移动互联网下可信移动平台接入机制

吴振强，周彦伟，乔子芮
(陕西师范大学 计算机科学学院，陕西 西安 710062)

摘 要：TCG MTM 规范的发布，确保了移动终端的安全性，但 MTM 芯片的推广导致移动终端通信方式的改变，从而提出移动互联网下可信移动平台(带有 MTM 芯片的移动终端，TMP)的接入机制，该机制在服务域中引入策略决策者管理本域的 TMP 及 Internet 服务提供商，定义了移动互联网下 TMP 的 2 种访问模式──本域服务和跨域访问，并详细介绍各模式的具体工作流程，其中将跨域访问模式定义为漫游服务和资源请求 2 种场景，重点描述 TMP 接入机制的可信性认证体系。运用通用可组合安全模型对 TMP 的 2 种访问方式进行安全性分析，分析表明，该机制可安全实现移动互联网下 TMP 的可信接入，同时具有实用、高效的特点。

关键词：可信计算；移动可信平台；移动可信模块；通用可组合安全
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2010)10-0158-12

Access mechanism of TMP under mobile network

WU Zhen-qiang, ZHOU Yan-wei, QIAO Zi-rui
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: The publication of TCG MTM standard ensured the safety of mobile terminal and its promotion results in the changes of communication on mobile terminals. An access mechanism to trusted mobile platform (mobile terminals with MTM chips, TMP) was proposed on mobile Internet. This mechanism defined an extended service set as a service field, introduced TMP and Internet ISP of strategy decider management field, and defined two visit mode of TMP on mobile Internet, self field service and cross field visit. The progress of each mode was described in details. Cross field visit mode was defined as roaming service and resource request. The trusted evaluation system of TMP access mechanism was specifically described. Universal combinational safe mode was used to analyze the safety of the two TMP access. The analysis shows that this mechanism brings about trusted TMP access on mobile Internet and is safe, practical and high efficient.

Key words: trusted computing; trusted mobile platform; mobile trusted module; universally composable security

1 引言

随着无线通信技术与计算机技术的不断融合，移动设备朝着智能化的方向发展，其所支持的功能越来越多，移动平台的开放性和灵活性也使得手机等移动设备得以普及，但伴随计算和存储资源的不断丰富，移动操作系统和各种无线应用技术的问世，移动设备中存储信息的敏感程度不断增加，PC 计算平台的安全威胁正发生在移动终端上，如手机病毒的出现，使数据丢失或被窃的情况日益严重

收稿日期：2010-04-08；**修回日期**：2010-09-28
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2007AA01Z438200）；国家自然科学重点基金资助项目（60633020）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2007AA01Z438200); The National Natural Science Foundation of China (60633020)

等，而且，有可能通过受感染的手机来影响到个人 PC 的安全。此外，移动终端本身也面临诸多安全威胁，移动设备的安全性已成为公众关注的焦点[1]。

目前为了确保系统的安全，比较常用的方法是通过 SSL 协议来验证经过加密的证书，通过原始数据来验证通信方的身份，但是这些措施不能保护任何系统特性，如软件的完整性等。因此，迫切需要及早研究移动设备的安全需求，并提出相应的安全通信方案。为了确保移动设备信息的安全，2006 年 9 月可信计算组织(TCG, trusted computing group)[2]的移动电话工作组发布了移动可信模块(MTM, mobile trusted module)[3]规范 V1.0，意在移动终端上建立可信的安全机制来保护用户的隐私信息和敏感数据，构建一个安全可靠的移动平台。

MTM 规范的发布，保证了移动设备的安全性，同时 MTM 的使用导致移动终端通信模式的改变，然而 MTM 规范中并没有制定在移动互联网下持有 MTM 芯片的移动终端(TMP, trusted mobile platform)间的通信方案，本文针对 TMP 通信模式的改变，提出移动互联网下 TMP 的可信接入机制，定义了 TMP 的 2 种访问模式——本域服务和跨域访问。

本文第 2 节介绍 TMP 的相关研究工作；第 3 节提出移动互联网下的 TMP 可信接入机制，对 TMP 的 2 种工作模型进行详细介绍；第 4 节运用通用可组合安全模型对 TMP 可信接入机制的安全性进行分析；第 5 节为性能分析，并详细介绍 TMP 接入机制的可信性评估体系；第 6 节是结束语。

2　相关工作介绍

国内外众多研究机构、学者开展了该领域的探索，并取得了一定的成果。

TCG 移动工作组致力于将 TCG 相关规范进行扩展，用于解决移动平台的安全问题[3,4]；Intel、IBM、NTT 等公司推出以 TCG MTM 为基础的移动终端可信性研究计划，提出了可信移动平台的软件、硬件体系结构和协议规范[5]。

我国在可信移动平台和移动互联网方面的研究已初具规模。文献[1]分析了可信移动设备的体系结构、TMP 的可信链及远程证明机制，并提出一种新的远程证明模型来确保 TMP 平台的完整性；文献[6]针对移动终端的特性，提出基于 MTM 的 TMP 体系结构；文献[7]提出带有 MTM 的 TMP 设计方案，平台采用基带处理器和应用处理器分离的结构，利用 MTM 构建以应用处理器为中心的可信区域；文献[8]针对现有网络用户身份管理难题及身份管理方案存在的不足，基于 TMP 完整性校验、保护存储及远程平台校验等安全特性，提出 TMP 身份管理方案和协议[9]。

国家自然科学基金项目“移动互联网络理论与关键技术”和国家 973 项目“一体化可信网络与普适服务体系基础研究”从分析移动互联网的体系结构和特点出发，研究移动互联网中的路由优化原理；建立适用于移动终端和移动子网的移动互联网路由协议[10]；文献[11]对现有应用于移动互联网的 P2P 技术进行分析，提出将 P2P 技术应用在移动互联网所面临的挑战和应用模式。

3　移动互联网下 TMP 可信接入机制

本文的 TMP 可信接入机制中将移动互联网下的一个扩展服务集定义为一个服务域，在每个服务域中引入绝对可信的第三方—策略决策者(PDP, policy decision point)管理整个域的 TMP 及协助 Internet 服务提供者(ISP, Internet service provider)验证 TMP 的可信性，同时受理其他域 TMP 的跨域服务请求消息，PDP 根据对其的可信性评估结果制定相应的访问控制策略。

如图 1 所示本文的 TMP 接入机制涉及的实体主要有 TMP、ISP 和 PDP，其中 TMP 是带有 MTM 安全芯片的移动终端，是请求接入的实体，其功能为发出访问请求，收集可信性度量值并发送给 PDP，等待 PDP 对其平台的可信性评估结果；ISP 是网络服务提供者，为 TMP 提供服务；PDP 主要完成本域中 TMP 平台的真实性及完整性验证，负责为本域中 TMP 颁发成员证书，同时受理其他域中 TMP 的跨域服务请求，PDP 根据对其的可信性评估结果为其颁发跨域访问证书，并且负责制定和分发 TMP 的身份鉴别策略及平台可信性评估策略，对 TMP 的身份进行鉴别，验证 TMP 证书的有效性，校验 TMP 平台的可信性。

