# 量子密盾产品白皮书

## （QE-KEY）

**深圳科盾量子信息科技有限公司**

**2022 年 12 月 01 日**

版权声明

量子密盾产品白皮书

**首先，我们非常感谢您查看本文档：**

本文档介绍了量子密盾的架构、功能和特点，为用户在选用本系统时提供参考。本手册仅提供电子文档。

**未经书面许可，用户不得以任何形式或通过任何途径，包括使用影印、录制在内的电子或机械手段等对该书任何部分进行复制或传播。**

**警告和承诺：**

本文档用于提供关于“量子密盾”的产品信息。尽管我们尽最大的努力使本文档尽可能的完善和准确，但疏漏和缺陷之处在所难免。

任何人或实体由于本文档提供的信息造成的任何损失或损害，深圳科盾量子信息科技有限公司不承担任何义务或责任。

本书中表达的观点权属于深圳科盾量子信息科技有限公司。

**系统版权：**

中文名称：量子密盾

开发单位：深圳科盾量子信息科技有限公司

**本系统的版权单位：**

公司：深圳科盾量子信息科技有限公司

地址：深圳市福田区华富街道田面社区深南中路4028号田面城市大厦21E

编码：518000

电话：（0755）82799013

邮箱：kedunliangzi@kdquantum.com

量子密盾是深圳科盾量子信息科技有限公司自主研发的受法律保护的商业产品。遵守法律是共同的责任，任何人未经授权人许可，不得以任何形式或方法以及出于任何目的复制或传播本产品，权利人将追究侵权者责任并保留要求赔偿的权利。

本产品及其文档中使用到其他公司的有关资源，其版权归相应公司所有，亦受到法律的严格保护。

**反馈信息：**

您的反馈意见将使我们受益非浅。如果您对本手册有任何疑问、意见或建议，请与我们联系：（0755）82799013，感谢您对我们的支持和帮助。

目 录

[1. 产品简介 4](#_Toc26791)

[2. 产品特点 5](#_Toc29411)

[2.1. 数据更安全 5](#_Toc10041)

[2.2. 身份认证增强 5](#_Toc24006)

[2.3. 量子密钥充注 5](#_Toc6502)

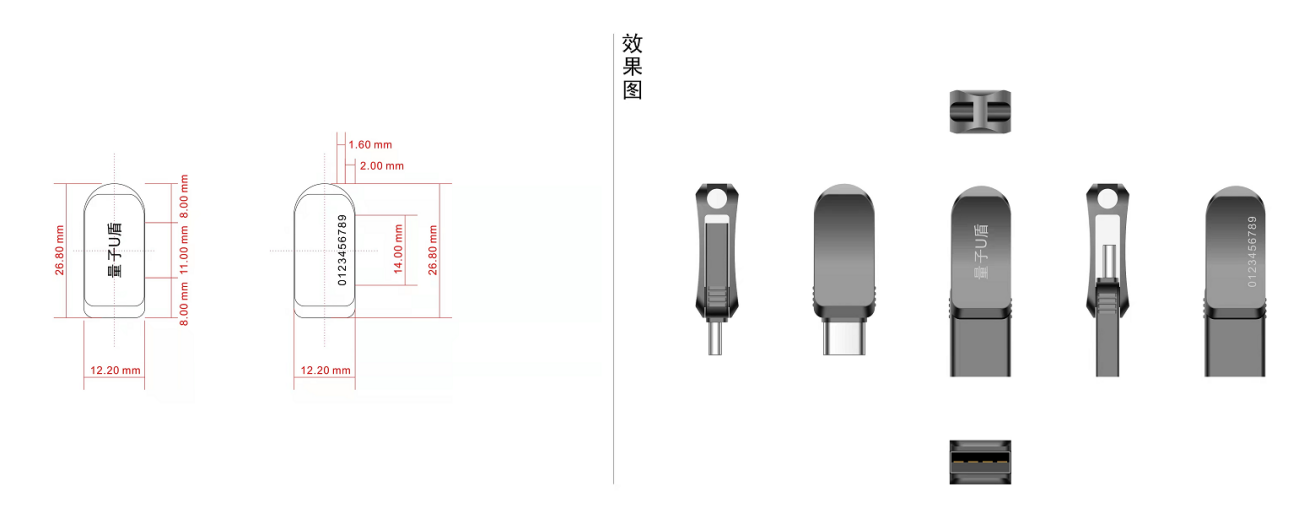
[2.4. 多平台接口支持 5](#_Toc31456)

