

ICS 01.040.33  
M 04



# 中华人民共和国通信行业标准

YD/T 2258-2011

---

## 移动通信网安全术语集

Terminology of mobile communication network security

2011-06-01 发布

2011-06-01 实施

---

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 安全词汇中英对照.....1

附录 A（资料性附录） 安全词汇缩略语.....7

## 前 言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：诺基亚通信有限公司、上海贝尔股份有限公司、杭州摩托罗拉移动通信设备有限公司、诺基亚西门子通信（上海）有限公司、中国联合网络通信集团有限公司、南京爱立信熊猫通信有限公司、中国普天信息产业股份有限公司。

本标准主要起草人：张大江、胡志远、左崴东、李 钢、陆 伟、韩 冬、杜志敏、张 尼、李云喜、朱 锋。

# 移动通信网安全术语集

## 1 范围

本标准规定了数字蜂窝移动通信网中安全术语的中英文对照及缩略语\*和术语的对照。  
本标准适用于数字蜂窝移动通信网。

## 2 安全词汇中英对照\*

### 2.1 A

Advanced encryption standard	高级加密标准
Anonymity key	匿名密钥
Authentication	认证（鉴权）**
Authentication algorithm version	认证算法版本
Authentication and key agreement	认证和密钥协商
Authentication authorization accounting	认证、授权和计费
Authentication center	认证中心
Authentication header	认证头协议
Authentication key	认证密钥
Authentication management field	认证管理字段
Authentication proxy	认证代理
Authentication response	认证响应
Authentication token	认证令牌
Authentication unique challenge response	唯一认证挑战响应
Authentication vector	认证向量
Authorization	授权

### 2.2 B

Backdoor	后门
Backward security	后向安全
Bandwidth consumption attack	带宽消耗攻击
Base cryptographic functions	基本加密函数
Biometric identification	生物识别
Blacklist	黑名单
Blended attack	混合攻击

\*附录 A 列出了部分词汇的缩略语，供参考。

\*\* 括号内的内容为目前并存的其它翻译方式，本标准不建议使用。

Blended threat	混合威胁
Blind spoofing attack	盲欺骗攻击
Block cipher	分组密码算法
Bootstrapping server function	自举服务器功能
Browser hijacker	浏览器劫持
Brute force attack	暴力攻击
Bucket brigade attack	偷梁换柱攻击（中间人攻击）
Bulk encryption	批量加密

2.3 C

Cellular authentication and voice encryption	蜂窝认证和语音加密算法
Cellular message encryption algorithm	蜂窝消息加密算法
Certification authority	证书授权中心
Certificate revocation list	撤销证书列表
Challenge-handshake authentication protocol	询问握手认证协议
Cipher	密码算法；加密
Cipher key	加密密钥
Cipher key sequence number	加密密钥序列号
Confidentiality	机密性
Connectivity credentials issuing function	连接信任凭证签发功能
Credential	信任凭证
Cryptography	密码编码学

2.4 D

Data confidentiality	数据机密性
Data encryption standard	数据加密标准
Data integrity	数据完整性
Datagram transport layer security	数据报传输层安全
Data origin authentication	数据源认证
Decipher	解密
Decryption	解密
Diffie-Hellman key exchange	DH密钥交换
Digital signature	数字签名

2.5 E

Eavesdropping	窃听
Electronic code book	电子代码本
Electronic signature	电子签名
Encapsulating security payload	封装安全载荷协议
Encrypted key exchange	加密密钥交换协议