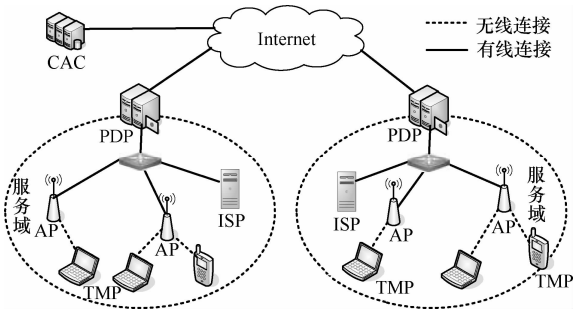


图 1　移动互联网下 TMP 接入机制

在本文架构中，根据 TMP 的具体工作过程定义了 2 种访问模式。

1) 本域服务模式：TMP 向本服务域的 PDP 注册服务，申请 PDP 颁发的成员证书，获得该证书后，TMP 即可持其与本域内的任何 ISP 进行服务交互，ISP 通过验证证书的合法性完成对 TMP 的可信性评估。

2) 跨域访问模式：TMP 请求与其他域的 ISP 进行通信，在该模式中，TMP 漫游进入其他服务域，或申请其他域中 ISP 为其提供服务，通过与其他域 PDP 和 ISP 的交互，可信 TMP 获得 ISP 提供的相关服务，完成跨域访问。

假设 1 服务域中的 PDP 获得由可信中心 CAC 签发的公钥证书，证书包含 PDP 的公钥及 CAC 签名等信息，并通过安全途径向外公布公钥，在 CAC 的协助下各 PDP 间可安全地协商会话密钥。实体 A 的身份证书格式如下。

$Cert_A$={ID_A，K_{PubA}，$Date_A$，LF_A，E_{KSCAC}{ ID_A，KP_A，$Date_A$，LF_A }}，其中 K_{PubA} 是 A 的公钥，*KSCA* 是 CAC 的私钥，$Date_A$ 是证书的签署日期，LF_A 是证书的有效期。

假设 2 TMP 分别由各自的 MTM 产生公私钥，并将公钥通过安全的途径向外发布，交互过程中加/解密、随机数产生等操作均由 MTM 完成。

3.1 本域服务模式

TMP 欲向本服务域 ISP 申请服务时，首先向本域 PDP 注册服务，申请其颁发的成员证书，获得该证书后，TMP 即可持其与本域内 ISP 完成服务交互，ISP 通过验证成员证书的合法性来验证 TMP 平台的可信性。

3.1.1 注册服务

如图 2 所示 TMP 与 PDP 建立连接，申请由 PDP 颁发的成员证书。链接建立前 TMP 基于 MTM 进行完整性度量，申请获得相关证书颁发者签发的 AIK 证书及平台属性证书。TMP 通过与 PDP 的协商完成 TMP 与 PDP 间双向的身份认证及 PDP 对 TMP 平台的可信性评估。TMP 通过身份认证和平台可信性评估后，PDP 为 TMP 颁发成员证书，在该证书的有效时间内用户持该证书即可与本域内 ISP 建立服务连接。

① TMP→PDP: RequestHello[*Nonce*‖*ID*‖ TMP_{PK}]。

② PDP→TMP：ResponseHello[*Nonce* ‖ PDP_{PK} ‖R_{PDP}]。

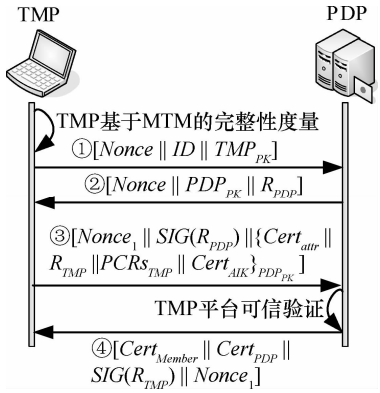


图 2 TMP 向本域 PDP 注册

通过 Hello 消息 TMP 与 PDP 进行会话前的协商，*Nonce* 由时间戳和随机数组成，用以验证发送的消息是否得到相应的回复，*ID* 是 TMP 的身份 ID 号，TMP_{PK} 是 TMP 的公钥；PDP_{PK} 是 PDP 的公钥，R_{PDP} 是 PDP 产生的用于 TMP 签名的随机数。

③ TMP→PDP：Authentication[$Nonce_1$‖*SIG* (R_{PDP}) ‖{$Cert_{attr}$‖ R_{TMP} ‖$PCRs_{TMP}$ ‖ $Cert_{AIK}$} $_{PDP_{PK}}$]。

TMP 首先对 PDP 产生的随机数 R_{PDP} 进行签名，将 AIK 证书、属性证书和平台完整性度量值用 PDP 的公钥加密后，连同签名值发送给 PDP，其中 R_{TMP} 是 TMP 产生的用于 PDP 签名的随机数，*SIG*(R_{PDP}) 是 TMP 对随机数 R_{PDP} 的签名值，$Cert_{AIK}$ 是 AIK 证书，$Cert_{attr}$ 是属性证书，$PCRs_{TMP}$ 是 TMP 平台的完整性度量信息。

④ PDP→ TMP：CertTransmission[$Cert_{Member}$ ‖ $Cert_{PDP}$ ‖ *SIG*(R_{TMP}) ‖ $Nonce_1$]。

PDP 首先验证 TMP 签名的合法性，通信双方对签名值的验证确保双方身份的真实性。PDP 解密消息获知 TMP 的属性证书等信息，对 TMP 平台的可信性进行评估，即验证 TMP 持有 AIK 证书及属性证书的合法性，可信性评估通过后，PDP 为 TMP 颁发成员证书 $Cert_{Member}$。其中 *SIG*(R_{TMP})是 PDP 对随机数 R_{TMP} 的签名值，$Cert_{Member}$ 是 PDP 颁发的成员证书。

TMP 通过对 PDP 的身份证书和签名的合法性验证确认 PDP 的身份。TMP 获得成员证书后，即持该证书向本域 ISP 申请服务，ISP 通过验证证书的合法性，完成对 TMP 的可信性评估，为可信的 TMP 提供服务。

3.1.2 证书结构及合法性验证

TMP 过频地向 PDP 申请服务，将导致 PDP 的工作效率降低，同时增加 TMP 的完整性度量负载，

为提高 TMP 接入机制的工作效率，本文使用证书机制以减少服务申请过程的可信性验证次数，证书结构如图 3 所示。

Validity	*Time*	*ID*	*Signature*

图 3　成员证书结构

其中：*Validity*：证书的有效授权时长；*Time*：证书的颁发时间；*ID*：证书授权对象的 ID 号；*Signature*：PDP 对证书的签名信息。

在证书的有效期内，TMP 持该证书多次申请服务，通过验证证书的合法性来判断 TMP 平台的可信性。假设当前时间为 T_{Now}，通过以下步骤验证证书的合法性。

1) 首先验证签名信息的有效性，该项检查验证证书颁发者的身份，同时检查证书内容是否被篡改。

2) 其次验证 $T_{\mathrm{NOW}} \leqslant Validity + Time$ 是否成立，该项检查验证证书在当前时间是否有效。

3) 最后验证 $TMP_{ID} = ID$ 是否成立，该项检查验证证书持有者是否是证书的申请者。

若上述验证都通过，表明 TMP 所持的证书在当前时间合法且有效。

3.1.3　可信性评估

TMP 平台的可信性评估包括对 MTM 的真实性验证和平台的完整性验证，即通过验证 TMP 持有的 AIK 证书及属性证书的合法性，完成对 TMP 平台真实性及完整性的验证。下面详细叙述 AIK 证书及属性证书的合法性验证过程。

