



中华人民共和国公共安全行业标准

GA/T 1251—2015

公安数字证书硬件介质存储空间划分规则

Rules for storage media space division of police certificate

2015-04-23 发布

2015-04-23 实施

中华人民共和国公安部 发布

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：公安部科技信息化局、公安部第三研究所、上海辰锐信息科技有限公司。

本标准主要起草人：邵旭东、顾流、陈家明、李江、刘爱江、刘洋、苏文钦。

公安数字证书硬件介质存储空间划分规则

1 范围

本标准规定了公安数字证书硬件介质存储空间的划分规则。
本标准适用于公安数字证书的制作和使用。

2 存储空间划分

2.1 存储空间结构

公安数字证书硬件介质存储空间划分为基本空间和扩展空间。

2.2 存储空间容量

公安数字证书硬件介质存储空间应不小于 128 KB。

2.3 基本空间

基本空间存储容量为 32 KB,从初始地址依次划分为索引、密钥、证书和预留空间,如图 1 所示,其中:

- a) 索引空间为 1.25 KB,用于存放索引文件;
- b) 密钥空间为 15 KB,用于存放非对称密钥和对称密钥;
- c) 证书空间为 14 KB,用于存放签名证书、加密证书、证书备份和数据索引;
- d) 预留空间为 1.75 KB。

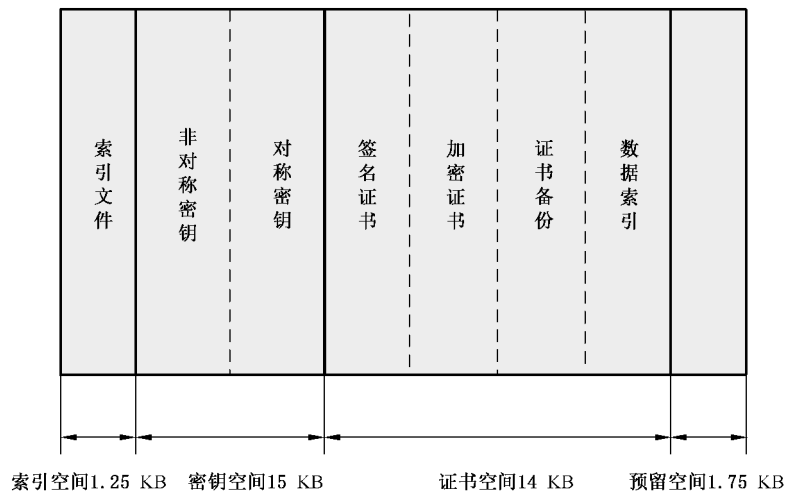


图 1 基本空间划分示意图

2.4 扩展空间

扩展空间存储容量不小于 96 KB,划分为电子签章和预留空间,如图 2 所示,其中: