位位组，比特 0 有意义。若比特 0 的值为 0，则组件类型级汇聚平台完整性评估策略字段不存在。若比特 0 的值为 1，则组件类型级汇聚平台完整性评估策略字段存在。当组件类型级平台完整性评估策略条目数字段的值为 1 时，组件类型级汇聚平台完整性评估策略字段不存在。

——组件类型级平台完整性评估策略条目数字段长度为 2 个八位位组，其值为组件类型级平台完整性评估策略条目的个数。

——条目序号 1、条目序号 2、…分别对应各自后续字段中的组件类型级平台完整性评估策略条目 1、组件类型级平台完整性评估策略条目 2、…，其值为 2 个八位位组的整型数据。

——组件类型级平台完整性评估策略条目 1、组件类型级平台完整性评估策略条目 2、…为 7.2.2.1.1 中 e)定义的组件类型级平台完整性评估策略条目。

——组件类型级汇聚平台完整性评估策略字段长度为可变，其格式为 7.2.2.1.2 中 j)定义的汇聚平台完整性评估策略。当组件类型级汇聚平台完整性评估策略字段中的汇聚平台完整性评估策略类型字段的值为 1 时，组件类型级汇聚平台完整性评估策略字段中的汇聚平台完整性评估策略值字段的值为条目序号 1、条目序号 2、…的或与表达式。

平台完整性评估策略可以被分割为多个部分，其中每一个分割部分的格式与平台完整性评估策略

的格式定义相同。平台完整性评估策略的分割方法如下：首先选取组件类型级汇聚平台完整性评估策略字段中的汇聚平台完整性评估策略值字段中的一个或多个或表达式，若所选取部分中不包含其他部分中的任意条目序号，则依据所选取部分和所选取部分中各个条目序号所对应的组件类型级平台完整性评估策略条目构成平台完整性评估策略的一个分割部分，然后依此方法继续分割直至选取完组件类型级汇聚平台完整性评估策略字段中的汇聚平台完整性评估策略值字段中的所有或表达式。平台完整性评估策略的一个分割部分中的条目序号及对应组件类型级平台完整性评估策略条目不包含在其他分割部分中。

d) 平台完整性度量值

平台完整性度量值如图 55 所示。

类型(1)	长度(4)	
FLAG(1)	完整性报告(可变)	组件类型级平台完整性度量值条目数(2)
组件类型级平台完整性度量值条目 1(可变)		
组件类型级平台完整性度量值条目 2(可变)		
……		

图 55 平台完整性度量值

其中：

——FLAG 字段长度为 1 个八位位组，比特 0 有意义。若比特 0 的值为 1，则完整性报告字段存在；否则不存在。对于 PAI-1 协议，比特 0 的值设置为 0。对于 PAI-2 协议，比特 0 的值设置为 1。

——组件类型级平台完整性度量值条目数字段长度为 2 个八位位组，其值为组件类型级平台完整性度量值条目的个数。

——组件类型级平台完整性度量值条目 1、组件类型级平台完整性度量值条目 2、…为 7.2.2.1.1 中 h)定义的组件类型级平台完整性度量值条目。

e) Quote 数据值

Quote 数据值如图 56 所示。

类型(1)	长度(4)
保留(1)	组件类型级 Quote 数据值条目数(2)
组件类型级 Quote 数据值条目 1(可变)	
组件类型级 Quote 数据值条目 2(可变)	
……	

图 56 Quote 数据值

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型级 Quote 数据值条目数字段长度为 2 个八位位组，其值为组件类型级 Quote 数据值条目的个数。

——组件类型级 Quote 数据值条目 1、组件类型级 Quote 数据值条目 2、…为 7.2.2.1.1 中 j)定义的组件类型级 Quote 数据值条目。

f) 平台配置保护策略

平台配置保护策略如图 57 所示。

类型(1)	长度(4)
保留(1)	组件类型级平台配置保护策略条目数(2)
组件类型级平台配置保护策略条目 1(可变)	
组件类型级平台配置保护策略条目 2(可变)	
……	

图 57　平台配置保护策略

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型级平台配置保护策略条目数字段长度为 2 个八位位组，其值为组件类型级平台配置保护策略条目的个数。

——组件类型级平台配置保护策略条目 1、组件类型级平台配置保护策略条目 2、…为 7.2.2.1.1 中 l)定义的组件类型级平台配置保护策略条目。

g)　PIK 证书验证和平台完整性评估结果

PIK 证书验证和平台完整性评估结果如图 58 所示。

类型　(1)	长度　(2)
一次性随机数 1　(32)	
PIK 证书 1(可变)	PIK 证书验证结果 1　(1)
平台完整性度量值 1(可变)	平台配置保护策略 1(可变)
平台完整性评估策略 1(可变)	平台完整性评估结果 1(1)
平台修补信息 1(可变)	错误原因信息 1(可变)
Quote 数据(值)1(可变)	用于下一个平台鉴别过程的平台完整性评估策略 1(可变)
一次性随机数 2　(32)	
PIK 证书 2(可变)	PIK 证书验证结果 2(1)
平台完整性度量值 2(可变)	平台配置保护策略 2(可变)
平台完整性评估策略 2(可变)	平台完整性评估结果 2(1)
平台修补信息 2(可变)	错误原因信息 2(可变)
Quote 数据(值)2(可变)	用于下一个平台鉴别过程的平台完整性评估策略 2(可变)

图 58　PIK 证书验证和平台完整性评估结果

其中：

——一次性随机数 1、一次性随机数 2 的长度为可变，一次性随机数 1、一次性随机数 2 为 7.2.2.1.1 中 b)定义的一次性随机数。

——PIK 证书 1、PIK 证书 2 字段长度可变，PIK 证书 1、PIK 证书 2 为 PIK 证书。PIK 证书的定义

不在本标准中规定。

——PIK 证书验证结果 1、PIK 证书验证结果 2 字段长度可变，PIK 证书验证结果 1、PIK 证书验证结果 2 字段的值如下：

0　表示证书有效；

1　表示证书的颁发者不明确；

2　表示证书基于不可信任的根证书；

3　表示证书未到生效期或已过期；

4　表示签名错误；

5　表示证书已吊销；

6　表示证书未按规定用途使用；

7　表示证书吊销状态未知；

8　表示证书错误原因未知；

其他值保留。

——平台完整性度量值 1、平台完整性度量值 2 字段长度为可变，平台完整性度量值 1、平台完整性度量值 2 为本节 d)中定义的平台完整性度量值。

——平台配置保护策略 1、平台配置保护策略 2 字段长度为可变，平台配置保护策略 1、平台配置保护策略 2 为本节 f)中定义的平台配置保护策略。

——平台完整性评估策略 1、平台完整性评估策略 2 字段长度为可变，平台完整性评估策略 1、平台完整性评估策略 2 为本节 c)中定义的平台完整性评估策略。

——平台完整性评估结果 1、平台完整性评估结果 2 字段长度可变，平台完整性评估结果 1、平台完整性评估结果 2 字段的值如下：

1　符合策略；

2　不符合策略且能修补；

3　不符合策略因为错误；

4　不符合策略且不能修补；

其他值保留。

——平台修补信息 1、平台修补信息 2 字段长度可变，平台修补信息 1、平台修补信息 2 为本节 h)中定义的平台修补信息。

——错误原因信息 1、错误原因信息 2 字段长度可变，错误原因信息 1、错误原因信息 2 为本节 i)中定义的错误原因信息。

——Quote 数据(值)1、Quote 数据(值)2 字段长度可变，Quote 数据值 1、Quote 数据值 2 为本节 e)中定义 Quote 数据值。Quote 数据 1、Quote 数据 2 为两个 Quote 数据，其中 Quote 数据的定义不在本标准中规定。

——下一个平台鉴别过程的平台完整性评估策略 1、下一个平台鉴别过程的平台完整性评估策略 2 字段长度可变，下一个平台鉴别过程的平台完整性评估策略 1、下一个平台鉴别过程的平台完整性评估策略 2 为本节 c)中定义的平台完整性评估策略。

或表达式对应的平台完整性评估结果、组件类型级平台完整性评估结果、组件产品级平台完整性评估结果和组件属性级平台完整性评估结果的定义与上述平台完整性评估结果相同。

h)　平台修补信息

平台修补信息如图 59 所示。

类型（1）	长度(2)
保留（1）	组件类型级平台修补信息条目数（2）
组件类型级平台修补信息条目 1(可变)	
组件类型级平台修补信息条目 2(可变)	
……	

图 59　平台修补信息

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型级平台修补信息条目数字段长度为 2 个八位位组，其值为组件类型级平台修补信息的条目的个数。

——组件类型级平台修补信息条目 1、组件类型级平台修补信息条目 2、…为 7.2.2.1.1 中 o)定义的组件类型级平台修补信息条目。

i)　错误原因信息

错误原因信息如图 60 所示。

类型（1）	长度(2)
保留（1）	组件类型级错误原因信息条目数（2）
组件类型级错误原因信息条目 1(可变)	
组件类型级错误原因信息条目 2(可变)	
……	

图 60　错误原因信息

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——组件类型级错误原因信息条目数字段长度为 2 个八位位组，其值为组件类型级错误原因信息的条目的个数。

——组件类型错误原因信息条目 1、组件类型级错误原因信息条目 2、为 7.2.2.1.1 中 q)定义的组件类型级错误原因信息条目。

j)　汇聚平台完整性评估策略

汇聚平台完整性评估策略如图 61 所示。

汇聚平台完整性评估策略 类型(1)	汇聚平台完整性评估策略 长度(4)	汇聚平台完整性评估策略 值(可变)

图 61　汇聚平台完整性评估策略

其中：

——汇聚平台完整性评估策略类型字段长度为 1 个八位位组，其值如下：

1　表示汇聚平台完整性评估策略值是基于逻辑与和逻辑或的逻辑表达式，且为或与表达式；

其他值保留。

——汇聚平台完整性评估策略长度字段长度为 4 个八位位组，其值为汇聚平台完整性评估策略值字段的八位位组数。

——汇聚平台完整性评估策略值字段长度为可变。当汇聚平台完整性评估策略类型字段的值为 1 时，则汇聚平台完整性评估策略值为或与表达式，即各个或表达式的与其中或表达式包括单元素或表达式和多元素或表达式（前者仅为一个元素，后者为多个元素的或）。

7.2.2.2 PAI 协议过程

7.2.2.2.1 PAI-1 协议

7.2.2.2.1.1 消息 1

消息 1 的数据字段格式如图 62 所示。

标识 FLAG	TNCAP 挑战	对 AR 的平台完整性度量请求参数
2	32	可变

八位位组数：

图 62 消息 1 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前，比特 0 有意义。比特 0 的值是 TNCAP 依据本轮 PAI 协议中的对 AR 的平台鉴别需求来设置的。在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台鉴别需求为 TNCAP 初始配置的对 AR 的平台鉴别需求；当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台鉴别需求为上一个平台鉴别过程中 TNCAP 设置的用于下一个平台鉴别过程的对 AR 的平台鉴别需求；当本轮 PAI 协议为非首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台鉴别需求为上一轮 PAI 协议中 TNCAP 设置的用于下一轮 PAI 协议的对 AR 的平台鉴别需求。

——TNCAP 挑战字段长度为 32 个八位位组，其值由 TNCAP 采用随机数生成算法生成。当标识 FLAG 字段中比特 0 的值为 0 时，TNCAP 挑战字段不存在。

——对 AR 的平台完整性度量请求参数字段长度为可变，定义如前。当标识 FLAG 字段中比特 0 的值为 0 时，对 AR 的平台完整性度量请求参数字段不存在。对 AR 的平台完整性度量请求参数字段的值是 TNCAP 依据本轮 PAI 协议中的对 AR 的平台完整性评估策略生成的，其中平台完整性评估策略的定义如前。在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台完整性评估策略为 TNCAP 初始配置的对 AR 的平台完整性评估策略或 TNCAP 初始配置的对 AR 的平台完整性评估策略的第一分割部分；当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台完整性评估策略为上一个平台鉴别过程中 TNCAP 设置的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略或上一个平台鉴别过程中 TNCAP 设置的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略的第一分割部分；当本轮 PAI 协议为非首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台完整性评估策略为上一轮 PAI 协议中 TNCAP 设置的用于下一轮 PAI 协议的对 AR 的平台完整性评估策略。TNCAP 初始配置的对 AR 的平台完整性评估策略的分割方法见 7.2.2.1.2 中的 c）。

在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，TNCAP 收到 NAC 发送的平台鉴别请求后向 TNCC 发送消息 1。当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，若本平台鉴别过程是一个双向平台鉴别过程，则 TNCAP 在 AC 完成平台修补且等

待一个最大平台修补时间后向 TNCC 发送消息 1;若本平台鉴别过程是一个对 AR 的单向平台鉴别过程,则 TNCAP 在等待一个最大平台修补时间后向 TNCC 发送消息 1;若本平台鉴别过程是一个对 AC 的平台鉴别过程,则 TNCAP 在 AC 完成平台修补后向 TNCC 发送消息 1。当本轮 PAI 协议为非首轮 PAI 协议时,TNCAP 在本轮 PAI 协议所在的平台鉴别过程还未完成时向 TNCC 发送消息 1。值得注意的是:当本轮 PAI 协议为非首个平台鉴别过程中的一轮 PAI 协议时,若 TNCAP 收到 AR 的平台鉴别错误指示为 2,则 TNCAP 等待一个最大平台修补时间后向 TNCC 发送消息 1。最大平台修补时间不在本标准中规定。消息 1 的生成步骤如下:

a) 若本轮 PAI 协议中的对 AR 的平台鉴别需求的值为 1,即表示 TNCAP 需要对 AR 进行平台鉴别,则 TNCAP 设置标识 FLAG 字段中比特 0 的值为 1。若本轮 PAI 协议中的对 AR 的平台鉴别需求的值为 0,即表示 TNCAP 不需要对 AR 进行平台鉴别,则 TNCAP 设置标识 FLAG 字段中比特 0 的值为 0。若标识 FLAG 字段中的比特 0 的值为 0,则 TNCAP 执行步骤 b);否则执行步骤 c)。

b) 根据标识 FLAG 构成消息 1,并发送给 TNCC。

c) 首先生成 TNCAP 挑战,然后依据本轮 PAI 协议中的对 AR 的平台完整性评估策略生成对 AR 的平台完整性度量请求参数,最后根据标识 FLAG、TNCAP 挑战和对 AR 的平台完整性度量请求参数构成消息 1,并发送给 TNCC。

在依据本轮 PAI 协议中的对 AR 的平台完整性评估策略生成对 AR 的平台完整性度量请求参数的过程中,本轮 PAI 协议中的对 AR 的平台完整性评估策略中的一个组件类型级平台完整性评估策略条目生成对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目,其中该组件类型级平台完整性度量请求参数条目中的消息类型与该组件类型级平台完整性评估策略条目中的消息类型相同,该组件类型级平台完整性度量请求参数条目中的一个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型与该组件类型级平台完整性评估策略条目中的一个或多个组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型相同。若该组件类型级平台完整性评估策略条目所对应的条目序号在本轮 PAI 协议中的对 AR 的平台完整性评估策略中的组件类型级汇聚平台完整性评估策略中是一个单元素或表达式,则该组件类型级平台完整性度量请求参数条目中的 FLAG 字段中比特 0 的值为 1,表示该组件类型级平台完整性度量请求参数条目是不可跳过的。

TNCC 接收到 TNCAP 发送的消息 1 后,进行如下处理:

a) 检查标识 FLAG 字段中的比特 0 的值,若比特 0 的值为 0,执行步骤 b);否则执行步骤 c)。

b) 若本轮 PAI 协议中的对 AC 的平台鉴别需求的值为 0,即表示 TNCC 不需要对 AC 进行平台鉴别,则 TNCC 丢弃消息 1;否则:设置标识 FLAG 字段中的比特 4 的值为 1;若本轮 PAI 协为首个平台鉴别过程中的首轮 PAI 协议且 TNCC 需要验证 AC 的 PIK 证书的有效性,则设置标识 FLAG 字段中的比特 8 的值为 1;生成 TNCC 挑战;依据本轮 PAI 协议中的对 AC 的平台完整性评估策略生成对 AC 的平台完整性度量请求参数;根据标识 FLAG、TNCC 挑战、对 AC 的平台完整性度量请求参数和本轮 PAI 协议中的对 AC 的平台完整性评估策略构成消息 2,并发送给 TNCAP。

c) 若本轮 PAI 协议是非首个平台鉴别过程中的 PAI 协议,且 AR 的平台修补未完成,则 TNCC 首先设置标识 FLAG 字段中比特 1 的值为 1 和 AR 的平台鉴别错误指示为 2,并设置本轮 PAI 协议中的对 AC 的平台鉴别需求和对 AC 的平台完整性评估策略分别为用于下一轮 PAI 协议的对 AC 的平台鉴别需求和对 AC 的平台完整性评估策略,然后根据标识 FLAG、TNCAP 挑战和 AR 的平台鉴别错误指示构造消息 2,并发送给 TNCAP;否则执行步骤 d)。

d) 若本轮 PAI 协议是首个平台鉴别过程中的 PAI 协议，则首先依据 TNCC 上端的各个 IMC 支持的消息类型检查对 AR 的平台完整性度量请求参数，若不支持对 AR 的平台完整性度量请求参数中不可跳过的组件类型级平台完整性度量请求参数条目（即不可跳过的组件类型级平台完整性度量请求参数条目中的消息类型不包含在 TNCC 上端的各个 IMC 支持的消息类型中），则设置标识 FLAG 字段中比特 1 的值为 1 和 AR 的平台鉴别错误指示为 1，然后根据标识 FLAG、TNCAP 挑战和 AR 的平台鉴别错误指示构造消息 2，并发送给 TNCAP；否则执行步骤 e）。

e) 若本轮 PAI 协议中的对 AC 的平台鉴别需求的值为 1，即表示 TNCC 需要对 AC 进行平台鉴别，则 TNCC 设置标识 FLAG 字段中比特 4 的值为 1。若本轮 PAI 协议中的对 AC 的平台鉴别需求的值为 0，即表示 TNCC 不需要对 AC 进行平台鉴别，则 TNCC 设置标识 FLAG 字段中比特 4 的值为 0。若标识 FLAG 字段中比特 4 的值为 0，则执行步骤 f）；否则执行步骤 g）。

f) 依据 TNCAP 挑战、对 AR 的平台完整性度量请求参数生成 AR 的平台完整性度量值、AR 的 Quote 数据值，并在生成 AR 的 Quote 数据值时设置标识 FLAG 字段中比特 11 的值为 1；若 TNCC 需要对 AR 的平台配置进行保护，则依据对 AR 的平台完整性度量请求参数和 TNCC 初始配置的 AR 的平台配置保护策略生成 AR 的平台配置保护策略，并在生成 AR 的平台配置保护策略时设置标识 FLAG 字段中比特 2 的值为 1；当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，依据本地创建的 ConnectionID 获取 AR 的 PIK 证书，并设置标识 FLAG 字段中比特 3 的值为 1；依据标识 FLAG、TNCAP 挑战、AR 的平台完整性度量值、AR 的 Quote 数据值、AR 的平台配置保护策略和 AR 的 PIK 证书构成消息 2，并发送给 TNCAP。

g) 依据 TNCAP 挑战、对 AR 的平台完整性度量请求参数生成 AR 的平台完整性度量值、AR 的 Quote 数据值，并在生成 AR 的 Quote 数据值时设置标识 FLAG 字段中比特 11 的值为 1；若 TNCC 需要对 AR 的平台配置进行保护，则依据对 AR 的平台完整性度量请求参数和 TNCC 初始配置的 AR 的平台配置保护策略生成 AR 的平台配置保护策略，并在生成 AR 的平台配置保护策略时设置标识 FLAG 字段中比特 2 的值为 1；当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，依据本地创建的 ConnectionID 获取 AR 的 PIK 证书，并设置标识 FLAG 字段中比特 3 的值为 1；若本轮 PAI 协为首个平台鉴别过程中的首轮 PAI 协议且 TNCC 需要验证 AC 的 PIK 证书的有效性，则设置标识 FLAG 字段中的比特 8 的值为 1；生成 TNCC 挑战；依据本轮 PAI 协议中的对 AC 的平台完整性评估策略生成对 AC 的平台完整性度量请求参数；依据标识 FLAG、TNCAP 挑战、AR 的平台完整性度量值、AR 的 Quote 数据值、AR 的平台配置保护策略、AR 的 PIK 证书、TNCC 挑战、对 AC 的平台完整性度量请求参数和本轮 PAI 协议中的对 AC 的平台完整性评估策略构成消息 2，并发送给 TNCAP。

在依据本轮 PAI 协议中的对 AC 的平台完整性评估策略生成对 AC 的平台完整性度量请求参数的过程中，本轮 PAI 协议中的对 AC 的平台完整性评估策略中的一个组件类型级平台完整性评估策略条目生成对 AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目，其中该组件类型级平台完整性度量请求参数条目中的消息类型与该组件类型级平台完整性评估策略条目中的消息类型相同，该组件类型级平台完整性度量请求参数条目中的一个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型与该组件类型级平台完整性评估策略条目中的一个或多个组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型相同。若该组件类型级平台完整性评估策略条目所对应的条目序号在本轮 PAI 协议中的对 AC 的平台完整性评估策略中的组件类型级汇聚平台完整性评估策略中是一个单元素或表达式，则该组件类型级平台完整性度量请求参数条目中的 FLAG 字段中比特 0 的值为 1，表示该组件类型级平台完整性度量请求参数条目是不可跳过的。

在依据 TNCAP 挑战、对 AR 的平台完整性度量请求参数生成 AR 的平台完整性度量值、AR 的

Quote 数据值的过程中，对于对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目，若该组件类型级平台完整性度量请求参数条目不为 TNCC 上端的任意一个 IMC 所支持，则生成一个组件类型级平台完整性度量值条目，其状态码的值设置为 2；否则利用 AR 中的 IF-IMC 功能函数 TCA_IMC_RequestMeasurementInfo 将 TNCAP 挑战和该组件类型级平台完整性度量请求参数条目中的各个组件属性级平台完整性度量请求参数条目发送给 TNCC 上端的相应 IMC。当 TNCC 上端的一个 IMC 收到 TNCAP 挑战和一个组件类型级平台完整性度量请求参数条目中的各个组件属性级平台完整性度量请求参数条目时，该 IMC 首先依据 TNCAP 挑战和各个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型执行平台完整性度量（具体度量过程不在本标准中规定），并生成一个 IF-IM 消息和一个 Quote 数据（当该 IF-IM 消息中包含 Quote 数据时该 Quote 数据才被生成），然后利用 AR 中的 IF-IMC 功能函数 TCA_TNCC_SendMessage 将该 IF-IM 消息发送给 TNCC，并利用 AR 中的 IF-IMC 功能函数 TCA_TNCC_ProvideQuoteData 将该 Quote 数据发送给 TNCC（不管是否生成该 IF-IM 消息对应的 Quote 数据，本功能函数都必须执行）。当从 TNCC 上端的一个 IMC 收到一个 IF-IM 消息时，TNCC 依据该 IF-IM 消息生成一个 IF-IM 级平台完整性度量值条目，若对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目对应的所有 IF-IM 消息都已收到，则利用该组件类型级平台完整性度量请求参数条目对应的各个 IF-IM 级平台完整性度量值条目生成一个组件类型级平台完整性度量值条目，若对 AR 的平台完整性度量请求参数对应的所有 IF-IM 消息都已收到，则利用对 AR 的平台完整性度量请求参数对应的各个组件类型级平台完整性度量值条目生成 AR 的平台完整性度量值。当从 TNCC 上端的一个 IMC 收到一个 Quote 数据时，TNCC 依据该 Quote 数据生成一个 IF-IM 级 Quote 数据值条目，若对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目对应的所有 Quote 数据都已收到，则利用该组件类型级平台完整性度量请求参数条目对应的各个 IF-IM 级 Quote 数据值条目生成一个组件类型级 Quote 数据条目，若对 AR 的平台完整性度量请求参数对应的所有 Quote 数据都已收到，则利用对 AR 的平台完整性度量请求参数对应的各个组件类型级 Quote 数据条目生成 AR 的 Quote 数据值。

在依据对 AR 的平台完整性度量请求参数和 TNCC 初始配置的 AR 的平台配置保护策略生成 AR 的平台配置保护策略的过程中，对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目生成 AR 的平台配置保护策略中的零个或一个组件类型级平台配置保护策略条目，其中该组件类型级平台配置保护策略条目中的消息类型与该组件类型级平台完整性度量请求参数条目中的消息类型相同，该组件类型级平台配置保护策略条目中的一个或多个组件属性级平台配置保护策略条目中的组件属性类型厂家 ID 及组件属性类型与该组件类型级平台完整性度量请求参数条目中的一个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型相同。当在 TNCC 预配置的 AR 的平台配置保护策略中找不到该组件类型级平台完整性度量请求参数条目中的消息类型时，TNCC 不能生成该组件类型级平台完整性度量请求参数条目对应的组件类型级平台配置保护策略条目。当在 TNCC 预配置的 AR 的平台配置保护策略中找不到该组件类型级平台完整性度量请求参数条目中的任意组件属性类型厂家 ID 及组件属性类型时，TNCC 不能生成该组件类型级平台完整性度量请求参数条目对应的组件类型级平台配置保护策略条目。

对于一个消息类型，TNCC 上端的一个 IMC 可以支持该消息类型下的多个组件产品的平台完整性度量，但是 TNCC 上端的多个 IMC 不可以支持该消息类型下的同一个组件产品的平台完整性度量。

7.2.2.2.1.2 消息 2

消息 2 的数据字段格式如图 63 所示。

	标识 FLAG	TNCAP 挑战	AR的平台鉴别错误指示	AR的平台完整性度量值	AR的 Quote 数据值	AR的平台配置保护策略	AR的 PIK 证书	TNCC 挑战	对AC的平台完整性度量请求参数	对AC的平台完整性评估策略
八位位组数：	2	32	1	可变	可变	可变	可变	32	可变	可变

图 63　消息 2 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前。比特 0、1、2、3、4、8 和 11 有意义。比特 0 的值与消息 1 中标识 FLAG 字段中的比特 0 的值相同。比特 4 的值是 TNCC 依据本轮 PAI 协议中的对 AC 的平台鉴别需求来设置的。在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台鉴别需求为 TNCC 初始配置的对 AC 的平台鉴别需求；当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台鉴别需求为上一个平台鉴别过程中 TNCC 设置的用于下一个平台鉴别过程的对 AC 的平台鉴别需求；当本轮 PAI 协议为非首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台鉴别需求为上一轮 PAI 协议中 TNCC 设置的用于下一轮 PAI 协议的对 AC 的平台鉴别需求。

——TNCAP 挑战字段长度为 32 个八位位组，其值与消息 1 中的 TNCAP 挑战相同。当标识 FLAG 字段中比特 0 的值为 0 时，TNCAP 挑战字段不存在。

——AR 的平台鉴别错误指示字段长度为 1 个八位位组。当标识 FLAG 字段中比特 1 的值为 0 时，AR 的平台鉴别错误指示字段不存在。AR 的平台鉴别错误指示字段的值如下：

1　发生不可跳过错误；

2　平台修补未完成；

其他值保留。

——AR 的平台完整性度量值字段长度为可变，定义如前。若 AR 和 PM 之间存在安全通道，则 AR 的平台完整性度量值在安全通道中传递给 PM；否则 AR 的平台完整性度量值可采用数字信封（参见附录 C）的方式传递给 PM。AR 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。

——AR 的 Quote 数据值字段长度为可变，定义如前。当标识 FLAG 字段中比特 11 的值为 0 时，AR 的 Quote 数据值字段不存在。

——AR 的平台配置保护策略字段长度为可变，定义如前。当标识 FLAG 字段中比特 2 的值为 0 时，AR 的平台配置保护策略字段不存在。若 AR 和 PM 之间存在安全通道，则 AR 的平台配置保护策略在安全通道中传递给 PM；否则 AR 的平台配置保护策略可采用数字信封（参见附录 C）的方式传递给 PM。AR 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。

——AR 的 PIK 证书字段长度为可变，其定义不在本标准中规定。当标识 FLAG 字段中比特 3 的值为 0 时，AR 的 PIK 证书字段不存在。

——TNCC 挑战字段长度为 32 个八位位组，由 TNCC 采用随机数生成算法生成。当 FLAG 标识字段的比特 4 的值为 0 时，本字段不存在。

——对 AC 的完整性度量请求参数字段为可变长度，定义如前。当 FLAG 标识字段的比特 4 的值为 0 时，本字段不存在。对 AC 的平台完整性度量请求参数字段的值是 TNCC 依据本轮 PAI 协议中的对 AC 的平台完整性评估策略生成的，其中平台完整性评估策略的定义如前。在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，本轮