(1) 真实性验证—AIK 证书合法性验证

在 TCG 制定的 DAA 方案中，DAA 颁发者是一个发布 DAA 签名的权威机构，各个不同的 TPM 厂商都设置有自己的 DAA 颁发者，这样就形成了相对独立的信任域，不同的信任域有不同的 DAA 颁发者，不同信任域内的参与者将信任不同的 DAA 颁发者，导致现有的 DAA 方案只适用于单信任域的情况，当位于不同信任域的验证者和示证者需要交互时，本节给出的跨域匿名认证方案可以完成 TMP 和 PDP 间的匿名认证。这一过程分为域内匿名认证和域间匿名认证 2 种情况。

1) 域内匿名认证：当示证者 TMP 与验证者 PDP 是同一可信域的 MTM 用户时，PDP 使用改进的直接匿名认证方案[12]对 TMP 的真实性进行匿名验证。

2) 域间匿名认证：当 TMP 与 PDP 分属不同的可信域时，提出跨域认证方案完成 PDP 对 TMP 平台的真实性验证。

如图 4 所示的一个服务域内的跨域匿名认证框架中，包含可信第三方策略决策者 PDP 和 2 个不同 MTM 芯片商的可信域 DO_A，DO_B，实体有 TMP、PDP 和 DAA 证书颁发者，其中 TMP 是发出跨域认证服务请求的 MTM 用户；DAA 证书颁发者为 DAA 方案中的证书颁发者，只有持有该证书的 TMP 方可申请跨可信域的匿名认证服务；PDP 对 TMP AIK 证书的可信性进行验证。

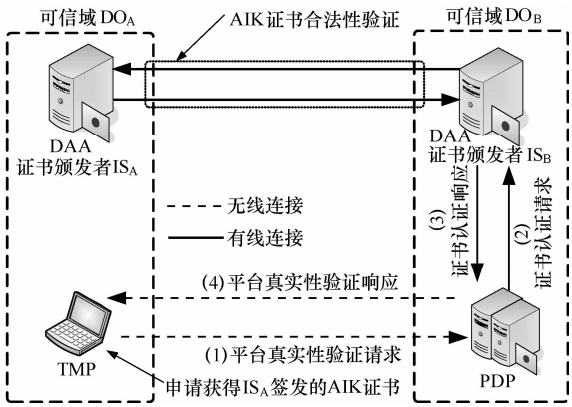


图 4　跨域认证框架

跨域直接匿名认证机制的基本思想是：若可信域 DO_A 的可信移动平台 $\mathrm{TMP_A}$ 要向可信域 DO_B 的策略决策者 PDP 证明其 AIK 证书的合法性，其中 $\mathrm{TMP_A}$ 与 PDP 属于同一服务域的不同可信域，$\mathrm{TMP_A}$ 首先获得本可信域 DAA 证书颁发者 $\mathrm{IS_A}$ 的认证，$\mathrm{TMP_A}$ 获得 AIK 证书后，向 PDP 发送平台真实性认证请求，$\mathrm{TMP_A}$ 使用本地域 AIK 证书向 PDP 证明其身份，PDP 在可信域 DO_B DAA 证书颁发者 $\mathrm{IS_B}$ 的协助下，通过与 $\mathrm{TMP_A}$ 所在域的 DAA 证书颁发者 $\mathrm{IS_A}$ 间的消息交互验证 $\mathrm{TMP_A}$ AIK 证书的可信性，即 PDP 在 $\mathrm{IS_A}$ 和 $\mathrm{IS_B}$ 的协助下完成对 $\mathrm{TMP_A}$ AIK 证书的真实性验证，实现服务域内不同可信域间平台真实性的跨域认证过程。

本文跨可信域匿名认证机制实现 PDP 对服务域内不同可信域 MTM 的真实性验证，确保 TMP 可信接入机制中 TMP 平台的真实性。

(2) 完整性验证—属性证书合法性验证

基于属性证书完成对用户平台的完整性验证过程如图 5 所示。

Step 1　平台完整性验证请求。TMP 发送完整性验证请求消息 *c* 给属性证书发布者。

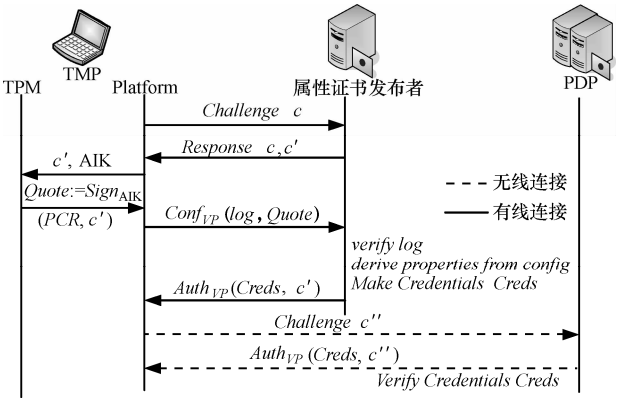


图 5 TMP 平台完整性验证过程

Step 2 平台完整性验证响应。当证书发布者收到 TMP 发送的证书请求消息后，验证 TMP 的合法性，如果其合法，则发送平台完整性信息的消息标识 c'及 TMP 发送的挑战消息 c 给 TMP。

Step 3 TMP 收到证书发布者发布的平台完整性验证挑战消息后，触发 MTM 进行 PCR 值的获取。

Step 4 平台向 MTM 请求获得相应的 PCR 值，并使用 AIK 私钥对 PCR 值和随机数 c'进行签名。

Step 5 平台收集并规格化完整性度量日志，将规格化后的完整性度量日志、Quote 及相关信息以标准的完整性报告格式发送给证书发布者。

Step 6 证书发布者收到平台发送的完整性信息后，提取出平台的属性信息，并对这些属性信息进行验证，产生相应的证书。

Step 7 将构建的属性证书以安全的方式发送给 TMP。

通过上述步骤 TMP 申请获得属性证书，在向 PDP 申请相关证书时完成下述 2 步，即验证属性证书的合法性。

Step 8 TMP 获得由证书发布者颁发的属性证书后，持该证书向 PDP 发送完整性验证消息。

Step 9 PDP 收到 TMP 发送的属性证书后，基于相应的策略对其所显示的平台完整性进行验证。

3.2 跨域访问

在跨域访问中，根据访问形式的不同本文定义了 2 种跨域访问场景。

1) 漫游服务场景：TMP 请求进入其他服务域网络，即 TMP 移动进入其他域，与该域中的 ISP 进行服务交互。

2) 资源请求场景：TMP 请求访问其他服务域资源，TMP 向其他域的 ISP 发出服务请求，请求对方为其提供服务。

假设 3 本地域 A 和远程域 B 的策略决策者（即 LPDP 与 RPDP）的密钥对分别为$\{K_{\mathrm{PubA}}、K_{\mathrm{PrivA}}\}$和$\{K_{\mathrm{PubB}}、K_{\mathrm{PrivB}}\}$。

假设 4 通过协商 TMP 与 RPDP 间的会话密钥为 K_S；LPDP 与 RPDP 间的会话密钥为 K_T；TMP 与 ISP 的会话密钥为 K_M；ISP 与 RPDP 间的会话密钥为 K_N；TMP 与 LPDP 间的会话密钥为 K_W。

3.2.1 漫游服务场景

如图 6 所示在漫游服务场景中，当本地域中的 TMP 请求接入远程域网络时，TMP 将可信性验证信息以“推”的方式发送给远程域 RPDP，根据来自 TMP 的请求，RPDP 对可信的 TMP 颁发跨域访问证书，该证书一次颁发，多次使用，提高域中策略决策者的认证效率，同时防止策略决策者成为系统瓶颈。