Encryption	加密
Encryption algorithm	加密算法
End-to-end encryption	端到端加密
Enhanced cellular message encryption algorithm	增强的蜂窝消息加密算法
Entity authentication	实体认证
Escrowed encryption standard	托管加密标准
Escrow Passwords	托管口令
Extensible authentication protocol	可扩展认证协议
2.6 F	
Finger image	指纹影像
Fingerprinting	指纹
Fingerprint scanning	指纹扫描
Firewall	防火墙
Fishing	钓鱼攻击
Flooding	泛洪攻击
Forward security	前向安全
2.7 G	
GBA user security setting	GBA用户安全设置
GBA with UICC-based enhancements	基于UICC的增强型GBA
Generic authentication architecture	通用认证架构
Generic bootstrapping architecture	通用自举架构
GPRS encryption algorithm	GPRS加密算法
GPRS-IMS-bundled authentication	GPRS-IMS捆绑认证
2.8 H	
Hijacking	劫持
Home AAA	归属域AAA
HTTP over TLS	安全HTTP 协议
Hybrid attack	混合攻击
Hybrid encryption	混合加密
Hybrid virus	混合病毒
2.9 I	
Integrity key	完整性保护密钥
Internet key exchange	互联网密钥交换协议
Interception	监听
IP security	IP安全协议
IPsec security association	IPsec安全关联（IPsec安全联盟）
Internet security association key management protocol	互联网安全关联密钥管理协议

ISAKMP security association	ISAKMP安全关联
2.10 J	
2.11 K	
Key	密钥
Key agreement	密钥协商
Key confirmation	密钥确认
Key control	密钥控制
Key derivation function	密钥衍生函数
Key distribution centre	密钥分发中心
Key escrow	密钥托管
Key exchange	密钥交换
Key management center	密钥管理中心
Key refresh	密钥更新
Key set identifier	密钥集标识符
Keyed-hash message authentication code	基于密钥的哈希消息认证码
2.12 L	
Lawful interception	合法监听
Local AAA	本地AAA
Location dependent interception	位置相关监听
2.13 M	
Master secret	主密钥
Master session key	主会话密钥
ME-based GBA	基于ME的GBA
Message authentication code	消息认证码
Message digest version 5	消息摘要版本5算法
2.14 N	
NDS/IP	基于IP协议的网络域安全
Network domain security	网络域安全
Network security	网络安全
Non-repudiation	抗抵赖
2.15 O	
One-way hash function	单向散列函数
Online authentication certificate	在线认证证书
Online crypto-operation	在线密码运算
Online certificate status protocol	在线证书状态协议
2.16 P	
Packet filter firewall	包过滤防火墙



Pairwise key	成对的密钥
Passive threat	被动威胁
Password	口令
Peer-entity authentication	对等实体认证
Person identification number	个人识别号
Physical security	物理安全
Plain text	明文
Pre-master key	预主密钥
Pre-shared key	预共享密钥
Pre-signature	预签名
Principle of least privilege	最小特权原则
Privacy	私密性
Private Key	私钥
Private signature key	私有签名密钥
Public key	公钥
Public key certificate	公钥证书
Public-key cryptography standards	公钥密码标准
Public key infrastructure	公钥基础设施
Pseudo-random function	伪随机数产生函数
2.17 Q	
Quintet	五元组
2.18 R	
Random number	随机数
Redundancy	冗余
Reflection attack	反射攻击
Reflection protection	反射保护
Replay attack	重放攻击
Repudiation	抵赖
Role based access control	基于角色的访问控制
2.19 S	
Secret sharing	秘密分享
Security association	安全关联
Security association database	安全关联数据库
Security capabilities	安全能力
Security context	安全上下文
Security domain	安全域
Security gateway	安全网关



Secure hash algorithm	安全哈希算法
Security mode command	安全模式命令
Security parameters index	安全参数索引
Security policy database	安全策略数据库
Secure socket layer	安全套接字
Sequence number	序列号
Shared secret data	共享秘密数据
Signed response	签名响应
Spoofing	欺骗
2.20 T	
Transport layer security	传输层安全协议
Trust chain	信任链
Trusted computing group	可信计算工作组
Trusted platform module	可信平台模块
Trusted environment	可信环境
Triplet	三元组
2.21 U	
User authentication	用户认证
User security setting	用户安全设置
2.22 V	
Validation	确认
Verification	验证
Vulnerability	脆弱性
2.23 W	
Watermark	水印
Weak encryption	弱加密
Weak key	弱密钥
Weak password	弱口令
Wired equivalent privacy	有线等效加密协议
WLAN access point attack	WLAN 接入点攻击
Wireless transport layer security	无线传输层安全协议
2.24 X	
XML key management specification	XML密钥管理规范
XML digital signatures	XML数字签名
XML encryption	XML加密