PAI 协议中的对 AC 的平台完整性评估策略为 TNCC 初始配置的对 AC 的平台完整性评估策略或 TNCC 初始配置的对 AC 的平台完整性评估策略的第一分割部分；当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台完整性评估策略为上一个平台鉴别过程中 TNCC 设置的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略或上一个平台鉴别过程中 TNCC 设置的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略的第一分割部分；当本轮 PAI 协议为非首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台完整性评估策略为上一轮 PAI 协议中 TNCC 设置的用于一轮 PAI 协议的对 AC 的平台完整性评估策略。TNCC 初始配置的对 AC 的平台完整性评估策略的分割方法见 7.2.2.1.2 中的 c)。

——对 AC 的平台完整性评估策略字段长度为可变，定义如前。当 FLAG 标识字段的比特 4 的值为 0 时，本字段不存在。若 AR 和 PM 之间存在安全通道，则 AR 的完整性评估策略在安全通道中传递给 PM；否则 AR 的完整性评估策略可采用数字信封（参见附录 C）的方式传递给 PM。AR 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。

当 TNCC 接收到 TNCAP 发送的消息 1，TNCC 向 TNCAP 发送消息 2。

TNCAP 接收到 TNCC 发送的消息 2 后，进行如下处理：

a) 检查标识 FLAG 字段中比特 0 的值，若值为 0，则执行步骤 b)；否则步骤 d)。

b) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则丢弃消息 2；否则执行步骤 c)。

c) 若本轮 PAI 协议为首个平台鉴别过程中的 PAI 协议，则首先依据 TNCAP 上端的各个 IMC 支持的消息类型检查对 AC 的平台完整性度量请求参数，若不支持对 AC 的平台完整性度量请求参数中不可跳过的组件类型级平台完整性度量请求参数条目（即不可跳过的组件类型级平台完整性度量请求参数条目中的消息类型不包含在 TNCAP 上端的各个 IMC 支持的消息类型中），则设置标识 FLAG 字段中比特 5 的值为 1 和 AC 的平台鉴别错误指示字段的值为 1，然后根据标识 FLAG、TNCC 挑战和 AC 的平台鉴别错误指示构造消息 5，并发送给 TNCC；否则：依据 TNCC 挑战、对 AC 的平台完整性度量请求参数生成 AC 的平台完整性度量值、AC 的 Quote 数据值；若 TNCAP 需要对 AC 的平台配置进行保护，则依据对 AC 的平台完整性度量请求参数和 TNCAP 初始配置的 AC 的平台配置保护策略生成 AC 的平台配置保护策略，并在生成 AC 的平台配置保护策略后设置标识 FLAG 字段中比特 6 的值为 1；当标识 FLAG 字段中比特 8 的值为 1 时，TNCAP 依据本地创建的 ConnectionID 获取 AC 的 PIK 证书，并设置标识 FLAG 字段中比特 7 的值为 1；依据标识 FLAG、TNCC 挑战、AC 的 PIK 证书、AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略构成消息 3，并发送给 EPS。

d) 检查标识 FLAG 字段中的比特 1 的值，若比特 1 的值为 1，则执行步骤 e)；否则执行步骤 f)。

e) 检查 TNCAP 挑战字段的值，若值与消息 1 中的 TNCAP 挑战字段不相同，则丢弃消息 2；否则继续检查 AR 的平台鉴别错误指示字段的值，若值为 2，则 TNCAP 在等待一个最大平台修补时间后执行下一轮 PAI 协议，并设置用于下一轮 PAI 协议的对 AR 的平台鉴别需求和对 AR 的平台完整性评估策略分别为本轮 PAI 协议中的对 AR 的平台鉴别需求和对 AR 的平台完整性评估策略；若值为 1，则 TNCAP 生成 AC 的访问决策为禁止（将 AC 的访问决策发送给 NAC），并设置标识 FLAG 字段中比特 10 的值为 1，然后依据标识 FLAG、TNCAP 挑战、AC 的访问决策构成消息 5，并发送给 TNCC。

f) 检查 TNCAP 挑战字段的值，若与消息 1 中的 TNCAP 挑战字段不相同，则丢弃消息 2；否则检查标识 FLAG 字段中比特 11 的值，若值为 1，则执行步骤 g)；否则执行步骤 h)。

g) 验证 AR 的 Quote 数据值中的各个 PIK 签名，若验证不通过，则丢弃消息 2；否则执行步

骤 h)。

h) 检查标识 FLAG 字段中比特 4 的值,若值为 0,则执行步骤 i);否则执行步骤 j)。

i) 生成 TNCAP 平台鉴别挑战;若本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议且 TNCAP 需要验证 AR 的 PIK 证书有效性,则设置标识 FLAG 字段中比特 3 的值为 1;依据标识 FLAG、TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略构成消息 3,并发送给 EPS。

j) 若本轮 PAI 协议是首个平台鉴别过程中的 PAI 协议,则首先依据 TNCAP 上端的各个 IMC 支持的消息类型检查对 AC 的平台完整性度量请求参数,若不支持对 AC 的平台完整性度量请求参数中不可跳过的组件类型级平台完整性度量请求参数条目(即不可跳过的组件类型级平台完整性度量请求参数条目中的消息类型不包含在 TNCAP 上端的各个 IMC 支持的消息类型中),则设置标识 FLAG 字段中比特 5 的值为 1 和 AC 的平台鉴别错误指示的值为 1,然后根据标识 FLAG、TNCC 挑战和 AC 的平台鉴别错误指示构造消息 5,并发送给 TNCC;否则:依据 TNCC 挑战、对 AC 的平台完整性度量请求参数生成 AC 的平台完整性度量值、AC 的 Quote 数据值;若 TNCAP 需要对 AC 的平台配置进行保护,则依据对 AC 的平台完整性度量请求参数和 TNCAP 初始配置的 AC 的平台配置保护策略生成 AC 的平台配置保护策略,并在生成 AC 的平台配置保护策略后设置标识 FLAG 字段中比特 6 的值为 1;当标识 FLAG 字段中比特 8 的值为 1 时,TNCAP 依据本地创建的 ConnectionID 获取 AC 的 PIK 证书,并设置标识 FLAG 字段中比特 7 的值为 1;生成 TNCAP 平台鉴别挑战;若本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议且 TNCAP 需要验证 AR 的 PIK 证书有效性,则设置标识 FLAG 字段中比特 3 的值为 1;依据标识 FLAG、TNCAP 平台鉴别挑战、TNCC 挑战、AR 的 PIK 证书、AC 的 PIK 证书、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略构成消息 3,并发送给 EPS。

在依据 TNCC 挑战、对 AC 的平台完整性度量请求参数生成 AC 的平台完整性度量值、AC 的 Quote 数据值的过程中,对于对 AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目,若该组件类型级平台完整性度量请求参数条目不为 TNCAP 上端的任意一个 IMC 所支持,则生成一个组件类型级平台完整性度量值条目,其状态码的值设置为 2;否则利用 AC 中的 IF-IMC 功能函数 TCA_IMC_RequestMeasurementInfo 将 TNCC 挑战和该组件类型级平台完整性度量请求参数条目中的各个组件属性级平台完整性度量请求参数条目发送给 TNCAP 上端的相应 IMC。当 TNCAP 上端的一个 IMC 收到 TNCC 挑战和一个组件类型级平台完整性度量请求参数条目中的各个组件属性级平台完整性度量请求参数条目时,该 IMC 首先依据 TNCC 挑战和各个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型执行平台完整性度量(具体度量过程不在本标准中规定),并生成一个 IF-IM 消息和一个 Quote 数据(当该 IF-IM 消息中包含 Quote 数据时该 Quote 数据才被生成),然后利用 AC 中的 IF-IMC 功能函数 TCA_TNCAP_SendMessage 将该 IF-IM 消息发送给 TNCAP,并利用 AC 中的 IF-IMC 功能函数 TCA_TNCAP_ProvideQuoteData 将该 Quote 数据发送给 TNCAP(不管是否生成该 IF-IM 消息对应的 Quote 数据,本功能函数都必须执行)。当从 TNCAP 上端的一个 IMC 收到一个 IF-IM 消息时,TNCAP 依据该 IF-IM 消息生成一个 IF-IM 级平台完整性度量值条目,若对 AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目对应的所有 IF-IM 消息都已收到,则利用该组件类型级平台完整性度量请求参数条目对应的各个 IF-IM 级平台完整性度量值条目生成一个组件类型级平台完整性度量值条目,若对 AC 的平台完整性度量请求参数对应的所有 IF-IM 消息都已收到,则利用对 AC 的平台完整性度量请求参数对应的各个组件类型级平台完整性度量值条目生成 AC 的平台完整性度量值。当从 TNCAP 上端的一个 IMC 收到一个 Quote 数据时,TNCAP 依据该 Quote 数据生成一个 IF-IM 级 Quote 数据值条目,若对

AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目对应的所有 Quote 数据都已收到，则利用该组件类型级平台完整性度量请求参数条目对应的各个 IF-IM 级 Quote 数据值条目生成一个组件类型级 Quote 数据条目，若对 AC 的平台完整性度量请求参数对应的所有 Quote 数据都已收到，则利用对 AC 的平台完整性度量请求参数对应的各个组件类型级 Quote 数据条目生成生成 AC 的 Quote 数据值。

在依据对 AC 的平台完整性度量请求参数和 TNCAP 初始配置的 AC 的平台配置保护策略生成 AC 的平台配置保护策略的过程中，对 AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目生成 AC 的平台配置保护策略中的零个或一个组件类型级平台配置保护策略条目，其中该组件类型级平台配置保护策略条目中的消息类型与该组件类型级平台完整性度量请求参数条目中的消息类型相同，该组件类型级平台配置保护策略条目中的一个或多个组件属性级平台配置保护策略条目中的组件属性类型厂家 ID 及组件属性类型与该组件类型级平台完整性度量请求参数条目中的一个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型相同。当在 TNCAP 预配置的 AC 的平台配置保护策略中找不到该组件类型级平台完整性度量请求参数条目中的消息类型时，TNCAP 不能生成该组件类型级平台完整性度量请求参数条目对应的组件类型级平台配置保护策略条目。当在 TNCAP 预配置的 AC 的平台配置保护策略中找不到该组件类型级平台完整性度量请求参数条目中的任意组件属性类型厂家 ID 及组件属性类型时，TNCAP 不能生成该组件类型级平台完整性度量请求参数条目对应的组件类型级平台配置保护策略条目。

对于一个消息类型，TNCAP 上端的一个 IMC 可以支持该消息类型下的多个组件产品的平台完整性度量，但是 TNCAP 上端的多个 IMC 不可以支持该消息类型下的同一个组件产品的平台完整性度量。

7.2.2.2.1.3 消息 3

消息 3 的数据字段格式如图 64 所示。

	标识 FLAG	TNCAP 平台鉴别挑战	TNCC 挑战	AR 的 PIK 证书	AC的 PIK 证书	AR的平台完整性度量值	AR的平台配置保护策略	对AR的平台完整性评估策略	AC的平台完整性度量值	AC的平台配置保护策略	对AC的平台完整性评估策略
八位位组数：	2	32	32	可变	可变	可变	可变	可变	可变	可变	可变

图 64 消息 3 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前。比特 0、2、3、4、6 和 7 有意义。比特 0、2 和 4 的值分别与消息 2 中标识 FLAG 字段中比特 0、2 和 4 的值相同。

——TNCAP 平台鉴别挑战字段长度为 32 个八位位组，由 TNCAP 采用随机数生成算法产生的，用于与 EPS 进行信息交互。当标识 FLAG 字段中比特 0 的值为 0 时，本字段不存在。

——TNCC 挑战字段长度为 32 个八位位组，本字段的值与消息 2 中 TNCC 挑战字段的值相同。当标识 FLAG 字段中比特 4 的值为 0 时，本字段不存在。

——AR 的 PIK 证书字段长度为可变，本字段的值与消息 2 中 AR 的 PIK 证书字段的值相同。当标识 FLAG 字段中比特 3 的值为 0 时，本字段不存在。

——AC 的 PIK 证书字段长度为可变，其定义不在本标准中规定。当标识 FLAG 字段中比特 7 的值为 0 时，本字段不存在。

——AR 的平台完整性度量值字段长度为可变，本字段的值与消息 2 中 AR 的平台完整性度量值

字段的值相同。当标识 FLAG 字段中比特 0 的值为 0 时，本字段不存在。

——AR 的平台配置保护策略字段长度为可变，本字段的值与消息 2 中 AR 的平台配置保护策略字段的值相同。当标识 FLAG 字段中比特 2 的值为 0 时，本字段不存在。

——对 AR 的平台完整性评估策略字段长度为可变，定义如前。若 AC 和 PM 之间存在安全通道，则对 AR 的平台完整性评估策略在该安全通道中传递给 PM；否则对 AR 的平台完整性评估策略可采用数字信封（参见附录 C）的方式传递给 PM。AC 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。当标识 FLAG 字段中比特 0 的值为 0 时，本字段不存在。

——AC 的平台完整性度量值字段长度为可变，定义如前。若 AC 和 PM 之间存在安全通道，则 AC 的平台完整性度量值在该安全通道中传递给 PM；否则 AC 的平台完整性度量值可采用数字信封（参见附录 C）的方式传递给 PM。AC 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。当标识 FLAG 字段中比特 4 的值为 0 时，本字段不存在。

——AC 的平台配置保护策略字段长度为可变，定义如前。当标识 FLAG 字段中比特 6 的值为 0 时，本字段不存在。若 AC 和 PM 之间存在安全通道，则 AC 的平台配置保护策略在该安全通道中传递给 PM；否则 AC 的平台配置保护策略可采用数字信封（参见附录 C）的方式传递给 PM。AC 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。当标识 FLAG 字段中比特 6 的值为 1 时，本字段存在。

——对 AC 的平台完整性评估策略字段长度为可变，本字段的值与消息 2 中对 AC 的平台完整性评估策略字段的值相同。当标识 FLAG 字段中比特 4 的值为 0 时，本字段不存在。

当 TNCAP 接收到 TNCC 发送的消息 2 时，TNCAP 向 EPS 发送消息 3，或向 TNCC 发送消息 5。

EPS 接收到 TNCAP 发送的消息 3 后，进行如下处理：

a) 检查标识 FLAG 字段中比特 0 的值，若值为 0，则执行步骤 b)；否则执行步骤 d)。

b) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则丢弃消息 3；否则执行步骤 c)。

c) 若标识 FLAG 字段中比特 7 的值为 1，则验证 AC 的 PIK 证书，并生成 AC 的 PIK 证书验证结果；依据 AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略生成 AC 的平台完整性评估结果、AC 的平台修补信息、AC 的错误原因信息、AC 的 Quote 数据值和下一个平台鉴别过程的对 AC 的平台完整性评估策略；若生成 AC 的 Quote 数据值，则设置标识 FLAG 字段中比特 12 的值为 1；生成 PIK 证书验证和平台完整性评估结果；利用 PM 的用户证书的私钥生成对 PIK 证书验证和平台完整性评估结果的签名；依据标识 FLAG、PIK 证书验证和平台完整性评估结果、对 PIK 证书验证和平台完整性评估结果的签名构成消息 4，并发送给 TNCAP。

d) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则执行步骤 e)；否则执行步骤 f)。

e) 若标识 FLAG 字段中比特 3 的值为 1，则验证 AR 的 PIK 证书，并生成 AR 的 PIK 证书验证结果；依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略；若生成 AR 的 Quote 数据值，则设置标识 FLAG 字段中比特 11 的值为 1；生成 PIK 证书验证和平台完整性评估结果；利用 PM 的用户证书的私钥生成对 PIK 证书验证和平台完整性评估结果的签名；依据标识 FLAG、PIK 证书验证和平台完整性评估结果、对 PIK 证书验证和平台完整性评估结果的签名构成消息 4，并发送给 TNCAP。

f) 若标识 FLAG 字段中比特 3 的值为 1，则验证 AR 的 PIK 证书，并生成 AR 的 PIK 证书验证结果；依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略

生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略；若生成 AR 的 Quote 数据值，则设置标识 FLAG 字段中比特 11 的值为 1；若标识 FLAG 字段中比特 7 的值为 1，则验证 AC 的 PIK 证书，并生成 AC 的 PIK 证书验证结果；依据 AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略生成 AC 的平台完整性评估结果、AC 的平台修补信息、AC 的错误原因信息、AC 的 Quote 数据值和下一个平台鉴别过程的对 AC 的平台完整性评估策略；若生成 AC 的 Quote 数据值，则设置标识 FLAG 字段中比特 12 的值为 1；生成 PIK 证书验证和平台完整性评估结果；利用 PM 的用户证书的私钥生成对 PIK 证书验证和平台完整性评估结果的签名；依据标识 FLAG、PIK 证书验证和平台完整性评估结果、对 PIK 证书验证和平台完整性评估结果的签名构成消息 4，并发送给 TNCAP。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，对于对 AR 的平台完整性评估策略中的一个组件类型级平台完整性评估策略条目，若该组件类型级平台完整性评估策略条目中的消息类型不为 EPS 上端的任意一个 IMV 所支持，则生成一个组件类型级平台完整性评估结果(值设置为 3)和一个组件类型级错误原因信息条目(组件类型级错误原因信息码字段的值设置为 1)；否则依据该组件类型级平台完整性评估策略条目中的消息类型从 AR 的平台完整性度量值中读取相应组件类型级平台完整性度量值条目，若该组件类型级平台完整性度量值条目中状态码字段的值为 2，则生成一个组件类型级平台完整性评估结果(值设置为 3)和一个组件类型级错误原因信息条目(组件类型级错误原因信息码字段的值设置为 2)；否则利用 PM 中的 IF-IMV 功能函数 TCA_IMV_RequestEvaluationInfo 将该组件类型级平台完整性评估策略条目中的各个组件产品级平台完整性评估策略条目、该组件类型级平台完整性度量值条目中的各个 IF-IM 级平台完整性度量值条目、AR 的平台配置保护策略中对应该组件类型级平台完整性评估策略条目的组件类型级平台配置保护策略条目中的各个组件产品级平台配置保护策略条目发送给 EPS 上端的各个相应 IMV。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，当 EPS 上端的一个 IMV 收到一个组件产品级平台完整性评估策略条目(其组件产品序号为非 0xff 值)及相应条目序号、各个组件产品级平台配置保护策略条目、各个 IF-IM 级平台完整性度量值条目时，若该 IMV 不支持该组件产品级平台完整性评估策略条目所对应的组件产品序号及组件产品，则首先生成一个组件产品级平台完整性评估结果(值设置为 3)和一个组件产品级错误原因信息条目(组件产品级错误原因信息码字段的值设置为 1)，然后利用 PM 中的 IF-IMV 功能函数 TCA_EPS_ProvideEvaluationResult 将该组件产品级平台完整性评估结果和该组件产品级错误原因信息条目发送给 EPS；否则检查各个 IF-IM 级平台完整性度量值条目，若找不到该组件产品级平台完整性评估策略条目所对应的组件产品，则生成一个组件产品级平台完整性评估结果(值设置为 3)和一个组件产品级错误原因信息条目(组件产品级错误原因信息码字段的值设置为 3)，然后利用 PM 中的 IF-IMV 功能函数 TCA_EPS_ProvideEvaluationResult 将该组件产品级平台完整性评估结果和该组件产品级错误原因信息条目发送给 EPS；否则依据该组件产品级平台完整性评估策略条目中的各个组件属性级平台完整性评估策略条目及组件属性级汇聚平台完整性评估策略、该组件产品级平台完整性评估策略条目对应的 IF-IM 级平台完整性度量值条目和该组件产品级平台完整性评估策略条目对应的组件产品级平台配置保护策略条目执行平台完整性评估，并生成一个组件产品级平台完整性评估结果、一个 IF-IM 级平台修补信息条目、一个组件产品级错误原因信息条目、一个 IF-IM 级 Quote 数据值条目和一个用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目，其具体过程如图 65 所示。

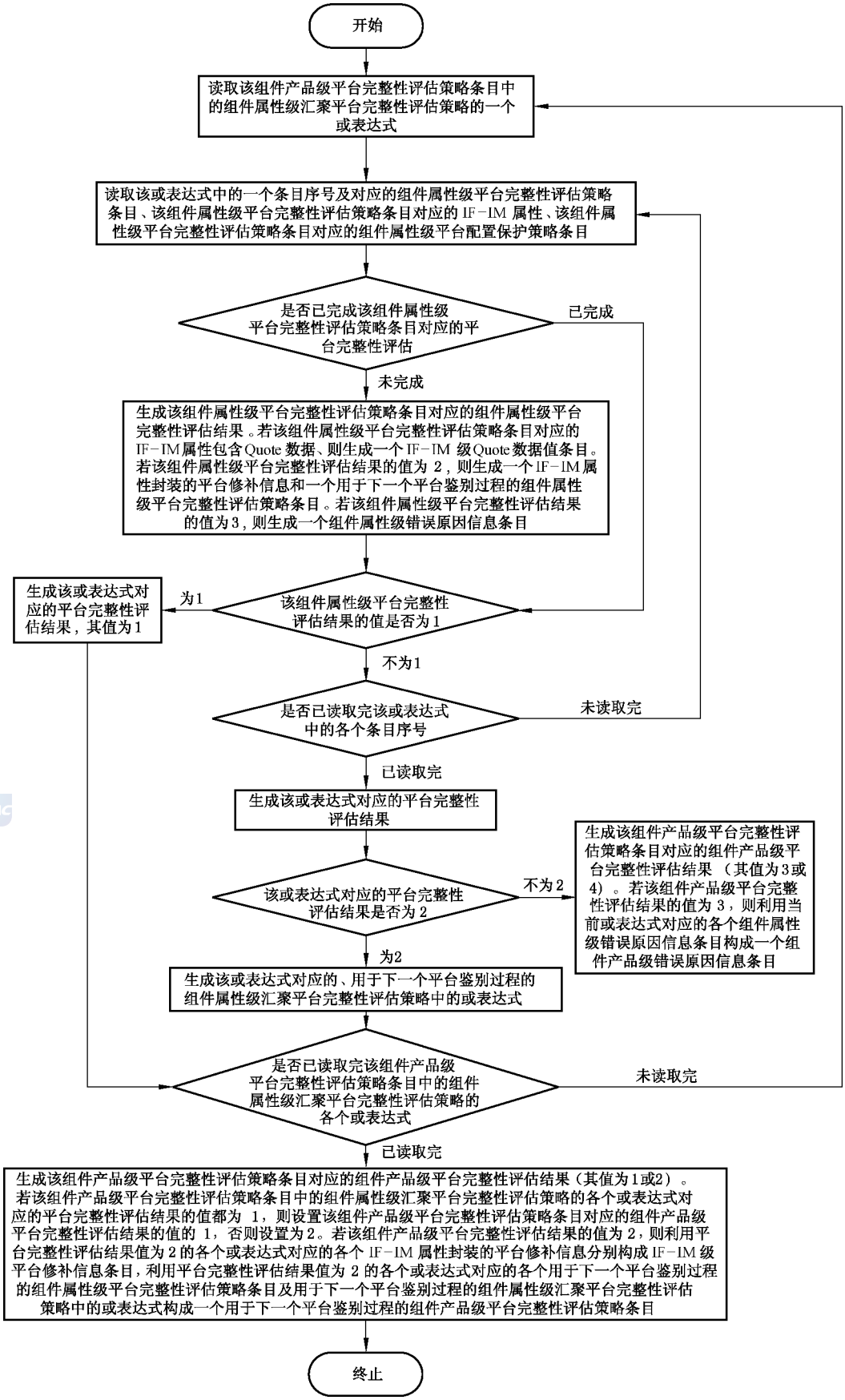

图 65　PAI-1 协议中 IMV 生成组件产品级平台完整性评估结果及其他参数的具体过程

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，当 EPS 上端的一个 IMV 收到一个组件产品级平台完整性评估策略条目（其组件产品序号为 0xff 值）及相应条目序号、各个组件产品级平台配置保护策略条目、各个 IF-IM 级平台完整性度量值条目时，若该 IMV 不支持该组件产品级平台完整性评估策略条目所对应的组件产品序号、组件属性类型厂家 ID 及组件属性类型，则首先生成一个组件产品级平台完整性评估结果（值设置为 3）和一个组件产品级错误原因信息条目（组件产品级错误原因信息码字段的值设置为 2），然后利用 PM 中的 IF-IMV 功能函数 TCA_EPS_ProvideEvaluationResult 将该组件产品级平台完整性评估结果和该组件产品级错误原因信息条目发送给 EPS；否则检查各个 IF-IM 级平台完整性度量值条目，若找不到该组件产品级平台完整性评估策略条目中的组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型，则生成一个组件产品级平台完整性评估结果（值设置为 4）；否则检查各个 IF-IM 级平台完整性度量值条目，若只能找到该组件产品级平台完整性评估策略条目中的组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型对应的 IF-IM 错误信息，则生成一个组件产品级平台完整性评估结果（值设置 3）和一个组件产品级错误原因信息条目（组件产品级错误原因信息码字段的值设置为 4）；否则依据该组件产品级平台完整性评估策略条目中的组件属性级平台完整性评估策略条目执行平台完整性评估，若各个 IF-IM 级平台完整性度量值条目中的所有组件产品的各个包含该组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型的 IF-IM 属性都符合该组件属性级平台完整性评估策略条目对应的组件属性级平台完整性评估策略，则生成一个组件产品级平台完整性评估结果（值设置为 1）；否则生成一个组件产品级平台完整性评估结果（值设置为 4）。

对于一个消息类型，EPS 上端的一个 IMV 可以支持该消息类型下的多个组件产品级平台完整性评估策略条目对应的平台完整性评估，但是 EPS 上端的多个 IMV 不可以支持该消息类型下的同一个组件产品级平台完整性评估策略条目对应的平台完整性评估。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，对于一个组件产品级平台完整性评估策略条目，EPS 从 EPS 上端相应的各个 IMV 接收该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目、IF-IM 级 Quote 数据值条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目，若从每个 IMV 都接收到一个组件产品级错误原因信息条目，且该组件产品级错误原因信息条目中的组件产品级错误原因信息码字段的值为 1 或 2，则 EPS 以任意一个从 IMV 接收到的该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目、IF-IM 级 Quote 数据值条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目作为 EPS 生成的该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目、IF-IM 级 Quote 数据值条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目；否则以一个从 IMV 接收到的、组件产品级错误原因信息条目中的组件产品级错误原因信息码字段的值不为 1 或 2 的该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目、IF-IM 级 Quote 数据值条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目作为 EPS 生成的该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目、IF-IM 级 Quote 数据值条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，对于一个组件类型级平台完整性评估策略条目，EPS 依据该组件类型级平台完整性评估策略条目中的组件产品级汇聚平台完整性评估策略生成该组件类型级平台完整性评估策略条目对应的条目序号、组件类型级平台完整性评估结果、组件类型级平

台修补信息条目、组件类型级错误原因信息条目、组件类型级 Quote 数据值条目和用于下一个平台鉴别过程的组件类型级平台完整性评估策略条目的具体过程如图 66 所示。