漫游服务场景中涉及本地域和远程域 2 个域，其基本思想是：本地域 A 中的 TMP 在移动接入远程域 B 之前，向远程域 B 的 RPDP 发送跨域证书申请，RPDP 收到 TMP 的申请消息后，通过与 TMP 所在域的策略决策者 LPDP 间的消息交互，完成对 TMP 可信性评估，LPDP 将 TMP 的可信性评估结果签名后发送给 RPDP，RPDP 根据 LPDP 对 TMP 的可信性评估结果对可信的 TMP 颁发跨域访问证书，TMP 获得 RPDP 颁发的跨域访问证书后，进入远程域 B，并与该域的 ISP 完成服务交互。图 7 给出了漫游服务场景的消息流程。

Step 1 本地域 A 中 TMP 访问远程域 B 服务之前，TMP 向 RPDP 发送请求消息申请跨域访问证书。

$TMP \rightarrow RPDP$: $CertRequest=K_S\{K_{\mathrm{PubB}}\{TS_1 \| Nonce_1$

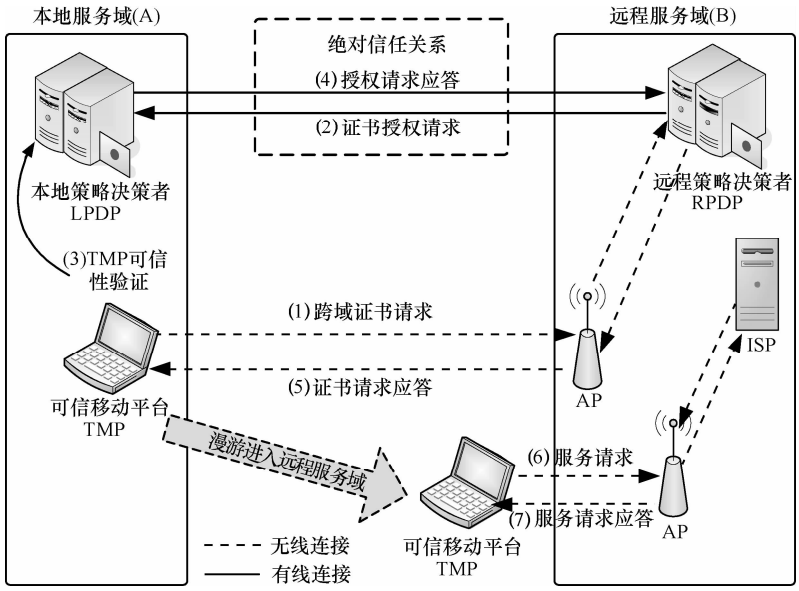


图 6 漫游服务场景

$\| K_{LPDP_{PK}} \{Cert_{attr\text{-}TMP} \| PCRs_{TMP} \| Cert_{AIK\text{-}TMP}\}\}$

TMP 将 AIK 证书 $Cert_{AIK\text{-}TMP}$、属性证书 $Cert_{attr\text{-}TMP}$ 和平台的完整性度量值 $PCRs_{TMP}$ 用本地域 LPDP 的公钥加密，连同随机数 $Nonce_1$ 和时戳 TS_1 用 RPDP 的公钥加密，将加密后的消息用 TMP 与 RPDP 间的会话密钥 K_S 加密后发送给 RPDP。

Step 2　可信域 B 中的策略决策者 RPDP 接收到 TMP 的跨域证书申请后，首先检查请求消息时戳的新鲜性，RPDP 解密 TMP 的请求消息，向本地域 A 中的策略决策者 LPDP 发出证书验证请求。

$RPDP \rightarrow LPDP$: $CertAuthenRequest = K_T\{K_{PrivB}\{K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP} \| PCRs_{TMP} \| Cert_{AIK\text{-}TMP}\} \| Nonce_2 \| TS_2 \| Cert_{RPDP}\}\}$

RPDP 将收到的 TMP 的平台可信性验证信息 $K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP} \| PCRs_{TMP} \| Cert_{AIK\text{-}TMP}\}$和时间戳 TS_2、随机数 $Nonce_2$ 及 RPDP 的证书 $Cert_{RPDP}$ 用 RPDP 的私钥签名，然后用 RPDP 与 LPDP 间的会话密钥 K_T 加密后发送给 LPDP。

Step 3　本地域 A 中的策略决策者 LPDP 首先验证 RPDP 证书的合法性及时戳的新鲜性，响应合法的认证请求，对 TMP 平台的可信性进行验证。

Step 4　本地域 A 中的 LPDP 根据相关信息验证 TMP 平台的可信性，并将验证结果签名后发送给远程域 B 中的 RPDP。

$LPDP \rightarrow RPDP$:$CertAuthenReplay = K_T\{K_{PrivA}\{ID_A \| Nonce_2 \| TS_3 \| Cert_{LPDP} \| Result_A\}$

LPDP 为 TMP 赋予一个唯一的 *ID* 号，该 *ID* 号相当于标识 TMP 的一个假名；LPDP 将 TMP 可信性评估结果 $Results_A$、TMP 的 *ID* 号 ID_A、时戳 TS_3、LPDP 的证书 $Cert_{LPDP}$ 和随机数 $Nonce_2$ 用 LPDP 私钥签名，然后用 LPDP 与 RPDP 间的会话密钥 K_T 加密后发给 RPDP。

Step 5　远程域 B 中的 RPDP 首先验证 LPDP 签名的完整性、证书的合法性及时戳的新鲜性，对可信的 TMP 颁发跨域访问证书 *Tickets*。

$RPDP \rightarrow TMP$：$CertReplay = K_S\{K_{PrivB}\{ID_A \| TS_4 \| Nonce_1 \| Tickets\}\}$

RPDP 将 TMP 的 *ID* 号 ID_A、跨域访问证书 *Tickets*、时戳 TS_4 和随机数 $Nonce_1$ 用私钥签名，然后用 RPDP 与 TMP 间的会话密钥 K_S 加密后发给 TMP，RPDP 为可信合法的 TMP 颁发跨域访问证书 *Tickets*。

Step 6　TMP 获得远程域 B 的跨域访问证书后，即可漫游进入远程域 B，进入后与远程域 B 中 ISP 协商会话密钥 K_{ONE}，然后向其发出服务请求。

$TMP \rightarrow ISP$：$ServicesRequest = K_{ONE}\{ID_A \| TS \| Nonce \| Tickets \| Data\}$

TMP 将 ID 号 ID_A、时戳 *TS*、TMP 持有的跨域访问证书 *Tickets* 和服务请求数据 *Data* 用 TMP 与 ISP 间协商的会话密钥 K_{ONE} 加密后发送给服务提供商 ISP。

Step 7　ISP 验证 TMP 跨域访问证书 *Tickets* 的

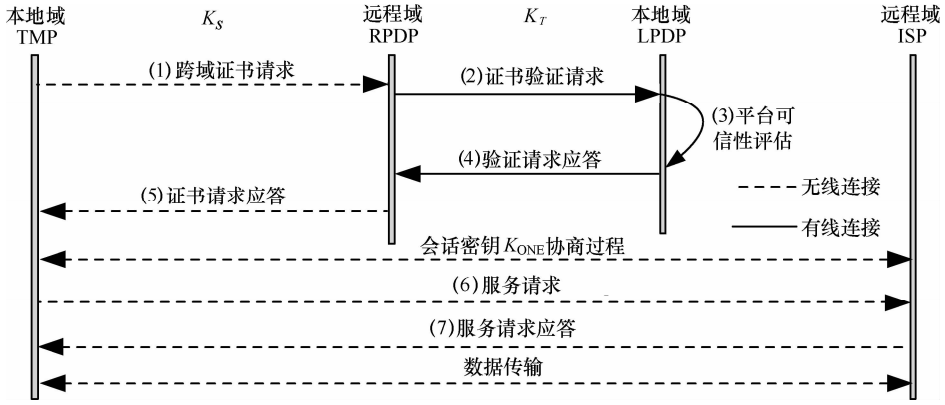


图 7 漫游评估场景信息流程

合法性，为持有合法跨域访问证书的 TMP 提供服务。

ISP→TMP：$ServicesReplay=K_{ONE}\{Nonce \parallel ServiceData\}$

3.2.2 资源请求场景

如图 8 所示在资源请求场景中，定义了 TMP 访问远程域的场景，远程域中的 ISP 通过与 RPDP 间的会话完成对 TMP 的可信性验证，ISP 根据 RPDP 的验证结果制定相应的访问控制策略。

