ICS 35.240
L 70/84

团　　体　　标　　准

T/ZSA 37-2020

移动智能终端密码技术政企应用指南

Cryptographic application guide for enterprise mobile smart terminal

2020-12-17 发布　　2020-12-18 实施

中关村标准化协会　　发布

目 次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。中关村标准化协会不承担识别专利的责任。

本文件由中关村标准化协会技术委员会提出并归口。

本文件涉及的密码算法按照国家密码管理部门的要求使用。

本文件起草单位：中关村网络安全与信息化产业联盟、成都卫士通信息产业股份有限公司、奇安信科技集团股份有限公司、江苏通付盾科技有限公司、江南信安（北京）科技有限公司、北京芯盾时代科技有限公司、北京数字认证股份有限公司、北京江南天安科技有限公司。

本文件主要起草人：刘洋、王克、汪德嘉、傅文斌、任飞、刘中、边晓彬、张凡、张浩、黄振海、徐剑南、孔维强等。

引　言

移动智能终端（mobile smart terminal MST）已成为政府、企事业单位信息处理的重要工具，密码技术在保护移动互联系统安全中得到越来越广泛应用。

T/EMCG 001-2019《移动智能终端密码模块技术框架》规范了移动智能终端四种密码模块技术架构，用于指导厂家设计、实现移动智能终端密码模块产品。

密码模块使用者——政府、企事业单位在规划移动互联信息系统时需了解密码技术作用，选择密码技术使用场景以及正确使用商用密码产品是促进密码技术推广使用的重要方面。

本文件指出了政企移动智能终端范围、使用环境以及面临的网络安全威胁，对10个移动智能终端密码技术典型应用（包括4种基础应用和6种系统应用）进行规范性说明，包括密码保护原理、密码模块部署以及密钥管理，附录A、B给出了网络安全等级保护基本要求有关条款与本文件章节对照以及信息系统密码应用基本要求条款与本文件章节对照，附录C、D给出了部分移动智能终端密码应用系统方案实例。

移动智能终端密码技术政企应用指南

1 范围

本文件提供了移动智能终端可信启动、App签名与验证、无线局域网接入、网络传输加密、语音电话加密、电子邮件加密、用户证书登录、电子签章、即时通讯加密、文件加密等方面的指导。

本文件适用于政府、企事业单位开展移动智能终端密码应用系统规划、设计和建设。相关厂商可参考本文件开展移动智能终端密码应用系统建设和服务。其他单位可参考本文件开展移动智能终端密码技术应用。

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 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/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 38540 信息安全技术 安全电子签章密码技术规范

GB/T 38541 信息安全技术 电子文件密码应用指南

GM/T 0024 SSL VPN技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0030 服务器密码机技术规范

GM/T 0034 基于SM2密码算法的证书认证系统密码及其相关安全技术规范

GM/T 0054 信息系统密码应用基本要求

GM/T 0055 电子文件密码应用技术规范

T/ZSA 3001.01 企业移动智能终端应用开发、安装、运行管控机制指南

T/EMCG 001-2019（所有部分） 移动智能终端密码模块技术框架

3 术语和定义

GM/Z 4001-2013界定的以及下列术语和定义适用于本文件。

3.1

App（移动应用软件）application

安装在移动智能终端上，能够利用移动智能终端设备上操作系统提供的开发接口，实现某项或某几项特定任务的应用程序，包括移动智能终端预置的应用程序，以及通过网站、应用商店等移动分发平台下载、安装和升级的应用程序。

[来源：T/ZSA 3001.01-2016，3.2]

3.2

App 分发渠道 App distribute medium

移动智能终端下载、安装App的媒介和途径。

3.3

App 开发者 App developer

从事企业移动智能终端应用软件开发的社会组织。

3.4

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

[来源：GM/Z 4001，2.19]

3.5

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

[来源：GM/Z 4001，2.23]

3.6

服务端密码组件 server side cryptographic components；SS-CC

部署在服务端中的密码组件，与移动智能终端密码组件（MST-CC）一起构成移动智能终端密码模块。

[来源：T/EMCG 001.2-2019，3.12]

3.7

官方机构 official authority

社会合法（公认）的组织，可是政府机构，也可是社会团体、企业、联盟、协会等实体，负责审核、管理和分发App。

[来源：T/ZSA 3001.01-2016，3.4]

3.8

公钥 public key

非对称密码算法中可以公开的密钥。

[来源：GM/Z 4001，2.28]

3.9

会话密钥 session key

在一次(通信)会话中使用的数据加密密钥。

[来源：GM/Z 4001，2.32]

3.10

加密公私钥对 key pair for encryption

非对称密码算法中用于实现数据机密性的公钥和私钥。

3.11

接入点 access point；AP

任何一个具备站点功能，通过无线媒体为关联的站点提供访问分布式服务的能力的实体。

[来源：GB 15629.11，3.2]

3.12

密码机 cryptographic machine

能够独立运行的，实现密码运算、密钥管理等功能，提供密码服务的设备。

[来源：GM/Z 4001，2.51]

3.13

密码组件 cryptographic component；CC

是密码模块的一部分，包括实现了安全功能的硬件、软件和/或固件。

[来源：T/EMCG 001.1-2019，3.4]

3.14

密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

[来源：GM/Z 4001，2.73]

3.15

密钥管理中心 key management center；KMC

负责密钥管理的机构。

[来源：GM/Z 4001，2.75]

3.16

密钥协商/密钥交换 key agreement/key exchange

两个或多个实体通过相互传送一些消息来共同建立一个共享的秘密密钥的协议，且各个实体无法预先确定这个秘密密钥的值。

[来源：GM/Z 4001，2.83]

3.17

签名公私钥对 key pair for signature

非对称密码算法中用于签名和验证的私钥和公钥。

3.18

SM2算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256比特。

[来源：GM/Z 4001，2.118]

3.19

SM3算法 SM3 algorithm

一种密码杂凑算法，其输出为256比特。

[来源：GM/Z 4001，2.119]

3.20

SM4 算法 SM4 algorithm

一种分组密码算法，分组长度为128比特，密钥长度为128比特。

[来源：GM/Z 4001，2.120]

3.21

商用密码 commercial cryptography

国家对密码实行分类管理，密码分为核心密码、普通密码和商用密码。商用密码是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

3.22

数字签名（密码签名、电子签名）digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

[来源：GM/Z 4001，2.113]

3.23

数字证书 digital certificate

也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

[来源：GM/Z 4001，2.115]

3.24

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

[来源：GM/Z 4001，2.116]

3.25

信息系统 information system

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目的和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

[来源：GB/T 25069，2.1.13]

注：在本文件中，信息系统特指政企单位建设的信息系统。

3.26

移动接入网关 mobile access gateway

能够独立运行的，并与移动智能终端一起实现对称密钥协商功能，保证数据传输的完整性、机密性和不可否认性的设备。

3.27

移动智能终端 mobile smart terminal；MST

能够接入移动通信网，具有提供应用软件开发接口的开放操作系统，并能够安装和运行第三方移动应用软件的移动设备。包括手机、Pad，这些设备可以是市场通用型的，也可以是政企机构专用型的。

[来源：T/EMCG 001.1-2019，5]

3.28

移动智能终端密码组件 mobile smart terminal cryptographic components；MST-CC

部署在移动智能终端中的密码组件，或独立构成，或与服务端密码组件（SS-CC）一起构成移动智能终端密码模块。

[来源：T/EMCG 001.2-2019，3.7]

3.29

ZUC算法 ZUC stream cipher algorithm

祖冲之序列密码算法，一种序列密码算法。

[来源：GM/Z 4001，2.154]

3.30

主密钥 master key；MK

处于对称密码系统层次化密钥结构中的顶层，用于下层密钥的产生或保护。

[来源：GM/Z 4001，2.152]

3.31

证书认证机构（证书认证中心、CA机构） certificate authority

负责生成、签发和管理证书的、受用户信任的权威机构。

[来源：GB/T 17901.1，3.5]

4 符号和缩略语

下列符号和缩略语适用于本文件。

AP：无线接入点 (WLAN) access point

API：应用程序接口 application programming interface

CA：证书认证机构 certificate authority

MK：主密钥 master key

MST：移动智能终端 mobile smart terminal

MST-CC：移动智能终端密码组件 mobile smart terminal cryptographic components

SS-CC：服务端密码组件 server side cryptographic components

等级保护：网络安全等级保护 classified protection of cybersecurity

TEE：可信执行环境 trust execution environment

TPM：可信平台模块 trust platform module

VPN：虚拟专用网络 virtual private network

WLAN：无线局域网 wireless local area network

WAPI：无线局域网鉴别与保密基础结构 wireless LAN authentication and privacy infrastructure

5 总则

5.1 移动智能终端

政企单位使用的移动智能终端（mobile smart terminal MST，或称移动终端）是政企单位人员用于处理工作事务（如移动办公、移动作业）的电子设备，如手机、平板电脑（PAD），MST可访问政企（非密）内部网络、数据及应用，也可与其他MST进行通信。

注：为益于阅读，本文件使用“政企”一词，其含义可泛指政府、企事业单位。

5.2 MST 接入政企网络

MST可通过公共移动网络设施，如蜂窝网、无线局域网（WLAN）、公共互联网（internet网络）访问政企（非密）内网信息系统，也可通过政企单位自建无线局域网（WLAN）访问政企（非密）内网信息系统。MST接入政企内网信息系统方式如图1所示。

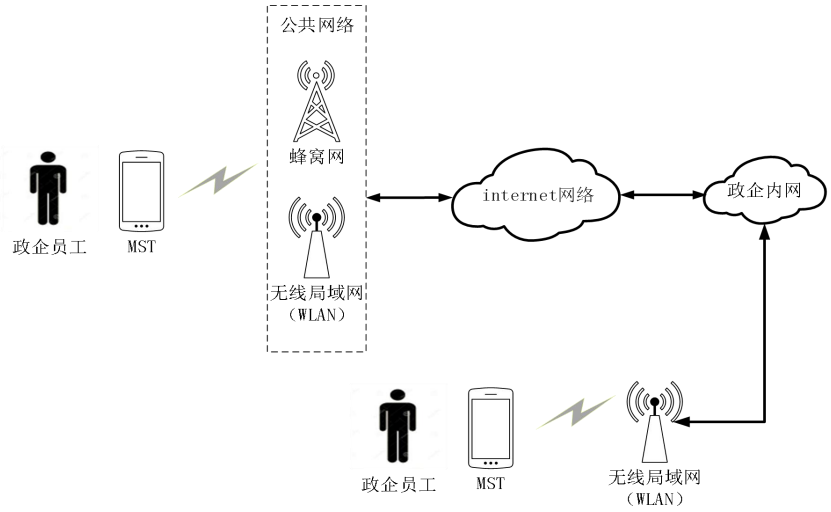


图1 MST接入政企内网信息系统方式

5.3 防范移动安全威胁

政企单位MST主要防范以下安全威胁：

——网络窃听。攻击者可在无线网络信道上或网络基础设施中窃听MST通信内容，包括文件、语音、图片、视频以及密码信息等。

——网络攻击。攻击者可在无线网络信道上或网络基础设施中主动向MST发起攻击（包括假冒、修改通信内容等），对MST中的应用软件（App）进行恶意更新，使MST访问恶意网址，以及添加带有恶意代码的电子邮件附件等。

——物理介入。MST丢失或被窃后，攻击者可通过其他设备、终端用户界面访问MST获取用户敏感数据，或直接破坏MST设备，读取设备中的存储介质，获取用户敏感数据。

——应用软件（App）攻击。MST可能下载恶意或谋利软件代码，这些代码可能是App开发者有意或无意加入，也可能来自开源软件库。恶意App可窃取MST数据，也可获得系统权限导致新的攻击，如，控制移动终端GPS、摄像头及麦克风等。

——高级持续威胁APT（advanced persistent threat）。由于受到攻击，MST丧失安全性，攻击者可以持续对MST数据实施控制，且如合法用户一样不被察觉。

5.4 MST 安全性

政企MST宜具备MST接入认证、用户身份验证、移动网络加密通信、MST文件加密、移动应用app签名/验证等安全功能，以应对网络信息系统移动安全威胁。

——保证信息机密性。采用密码技术对移动通信以及MST中的信息进行加密，使他人（没有密钥）不能读懂加密信息。如本文件给出的网络传输加密、语音电话加密、邮件加密及即时通讯加密、文件加密等技术。

——保证信息完整性。采用密码摘要算法（Hash算法）技术对移动通信以及MST中的软件、信息进行摘要计算，保证数据不被修改。如本文件给出的移动终端可信启动技术。

——保证用户行为不可抵赖性。采用密码技术对移动通信以及MST中的信息进行数字签名，使信息签名者不能抵赖其签名的行为。如本文件给出的App签名与验证、用户证书登录、电子签章技术。

MST宜具备一定的安全功能，如数据存储保护、文件访问控制、App签名验证、用户安全登录以及移动设备管理等，以保证本文件以下章节中的密码技术实施。

5.5 移动信息系统合规

政企单位开展移动信息系统建设遵守《中华人民共和国网络安全法》、《中华人民共和国密码法》等国家法规，宜满足GB/T 22239《信息安全技术 网络安全等级保护基本要求》、GM/T 0054《信息系统密码应用基本要求》、GB/T 35273《信息安全技术 个人信息安全规范》等国家、行业标准要求。

6 基础应用

6.1 可信启动

6.1.1 应用场景

MST可信启动是使用密码技术，在MST启动引导过程中对系统引导程序、操作系统内核进行完整性校验，防止系统引导程序及操作系统内核被非法篡改。

对于MST可信启动的重要性宜了解国家、行业标准：

- GB/T 22239对计算环境提出了可信验证要求，见附录A。
- GM/T 0054对设备和计算安全提出了重要程序或文件进行完整性保护要求，见附录B。

6.1.2 密码保护原理

为了保证MST引导程序及操作系统内核不被非法修改，在MST硬件、软件开机“启动链”（开机ROM指令→引导程序→操作系统内核加载到处理）中，使用公钥密码或摘要算法技术对引导程序、操作系统内核代码逐层进行完整性验证，直至MST完全启动，一旦某一层验证不通过则终止系统启动。MST可信启动原理如图2所示。

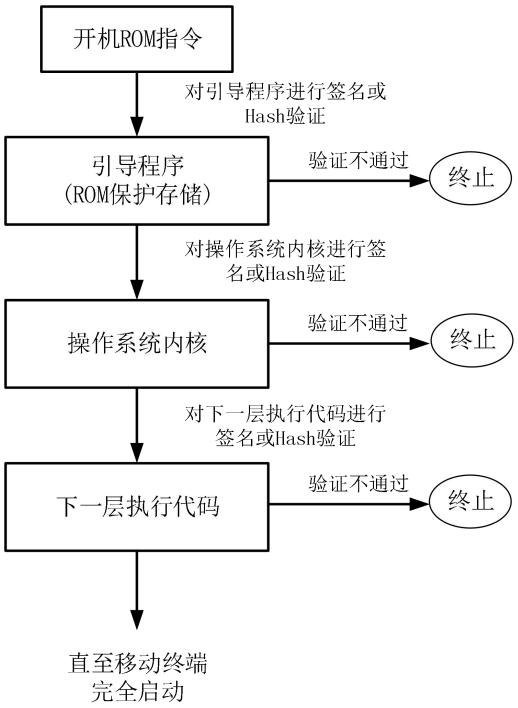


图 2 MST 可信启动原理

6.1.3 密码模块部署

MST可信启动一般使用MST出厂搭载的硬件密码模块（如TPM安全芯片、TEE芯片），由启动链各层代码调用。硬件密码模块可采用T/EMCG 001.5-2019技术架构实现，并经国家商用密码检测机构检测认证。

6.1.4 密钥管理

MST可信启动使用国家密码主管部门批准的非对称密码算法（如SM2）、摘要算法(如SM3)，涉及的密钥包括：

——引导程序签名验证公钥。非对称密钥，由MST厂家生成，保存在不可修改的存储器中，用于MST开机时对引导程序进行签名验证。

——操作系统内核签名验证公钥。非对称密钥，由MST厂家（或操作系统厂家）生成，保存在引导程序中，用于引导程序时对操作系统内核进行签名验证。

——下一层执行代码签名公钥。非对称密钥，由执行代码开发者生成，保存在操作系统内核中，用于操作系统内核对下一层执行代码进行签名验证。

MST可信启动密钥管理宜遵循GM/T 0054密钥管理要求，见附录B。

6.2 App 签名与验证

6.2.1 应用场景

App签名与验证是采用公钥密码技术对政企移动App进行实名签名与验证，以防止App被篡改和仿冒，保证App完整性以及App责任可溯源性，且保护App知识产权。

a) **App签名**

1) 移动App签名包括App开发者签名和官方机构（App分发渠道）签名。
2) App开发者签名是开发者使用公钥密码技术对开发的App进行数字签名。
3) 官方机构（App分发渠道）签名是官方机构使用公钥密码技术对其审核、管理和发布的App进行数字签名，防止恶意App传播。

b) **App验证**

1) 移动App签名验证包括官方机构（App分发渠道）验证和MST验证。
2) 官方机构（App分发渠道）验证是官方机构（App分发渠道）在审核、管理及发布App时使用公钥密码技术对App开发者的App进行签名验证，确保App开发者的真实性。
3) MST验证是MST在安装、运行App时操作系统使用公钥密码技术对官方机构（App分发渠道）发布的App进行签名验证，以决定是否安装和运行该App，可实现政企在自己专用MST上运行指定官方机构（App分发渠道）分发的App。

对于MST App签名与验证的重要性宜了解国家、行业标准：

- GB/T 22239对移动App提出了签名与验证要求，见附录A。
- GM/T 0054对应用和数据安全提出了重要程序的加载和卸载进行安全控制要求，见附录B。

6.2.2 密码保护原理

App开发者签名。App开发者使用其在官方机构（App分发渠道）登记的私钥对其开发的App进行数字签名。由于数字签名可保证签名数据完整性，官方机构（App分发渠道）及MST可通过验证App签名识别App开发者真实身份，从而决定是否发布、安装和运行该App。如果App被篡改或仿冒，可通过验证App签名发现。如果App没有被篡改，依据《中华人民共和国电子签名法》该App开发者应对App运行结果负法律责任。因此，数字签名不可抵赖性保证了App软件责任可溯源。

对App实施数字签名是将软件安全关口向开发阶段前移，从而增强App开发者责任意识，对提高计算机网络安全性起到重要作用。

官方机构（App分发渠道）签名。官方机构（App分发渠道）使用自己的私钥对开发者签名的App进行二次签名，仍保持App开发者签名的有效性，即“双签名”。采用双签名机制保证App是经过官方机构安全审核、检测的，防止恶意App传播，进一步降低App安全风险。

App开发者和官方机构（App分发渠道）App双签名原理如图3所示。

图 3 App 开发者和官方机构（App 分发渠道）App 双签名原理

MST验证App签名。MST在安装或运行App时使用开发者数字证书中开发者公钥，对App开发者签名进行验证，验证App是否被篡改，再使用指定官方机构（App分发渠道）公钥，对开发者数字证书进行验证，验证开发者是否真实；MST使用指定官方机构（App分发渠道）公钥，对官方机构（App分发渠道）App签名进行验证，验证App是否是指定官方机构（App分发渠道）发布。MST App开发者签名验证及官方机构（App分发渠道）App签名验证，即MST“双验证”。

官方机构（App分发渠道）验证App签名。官方机构（App分发渠道）收到App开发者开发的App，用开发者数字证书中的公钥，对其App签名进行验证，验证App是否被篡改，再使用官方机构（App分发渠道）公钥，对该App开发者的数字证书进行验证，验证其是否是本官方机构（App分发渠道）签发，如是，则说明该开发者是经本官方机构审核、注册的，从而保证开发者身份的有效性、真实性，并且此App没有被篡改。

App开发者、官方机构（App分发渠道）以及MST App签名与验证过程宜遵循T/ZSA 3001.01。

6.2.3 密码模块部署

App 签名与验证宜采用以下密码模块部署：

a) 在 App 开发者软件开发系统以及官方机构（App 分发渠道）系统中部署硬件或软件密码组件/模块对 App 进行数字签名与验证；

b) 在 MST 操作系统中部署移动终端密码组件（MST-CC）在 App 安装、运行时对 App 进行数字签名验证；

c) 密码组件/模块可采用 T/EMCG001-2019 技术架构实现，并经国家商用密码检测机构检测认证。

App 签名与验证密码组件/模块部署如图 4 所示。

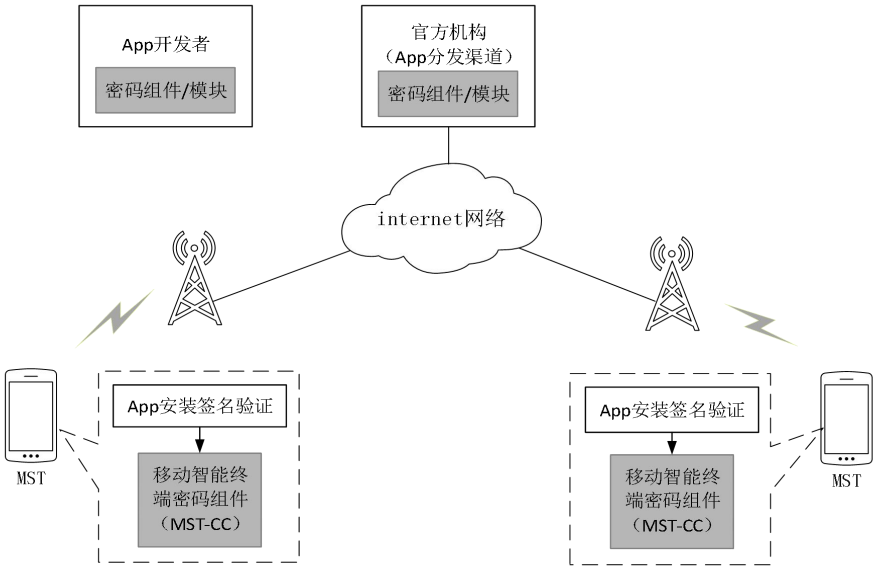


图 4 App 签名与鉴别密码模块部署

6.2.4 密钥管理

MST App数字签名与验证使用国家密码主管部门批准的非对称密码算法（如SM2），涉及管理的密钥：

——官方机构（App 分发渠道）签名公钥和私钥。非对称密钥，由官方机构使用的密码组件/模块产生，私钥在官方机构（App 分发渠道）的密码组件/模块中保护，公钥以官方机构数字证书形式保存在 MST（操作系统）中。

——App 开发者签名公钥和私钥。非对称密钥，由 App 开发者使用的密码组件/模块产生，私钥在开发系统的密码组件/模块中保护，公钥以开发者数字证书方式由官方机构（App 分发渠道）签发给 App 开发者，App 开发者向官方机构提交 App 时，将开发者数字证书一同提供给官方机构。

MST App 数字签名密钥管理宜遵循 GM/T 0054 密钥管理要求，见附录 B。

6.3 无线局域网接入

6.3.1 应用场景

在政企内网中架设无线局域网（WLAN），如WAPI（无线局域网鉴别与保密基础结构）、WiFi，MST通过WLAN接入单位信息系统是政企移动作业的一种方式。由于WAPI协议具有完备的密码技术保障，本文件以WAPI为例说明无线局域网接入密码应用。

采用WAPI对无线局域网空口接入进行控制，实现MST与无线接入点（AP）身份鉴别、接入控制、密钥管理及数据保密通信等功能，防止非法MST接入政企内网、政企MST接入非法网络，防范无线传输数据泄露。

对于MST无线局域网安全接入的重要性宜了解国家、行业标准：

- GB/T 22239对三级以上系统移动互联访问控制密码使用提出了要求，见附录A。
- GM/T 0054对网络和通信安全提出了连接到内部网络的设备进行安全认证要求，见附录B。

6.3.2 密码保护原理

政企信息系统运行前，MST、AP在政企证书认证中心（CA）、密钥管理中心进行注册并生成自己的公钥、私钥及数字证书。当MST通过WLAN接入政企信息系统时，MST和AP使用自己的数字证书及私钥通过鉴别服务器进行双向身份鉴别，鉴别服务器通过事先注册的MST和AP的数字证书判别它们是否是政企单位的合法设备，鉴别成功后，MST方可接入政企信息系统，并采用对称加密算法对通信内容进行加密保护。WAPI协议技术要求宜遵循GB 15629.11。