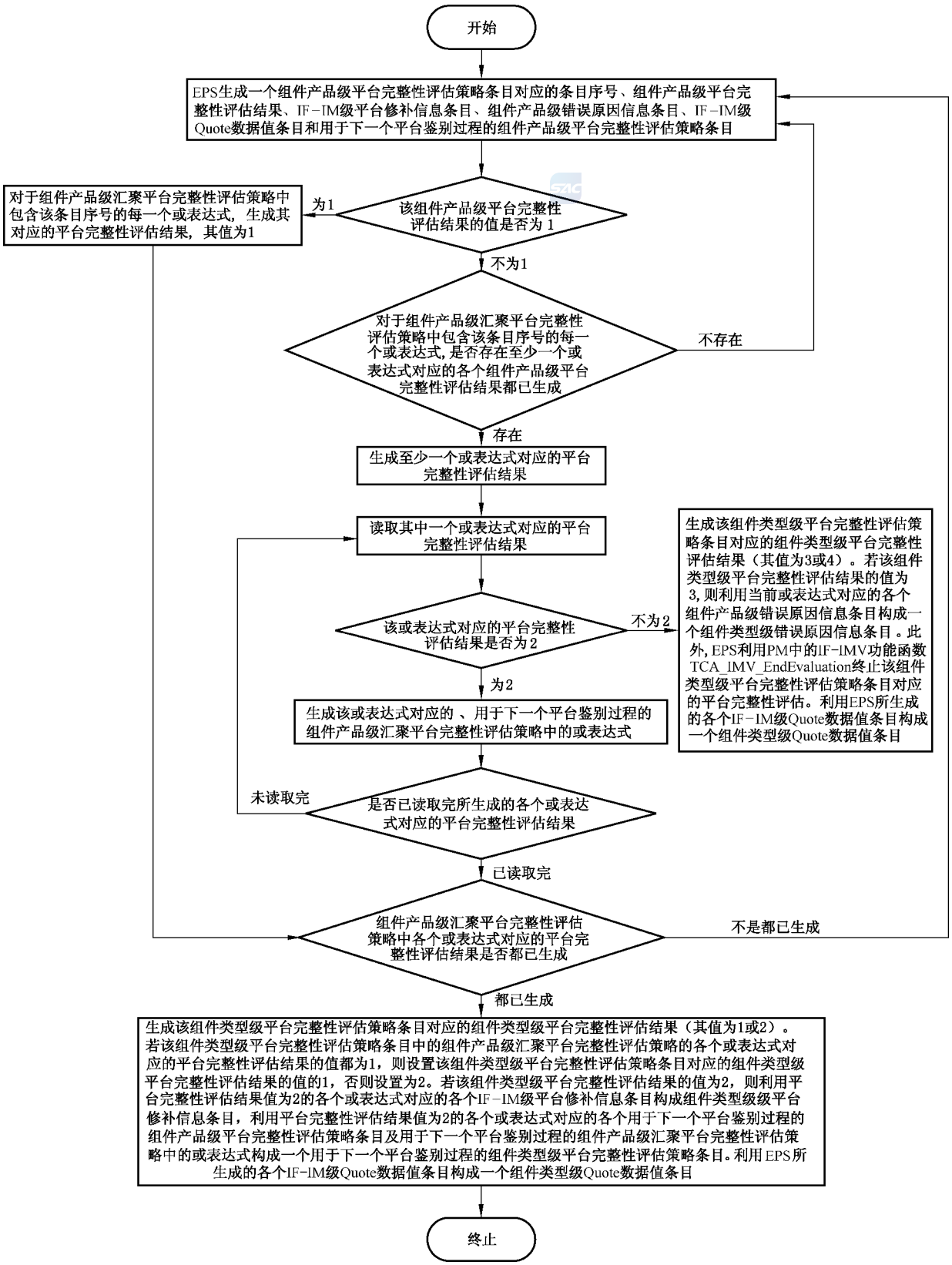

图 66　PAI-1 协议中 EPS 生成组件类型级平台完整性评估结果及其他参数的具体过程

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，对于对 AR 的平台完整性评估策略，EPS 依据对 AR 的平台完整性评估策略中的组件类型级汇聚平台完整性评估策略生成对 AR 的平台完整性评估策略对应的 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略的具体过程如图 67 所示。

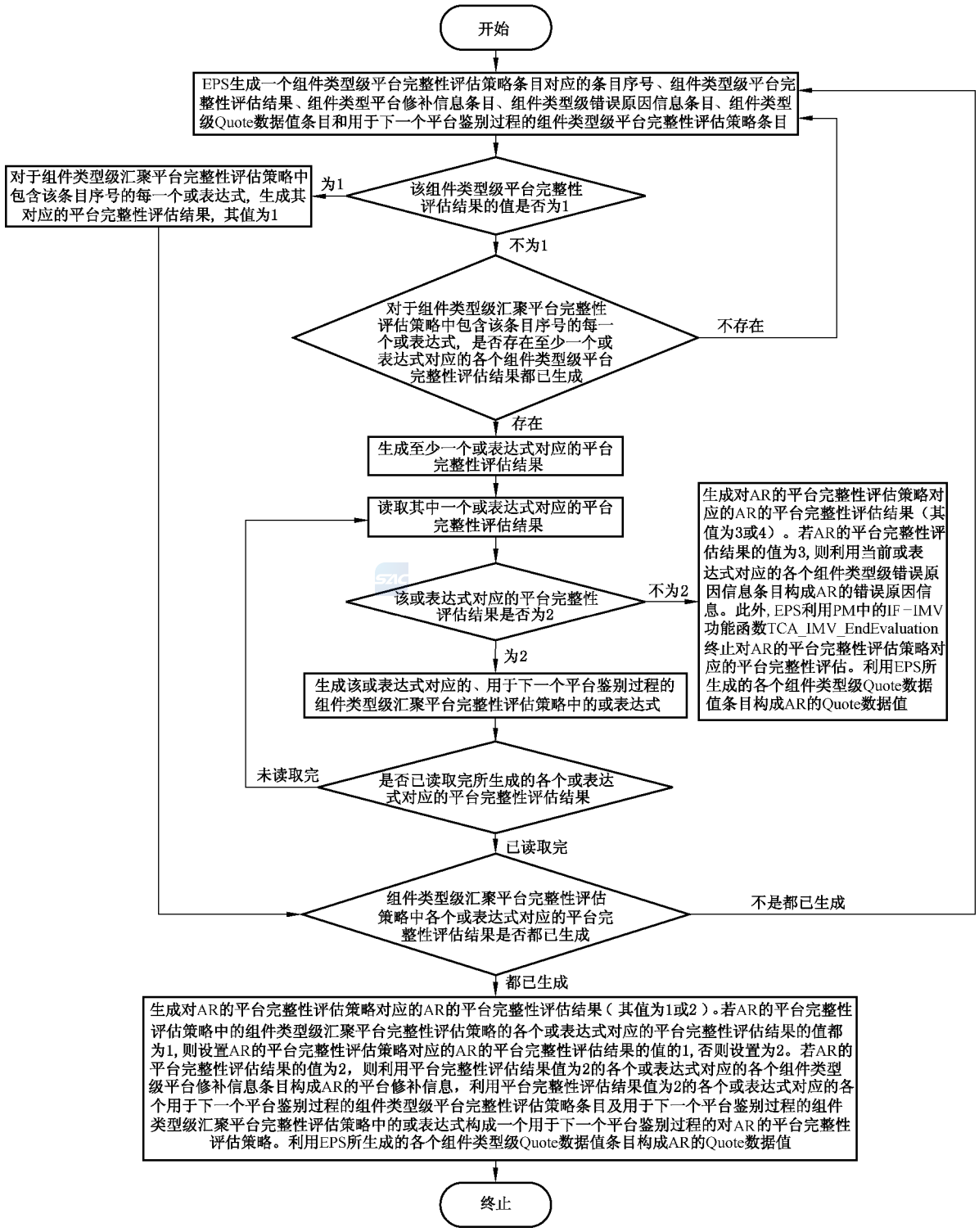

图 67　PAI-1 协议中 EPS 生成 AR 的平台完整性评估结果及其他参数的具体过程

依据 AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略生成 AC 的平台完整性评估结果、AC 的平台修补信息、AC 的错误原因信息、AC 的 Quote 数据值和下一个平台鉴别过程的对 AC 的平台完整性评估策略的过程与依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程完全类同。

在或表达式对应的平台完整性评估结果、组件属性级平台完整性评估结果、组件产品级平台完整性评估结果和组件类型级平台完整性评估结果的汇聚过程中，或运算规则如表 1 所示。

表 1　平台完整性评估结果的或运算规则

或	1	2	3	4
1	1	1	1	1
2	1	2	2	2
3	1	2	3	3
4	1	2	3	4

在或表达式对应的平台完整性评估结果、组件属性级平台完整性评估结果、组件产品级平台完整性评估结果和组件类型级平台完整性评估结果的汇聚过程中，与运算规则如表 2 所示。

表 2　平台完整性评估结果的与运算规则

与	1	2	3	4
1	1	2	3	4
2	2	2	3	4
3	3	3	3	4
4	4	4	4	4

7.2.2.2.1.4　消息 4

消息 4 的数据字段格式如图 68 所示。

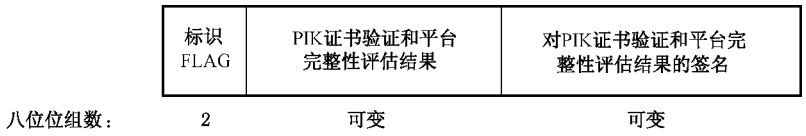

图 68　消息 4 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前。比特 0、2、3、4、6、7、11 和 12 有意义。比特 0、2、3、4、6 和 7 的值分别与消息 3 中比特 0、2、3、4、6 和 7 的值相同。当 PIK 证书验证和平台完整性评估结果字段中包含 AR 的 Quote 数据值时，设置标识 FLAG 字段中比特 11 的值为 1。当 PIK 证书验证和平台完整性评估结果字段中包含 AC 的 Quote 数据值时，设置标识

FLAG 字段中比特 12 的值为 1。

——PIK 证书验证和平台完整性评估结果字段采用 PIK 证书验证和平台完整性评估结果属性表示，其格式定义如前。一次性随机数 1、PIK 证书 1、PIK 证书验证结果 1、平台完整性度量值 1、平台配置保护策略 1、平台完整性评估策略 1、平台完整性评估结果 1、平台修补信息 1、错误原因信息 1、Quote 数据值 1、用于下一个平台鉴别过程的平台完整性评估策略 1、一次性随机数 2、PIK 证书 2、PIK 证书验证结果 2、平台完整性度量值 2、平台配置保护策略 2、平台完整性评估策略 2、平台完整性评估结果 2、平台修补信息 2、错误原因信息 2、Quote 数据值 2、用于下一个平台鉴别过程的平台完整性评估策略 2 分别为 TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的 PIK 证书验证结果、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略、TNCC 挑战、AC 的 PIK 证书、AC 的 PIK 证书验证结果、AC 的平台完整性度量值、AC 的平台配置保护策略、对 AC 的平台完整性评估策略、AC 的平台完整性评估结果、AC 的平台修补信息、AC 错误原因信息、AC 的 Quote 数据值、用于下一个平台鉴别过程的对 AC 的平台完整性评估策略。本字段中的 TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、TNCC 挑战、AC 的 PIK 证书、AC 的平台完整性度量值、AC 的平台配置保护策略、对 AC 的平台完整性评估策略分别与消息 3 中的 TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、TNCC 挑战、AC 的 PIK 证书、AC 的平台完整性度量值、AC 的平台配置保护策略、对 AC 的平台完整性评估策略相同。当标识 FLAG 字段中比特 0 的值为 0 时，TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的 PIK 证书验证结果、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据值、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略不存在。当标识 FLAG 字段中比特 4 的值为 0 时，TNCC 挑战、AC 的 PIK 证书、AC 的 PIK 证书验证结果、AC 的平台完整性度量值、AC 的平台配置保护策略、对 AC 的平台完整性评估策略、AC 的平台完整性评估结果、AC 的平台修补信息、AC 错误原因信息、AC 的 Quote 数据值、用于下一个平台鉴别过程的对 AC 的平台完整性评估策略不存在。当标识 FLAG 字段中比特 2 的值为 0 时，AR 的平台配置保护策略不存在。当标识 FLAG 字段中比特 3 的值都为 0 时，AR 的 PIK 证书和 AR 的 PIK 证书验证结果不存在。当标识 FLAG 字段中比特 6 的值为 0 时，AC 的平台配置保护策略不存在。当标识 FLAG 字段中比特 7 的值都为 0 时，AC 的 PIK 证书和 AC 的 PIK 证书验证结果不存在。当标识 FLAG 字段中比特 11 的值为 0 时，AR 的 Quote 数据值不存在。当标识 FLAG 字段中比特 12 的值为 0 时，AC 的 Quote 数据值不存在。当 AR 的平台完整性评估结果字段的值为 1 时，AR 的平台修补信息、AR 的错误原因信息、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略不存在。当 AR 的平台完整性评估结果字段的值为 2 时，AR 的错误原因信息不存在。当 AR 的平台完整性评估结果字段的值为 3 时，AR 的平台修补信息、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略不存在。当 AR 的平台完整性评估结果字段的值为 4 时，AR 的平台修补信息、AR 的错误原因信息、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略不存在。当 AC 的平台完整性评估结果字段的值为 1 时，AC 的平台修补信息、AC 的错误原因信息、用于下一个平台鉴别过程的对 AC 的平台完整性评估策略不存在。当 AC 的平台完整性评估结果字段的值为 2 时，AC 的错误原因信息不存在。当 AC 的平台完

整性评估结果字段的值为3时，AC的平台修补信息、用于下一个平台鉴别过程的对AC的平台完整性评估策略不存在。当AC的平台完整性评估结果字段的值为4时，AC的平台修补信息、AC的错误原因信息、用于下一个平台鉴别过程的对AC的平台完整性评估策略不存在。若AR和PM之间存在安全通道，则AR的平台修补信息和用于下一个平台鉴别过程的对AC的平台完整性评估策略在该安全通道中传递给AR；否则AR的平台修补信息和用于下一个平台鉴别过程的对AC的平台完整性评估策略可采用数字信封（参见附录C）的方式传递给AR。若AC和PM之间存在安全通道，则AC的平台修补信息和用于下一个平台鉴别过程的对AR的平台完整性评估策略在该安全通道中传递给AC；否则AC的平台修补信息和用于下一个平台鉴别过程的对AR的平台完整性评估策略可采用数字信封（参见附录C）的方式传递给AC。AR和PM之间、AC和PM之间的安全通道可以采取EWAI协议和ETLS协议来建立，具体见6.2.1.3.5和6.2.2.2.4。

——对PIK证书验证和平台完整性评估结果的签名采用签名属性表示，是利用PM的用户证书的私钥生成的签名，定义如前。

当EPS接收到TNCAP发送的消息3时，EPS向TNCAP发送消息4。

TNCAP接收到EPS发送的消息4后，进行如下处理：

a) 检查标识FLAG字段中比特0的值，若值为0，则执行步骤b)；否则执行步骤e)。

b) 检查标识FLAG字段中比特4的值，若值为0，则丢弃消息4；否则：检查PIK证书验证和平台完整性评估结果中的AC的平台完整性评估结果的值，若值为2；则执行步骤c)，否则执行步骤d)。

c) 验证PIK证书验证和平台完整性评估结果及签名（PIK证书验证和平台完整性评估结果中的AC的Quote数据值是TNCAP生成的AC的Quote数据值的子集），若验证不通过，则丢弃消息4；否则利用AC的IF-IMC功能函数TCA_IMC_ReceiveMessage将PIK证书验证和平台完整性评估结果中的AC的平台修补信息发送给TNCAP上端的相应IMC。

d) 依据标识FLAG、TNCC挑战、TNCAP生成的AC的Quote数据值、AC的PIK证书、复合PIK证书验证和平台完整性评估结果构成消息5，并发送给TNCC。

e) 检查标识FLAG字段中比特4的值，若值为0，则执行步骤f)；否则执行步骤n)。

f) 验证PIK证书验证和平台完整性评估结果及签名（PIK证书验证和平台完整性评估结果中的AR的Quote数据值是消息2中的AR的Quote数据值的子集），若验证不通过，则丢弃消息4；否则继续检查AR的PIK证书验证结果和AR的平台完整性评估结果的值，若AR的PIK证书验证结果的值为非0，或者AR的平台完整性评估结果的值为3或4，则首先生成AC的访问决策，其值为禁止（将AC的访问决策通知NAC），并设置标识FLAG字段中比特10的值为1，然后依据标识FLAG、TNCAP挑战和AC的访问决策构成消息5，并发送给TNCC；否则执行步骤g)。

g) 验证TNCAP是否已读取完各个分割部分的对AR的平台完整性评估策略，若TNCAP未读取完各个分割部分的对AR的平台完整性评估策略，则执行步骤h)；否则执行k)。

h) 检查PIK证书验证和平台完整性评估结果中的AR的平台完整性评估结果的值，若值为2，则执行步骤i)；否则执行步骤j)。

i) 设置下一轮PAI协议中的对AR的平台鉴别需求为1和下一轮PAI协议中的对AR的平台完整性评估策略为下一个分割部分的对AR的平台完整性评估策略；首先设置标识FLAG字段中比特13的值为1，然后依据标识FLAG字段、TNCAP挑战、复合PIK证书验证和平台完整性评估结果构成消息5，并发送给TNCC。

j) 设置下一轮 PAI 协议中的对 AR 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AR 的平台完整性评估策略为下一个分割部分的对 AR 的平台完整性评估策略，本轮 PAI 协议完成。

k) 检查 PIK 证书验证和平台完整性评估结果中的 AR 的平台完整性评估结果的值，若值为 2，则执行步骤 l)；否则执行步骤 m)。

l) 依据各轮 PAI 协议中的 AR 的平台完整性评估结果生成该平台鉴别过程的 AR 的平台完整性评估结果(执行与运算而得，值为 1 或 2)；若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 1，则首先生成 AC 的访问决策，其值为允许；若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 2，则首先生成 AC 的访问决策，其值为隔离；将 AC 的访问决策通知 NAC；若 AC 的访问决策为隔离，则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AR 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略为用于下一个平台鉴别过程的对 AR 的平台完整性评估策略中的一个分割部分)，并设置对 AR 的平台鉴别需求的值为 1；首先设置标识 FLAG 字段中比特 10 和 13 的值为 1，然后依据标识 FLAG、TNCAP 挑战、AC 的访问决策、复合 PIK 证书验证和平台完整性评估结果构成消息 5，并发送给 TNCC。

m) 依据各轮 PAI 协议中的 AR 的平台完整性评估结果生成该平台鉴别过程的 AR 的平台完整性评估结果(执行与运算而得，值为 1 或 2)；若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 1，则生成 AC 的访问决策，其值为允许；若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 2，则生成 AC 的访问决策，其值为隔离；将 AC 的访问决策通知 NAC；若 AC 的访问决策为隔离，则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AR 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略为用于下一个平台鉴别过程的对 AR 的平台完整性评估策略中的一个分割部分)，并设置对 AR 的平台鉴别需求的值为 1；首先设置标识 FLAG 字段中比特 10 的值为 1，然后依据标识 FLAG、TNCAP 挑战、AC 的访问决策构成消息 5，并发送给 TNCC。

n) 验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据值是消息 2 中的 AR 的 Quote 数据值的子集，PIK 证书验证和平台完整性评估结果中的 AC 的 Quote 数据值是消息 2 中的 AC 的 Quote 数据值的子集)，若验证不通过，则丢弃消息 4；否则继续检查 AR 的 PIK 证书验证结果和 AR 的平台完整性评估结果的值，若 AR 的 PIK 证书验证结果的值为非 0，或者 AR 的平台完整性评估结果的值为 3 或 4，则首先生成 AC 的访问决策，其值为禁止(将 AC 的访问决策通知 NAC)，并设置标识 FLAG 字段中比特 10 的值为 1，然后依据标识 FLAG、TNCAP 挑战和 AC 的访问决策构成消息 5，并发送给 TNCC；否则执行步骤 o)。

o) 检查 PIK 证书验证和平台完整性评估结果中的 AC 的平台完整性评估结果的值，若值为 2，则执行步骤 p)；否则执行步骤 q)。

p) 利用 AC 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AC 的平台修补信息发送给 TNCAP 上端的相应 IMC。

q) 验证 TNCAP 是否已读取完各个分割部分的对 AR 的平台完整性评估策略，若 TNCAP 未读取完各个分割部分的对 AR 的平台完整性评估策略，则首先设置下一轮 PAI 协议中的对 AR 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AR 的平台完整性评估策略为下一个分割部

分的对 AR 的平台完整性评估策略，然后依据标识 FLAG、TNCC 挑战、TNCAP 生成的 AC 的 Quote 数据值、AC 的 PIK 证书、复合 PIK 证书验证和平台完整性评估结果构成消息 5，并发送给 TNCC；否则：依据各轮 PAI 协议中的 AR 的平台完整性评估结果生成该平台鉴别过程的 AR 的平台完整性评估结果（执行与运算而得，值为 1 或 2）；若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 1，则生成 AC 的访问决策，其值为允许；若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 2，则生成 AC 的访问决策，其值为隔离；将 AC 的访问决策通知 NAC；若 AC 的访问决策为隔离，则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AR 的平台完整性评估策略（每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略为用于下一个平台鉴别过程的对 AR 的平台完整性评估策略中的一个分割部分），并设置对 AR 的平台鉴别需求的值为 1；首先设置标识 FLAG 字段中比特 10 的值为 1，然后依据标识 FLAG、TNCAP 挑战、AC 的访问决策、TNCC 挑战、AC 的 Quote 数据值、AC 的 PIK 证书、复合 PIK 证书验证和平台完整性评估结果构成消息 5，并发送给 TNCC。

7.2.2.2.1.5 消息 5

消息 5 的数据字段格式如图 69 所示。

	标识 FLAG	TNCAP 挑战	AC的访问决策	TNCC 挑战	AC的平台鉴别错误指示	AC的 Quote数据值	AC的PIK 证书	复合PIK证书验证和平台完整性评估结果
八位位组数：	2	32	1	32	1	可变	可变	可变

图 69 消息 5 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前。比特 0、2、3、4、5、6、7、10 和 12 有意义。比特 0、2、3、4、6、7 和 12 的值分别与消息 4 中比特 0、2、3、4、6、7 和 12 的值相同。

——TNCAP 挑战字段长度为 32 个八位位组，定义如前。TNCAP 挑战字段的值与消息 1 中 TNCAP 挑战字段的值相同。

——AC 的访问决策字段长度为 1 个八位位组，其值为允许、隔离或禁止。当标识 FLAG 字段中比特 10 的值为 1 时，本字段存在。

——TNCC 挑战字段长度为 32 个八位位组，定义如前。TNCC 挑战字段的值与消息 2 中 TNCC 挑战字段的值相同。

——AC 的平台鉴别错误指示字段长度为 1 个八位位组。当标识 FLAG 字段中比特 5 的值为 1 时，本字段存在。AC 的平台鉴别错误指示字段的值如下：

1 不可跳过错误；

其他值保留。

——AC 的 Quote 数据值字段长度可变，其值为 TNCAP 生成的 AC 的 Quote 数据值。当标识 FLAG 字段中比特 12 的值为 1 时，本字段存在。

——AC 的 PIK 证书字段长度为可变，定义如前。当标识 FLAG 字段中比特 7 的值的 1 时，本字段存在。

——复合 PIK 证书验证和平台完整性评估结果字段长度为可变，其内容为消息 4 中除标识 FLAG

字段的其他字段。

当 TNCAP 接收到 EPS 发送的消息 4 时，TNCAP 向 TNCC 发送消息 5。

TNCC 接收到 TNCAP 发送的消息 5 后，进行如下处理：

a) 检查标识 FLAG 字段中比特 0 的值，若值为 0，则执行步骤 b)；否则执行步骤 e)。

b) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则丢弃消息 5；否则检查标识 FLAG 字段中比特 5 的值，若值为 1 且 AC 的平台鉴别错误指示的值为 1，则 TNCC 首先生成 AR 的访问决策，其值为禁止(将 AR 的访问决策通知 NAR)，并设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP；否则执行步骤 c)。

c) 验证 AC 的 Quote 数据值中的各个 PIK 签名(当标识 FLAG 字段中比特 12 的值为 1 时才需要验证 AC 的 Quote 数据值中的各个 PIK 签名)，若验证不通过，则丢弃消息 5；否则验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AC 的 Quote 数据值是消息 5 中的 AC 的 Quote 数据值的子集)，若验证不通过，则丢弃消息 5；否则继续检查 AC 的 PIK 证书验证结果和 AC 的平台完整性评估结果的值，若 AC 的 PIK 证书验证结果的值为非 0，或者 AC 的平台完整性评估结果的值为 3 或 4，则首先生成 AR 的访问决策，其值为禁止(将 AR 的访问决策通知 NAR)，并设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP；否则执行步骤 d)。

d) 验证 TNCC 是否已读取完各个分割部分的对 AC 的平台完整性评估策略，若 TNCC 未读取完各个分割部分的对 AC 的平台完整性评估策略，则设置下一轮 PAI 协议中的对 AC 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AC 的平台完整性评估策略为下一个分割部分的对 AC 的平台完整性评估策略，本轮 PAI 协议完成；否则：依据各轮 PAI 协议中的 AC 的平台完整性评估结果生成该平台鉴别过程的 AC 的平台完整性评估结果(执行与运算而得，值为 1 或 2)；若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 1，则生成 AR 的访问决策，其值为允许；若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 2，则首先生成 AR 的访问决策，其值为隔离；将 AR 的访问决策通知 NAR；若 AR 的访问决策为隔离，则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AC 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略为用于下一个平台鉴别过程的对 AC 的平台完整性评估策略中的一个分割部分)，并设置对 AC 的平台鉴别需求的值为 1；首先设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP。

e) 检查标识 FLAG 字段中比特 10 的值，若值为 0，则执行步骤 f)；否则执行步骤 m)。

f) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则执行步骤 g)；否则执行步骤 h)。

g) 检查标识 FLAG 字段比特 13 的值，若值为 0，则丢弃消息 5；否则：验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据值是 TNCC 生成的 AR 的 Quote 数据值的子集)，若验证不通过，则丢弃消息 5；否则利用 AR 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AR 的平台修补信息发送给 TNCC 上端的相应 IMC，本轮 PAI 协议结束。

h) 检查标识 FLAG 字段中比特 5 的值，若值为 1 且 AC 的平台鉴别错误指示的值为 1，则 TNCC 首先生成 AR 的访问决策，其值为禁止(将 AR 的访问决策通知 NAR)，并设置标识 FLAG 字

段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP；否则执行步骤 i）。

i） 验证 AC 的 Quote 数据值中的各个 PIK 签名（当标识 FLAG 字段中比特 12 的值为 1 时才需要验证 AC 的 Quote 数据值中的各个 PIK 签名），若验证不通过，则丢弃消息 5；否则验证 PIK 证书验证和平台完整性评估结果及签名（PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据值是 TNCC 生成的 AR 的 Quote 数据值的子集，PIK 证书验证和平台完整性评估结果中的 AC 的 Quote 数据值是消息 5 中的 AC 的 Quote 数据值的子集），若验证不通过，则丢弃消息 5；否则继续检查 AC 的 PIK 证书验证结果和 AC 的平台完整性评估结果的值，若 AC 的 PIK 证书验证结果的值为非 0，或者 AC 的平台完整性评估结果的值为 3 或 4，则首先生成 AR 的访问决策，其值为禁止（将 AR 的访问决策通知 NAR），并设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP；否则执行步骤 j）。

j） 检查 PIK 证书验证和平台完整性评估结果中的 AR 的平台完整性评估结果的值，若值为 2，则执行步骤 k）；否则执行步骤 l）。

k） 利用 AR 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AR 的平台修补信息发送给 TNCC 上端的相应 IMC。

l） 验证 TNCC 是否已读取完各个分割部分的对 AC 的平台完整性评估策略，若 TNCC 未读取完各个分割部分的对 AC 的平台完整性评估策略，则设置下一轮 PAI 协议中的对 AC 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AC 的平台完整性评估策略为下一个分割部分的对 AC 的平台完整性评估策略，本轮 PAI 协议结束；否则：依据各轮 PAI 协议中的 AC 的平台完整性评估结果生成该平台鉴别过程的 AC 的平台完整性评估结果（执行与运算而得，值为 1 或 2）；若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 1，则生成 AR 的访问决策，其值为允许；若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 2，则生成 AR 的访问决策，其值为隔离；将 AR 的访问决策通知 NAR；若 AR 的访问决策为隔离，则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AC 的平台完整性评估策略（每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略为用于下一个平台鉴别过程的对 AC 的平台完整性评估策略中的一个分割部分），并设置对 AC 的平台鉴别需求的值为 1；首先设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP。

m） 利用 AR 中的 IF-IMC 功能函数 TCA_IMC_NotifyConnectionChange 将 AC 的访问决策通知 TNCC 上端的各个 IMC。若 AC 的访问决策为禁止，则 TNCC 通知 NAR 断开与 AC 的连接；否则执行步骤 n）。

n） 检查标识 FLAG 字段中比特 4 的值，若值为 0，则执行步骤 o）；否则执行步骤 p）。

o） 检查标识 FLAG 字段比特 13 的值，若值为 0，本轮 PAI 协议结束；否则：验证 PIK 证书验证和平台完整性评估结果及签名（PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据值是 TNCC 生成的 AR 的 Quote 数据值的子集），若验证不通过，则丢弃消息 5；否则利用 AR 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AR 的平台修补信息发送给 TNCC 上端的相应 IMC，本轮 PAI 协议结束。

p） 验证 AC 的 Quote 数据值中的各个 PIK 签名（当标识 FLAG 字段中比特 12 的值为 1 时才需要验证 AC 的 Quote 数据值中的各个 PIK 签名），若验证不通过，则丢弃消息 5；否则验证 PIK

证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据值是 TNCC 生成的 AR 的 Quote 数据值的子集,PIK 证书验证和平台完整性评估结果中的 AC 的 Quote 数据值是消息 5 中的 AC 的 Quote 数据值的子集),若验证不通过,则丢弃消息 5;否则继续检查 AC 的 PIK 证书验证结果和 AC 的平台完整性评估结果的值,若 AC 的 PIK 证书验证结果的值为非 0,或者 AC 的平台完整性评估结果的值为 3 或 4,则首先生成 AR 的访问决策,其值为禁止(将 AR 的访问决策通知 NAR),并设置标识 FLAG 字段中比特 9 的值为 1,然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6,并发送给 TNCAP;否则执行步骤 q)。

q) 检查 PIK 证书验证和平台完整性评估结果中的 AR 的平台完整性评估结果的值,若值为 2,则执行步骤 r);否则执行步骤 s)。

r) 利用 AR 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AR 的平台修补信息发送给 TNCC 上端的相应 IMC。

s) 验证 TNCC 是否已读取完各个分割部分的对 AC 的平台完整性评估策略,若 TNCC 未读取完各个分割部分的对 AC 的平台完整性评估策略,则设置下一轮 PAI 协议中的对 AC 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AC 的平台完整性评估策略为下一个分割部分的对 AC 的平台完整性评估策略,本轮 PAI 协议结束;否则:依据各轮 PAI 协议中的 AC 的平台完整性评估结果生成该平台鉴别过程的 AC 的平台完整性评估结果(执行与运算而得,值为 1 或 2);若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 1,则生成 AR 的访问决策,其值为允许;若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 2,则生成 AR 的访问决策,其值为隔离;将 AR 的访问决策通知 NAR;若 AR 的访问决策为隔离,则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AC 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略为用于下一个平台鉴别过程的对 AC 的平台完整性评估策略中的一个分割部分),并设置对 AC 的平台鉴别需求的值为 1;首先设置标识 FLAG 字段中比特 9 的值为 1,然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6,并发送给 TNCAP。

7.2.2.2.1.6 消息 6

消息 6 的数据字段格式如图 70 所示。

	标识FLAG	TNCC挑战	AR的访问决策
八位位组数:	2	32	1

图 70 消息 6 的数据字段格式

其中:

——标识 FLAG 字段长度为 2 个八位位组,定义如前。比特 4 和 9 有意义。比特 4 的值与消息 5 中比特 4 的值相同。

——TNCC 挑战字段长度为 32 个八位位组,定义如前。TNCC 挑战字段的值与消息 2 中的 TNCC 挑战字段的值相同。

——AR 的访问决策字段长度为 1 个八位位组,定义如前。

TNCAP 接收到 TNCC 发送的消息 6 后,进行如下处理:

a) 检查标识 FLAG 字段中比特 4 的值,若值为 0,则丢弃消息 6;否则执行步骤 b)。

b) 检查标识 FLAG 字段中比特 9 的值,若值为 0,则丢弃消息 6;否则执行步骤 c)。

c) 利用 AC 中的 IF-IMC 功能函数 TCA_IMC_NotifyConnectionChange 将 AR 的访问决策通知 TNCAP 上端的各个 IMC。若 AR 的访问决策为禁止，则 TNCAP 通知 NAC 断开与 AR 的连接。

7.2.2.2.2 PAI-2 协议

7.2.2.2.2.1 消息 1

消息 1 的数据字段格式如图 71 所示。

	标识FLAG	TNCAP挑战	对AR的平台完整性度量请求参数
八位位组数：	2	32	可变

图 71 消息 1 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前，比特 0 有意义。比特 0 的值是 TNCAP 依据本轮 PAI 协议中的对 AR 的平台鉴别需求来设置的。在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台鉴别需求为 TNCAP 初始配置的对 AR 的平台鉴别需求；当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台鉴别需求为上一个平台鉴别过程中 TNCAP 设置的用于下一个平台鉴别过程的对 AR 的平台鉴别需求；当本轮 PAI 协议为非首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台鉴别需求为上一轮 PAI 协议中 TNCAP 设置的用于下一轮 PAI 协议的对 AR 的平台鉴别需求。

——TNCAP 挑战字段长度为 32 个八位位组，其值由 TNCAP 采用随机数生成算法生成。当标识 FLAG 字段中比特 0 的值为 0 时，TNCAP 挑战字段不存在。

——对 AR 的平台完整性度量请求参数字段长度为可变，定义如前。当标识 FLAG 字段中比特 0 的值为 0 时，对 AR 的平台完整性度量请求参数字段不存在。对 AR 的平台完整性度量请求参数字段的值是 TNCAP 依据本轮 PAI 协议中的对 AR 的平台完整性评估策略生成的，其中平台完整性评估策略的定义如前。在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台完整性评估策略为 TNCAP 初始配置的对 AR 的平台完整性评估策略或 TNCAP 初始配置的对 AR 的平台完整性评估策略的第一分割部分；当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台完整性评估策略为上一个平台鉴别过程中 TNCAP 设置的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略或上一个平台鉴别过程中 TNCAP 设置的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略的第一分割部分；当本轮 PAI 协议为非首轮 PAI 协议时，本轮 PAI 协议中的对 AR 的平台完整性评估策略为上一轮 PAI 协议中 TNCAP 设置的用于下一轮 PAI 协议的对 AR 的平台完整性评估策略。TNCAP 初始配置的对 AR 的平台完整性评估策略的分割方法见 7.2.2.1.2 中的 c)。

在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，TNCAP 收到 NAC 发送的平台鉴别请求后向 TNCC 发送消息 1。当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，若本平台鉴别过程是一个双向平台鉴别过程，则 TNCAP 在 AC 完成平台修补且等待一个最大平台修补时间后向 TNCC 发送消息 1；若本平台鉴别过程是一个对 AR 的单向平台鉴别过程，则 TNCAP 在等待一个最大平台修补时间后向 TNCC 发送消息 1；若本平台鉴别过程是一个对 AC

的平台鉴别过程，则 TNCAP 在 AC 完成平台修补后向 TNCC 发送消息 1。当本轮 PAI 协议为非首轮 PAI 协议时，TNCAP 在本轮 PAI 协议所在的平台鉴别过程还未完成时向 TNCC 发送消息 1。值得注意的是：当本轮 PAI 协议为非首个平台鉴别过程中的一轮 PAI 协议时，若 TNCAP 收到 AR 的平台鉴别错误指示为 2，则 TNCAP 等待一个最大平台修补时间后向 TNCC 发送消息 1。最大平台修补时间不在本标准中规定。消息 1 的生成步骤如下：

a) 若本轮 PAI 协议中的对 AR 的平台鉴别需求的值为 1，即表示 TNCAP 需要对 AR 进行平台鉴别，则 TNCAP 设置标识 FLAG 字段中比特 0 的值为 1。若本轮 PAI 协议中的对 AR 的平台鉴别需求的值为 0，即表示 TNCAP 不需要对 AR 进行平台鉴别，则 TNCAP 设置标识 FLAG 字段中比特 0 的值为 0。若标识 FLAG 字段中的比特 0 的值为 0，则 TNCAP 执行步骤 b)；否则执行步骤 c)。

b) 根据标识 FLAG 构成消息 1，并发送给 TNCC。

c) 首先生成 TNCAP 挑战，然后依据本轮 PAI 协议中的对 AR 的平台完整性评估策略生成对 AR 的平台完整性度量请求参数，最后根据标识 FLAG、TNCAP 挑战和对 AR 的平台完整性度量请求参数构成消息 1，并发送给 TNCC。

在依据本轮 PAI 协议中的对 AR 的平台完整性评估策略生成对 AR 的平台完整性度量请求参数的过程中，本轮 PAI 协议中的对 AR 的平台完整性评估策略中的一个组件类型级平台完整性评估策略条目生成对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目，其中该组件类型级平台完整性度量请求参数条目中的消息类型与该组件类型级平台完整性评估策略条目中的消息类型相同，该组件类型级平台完整性度量请求参数条目中的一个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型与该组件类型级平台完整性评估策略条目中的一个或多个组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型相同。若该组件类型级平台完整性评估策略条目所对应的条目序号在本轮 PAI 协议中的对 AR 的平台完整性评估策略中的组件类型级汇聚平台完整性评估策略中是一个单元素或表达式，则该组件类型级平台完整性度量请求参数条目中的 FLAG 字段中比特 0 的值为 1，表示该组件类型级平台完整性度量请求参数条目是不可跳过的。

TNCC 接收到 TNCAP 发送的消息 1 后，进行如下处理：

a) 检查标识 FLAG 字段中的比特 0 的值，若比特 0 的值为 0，执行步骤 b)；否则执行步骤 c)。

b) 若本轮 PAI 协议中的对 AC 的平台鉴别需求的值为 0，即表示 TNCC 不需要对 AC 进行平台鉴别，则 TNCC 丢弃消息 1；否则：设置标识 FLAG 字段中的比特 4 的值为 1；若本轮 PAI 协为首个平台鉴别过程中的首轮 PAI 协议且 TNCC 需要验证 AC 的 PIK 证书的有效性，则设置标识 FLAG 字段中的比特 8 的值为 1；生成 TNCC 挑战；依据本轮 PAI 协议中的对 AC 的平台完整性评估策略生成对 AC 的平台完整性度量请求参数；根据标识 FLAG、TNCC 挑战、对 AC 的平台完整性度量请求参数和本轮 PAI 协议中的对 AC 的平台完整性评估策略构成消息 2，并发送给 TNCAP。

c) 若本轮 PAI 协议是非首个平台鉴别过程中的 PAI 协议，且 AR 的平台修补未完成，则 TNCC 首先设置标识 FLAG 字段中比特 1 的值为 1 和 AR 的平台鉴别错误指示为 2，并设置本轮 PAI 协议中的对 AC 的平台鉴别需求和对 AC 的平台完整性评估策略分别为用于下一轮 PAI 协议的对 AC 的平台鉴别需求和对 AC 的平台完整性评估策略，然后根据标识 FLAG、TNCAP 挑战和 AR 的平台鉴别错误指示构造消息 2，并发送给 TNCAP；否则执行步骤 d)。

d) 若本轮 PAI 协议是首个平台鉴别过程中的 PAI 协议，则首先依据 TNCC 上端的各个 IMC 支持的消息类型检查对 AR 的平台完整性度量请求参数，若不支持对 AR 的平台完整性度量请

求参数中不可跳过的组件类型级平台完整性度量请求参数条目(即不可跳过的组件类型级平台完整性度量请求参数条目中的消息类型不包含在 TNCC 上端的各个 IMC 支持的消息类型中),则设置标识 FLAG 字段中比特 1 的值为 1 和 AR 的平台鉴别错误指示为 1,然后根据标识 FLAG、TNCAP 挑战和 AR 的平台鉴别错误指示构造消息 2,并发送给 TNCAP;否则执行步骤 e)。

e) 若本轮 PAI 协议中的对 AC 的平台鉴别需求的值为 1,即表示 TNCC 需要对 AC 进行平台鉴别,则 TNCC 设置标识 FLAG 字段中比特 4 的值为 1。若本轮 PAI 协议中的对 AC 的平台鉴别需求的值为 0,即表示 TNCC 不需要对 AC 进行平台鉴别,则 TNCC 设置标识 FLAG 字段中比特 4 的值为 0。若标识 FLAG 字段中比特 4 的值为 0,则执行步骤 f);否则执行步骤 g)。

f) 依据 TNCAP 挑战、对 AR 的平台完整性度量请求参数生成 AR 的平台完整性度量值、AR 的 Quote 数据,并在生成 AR 的 Quote 数据时设置标识 FLAG 字段中比特 11 的值为 1;若 TNCC 需要对 AR 的平台配置进行保护,则依据对 AR 的平台完整性度量请求参数和 TNCC 初始配置的 AR 的平台配置保护策略生成 AR 的平台配置保护策略,并在生成 AR 的平台配置保护策略时设置标识 FLAG 字段中比特 2 的值为 1;当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时,依据本地创建的 ConnectionID 获取 AR 的 PIK 证书,并设置标识 FLAG 字段中比特 3 的值为 1;依据标识 FLAG、TNCAP 挑战、AR 的平台完整性度量值、AR 的 Quote 数据、AR 的平台配置保护策略和 AR 的 PIK 证书构成消息 2,并发送给 TNCAP。

g) 依据 TNCAP 挑战、对 AR 的平台完整性度量请求参数生成 AR 的平台完整性度量值、AR 的 Quote 数据,并在生成 AR 的 Quote 数据时设置标识 FLAG 字段中比特 11 的值为 1;若 TNCC 需要对 AR 的平台配置进行保护,则依据对 AR 的平台完整性度量请求参数和 TNCC 初始配置的 AR 的平台配置保护策略生成 AR 的平台配置保护策略,并在生成 AR 的平台配置保护策略时设置标识 FLAG 字段中比特 2 的值为 1;当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时,依据本地创建的 ConnectionID 获取 AR 的 PIK 证书,并设置标识 FLAG 字段中比特 3 的值为 1;若本轮 PAI 协为首个平台鉴别过程中的首轮 PAI 协议且 TNCC 需要验证 AC 的 PIK 证书的有效性,则设置标识 FLAG 字段中的比特 8 的值为 1;生成 TNCC 挑战;依据本轮 PAI 协议中的对 AC 的平台完整性评估策略生成对 AC 的平台完整性度量请求参数;依据标识 FLAG、TNCAP 挑战、AR 的平台完整性度量值、AR 的 Quote 数据、AR 的平台配置保护策略、AR 的 PIK 证书、TNCC 挑战、对 AC 的平台完整性度量请求参数和本轮 PAI 协议中的对 AC 的平台完整性评估策略构成消息 2,并发送给 TNCAP。

在依据本轮 PAI 协议中的对 AC 的平台完整性评估策略生成对 AC 的平台完整性度量请求参数的过程中,本轮 PAI 协议中的对 AC 的平台完整性评估策略中的一个组件类型级平台完整性评估策略条目生成对 AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目,其中该组件类型级平台完整性度量请求参数条目中的消息类型与该组件类型级平台完整性评估策略条目中的消息类型相同,该组件类型级平台完整性度量请求参数条目中的一个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型与该组件类型级平台完整性评估策略条目中的一个或多个组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型相同。若该组件类型级平台完整性评估策略条目所对应的条目序号在本轮 PAI 协议中的对 AC 的平台完整性评估策略中的组件类型级汇聚平台完整性评估策略中是一个单元素或表达式,则该组件类型级平台完整性度量请求参数条目中的 FLAG 字段中比特 0 的值为 1,表示该组件类型级平台完整性度量请求参数条目是不可跳过的。

在依据 TNCAP 挑战、对 AR 的平台完整性度量请求参数生成 AR 的平台完整性度量值、AR 的

Quote 数据的过程中，对于对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目，若该组件类型级平台完整性度量请求参数条目不为 TNCC 上端的任意一个 IMC 所支持，则生成一个组件类型级平台完整性度量值条目，其状态码的值设置为 2；否则利用 AR 中的 IF-IMC 功能函数 TCA_IMC_RequestMeasurementInfo 将该组件类型级平台完整性度量请求参数条目中的各个组件属性级平台完整性度量请求参数条目发送给 TNCC 上端的相应 IMC。当 TNCC 上端的一个 IMC 收到一个组件类型级平台完整性度量请求参数条目中的各个组件属性级平台完整性度量请求参数条目时，该 IMC 首先各个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型执行平台完整性度量（具体度量过程不在本标准中规定），并生成一个 IF-IM 消息和一个完整性报告索引信息（当该 IF-IM 消息中包含完整性报告索引信息时该完整性报告索引信息才被生成），然后利用 AR 中的 IF-IMC 功能函数 TCA_TNCC_SendMessage 将该 IF-IM 消息发送给 TNCC，并利用 AR 中的 IF-IMC 功能函数 TCA_TNCC_ProvideReportIndex 将该完整性报告索引信息发送给 TNCC（不管是否生成该 IF-IM 消息对应的完整性报告索引信息，本功能函数都必须执行）。当从 TNCC 上端的一个 IMC 收到一个完整性报告索引信息时，若对 AR 的平台完整性度量请求参数对应的所有完整性报告索引信息都已收到，则利用 TNCAP 挑战和这些完整性报告索引信息生成 AR 的完整性报告和该完整性报告对应的 Quote 数据（具体生成方法不在本标准中规定），其中该完整性报告对应的 Quote 数据即为 AR 的 Quote 数据。当从 TNCC 上端的一个 IMC 收到一个 IF-IM 消息时，TNCC 依据该 IF-IM 消息生成一个 IF-IM 级平台完整性度量值条目，若对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目对应的所有 IF-IM 消息都已收到，则利用该组件类型级平台完整性度量请求参数条目对应的各个 IF-IM 级平台完整性度量值条目生成一个组件类型级平台完整性度量值条目，若对 AR 的平台完整性度量请求参数对应的所有 IF-IM 消息都已收到，则利用对 AR 的平台完整性度量请求参数对应的各个组件类型级平台完整性度量值条目和 AR 的完整性报告生成 AR 的平台完整性度量值。

在依据对 AR 的平台完整性度量请求参数和 TNCC 初始配置的 AR 的平台配置保护策略生成 AR 的平台配置保护策略的过程中，对 AR 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目生成 AR 的平台配置保护策略中的零个或一个组件类型级平台配置保护策略条目，其中该组件类型级平台配置保护策略条目中的消息类型与该组件类型级平台完整性度量请求参数条目中的消息类型相同，该组件类型级平台配置保护策略条目中的一个或多个组件属性级平台配置保护策略条目中的组件属性类型厂家 ID 及组件属性类型与该组件类型级平台完整性度量请求参数条目中的一个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型相同。当在 TNCC 预配置的 AR 的平台配置保护策略中找不到该组件类型级平台完整性度量请求参数条目中的消息类型时，TNCC 不能生成该组件类型级平台完整性度量请求参数条目对应的组件类型级平台配置保护策略条目。当在 TNCC 预配置的 AR 的平台配置保护策略中找不到该组件类型级平台完整性度量请求参数条目中的任意组件属性类型厂家 ID 及组件属性类型时，TNCC 不能生成该组件类型级平台完整性度量请求参数条目对应的组件类型级平台配置保护策略条目。

对于一个消息类型，TNCC 上端的一个 IMC 可以支持该消息类型下的多个组件产品的平台完整性度量，但是 TNCC 上端的多个 IMC 不可以支持该消息类型下的同一个组件产品的平台完整性度量。

7.2.2.2.2.2 消息 2

消息 2 的数据字段格式如图 72 所示。

	标识 FLAG	TNCAP 挑战	AR的平台鉴别错误指示	AR的平台完整性度量值	AR的 Quote 数据	AR的平台配置保护策略	AR的 PIK 证书	TNCC 挑战	对AC的平台完整性度量请求参数	对AC的平台完整性评估策略
八位位组数：	2	32	1	可变	可变	可变	可变	32	可变	可变

图 72　消息 2 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前。比特 0、1、2、3、4、8 和 11 有意义。比特 0 的值与消息 1 中标识 FLAG 字段中的比特 0 的值相同。比特 4 的值是 TNCC 依据本轮 PAI 协议中的对 AC 的平台鉴别需求来设置的。在一次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台鉴别需求为 TNCC 初始配置的对 AC 的平台鉴别需求；当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台鉴别需求为上一个平台鉴别过程中 TNCC 设置的用于下一个平台鉴别过程的对 AC 的平台鉴别需求；当本轮 PAI 协议为非首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台鉴别需求为上一轮 PAI 协议中 TNCC 设置的用于下一轮 PAI 协议的对 AC 的平台鉴别需求。

——TNCAP 挑战字段长度为 32 个八位位组，其值与消息 1 中的 TNCAP 挑战相同。当标识 FLAG 字段中比特 0 的值为 0 时，TNCAP 挑战字段不存在。

——AR 的平台鉴别错误指示字段长度为 1 个八位位组。当标识 FLAG 字段中比特 1 的值为 0 时，AR 的平台鉴别错误指示字段不存在。AR 的平台鉴别错误指示字段的值如下：

1　发生不可跳过错误；

2　平台修补未完成；

其他值保留。

——AR 的平台完整性度量值字段长度为可变，定义如前。若 AR 和 PM 之间存在安全通道，则 AR 的平台完整性度量值在安全通道中传递给 PM；否则 AR 的平台完整性度量值可采用数字信封（参见附录 C）的方式传递给 PM。AR 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。

——AR 的 Quote 数据字段长度为可变，定义如前。当标识 FLAG 字段中比特 11 的值为 0 时，AR 的 Quote 数据字段不存在。

——AR 的平台配置保护策略字段长度为可变，定义如前。当标识 FLAG 字段中比特 2 的值为 0 时，AR 的平台配置保护策略字段不存在。若 AR 和 PM 之间存在安全通道，则 AR 的平台配置保护策略在安全通道中传递给 PM；否则 AR 的平台配置保护策略可采用数字信封（参见附录 C）的方式传递给 PM。AR 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。

——AR 的 PIK 证书字段长度为可变，其定义不在本标准中规定。当标识 FLAG 字段中比特 3 的值为 0 时，AR 的 PIK 证书字段不存在。

——TNCC 挑战字段长度为 32 个八位位组，由 TNCC 采用随机数生成算法生成。当 FLAG 标识字段的比特 4 的值为 0 时，本字段不存在。

——对 AC 的完整性度量请求参数字段为可变长度，定义如前。当 FLAG 标识字段的比特 4 的值为 0 时，本字段不存在。对 AC 的平台完整性度量请求参数字段的值是 TNCC 依据本轮 PAI 协议中的对 AC 的平台完整性评估策略生成的，其中平台完整性评估策略的定义如前。在一

次可信网络连接过程中，当本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台完整性评估策略为 TNCC 初始配置的对 AC 的平台完整性评估策略或 TNCC 初始配置的对 AC 的平台完整性评估策略的第一分割部分；当本轮 PAI 协议为非首个平台鉴别过程中的首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台完整性评估策略为上一个平台鉴别过程中 TNCC 设置的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略或上一个平台鉴别过程中 TNCC 设置的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略的第一分割部分；当本轮 PAI 协议为非首轮 PAI 协议时，本轮 PAI 协议中的对 AC 的平台完整性评估策略为上一轮 PAI 协议中 TNCC 设置的用于一轮 PAI 协议的对 AC 的平台完整性评估策略。TNCC 初始配置的对 AC 的平台完整性评估策略的分割方法见 7.2.2.1.2 中的 c)。

——对 AC 的平台完整性评估策略字段长度为可变，定义如前。当 FLAG 标识字段的比特 4 的值为 0 时，本字段不存在。若 AR 和 PM 之间存在安全通道，则 AR 的完整性评估策略在安全通道中传递给 PM；否则 AR 的完整性评估策略可采用数字信封（参见附录 C）的方式传递给 PM。AR 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。

当 TNCC 接收到 TNCAP 发送的消息 1，TNCC 向 TNCAP 发送消息 2。

TNCAP 接收到 TNCC 发送的消息 2 后，进行如下处理：

a) 检查标识 FLAG 字段中比特 0 的值，若值为 0，则执行步骤 b)；否则步骤 d)。

b) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则丢弃消息 2；否则执行步骤 c)。

c) 若本轮 PAI 协议为首个平台鉴别过程中的 PAI 协议，则首先依据 TNCAP 上端的各个 IMC 支持的消息类型检查对 AC 的平台完整性度量请求参数，若不支持对 AC 的平台完整性度量请求参数中不可跳过的组件类型级平台完整性度量请求参数条目（即不可跳过的组件类型级平台完整性度量请求参数条目中的消息类型不包含在 TNCAP 上端的各个 IMC 支持的消息类型中），则设置标识 FLAG 字段中比特 5 的值为 1 和 AC 的平台鉴别错误指示字段的值为 1，然后根据标识 FLAG、TNCC 挑战和 AC 的平台鉴别错误指示构造消息 5，并发送给 TNCC，否则：依据 TNCC 挑战、对 AC 的平台完整性度量请求参数生成 AC 的平台完整性度量值、AC 的 Quote 数据；若 TNCAP 需要对 AC 的平台配置进行保护，则依据对 AC 的平台完整性度量请求参数和 TNCAP 初始配置的 AC 的平台配置保护策略生成 AC 的平台配置保护策略，并在生成 AC 的平台配置保护策略后设置标识 FLAG 字段中比特 6 的值为 1；当标识 FLAG 字段中比特 8 的值为 1 时，TNCAP 依据本地创建的 ConnectionID 获取 AC 的 PIK 证书，并设置标识 FLAG 字段中比特 7 的值为 1；依据标识 FLAG、TNCC 挑战、AC 的 PIK 证书、AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略构成消息 3，并发送给 EPS。

d) 检查标识 FLAG 字段中的比特 1 的值，若比特 1 的值为 1，则执行步骤 e)；否则执行步骤 f)。

e) 检查 TNCAP 挑战字段的值，若值与消息 1 中的 TNCAP 挑战字段不相同，则丢弃消息 2；否则继续检查 AR 的平台鉴别错误指示字段的值，若值为 2，则 TNCAP 在等待一个最大平台修补时间后执行下一轮 PAI 协议，并设置用于下一轮 PAI 协议的对 AR 的平台鉴别需求和对 AR 的平台完整性评估策略分别为本轮 PAI 协议中的对 AR 的平台鉴别需求和对 AR 的平台完整性评估策略；若值为 1，则 TNCAP 生成 AC 的访问决策为禁止（将 AC 的访问决策发送给 NAC），并设置标识 FLAG 字段中比特 10 的值为 1，然后依据标识 FLAG、TNCAP 挑战、AC 的访问决策构成消息 5，并发送给 TNCC。

f) 检查 TNCAP 挑战字段的值，若与消息 1 中的 TNCAP 挑战字段不相同，则丢弃消息 2；否则检查标识 FLAG 字段中比特 11 的值，若值为 1，则执行步骤 g)；否则执行步骤 h)。

g) 验证 AR 的 Quote 数据中的 PIK 签名，若验证不通过，则丢弃消息 2；否则执行步骤 h)。

h) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则执行步骤 i)；否则执行步骤 j)。

i) 生成 TNCAP 平台鉴别挑战；若本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议且 TNCAP 需要验证 AR 的 PIK 证书有效性，则设置标识 FLAG 字段中比特 3 的值为 1；依据标识 FLAG、TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略构成消息 3，并发送给 EPS。

j) 若本轮 PAI 协议是首个平台鉴别过程中的 PAI 协议，则首先依据 TNCAP 上端的各个 IMC 支持的消息类型检查对 AC 的平台完整性度量请求参数，若不支持对 AC 的平台完整性度量请求参数中不可跳过的组件类型级平台完整性度量请求参数条目(即不可跳过的组件类型级平台完整性度量请求参数条目中的消息类型不包含在 TNCAP 上端的各个 IMC 支持的消息类型中)，则设置标识 FLAG 字段中比特 5 的值为 1 和 AC 的平台鉴别错误指示的值为 1，然后根据标识 FLAG、TNCC 挑战和 AC 的平台鉴别错误指示构造消息 5，并发送给 TNCC；否则：依据 TNCC 挑战、对 AC 的平台完整性度量请求参数生成 AC 的平台完整性度量值、AC 的 Quote 数据；若 TNCAP 需要对 AC 的平台配置进行保护，则依据对 AC 的平台完整性度量请求参数和 TNCAP 初始配置的 AC 的平台配置保护策略生成 AC 的平台配置保护策略，并在生成 AC 的平台配置保护策略后设置标识 FLAG 字段中比特 6 的值为 1；当标识 FLAG 字段中比特 8 的值为 1 时，TNCAP 依据本地创建的 ConnectionID 获取 AC 的 PIK 证书，并设置标识 FLAG 字段中比特 7 的值为 1；生成 TNCAP 平台鉴别挑战；若本轮 PAI 协议为首个平台鉴别过程中的首轮 PAI 协议且 TNCAP 需要验证 AR 的 PIK 证书有效性，则设置标识 FLAG 字段中比特 3 的值为 1；依据标识 FLAG、TNCAP 平台鉴别挑战、TNCC 挑战、AR 的 PIK 证书、AC 的 PIK 证书、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略构成消息 3，并发送给 EPS。

在依据 TNCC 挑战、对 AC 的平台完整性度量请求参数生成 AC 的平台完整性度量值、AC 的 Quote 数据的过程中，对于对 AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目，若该组件类型级平台完整性度量请求参数条目不为 TNCAP 上端的任意一个 IMC 所支持，则生成一个组件类型级平台完整性度量值条目，其状态码的值设置为 2；否则利用 AC 中的 IF-IMC 功能函数 TCA_IMC_RequestMeasurementInfo 将该组件类型级平台完整性度量请求参数条目中的各个组件属性级平台完整性度量请求参数条目发送给 TNCAP 上端的相应 IMC。当 TNCAP 上端的一个 IMC 收到一个组件类型级平台完整性度量请求参数条目中的各个组件属性级平台完整性度量请求参数条目时，该 IMC 首先依据各个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型执行平台完整性度量(具体度量过程不在本标准中规定)，并生成一个 IF-IM 消息和一个完整性报告索引信息(当该 IF-IM 消息中包含完整性报告索引信息时该完整性报告索引信息才被生成)，然后利用 AC 中的 IF-IMC 功能函数 TCA_TNCAP_SendMessage 将该 IF-IM 消息发送给 TNCAP，并利用 AC 中的 IF-IMC 功能函数 TCA_TNCC_ProvideReportIndex 将该完整性报告索引信息发送给 TNCAP(不管是否生成该 IF-IM 消息对应的完整性报告索引信息，本功能函数都必须执行)。当从 TNCAP 上端的一个 IMC 收到一个完整性报告索引信息时，若对 AC 的平台完整性度量请求参数对应的所有完整性报告索引信息都已收到，则利用 TNCC 挑战和这些完整性报告索引信息生成 AC 的完整性报告和该完整性报告对应的 Quote 数据(具体生成方法不在本标准中规定)，其中该完整性报告对应的 Quote 数据即为 AC 的 Quote 数据。当从 TNCAP 上端的一个 IMC 收到一个 IF-IM 消息时，TNCAP 依据该 IF-IM 消息生成一个 IF-IM 级平台完整性度量值条目，若对 AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目对应的所有 IF-IM 消息都已收到，则利用该组件类型级平台完整性度量请求参数条目对应的各个 IF-IM 级平台完整性度量值条目生成一个组件类型级平台完整性度量值条目，若对 AC 的平台完整性度量请求参数对应的所有 IF-IM 消息都已收到，

则利用对 AC 的平台完整性度量请求参数对应的各个组件类型级平台完整性度量值条目和 AC 的完整性报告生成 AC 的平台完整性度量值。

在依据对 AC 的平台完整性度量请求参数和 TNCAP 初始配置的 AC 的平台配置保护策略生成 AC 的平台配置保护策略的过程中，对 AC 的平台完整性度量请求参数中的一个组件类型级平台完整性度量请求参数条目生成 AC 的平台配置保护策略中的零个或一个组件类型级平台配置保护策略条目，其中该组件类型级平台配置保护策略条目中的消息类型与该组件类型级平台完整性度量请求参数条目中的消息类型相同，该组件类型级平台配置保护策略条目中的一个或多个组件属性级平台配置保护策略条目中的组件属性类型厂家 ID 及组件属性类型与该组件类型级平台完整性度量请求参数条目中的一个组件属性级平台完整性度量请求参数条目中的组件属性类型厂家 ID 及组件属性类型相同。当在 TNCAP 预配置的 AC 的平台配置保护策略中找不到该组件类型级平台完整性度量请求参数条目中的消息类型时，TNCAP 不能生成该组件类型级平台完整性度量请求参数条目对应的组件类型级平台配置保护策略条目。当在 TNCAP 预配置的 AC 的平台配置保护策略中找不到该组件类型级平台完整性度量请求参数条目中的任意组件属性类型厂家 ID 及组件属性类型时，TNCAP 不能生成该组件类型级平台完整性度量请求参数条目对应的组件类型级平台配置保护策略条目。

对于一个消息类型，TNCC 上端的一个 IMC 可以支持该消息类型下的多个组件产品的平台完整性度量，但是 TNCC 上端的多个 IMC 不可以支持该消息类型下的同一个组件产品的平台完整性度量。

7.2.2.2.2.3 消息 3

消息 3 的数据字段格式如图 73 所示。

	标识 FLAG	TNCAP 平台鉴别挑战	TNCC 挑战	AR 的 PIK 证书	AC 的 PIK 证书	AR 的平台完整性度量值	AR 的平台配置保护策略	对AR的平台完整性评估策略	AC的平台完整性度量值	AC的平台配置保护策略	对AC的平台完整性评估策略
八位位组数：	2	32	32	可变	可变	可变	可变	可变	可变	可变	可变

图 73 消息 3 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前。比特 0、2、3、4、6 和 7 有意义。比特 0、2 和 4 的值分别与消息 2 中标识 FLAG 字段中比特 0、2 和 4 的值相同。

——TNCAP 平台鉴别挑战字段长度为 32 个八位位组，由 TNCAP 采用随机数生成算法产生的，用于与 EPS 进行信息交互。当标识 FLAG 字段中比特 0 的值为 0 时，本字段不存在。

——TNCC 挑战字段长度为 32 个八位位组，本字段的值与消息 2 中 TNCC 挑战字段的值相同。当标识 FLAG 字段中比特 4 的值为 0 时，本字段不存在。

——AR 的 PIK 证书字段长度为可变，本字段的值与消息 2 中 AR 的 PIK 证书字段的值相同。当标识 FLAG 字段中比特 3 的值为 0 时，本字段不存在。

——AC 的 PIK 证书字段长度为可变，其定义不在本标准中规定。当标识 FLAG 字段中比特 7 的值为 0 时，本字段不存在。

——AR 的平台完整性度量值字段长度为可变，本字段的值与消息 2 中 AR 的平台完整性度量值字段的值相同。当标识 FLAG 字段中比特 0 的值为 0 时，本字段不存在。

——AR 的平台配置保护策略字段长度为可变，本字段的值与消息 2 中 AR 的平台配置保护策略字段的值相同。当标识 FLAG 字段中比特 2 的值为 0 时，本字段不存在。

——对 AR 的平台完整性评估策略字段长度为可变，定义如前。若 AC 和 PM 之间存在安全通道，则对 AR 的平台完整性评估策略在该安全通道中传递给 PM；否则对 AR 的平台完整性评估

策略可采用数字信封(参见附录 C)的方式传递给 PM。AC 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立,具体见 6.2.1.3.5 和 6.2.2.2.4。当标识 FLAG 字段中比特 0 的值为 0 时,本字段不存在。

——AC 的平台完整性度量值字段长度为可变,定义如前。若 AC 和 PM 之间存在安全通道,则 AC 的平台完整性度量值在该安全通道中传递给 PM;否则 AC 的平台完整性度量值可采用数字信封(参见附录 C)的方式传递给 PM。AC 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立,具体见 6.2.1.3.5 和 6.2.2.2.4。当标识 FLAG 字段中比特 4 的值为 0 时,本字段不存在。

——AC 的平台配置保护策略字段长度为可变,定义如前。当标识 FLAG 字段中比特 6 的值为 0 时,本字段不存在。若 AC 和 PM 之间存在安全通道,则 AC 的平台配置保护策略在该安全通道中传递给 PM;否则 AC 的平台配置保护策略可采用数字信封(参见附录 C)的方式传递给 PM。AC 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立,具体见 6.2.1.3.5 和 6.2.2.2.4。当标识 FLAG 字段中比特 6 的值为 1 时,本字段存在。

——对 AC 的平台完整性评估策略字段长度为可变,本字段的值与消息 2 中对 AC 的平台完整性评估策略字段的值相同。当标识 FLAG 字段中比特 4 的值为 0 时,本字段不存在。

当 TNCAP 接收到 TNCC 发送的消息 2 时,TNCAP 向 EPS 发送消息 3,或向 TNCC 发送消息 5。EPS 接收到 TNCAP 发送的消息 3 后,进行如下处理:

a) 检查标识 FLAG 字段中比特 0 的值,若值为 0,则执行步骤 b);否则执行步骤 d)。

b) 检查标识 FLAG 字段中比特 4 的值,若值为 0,则丢弃消息 3;否则执行步骤 c)。

c) 若标识 FLAG 字段中比特 7 的值为 1,则验证 AC 的 PIK 证书,并生成 AC 的 PIK 证书验证结果;依据 AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略生成 AC 的平台完整性评估结果、AC 的平台修补信息、AC 的错误原因信息、AC 的 Quote 数据和下一个平台鉴别过程的对 AC 的平台完整性评估策略;若生成 AC 的 Quote 数据,则设置标识 FLAG 字段中比特 12 的值为 1;生成 PIK 证书验证和平台完整性评估结果;利用 PM 的用户证书的私钥生成对 PIK 证书验证和平台完整性评估结果的签名;依据标识 FLAG、PIK 证书验证和平台完整性评估结果、对 PIK 证书验证和平台完整性评估结果的签名构成消息 4,并发送给 TNCAP。

d) 检查标识 FLAG 字段中比特 4 的值,若值为 0,则执行步骤 e);否则执行步骤 f)。

e) 若标识 FLAG 字段中比特 3 的值为 1,则验证 AR 的 PIK 证书,并生成 AR 的 PIK 证书验证结果;依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略;若生成 AR 的 Quote 数据,则设置标识 FLAG 字段中比特 11 的值为 1;生成 PIK 证书验证和平台完整性评估结果;利用 PM 的用户证书的私钥生成对 PIK 证书验证和平台完整性评估结果的签名;依据标识 FLAG、PIK 证书验证和平台完整性评估结果、对 PIK 证书验证和平台完整性评估结果的签名构成消息 4,并发送给 TNCAP。

f) 若标识 FLAG 字段中比特 3 的值为 1,则验证 AR 的 PIK 证书,并生成 AR 的 PIK 证书验证结果;依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略;若生成 AR 的 Quote 数据,则设置标识 FLAG 字段中比特 11 的值为 1;若标识 FLAG 字段中比特 7 的值为 1,则验证 AC 的 PIK 证书,并生成 AC 的 PIK 证书验证结果;依据 AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略生成 AC 的平台完整性评估结果、AC 的平台修补信息、AC 的错误原因信息、AC 的 Quote 数据和下一个平台鉴别过程的对 AC 的平台完整性评估策

略；若生成 AC 的 Quote 数据，则设置标识 FLAG 字段中比特 12 的值为 1；生成 PIK 证书验证和平台完整性评估结果；利用 PM 的用户证书的私钥生成对 PIK 证书验证和平台完整性评估结果的签名；依据标识 FLAG、PIK 证书验证和平台完整性评估结果、对 PIK 证书验证和平台完整性评估结果的签名构成消息 4，并发送给 TNCAP。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，若 AR 的平台完整性度量值中不包含一个完整性报告，则验证对 AR 的平台完整性评估策略中的各个组件类型级平台完整性评估策略条目；否则：验证该完整性报告（具体验证方法不在本标准中规定），若验证不通过，则丢弃消息 3；否则首先依据该完整性报告生成 AR 的 Quote 数据，然后验证对 AR 的平台完整性评估策略中的各个组件类型级平台完整性评估策略条目。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，对于对 AR 的平台完整性评估策略中的一个组件类型级平台完整性评估策略条目，若该组件类型级平台完整性评估策略条目中的消息类型不为 EPS 上端的任意一个 IMV 所支持，则生成一个组件类型级平台完整性评估结果（值设置为 3）和一个组件类型级错误原因信息条目（组件类型级错误原因信息码字段的值设置为 1）；否则依据该组件类型级平台完整性评估策略条目中的消息类型从 AR 的平台完整性度量值中读取相应组件类型级平台完整性度量值条目，若该组件类型级平台完整性度量值条目中状态码字段的值为 2，则生成一个组件类型级平台完整性评估结果（值设置为 3）和一个组件类型级错误原因信息条目（组件类型级错误原因信息码字段的值设置为 2）；否则利用 PM 中的 IF-IMV 功能函数 TCA_IMV_RequestEvaluationInfo 将该组件类型级平台完整性评估策略条目中的各个组件产品级平台完整性评估策略条目、该组件类型级平台完整性度量值条目中的各个 IF-IM 级平台完整性度量值条目、AR 的平台配置保护策略中对应该组件类型级平台完整性评估策略条目的组件类型级平台配置保护策略条目中的各个组件产品级平台配置保护策略条目、AR 的平台完整性度量值中的完整性报告发送给 EPS 上端的各个相应 IMV。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，当 EPS 上端的一个 IMV 收到一个组件产品级平台完整性评估策略条目（其组件产品序号为非 0xff 值）及相应条目序号、各个组件产品级平台配置保护策略条目、各个 IF-IM 级平台完整性度量值条目、一个完整性报告时，若该 IMV 不支持该组件产品级平台完整性评估策略条目所对应的组件产品序号及组件产品，则首先生成一个组件产品级平台完整性评估结果（值设置为 3）和一个组件产品级错误原因信息条目（组件产品级错误原因信息码字段的值设置为 1），然后利用 PM 中的 IF-IMV 功能函数 TCA_EPS_ProvideEvaluationResult 将该组件产品级平台完整性评估结果和该组件产品级错误原因信息条目发送给 EPS；否则检查各个 IF-IM 级平台完整性度量值条目和该完整性报告，若找不到该组件产品级平台完整性评估策略条目所对应的组件产品，则生成一个组件产品级平台完整性评估结果（值设置为 3）和一个组件产品级错误原因信息条目（组件产品级错误原因信息码字段的值设置为 3），然后利用 PM 中的 IF-IMV 功能函数 TCA_EPS_Provide-EvaluationResult 将该组件产品级平台完整性评估结果和该组件产品级错误原因信息条目发送给 EPS；否则依据该组件产品级平台完整性评估策略条目中的各个组件属性级平台完整性评估策略条目及组件属性级汇聚平台完整性评估策略、该组件产品级平台完整性评估策略条目对应的 IF-IM 级平台完整性度量值条目和该完整性报告、该组件产品级平台完整性评估策略条目对应的组件产品级平台配置保护策略条目执行平台完整性评估，并生成一个组件产品级平台完整性评估结果、一个 IF-IM 级平台修补信息条目、一个组件产品级错误原因信息条目和一个用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目，其具体过程如图 74 所示。

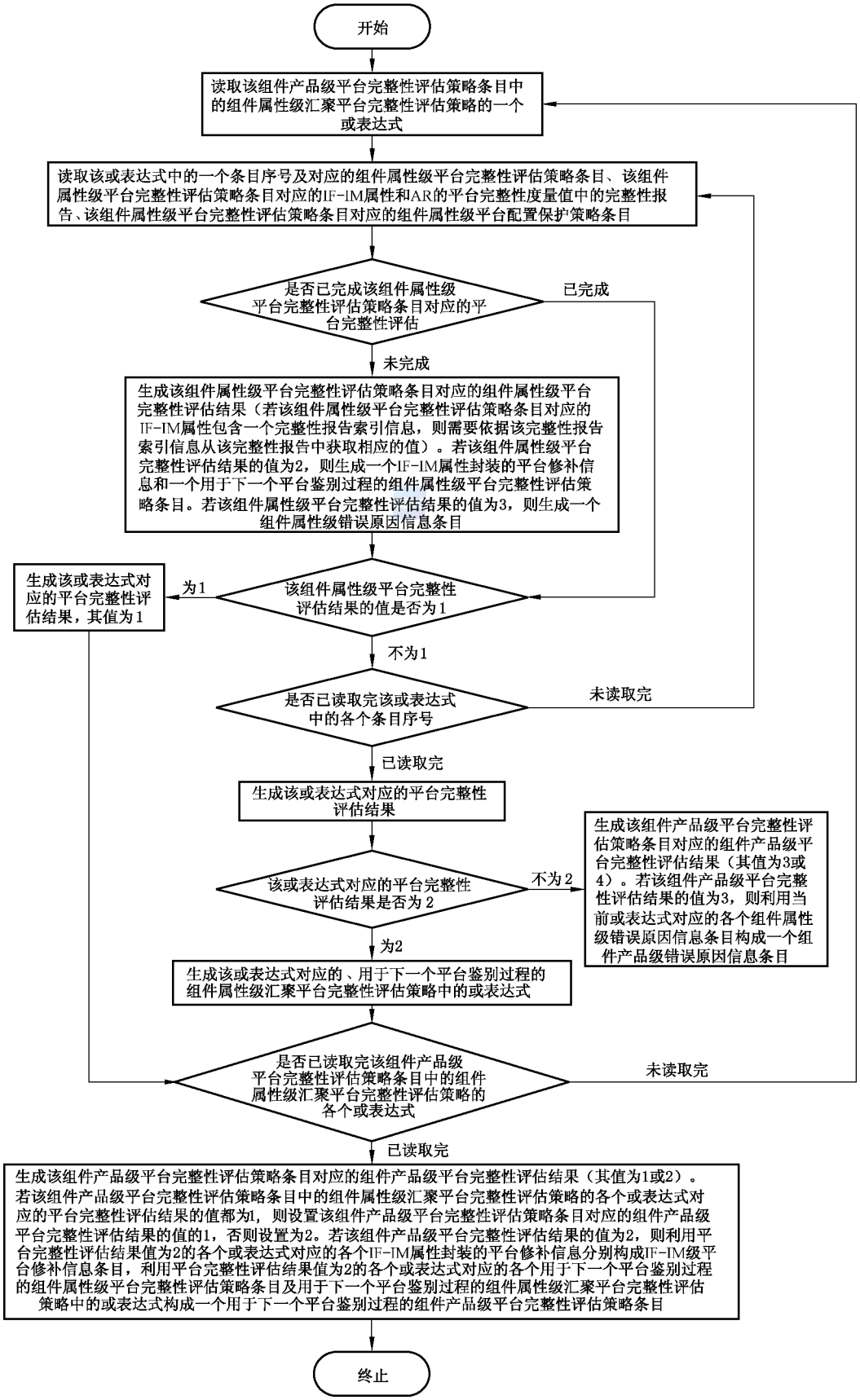

图 74　PAI-2 协议中 IMV 生成组件产品级平台完整性评估结果及其他参数的具体过程

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，当 EPS 上端的一个 IMV 收到一个组件产品级平台完整性评估策略条目(其组件产品序号为 0xff 值)及相应条目序号、各个组件产品级平台配置保护策略条目、各个 IF-IM 级平台完整性度量值条目、一个完整性报告时，若该 IMV 不支持该组件产品级平台完整性评估策略条目所对应的组件产品序号、组件属性类型厂家 ID 及组件属性类型，则首先生成一个组件产品级平台完整性评估结果(值设置为 3)和一个组件产品级错误原因信息条目(组件产品级错误原因信息码字段的值设置为 2)，然后利用 PM 中的 IF-IMV 功能函数 TCA_EPS_ProvideEvaluationResult 将该组件产品级平台完整性评估结果和该组件产品级错误原因信息条目发送给 EPS，否则检查各个 IF-IM 级平台完整性度量值条目和该完整性报告，若找不到该组件产品级平台完整性评估策略条目中的组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型，则生成一个组件产品级平台完整性评估结果(值设置为 4)；否则检查各个 IF-IM 级平台完整性度量值条目和该完整性报告，若只能找到该组件产品级平台完整性评估策略条目中的组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型对应的 IF-IM 错误信息，则生成一个组件产品级平台完整性评估结果(值设置 3)和一个组件产品级错误原因信息条目(组件产品级错误原因信息码字段的值设置为 4)；否则依据该组件产品级平台完整性评估策略条目中的组件属性级平台完整性评估策略条目执行平台完整性评估，若各个 IF-IM 级平台完整性度量值条目及该完整性报告中的所有组件产品的各个包含该组件属性级平台完整性评估策略条目中的组件属性类型厂家 ID 及组件属性类型的 IF-IM 属性都符合该组件属性级平台完整性评估策略条目对应的组件属性级平台完整性评估策略(若该 IF-IM 属性包含一个完整性报告索引信息，则依据该完整性报告索引信息从该完整性报告中获取相应的值)，则生成一个组件产品级平台完整性评估结果(值设置为 1)；否则生成一个组件产品级平台完整性评估结果(值设置为 4)。

对于一个消息类型，EPS 上端的一个 IMV 可以支持该消息类型下的多个组件产品级平台完整性评估策略条目对应的平台完整性评估，但是 EPS 上端的多个 IMV 不可以支持该消息类型下的同一个组件产品级平台完整性评估策略条目对应的平台完整性评估。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，对于一个组件产品级平台完整性评估策略条目，EPS 从 EPS 上端相应的各个 IMV 接收该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目，若从每个 IMV 都接收到一个组件产品级错误原因信息条目，且该组件产品级错误原因信息条目中的组件产品级错误原因信息码字段的值为 1 或 2，则 EPS 以任意一个从 IMV 接收到的该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目作为 EPS 生成的该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目；否则以一个从 IMV 接收到的、组件产品级错误原因信息条目中的组件产品级错误原因信息码字段的值不为 1 或 2 的该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目作为 EPS 生成的该组件产品级平台完整性评估策略条目对应的条目序号、组件产品级平台完整性评估结果、IF-IM 级平台修补信息条目、组件产品级错误原因信息条目和用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目。

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，对于一个组件类型级平台完整性评估策略条目，

EPS依据该组件类型级平台完整性评估策略条目中的组件产品级汇聚平台完整性评估策略生成该组件类型级平台完整性评估策略条目对应的条目序号、组件类型级平台完整性评估结果、组件类型级平台修补信息条目、组件类型级错误原因信息条目和用于下一个平台鉴别过程的组件类型级平台完整性评估策略条目的具体过程如图75所示。

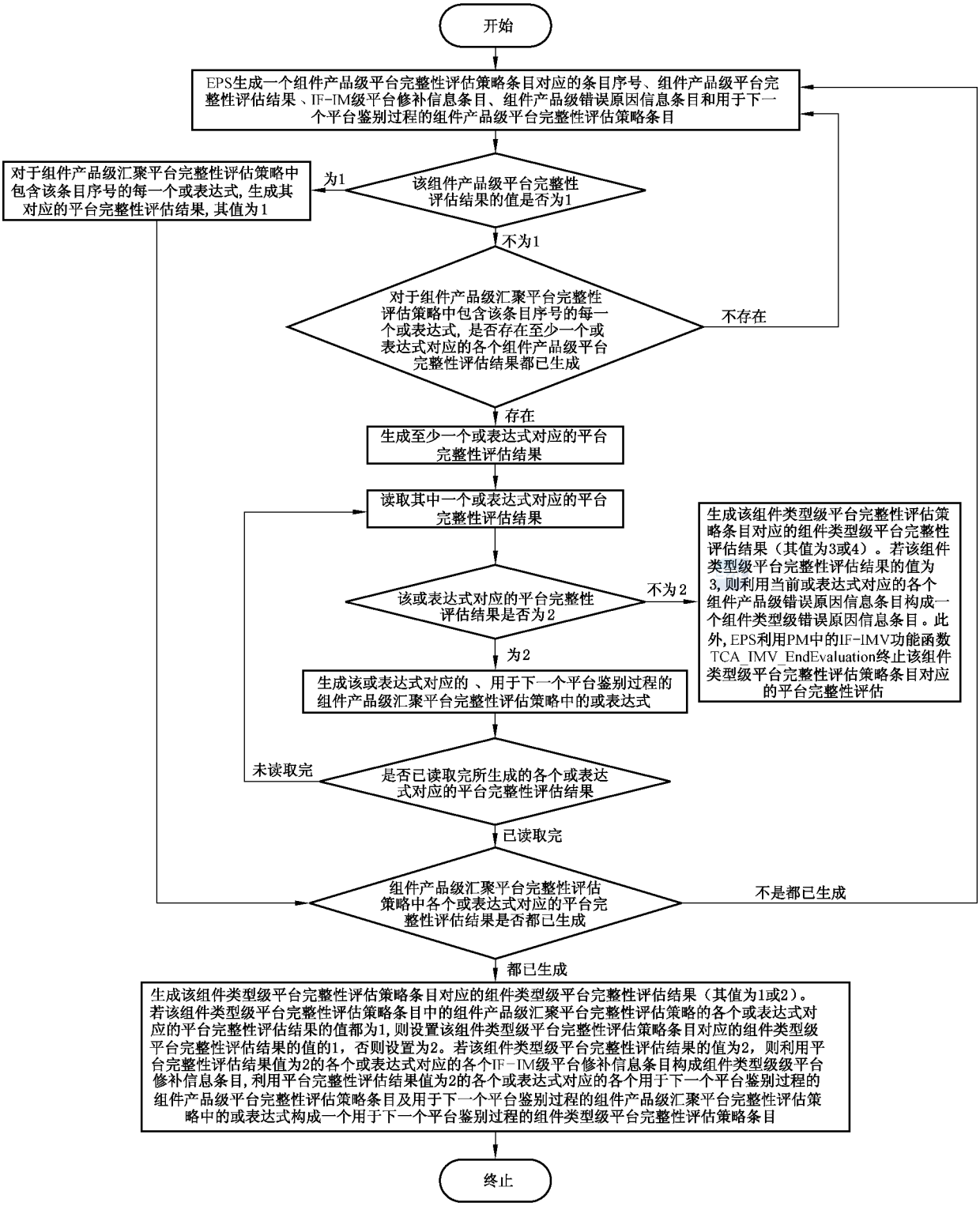

图75　PAI-2协议中EPS生成组件类型级平台完整性评估结果及其他参数的具体过程

在依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程中，对于对 AR 的平台完整性评估策略，EPS 依据对 AR 的平台完整性评估策略中的组件类型级汇聚平台完整性评估策略生成对 AR 的平台完整性评估策略对应的 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息和下一个平台鉴别过程的对 AR 的平台完整性评估策略的具体过程如图 76 所示。

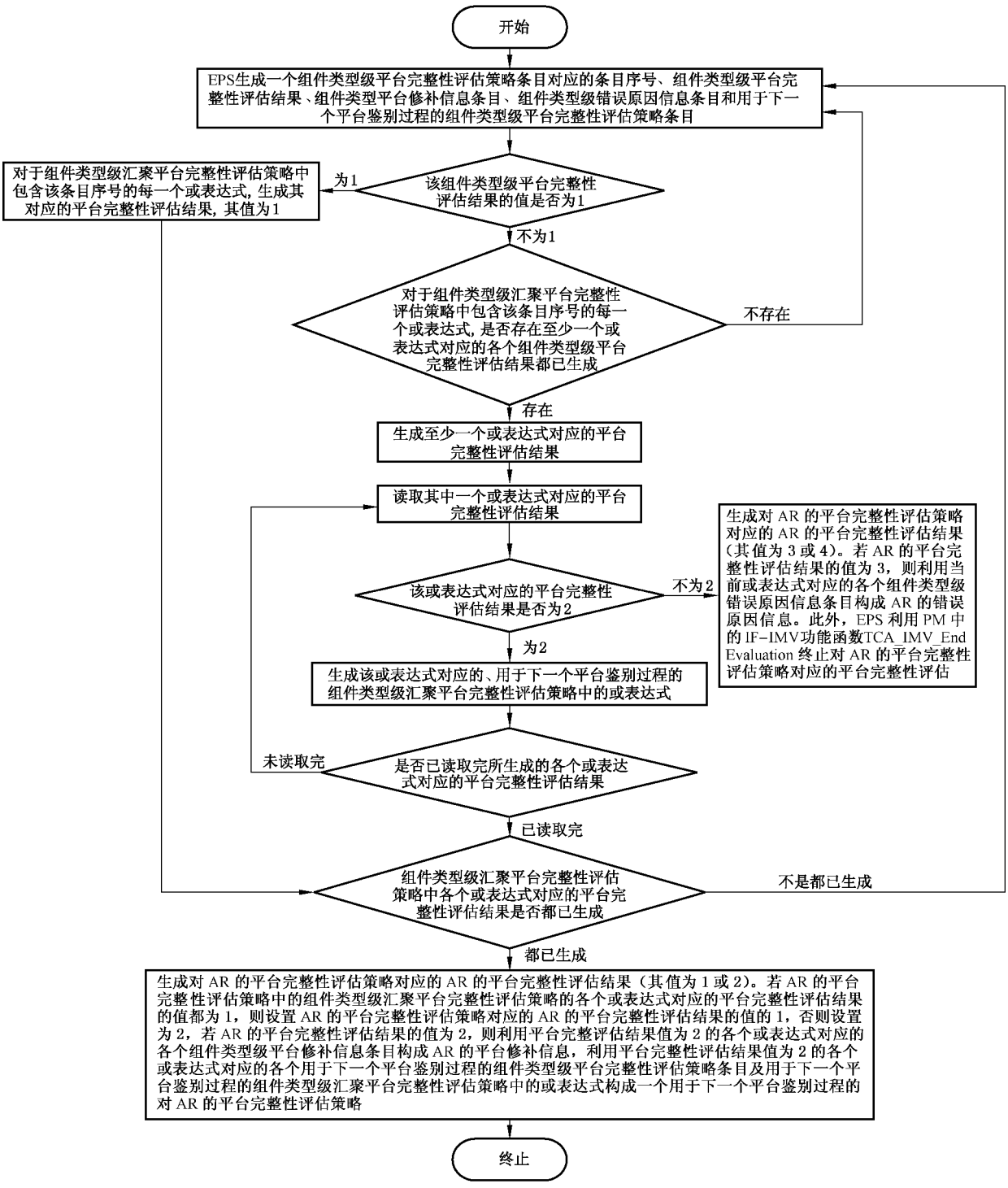

图 76　PAI-2 协议中 EPS 生成 AR 的平台完整性评估结果及其他参数的具体过程

依据 AC 的平台完整性度量值、AC 的平台配置保护策略和对 AC 的平台完整性评估策略生成 AC 的平台完整性评估结果、AC 的平台修补信息、AC 的错误原因信息、AC 的 Quote 数据和下一个平台鉴别过程的对 AC 的平台完整性评估策略的过程与依据 AR 的平台完整性度量值、AR 的平台配置保护策略和对 AR 的平台完整性评估策略生成 AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据和下一个平台鉴别过程的对 AR 的平台完整性评估策略的过程完全类同。