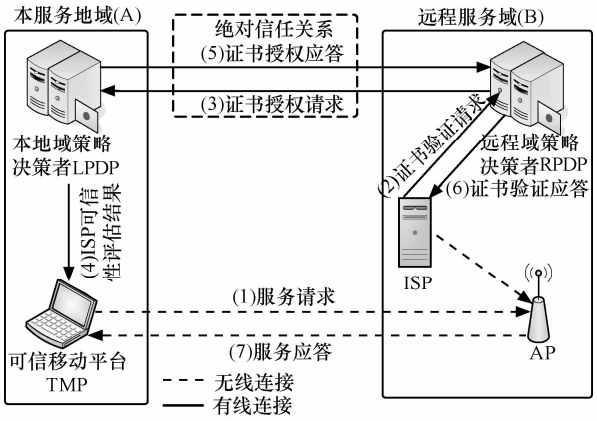


图 8 资源请求场景

资源请求场景的基本思想：本地域 A 的 TMP 向远程域 B 中的 ISP 发出服务请求消息，ISP 收到服务请求消息后，向本域的策略决策者 RPDP 发送可信性评估请求，RPDP 与 TMP 所在域的策略决策者 LPDP 进行交互，完成对 TMP 的可信性评估，LPDP 将 TMP 的评估结果签名后发给 RPDP，RPDP 对可信的 TMP 授权，并将授权结果发给 ISP，ISP 根据 RPDP 的授权消息，制定相应的访问控制策略，响应可信 TMP 的请求对其提供服务。图 9 给出了资源请求场景的消息流程。

Step 1 本地域 A 中持有 AIK 证书的 TMP 向远程域 B 中的 ISP 发送服务请求，该请求中包含 TMP 的完整性度量数据和其所属的域名。

$TMP\rightarrow ISP$：$ServicesRequest=K_M\{TS_1 \parallel Nonce_1 \parallel K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP} \| PCRs_{TMP} \| Cert_{AIK\text{-}TMP}\} \| A \| ISP\}$

TMP 将证书 $Cert_{AIK\text{-}TMP}$、属性证书 $Cert_{attr\text{-}TMP}$ 和平台的完整性度量值 $PCRs_{TMP}$ 用本地域 LPDP 的公钥加密后，连同其所在域的标识 A、所要访问资源标识 ISP、时戳 TS_1 和随机数 $Nonce_1$ 用与 ISP 间的会话密钥 K_S 加密后发送给 ISP。

Step 2 远程域 B 的 ISP 接收到 TMP 的服务请求后，ISP 首先检查时戳的新鲜性，响应合法的请求消息，即向本域中的策略决策者 RPDP 发送可信性评估请求，同时发送 ISP 自身的完整性度量信息

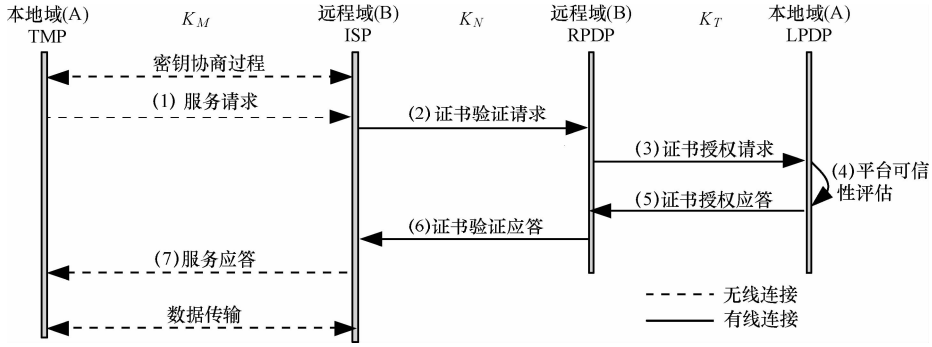


图 9 资源请求场景信息流程

给 RPDP。

ISP→RPDP： *CertAuthenRequest*= $K_N\{K_{\text{PubB}}\{PCRs_{ISP}\| K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP}\|PCRs_{TMP}\| Cert_{AIK\text{-}TMP}\}\| A \| Nonce_2\| TS_2\}$

ISP 将收到的 TMP 的完整性度量信息 $K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP}\|PCRs_{TMP}\| Cert_{AIK\text{-}TMP}\}$、TMP 所在域标识 A 和时间 TS_2、随机数 $Nonce_2$ 及 ISP 平台的完整性度量值 $PCRs_{ISP}$ 用 RPDP 的 AIK 公钥签名，然后用 TMP 与 RPDP 间的会话密钥 K_N 加密后发给 RPDP。

Step 3　RPDP 向本地域 A 中的策略决策者 LPDP 发送 TMP 可信性评估请求，同时将 ISP 的平台可信性评估结果信息签名后发送给 LPDP。

RPDP→LPDP：*CertAuthorRequest*= $K_T\{K_{\text{PrivB}}\{Cert_{RPDP} \| Nonce_3 \| TS_3 \| K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP} \|PCRs_{TMP}\| Cert_{AIK\text{-}TMP}\}\| Result_{ISP}\}\}$

RPDP 将收到的 TMP 的完整性度量信息 $K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP} \|PCRs_{TMP}\| Cert_{AIK\text{-}TMP}\}$和时戳 TS_3、随机数 $Nonce_3$、RPDP 的证书 $Cert_{RPDP}$ 及 RPDP 对 ISP 的可信性评估结果 $Result_{ISP}$ 用 RPDP 的私钥签名，然后再用 RPDP 与 LPDP 的会话密钥 K_T 加密后发送给 LPDP。

Step 4　本地域 A 的 LPDP 验证 RPDP 签名信息的真实性、身份证书的合法性及时戳的新鲜性，响应合法的认证请求消息。LPDP 将 ISP 的可信性估结果签名后发送给 TMP，同时对 TMP 可信性进行评估。

LPDP→TMP：*Request*=$K_W\{K_{\text{PrivA}}\{ ID_A \| Result_{ISP} \}\}$

LPDP 将 ISP 的可信性评估结果签名后发送给 TMP，TMP 首先验证 LPDP 签名信息的真实性，即可获知 ISP 的可信性评估结果。

Step 5　LPDP 将 TMP 可信性评估结果签名后发给远程域 B 的 RPDP。

LPDP→RPDP： *CertAuthenReplay*= $K_T\{K_{\text{PrivA}}\{ID_A \| Nonce_3 \| TS_4 \| Result_{TMP} \| Cert_{LPDP}\}$