注：密钥管理中心、鉴别服务器也可布置在第三方公共平台上。

WLAN接入密码保护基本原理如图5所示。

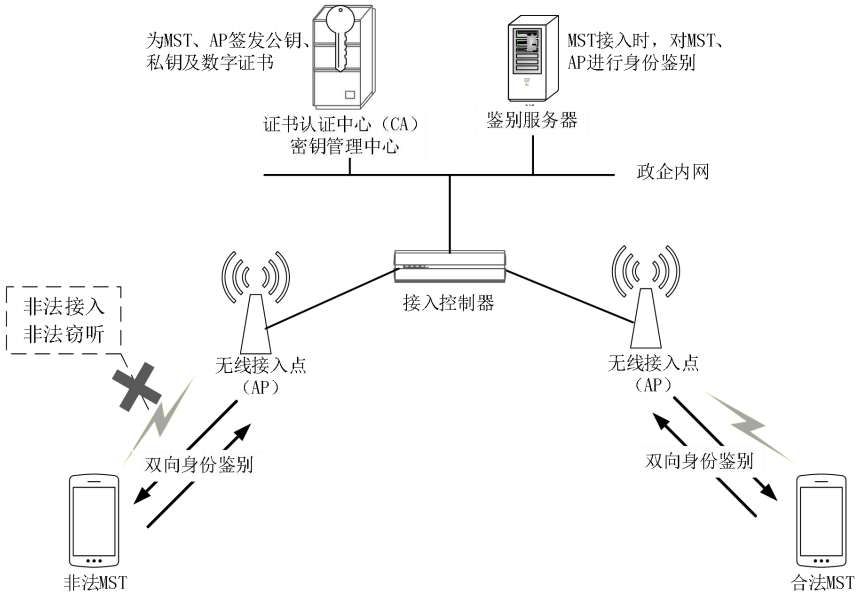


图5 WLAN接入密码保护基本原理框图

6.3.3 密码模块部署

WAPI无线局域网接入安全宜使用硬件或软件密码组件/模块进行保护。其中支持对称密码算法的密码组件/模块部署在MST和AP上，支持签名和杂凑算法的密码组件/模块部署在MST、AP以及鉴别服务器上。WAPI接入密码模块部署如图6所示。

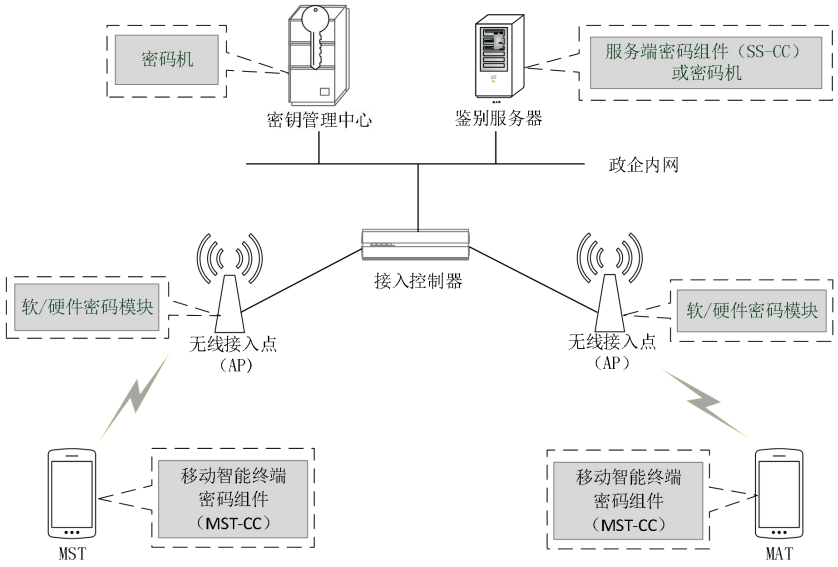


图6 WAPI接入安全密码模块部署

a) WAPI系统中，MST和AP使用硬件或软件密码组件/模块实现数字证书下载或导入、身份鉴别、密钥协商、通信数据加解密以及密钥参数管理和保护。

b) 鉴别服务器使用硬件或软件密码组件/模块实现数字证书有效性验证及验证结果处理。

c) 密码组件/模块应支持国家密码管理部门批准的用于无线局域网的非对称密码算法和对称密码算法，宜满足GM/T 0028要求，并经国家商用密码检测机构检测认证。

d) 密钥管理中心部署服务器密码机，提供相关密码服务，服务器密码机应使用并经国家商用密码检测机构检测认证的产品。密码机宜符合GM/T 0030要求。

e) 可采用符合GM/T 0034的密钥管理中心，并经国家商用密码检测机构检测认证。

6.3.4 密钥管理

在WAPI系统使用国家密码管理部门批准的对称密码算法（如SM4）、摘要算法和非对称密码算法，实现MST和AP的安全加密保护，涉及管理的密钥：

——MST 和 AP 的公钥和私钥。非对称密钥，密钥管理中心负责其生命周期管理，包括密钥的生成、分发、存储、更新及销毁等。

——MST 和 AP 的私钥可遵循 T/EMCG 001-2019 保存在各自的密码组件/模块中。

——MST 和 AP 的公钥由证书认证中心放入各自证书中，发到 MST 和 AP 中。

——MST 和 AP 的通信加密会话密钥，在 MST 接入鉴别成功后通过 WAPI 协议协商得到，用于对通信信息进行加密。

无线局域网接入密钥管理宜遵循 GM/T 0054 密钥管理要求，见附录 B。

6.4 网络传输加密

6.4.1 应用场景

移动网络传输加密是使用密码技术对移动互联网通信数据实施加解密计算，可实现政企信息系统MST实体鉴别和数据传输加密保护，防止政企数据在网络传输中泄露和篡改。

对于MST网络传输加密的重要性宜了解国家、行业标准：

- GB/T 22239对三级以上系统传输数据完整性、保密性提出了要求，见附录A。
- GM/T 0054对网络和通信安全提出了身份认证、传输数据机密性、完整性要求，见附录B。

注：GB/T 22239、GM/T 0054所述的保密性和机密性词义相同。

6.4.2 密码保护原理

移动网络传输加密是在移动网络传输中加入密码保护机制，在政企信息系统移动接入网关和MST之间建立一条保密通道，实现通信数据加密传输以及MST实体鉴别。

MST与移动接入网关采用非对称密码算法，通过它们在证书认证中心签发的公钥和私钥生成用于数据传输加密的“会话密钥”，对通信信息进行加解密，使得加密信息在MST和移动接入网关之间经过的线路（包括无线、有线）及设备中（在没有获得解密密钥情况下）无法还原信息明文，保证MST和移动接入网关通信信息的全程传输安全，也保证了MST接入政企内网的合法性。移动网络传输加密宜遵循GM/T 0024实施。

移动网络传输加密原理如图7所示。

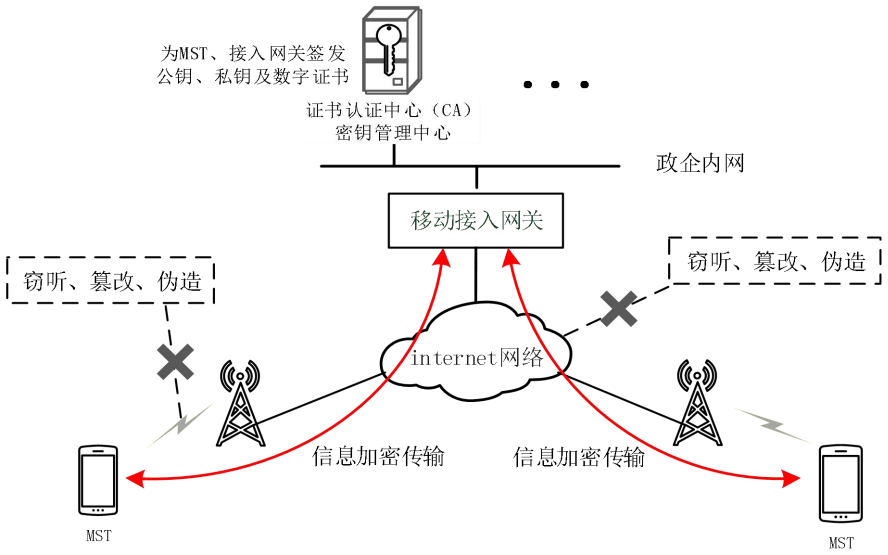


图7 网络传输加密密码应用原理

6.4.3 密码模块部署

移动网络传输加密宜使用硬件或软件密码组件/模块实施移动通信数据加密。网络传输加密密码模块部署如图8所示。

a) MST密码组件（MST-CC）部署在MST上，由MST通信客户端软件调用，服务端密码组件（SS-CC）或密码机部署在政企内网移动接入网关上。

b) 可采用T/EMCG 001-2019技术架构实现的密码组件/模块，并经国家商用密码检测机构检测认证。

c) 可采用符合GM/T 0030的密码机，并经国家商用密码检测机构检测认证。

d) 可采用符合GM/T 0034的证书认证中心和密钥管理中心，并经国家商用密码检测机构检测认证。

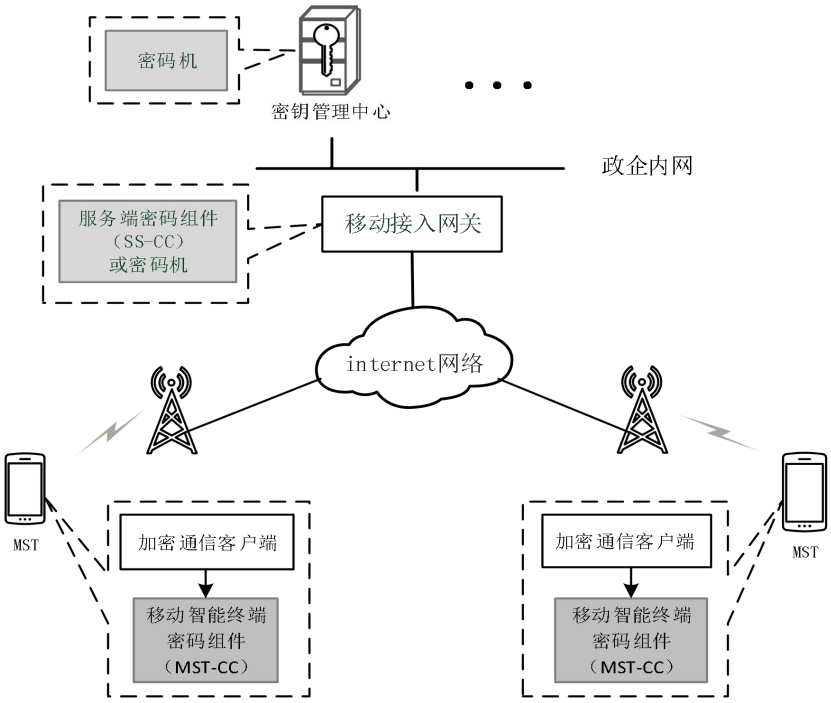


图8 网络传输加密密码模块部署

6.4.4 密钥管理

网络传输加密需要使用国家密码主管部门批准的对称密码算法（如SM4、ZUC）、Has算法(如SM3)和非对称密码算法（如SM2），涉及管理的密钥：

——移动接入网关加密公私钥对：公钥（P_S）和私钥（d_S）。非对称密钥，由密钥管理中心密码机产生，用于“会话密钥”加密保护，P_S 预置在 MST-CC 中，ds 在密钥管理中心和移动接入网关密码组件/模块中存储。

——MST 加密公私钥对：公钥（P_M）和私钥（d_M）。非对称密钥，MST-CC 初始化时有密钥管理中心产生，用于“会话密钥”加密保护，d_M 用 MST 主密钥（MK）加密保存在 MST-CC 中，并加密备份保存在密钥管理中心中。

——MST 主密钥（MK）。对称密钥，MST-CC 初始化时产生，由 MST 用户掌握，不在 MST-CC 和信息系统中保存，用于 MST-CC 私钥 d_M 加密保护。 MK 生成和使用遵循 T/EMCG 001-2019。

——会话密钥。对称密钥，每次加密通信建立时，由 MST 和移动接入网关协商产生，用于通信信息加密，用公钥密码算法保护。

网络传输加密密钥管理宜遵循 GM/T 0054 密钥管理要求，见附录 B。

7 系统应用

7.1 语音电话加密

7.1.1 应用场景

移动语音电话加密是使用密码技术对MST通话双方（不包括电话会议）的语音信息进行加密处理，实现政企工作人员之间使用MST进行语音通信的加密保护。

对于MST语音电话加密的重要性宜了解国家、行业标准：

- GB/T 22239对三级以上系统传输数据完整性、保密性提出了要求，见附录A。
- GM/T 0054对应用和数据安全提出了保证重要数据在传输过程中的机密性、完整性要求，见附录B。