7.2.2.2.2.4 消息 4

消息 4 的数据字段格式如图 77 所示。

	标识 FLAG	PIK证书验证和平台 完整性评估结果	对PIK证书验证和平台完 整性评估结果的签名
八位位组数：	2	可变	可变

图 77 消息 4 的数据字段格式

其中：

——标识 FLAG 字段长度为 2 个八位位组，定义如前。比特 0、2、3、4、6、7、11 和 12 有意义。比特 0、2、3、4、6 和 7 的值分别与消息 3 中比特 0、2、3、4、6 和 7 的值相同。当 PIK 证书验证和平台完整性评估结果字段中包含 AR 的 Quote 数据时，设置标识 FLAG 字段中比特 11 的值为 1。当 PIK 证书验证和平台完整性评估结果字段中包含 AC 的 Quote 数据时，设置标识 FLAG 字段中比特 12 的值为 1。

——PIK 证书验证和平台完整性评估结果字段采用 PIK 证书验证和平台完整性评估结果属性表示，其格式定义如前。一次性随机数 1、PIK 证书 1、PIK 证书验证结果 1、平台完整性度量值 1、平台配置保护策略 1、平台完整性评估策略 1、平台完整性评估结果 1、平台修补信息 1、错误原因信息 1、Quote 数据 1、用于下一个平台鉴别过程的平台完整性评估策略 1、一次性随机数 2、PIK 证书 2、PIK 证书验证结果 2、平台完整性度量值 2、平台配置保护策略 2、平台完整性评估策略 2、平台完整性评估结果 2、平台修补信息 2、错误原因信息 2、Quote 数据 2、用于下一个平台鉴别过程的平台完整性评估策略 2 分别为 TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的 PIK 证书验证结果、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略、TNCC 挑战、AC 的 PIK 证书、AC 的 PIK 证书验证结果、AC 的平台完整性度量值、AC 的平台配置保护策略、对 AC 的平台完整性评估策略、AC 的平台完整性评估结果、AC 的平台修补信息、AC 错误原因信息、AC 的 Quote 数据、用于下一个平台鉴别过程的对 AC 的平台完整性评估策略。本字段中的 TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、TNCC 挑战、AC 的 PIK 证书、AC 的平台完整性度量值、AC 的平台配置保护策略、对 AC 的平台完整性评估策略分别与消息 3 中的 TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、TNCC 挑战、AC 的 PIK 证书、AC 的平台完整性度量值、AC 的平台配置保护策略、对 AC 的平台完整性评估策略相同。当标识 FLAG 字段中比特 0 的值为 0 时，TNCAP 平台鉴别挑战、AR 的 PIK 证书、AR 的 PIK 证书验证结果、AR 的平台完整性度量值、AR 的平台配置保护策略、对 AR 的平台完整性评估策略、AR 的平台完整性评估结果、AR 的平台修补信息、AR 的错误原因信息、AR 的 Quote 数据、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略不存在。当标识 FLAG 字段中比特 4 的值为 0 时，TNCC 挑战、AC 的 PIK 证

书、AC 的 PIK 证书验证结果、AC 的平台完整性度量值、AC 的平台配置保护策略、对 AC 的平台完整性评估策略、AC 的平台完整性评估结果、AC 的平台修补信息、AC 错误原因信息、AC 的 Quote 数据、用于下一个平台鉴别过程的对 AC 的平台完整性评估策略不存在。当标识 FLAG 字段中比特 2 的值为 0 时，AR 的平台配置保护策略不存在。当标识 FLAG 字段中比特 3 的值都为 0 时，AR 的 PIK 证书和 AR 的 PIK 证书验证结果不存在。当标识 FLAG 字段中比特 6 的值为 0 时，AC 的平台配置保护策略不存在。当标识 FLAG 字段中比特 7 的值都为 0 时，AC 的 PIK 证书和 AC 的 PIK 证书验证结果不存在。当标识 FLAG 字段中比特 11 的值为 0 时，AR 的 Quote 数据不存在。当标识 FLAG 字段中比特 12 的值为 0 时，AC 的 Quote 数据不存在。当 AR 的平台完整性评估结果字段的值为 1 时，AR 的平台修补信息、AR 的错误原因信息、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略不存在。当 AR 的平台完整性评估结果字段的值为 2 时，AR 的错误原因信息不存在。当 AR 的平台完整性评估结果字段的值为 3 时，AR 的平台修补信息、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略不存在。当 AR 的平台完整性评估结果字段的值为 4 时，AR 的平台修补信息、AR 的错误原因信息、用于下一个平台鉴别过程的对 AR 的平台完整性评估策略不存在。当 AC 的平台完整性评估结果字段的值为 1 时，AC 的平台修补信息、AC 的错误原因信息、用于下一个平台鉴别过程的对 AC 的平台完整性评估策略不存在。当 AC 的平台完整性评估结果字段的值为 2 时，AC 的错误原因信息不存在。当 AC 的平台完整性评估结果字段的值为 3 时，AC 的平台修补信息、用于下一个平台鉴别过程的对 AC 的平台完整性评估策略不存在。当 AC 的平台完整性评估结果字段的值为 4 时，AC 的平台修补信息、AC 的错误原因信息、用于下一个平台鉴别过程的对 AC 的平台完整性评估策略不存在。若 AR 和 PM 之间存在安全通道，则 AR 的平台修补信息和用于下一个平台鉴别过程的对 AC 的平台完整性评估策略在该安全通道中传递给 AR；否则 AR 的平台修补信息和用于下一个平台鉴别过程的对 AC 的平台完整性评估策略可采用数字信封（参见附录 C）的方式传递给 AR。若 AC 和 PM 之间存在安全通道，则 AC 的平台修补信息和用于下一个平台鉴别过程的对 AR 的平台完整性评估策略在该安全通道中传递给 AC；否则 AC 的平台修补信息和用于下一个平台鉴别过程的对 AR 的平台完整性评估策略可采用数字信封（参见附录 C）的方式传递给 AC。AR 和 PM 之间、AC 和 PM 之间的安全通道可以采取 EWAI 协议和 ETLS 协议来建立，具体见 6.2.1.3.5 和 6.2.2.2.4。

——对 PIK 证书验证和平台完整性评估结果的签名采用签名属性表示，是利用 PM 的用户证书的私钥生成的签名，定义如前。

当 EPS 接收到 TNCAP 发送的消息 3 时，EPS 向 TNCAP 发送消息 4。

TNCAP 接收到 EPS 发送的消息 4 后，进行如下处理：

a) 检查标识 FLAG 字段中比特 0 的值，若值为 0，则执行步骤 b)；否则执行步骤 e)。

b) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则丢弃消息 4；否则检查 PIK 证书验证和平台完整性评估结果中的 AC 的平台完整性评估结果的值，若值为 2，则执行步骤 c)；否则执行步骤 d)。

c) 验证 PIK 证书验证和平台完整性评估结果及签名（PIK 证书验证和平台完整性评估结果中的 AC 的 Quote 数据是 TNCAP 生成的 AC 的 Quote 数据），若验证不通过，则丢弃消息 4；否则利用 AC 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AC 的平台修补信息发送给 TNCAP 上端的相应 IMC。

d) 依据标识 FLAG、TNCC 挑战、TNCAP 生成的 AC 的 Quote 数据、AC 的 PIK 证书、复合 PIK 证书验证和平台完整性评估结果构成消息 5，并发送给 TNCC。

e) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则执行步骤 f)；否则执行步骤 n)。

f) 验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据是消息 2 中的 AR 的 Quote 数据),若验证不通过,则丢弃消息 4;否则继续检查 AR 的 PIK 证书验证结果和 AR 的平台完整性评估结果的值,若 AR 的 PIK 证书验证结果的值为非 0,或者 AR 的平台完整性评估结果的值为 3 或 4,则首先生成 AC 的访问决策,其值为禁止(将 AC 的访问决策通知 NAC),并设置标识 FLAG 字段中比特 10 的值为 1,然后依据标识 FLAG、TNCAP 挑战和 AC 的访问决策构成消息 5,并发送给 TNCC;否则执行步骤 g)。

g) 验证 TNCAP 是否已读取完各个分割部分的对 AR 的平台完整性评估策略,若 TNCAP 未读取完各个分割部分的对 AR 的平台完整性评估策略,则执行步骤 h);否则执行 k)。

h) 检查 PIK 证书验证和平台完整性评估结果中的 AR 的平台完整性评估结果的值,若值为 2,则执行步骤 i);否则执行步骤 j)。

i) 设置下一轮 PAI 协议中的对 AR 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AR 的平台完整性评估策略为下一个分割部分的对 AR 的平台完整性评估策略;首先设置标识 FLAG 字段中比特 13 的值为 1,然后依据标识 FLAG 字段、TNCAP 挑战、复合 PIK 证书验证和平台完整性评估结果构成消息 5,并发送给 TNCC。

j) 设置下一轮 PAI 协议中的对 AR 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AR 的平台完整性评估策略为下一个分割部分的对 AR 的平台完整性评估策略,本轮 PAI 协议完成。

k) 检查 PIK 证书验证和平台完整性评估结果中的 AR 的平台完整性评估结果的值,若值为 2,则执行步骤 l);否则执行步骤 m)。

l) 依据各轮 PAI 协议中的 AR 的平台完整性评估结果生成该平台鉴别过程的 AR 的平台完整性评估结果(执行与运算而得,值为 1 或 2);若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 1,则首先生成 AC 的访问决策,其值为允许;若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 2,则首先生成 AC 的访问决策,其值为隔离;将 AC 的访问决策通知 NAC;若 AC 的访问决策为隔离,则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AR 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略为用于下一个平台鉴别过程的对 AR 的平台完整性评估策略中的一个分割部分),并设置对 AR 的平台鉴别需求的值为 1;首先设置标识 FLAG 字段中比特 10 和 13 的值为 1,然后依据标识 FLAG、TNCAP 挑战、AC 的访问决策、复合 PIK 证书验证和平台完整性评估结果构成消息 5,并发送给 TNCC。

m) 依据各轮 PAI 协议中的 AR 的平台完整性评估结果生成该平台鉴别过程的 AR 的平台完整性评估结果(执行与运算而得,值为 1 或 2);若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 1,则生成 AC 的访问决策,其值为允许;若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 2,则生成 AC 的访问决策,其值为隔离;将 AC 的访问决策通知 NAC;若 AC 的访问决策为隔离,则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AR 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略为用于下一个平台鉴别过程的对 AR 的平台完整性评估策略中的一个分割部分),并设置对 AR 的平台鉴别需求的值为 1;首先设置标识 FLAG 字段中比特 10 的值为 1,然后依据标识 FLAG、TNCAP 挑战、AC 的访问决策构成消息 5,并发送给 TNCC。

n) 验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据是消息 2 中的 AR 的 Quote 数据,PIK 证书验证和平台完整性评估结果中

的 AC 的 Quote 数据是消息 2 中的 AC 的 Quote 数据),若验证不通过,则丢弃消息 4;否则继续检查 AR 的 PIK 证书验证结果和 AR 的平台完整性评估结果的值,若 AR 的 PIK 证书验证结果的值为非 0,或者 AR 的平台完整性评估结果的值为 3 或 4,则首先生成 AC 的访问决策,其值为禁止(将 AC 的访问决策通知 NAC),并设置标识 FLAG 字段中比特 10 的值为 1,然后依据标识 FLAG、TNCAP 挑战和 AC 的访问决策构成消息 5,并发送给 TNCC;否则执行步骤 o)。

o) 检查 PIK 证书验证和平台完整性评估结果中的 AC 的平台完整性评估结果的值,若值为 2,则执行步骤 p);否则执行步骤 q)。

p) 利用 AC 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AC 的平台修补信息发送给 TNCAP 上端的相应 IMC。

q) 验证 TNCAP 是否已读取完各个分割部分的对 AR 的平台完整性评估策略,若 TNCAP 未读取完各个分割部分的对 AR 的平台完整性评估策略,则首先设置下一轮 PAI 协议中的对 AR 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AR 的平台完整性评估策略为下一个分割部分的对 AR 的平台完整性评估策略,然后依据标识 FLAG、TNCC 挑战、TNCAP 生成的 AC 的 Quote 数据、AC 的 PIK 证书、复合 PIK 证书验证和平台完整性评估结果构成消息 5,并发送给 TNCC;否则:依据各轮 PAI 协议中的 AR 的平台完整性评估结果生成该平台鉴别过程的 AR 的平台完整性评估结果(执行与运算而得,值为 1 或 2);若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 1,则生成 AC 的访问决策,其值为允许;若 AR 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AR 的平台完整性评估结果的值为 2,则生成 AC 的访问决策,其值为隔离;将 AC 的访问决策通知 NAC;若 AC 的访问决策为隔离,则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AR 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AR 的平台完整性评估策略为用于下一个平台鉴别过程的对 AR 的平台完整性评估策略中的一个分割部分),并设置对 AR 的平台鉴别需求的值为 1;首先设置标识 FLAG 字段中比特 10 的值为 1,然后依据标识 FLAG、TNCAP 挑战、AC 的访问决策、TNCC 挑战、AC 的 Quote 数据、AC 的 PIK 证书、复合 PIK 证书验证和平台完整性评估结果构成消息 5,并发送给 TNCC。

7.2.2.2.2.5 消息 5

消息 5 的数据字段格式如图 78 所示。

	标识 FLAG	TNCAP 挑战	AC的访问决策	TNCC 挑战	AC的平台鉴别错误指示	AC的Quote数据	AC的PIK证书	复合PIK证书验证和平台完整性评估结果
八位位组数:	2	32	1	32	1	可变	可变	可变

图 78 消息 5 的数据字段格式

其中:

——标识 FLAG 字段长度为 2 个八位位组,定义如前。比特 0、2、3、4、5、6、7、10 和 12 有意义。比特 0、2、3、4、6、7 和 12 的值分别与消息 4 中比特 0、2、3、4、6、7 和 12 的值相同。

——TNCAP 挑战字段长度为 32 个八位位组,定义如前。TNCAP 挑战字段的值与消息 1 中 TNCAP 挑战字段的值相同。

——AC 的访问决策字段长度为 1 个八位位组,其值为允许、隔离或禁止。当标识 FLAG 字段中比特 10 的值为 1 时,本字段存在。

——TNCC 挑战字段长度为 32 个八位位组，定义如前。TNCC 挑战字段的值与消息 2 中 TNCC 挑战字段的值相同。

——AC 的平台鉴别错误指示字段长度为 1 个八位位组。当标识 FLAG 字段中比特 5 的值为 1 时，本字段存在。AC 的平台鉴别错误指示字段的值如下：

1 不可跳过错误；

其他值保留。

——AC 的 Quote 数据字段长度可变，其值为 TNCAP 生成的 AC 的 Quote 数据。当标识 FLAG 字段中比特 12 的值为 1 时，本字段存在。

——AC 的 PIK 证书字段长度为可变，定义如前。当标识 FLAG 字段中比特 7 的值的 1 时，本字段存在。

——复合 PIK 证书验证和平台完整性评估结果字段长度为可变，其内容为消息 4 中除标识 FLAG 字段的其他字段。

当 TNCAP 接收到 EPS 发送的消息 4 时，TNCAP 向 TNCC 发送消息 5。

TNCC 接收到 TNCAP 发送的消息 5 后，进行如下处理：

a) 检查标识 FLAG 字段中比特 0 的值，若值为 0，则执行步骤 b)；否则执行步骤 e)。

b) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则丢弃消息 5；否则检查标识 FLAG 字段中比特 5 的值，若值为 1 且 AC 的平台鉴别错误指示的值为 1，则 TNCC 首先生成 AR 的访问决策，其值为禁止(将 AR 的访问决策通知 NAR)，并设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP；否则执行步骤 c)。

c) 验证 AC 的 Quote 数据中的 PIK 签名(当标识 FLAG 字段中比特 12 的值为 1 时才需要验证 AC 的 Quote 数据中的 PIK 签名)，若验证不通过，则丢弃消息 5；否则验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AC 的 Quote 数据是消息 5 中的 AC 的 Quote 数据)，若验证不通过，则丢弃消息 5；否则继续检查 AC 的 PIK 证书验证结果和 AC 的平台完整性评估结果的值，若 AC 的 PIK 证书验证结果的值为非 0，或者 AC 的平台完整性评估结果的值为 3 或 4，则首先生成 AR 的访问决策，其值为禁止(将 AR 的访问决策通知 NAR)，并设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP；否则执行步骤 d)。

d) 验证 TNCC 是否已读取完各个分割部分的对 AC 的平台完整性评估策略，若 TNCC 未读取完各个分割部分的对 AC 的平台完整性评估策略，则设置下一轮 PAI 协议中的对 AC 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AC 的平台完整性评估策略为下一个分割部分的对 AC 的平台完整性评估策略，本轮 PAI 协议完成；否则依据各轮 PAI 协议中的 AC 的平台完整性评估结果生成该平台鉴别过程的 AC 的平台完整性评估结果(执行与运算而得，值为 1 或 2)；若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 1，则生成 AR 的访问决策，其值为允许；若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 2，则首先生成 AR 的访问决策，其值为隔离；将 AR 的访问决策通知 NAR；若 AR 的访问决策为隔离，则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AC 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略为用于下一个平台鉴别过程的对 AC 的平台完整性评估策略中的一个分割部分)，并设置对 AC 的平台鉴别需求的值为 1；首先设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP。

e) 检查标识 FLAG 字段中比特 10 的值，若值为 0，则执行步骤 f)；否则执行步骤 m)。

f) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则执行步骤 g)；否则执行步骤 h)。

g) 检查标识 FLAG 字段比特 13 的值，若值为 0，则丢弃消息 5；否则验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据是 TNCC 生成的 AR 的 Quote 数据)，若验证不通过，则丢弃消息 5；否则利用 AR 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AR 的平台修补信息发送给 TNCC 上端的相应 IMC，本轮 PAI 协议结束。

h) 检查标识 FLAG 字段中比特 5 的值，若值为 1 且 AC 的平台鉴别错误指示的值为 1，则 TNCC 首先生成 AR 的访问决策，其值为禁止(将 AR 的访问决策通知 NAR)，并设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP，否则执行步骤 i)。

i) 验证 AC 的 Quote 数据中的 PIK 签名(当标识 FLAG 字段中比特 12 的值为 1 时才需要验证 AC 的 Quote 数据中的 PIK 签名)，若验证不通过，则丢弃消息 5；否则验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据是 TNCC 生成的 AR 的 Quote 数据，PIK 证书验证和平台完整性评估结果中的 AC 的 Quote 数据是消息 5 中的 AC 的 Quote 数据)，若验证不通过，则丢弃消息 5；否则继续检查 AC 的 PIK 证书验证结果和 AC 的平台完整性评估结果的值，若 AC 的 PIK 证书验证结果的值为非 0，或者 AC 的平台完整性评估结果的值为 3 或 4，则首先生成 AR 的访问决策，其值为禁止(将 AR 的访问决策通知 NAR)，并设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP；否则执行步骤 j)。

j) 检查 PIK 证书验证和平台完整性评估结果中的 AR 的平台完整性评估结果的值，若值为 2，则执行步骤 k)；否则执行步骤 l)。

k) 利用 AR 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AR 的平台修补信息发送给 TNCC 上端的相应 IMC。

l) 验证 TNCC 是否已读取完各个分割部分的对 AC 的平台完整性评估策略，若 TNCC 未读取完各个分割部分的对 AC 的平台完整性评估策略，则设置下一轮 PAI 协议中的对 AC 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AC 的平台完整性评估策略为下一个分割部分的对 AC 的平台完整性评估策略，本轮 PAI 协议结束；否则：依据各轮 PAI 协议中的 AC 的平台完整性评估结果生成该平台鉴别过程的 AC 的平台完整性评估结果(执行与运算而得，值为 1 或 2)；若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 1，则生成 AR 的访问决策，其值为允许；若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 2，则生成 AR 的访问决策，其值为隔离；将 AR 的访问决策通知 NAR；若 AR 的访问决策为隔离，则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AC 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略为用于下一个平台鉴别过程的对 AC 的平台完整性评估策略中的一个分割部分)，并设置对 AC 的平台鉴别需求的值为 1；首先设置标识 FLAG 字段中比特 9 的值为 1，然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6，并发送给 TNCAP。

m) 利用 AR 中的 IF-IMC 功能函数 TCA_IMC_NotifyConnectionChange 将 AC 的访问决策通知 TNCC 上端的各个 IMC。若 AC 的访问决策为禁止，则 TNCC 通知 NAR 断开与 AC 的连接；否则执行步骤 n)。

n) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则执行步骤 o)；否则执行步骤 p)。

o) 检查标识 FLAG 字段比特 13 的值，若值为 0，本轮 PAI 协议结束；否则验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据是

TNCC 生成的 AR 的 Quote 数据),若验证不通过,则丢弃消息 5;否则利用 AR 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AR 的平台修补信息发送给 TNCC 上端的相应 IMC,本轮 PAI 协议结束。

p) 验证 AC 的 Quote 数据中的 PIK 签名(当标识 FLAG 字段中比特 12 的值为 1 时才需要验证 AC 的 Quote 数据中的 PIK 签名),若验证不通过,则丢弃消息 5;否则验证 PIK 证书验证和平台完整性评估结果及签名(PIK 证书验证和平台完整性评估结果中的 AR 的 Quote 数据是 TNCC 生成的 AR 的 Quote 数据,PIK 证书验证和平台完整性评估结果中的 AC 的 Quote 数据是消息 5 中的 AC 的 Quote 数据),若验证不通过,则丢弃消息 5;否则继续检查 AC 的 PIK 证书验证结果和 AC 的平台完整性评估结果的值,若 AC 的 PIK 证书验证结果的值为非 0,或者 AC 的平台完整性评估结果的值为 3 或 4,则首先生成 AR 的访问决策,其值为禁止(将 AR 的访问决策通知 NAR),并设置标识 FLAG 字段中比特 9 的值为 1,然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6,并发送给 TNCAP;否则执行步骤 q)。

q) 检查 PIK 证书验证和平台完整性评估结果中的 AR 的平台完整性评估结果的值,若值为 2,则执行步骤 r);否则执行步骤 s)。

r) 利用 AR 的 IF-IMC 功能函数 TCA_IMC_ReceiveMessage 将 PIK 证书验证和平台完整性评估结果中的 AR 的平台修补信息发送给 TNCC 上端的相应 IMC。

s) 验证 TNCC 是否已读取完各个分割部分的对 AC 的平台完整性评估策略,若 TNCC 未读取完各个分割部分的对 AC 的平台完整性评估策略,则设置下一轮 PAI 协议中的对 AC 的平台鉴别需求为 1 和下一轮 PAI 协议中的对 AC 的平台完整性评估策略为下一个分割部分的对 AC 的平台完整性评估策略,本轮 PAI 协议结束;否则:依据各轮 PAI 协议中的 AC 的平台完整性评估结果生成该平台鉴别过程的 AC 的平台完整性评估结果(执行与运算而得,值为 1 或 2);若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 1,则生成 AR 的访问决策,其值为允许;若 AC 的 PIK 证书验证结果的值为 0 且该平台鉴别过程的 AC 的平台完整性评估结果的值为 2,则生成 AR 的访问决策,其值为隔离;将 AR 的访问决策通知 NAR;若 AR 的访问决策为隔离,则依据各轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略生成用于下一个平台鉴别过程的对 AC 的平台完整性评估策略(每一轮 PAI 协议中的用于下一个平台鉴别过程的对 AC 的平台完整性评估策略为用于下一个平台鉴别过程的对 AC 的平台完整性评估策略中的一个分割部分),并设置对 AC 的平台鉴别需求的值为 1;首先设置标识 FLAG 字段中比特 9 的值为 1,然后依据标识 FLAG、TNCC 挑战和 AR 的访问决策构成消息 6,并发送给 TNCAP。

7.2.2.2.2.6 消息 6

消息 6 的数据字段格式如图 79 所示。

	标识FLAG	TNCC挑战	AR的访问决策
八位位组数:	2	32	1

图 79 消息 6 的数据字段格式

其中:

——标识 FLAG 字段长度为 2 个八位位组,定义如前。比特 4 和 9 有意义。比特 4 的值与消息 5 中比特 4 的值相同。

——TNCC 挑战字段长度为 32 个八位位组,定义如前。TNCC 挑战字段的值与消息 2 中的 TNCC 挑战字段的值相同。

——AR 的访问决策字段长度为 1 个八位位组，定义如前。

TNCAP 接收到 TNCC 发送的消息 6 后，进行如下处理：

a) 检查标识 FLAG 字段中比特 4 的值，若值为 0，则丢弃消息 6；否则执行步骤 b)。

b) 检查标识 FLAG 字段中比特 9 的值，若值为 0，则丢弃消息 6；否则执行步骤 c)。

c) 利用 AC 中的 IF-IMC 功能函数 TCA_IMC_NotifyConnectionChange 将 AR 的访问决策通知 TNCAP 上端的各个 IMC。若 AR 的访问决策为禁止，则 TNCAP 通知 NAC 断开与 AR 的连接。

8 完整性度量层

8.1 概述

完整性度量层包含两种组件：IMC 和 IMV。AR 中的各个 IMC 负责收集 AR 的平台完整性信息，AC 中的各个 IMC 负责收集 AC 的平台完整性信息，而 PM 中的各个 IMV 负责校验和评估 AR 和 AC 的平台完整性信息。

IF-IM 是 IMC 和 IMV 之间的接口，它定义了 IMC 和 IMV 之间的消息交换协议，称为 IF-IM 消息协议。IMC 和 IMV 之间交换的消息称为 IF-IM 消息。

8.2 IF-IM 消息协议

8.2.1 IF-IM 消息传递模型

IF-IM 消息承载在可信平台评估层的 PAI 协议中进行传递，具体见 7.2.2。每一轮 PAI 协议可以传递一个或多个 IF-IM 消息。每一个 IF-IM 消息可以包含一个或多个的 IF-IM 属性。

8.2.2 IF-IM 与 PAI 协议的关系

IF-IM 与 PAI 协议之间的重要关系就是消息类型。TNCC 和 TNCAP 利用消息类型路由 IF-IM 消息至各个 IMC。EPS 利用消息类型路由 IF-IM 消息至各个 IMV。每一个 IMC 和 IMV 支持各种消息类型。消息类型表明了 IF-IM 消息的组件类型。消息类型由两个部分构成：组件类型厂家 ID 和组件类型。本标准定义的组件类型如表 3 所示。

表 3 本标准定义的组件类型

组件类型标识符	组件类型名称	描　　述
0x00000001	操作系统	基于主机的操作系统
0x00000002	反病毒软件	基于主机的反病毒软件
0x00000003	反间谍软件	基于主机的反间谍软件
0x00000004	反恶意软件	基于主机的反恶意软件，不包括反病毒软件和反间谍软件
0x00000005	防火墙	基于主机的防火墙
0x00000006	入侵检测/防御系统	基于主机的入侵检测和/或防御软件
0x00000007	VPN（见 ISO/IEC 18028-5：2006 和 RFC 2547）	基于主机的 VPN 软件
0x00000008	引导系统	基于主机的引导系统
0x00000009	TCA	基于主机的 TCA
0xffffffff	任意组件类型	基于主机的任意组件产品
0x0000000a～0xfffffffe	保留	—

对于本标准定义的组件类型，其对应的组件类型厂家 ID 的值为 0。

IF-IM 消息在 PAI 协议中的具体封装见 7.2.2。

8.2.3 IF-IM 消息的格式

IF-IM 消息的格式如图 80 所示。

版本(1)	保留(3)
IF-IM 消息挑战(4)	IF-IM 属性的个数(2)
IF-IM 属性 1(可变)	
IF-IM 属性 2(可变)	
.....	

图 80 IF-IM 消息的格式

其中：

——版本字段长度为 1 个八位位组，表示 IF-IM 消息协议版本号。当前版本为 1。

——保留字段长度为 3 个八位位组，其值默认为 0。

——IF-IM 消息挑战字段长度为 4 个八位位组，是 IF-IM 消息发送者随机产生的值，用于标识响应的 IF-IM 消息。

——IF-IM 属性的个数字段长度为 2 个八位位组，其值为 IF-IM 属性的个数。

——IF-IM 属性 1、IF-IM 属性 2、…为 8.2.4 定义的 IF-IM 属性。

8.2.4 IF-IM 属性

8.2.4.1 概述

IF-IM 属性的格式如图 81 所示。

FLAG(1)	IF-IM 属性类型厂家 ID(3)
IF-IM 属性类型(4)	
IF-IM 属性长度(4)	
组件产品关联标识(4)	
IF-IM 属性值(可变)	

图 81 IF-IM 属性的格式

其中：

——FLAG 字段长度为 1 个八位位组，比特 0 有意义。若比特 0 的值为 1，则组件产品关联标识存在；否则不存在。

——IF-IM 属性类型厂家 ID 字段长度为 3 个八位位组，当 IF-IM 属性类型厂家 ID 的值为 0 时，IF-IM 属性为本标准定义的 IF-IM 属性。当 IF-M 属性厂家 ID 的值为 0x000001～0xffffff 时，IF-IM 属性为厂家自己定义的 IF-IM 属性。

——IF-IM 属性类型字段长度为 4 个八位位组，本标准定义的 IF-IM 属性类型如表 4 所示。

——IF-IM 属性长度字段长度为 4 个八位位组，表示 IF-IM 属性值的长度。

——组件产品关联标识字段长度为 4 个八位位组，用于标识相同组件类型下的不同组件产品。例

如，一个 IMC 向一个 IMV 报告一个相同组件类型下的不同组件产品时就需要设置组件产品关联标识。组件产品关联标识字段的值是 IMC 本地创建的计数器数，其初始值为 1。当组件产品关联标识字段的值为 0xffffffff 时，该 IF-IM 属性对应于 IF-IM 消息中的所有组件产品。

——IF-IM 属性值字段长度为可变，表示 IF-IM 属性值的内容。

表 4　本标准定义的 IF-IM 属性类型

IF-IM 属性类型标识符	IF-IM 属性类型名称	描　　述
0x00000001	产品信息	描述组件产品的产品信息
0x00000002	数字版本	描述组件产品的数字版本
0x00000003	字符串版本	描述组件产品的字符串版本
0x00000004	操作状态	描述组件产品的操作状态
0x00000005	完整性报告	描述一个或多个组件产品的完整性报告
0x00000006	完整性报告索引信息	描述一个或多个组件产品的完整性报告索引信息
0x00000007	平台修补信息	描述组件产品的平台修补指示
0x00000008	IF-IM 错误信息	描述 IF-IM 错误指示
0x00000009～0xffffffff	保留	—

在执行平台完整性度量时，IMC 依据组件属性类型厂家 ID 和组件属性类型生成相应的 IF-IM 属性，其中该 IF-IM 属性中的 IF-IM 属性类型厂家 ID 与组件属性类型厂家 ID 相同，该 IF-IM 属性中的 IF-IM 属性类型与组件属性类型对应，例如：完整性报告和完整性报告索引信息的 IF-IM 属性对应完整性信息的组件属性类型，具体见 7.2.2.1.1 中的 d)。

8.2.4.2　产品信息

产品信息的 IF-IM 属性值如图 82 所示。

产品厂家 ID(3)
产品 ID(2)
产品名称(可变)

图 82　产品信息的 IF-IM 属性值

其中：

——产品厂家 ID 字段长度为 3 个八位位组，其值为组件产品的产品厂家 ID，用于标识创建该组件产品的厂家。

——组件产品 ID 字段长度为 2 个八位位组，其值为组件产品的产品 ID，用于标识产品厂家 ID 字段的值对应的一个组件产品。

——产品名称字段长度为可变，其值为组件产品的产品名称。

8.2.4.3　数字版本

数字版本的 IF-IM 属性值如图 83 所示。

主版本号(4)	
次版本号(4)	
编译号(4)	
服务包主版本号(2)	服务包次版本号(2)

图 83　数字版本的 IF-IM 属性值

其中：

——主版本号字段长度为 4 个八位位组，其值为组件产品的主版本号。

——次版本号字段长度为 4 个八位位组，其值为组件产品的次版本号。

——编译号字段长度为 4 个八位位组，其值为组件产品的编译号。

——服务包主版本号字段长度为 2 个八位位组，其值为组件产品的服务包主版本号。

——服务包次版本号字段长度为 2 个八位位组，其值为组件产品的服务包次版本号。

8.2.4.4　字符串版本

字符串版本的 IF-IM 属性值如图 84 所示。

组件版本号长度(1)	组件版本号(可变)
内部编译号长度(1)	内部编译号(可变)
配置版本号长度(1)	配置版本号(可变)

图 84　字符串版本的 IF-IM 属性值

其中：

——组件版本号长度字段长度为 1 个八位位组，其值为组件版本号的八位位组数。

——组件版本号字段长度为可变，其值是对应组件产品的版本号的字符串。

——内部编译号字段长度为 1 个八位位组，其值为内部编译号的八位位组数。

——内部编译号字段长度为可变，其值是对应组件产品的厂家内部工程编译号的字符串。

——配置版本号字段长度为 1 个八位位组，其值为配置版本号的八位位组数。

——配置版本号字段长度为可变，其值是对应组件产品的配置版本的字符串。

8.2.4.5　操作状态

操作状态的 IF-IM 属性值如图 85 所示。

状态码(1)	保留(3)
使用情况(可变)	

图 85　操作状态的 IF-IM 属性值

其中：

——状态码字段长度为 1 个八位位组，其值如下：

1　组件产品未安装；

2　组件产品已安装，但未正在运行；

3　组件产品正在运行；

其他值保留。

——保留字段长度为 3 个八位位组，其值默认为 0。

——使用情况字段长度为可变，其值不在本标准中规定。

8.2.4.6 完整性报告

完整性报告由快照和 Quote 数据构成，其中快照包含运行时完整性度量值，Quote 数据包含 PIK 签名。完整性报告、快照和 Quote 数据的具体定义不在本标准中规定。

8.2.4.7 完整性报告索引信息

完整性报告索引信息用于生成完整性报告，具体定义不在本标准中规定。

8.2.4.8 平台修补信息

平台修补信息的 IF-IM 属性值如图 86 所示。

保留(1)	平台修补信息类型厂家 ID(3)
平台修补信息类型(4)	
平台修补信息长度(4)	
平台修补信息值(可变)	

图 86 平台修补信息的 IF-IM 属性值

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——平台修补信息类型厂家 ID 字段长度为 3 个八位位组，其值如下：

0 本标准定义的平台修补信息；

其他值保留。

——平台修补信息类型字段为 4 个八位位组，其值如下：

1 基于 URI 的修补指示；

其他值保留。

——平台修补信息长度字段长度为 4 个八位位组，其值为平台修补信息值的八位位组数。

——平台修补信息值字段长度为可变。当平台修补信息类型字段的值为 1 时，平台修补信息值为基于 URI 的修补指示，如图 87 所示。

URI 长度(2)	修补指示的 URI 值(可变)
修补指示消息长度(2)	修补指示消息值(可变)

图 87 基于 URI 的修补指示

其中，URI 长度字段长度为 2 个八位位组，其值为修补指示的 URI 值字段的八位位组数；修补指示的 URI 值字段长度为可变，其值不在本标准中规定；修补指示消息长度字段长度为 2 个八位位组，其值为修补指示消息值字段的八位位组数；修补指示消息值字段长变为可变，其值不在本标准中规定。

8.2.4.9 IF-IM 错误信息

IF-IM 错误信息的 IF-IM 属性值如图 88 所示。

保留(1)	IF-IM 错误信息代码厂家 ID(3)
IF-IM 错误信息代码(4)	
IF-IM 错误信息值(可变)	

图 88　IF-IM 错误信息

其中：

——保留字段长度为 1 个八位位组，其值默认为 0。

——IF-IM 错误信息代码厂家 ID 字段长度为 3 个八位位组，其值如下：

0　本标准定义的 IF-IM 错误信息；

其他值保留。

——IF-IM 错误信息代码字段为 4 个八位位组，其值如下：

1　组件属性类型厂家 ID 及组件属性类型不为 IMC 所支持；

2　组件属性类型厂家 ID 及组件属性类型对应的组件属性修补失败；

其他值保留。

——IF-IM 错误信息值字段长度为可变。当 IF-IM 错误信息代码字段的值为 1 或 2 时，IF-IM 错误信息值由组件属性类型厂家 ID 及组件属性类型构成。

9　IF-IMC 和 IF-IMV

9.1　概述

TCA 的 IF-IMC 包括 AR 中的 IF-IMC 和 AC 中的 IF-IMC。前者是 TNCC 与它上端的各个 IMC 之间的接口，定义了一些功能函数来交互一些平台鉴别相关信息，用于协助完成可信平台评估层的 PAI 协议(见 9.2)。后者是 TNCAP 与它上端的各个 IMC 之间的接口，定义了一些功能函数来交互一些平台鉴别相关信息，用于协助完成可信平台评估层的 PAI 协议(见 9.2)。

TCA 的 IF-IMV 是 EPS 与它上端的各个 IMV 之间接口，定义了一些功能函数来交互一些平台鉴别相关信息，用于协助完成可信平台评估层的 PAI 协议(见 9.3)。

9.2　IF-IMC

9.2.1　常量值

9.2.1.1　IF-IMC 的功能函数结果状态码

IF-IMC 的功能函数结果状态码如表 5 所示。

表 5　IF-IMC 的功能函数结果状态码

IF-IMC 的功能函数结果状态码	标识符	描　　述
TCA_RESULT_SUCCESS	0x00000001	功能函数成功完成
TCA_RESULT_NOT_INITIALIZED	0x00000002	TCA_IMC_Initialize 还没有被调用
TCA_RESULT_ALREADY_INITIALIZED	0x00000003	在调用 TCA_IMC_Terminate 之前已调用两次 TCA_IMC_Initialize

表 5（续）

IF-IMC 的功能函数结果状态码	标识符	描　　述
TCA_RESULT_NO_COMMON_VERSION	0x00000004	在 IMC 和 TNCC(或 TNCAP)之间不存在共同的 IF-IMC 应用接口函数版本
TCA_RESULT_CANT_RETRY	0x00000005	TNCC(或 TNCAP)不能执行下一个平台鉴别过程
TCA_RESULT_WONT_RETRY	0x00000006	TNCC(或 TNCAP)拒绝执行下一个平台鉴别过程
TCA_RESULT_INVALID_PARAMETER	0x00000007	功能函数的参数无效
—	0x00000008～0xffffffff	保留

9.2.1.2　IF-IMC 应用接口函数版本号

IF-IMC 应用接口函数版本号如下：

1　TCA_IFIMC_Version_1，表示本标准规定的 IF-IMC 应用接口函数版本号；

其他值保留。

9.2.1.3　网络连接状态值

网络连接状态值如表 6 所示。

表 6　网络连接状态值

网络连接状态值	标　识　符	描　　述
TCA_CONNECTION_STATE_CREATE	0x00000001	创建网络连接
TCA_CONNECTION_STATE_HANDSHAKE	0x00000002	开始执行一个平台鉴别过程
TCA_CONNECTION_STATE_ACCESS_ALLOWED	0x00000003	网络连接状态为允许
TCA_CONNECTION_STATE_ACCESS_ISOLATED	0x00000004	网络连接状态为隔离
TCA_CONNECTION_STATE_ACCESS_NONE	0x00000005	网络连接状态为禁止
TCA_CONNECTION_STATE_DELETE	0x00000006	删除 ConnectionID，并断开连接
—	0x00000007～0xffffffff	保留

9.2.1.4　执行下一个平台鉴别过程的原因值

执行下一个平台鉴别过程的原因值如表 7 所示。

表 7　执行下一个平台鉴别过程的原因值

执行下一个平台鉴别过程的原因值	标　识　符	描　　述
TCA_RETRY_REASON_IMC_REMEDIATION_COMPLETE	0x00000001	IMC 已经完成平台修补
—	0x00000002～0xffffffff	保留

9.2.2 AR 中的 IF-IMC

9.2.2.1 AR 中的 IF-IMC 功能函数

AR 中的 IF-IMC 定义如下功能函数。

9.2.2.1.1 TCA_IMC_Initialize

TCA_IMC_Initialize{imcID,minVersion,maxVersion,*pOutActualVersion},用于初始化 AR 中的一个 IMC,由该 IMC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCC 为该 IMC 分配的 IMC 标识。

——minVersion 长度为 4 个八位位组,整型数据,表示 TNCC 支持的应用接口函数次版本号。

——maxVersion 长度为 4 个八位位组,整型数据,表示 TNCC 支持的应用接口函数主版本号。

——*pOutActualVersion 长度为 8 个八位位组,表示 TNCC 实际使用的应用接口函数版本号,包括主版本号和次版本号。

TCA_IMC_Initialize 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_ALREADY_INITIALIZED,TCA_RESULT_NO_COMMON_VERSION,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.2 TCA_TNCC_ReportMessageTypes

TCA_TNCC_ReportMessageTypes{imcID,typeCount,supportedTypes},用于 AR 中的一个 IMC 向 TNCC 通告它所支持的消息类型,由 TNCC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCC 为该 IMC 分配的 IMC 标识。

——typeCount 长度为 2 个八位位组,整型数据,表示该 IMC 所支持的消息类型的数目。

——supportedTypes 长度为可变,表示该 IMC 所支持的各个消息类型,每个消息类型由组件类型厂家 ID 和组件类型。

TCA_TNCC_ReportMessageTypes 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.3 TCA_IMC_Terminate

TCA_IMC_Terminate{imcID},用于 TNCC 终止 AR 中的一个 IMC,由该 IMC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCC 为该 IMC 分配的 IMC 标识。

TCA_IMC_Terminate 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_NOT_INITIALIZED,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.4 TCA_IMC_NotifyConnectionChange

TCA_IMC_NotifyConnectionChange{imcID,connectionID,newState},用于 TNCC 向 AR 中的一个 IMC 通告网络连接状态,由该 IMC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCC 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组,整型数据,表示 TNCC 创建的网络连接标识,用于标识每一对 TNCC 和 TNCAP 的网络连接。

——newState 长度为 2 个八位位组,表示网络连接状态。

TCA_IMC_NotifyConnectionChange 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_NOT_INITIALIZED,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.5 TCA_IMC_RequestMeasurementInfo

TCA_IMC_RequestMeasurementInfo{imcID,connectionID,messageType,yn,nonce, componentAttributeCount,componentAttributes},用于 TNCC 向 AR 中的一个 IMC 请求执行平台完整性度量,由该 IMC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCC 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组,整型数据,表示 TNCC 创建的网络连接标识,用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组,表示消息类型,由组件类型厂家 ID 和组件类型构成。

——yn 为布尔值。

——nonce 长度为 32 个八位位组,表示随机数。

——componentAttributeCount 长度为 2 个八位位组,整型数据,表示组件属性级平台完整性度量请求参数条目数。

——componentAttributes 长度可变,表示各个组件属性级平台完整性度量请求参数条目。

当 yn 的值为 0 时,nonce 的值为 NULL。当 yn 的值为 1 时,nonce 的值为 TNCAP 挑战。

当 TCA_IMC_RequestMeasurementInfo 用于 PAI-1 协议时,yn 的值设置为 1。当 TCA_IMC_RequestMeasurementInfo 用于 PAI-2 协议时,yn 的值设置为 0。

TCA_IMC_RequestMeasurementInfo 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_NOT_INITIALIZED,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.6 TCA_TNCC_ProvideQuoteData

TCA_TNCC_ProvideQuoteData{imcID,connectionID,messageType,yn,quoteData},用于 AR 中的一个 IMC 向 TNCC 提供一个 IF-IM 消息对应的 Quote 数据,由 TNCC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCC 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组,整型数据,表示 TNCC 创建的网络连接标识,用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组,定义如前。

——yn 为布尔值。

——quoteData 长度可变,表示该 IF-IM 消息对应的 Quote 数据。

当 yn 的值为 0 时,即该 IF-IM 消息不包含 Quote 数据,quoteData 的值为 NULL。

TCA_TNCC_ProvideQuoteData 功能函数用于 PAI-1 协议。在本标准中,若该 IF-IM 消息中包含一个完整性报告的 IF-IM 属性,则该 IF-IM 消息包含 Quote 数据。

TCA_TNCC_ProvideQuoteData 的功能函数结果状态码为 TCA_RESULT_SUCCESS, TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.7 TCA_TNCC_ProvideReportIndex

TCA_TNCC_ProvideReportIndex{imcID,connectionID,messageType,yn,reportIndex},用于 AR 中的一个 IMC 向 TNCC 提供一个 IF-IM 消息对应的完整性报告索引信息,由 TNCC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCC 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组,整型数据,表示 TNCC 创建的网络连接标识,用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组,定义如前。

——yn 为布尔值。

——reportIndex 长度可变，为该 IF-IM 消息对应的完整性报告索引信息。

当 yn 的值为 0 时，reportIndex 的值为 NULL。

TCA_TNCC_ProvideReportIndex 用于 PAI-2 协议。在本标准中，若该 IF-IM 消息中包含一个完整性报告索引信息的 IF-IM 属性，则该 IF-IM 消息包含完整性报告索引信息。

TCA_TNCC_ProvideReportIndex 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.8 TCA_TNCC_SendMessage

TCA_TNCC_SendMessage{imcID，connectionID，messageType，message}，用于 AR 中的一个 IMC 向 TNCC 发送一个 IF-IM 消息，由 TNCC 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCC 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCC 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组，定义如前。

——messgae 长度可变，为 IF-IM 消息。

TCA_TNCC_SendMessage 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.9 TCA_IMC_ReceiveMessage

TCA_IMC_ReceiveMessage{imcID，connectionID，messageType，message}，用于 TNCC 向 AR 中的一个 IMC 发送已收到的 IF-IM 消息，由该 IMC 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCC 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCC 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组，定义如前。

——messgae 长度可变，定义如前。

TCA_IMC_ReceiveMessage 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.1.10 TCA_TNCC_RequestHandshakeRetry

TCA_TNCC_RequestHandshakeRetry{imcID，connectionID，reason}，用于 AR 中的一个 IMC 向 TNCC 请求执行下一个平台鉴别过程，由 TNCC 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCC 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCC 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——reason 长度为 2 个八位位组，为请求执行下一个平台鉴别过程的原因值。

TCA_TNCC_RequestHandshakeRetry 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_CANT_RETRY，TCA_RESULT_WONT_RETRY，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.2.2 AR 中的 IF-IMC 交互示意图

AR 中的 IF-IMC 交互示意图如图 89 所示。

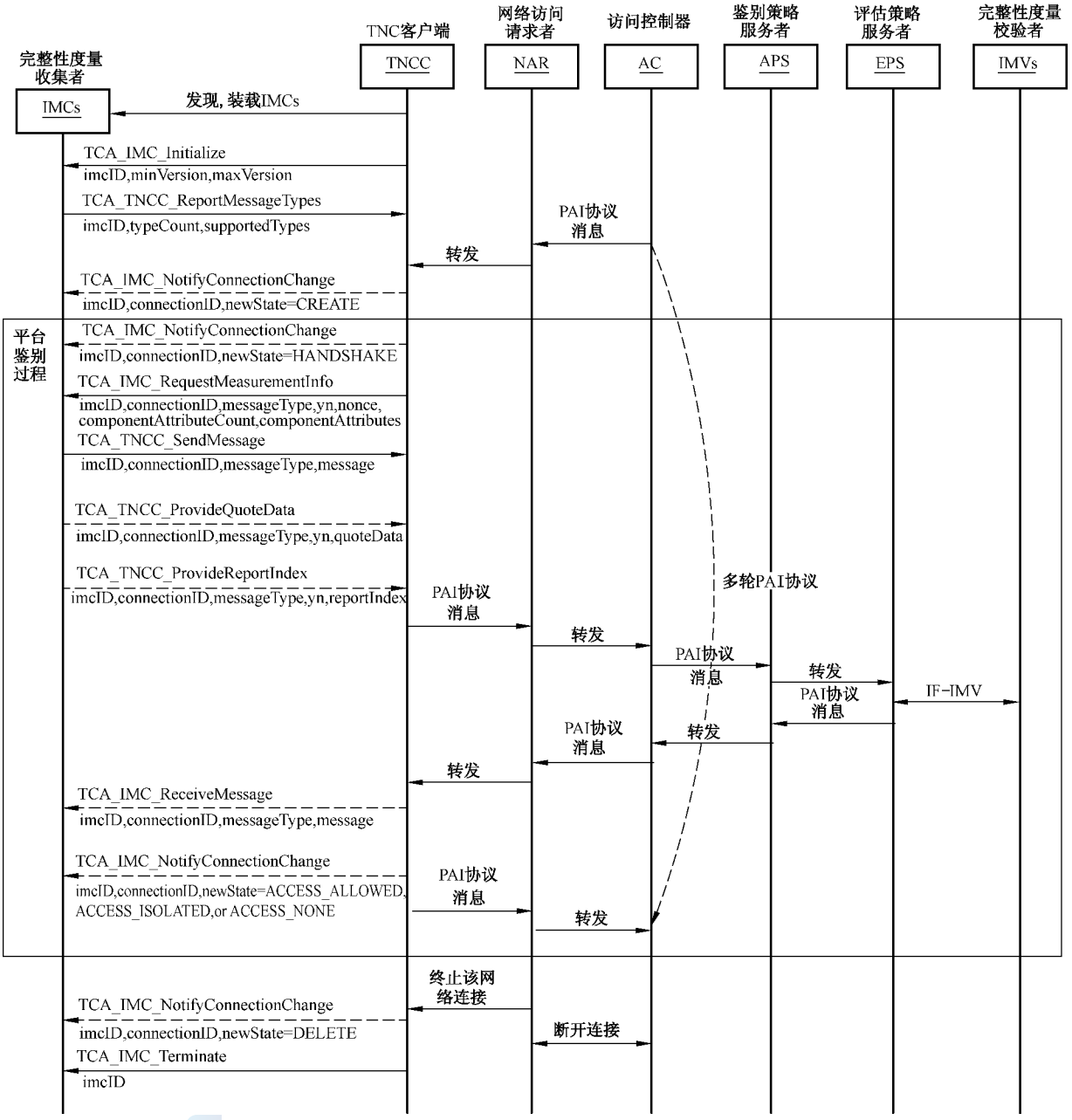

图 89　AR 中的 IF-IMC 交互示意图

在图 89 中，AR 中 IF-IMC 的虚线功能函数调用箭头表示可选的，而实线功能函数调用箭头表示必备的，一个平台鉴别过程中的 PAI 协议可以是多轮次的。图 89 中的 TCA_TNCC_ProvideQuoteData 函数仅用于 PAI-1 协议，而 TCA_TNCC_ProvideReportIndex 函数仅用于 PAI-2 协议。

9.2.3　AC 中的 IF-IMC

9.2.3.1　AC 中的 IF-IMC 功能函数

AC 中的 IF-IMC 定义如下功能函数。

9.2.3.1.1 TCA_IMC_Initialize

TCA_IMC_Initialize{imcID,minVersion,maxVersion,*pOutActualVersion},用于初始化 AC 中的一个 IMC,由该 IMC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCAP 为该 IMC 分配的 IMC 标识。

——minVersion 长度为 4 个八位位组,整型数据,表示 TNCAP 支持的应用接口函数次版本号。

——maxVersion 长度为 4 个八位位组,整型数据,表示 TNCAP 支持的应用接口函数主版本号。

——*pOutActualVersion 长度为 8 个八位位组,表示 TNCAP 实际使用的应用接口函数版本号,包括主版本号和次版本号。

TCA_IMC_Initialize 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_ALREADY_INITIALIZED,TCA_RESULT_NO_COMMON_VERSION,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.2 TCA_TNCAP_ReportMessageTypes

TCA_TNCAP_ReportMessageTypes{imcID,typeCount,supportedTypes},用于 AC 中的一个 IMC 向 TNCAP 通告它所支持的消息类型,由 TNCAP 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCAP 为该 IMC 分配的 IMC 标识。

——typeCount 长度为 2 个八位位组,整型数据,表示该 IMC 所支持的消息类型的数目。

——supportedTypes 长度为可变,表示该 IMC 所支持的各个消息类型,每个消息类型由组件类型厂家 ID 和组件类型。

TCA_TNCAP_ReportMessageTypes 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.3 TCA_IMC_Terminate

TCA_IMC_Terminate{imcID},用于 TNCAP 终止 AC 中的一个 IMC,由该 IMC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCAP 为该 IMC 分配的 IMC 标识。

TCA_IMC_Terminate 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_NOT_INITIALIZED,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.4 TCA_IMC_NotifyConnectionChange

TCA_IMC_NotifyConnectionChange{imcID,connectionID,newState},用于 TNCAP 向 AC 中的一个 IMC 通告网络连接状态,由该 IMC 实现。

——imcID 长度为 2 个八位位组,整型数据,表示 TNCAP 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组,整型数据,表示 TNCC 创建的网络连接标识,用于标识每一对 TNCC 和 TNCAP 的网络连接。

——newState 长度为 2 个八位位组,表示网络连接状态。

TCA_IMC_NotifyConnectionChange 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_NOT_INITIALIZED,TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.5 TCA_IMC_RequestMeasurementInfo

TCA_IMC_RequestMeasurementInfo{imcID,connectionID,messageType,yn,nonce,componentAttributeCount,componentAttributes},用于 TNCAP 向 AC 中的一个 IMC 请求执行平台完整性度量,由该 IMC 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCAP 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCAP 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组，表示消息类型，由组件类型厂家 ID 和组件类型构成。

——yn 为布尔值。

——nonce 长度为 32 个八位位组，表示随机数。

——componentAttributeCount 长度为 2 个八位位组，整型数据，表示组件属性级平台完整性度量请求参数条目数。

——componentAttributes 长度可变，表示各个组件属性级平台完整性度量请求参数条目。

当 yn 的值为 0 时，nonce 的值为 NULL。当 yn 的值为 1 时，nonce 的值为 TNCC 挑战。

当 TCA_IMC_RequestMeasurementInfo 用于 PAI-1 协议时，yn 的值设置为 1。当 TCA_IMC_RequestMeasurementInfo 用于 PAI-2 协议时，yn 的值设置为 0。

TCA_IMC_RequestMeasurementInfo 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_NOT_INITIALIZED，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.6 TCA_TNCAP_ProvideQuoteData

TCA_TNCAP_ProvideQuoteData{imcID，connectionID，messageType，yn，quoteData}，用于 AC 中的一个 IMC 向 TNCAP 提供一个 IF-IM 消息对应的 Quote 数据，由 TNCAP 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCAP 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCAP 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组，定义如前。

——yn 为布尔值。

——quoteData 长度可变，表示该 IF-IM 消息对应的 Quote 数据。

当 yn 的值为 0 时，即该 IF-IM 消息不包含 Quote 数据，quoteData 的值为 NULL。

TCA_TNCAP_ProvideQuoteData 功能函数用于 PAI-1 协议。在本标准中，若该 IF-IM 消息中包含一个完整性报告的 IF-IM 属性，则该 IF-IM 消息包含 Quote 数据。

TCA_TNCAP_ProvideQuoteData 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.7 TCA_TNCAP_ProvideReportIndex

TCA_TNCAP_ProvideReportIndex{imcID，connectionID，messageType，yn，reportIndex}，用于 AC 中的一个 IMC 向 TNCAP 提供一个 IF-IM 消息对应的完整性报告索引信息，由 TNCAP 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCAP 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCAP 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组，定义如前。

——yn 为布尔值。

——reportIndex 长度可变，为该 IF-IM 消息对应的完整性报告索引信息。

当 yn 的值为 0 时，reportIndex 的值为 NULL。

TCA_TNCC_ProvideReportIndex 用于 PAI-2 协议。在本标准中，若该 IF-IM 消息中包含一个完

整性报告索引信息的 IF-IM 属性，则该 IF-IM 消息包含完整性报告索引信息。

TCA_TNCC_ProvideReportIndex 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.8 TCA_TNCAP_SendMessage

TCA_TNCAP_SendMessage{imcID，connectionID，messageType，message}，用于 AC 中的一个 IMC 向 TNCAP 发送一个 IF-IM 消息，由 TNCAP 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCAP 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCAP 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组，定义如前。

——messgae 长度可变，为 IF-IM 消息。

TCA_TNCAP_SendMessage 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.9 TCA_IMC_ReceiveMessage

TCA_IMC_ReceiveMessage{imcID，connectionID，messageType，message}，用于 TNCAP 向 AC 中的一个 IMC 发送已收到的 IF-IM 消息，由该 IMC 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCAP 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCAP 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——messageType 长度为 7 个八位位组，定义如前。

——messgae 长度可变，为 IF-IM 消息。

TCA_IMC_ReceiveMessage 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.1.10 TCA_TNCAP_RequestHandshakeRetry

TCA_TNCAP_RequestHandshakeRetry{imcID，connectionID，reason}，用于 AC 中的一个 IMC 向 TNCAP 请求执行下一个平台鉴别过程，由 TNCAP 实现。

——imcID 长度为 2 个八位位组，整型数据，表示 TNCAP 为该 IMC 分配的 IMC 标识。

——connectionID 长度为 2 个八位位组，整型数据，表示 TNCAP 创建的网络连接标识，用于标识每一对 TNCC 和 TNCAP 的网络连接。

——reason 长度为 2 个八位位组，为请求执行下一个平台鉴别过程的原因值。

TCA_TNCAP_RequestHandshakeRetry 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_CANT_RETRY，TCA_RESULT_WONT_RETRY，TCA_RESULT_INVALID_PARAMETER 或其他。