LPDP 为 TMP 赋予一个唯一的 *ID* 号，该 *ID* 号相当于标识 TMP 的一个假名；LPDP 将 TMP 可信性评估结果 $Results_{TMP}$、TMP 的 *ID* 号 ID_A、LPDP 的证书 $Cert_{LPDP}$、时戳 TS_4 和随机数 $Nonce_3$ 用 LPDP 私钥签名，然后用 LPDP 与 RPDP 间的会话密钥 K_T 加密后发给 RPDP。

Step 6　远程域 B 中的 RPDP 验证 LPDP 签名值的真实性、身份证书的合法性及时戳的新鲜性，解密响应消息获得 TMP 可信性评估结果，RPDP 将证书的可信性评估结果签名后发往 ISP。

RPDP→ISP：*CertAuthorReplay*= $K_N\{K_{\text{PrivB}}\{ ID_A \| Cert_{RPDP} \| Result_{TMP} \| Nonce_2 \| TS_5\}\}$

RPDP 将 TMP 的 *ID* 号、TMP 的可信性评估结果 $Result_{TMP}$、RPDP 的证书 $Cert_{RPDP}$、随机数 $Nonce_2$ 及时戳 TS_5 用 RPDP 的私钥签名，然后用 ISP 与 RPDP 间的会话密钥 K_N 加密后发送给 ISP。

Step 7　ISP 首先验证 RPDP 签名信息的真实性，ISP 根据 TMP 的可信性评估结果对其请求消息进行响应。

*ISP→TMP*M：*ServicesReplay*=$K_M\{ ID_A \| TS_6 \| Nonce_1\}$

至此 TMP 与 ISP 间完成双向的身份认证与双向的可信性评估，ISP 为可信合法的 TMP 提供跨域服务。

4　接入机制的安全性证明

Bellare 等在 1998 年引入可证明安全理论模块化的设计思想，后来由 Canetti 等于 2001 年进一步扩展，称之为通用可组合安全（UC）模型。本文采用该安全模型来分析、证明 TMP 接入机制认证协议的安全性。相关文献对 UC 模型证明过程所用的通用可组合安全、DDH 假设和多项式时间不可区分性等安全假设进行了详细介绍[13,14]。

本文以跨域访问模式中漫游服务场景为例，利用 UC 模型对移动互联网下的 TMP 可信接入机制进行安全性证明。该场景在 TMP 漫游进入远程服务域时，完成对 TMP 的身份合法性及平台可信性的验证，其中消息 $K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP} \|PCRs_{TMP}\| Cert_{AIK\text{-}TMP}\}$是 TMP 发送给 RPDP 的消息， RPDP 在 LPDP 的协助下通过该消息完成对 TMP 身份合法性及平台可信性的验证。对于 RPDP 而言，只要保证消息 $K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP} \|PCRs_{TMP}\| Cert_{AIK\text{-}TMP}\}$确实来自 TMP 且在传输过程中并未被篡改，就可以确保对 TMP 身份合法性及平台可信性验证的正确性，协议中证书和签名等机制的使用可以保证 $K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP} \|PCRs_{TMP}\| Cert_{AIK\text{-}TMP}\}$消息的上述性质。

安全性证明前，首先给出漫游服务场景的 TMP

接入认证协议的抽象描述$\prod$，抽象协议只给出必要的信息。因为 RPDP 在 LPDP 的协助下完成对 TMP 身份合法性及平台可信性验证， RPDP 与 LPDP 间存在安全的通信信道，ISP 绝对信任 RPDP 对 TMP 可信验证结果，同时根据该结果制定 TMP 相应的访问控制策略，并且 ISP 与 RPDP 间存在安全的通信信道，所以在抽象模型协议中将 RPDP、ISP 和 LPDP 作为一个整体来考虑。假设协议$\prod$在 2 个实体 I 和 R 间进行，如下所示：

$R\rightarrow I$：M_1，$MAC_{R,1}$；

$I\rightarrow R$：M_2，$MAC_{I,1}$，$SIG_{I,1}$；

$R\rightarrow I$：M_3，$MAC_{R,2}$，SIG_R；

$I\rightarrow R$：M_4，$MAC_{I,2}$，$SIG_{I,2}$。

TS 为实体产生的时戳，$Nonce$ 为随机数用于验证先前发送的消息是否得到回复，MAC 为消息认证码，SIG 为实体签名的身份认证信息。

其中：$M_0=K_{LPDP_{PK}}\{Cert_{attr\text{-}TMP}\|PCRs_{TMP}\|Cert_{AIK\text{-}TMP}\}$；

$M_1=TS_{R,1}\|Nonce_1\|M_0$；

$M_2=TS_{I,1}\|Nonce_1\|Tickets$；

$M_3=TS_{R,2}\|Nonce_2\|Tickets$；

$M_4=TS_{I,2}\|Nonce_2$；

$MAC_{R,1}=H_{MAC}(M_1)$；

$MAC_{I,1}=H_{MAC}(M_2)$；

$MAC_{R,2}=H_{MAC}(M_3)$；

$MAC_{I,2}=H_{\mathrm{MAC}}(M_4)$；

$SIG_{I,1}=H_{SIG}(M_2)$；

$SIG_R=H_{SIG}(M_3)$；

$SIG_{I,2}=H_{SIG}(M_4\|Server\text{-}Data)$，$H_{\mathrm{MAC}}$ 和 H_{SIG} 为相关密钥加密的算法。

定理 1 真实模型下的协议$\prod$安全实现理想函数 F_{KE}，因此对任何环境机 Z，等式 $REAL_{\prod^{1},I,Z}\approx IDEAL_{FKE,R,Z}$均成立，即$\prod$是 UC 安全的。

证明 协议$\prod$证明思路：首先构造一个能够安全实现签名的理想函数 F_{sig} 的协议 P_s；其次，给出安全密钥交换的理想函数 F_{KE}，同时构造一个协议$\prod_1$，并证明$\prod_1$在混合模式 F_{sig}-*hybrid* 下安全实现了 F_{KE}；将协议 P_s 与$\prod$进行组合，通过 UC 安全组合定理，证明组合后的协议与$\prod_1$等价，且在现实模型下安全实现了 F_{KE}。

引理 1 Sig=(gen，ID，ver)是文献[14]中描述的签名，那么在真实环境下，协议 P_s 可以安全实现 F_{sig}，当且仅当 S 是抗击选择消息存在性伪造。

引理 2 如果 DDH 假设成立，且消息认证算法是安全的，则协议$\prod_1$在 F_{sig}-*hybrid* 下安全实现 F_{KE}。

证明 $\prod_1$ 为基于密钥交换理想函数 F_{KE} 的协议，令协议$\prod_1$是在混合模型 F_{sig}-*hybrid* 下的协议，H 为攻击模型中的攻击者。构造一个理想环境下的攻击者 S(仿真器)，使得任何环境机 Z 都不能辨别 S 是与 H 及$\prod_1$在 F_{sig}-*hybrid* 下进行的交互，还是与 S 及 F_{KE}在 *Ideal-life* 下进行交互，即对任何环境机 Z，等式 $REAL_{\prod^{1},H,Z}\approx IDEAL_{FKE,S,Z}$均成立。

本文使用文献[15]中构造的仿真器 S。假设在仿真器 S 的执行下，存在一个环境机 Z'，成功辨别与 H 及$\prod_{1.1}$在 F_{sig}-*hybrid* 下进行交互与 S 及 F_{KE}在 *Ideal-life* 下进行交互的概率不可忽略，即 $prob(REAL_{\prod^{1.1},H,Z}\neq IDEAL_{FKE,S,Z})$为 1/2 加上一个不可忽略的优势$\varepsilon$。那么使用文献[15]中构造的区分器 D，利用环境机 Z'来破解 DDH 问题，进而规约到矛盾。

