ICS 35.240.99
A90

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

移动警务 数字证书格式要求

Mobile police service -

Profile requirements for digital certificates

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　　发布

目　　次

前　　言 II
1 范围 1
2 规范性引用文件 1
3 缩略语 1
4 证书类型 1
5 证书格式 1
5.1 字符编码要求 1
5.2 人员证书格式 2
5.3 机构证书格式 3
5.4 设备证书格式 5
5.5 应用证书格式 7
6 编码 8
6.1 证书类型编码规则 8
6.2 证书分类代码 9
6.3 人员证书编码 10
6.4 机构证书编码 10
6.5 设备证书编码 10
6.6 应用证书编码 10

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由公安部科技信息化局提出。

本标准由公安部计算机与信息处理标准化技术委员会归口。

本标准起草单位：吉林省公安厅、公安部科技信息化局、公安部第三研究所、长春吉大正元信息技术股份有限公司、格尔软件股份有限公司、公安部第一研究所、郑州信大捷安信息技术股份有限公司、上海辰锐信息科技公司。

本标准主要起草人：温贵江、张亮亮、杨思晟、马千龙、袁艺芳、陈家明、尹心明、樊志杰、刘骥、张志会、陈骁、陈建华、艾岳、韩秀德、蔡新玮、张重磊。

移动警务 数字证书格式要求

1 范围

本标准规定了移动警务数字证书类型、证书格式和编码要求。

本标准适用于移动警务II类系统和III类系统所使用数字证书格式的设计与管理。

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/T 2659 世界各国和地区名称代码

GB 11643 公民身份号码

GB 18030 信息技术 中文编码字符集

GB 32100 法人和其他组织统一社会信用代码编码规则

GA/T 380 全国公安机关机构代码编制规则

GM/T 0015 基于SM2密码算法的数字证书格式规范

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

3 缩略语

下列缩略语适用于本文件。

C：国家名称（Country Name）

CA：证书认证机构（Certification Authority）

CN：名称（Common Name）

L：地市名称（Local City Name）

O：组织名称（Organization Name）

OU：机构名称（Organization Unit Name）

POS：销售点（Point Of Sales）

S：省份名称（State Name）

SIM：用户身份识别卡（Subscriber Identity Module）

4 证书类型

移动警务数字证书分为人员证书、机构证书、设备证书和应用证书四个类型，具体为：

a) 人员证书：用于人员认证，分为移动警务警员证书和移动警务警务辅助人员证书；

b) 机构证书：用于机构认证，分为公安机关、党/政/军部门以及其他机构证书；

c) 设备证书：用于终端设备、安全设备、服务器设备认证；

d) 应用证书：用于移动警务应用认证。

5 证书格式

5.1 字符编码要求

移动警务数字证书中所有字符编码应采用GB 18030规定的中文编码字符集。

5.2 人员证书格式

移动警务人员证书中警员/警务辅助人员证书格式如表1所示。

表1 警员/警务辅助人员证书格式表

序号	数据项名称		数据类型	采用标准	内容	说明
1	版本号		INTEGER	RFC 5280	2	
2	序列号		INTEGER	RFC 5280		正整数
3	签名算法		ObjectIdentifier	RFC 5280 GM/T 0015	SM3WithSM2Encryption	OID 为 1.2.156.10197.1.501
4	签发单位	名称(CN)	UTF-8String	GA/T 380	YD**********CA	其中“**********”采用 GA/T 380 中规定的全国公安机关机构代码
		区/县（L）	UTF-8String		00	
		市(L)	UTF-8String		00	
		省(S)	UTF-8String	GA/T 380		机构代码第 1、2 位
		国家(C)	PrintableString	GB/T 2659	CN	
5	有效期	生效日期	UTCTime/ GeneralTime	GM/T 0015	YYMMDDHHMMSSZ/YYYYMMDDHHMMSSZ	UTCTime 用于 2049 之前的年份(含 2049) GeneralTime 用于 2049 之后的年份
		失效日期	UTCTime/ GeneralTime	GM/T 0015	YYMMDDHHMMSSZ/YYYYMMDDHHMMSSZ	UTCTime 用于 2049 之前的年份(含 2049) GeneralTime 用于 2049 之后的年份
6	证书持有者信息	名称(CN)	UTF-8String			人员证书编码，见 6.3
		三级部门(OU)	UTF-8String	GA/T 380		机构代码第 11、12 位
		二级部门(OU)	UTF-8String	GA/T 380		机构代码第 9、10 位
		一级部门(O)	UTF-8String	GA/T 380		机构代码第 7、8 位
		区/县（L）	UTF-8String	GA/T 380		机构代码第 5、6 位
		市(L)	UTF-8String	GA/T 380		机构代码第 3、4 位

表 1（续）

序号	数据项名称		数据类型	采用标准	内容	说明
6	证书持有者信息	省(S)	UTF-8String	GA/T 380		机构代码第 1、2 位
		国家(C)	PrintableString	GB/T 2659	CN	
		邮件地址(E)	IA5String	RFC 5280		
7	证书持有者公钥信息		BITString	GM/T 0015		
8	扩展项	CRL 分布点		GM/T 0015		
		证书持有者密钥标识符	OCTETString	GM/T 0015		
		签发单位的密钥标识符	OCTETString	GM/T 0015		
		密钥用途		GM/T 0015		签名：数字签名、防抵赖 加密：密钥加密
		证书持有者职级	PrintableString			OID 为 1.2.86.53525105.0.2
		证书持有者工作岗位	PrintableString			OID 为 1.2.86.53525105.0.1
		证书持有者职务	PrintableString			OID 为 1.2.86.53525105.0.4
		证书持有者警种	PrintableString			OID 为 1.2.86.53525105.0.3
		证书分类代码	PrintableString			证书分类代码，见 6.2。 OID 为 1.2.86.53525105.0.5
		证书持有者组织结构代码	UTF-8String	GA/T 380		采用 GA/T 380 中规定的全国公安机关机构代码。 OID 为 1.2.86.53525105.0.6
9	签名项		BITString	GM/T 0015		

5.3 机构证书格式

机构证书格式如表2所示。

表2　机构证书格式表

序号	数据项名称		数据类型	采用标准	内容	说明
1	版本号		INTEGER	RFC 5280	2	
2	序列号		INTEGER	RFC 5280		正整数
3	签名算法		ObjectIdentifier	RFC 5280 GM/T 0015	SM3WithSM2Encryption	OID 为 1.2.156.10197.1.501
4	签发单位	名称(CN)	UTF-8String	GA/T 380	YD**********CA	其中“**********”采用 GA/T 380 中规定的全国公安机关机构代码
		区/县（L）	UTF-8String		00	
		市(L)	UTF-8String		00	
		省(S)	UTF-8String	GA/T 380		机构代码第 1、2 位
		国家(C)	PrintableString	GB/T 2659	CN	
5	有效期	生效日期	UTCTime/ GeneralTime	GM/T 0015	YYMMDDHHMMSSZ/YYYYMMDDHHMMSSZ	UTCTime 用于 2049 之前的年份(含 2049) GeneralTime 用于 2049 之后的年份
		失效日期	UTCTime/ GeneralTime	GM/T 0015	YYMMDDHHMMSSZ/YYYYMMDDHHMMSSZ	UTCTime 用于 2049 之前的年份(含 2049) GeneralTime 用于 2049 之后的年份
6	机构信息	机构名称(CN)	UTF-8String			机构证书编码，见 6.4
		三级部门(OU)	UTF-8String	GA/T 380		机构代码第 11、12 位
		二级部门(OU)	UTF-8String	GA/T 380		机构代码第 9、10 位
		一级部门(O)	UTF-8String	GA/T 380		机构代码第 7、8 位
		区/县（L）	UTF-8String	GA/T 380		机构代码第 5、6 位
		市(L)	UTF-8String	GA/T 380		机构代码第 3、4 位
		省(S)	UTF-8String	GA/T 380		机构代码第 1、2 位
		国家(C)	PrintableString	GB/T 2659	CN	

表 2（续）

序号	数据项名称		数据类型	采用标准	内容	说明
7	机构公钥信息		BITString	GM/T 0015		
8	扩展项	CRL 分布点		GM/T 0015		
		机构密钥标识符	OCTETString	GM/T 0015		
		签发单位的密钥标识符	OCTETString	GM/T 0015		
		密钥用途		GM/T 0015		
		证书分类代码	PrintableString			证书分类代码，见 6.2 OID 为 1.2.86.53525105.0.5
		机构组织结构代码	UTF-8String	GA/T 380		采用 GA/T 380 中规定的全国公安机关机构代码。 OID 为 1.2.86.53525105.0.6
9	签名项		BITString	GM/T 0015		

