安全数据库产品密码检测准则

Cipher Test Criteria for Secure Database Systems

国家密码管理局商用密码检测中心

2009 年 4 月

目　次

1 范围 2
2 规范性引用文件 2
3 术语、定义和缩略语 2
4 检测内容 3
4.1 密码算法的正确性和一致性检测 3
4.2 密码功能应用有效性检测 3
4.3 密钥管理检测 5
4.4 密码性能检测 6
4.5 随机数质量检测 6
4.6 素性检测 6
5 文档要求 6
5.1 系统框架结构 6
5.2 密码子系统框架结构 6
5.3 密码子系统函数接口 7
5.4 密码子系统函数接口示例代码 7
5.5 源代码 8
5.6 不存在隐式通道的声明 8
5.7 密码自测试或自评估报告 8
附录 A 静态库、动态库及类似封装形式说明表示例 9

安全数据库产品密码检测准则

1 范围

本准则规定了安全数据库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数据库产品的密码检测。

2 规范性引用文件

下列文件中的条款通过本准则的引用而成为本准则的条款。凡是标注日期的引用文件，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准则，然而，鼓励根据本准则达成协议的各方研究是否可使用这些文件的最新版本。凡是不标注日期的引用文件，其最新版本适用于本准则。

GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求

《随机性检测规范》 国家密码管理局

3 术语、定义和缩略语

3.1 术语和定义

3.1.1 安全数据库产品 Secure Database System

本准则所指的安全数据库产品是指从系统设计、实现、使用和管理等各个阶段都遵循一套完整的系统安全策略，并实现了 GB 17859-1999《计算机信息系统安全保护等级划分准则》所确定的安全等级三级（含）以上的数据库。包括独立的安全数据库产品软件产品和集成或内置了安全数据库的产品。

3.1.2 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。

3.1.3 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。

3.1.4 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，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。