9.2.3.2 AC 中的 IF-IMC 交互示意图

AC 中的 IF-IMC 交互示意图如图 90 所示。

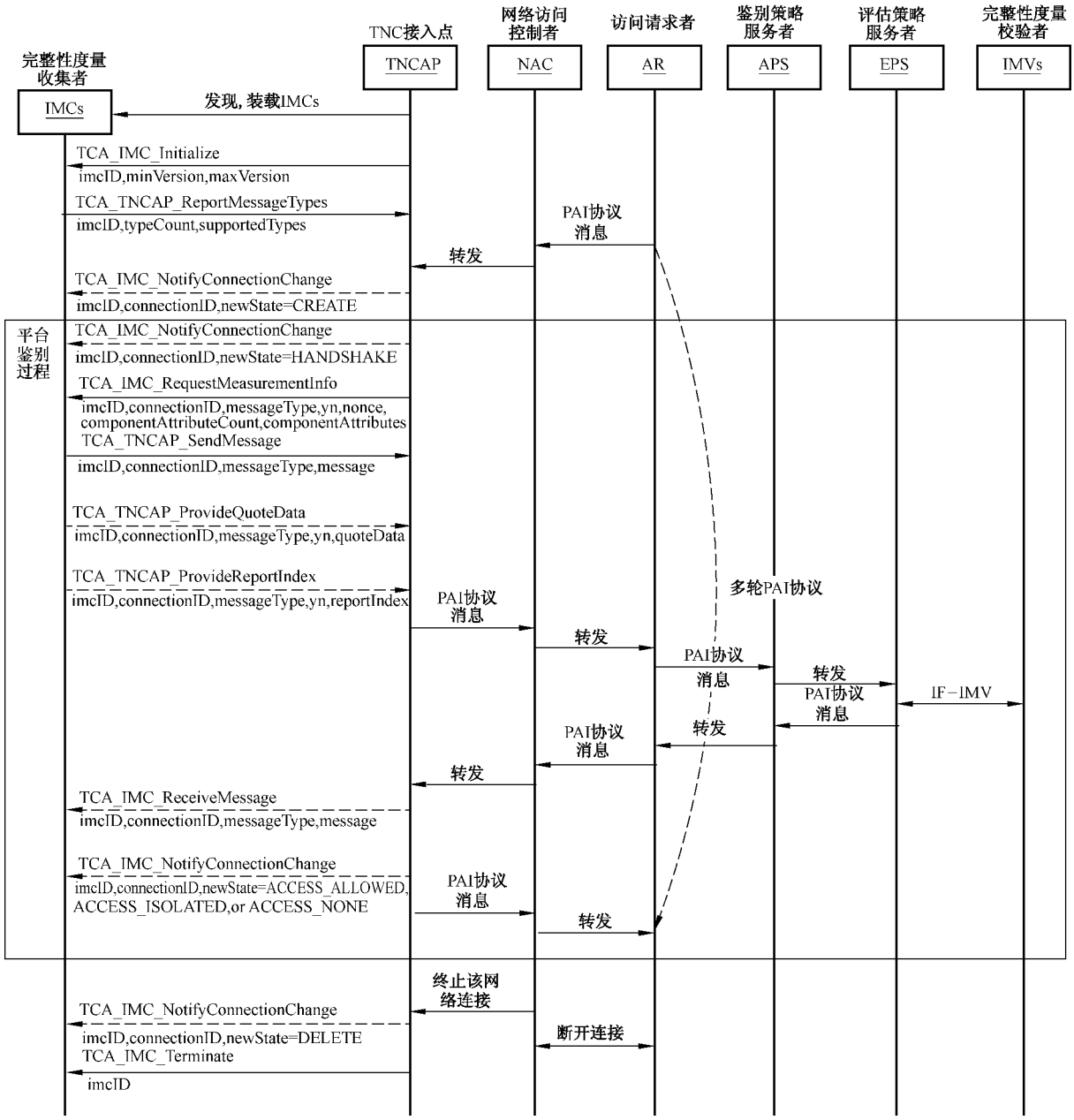

图 90　AC 中的 IF-IMC 交互示意图

在图 90 中，AC 中 IF-IMC 的虚线功能函数调用箭头表示可选的，而实线功能函数调用箭头表示必备的，平台鉴别过程中的 PAI 协议可以是多轮次的。图 90 中的 TCA_TNCAP_ProvideQuoteData 函数仅用于 PAI-1 协议，而 TCA_TNCAP_ProvideReportIndex 函数仅用于 PAI-2 协议。

9.3　IF-IMV

9.3.1　常量值

9.3.1.1　IF-IMV 的功能函数结果状态码

IF-IMV 的功能函数结果状态码如表 8 所示。

表 8　IF-IMV 的功能函数结果状态码

IF-IMV 的功能函数结果状态码	标　识　符	描　　述
TCA_RESULT_SUCCESS	0x00000001	功能函数成功完成
TCA_RESULT_NOT_INITIALIZED	0x00000002	TCA_IMV_Initialize 还没有被调用
TCA_RESULT_ALREADY_INITIALIZED	0x00000003	在调用 TCA_IMV_Terminate 之前已调用两次 TCA_IMV_Initialize
TCA_RESULT_NO_COMMON_VERSION	0x00000004	在 IMV 和 EPS 之间不存在共同的 IF-IMV 应用接口函数版本
TCA_RESULT_INVALID_PARAMETER	0x00000005	函数参数的参数无效
—	0x00000006～0xffffffff	保留

9.3.1.2　IF-IMV 应用接口函数版本号

IF-IMV 应用接口函数版本号如下：

1　TCA_IFIMV_Version_1，表示本标准规定的 IF-IMV 应用接口函数版本号；

其他值保留。

9.3.2　功能函数

IF-IMV 定义如下功能函数。

9.3.2.1　TCA_IMV_Initialize

TCA_IMV_Initialize{imvID，minVersion，maxVersion，* pOutActualVersion}，用于初始化 PM 中的一个 IMV，由该 IMV 实现。

——imvID 长度为 2 个八位位组，整型数据，表示 EPS 为该 IMV 分配的 IMV 标识。

——minVersion 长度为 4 个八位位组，整型数据，表示 EPS 支持的应用接口函数次版本号。

——maxVersion 长度为 4 个八位位组，整型数据，表示 EPS 支持的应用接口函数主版本号。

——* pOutActualVersion 长度为 8 个八位位组，表示 EPS 实际使用的应用接口函数版本号，包括主版本号和次版本号。

TCA_IMV_Initialize 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_ALREADY_INITIALIZED，TCA_RESULT_NO_COMMON_VERSION，TCA_RESULT_INVALID_PARAMETER 或其他。

9.3.2.2　TCA_EPS_ReportMessageTypes

TCA_EPS_ReportMessageTypes{imvID，typeCount，supportedTypes}，用于 PM 中的一个 IMV 向 EPS 通告所支持的消息类型，由 EPS 实现。

——imvID 长度为 2 个八位位组，整型数据，表示 EPS 为该 IMV 分配的 IMV 标识。

——typeCount 长度为 2 个八位位组，整型数据，表示该 IMV 所支持的消息类型的数目。

——supportedTypes 长度为可变，表示该 IMV 所支持的各个消息类型，每个消息类型由组件类型厂家 ID 和组件类型。

TCA_EPS_ReportMessageTypes 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.3.2.3 TCA_IMV_Terminate

TCA_IMV_Terminate{imvID},用于 EPS 终止 PM 中的一个 IMV,由该 IMV 实现。

——imvID 长度为 2 个八位位组,整型数据,表示 EPS 为该 IMV 分配的 IMV 标识。

TCA_IMV_Terminate 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_NOT_INITIALIZED,TCA_RESULT_INVALID_PARAMETER 或其他。

9.3.2.4 TCA_IMV_RequestEvaluationInfo

TCA_IMV_RequestEvaluationInfo{imvID,paiBindingID,entityRole,messageType,yn,yn2,componentEvaluationPolicyNum, componentEvaluationPolicy, componentProtectedPolicyCount, componentProtectedPolicies,componentMeasurementCount,componentMeasurements,report},用于 EPS 向 PM 中的一个 IMV 请求执行平台完整性评估,由 PM 中的 IMV 实现。

——imvID 长度为 2 个八位位组,整型数据,表示 EPS 为该 IMV 分配的 IMV 标识。

——paiBindingID 长度为 2 个八位位组,整型数据,表示 EPS 为一轮 PAI 协议生成的 PAI 协议标识。

——entityRole 为布尔值,表示实体角色。

——messageType 长度为 7 个八位位组,表示消息类型,由组件类型厂家 ID 和组件类型构成。

——yn 为布尔值。

——yn2 为布尔值。

——componentEvaluationPolicy 长度可变,为一个组件产品级平台完整性评估策略条目。

——componentEvaluationPolicyNum 长度为 2 个八位位组,整型数据,为 componentEvaluationPolicy 所对应的条目序号。

——componentProtectedPolicyCount 长度为 2 个八位位组,整型数据,为组件产品级平台配置保护策略条目数。

——componentProtectedPolicies 长度可变,为各个组件产品级平台配置保护策略条目。

——componentMeasurementCount 长度 2 个八位位组,整型数据,为 IF-IM 级平台完整性度量值条目数。

——componentMeasurements 长度可变,为各个 IF-IM 级平台完整性度量值条目。

——report 长度可变,为一个完整性报告。

当 yn 的值为 0 时,则 componentProtectedPolicyCount 和 componentProtectedPolicies 的值都为 NULL。当 yn2 的值为 0 时,则 report 的值为 NULL。

当 entityRole 的值为 0 时,表示实体角色为 AR。当 entityRole 的值为 1 时,表示实体角色为 AC。

当 TCA_IMV_RequestEvaluationInfo 用于 PAI-1 协议时,yn2 的值设置为 0。当 TCA_IMV_RequestEvaluationInfo 用于 PAI-2 协议时,yn2 的值设置为 0 或 1。

TCA_IMV_RequestEvaluationInfo 的功能函数结果状态码为 TCA_RESULT_SUCCESS,TCA_RESULT_NOT_INITIALIZED,TCA_RESULT_INVALID_PARAMETER 或其他。

9.3.2.5 TCA_EPS_ProvideEvaluationResult

TCA_EPS_ProvideEvaluationResult{imvID,paibindingID,entityRole,messageType, yn,componentEvaluationPolicyNum,componentEvaluationResult,ifimRemediationInfo,componentErrorInfo,ifimQuoteData,nextComponentEvaluationPolicy},用于 PM 中的一个 IMV 向 EPS 提供一个组件产品级平台完整性评估结果、一个 IF-IM 级平台修补信息条目、一个组件产品级错误原因信息条目、一个 IF-IM 级 Quote 数据值条目和一个用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目,

由 EPS 实现。

——imvID 长度为 2 个八位位组，整型数据，表示 EPS 为该 IMV 分配的 IMV 标识。

——paiBindingID 长度为 2 个八位位组，整型数据，表示 EPS 为一轮 PAI 协议生成的 PAI 协议标识。

——entityRole 为布尔值，表示实体角色。

——messageType 长度为 7 个八位位组，表示消息类型，由组件类型厂家 ID 和组件类型构成。

——yn 为布尔值。

——componentEvaluationPolicyNum 长度为 2 个八位位组，整型数据，为一个组件产品级平台完整性评估策略条目对应的条目序号。

——componentEvaluationResult 长度为 1 个位位组，整型数据，为一个组件产品级平台完整性评估结果。

——ifimRemediationInfo 长度可变，为一个 IF-IM 级平台修补信息条目。

——componentErrorInfo 长度可变，为一个组件产品级错误原因信息条目。

——ifimQuoteData 长度可变，为一个 IF-IM 级 Quote 数据值条目。

——nextComponentEvaluationPolicy 长度可变，为一个用于下一个平台鉴别过程的组件产品级平台完整性评估策略条目。

当 yn 的值为 0 时，ifimQuoteData 的值为 NULL。

当 componentEvaluationResult 的值为 1 时，ifimRemediationInfo、componentErrorInfo 和 nextComponentEvaluationPolicy 的值为 NULL。当 componentEvaluationResult 的值为 2 时，componentErrorInfo 的值为 NULL。当 componentEvaluationResult 的值为 3 时，ifimRemediationInfo 和 nextComponentEvaluationPolicy 的值为 NULL。当 componentEvaluationResult 的值为 4 时，ifimRemediationInfo、componentErrorInfo 和 nextComponentEvaluationPolicy 的值为 NULL。

当 TCA_EPS_ProvideEvaluationResult 用于 PAI-1 协议时，yn 的值设置为 0 或 1。当 TCA_EPS_ProvideEvaluationResult 用于 PAI-2 协议时，yn 的值设置为 0。

TCA_EPS_ProvideEvaluationResult 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_INVALID_PARAMETER 或其他。

9.3.2.6 TCA_IMV_EndEvaluation

TCA_IMV_EndEvaluation{imvID，paiBindingID，entityRole，messageType}，用于 EPS 向 PM 中的一个 IMV 请求终止平台完整性评估，由 PM 中的 IMV 实现。

——imvID 长度为 2 个八位位组，整型数据，表示 EPS 为该 IMV 分配的 IMV 标识。

——paiBindingID 长度为 2 个八位位组，整型数据，表示 EPS 为一轮 PAI 协议生成的 PAI 协议标识。

——entityRole 为布尔值，表示实体角色。

——messageType 长度为 7 个八位位组，表示消息类型，由组件类型厂家 ID 和组件类型构成。

当 TCA_IMV_EndEvaluation 被用于请求终止对一个实体的平台完整性评估时，messageType 的值为 NULL。

TCA_IMV_EndEvaluation 的功能函数结果状态码为 TCA_RESULT_SUCCESS，TCA_RESULT_NOT_INITIALIZED，TCA_RESUsLT_INVALID_PARAMETER 或其他。

9.3.3 交互示意图

IF-IMV 交互示意图如图 91 所示。

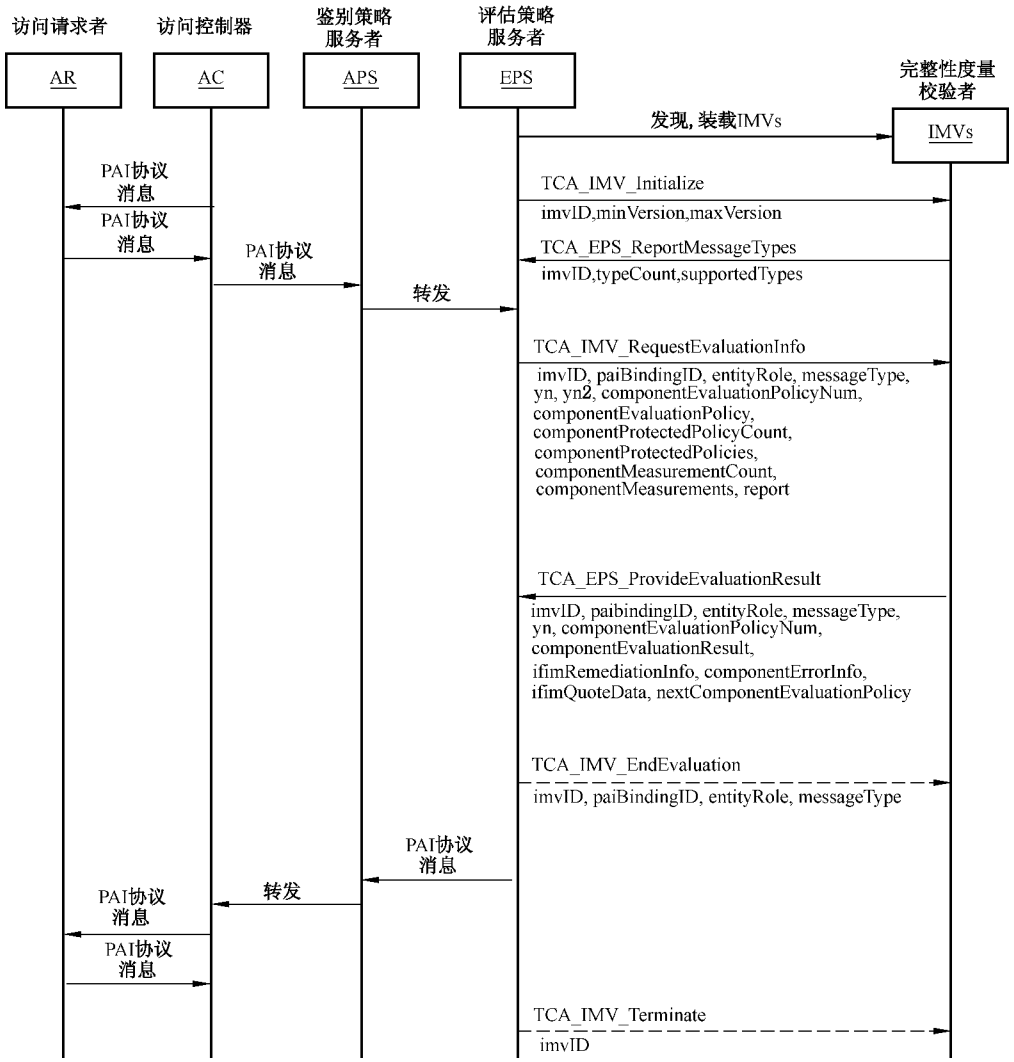

图 91　IF-IMV 交互示意图

在图 91 中，IF-IMV 的虚线功能函数调用箭头表示可选的，而实线功能函数调用箭头表示必备的。在一轮 PAI 协议中，一个 IMV 和 EPS 之间可能需要执行多次 TCA_IMV_RequestEvaluationInfo、TCA_EPS_ProvideEvaluationResult 和 TCA_IMV_EndEvaluation。

附 录 A
（资料性附录）
完整性管理框架

A.1 概述

在可信计算体系结构中，信任链扩展基于平台各组件的完整性：通过对平台组件自底向上逐层进行完整性度量，将度量结果与完整性参照值进行比较，以保证平台的可信性。平台各组件完整性参照值是可信度量的基准值，而管理框架抽象平台各组件完整性参照值的制作、发布、获取的过程。

A.2 完整性管理框架

完整性管理包括三部分内容：完整性参照值计算、授权和分发；完整性度量；完整性报告与验证。完整性管理框架如图 A.1 所示。

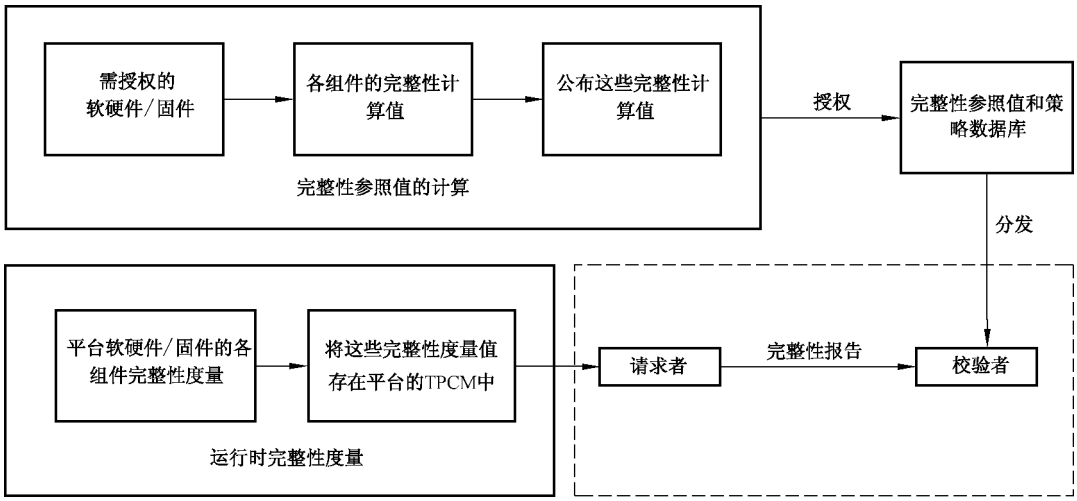

图 A.1 完整性管理框架

A.3 完整性参照值计算、授权和分发

生产厂商必须根据完整性参照值的制定规则，为生产的组件进行完整性度量，并按照完整性参照值发布的格式，填写度量值、相应的度量值说明（例如，组件名称、版本、制定时间、厂商等信息）并进行签名。

完整性参照值可由单个厂商发布，也可由某组织在收集各个厂商发布的完整性参照值后进行发布，但该组织需制定统一的完整性参照值目录或数据库，并向用户提供完整性校验服务。

用户进行完整性校验时，可采用厂商获取的方式或者从某组织的完整性参照值目录或数据库中获取所需的标准完整性参照值。可信计算平台安全启动过程中所需的完整性参照值必须在平台制造过程中，由各厂商或集成商获取相应的完整性参照值后存储在平台内部。如，对 BIOS、IPL 和 Option ROM 的完整性基准值保存在 TPCM 中，而操作系统、应用程序的完整性基准值保存在硬盘受保护区域中。

A.4 完整性度量

完整性度量指利用杂凑算法对可信计算平台各组件进行度量得到杂凑值的过程。完整性度量过程必须对从开机运行到应用程序加载的整个过程中，涉及的所有可信计算平台组件进行度量，并将度量值存放在 PCR 中。鉴于 PCR 数量有限，而平台组件众多，因此须将平台组件分类以对应不同的 PCR；由于 PCR 对完整性度量值进行迭代，为了进行完整性报告，需将度量过程中的每步度量结果存贮在 SML 中，以便验证者对完整性度量过程的所有细节进行验证。

A.5 完整性报告与验证过程

完整性报告实现将可信计算平台自身的完整性度量结果报告给请求者，以便向请求者报告自身的完整性状态。请求者根据提供者的完整性报告，结合完整性基准值进行验证。完整性报告与验证流程如下：

a) 请求者向提供者请求完整性报告；
b) 提供者的 TPCM 将 PCR 值使用身份证书进行签名；
c) 提供者将签名的 PCR 值和 SML 发送给请求者；
d) 请求者接收到提供者的数据，完整性报告过程结束；
e) 请求者验证提供者身份证书的有效性，如果无效，提供者平台不可信，退出；
f) 请求者根据 SML 计算得到 PCR 值，将其与提供者提供的 PCR 值进行比较，如果不一致，提供者平台不可信，退出；
g) 请求者根据 SML 向完整性参考服务器请求标准的完整性基准值，将 SML 中的值和标准的完整性参照值进行比较，如果不一致，提供者平台不可信，退出；
h) 提供者平台状态为可信，完整性报告与验证流程结束。

附 录 B
（资料性附录）
安全策略管理框架

B.1 概述

安全策略管理包括：安全策略的制定、分发与执行等。参与安全策略管理的实体包括：策略服务器和策略执行点。策略服务器负责制定和分发安全策略，而策略执行点负责执行由策略服务器制定并分发的安全策略。安全策略的管理需要一套策略分发协议和信任机制，保证策略传输的可靠性和安全性。安全策略管理框架如图 B.1 所示。

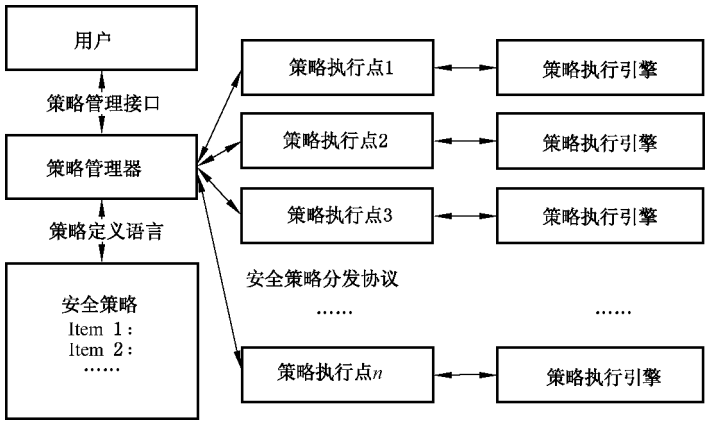

图 B.1 安全策略管理框架

B.2 策略管理器的基本功能

策略管理器的基本功能包括定义、编辑和管理策略。用户可以在策略管理器上通过策略管理接口和策略描述语言定义和编辑安全策略，策略管理器接口负责将这些安全策略使用策略语言进行描述，并检查策略语言的语法。在策略制定之后，按照策略分发协议将策略分发给策略执行点进行执行。

B.3 策略执行点的基本功能

策略执行点的基本功能是严格执行策略管理器下发的安全策略，利用安全策略分发协议保证接受的安全策略保密性、抗抵赖性和完整性，并调用策略执行引擎执行安全策略。

B.4 安全策略分发协议的基本功能

安全策略分发协议保证安全策略在策略管理器和策略执行点之间的安全传输。安全策略分发协议包括推策略和拉 策略两种。推策略由策略管理器将策略强制推行到各策略执行点，并保证策略执行点只接收来自策略管理器的策略。拉策略由策略执行点主动向策略管理器申请策略，策略管理器认证策略执行点的请求后将相应策略进行分发。安全策略分发协议必须实现策略管理器和策略执行点之间的

双向认证，并保证策略分发的保密性、抗抵赖性和完整性。

B.5 策略定义语言

策略定义语言是用于定义安全策略的语言。用户通过策略管理接口需对安全策略进行直观地描述，并使用策略语言编译功能将直观的安全策略转换为策略执行引擎可直接执行的安全策略。策略定义语言与认证、授权、访问控制等因素相关。

B.6 安全策略管理流程

安全策略管理的处理流程如下：

首先，策略管理器制定安全策略。即用户通过策略管理接口将安全策略进行直观地描述，继而利用策略语言编译功能将直观的安全策略转换为策略执行引擎可直接执行的安全策略。

其次，策略制定后，安全策略分发协议通过推策略和拉策略，保证安全策略在策略管理器和策略执行点之间的安全传输，实现策略管理器和策略执行点之间的双向认证。

最后，安全策略在策略执行点被执行。

附 录 C
（资料性附录）
数字信封

数字信封是公钥密码体制在实际中的一个应用，是用加密技术来保证只有规定的特定收信人才能阅读通信的内容。

在数字信封中，信息发送方采用对称密钥来加密信息内容，然后将此对称密钥用接收方的公开密钥来加密（这部分称数字信封）之后，将它和加密后的信息一起发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开加密信息。这种技术的安全性相当高。数字信封包括数字信封打包和数字信封拆解，数字信封打包是使用对方的公钥将加密密钥进行加密的过程，只有对方的私钥才能将加密后的数据（通信密钥）还原；数字信封拆解是使用私钥将加密过的数据解密的过程。数字信封的生成和解开过程如图 C.1 所示。

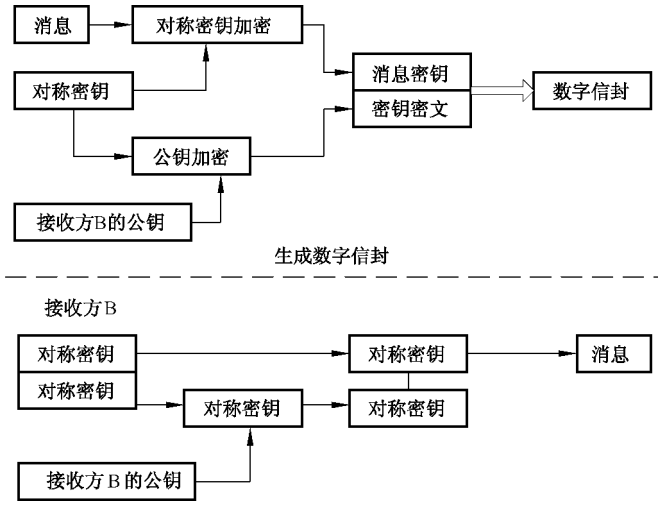

图 C.1 数字信封的生成和解开

数字信封的功能类似于普通信封，普通信封在法律的约束下保证只有收信人才能阅读信的内容；数字信封则采用密码技术保证了只有规定的接收人才能阅读信息的内容。数字信封中采用了对称密码体制和公钥密码体制。信息发送者首先利用随机产生的对称密码加密信息，再利用接收方的公钥加密对称密码，被公钥加密后的对称密码被称之为数字信封。在传递信息时，信息接收方若要解密信息，必须先用自己的私钥解密数字信封，得到对称密码，才能利用对称密码解密所得到的信息。这样就保证了数据传输的保密性、抗抵赖性和完整性。

在一些重要的电子商务交易中密钥必须经常更换，为了解决每次更换密钥的问题，结合对称加密技术和公开密钥技术的优点，它克服了秘密密钥加密中秘密密钥分发困难和公开密钥加密中加密时间长的问题，使用两个层次的加密来获得公开密钥技术的灵活性和秘密密钥技术高效性。信息发送方使用密码对信息进行加密，从而保证只有规定的收信人才能阅读信的内容。采用数字信封技术后，即使加密文件被他人非法截获，因为截获者无法得到发送方的通信密钥，故不可能对文件进行解密。

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 可信计算规范
可信连接架构
GB/T 29828—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014 年 4 月第一版
*
书号:155066·1-48211

GB/T 29828-2013