注：GB/T 22239、GM/T 0054所述的保密性和机密性词义相同。

7.1.2 密码保护原理

常用的语音加密方法有直接加密法和选择加密法。

- **直接加密法：**将需要加密的语音信息作为二进制数据，使用密码算法对整体语音信息进行加密。
- **选择加密法：**一般针对多媒体通信，只对其中较重要的语音信息进行加密。

以下以直接加密法为例进行说明。

在移动通信网络VoIP（Voice over Internet Protocol互联网协议语音传输）系统中加入密码保护机制，由MST上的VoIP语音通信客户端调用密码组件/模块实现对语音数据加密保护。

MST A与MST B在建立VoIP语音通道开始时，双方协商产生“会话密钥”,对语音信息进行加密，使得在语音加密信息经过的线路（包括无线、有线）及设备中（在没有获得解密密钥情况下）无法还原语音信息明文，保证通话内容从A到B全程安全传输。

MST语音电话加密原理如图9所示。

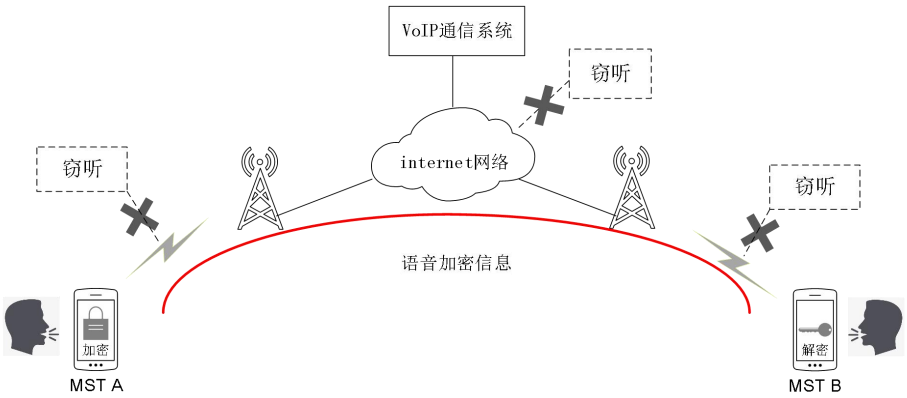


图9 MST语音电话加密原理

7.1.3 密码模块部署

移动语音电话加密宜使用密码组件/模块包括：MST密码组件（MST-CC）、服务端密码组件（SS-CC）或密码机。MST语音电话加密密码模块部署如图10所示。

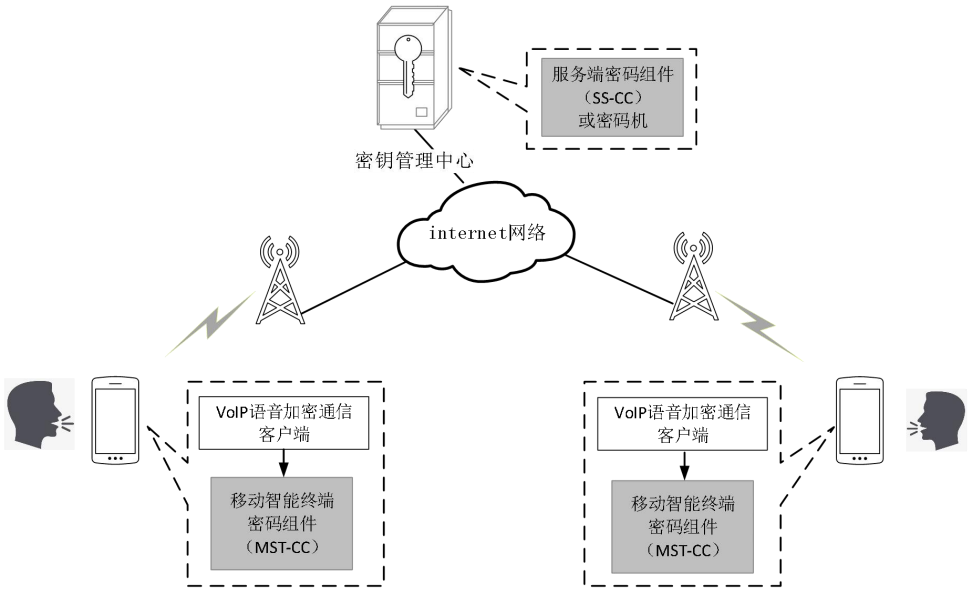


图 10 MST 语音电话加密密码模块部署

a) MST-CC 部署在 MST 上，由 VoIP 语音加密通信客户端通过调用密码组件/模块应用程序接口（API），实现语音信息加解密、密钥参数管理和保护。

b) SS-CC 或密码机部署在密钥管理中心，用于 MST-CC 初始化、密钥参数管理和保护。

c) 可采用 T/EMCG 001-2019 技术架构设计、实现 MST-CC 和 SS-CC。

d) 可采用符合 GM/T 0030 的密码机，并经国家商用密码检测机构检测认证。

e) 可采用符合 GM/T 0034 的密钥管理中心，并经国家商用密码检测机构检测认证。

7.1.4 密钥管理

移动语音电话加密需要使用国家密码主管部门批准的对称密码算法（如SM4、ZUC）、摘要算法(如SM3)和非对称密码算法（如SM2），涉及管理的密钥：

——密钥管理中心加密公私钥对：公钥（P_S）和私钥（d_S）。非对称密钥，由密钥管理中心密码机产生，P_S 预置在 MST-CC 中，ds 存储在密码机中，用于 MST 初始化时与 SS-CC 安全通信。

——MST（用户）加密公私钥对：公钥（P_M）和私钥（d_M）。非对称密钥，MST-CC 初始化时由密钥管理中心产生，并安全分发到 MST-CC，用于通话双方密钥协商时保护会话密钥，d_M 安全保存在 MST-CC 中，并加密备份保存在密钥管理中心。

——MST 用户主密钥（MK）。对称密钥，MST-CC 初始化时产生，由 MST 用户掌握，不在 MST-CC 和信息系统中存储，用于 MST-CC 敏感信息加密保护。MK 生成和使用遵循 T/EMCG 001-2019。

——会话密钥。对称密钥，用于语音信息加密，每次 VoIP 通话建立时，由通话双方 VoIP

语音加密通信客户采用非对称密码技术完成会话密钥协商生成。

语音电话加密密钥管理宜遵循 GM/T 0054 密钥管理要求，见附录 B。

注：也可采用密钥管理中心分配对称密钥的方法对会话密钥进行保护，本文件不作描述。

7.2 电子邮件加密

7.2.1 应用场景

移动电子邮件加密是使用密码技术对邮件内容(包括标题、正文、附件等)进行加密处理，防止邮件内容在传输中被非授权者知悉、篡改或伪造。

对于MST电子邮件加密的重要性宜了解国家、行业标准：

- GB/T 22239对三级以上系统传输数据完整性、保密性提出了要求，见附录A。
- GM/T 0054对应用和数据安全提出了保证重要数据在传输过程中的机密性、完整性要求，见附录B。

注：GB/T 22239、GM/T 0054所述的保密性和机密性词义相同。

7.2.2 密码保护原理

常用的电子邮件加密方法是数字信封加密法。数字信封加密法综合使用对称算法加密法和非对称算法加密法，避免了对称算法加密法密钥分配成本高，以及非对称算法加密法加解密效率低的问题。

以下以数字信封加密法为例进行说明。

在电子邮件系统中加入密码保护机制，由MST邮件客户端调用密码组件/模块对邮件内容(包括正文、附件等)加密，经由邮件服务器转发到接收方的邮箱中，接收方MST邮件客户端进行解密。从而实现邮件内容在传输经过的线路（包括无线、有线）及网络设备中（在没有获得解密密钥情况下）无法还原成明文，防止通信内容被窃听、篡改和伪造。邮件内容密文在MST邮件客户端和邮件服务端均加密存储，即使邮件服务商也不能知晓邮件内容。

MST电子邮件加密原理如图11所示。

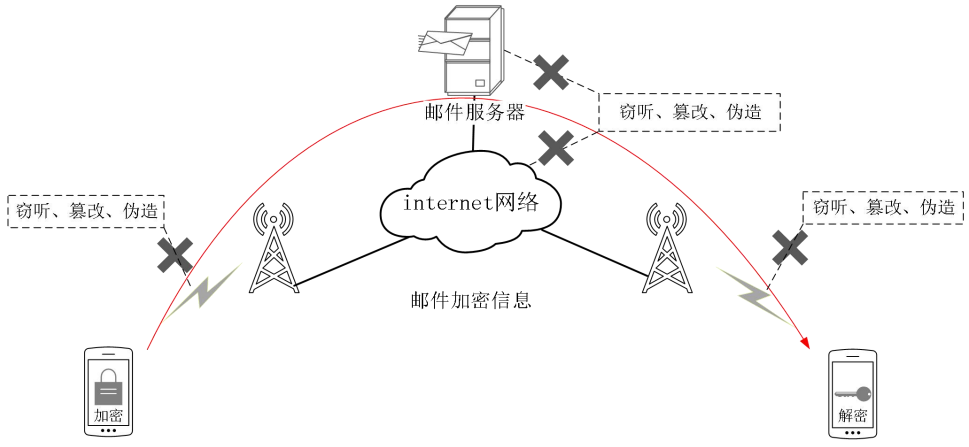


图 11 MST 电子邮件加密原理

7.2.3 密码模块部署

MST电子邮件加密宜使用密码模块包括：MST密码组件（MST-CC）、服务端密码组件（SS-CC）或密码机。MST电子邮件加密密码模块部署如图12所示。

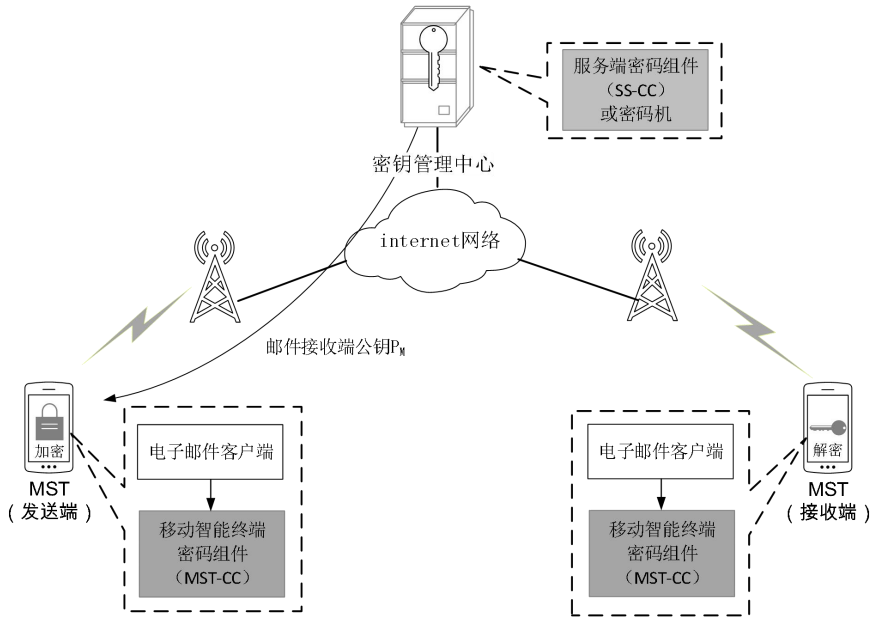


图 12 MST 电子邮件加密密码模块部署

a) MST-CC 部署在 MST 上，由电子邮件加密通信客户端通过调用密码组件/模块应用程序接口（API），实现邮件内容加解密、密钥参数管理和保护。

b) SS-CC 或密码机部署在政企内部（或第三方）密钥管理中心，用于 MST-CC 初始化、密钥参数管理和保护；发邮件时，密钥管理中心向邮件发送方提供邮件接收方公钥（P_M）。

c) 可采用 T/EMCG 001-2019 技术架构设计、实现 MST-CC 和 SS-CC，并经国家商用密码检测机构检测认证。

d) 可采用符合 GM/T 0030 的密码机，并经国家商用密码检测机构检测认证。

e) 可采用符合 GM/T 0034 的密钥管理中心，并经国家商用密码检测机构检测认证。

7.2.4 密钥管理

移动电子邮件加密使用国家密码主管部门批准的对称密码（如SM4、ZUC）、摘要算法(如SM3)和非对称密码算法（如SM2），涉及管理的密钥：

——密钥管理中心加密公私钥对：公钥（P_S）和私钥（d_S）。非对称密钥，由密码机产生，P_S 预置在 MST-CC 中，ds 存储在服务器密码机中，可用于 MST-CC 初始化时与 SS-CC 安全通信。

——MST（用户）公私钥对：公钥（P_M）和私钥（d_M）。非对称密钥，MST-CC 初始化时由密钥管理中心产生，并安全分发到 MST-CC，可用于 MST-CC 初始化时与 SS-CC 安全通信；d_M 安全保存在 MST-CC 中，加密备份存储在密钥管理中心中。

——MST 用户主密钥（MK）。对称密钥，MST-CC 初始化时产生，由 MST 用户掌握，不在 MST-CC 和信息系统中存储，用于 MST-CC 敏感信息加密保护。MK 生成和使用遵循 T/EMCG 001-2019。

——会话密钥。对称密钥，用于电子邮件内容加密，由 MST-CC 在随机产生，用邮件接收端 MST-CC 公钥 P_M 加密，发送给邮件接收端。

移动电子邮件加密密钥管理宜遵循 GM/T 0054 密钥管理要求，见附录 B。

7.3 用户证书登录

7.3.1 应用场景

MST用户使用密码技术登录政企信息系统（如移动办公系统、手机银行等），实现用户身份鉴别，防止非法人员访问政企信息系统。

对于MST用户证书登录的重要性宜了解国家、行业标准：

- GB/T 22239对三级以上系统用户身份鉴别密码使用提出了要求，见附录A。
- GM/T 0054对应用和数据安全提出了对登录的用户进行身份鉴别要求，见附录B。

7.3.2 密码保护原理

证书登录的安全性依赖于公钥密码数字签名的不可篡改性，其基本原理：用户和政企信息系统互相交换已签名数据，分别对对方的签名数据进行验证，以鉴别对方身份的真实性、合法性，从而保证政企信息系统不被非法用户访问，同时保证用户访问的政企信息系统也是真实的。

实现用户证书登录过程有多种，可根据实际情况参考ISO/IEC 9798-3:2019进行选择。以下给出一种用户证书登录过程，如图13所示。

假设，用户A是政企信息系统（简称信息系统）注册用户，已获得CA机构签发的公钥（P_M）、私钥（d_M）、包含P_M的数字证书Cert-M以及CA机构公钥（P_C）；信息系统也拥有CA机构签发的公钥（P_S）、私钥（d_S）、包含P_S的数字证书Cert-S以及CA机构公钥（P_C）。用户A证书登录信息系统基本步骤如下：

a) 用户 A 向信息系统发出登录请求；

b) 信息系统生成随机数 R_S，使用自己的私钥 d_S 对 R_S 签名得令牌 Token-S，将 Token-S、信息系统证书 Cert-S 发送给用户 A；

c) 用户 A 使用 CA 机构公钥（P_C）验证证书 Cert-S 合法性，再使用 Cert-S 中公钥 Ps 验证令牌 Token-S 合法性，获得 R_S；

d) 用户 A 生成随机数 R_M，使用自己私钥 d_M 对 R_S 和 R_M 合并签名，得到令牌 Token-M，将 Token-M 和用户 A 证书 Cert-M 发送给信息系统；

e) 信息系统使用 CA 机构公钥（P_C）验证 Cert-M 合法性；再使用 Cert-M 中公钥 P_M 验证令牌 Token-M 合法性，得到两个随机数 R_S、R_M；校验 R_S 与第 2）步生成的 R_S 是否一致，若一致则登录成功；

f) 信息系统通知用户 A 登录是否成功。

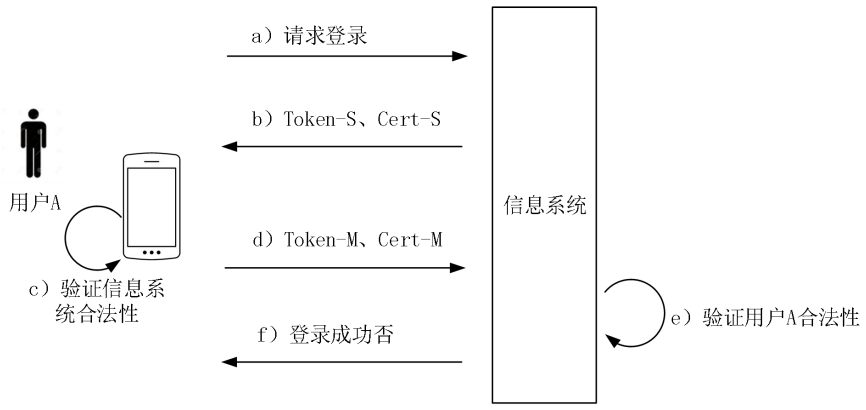


图 13　MST 用户证书登录原理

上述第2）步，信息系统使用自己私钥d_S对随机数R_S签名得到令牌Token-S，第3）步用户A使用信息系统的公钥Ps对Token-S验签，如果通过验签，根据公钥密码特性说明Token-S是信息系统签名，从而用户A认定信息系统是合法的。

同理，第4）步，用户A使用自己私钥d_M对随机数R_M签名得到令牌Token-M，第5）步信息系统使用用户A的公钥P_M对Token-M验签，如果通过验签，根据公钥密码特性说明Token-M是用户A签名，从而信息系统认定用户A是合法的。

第2）、4）步随机数R_S、R_M作用是防御登录认证过程网络重放攻击。

7.3.3 密码模块部署

移动用户证书登录宜使用密码模块包括：MST密码组件（MST-CC）、服务端密码组件（SS-CC）或密码机。

a)　MST 部署 MST-CC，由政企信息系统客户端调用。

b)　政企信息系统部署 SS-CC 或密码机。

c)　MST-CC 和 SS-CC 可采用 T/EMCG 001-2019 技术架构实现，并经国家商用密码产品测评机构认证。

d)　可采用符合 GM/T 0030 的服务器密码机，经国家商用密码产品测评机构认证的产品。

移动用户证书登录使用密码模块部署如图 14 所示。

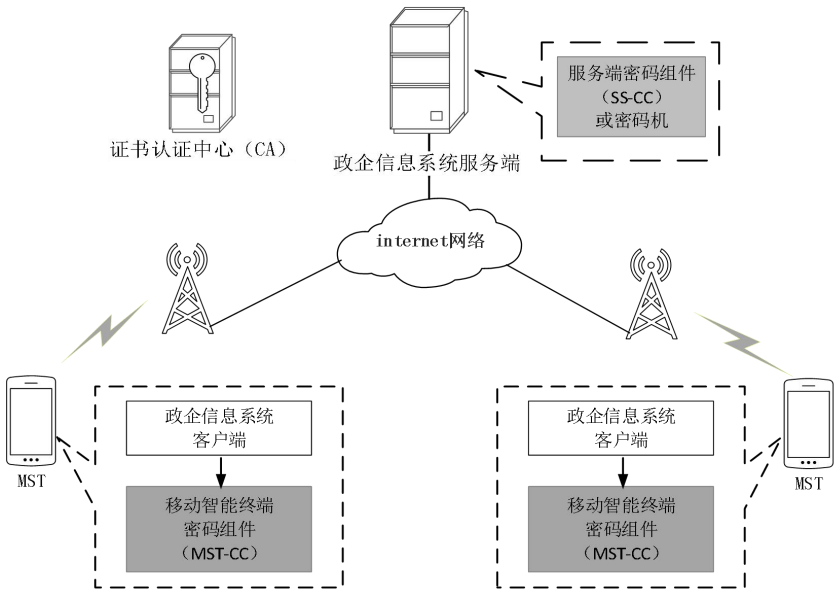


图 14 移动用户证书登录密码模块部署

7.3.4 密钥管理

移动用户证书登录主要使用国家密码主管部门批准的非对称密码算法（如SM2），涉及管理的密钥：

——MST(用户)公私钥对：公钥（P_M）和私钥（d_M）。非对称密钥，用户在向政企信息系统注册时由 MST-CC 产生，d_M在 MST-CC 中保护，P_M包含在用户数字证书中（由政企或第三方 CA 机构签发），存储在 MST-CC。

——政企信息系统公私钥对：公钥（P_S）和私钥（d_S）。非对称密钥，由 SS-CC 产生，d_S在 SS-CC 中保护，P_S包含在政企信息系统数字证书中（由政企或第三方 CA 机构签发），存储在政企信息系统服务端。

MST 用户证书登录密钥管理宜遵循 GM/T 0054 密钥管理要求，见附录 B。

7.4 电子签章

7.4.1 应用场景

MST电子签章将可视化印章图形与数字签名绑定，在MST电子文档中实现数字签名可视化，确保文件印章可信、文件内容未被篡改。根据《中华人民共和国电子签名法》，政企单位在网上移动办公进行公文流转、审批、签订电子合同时，使用的电子签章与纸质盖章、手写签名具有同等法律效力。

对于MST电子签章的重要性宜了解国家、行业标准：

- GB/T 22239对三级以上系统数据、涉及法律责任认定数据的完整性及抗抵赖提出了要求，见附录A。
- GM/T 0054对应用和数据安全提出了实体行为不可否认性的要求，见附录B。

7.4.2 密码保护原理

电子签章过程：“盖章”操作者（简称“盖章者”）经授权将政企电子印章数据与待盖章的电子文件进行绑定，即在电子文件上形成可视印章图形——带印文件（文件中包括电子印章数据、政企数字证书等信息），再使用政企单位私钥，通过公钥密码算法对带印文件进行数字签名，生成“电子签章文件”。电子签章原理如图15所示。

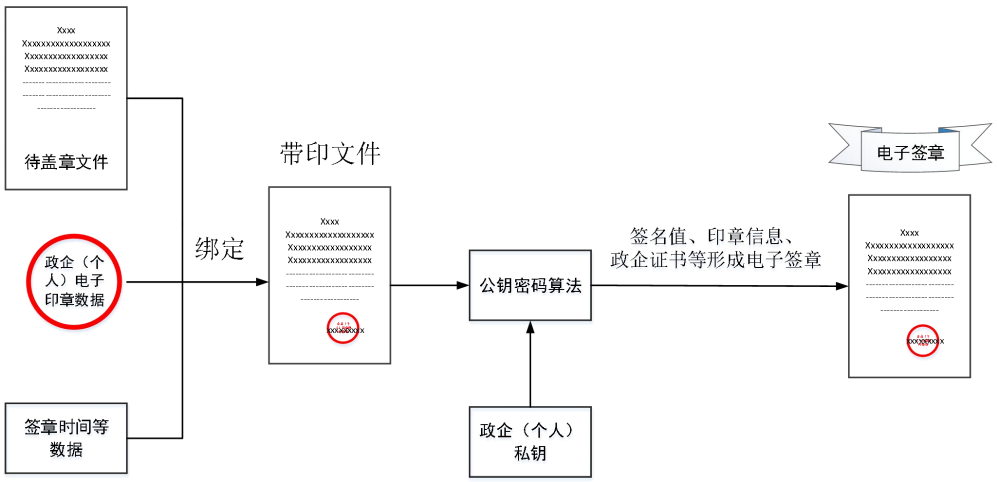


图15 电子签章原理

电子签章验证：使用政企单位的公钥对已签章文件的签章数据进行验证，包括数字签名、盖章者的数字证书等信息，如果验证通过，根据数字签名不可抵赖性原理，说明该电子文件的签章是政企单位的合法印章，且文件未被篡改，此电子签章与纸质签章具有同等法律效力。

电子印章及电子签章数据格式、生成与验证宜遵循GB/T 38540。

个人电子签章原理同政企电子签章。政企/个人数字证书由第三方CA机构签发。

在移动办公场景中，若使用软件密码模块，为保证盖章者私钥安全，宜采用协同方式生成MST与服务端各自的密钥分量，双方协同完成电子签章。服务端可在政企内部自行部署基于协同签名技术的签章系统，也可采用第三方提供的协同签章服务，完成密钥存储、密钥协商、电子签名等功能。

附录C给出一种基于多方协同方式的移动智能终端电子签章实例。

7.4.3 密码模块部署

在MST上宜部署移动终端密码组件（MST-CC），实现对电子文件签章和验证。

MST-CC可采用T/EMCG 001-2019技术架构实现，并经国家商用密码检测机构检测认证。

7.4.4 密钥管理

电子签章使用国家密码主管部门批准的非对称密码算法（如SM2），涉及管理的密钥：

——政企单位公钥和私钥：公钥（P_s）和私钥（d_s）。非对称密钥，d_s 可遵循 T/EMCG 001-2019 在授权盖章者移动终端密码组件（MST-CC）中安全存储，P_s 存放在由 CA 机构签

发的数字证书中。

对于采用多方协同方式实现电子签章：

——通过多方协同方式生成MST与服务端各自的密钥分量，各方通过密码设备/模块等方式进行加密保护。

——公钥存放在由CA机构签发的数字证书中。

——密钥分量生成及协同计算过程可遵循T/EMCG 001.4-2019。

MST电子签章密钥管理宜遵循GM/T 0054密钥管理要求，见附录B。

7.5 即时通讯加密

7.5.1 应用场景

移动即时通信加密是使用密码技术对即时通信系统（Instant Message System，IMS，如微信）群组通信内容（包括文字、语音、短视频、文件等）进行加密，防止消息内容在传输中被非授权者知悉、篡改和伪造。

对于MST即时通信加密的重要性宜了解国家、行业标准：

- GB/T 22239对三级以上系统传输数据完整性、保密性提出了要求，见附录A。
- GM/T 0054对应用和数据安全提出了保证重要数据在传输过程中的机密性、完整性要求，见附录B。

注：GB/T 22239、GM/T 0054所述的保密性和机密性词义相同。

7.5.2 密码保护原理

即时通讯加密通常使用对称算法加密法，消息收、发双方均使用对称密码算法（如SM4）进行消息加解密。消息发送方生成一个“会话密钥”对消息进行加密，得到消息密文，再使用事先分配的“群组密钥”加密会话密钥，将消息密文和会话密钥密文一同发给接收方；接收方使用事先分配的群组密钥解密会话密钥，再用会话密钥解密消息密文。进一步原理如下：

IMS在群组创建时，由密钥管理中心为每个群组（两个用户通信为最小群组）产生一个群组密钥，并秘密分配给群组所有成员，用于保护会话密钥；每个群组的群组密钥不同。秘密发送群组密钥方法参见附录D。

用户在即时通信时，消息发送方IMS客户端随机生成会话密钥，调用密码组件/模块对消息明文加密，再用群组密钥加密会话密钥，IMS客户端将消息密文以及会话密钥密文一起发送给IMS服务端，由IMS服务端转发到群组每个MST上，MST用群组密钥解密会话密钥，再用会话密钥解密消息密文。

加密的即时通信消息在传输经过的线路（包括无线、有线）及设备中（在没有获得解密密钥情况下）无法还原成明文，保证了通信内容不被窃听、篡改和伪造。

移动即时通信加密原理如图16所示。附录D给出基于商用密码的安全即时通讯系统实例。

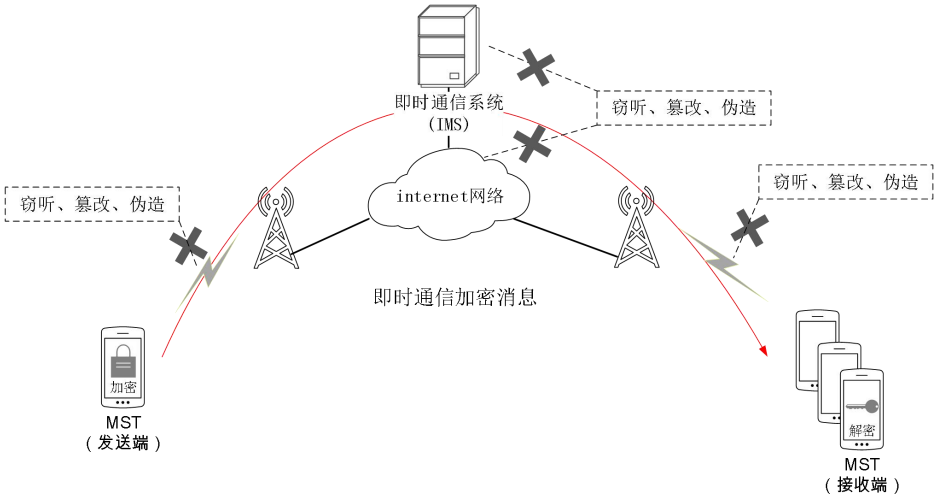


图 16 MST 即时通信加密原理

7.5.3 密码模块部署

移动即时通信加密宜使用密码模块包括：MST密码组件（MST-CC）、服务端密码组件（SS-CC）和密码机。密码模块部署如图17所示。

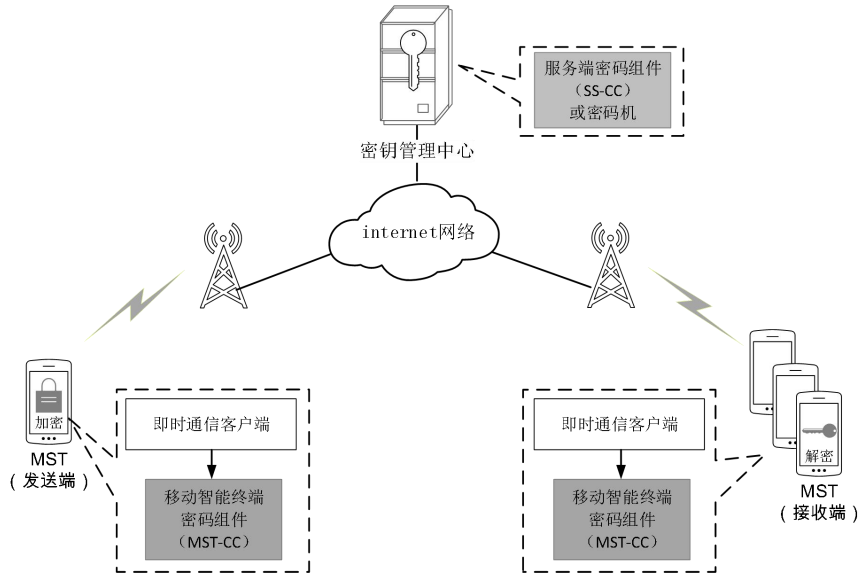


图 17 MST 即时通信加密密码模块部署

a) MST-CC 部署在 MST 上，由即时通信客户端通过调用密码组件/模块应用程序接口（API），实现即时消息加解密、密钥参数管理和保护。

b) SS-CC（或密码机）部署在企业（或第三方）密钥管理中心，用于 MST-CC 初始化、密钥参数传递、管理和保护；IMS 创建群组时，SS-CC 为群组生成“群组密钥”，用户进行即时通信时，SS-CC 不参与消息加解密过程。

c) 可采用 T/EMCG 001-2019 技术架构设计、实现 MST-CC 和 SS-CC，并经国家商用密码检

测机构检测认证。

d) 可采用符合 GM/T 0030 的密码机，并经国家商用密码检测机构检测认证。

e) 可采用符合 GM/T 0034 的密钥管理中心，并经国家商用密码检测机构检测认证。

7.5.4 密钥管理

移动即时通信加密使用国家密码主管部门批准的对称密码算法（如SM4、ZUC）、摘要算法(如SM3)和非对称密码算法（如SM2），涉及管理的密钥：

——即时通信系统服务端加密公私钥对：公钥（P_S）和私钥（d_S）。非对称密钥，由密码机产生，P_S预置在 MST-CC 中，d_S存储在 SS-CC（或密码机）中，用于 MST 与 IMS 服务端进行安全参数传递。

——MST（用户）公私钥对：公钥（P_M）和私钥（d_M）。非对称密钥，MST-CC 初始化时由密钥管理中心产生，并安全分发到 MST-CC，用于 MST 与 IMS 服务端进行群组密钥的安全传递； d_M安全保存在 MST-CC 中，并加密备份保存在密钥管理中心中。

——MST 用户主密钥（MK）。对称密钥，MST-CC 初始化时产生，由 MST 用户掌握，不在 MST-CC 和信息系统中存储，用于对 MST-CC 敏感信息加密存储保护。MK 生成和使用遵循 T/EMCG 001-2019。

——会话密钥。对称密钥，用于对即时通信内容进行加密的密钥，由 MST-CC 在加密即时消息时随机产生，用群组密钥加密保护，随加密消息发送给所有群组成员。

——群组密钥。对称密钥，由密码管理中心在 IMS 创建群组时产生并分配给每个群组成员 MST 保存，用于会话密钥加密保护；不同群组的群组密钥不同，以实现各群组会话密钥独立加密保护。

MST 即时通信加密密钥管理宜遵循 GM/T 0054 密钥管理要求，见附录 B。

7.6 文件加密

7.6.1 应用场景

政企单位使用MST开展业务时，MST可存有政企单位数据文件，采用密码技术对MST数据文件进行加密保护，以防止数据文件被非法读取，特别是保证在MST失控时数据文件不被泄露。

对于MST文件加密重要性宜了解国家、行业标准：

- GB/T 22239对三级以上系统计算环境数据保密性提出了要求，见附录A。
- GM/T 0054对应用和数据安全提出了密码应用技术要求，见附录B。

政企单位使用MST实施电子文件流转宜遵照GB/T 38541进行密码保护。

7.6.2 密码保护原理

MST文件加密使用对称密码算法和非对称密码算法对政企移动应用（App）的数据文件进行加密存储。由于只有政企App用户拥有加密密钥，政企用户可以安全读取MST文件，而没有加密密钥的App或非授权者不能获得文件明文，即使MST丢失，没有文件加密密钥也不能获得加密文件的明文。MST文件加密原理如图18表示。

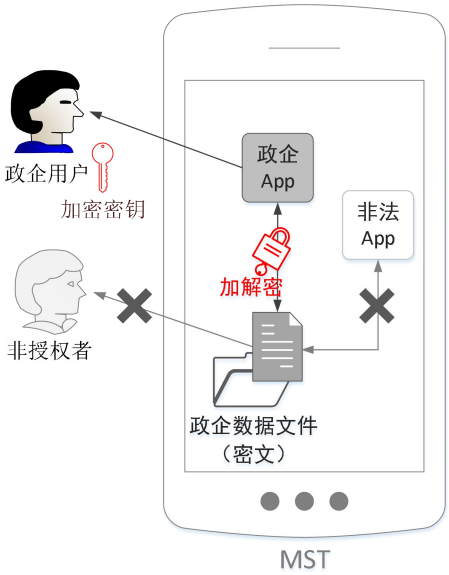


图18 MST文件加密原理

7.6.3 密码模块部署

宜在MST上部署软/硬件密码模块，政企App通过调用MST-CC应用程序接口（API），实现文件数据加解密以及“文件加密密钥”保护。

密码模块可采用T/EMCG 001-2019技术架构设计、实现，并经国家商用密码检测机构检测认证。

MST文件加密密码模块如图19表示。

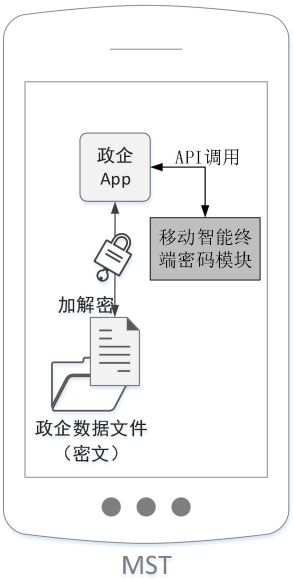


图19 MST文件加密密码模块

7.6.4 密钥管理

MST文件加密使用国家密码主管部门批准的对称密码算法（如SM4）和非对称密码算法（如SM2），涉及管理的密钥：

——MST 用户加密公私钥对：公钥（P_M）和私钥（d_M）。非对称密钥，MST 密码模块初始化时由密钥管理中心产生和备份，用于保护“文件加密密钥”,保存在 MST 密码模块中。

——MST 用户主密钥（MK）。对称密钥，MST 密码模块初始化时产生，由 MST 用户掌握，不在 MST-CC 存储，用于用户私钥 d_M加密存储。MK 生成和使用遵循 T/EMCG 001-2019。

——文件加密密钥。对称密钥，用于政企 App 文件数据加解密，每次调用密码模块对 App 文件数据进行加密时随机产生，实施加密后，用 P_M加密形成“文件标签”保存在 MST 文件系统中，当文件数据解密时使用 d_M对文件标签中的文件加密密钥密文进行解密。文件标签机制宜遵照 GM/T 0055 建立。