3.1.5 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。

3.1.6 测试对象 Target of Testing

本准则测试对象专指安全数据库产品。

3.1.7 隐式通道 Covert Channel

可用来按照违反安全策略的方式传送数据的传输通道。

3.1.8 调试版本 Debug Product

以调试模式编译的、带有调试信息的最终版本。

3.2 缩略语

SSODB Security Subsystem of Database System 数据库系统安全子系统

SSF SSODB Security Function SSODB 安全功能

4 检测内容

4.1 密码算法的正确性和一致性检测

安全数据库产品使用的密码算法应由密码硬件模块提供，密码硬件模块应从《商用密码通用产品名单》中选用。

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

安全数据库产品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

安全数据库产品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

安全数据库产品使用的杂凑算法，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 密码功能应用有效性检测

安全数据库产品中密码功能应用有效性应满足：

4.2.1 身份鉴别

（1） 基于强化管理的身份鉴别

用户登录系统采用强化管理的口令进行身份鉴别时，可使用密码，其密码功能应正确有效；

系统重新连接采用强化管理的口令进行身份鉴别时，可使用密码，其密码功能应正确有效。

（2） 基于令牌的动态口令身份鉴别

用户登录系统采用基于令牌的动态口令进行身份鉴别时，可使用密码，其密码功能应正确有效；

系统重新连接采用基于令牌的动态口令进行身份鉴别时，可使用密码，其密码功能应正确有效。

（3） 基于生物特征的身份鉴别

用户登录系统使用生物特征进行身份鉴别时，可使用密码，其密码功能应正确有效；

系统重新连接使用生物特征进行身份鉴别时，可使用密码，其密码功能应正确有效。

（4） 基于数字证书的身份鉴别

用户登录系统使用数字证书进行身份鉴别时，其密码功能应正确有效；

系统重新连接使用数字证书进行身份鉴别时，其密码功能应正确有效。

（5） 身份鉴别信息的存储

安全数据库产品对身份鉴别信息进行存储时，应使用密码进行安全保护，其密码功能应正确有效。

（6） 身份鉴别信息的传输

安全数据库产品对身份鉴别信息进行传输时，应使用密码进行安全保护，其密码功能应正确有效。

4.2.2 自主访问控制

安全数据库产品自主访问控制使用密码功能进行身份鉴别时，其使用的密码功能应正确有效。

4.2.3 强制访问控制

（1） 强制访问控制中的身份鉴别

安全数据库产品访问控制与使用密码的身份鉴别相结合时，其密码功能应正确有效；

（2） 强制访问控制中的用户数据保密性

安全数据库产品应实现跨网络的 SSODB 间用户数据的保密功能，其密码功能应正确有效；

（3） 强制访问控制中的用户数据完整性

安全数据库产品应保证跨网络的 SSODB 间用户数据的完整性，其密码功能应正确有效。

4.2.4 安全审计

（1） 安全审计身份鉴别

安全数据库产品安全审计在使用密码功能进行身份鉴别时，其使用的密码功能应正确有效。

（2） 安全审计自主访问控制

安全数据库产品安全审计与使用密码的自主访问控制相结合时，其使用的密码功能应正确有效。

（3） 安全审计数据完整性控制

安全数据库产品安全审计功能应具备数据完整性控制功能，并保证相关密码功能有效。

4.2.5 用户数据完整性

（1） 安全数据库产品数据存储完整性

安全数据库产品在对数据进行访问操作时，检查以库结构形式存储于数据库中的用户数据是否出现完整性错误，其使用的密码功能应正确有效。

（2） 安全数据库产品数据传输完整性

安全数据库产品在系统内部进行数据传输时，使用密码保证用户数据的完整性，其使用的密码功能应正确有效。

（3）安全审计的强制访问控制

安全数据库产品安全审计与使用密码的强制访问控制相结合时，其密码功能应正确有效；

（4） 安全数据库产品用户数据处理完整性

安全数据库产品管理系统中处理的用户数据，使用密码实现实体完整性功能，其使用的密码功能应正确有效。

4.2.6 用户数据保密性

（1） 用户数据存储保密

安全数据库产品使用密码对用户数据进行存储保护时，其密码功能应正确有效。

（2） 用户数据传输保密

安全数据库产品使用密码对用户数据进行传输保护时，其密码功能应正确有效。

4.2.7 可信路径

（1） 初始登录时可信路径建立

在用户进行初始登录时，SSODB 通过密码在它与用户之间建立一条安全的数据传输通路，其密码功能应正确有效。

（2） 身份鉴别时可信路径建立

在用户进行身份鉴别时，SSODB 通过密码在它与用户之间建立一条安全的数据传输通路，其密码功

能应正确有效。

4.2.8 SSODB 自身安全保护

（1） 输出 SSF 数据的保密性

安全数据库产品将 SSF 数据输出到远程信息系统的 SSF 时通过密码保证其不被未经授权的泄漏，其使用的密码功能应正确有效。

（2） 输出 SSF 数据的完整性

安全数据库产品通过密码检测 SSF 间传输的 SSF 数据的修改情况，并在检测到修改时将被修改的数据改正过来，其使用的密码功能应正确有效。

（3） SSODB 内 SSF 数据基本传输保护

安全数据库产品在 SSODB 的分离部分间传输 SSF 数据时通过密码保证其不被泄漏或修改，其使用的密码功能应正确有效。

（4） SSODB 内 SSF 数据分离传输保护

安全数据库产品在 SSODB 的分离部分间传输数据时通过密码分离用户数据和 SSF 数据，保证 SSF 数据不被泄漏或修改，其使用的密码功能应正确有效。

（5） SSODB 内 SSF 传输数据完整性保护

安全数据库产品通过密码检测 SSODB 的分离部分间传输的 SSF 数据的修改情况，并在检测到修改时将被修改的数据改正过来，其使用的密码功能应正确有效。

（6） SSF 间数据一致性保护

安全数据库产品在分布式或复合式环境下，与别的信息系统的 SSF 交换 SSF 数据时，通过密码确保数据一致性，其使用的密码功能应正确有效。

（7） SSODB 内 SSF 数据复制一致性保护

出现包含复制的 SSF 数据的 SSODB 部分断开时，SSF 在重连接后，处理任何与 SSF 数据复制的一致性相关请求前，通过密码实现被复制的 SSF 数据的一致性，其使用的密码功能应正确有效。

（8） 用户与 SSF 间可信路径建立

安全数据库产品通过密码在 SSF 与本地用户或远程用户之间建立一条可信的数据传输通路，其使用的密码功能应正确有效。

（9） SSF 间可信路径建立

安全数据库产品通过密码在 SSF 与远程信息系统的 SSF 之间建立一条可信的数据传输通路，其使用的密码功能应正确有效。

4.2.9 SS0DB 访问控制

安全数据库产品的 SSODB 访问控制应鉴别用户的身份，对用来建立会话的安全属性的范围进行限制，规定时限后，通过密码重新鉴别用户，其用户身份鉴别功能及相关密码功能应正确有效。

4.3 密钥管理检测

安全数据库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

安全数据库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

安全数据库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。

4.4 密码性能检测

安全数据库产品密码性能检测内容包括：

（1） 对称密码算法运算速率

（2） 非对称密码算法运算速率

（3） 杂凑算法运算速率

4.5 随机数质量检测

安全数据库产品生成和使用的随机数应符合《随机性检测规范》的要求。

4.6 素性检测

安全数据库产品非对称密码算法所使用的素数应满足素性要求。

5 文档要求

5.1 系统框架结构

以结构图的形式，说明整个安全数据库产品的框架结构，包括安全数据库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。