附 录 A  
(资料性附录)  
安全词汇缩略语

## A.1 A

A-Key	Authentication Key
AAA	Authentication Authorization Accounting
AC	Authentication Center
AES	Advanced Encryption Standard
AH	Authentication Header
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AP	Authentication Proxy
AUTHR	Authentication Response
AUTHU	Authentication Unique Challenge Response
AUTN	Authentication Token
AV	Authentication Vector

## A.2 B

BSF	Bootstrapping Server Function
-----	-------------------------------

## A.3 C

CA	Certification Authority
CAVE	Cellular Authentication and Voice Encryption
CCIF	Connectivity Credentials Issuing Function
CK	Cipher Key
CKSN	Cipher Key Sequence Number
CMEA	Cellular Message Encryption Algorithm
CRL	Certificate Revocation List

## A.4 D

DES	Data Encryption Standard
DH	Diffie-Hellman
DTLS	Datagram Transport Layer Security

## A.5 E

EAP	Extensible Authentication Protocol
ECMEA	Enhanced Cellular Message Encryption Algorithm

EKE	Encrypted Key Exchange
ESP	Encapsulating Security Payload

#### A.6 G

GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GBA_ME	ME-based GBA
GBA_U	GBA with UICC-based enhancements
GEA	GPRS Encryption Algorithm
GIBA	GPRS-IMS-Bundled Authentication
GUSS	GBA User Security Setting

#### A.7 H

H-AAA	Home AAA
HMAC	Keyed-Hash Message Authentication Code

#### A.8 I

IK	Integrity Key
IKE	Internet Key Exchange
IPsec	IP security
IPsec SA	IPsec Security Association
ISAKMP	Internet Security Association Key Management Protocol
ISAKMP SA	ISAKMP Security Association

#### A.9 K

KDC	Key Distribution Centre
KDF	Key Derivation Function
KMC	Key Management Center
KSI	Key Set Identifier

#### A.10 L

L-AAA	Local AAA
LDI	Location Dependent Interception
LI	Lawful Interception

#### A.11 M

MAC	Message Authentication Code
MD5	Message Digest Version 5
MSK	Master Session Key

A.12 N

NDS Network Domain Security

A.13 O

OCSP Online Certificate Status Protocol

A.14 P

PIN Person Identification Number  
PKCS Public-Key Cryptography Standards  
PKI Public Key Infrastructure  
PRF Pseudo-Random Function

A.15 R

RAND Random Challenge  
RBAC Role Based Access Control

A.16 S

SA Security Association  
SAD Security Association Database  
SEG/SEGW Security Gateway  
SHA Secure Hash Algorithm  
SMC Security Mode Command  
SPD Security Policy Database  
SPI Security Parameters Index  
SQN Sequence Number  
SRES Signed Response  
SSL Secure Socket Layer  
SSD Shared Secret Data

A.17 T

TCG Trusted Computing Group  
TLS Transport Layer Security  
TPM Trusted Platform Module  
TRE Trusted Environment

A.18 U

USS User Security Setting

A.19 W



中华人民共和国  
通信行业标准  
移动通信网安全术语集  
YD/T 2258-2011

\*

人民邮电出版社出版发行  
北京市崇文区夕照寺街14号A座  
邮政编码：100061  
宝隆元（北京）印刷技术有限公司印刷  
版权所有 不得翻印

\*

开本：880×1230 1/16                      2011年9月第1版  
印张：1                                      2011年9月北京第1次印刷  
字数：25千字

ISBN 978 - 7 - 115 - 2388/ 11 - 339  
定价：10元

本书如有印装质量问题，请与本社联系 电话：(010)67114922