MST文件加密密钥管理宜遵循GM/T 0054，见附录B。

注：根据MST文件实际情况（如文件大小、读取频次）可采用文件整体加解密、文件分块加解密策略。采用文件整体加解密时，一个文件对应一个文件加密密钥，并且每次加密操作应重新生成文件加密密钥；采用文件分块加解密时，一个文件块对应一个文件加密密钥，并且每次加密操作应重新生成文件加密密钥，这时一个文件可能对应多个文件加密密钥，可采用非固定长度文件标签对文件加密密钥进行加密存储和管理。

附录 A
（资料性附录）
网络安全等级保护基本要求有关条款与本文件章节对照

GB/T 22239-2019网络安全等级保护基本要求规定了网络安全等级保护第一级到第四级保护对象的安全通用要求和安全扩展要求，用于指导分等级的非涉密对象的安全建设和监督管理，是本文件遵循的标准之一。表A.1给出GB/T 22239-2019有关条款与本文件有关章节对照。

表A.1 GB/T 22239-2019 网络安全等级保护基本要求有关条款与本文件有关章节对照

GB/T 22239-2019 密码技术要求条款		本文件相关章节
6.第一级安全要求	**6.1 安全通用要求**	
	6.1.4.5.可信验证 可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。	6.1 可信启动
	6.3 移动互联安全扩展要求	
	6.3.4.1.移动应用软件采购 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。	6.2 App 签名与验证
7.第二级安全要求	**7.1 通用要求**	
	7.1.4.6 可信验证 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	6.1 可信启动
	7.1.9.3.产品采购和使用 b) 应确保密码产品与服务的采购和使用符合国家密码管理主要部门的要求。	6.1-6.4、7.1-7.6 密码模块部署
	7.1.10.9 密码管理 a) 应遵循密码相关国家标准和行业标准； b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	6.1-6.4、7.1-7.6 密码模块部署 密钥管理
	7.3 移动互联安全扩展要求	
	7.3.3.1.移动应用管控 b) 应只允许可靠证书签名的应用软件安装和运行。	6.2 App 签名与验证
	7.3.4.2.移动应用软件开发 b) 应保证开发移动业务应用软件的签名证书合法性。	6.2 App 签名与验证
8.第三级安全要求	**8.1 安全通用要求**	
	8.1.2.2.通信传输 a) 应采用校验技术或密码技术保证通信过程中数据的完整性； b) 应采用密码技术保证通信过程中数据的保密性。	6.4 网络传输加密
	8.1.4.1.身份鉴别 d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少使用密码技术来实现。	7.3 用户证书登录

	8.1.4.6.可信验证 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	6.1 可信启动
	8.1.4.7.数据完整性 a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	6.4 网络传输加密 7.1 语音电话加密 7.4 电子签章 7.5 即时通讯加密 7.6 文件加密
	8.1.4.8.数据保密性 a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	6.4 网络传输加密 7.1 语音电话加密 7.2 电子邮件加密 7.5 即时通讯加密 7.6 文件加密
	8.1.9.2.安全方案设计 b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包括密码技术相关内容，并形成配套文件；	整个标准
	8.1.9.3.产品采购和使用 b) 应确保密码产品与服务的采购和使用符合国家密码管理主要部门的要求；	6.1-6.4、7.1-7.6 密码模块部署
	8.1.9.7.测试验收 b) 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。	整个标准
	8.1.10.9 密码管理 a) 应遵循密码相关国家标准和行业标准； b) 应使用国家密码管理主管部门认证核准的密码技术和产品。	6.1-6.4、7.1-7.6 密码模块部署 密钥管理
	8.3 移动互联安全扩展要求	
	8.3.2.2.访问控制 无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。	6.3 无线局域网接入
	8.3.3.2.移动应用管控 b) 应只允许指定证书签名的应用软件安装和运行；	6.2 App 签名与验证
	8.3.4.2.移动应用软件开发 b) 应保证开发移动业务应用软件的签名证书合法性。	6.2 App 签名与验证
9.第四级安全要求	**9.1 安全通用要求**	
	9.1.2.2.通信传输 c) 应在通信前基于密码技术对通信的双方进行验证或认证； d) 应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。	6.4 网络传输加密

	9.1.3.6.可信验证 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。	6.1 可信启动
	9.1.4.1.身份鉴别 d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少使用密码技术来实现。	7.3 用户证书登录
	9.1.3.6.可信验证 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。	6.1 可信启动
	9.1.4.7.数据完整性 a) 应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； b) 应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； c) 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。	6.4 网络传输加密 7.1 语音电话加密 7.4 电子签章 7.5 即时通讯加密 7.6 文件加密
	9.1.4.8.数据保密性 a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	6.4 网络传输加密 7.1 语音电话加密 7.2 电子邮件加密 7.5 即时通讯加密 7.6 文件加密
	9.1.10.9 密码管理 a) 应遵循密码相关的国家标准和行业标准； b) 应使用国家密码主管部门认证核准的密码技术和产品； c) 应采用硬件密码模块实现密码运算和密钥管理。	6.1-6.4、7.1-7.6 密码模块部署 密钥管理
	9.3 移动互联安全扩展要求	
	9.3.2.2.访问控制 无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。	6.3 无线局域网接入
	9.3.3.2.移动应用管控 b) 应只允许指定证书签名的应用软件安装和运行；	6.2 App 签名与验证
	9.3.4.2.移动应用软件开发 b) 应保证开发移动业务应用软件的签名证书合法性。	6.2 App 签名与验证

附录 B
（资料性附录）
信息系统密码应用基本要求条款与本文件章节对照

GM/T 0054-2018信息系统密码应用基本要求规定了信息系统商用密码应用的基本要求，适用于指导、规范和评估信息系统中的商用密码应用，是本文件遵循的标准之一。表B.1给出GM/T 0054-2018有关条款与本文件有关章节的对照。

表B.1 GM/T 0054-2018信息系统密码应用基本要求有关条款与本文件有关章节的对照

GM/T 0054-2018 相关章节条款			本文件相关章节
7 密码技术应用要求	**7.2 网络和通信安全**	7.2.1 总则	
		a) 采用密码技术对连接到内部网络的设备进行安全认证；	6.3 无线局域网接入
		b) 采用密码技术对通信的双方身份进行认证； c) 采用密码技术保证通信过程中数据的完整性； d) 采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性；	6.4 网络传输加密
		e) 采用密码技术保证网络边界访问控制信息、系统资源访问控制信息的完整性；	6.3 无线局域网接入
	7.3 设备和计算安全	7.3.1 总则	
		a) 采用密码技术对登录的用户进行身份鉴别；	7.3 用户证书登录
		d) 采用密码技术的完整性功能对重要程序或文件进行完整性保护；	6.1 可信启动 6.2 App 签名与验证
	7.4 应用和数据安全	7.4.1 总则	
		a) 采用密码技术对登录的用户进行身份鉴别；	7.3 用户证书登录
		d) 采用密码技术保证重要数据在传输过程中的机密性、完整性；	7.5 即时通讯加密 7.1 语音电话加密 7.2 电子邮件加密
		e) 采用密码技术保证重要数据在存储过程中的机密性、完整性；	7.6 文件加密
		f) 采用密码技术对重要程序的加载和卸载进行安全控制；	6.2 App 签名与验证
		g) 采用密码技术实现实体行为的不可否认性；	7.4 电子签章
8 密钥管理	8.1 总则 信息系统密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程。		6.1-6.4、7.1-7.6 密钥管理
9 安全管理	9.1 制度 9.2 人员 9.3 实施 9.4 应急		6.1-6.4、7.1-7.6 密钥管理

附录 C
（资料性附录）
基于多方协同方式的移动智能终端电子签章实例

C.1 概述

基于多方协同方式的移动智能终端（MST）电子签章（以下简称电子签章），是7.4章节电子签章技术的一种实现方案。采用多方协同计算、数字签名等密码技术保证移动场景下MST访问政企业务系统的相关业务时对电子签章的安全性需求。

C.2 密码保护原理

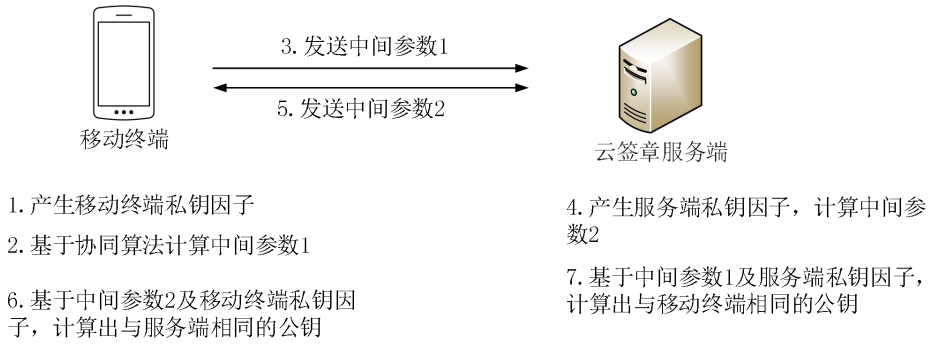
电子签章系统密码保护机制主要包括密钥产生、电子签章和验证。

密钥产生：

MST与云签章服务器采用多方协同方式生成密钥。首先MST与云签章服务器各自生成自己的密钥分量,亦称“密钥因子”，并通过交互协商出公钥。在协商过程中，交互协议保证双方在任何时候都不能获得完整的私钥。通常，签章者可到第三方证书认证机构，使用此公钥申请数字证书。

密钥因子产生后在各方的密码模块或设备中安全存储。密钥因子生成及协同计算过程可遵循T/EMCG 001.4-2019。

电子签章系统密钥产生原理如图C.1所示。



图C.1 电子签章系统密钥产生原理

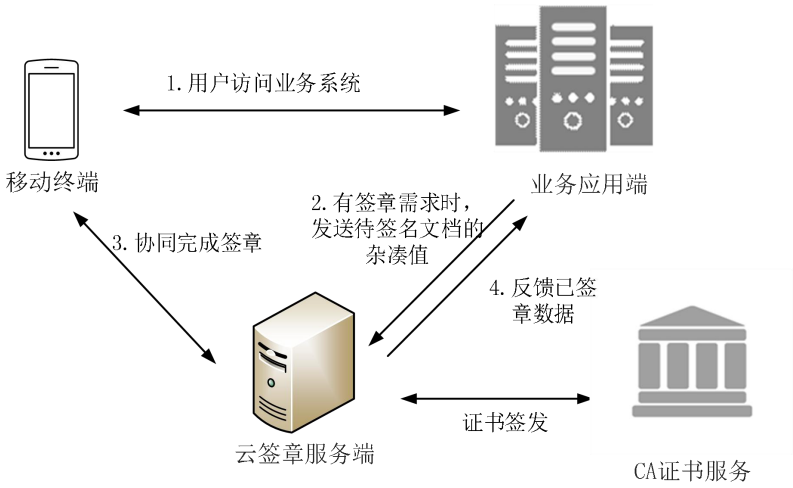
数字签名和验证：

政企业务系统为用户提供业务办理、业务查询等服务。当有签章需求时，业务系统将待签章文档杂凑数据发送到云签章服务端，云签章服务端基于多方计算的密钥管理技术，即移动终端、云签章服务端协同进行数字签名，完成文件的电子签章。只有持有对应密钥因子的签章者，针对特定的业务文件数据，正确使用数子签名才能完成签章操作。

电子印章是电子签章技术的重要数据，其格式、生成及验证可遵循GB/T 38540要求。

MST盖章者使用电子印章生成电子签章时，电子签章数据格式、生成及验证流程可遵循GB/T 38540要求。

电子签章系统密码应用过程原理如图C.2所示。



图C.2 电子签章系统密码应用原理框图

在验证电子签章的过程中，通过验证盖章者数字证书、数字签名等信息来确保电子签章是经授权的盖章者所为，符合电子签名技术要求，能够保障签章数据的真实性、完整性及签章行为的不可否认性。

C.3 密码模块部署

a) 在MST部署硬/软件密码模块，实现密钥因子的生成、加密存储、协同签名、电子签章等功能。
b) 在云签章服务端部署基于协同签名技术的签章系统和加密机/加密卡，实现密钥因子的生成、存储、协同签名、电子签章等功能。
c) 云签章服务端后台可通过连接第三方证书认证中心为系统和用户提供数字证书服务。
d) 业务系统可通过云签章网关与云签章服务端进行信息交互。
e) 密码模块可采用T/EMCG 001-2019技术架构实现，宜符合GM/T 0028二级及以上密码模块的要求，并经国家商用密码检测机构检测认证。

电子签章密码组件/模块部署如图C.3所示。

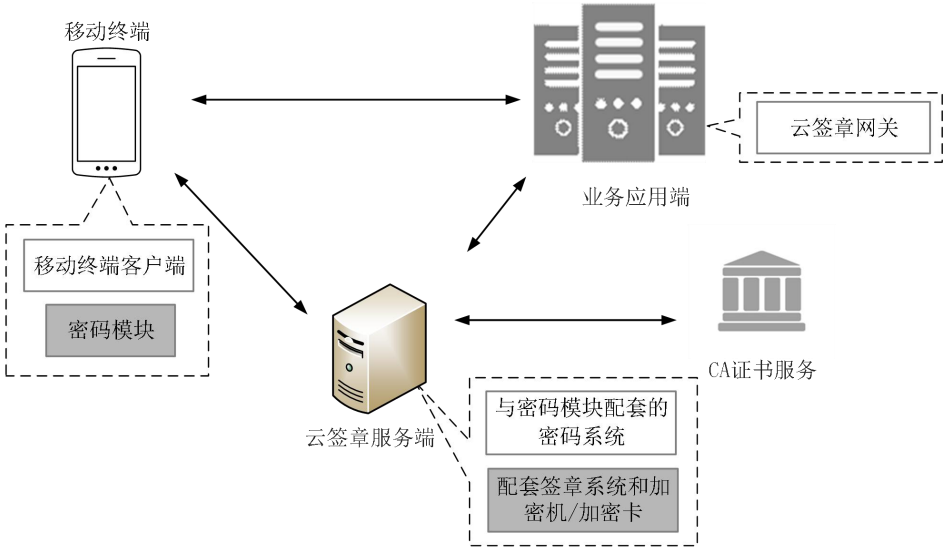


图 C.3 电子签章密码组件/模块部署

C.4 密钥管理

密钥因子分别存储在云签章服务端和MST，签章时通过协同计算得出最终签名结果。涉及的密钥产生及管理：

——MST 密钥因子由 MST 密码组件/模块产生并存储在 MST。

——云签章服务端密钥因子由云签章端的密码组件或加密机等设备生成，并进行加密存储。

附录 D
（资料性附录）
基于商用密码的安全即时通讯系统实例

D.1 概述

政企客户日常工作涉及大量非密敏感信息的及时交付，这些信息如果选择无合规密码保护措施的即时通讯应用进行传递，会给业务开展带来重大的安全隐患。因此，政企客户有必要采用安全的即时通讯服务实现即时消息安全传递，安全即时通讯服务的设计需要符合国家网络安全和密码管理的相关法律、标准和规范的要求。

安全即时通讯服务应支持主流即时通讯工具的基本功能，还应从身份认证、传输加密、存储加密、密钥管理等方面进行密码应用设计，依托国产商用密码技术和密码产品构建合规的密码保护体系，保证即时通讯数据的真实性、机密性和完整性。

安全即时通讯服务需支持加密即时消息收发、转发，包括点对点消息及群组消息。支持富媒体消息收发，包括文本、图片、语音、视频、表情、文件、投票、位置信息等的全程加密收发；消息在客户端和服务器端均加密存储。

基于商用密码的安全即时通讯系统是7.5节签章技术的一种实现方法。

D.2 密码保护原理

为保护即时消息的机密性，避免后加入群组的用户能解开群组中之前的消息密文和已退出群组的用户可以解开退出后新生产的消息密文，应采用一次一密的机制对消息内容进行加密保护，同时每次群组变化需要更新群组密钥，从而实现前向和后向安全。

安全即时通讯客户端在注册时需要完成MST密码组件/模块的初始化，由MST密码组件/模块产生用户公私钥对，并从服务端密码组件/模块获取加密公私钥对以及用户公钥证书和加密公私钥证书。加密公私钥对由密钥管理中心产生和管理，每个用户的加密公私钥对不同，并用MST签名公钥（MST-CC.PUK）加密保护后下发到客户端密码组件/模块，用于客户端与服务端建立安全传输通道。MST签名私钥（MST-CC.PRK）安全保存在MST密码组件/模块中。

在服务端密码组件/模块和客户端密码组件/模块准备好签名公私钥对和加密公私钥对后，密钥管理中心为用户分配密钥保护密钥（KDK），每个用户的KDK不同，KDK用于保护群组密钥及其他敏感参数。KDK用客户端签名公钥（MST-CC.PUK）加密保护后下发到客户端密码组件/模块，用于客户端解密群组密钥（GK）。

密钥管理中心在群组（点对点通信被当成只有两个用户的群组）创建时，为每个群组产生一个群组密钥（GK），每个群组的群组密钥不同，群组密钥用于保护加密即时消息的会话密钥（SK），每条消息的会话密钥不同。

即时消息加密过程中，GK用于加密临时产生的会话密钥SK，SK用于对消息、文件或流媒体等业务数据进行加密保护。

基于商用密码的安全即时通讯系统密码保护原理如图D.1所示。

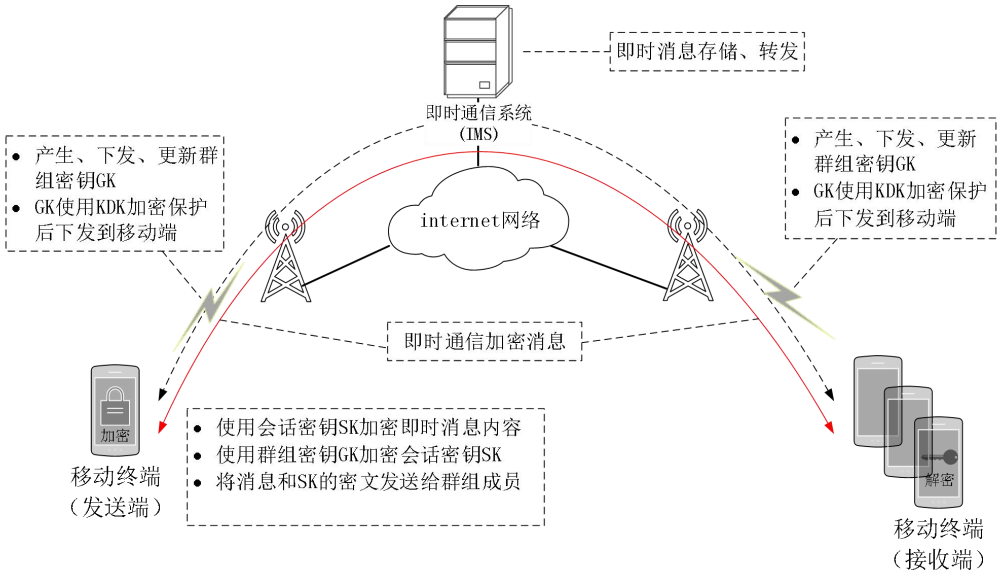


图 D.1 基于商用密码的安全即时通讯系统密码保护原理

D.3 密码模块部署

移动即时通信加密保护使用的密码模块包括：MST密码组件（MST-CC）和服务端密码组件（SS-CC）和服务器密码机等组件，在实现中可以参考图D.2所示的部署架构。

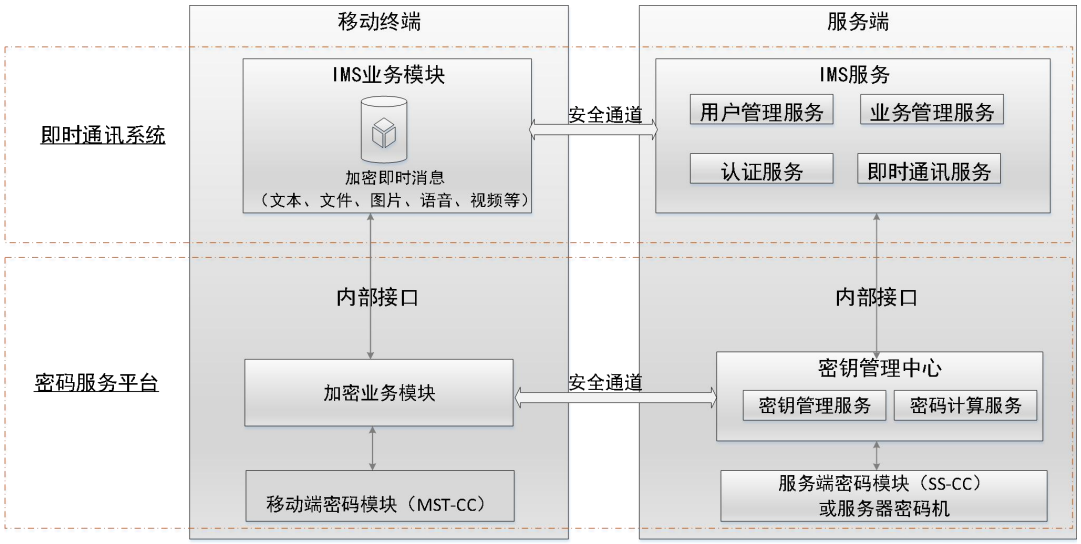


图 D.2 MST 即时通信加密密码组件/模块部署

安全即时通讯客户端在注册时需要完成MST密码组件/模块的初始化，主要内容包括：从MST密码组件MST-CC产生签名公私钥对，从服务端密码组件SS-CC获取加密公私钥对，从密钥管理中心获取签名公钥证书和加密公私钥证书。加密公私钥证书由密钥管理中心产生和管理，并用签名公钥加密保护后下发到客户端密码组件/模块，用于客户端与服务端建立安全传输通道。MST签名私钥安全保存在MST密码组件/模块中。

D.4 密钥管理

密钥管理是指对密钥进行全生命周期的管理，包括：密钥的产生、分发、存储、备份、更新、恢复、销毁等。在实现中需要考虑算法配用、密钥保护和密钥管理流程。

——密码配用

- 对称加密算法采用SM4算法，采用CBC工作模式，主要实现数据的加密和解密功能，提供数据的机密性保护。
- 非对称算法采用SM2算法，主要用于数字签名、验签、加密、解密以及密钥协商。
- 杂凑算法采用SM3算法，用于进行摘要计算。

——密钥保护

密钥安全是保障信息安全的关键，因此对密钥进行分层保护，分层保护原理如图D.3所示。

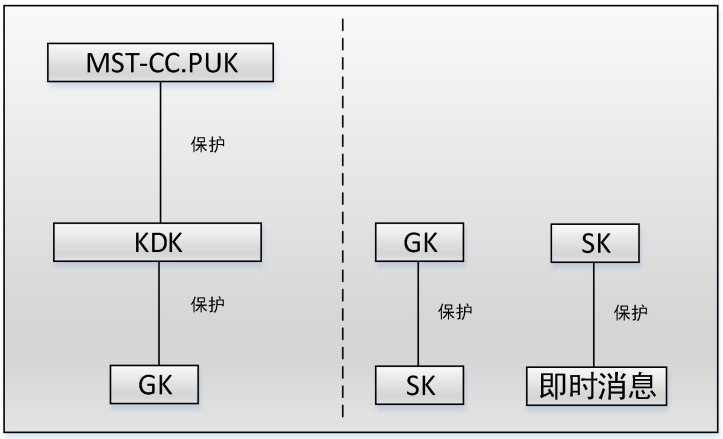


图 D.3 密钥分层保护原理

——密钥管理

1) 在服务端密码组件/模块和客户端密码组件/模块准备好签名公私钥对和加密公私钥对后，密钥管理中心为用户分配密钥保护密钥（KDK），每个用户的KDK不同，KDK用于保护群组密钥及其他敏感参数。KDK用客户端签名公钥（MST-CC.PUK）加密保护后下发到客户端密码组件/模块，用于客户端解密群组密钥（GK）。
2) 密钥管理中心在群组（点对点通信被当成只有两个用户的群组）创建时，为每个群组产生一个群组密钥（GK），每个群组的群组密钥不同，群组密钥用于保护加密即时消息的会话密钥（SK），每条消息的会话密钥不同。
3) 即时消息加密过程中，GK用于加密临时产生的会话密钥SK，SK用于对消息、文件或流媒体等业务数据进行加密保护。

参考文献

[1] GB/T 17901.1 信息技术 安全技术 密钥管理 第1部分：框架

[2] GB/T 25069 信息安全技术 术语

[3] GM/Z 4001 密码术语

[4] T/EMCG 001.4-2019 移动智能终端密码模块技术框架 第4部分：密钥多端协同计算保护技术架构

[5] ISO/IEC 9798-3:2019 IT Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques 信息技术 安全技术 实体鉴别 第3部分:用数字签名技术的机制