

安全路由器产品密码检测准则

Cipher Test Criteria for Secure Routers

国家密码管理局商用密码检测中心

2009年4月

目 次

1 适用范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	1
4 基础密码检测	2
4.1 密码算法的正确性和一致性检测.....	2
4.2 密钥管理检测	2
4.3 随机数质量检测	2
4.4 素性检测	3
5 IPsec VPN 模块密码检测	3
6 SSL VPN 模块密码检测	3
7 文档要求	3
7.1 系统框架结构	3
7.2 密码子系统框架结构	3
7.3 与密码实现和使用相关的硬件.....	3
7.4 源代码	3
7.5 不存在隐式通道的声明	3
7.6 密码自测试或自评估报告.....	3

安全路由器产品密码检测准则

1 适用范围

本准则规定了安全路由器产品的密码检测内容，适用于政府采购法规定范围内的安全路由器产品密码检测。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18018-2007 信息安全技术 路由器安全技术要求

《随机性检测规范》 国家密码管理局

《IPSec VPN 技术规范》 国家密码管理局

《SSL VPN 技术规范》 国家密码管理局

3 术语和定义、缩略语

3.1 术语和定义

3.1.1 对称密码算法 Symmetric Cryptographic Algorithm

加密密钥与解密密钥相同，或容易由其中任意一个密钥推导出另一个密钥，称该密码算法为对称密码算法。

3.1.2 非对称密码算法 Asymmetric Cryptographic Algorithm

加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。

3.1.3 杂凑算法 Hash Function

杂凑算法又称为散列算法、哈希算法或数据摘要算法，是能够将一个任意长的比特串映射到一个固定长的比特串的一类函数。

3.1.4 密钥管理 Key Management

在既定安全策略指导下密钥的生成、分发、存储、使用、更新、导入与导出、备份、恢复、归档和销毁。

3.2 缩略语

IPSec	Internet Protocol Security	Internet 协议安全
SSL	Secure Sockets Layer	安全套接层
VPN	Virtual Private Network	虚拟专用网

4 基础密码检测

4.1 密码算法的正确性和一致性检测

安全路由器产品使用的密码算法的正确性和一致性应满足：

(1) 对称密码算法的正确性和一致性

安全路由器产品中使用的对称密码算法，其运算结果应与标准数据和算法的标准运算结果相符。

(2) 非对称密码算法的正确性和一致性

安全路由器产品中使用的非对称密码算法，其运算结果应与标准数据和算法的标准运算结果相符。

(3) 杂凑算法的正确性和一致性

安全路由器产品中使用的杂凑算法，其运算结果应与标准数据和算法的标准运算结果相符。

4.2 密钥管理检测

安全路由器产品中的密钥管理应实现权限控制机制，密钥管理操作应由获得授权的主体实施，且应满足：

(1) 密钥生成

安全路由器产品能正确生成所用的各类密钥。生成的密钥应与密码算法强度相匹配，并具有密钥种类、用途、长度、拥有者信息、使用期限等密钥属性的审计信息。

(2) 密钥分发

密钥应按权限和密钥属性分发，防止分发过程中密钥泄漏或被篡改，并具备相应的应急处理和响应措施。密钥分发应有分发审计信息。

(3) 密钥存储

密钥应安全存储。对密钥存储的非授权操作应具备应急处理和响应措施。

(4) 密钥使用

密钥应按权限和密钥属性使用，并具备使用过程中的安全防护措施。密钥的使用应具有使用主体、使用时间和使用目的等审计信息。

(5) 密钥更新

密钥应按照密钥属性进行更新，并在出现安全隐患时能及时更新。密钥更新应有更新审计信息。

(6) 密钥导入

密钥应按权限和密钥属性进行导入，确保导入过程中密钥的安全，并应有导入审计信息。

(7) 密钥导出

密钥应按权限和密钥属性进行导出，确保导出过程中密钥的安全，并应有导出审计信息。

(8) 密钥备份

密钥应按权限和密钥属性进行备份，并保证备份密钥的安全存储。

(9) 密钥恢复

密钥应按权限和密钥属性进行恢复，并应有恢复审计信息。

(10) 密钥归档

密钥归档应防止密钥被非授权获取。归档的密钥只能用于确认该密钥以前提供的密码服务。

(11) 密钥销毁

安全路由器产品应具备密钥销毁功能，销毁的密钥不能被部分或全部恢复。密钥销毁应有销毁审计信息。

4.3 随机数质量检测

安全路由器产品生成和使用的随机数应符合《随机性检测规范》的要求。

4.4 素性检测

安全路由器产品非对称密码算法所使用的素数应满足素性要求。

5 IPSec VPN 模块密码检测

检测的项目为《IPSec VPN 技术规范》第 7 章“IPSec VPN 产品检测”规定的内容。

6 SSL VPN 模块密码检测

检测的项目为《SSL VPN 技术规范》第 8 章“产品检测”规定的内容。

7 文档要求

7.1 系统框架结构

以结构图的形式，说明整个安全路由器产品的框架结构，包括安全路由器产品的各个子系统的构成、各子系统的功能和各子系统的实现原理，并附以详细的文字说明。

详细描述安全路由器产品的安全机制、密码体制和密钥管理。

7.2 密码子系统框架结构

以流程图的形式详细描述各密码子系统的工作原理和 workflow，详细说明各子系统所调用的函数的名称和调用顺序，包括密钥生成、更新、销毁、归档等整个密钥生存周期各阶段所用到的函数，以及加密初始化函数、加密函数、解密函数、杂凑函数、签名函数、签名验证函数和加密后处理函数等。

7.3 与密码实现和使用相关的硬件

开发者应提供与密码实现和使用相关的硬件的电气原理图，并附以详细的文字说明。

7.4 源代码

开发者应提供与密码实现和使用相关的源代码，并提供源代码的说明文档。

7.5 不存在隐式通道的声明

开发者应提供安全路由器产品中涉及密码的部分不存在隐式通道的声明文件。

7.6 密码自测试或自评估报告

开发者应提供安全路由器产品的密码自测试或自评估报告。