FIPS PUB 140-2

联邦信息处理标准出版物

（取代1994年1月11日发布的FIPS PUB 140-1）

密码模块安全要求

类别：计算机安全　　子类别：密码

国家标准和技术研究所
信息技术实验室
Gaithersburg, MD 20899-8900
2001 年 5 月 25 日

美国商务部
部长：Donald L. Evans
技术管理局
主管技术副部长：Phillip J. Bond
国家标准和技术研究所
所长：Arden L. Bement, Jr.

目录

FIPS PUB 140-2
《密码模块安全要求》之
派生测试要求

2011 年 1 月 4 日（草案）

CMVP项目成员

（NIST、CSEC 和 CMVP 实验室）

国家标准和技术研究所
信息技术实验室
计算机安全处

Gaithersburg, MD 20899-8930

美国商务部
代理部长：**Rebecca M. Blank**

国家标准和技术研究所
副部长兼所长：**Patrick Gallagher**

目录