通过对区分器 D 执行过程的分析，并根据区分器的构造原理，得出 D 成功区分输入 Q_0 和 Q_1 的概率等于环境机 Z'成功辨别理想和混合 2 种环境的概率，即 D 能够以 1/2 加上一个不可忽略的优势ε成功区分 Q_0 和 Q_1，而这与 DDH 假设矛盾。

引理 3 令$\prod_1$是 F_{sig}-*hybrid* 下的协议，P_s 为安全实现 F_{sig} 的协议，那么对于任何攻击者 A 都存在一个攻击者 H，使得对任何环境机 Z 来说，等式 $REAL_{\prod^{1}Ps,A,Z}\approx IDEAL_{\prod^{1},H,Z}$均成立，即组合协议$\prod_1P_s$安全仿真了 F_{sig}-*hybrid* 下的$\prod_1$。

证明 根据 DDH 假设即可证明该引理成立。

引理 4 真实环境下，组合协议$\prod_1P_s$与协议$\prod$等价。

证明 将混合模型 F_{sig}-*hybrid* 下协议$\prod_1$对所有理想函数 F_{sig} 的访问均替换为对协议 P_s 的访问，可以得出协议$\prod_1P_s$与协议$\prod$等价。

定理 2 真实模型下的协议$\prod_1$安全实现理想函数 F_{KE}，即对任何环境机 Z，等式 $REAL_{\prod^{1},A,Z}\approx IDEAL_{FKE,H,Z}$均成立，即漫游服务场景中 TMP 接入协议是安全的。

证明 根据引理 1~4、DDH 假设和定理 1 即可证得定理 2 成立。

综上所述，使用 UC 模型同样可证得 TMP 注册服务和资源请求场景中接入协议的安全性，因此本文提出的无线环境下 TMP 的接入机制是安全、可靠的接入过程。

5　TMP 接入机制分析

5.1　性能分析

(1) 跨域性

DAA 主要是面对范围较小的单可信域环境，它无法提供向分属不同可信域 MTM 的真实性验证。而本文提出跨域认证机制解决现有 DAA 方案只适用于单可信域的缺陷，实现了验证者和 TMP 分属不同可信域时 MTM 的真实性验证。

(2) 高效性

本文 TMP 的接入机制对通过可信性评估的 TMP 颁发成员证书，该证书一次颁发，多次使用，TMP 发出服务请求时，ISP 无需再对 TMP 进行可信性评估，提高了 ISP 的工作效率，同时有效减少了 TMP 的完整性度量负载，同时防止 PDP 成为系统瓶颈。

本文的 TMP 接入机制中的部分运算（如加/解密、随机数生成等）均由 MTM 完成，不消耗 TMP CPU 的计算能力，MTM 作为独立的计算单元，可以加速模型中协议的执行，提高 TMP 接入机制的执行效率。

本文的 TMP 接入机制在第一轮交互中就对 TMP 的身份合法性和平台可信性进行验证，若验证未通过，PDP 在第一轮协议交互后就可终止协议，并拒绝该 TMP 接入，一定程度降低了 PDP 的执行负载。

(3) 匿名性

成员证书及跨域访问证书中均不包含 TMP 的相关平台信息，仅报告当前 TMP 平台的身份是否真实，平台的状态是否完整，而没有暴露出平台的基本配置信息，因此有效地保证了跨域申请者的隐私性，即证书具有匿名性，匿名性的强弱来自于有效授权时间的取值，有效授权时间越短则匿名性越强。

TMP 跨域访问机制中，为实现 TMP 身份的保密性，TMP 不向访问域 PDP 出示其属性证书、完整性度量值等信息，将这些信息用本地域 PDP 的公钥加密后发送给访问域 PDP，即访问域 PDP 对 TMP 的可信性认证是通过访问域 PDP 对本地域 PDP 的认证与本地域 PDP 对 TMP 的可信性评估来实现。

(4) 可控性

可控性的实现主要依赖于用户的假名（即 ID 号），在成员证书有效授权时间内只允许使用同一个假名，则 ISP 可以确认在证书有效期内完成的服务请求是否来自于同一个 TMP。

(5) 抗攻击性

被动攻击仅对通信内容进行截取、窃听和分析等操作，所以安全的密码体制可保证本文认证协议有抵抗被动攻击的能力；本文的 TMP 的接入机制中随机数及通信双方实体名的使用可以抵抗假冒攻击、重放攻击和中间人攻击等主动攻击方式。

5.2　模型分析

本文的 TMP 可信接入机制的优点如下。

1) PDP 无须验证 TMP 平台配置的能力，即 TMP 不需要向 PDP 揭示自己的平台信息，从而保护了 TMP 的隐私信息，具有匿名性强的特点。

2) PDP 可处于离线模式，同时 PDP 颁发成员证书之后，TMP 可以在后续通信中重复使用该证书，减少可信性评估次数，提高 PDP 工作效率，使 PDP 不会成为系统瓶颈。

3) 由于 TMP 运算能力的局限性，本文的 TMP 接入机制并未使用计算成本过高的算法，TMP 只需要进行对称加/解密运算，避免了指数运算。同时本文的 TMP 接入协议中消息长度较短，且 TMP 与远程服务域，本地服务域与远程服务域间只进行一轮信息交换，以适应移动互联网中由于通信带宽有限造成的误码率高的缺点。

5.3　可信性认证体系

本文的 TMP 接入机制的可信性评估体系如图 10 所示，其中证书仲裁中心（CAC, arbitration center of certificate）是可信第三方，负责为各可信域中的 PDP 签发身份证书。

证书仲裁中心是第 1 级管理中心，制定和发布总体标准，并对第 2 级各服务域 PDP 进行管理；第 2 级为由相关服务域的 PDP，实现本域内各 TMP 平台的可信性评估，在第 3 级企业 DAA 证书颁发者及属性证书发布者的协助下完成对 TMP 平台真实性及完整性验证；第 3 级为企业 DAA 证书服务器和属性证书发布者，负责为本企业 MTM 芯片颁发 AIK 证书和属性证书，同时协助 PDP 完成对 TMP 平台真实性及完整性验证；第 4 级为 TMP 和 ISP。

本文的 TMP 接入机制除具有跨域性、高效性和匿名性等特点外，其可信性认证体系还具有扩展性好、安全性高和健壮性高等特点。

1) 扩展性好。当需要部署新的服务域时，新服务域中的 PDP 只需向 CAC 发出注册申请，CAC 对 PDP 的身份合法性及平台可信性进行验证，对通过验证的 PDP 颁发其签名后的成员证书。

2) 安全性高。PDP 向 CAC 注册时，CAC 对其身份合法性及平台可信性同样进行验证，仅对通过

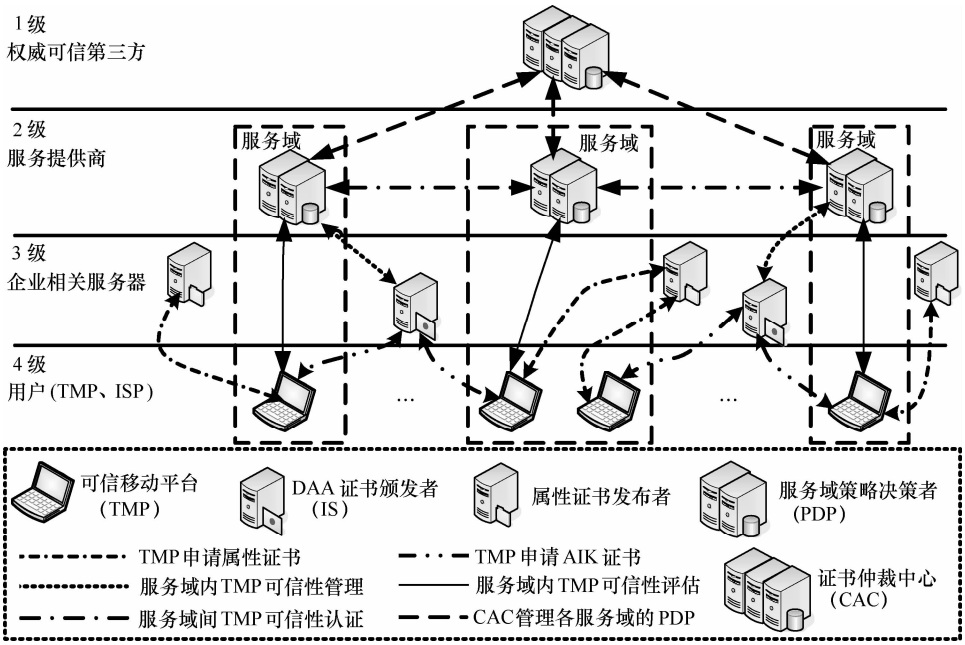


图 10 TMP 接入机制的可信性认证体系

验证的 PDP 颁发成员证书，同时 TMP 接入机制中，CAC 可定期对各成员 PDP 的身份合法性和平台可信性进行验证。

3) 健壮性高。本文的 TMP 接入机制采用分级管理，彼此信任的模式，即各服务域的 PDP 绝对信任其他域中 PDP 对 TMP 的可信性验证结果，PDP 信任 DAA 证书颁发者的真实性验证结果和属性证书发布者的完整性度量结果，任务分级处理，彼此信任的可信性认证体系有效防止各级服务器由于负载过重而成为系统瓶颈。

6 结束语

本文针对移动终端引入 MTM 芯片后通信模式的改变，结合其特点提出在移动互联网下的 TMP 通信方案，该方案中，以扩展服务集为服务域，每个服务域中引入可信第三方 PDP 来管理域中的 TMP 及 ISP，定义了 TMP 本域服务和跨域访问 2 种过程，并在跨域服务模式中根据访问途径的差异提出漫游服务场景和资源请求场景 2 种通信模式，运用通用可组合安全模型对通信方案进行安全性分析，分析表明本文模型是移动互联网下安全的 TMP 接入机制，具有安全、实用、高效的特点。

参考文献：

[1] 邢黎, 祝跃飞, 王美琴. 可信移动平台及其验证机制的研究[J]. 计算机工程与设计, 2008, 29(3): 1080-1082, 1085.
XING L, ZHU Y F, WANG M Q. Study on trusted mobile computing and its attestation scheme[J]. Computer Engineering and Design, 2008, 29(3): 1080-1082, 1085.

[2] Trusted Computing Group. TCG specification architecture overview (Version 1.2)[EB/OL].https://www.Trustedcomputinggroup.org/. 2007.

[3] Trusted Computing Group. TCG mobile trusted module specification version 1.0 [EB/OL]. https: // www. trustedcomputinggroup.org. 2007.

[4] Trusted Computing Group. TCG mobile reference architecture version 1.0 [EB/OL]. https: // www.trustedcomputinggroup.org. 2007.

[5] TMP. Trusted mobile platform hardware architecture description[EB/OL]. http: // www. trustedmobile.org/.

[6] 郑宇, 何大可, 何明星. 基于可信计算的移动终端用户认证方案[J]. 计算机学报, 2006, 29(8): 1255-1264.
ZHEN Y, HE D K, HE M X. Trusted computing based user authentication for mobile equipment[J]. Chinese Journal of Computers, 2006, 29(8): 1255-1264.

[7] 陈书义, 闻英友, 赵宏. 基于可信计算的移动平台设计方案[J]. 东北大学学报(自然科学版), 2008, 29(8): 1096-1099.
CHEN S Y, WEN Y Y, ZHAO H. Conceptual design of trusted mobile platform[J]. Journal of Northeastern University (Natural Science), 2008, 29(8): 1096-1099.

[8] 李建, 何永忠, 沈昌祥等. 基于可信移动平台的跨身份标志域访问模型[J]. 计算机应用研究, 2009, 26(1): 321-324.
LI J, HE Y Z, SHEN C X, *et al*. Access model spanning identifier domain based on trusted mobile platform[J]. Application Research of Computers, 2009, 26(1): 321-324.

[9] 李建, 何永忠, 沈昌祥等. 可信移动平台身份管理框架[J]. 计算机应用研究, 2009, 26(12): 3711-3714.

LI J, HE Y Z, SHEN C X, *et al*. Identity management framework based on trusted mobile platform[J]. Application Research of Computers, 2009, 26(12): 3711-3714.

[10] 苏伟. 移动互联网路由理论与关键技术研究[D]. 北京: 北京交通大学, 2008.

SU W. Research on Routing Theory and Key Technologies in Mobile Internet[D]. Beijing: Beijing Jiaotong University, 2008.

[11] 李伟, 徐正全, 杨铸. 应用于移动互联网的 Peer-to -Peer 关键技术[J]. 软件学报, 2009,20(8): 2199-2213.

LI W, XU Z Q, Y Z. Peer-to-peer key technologies in mobile internet[J]. Journal of Software, 2009,20(8): 2199-2213.

[12] 李洁, 吴振强, 于璐等. 一种改进的直接匿名认证方案[J]. 计算机应用, 2009, 29(2): 364-366, 397.

LI J, WU Z Q, YU L, *et al*. An improved directed anonymous attestation scheme[J]. Journal of Computer Applications, 2009, 29 (2): 364-366, 397.

[13] 杨超, 曹春杰, 马建峰. 通用可组合的 Mesh 网络认证协议[J]. 西安电子科技大学学报(自然科学版), 2007, 34(5): 814-817.

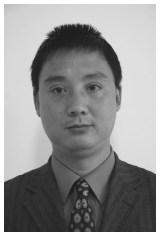
YANG C, CAO C J, MA J F. Universally composable secure authentication protocol for wireless mesh networks[J]. Journal of Xidian University, 2007, 34(5): 814-817.

[14] GOLDWASSER S, MICALI S, RIVEST R. A digital signature scheme secure against adaptive chosen-message attacks[J]. SIAM Journal on Computing, 1998, 17(2): 281-308.

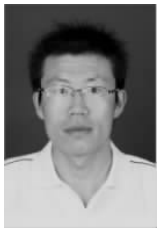
[15] 曹春杰, 杨超, 马建峰. WLAN Mesh 漫游接入认证协议[J]. 计算机研究与发展, 2009, 46(7): 1102-1108.

CAO C J, YANG C, MA J F. An authentication protocol for station roaming in WLAN mesh[J]. Journal of Computer Research and Development, 2009, 46(7): 1102 -1108.

作者简介：



吴振强（1968-），男，陕西柞水人，博士，陕西师范大学副教授，主要研究方向为匿名通信技术、可信计算、自适应安全、无线网络等。



周彦伟（1986-），男，甘肃通渭人，陕西师范大学硕士生，主要研究方向为匿名通信技术、可信计算。

乔子芮（1985-），女，陕西定边人，陕西师范大学硕士生，主要研究方向为智能信息处理。