详细描述安全数据库产品的安全机制、密码体制和密钥管理。

5.2 密码子系统框架结构

（1） 密码子系统的整体框架结构说明书

以结构图的形式，说明整个安全数据库产品中各密码子系统的框架结构，包括密码子系统的各个功能模块的构成、各功能模块的功能和各功能模块的实现原理，并附以详细的文字说明。

（2） 密码子系统的功能模块流程说明书

以流程图的形式详细描述各子模块的工作原理和工作流程，详细说明各模块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。

5.3 密码子系统函数接口

根据具体实现的软件技术不同，密码子系统调用的与密码相关的函数（5.2 节第 2 点所述）存在形式可以有静态库、动态库、硬件模块和源码直接编译四种方式（但不限于），函数接口说明应该具有以下 7 个方面的内容（但不限于）：

（1） 静态库函数接口说明

如果密码子系统中调用的函数是存放在静态库中，则应以列表形式（见附录 A）说明静态库中所有函数名称、参数形式、返回值、调用备注等相关信息，同时提供子系统的调试版本。

（2） 动态库函数接口说明

如果密码子系统中调用的函数是存放在动态库中，则应以列表形式（见附录 A）说明动态库中所有函数名称和函数序号、参数形式、返回值、调用备注等相关信息。

（3） 硬件调用函数接口说明

如果密码子系统中调用的函数是通过硬件实现的，则应具有硬件模块函数接口，并以列表形式（见附录 A）说明硬件调用函数接口名称、参数形式、返回值、调用备注等相关信息。

（4） 调试版本子系统说明

如果密码子系统通过源代码直接编译生成，则应提供子系统的调试版本，及函数接口名称、参数形式、返回值、调用备注等相关信息。

（5） 私钥专用检测函数接口说明

安全数据库产品应具有私钥专用检测函数接口，用以提取私钥并进行相关测试，并以列表形式（见附录 A）说明私钥检测专用函数接口名称、参数形式、返回值、调用备注等相关信息。该接口仅用于密码检测，正式产品不应存在此接口。

（6） 专用文件格式操作函数接口说明

安全数据库产品进行密钥存储、密钥备份、密钥归档、密文存储等操作时，若采用专用的文件格式，应提供专用文件格式的详细说明和专用文件格式操作函数接口说明。

（7） 专用数据格式操作函数接口说明

安全数据库产品进行密钥传输、密文传输等操作时，若采用专用的数据格式，应提供专用数据格式的详细说明和专用数据格式操作函数接口说明。

5.4 密码子系统函数接口示例代码

针对 5.3 中说明的函数接口，为了进一步说明函数之间的相互关系，应提供以下 7 个方面的示例代码内容（但不限于）：

（1） 静态库函数接口示例代码说明

如果调用的函数是存放在静态库中，则应以 C++示例代码的形式，说明如何成功调用静态库中与密码技术相关的函数接口。

（2） 动态库函数接口示例代码说明

如果调用的函数是存放在动态库中，则应以 C++示例代码的形式，说明如何成功调用动态库中与密码技术相关的函数接口。

（3） 硬件模块函数接口示例代码说明

如果密码功能是通过硬件实现的，则应以 C++示例代码的形式，说明如何成功调用硬件模块中与密码技术相关的函数接口。

（4） 调试版本子系统函数接口示例代码说明

如果密码子系统通过源代码直接编译生成，则应以 C++示例代码的形式，说明如何成功调用相关的功能函数。

（5） 私钥专用检测函数接口示例代码说明

密码子系统应具有私钥专用检测函数接口，用以提取私钥并进行相关测试。并以 C++示例代码的形式，说明如何成功调用相关的专用检测函数接口。

（6） 专用文件格式操作函数接口示例代码说明

安全数据库产品应具有专用文件格式的文件操作函数接口 C++示例代码详细说明书，用以说明对专用文件格式的正确操作。

（7） 专用数据格式操作函数接口示例代码说明

安全数据库产品应具有专用数据格式的数据操作函数接口 C++示例代码详细说明书，用以说明对专用数据格式的正确操作。

5.5 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。

5.6 不存在隐式通道的声明

开发者应提供安全数据库产品涉及密码的部分不存在隐式通道的声明文件。

5.7 密码自测试或自评估报告

开发者应提供安全数据库产品的密码自测试或自评估报告。

附录 A 静态库、动态库及类似封装形式说明表示例

Arithmetic.DLL 函数说明

序号	函数名称	返回值	参数及说明		备注
			参数	说明	
0x0002	GetDivide	bool //运算结果	Int iDividend	被除数	除数为 0 时，函数返回值为 false
			int iDivisor	除数	
			int* iQuotient	商	
			int* iResidue	余数	