5.4 设备证书格式

设备证书格式如表3所示。

表3 设备证书格式表

序号	数据项名称		数据类型	采用标准	内容	说明
1	版本号		INTEGER	RFC 5280	2	
2	序列号		INTEGER	RFC 5280		正整数
3	签名算法		ObjectIdentifier	RFC 5280 GM/T 0015	SM3WithSM2Encryption	OID 为 1.2.156.10197.1.501
4	签发单位	名称(CN)	UTF-8String	GA/T 380	YD**********CA	其中“**********”采用 GA/T 380 中规定的全国公安机关机构代码
		区/县（L）	UTF-8String		00	
		市(L)	UTF-8String		00	
		省(S)	UTF-8String	GA/T 380		机构代码第 1、2 位

表 3（续）

序号	数据项名称		数据类型	采用标准	内容	说明
		国家(C)	PrintableString	GB/T 2659	CN	
5	有效期	生效日期	UTCTime/ GeneralTime	GM/T 0015	YYMMDDHHMMSSZ/YYYYMMDDHHMMSSZ	UTCTime 用于 2049 之前的年份(含 2049) GeneralTime 用于 2049 之后的年份
		失效日期	UTCTime/ GeneralTime	GM/T 0015	YYMMDDHHMMSSZ/YYYYMMDDHHMMSSZ	UTCTime 用于 2049 之前的年份(含 2049) GeneralTime 用于 2049 之后的年份
6	设备信息	设备名称(CN)	UTF-8String			设备证书编码见 6.5
		三级部门(OU)	UTF-8String	GA/T 380		机构代码第 11、12 位
		二级部门(OU)	UTF-8String	GA/T 380		机构代码第 9、10 位
		一级部门(O)	UTF-8String	GA/T 380		机构代码第 7、8 位
		区/县（L）	UTF-8String	GA/T 380		机构代码第 5、6 位
		市(L)	UTF-8String	GA/T 380		机构代码第 3、4 位
		省(S)	UTF-8String	GA/T 380		机构代码第 1、2 位
		国家(C)	PrintableString	GB/T 2659	CN	
7	公钥信息		BITString	GM/T 0015		
8	扩展项	CRL 分布点		GM/T 0015		
		设备密钥标识符	OCTETString	GM/T 0015		
		签发单位的密钥标识符	OCTETString	GM/T 0015		
		密钥用途		GM/T 0015		
		证书分类代码	PrintableString			证书分类代码见 6.2 OID 为 1.2.86.53525105.0.5

表 3（续）

序号	数据项名称		数据类型	采用标准	内容	说明
		设备持有单位组织结构代码	UTF-8String	GA/T 380		采用 GA/T 380 中规定的全国公安机关机构代码 OID 为 1.2.86.53525105.0.6
9	签名项		BITString	GM/T 0015		

5.5 应用证书格式

应用证书格式如表4所示。

表4 应用证书格式表

序号	数据项名称		数据类型	采用标准	内容	说明
1	版本号		INTEGER	RFC 5280	2	
2	序列号		INTEGER	RFC 5280		正整数
3	签名算法		ObjectIdentifier	RFC 5280 GM/T 0015	SM3WithSM2Encryption	OID 为 1.2.156.10197.1.501
4	签发单位	名称(CN)	UTF-8String	GA/T 380	YD**********CA	其中“**********”采用 GA/T 380 中规定的全国公安机关机构代码
		区/县（L）	UTF-8String		00	
		市(L)	UTF-8String		00	
		省(S)	UTF-8String	GA/T 380		机构代码第 1、2 位
4	签发单位	国家(C)	PrintableString	GB/T 2659	CN	
5	有效期	生效日期	UTCTime/ GeneralTime	GM/T 0015	YYMMDDHHMMSSZ/YYYYMMDDHHMMSSZ	UTCTime 用于 2049 之前的年份(含 2049) GeneralTime 用于 2049 之后的年份
		失效日期	UTCTime/ GeneralTime	GM/T 0015	YYMMDDHHMMSSZ/YYYYMMDDHHMMSSZ	UTCTime 用于 2049 之前的年份(含 2049) GeneralTime 用于 2049 之后的年份
6	应用信息	应用名称(CN)	UTF-8String			应用证书编码，见 6.6

表 4（续）

序号	数据项名称		数据类型	采用标准	内容	说明
		三级部门(OU)	UTF-8String	GA/T 380		机构代码第 11、12 位
		二级部门(OU)	UTF-8String	GA/T 380		机构代码第 9、10 位
		一级部门(O)	UTF-8String	GA/T 380		机构代码第 7、8 位
		区/县（L）	UTF-8String	GA/T 380		机构代码第 5、6 位
6	应用信息	市(L)	UTF-8String	GA/T 380		机构代码第 3、4 位
		省(S)	UTF-8String	GA/T 380		机构代码第 1、2 位
		国家(C)	PrintableString	GB/T 2659	CN	
7	应用公钥信息		BITString	GM/T 0015		
8	扩展项	CRL 分布点		GM/T 0015		
		应用密钥标识符	OCTETString	GM/T 0015		
		签发单位的密钥标识符	OCTETString	GM/T 0015		
		密钥用途		GM/T 0015		
		证书分类代码	PrintableString			证书分类代码，见 6.2 OID 为 1.2.86.53525105.0.5
		应用持有单位组织结构代码	UTF-8String	GA/T 380		采用 GA/T 380 中规定的全国公安机关机构代码 OID 为 1.2.86.53525105.0.6
9	签名项		BITString	GM/T 0015		

6 编码

6.1 证书类型编码规则

证书类型编码用层次码表示，由4位数字组成。编码结构如图1所示。

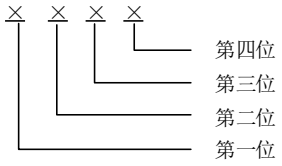


图 1 证书编码结构

第一位，表示存储介质；第二位表示证书类型；第三位表示发放对象；第四位表示终端类型。发放对象和终端类型无细目，则用“0”表示。

6.2 证书分类代码

移动警务数字证书分类代码如表5所示。

表5 移动警务数字证书分类代码表

密码模块类型	证书类型	发放对象	终端类型	证书分类代码
1-硬件密码模块	1-人员证书	1-警员	1-手机智能设备	1111
		2-警务辅助人员		1121
		1-警员	2-POS 机	1112
		2-警务辅助人员		1122
		1-警员	3-执法记录仪	1113
		2-警务辅助人员		1123
		1-警员	4-平板智能设备	1114
		2-警务辅助人员		1124
		1-警员	9-其他终端	1119
		2-警务辅助人员		1129
	2-机构证书	1-公安机关	0	1210
		2-党/政/军机关	0	1220
		9-其它机关单位	0	1290
	3-设备证书	0	0	1300
	4-应用证书	0	0	1400
	9-其他类型证书发放对象	0	0	1900
2-软件密码模块	1-人员证书	1-警员	1-手机智能设备	2111
		2-警务辅助人员		2121
		1-警员	2-POS 机	2112
		2-警务辅助人员		2122
		1-警员	3-执法记录仪	2113
		2-警务辅助人员		2123
		1-警员	4-平板智能设备	2114
		2-警务辅助人员		2124
		1-警员	9-其他终端	2119
		2-警务辅助人员		2129
	2-机构证书	1-公安机关	0	2210
		2-党/政/军机关	0	2220
		9-其它机关单位	0	2290
	3-设备用证书	0	0	2300
	4-移动应用证书	0	0	2400
	9-其他类型证书发放对象	0	0	2900

6.3 人员证书编码

人员证书编码最大长度为128字节，编码格式为：姓名“半角空格”公民身份号码，公民身份号码遵循GB 11643标准。

6.4 机构证书编码

机构证书编码最大长度为128字节，编码格式为：YDJG############，其中，“YD”表示移动警务，“JG” 表示组织机构，“############” 表示机构代码。

组织机构为公安机关的，机构代码遵循GA/T 380标准；组织机构为党/政/军部门的，机构代码遵循GB 32100标准。

6.5 设备证书编码

设备证书编码最大长度为128字节，编码格式为：YDSB############，其中，“YD” 表示移动警务，“SB” 表示设备，“############” 表示设备代码，设备代码各地自行定义。

6.6 应用证书编码

应用证书编码最大长度为128字节，编码格式为：YDYY############，其中，“YD” 表示移动警务，“YY” 表示应用，“############” 表示应用代码，应用代码各地自行定义。