[3. 服务架构 5](#_Toc17105)

[4. 性能参数 7](#_Toc27029)

[5. 公司介绍 8](#_Toc28271)

# 产品简介

量子密盾，即我司推出的并获得国家密码证书的客户端USBkey，符合GM/T 0009-2012《SM2密码算法使用规范》、GM/T 0015-2012《基于SM2密码算法的数字证书格式规范》、GM/T 0016-2012《智能密码钥匙密码应用接口规范》标准，是我司加密安全业务的高级别安全工具。量子密盾适用于我司所有客户，特别适合于安全级别要求较高的客户。量子密盾能为身份认证、数据加密传输、数据加密存储等业务提供安全保障。量子密盾是用于电子签名和数字认证，以及数据加解密的工具，它内置微型智能卡处理器，采用SM2非对称密钥算法对网上数据进行加密、解密和数字签名，支持SM3、SM4算法，符合国家商密标准，确保业务核心数据的保密性、真实性、完整性和不可否认性。

量子密盾（TYPE-C/USB）产品图

# 产品特点

## 数据更安全

拥有量子密盾，进行数据身份认证、数据加密传输时，客户不用再担心黑客、假网站、木马病毒等各种风险，量子密盾可以有效的保障客户的核心安全。

## 身份认证增强

内置身份认证增强功能，在PKI基础上，叠加量子密钥认证，拥有量子密盾后，客户可以进行身份认证同时，进行二次认证，进一步提高身份认证安全性。

## 量子密钥充注

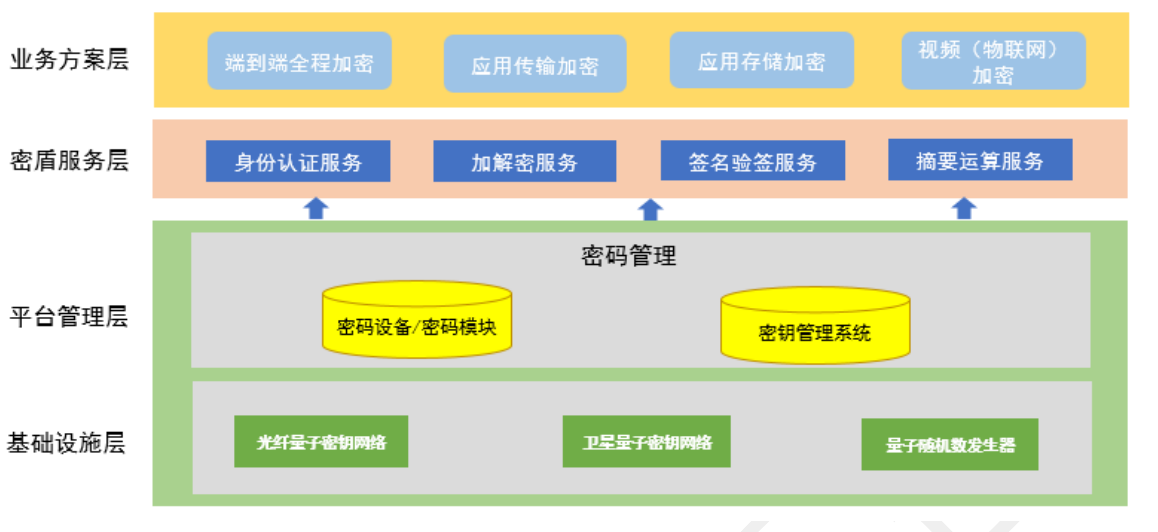
存储量子密钥、密钥数量可灵活定制，可通过在线/离线等多种方式进行量子密钥充注，确保对称业务密钥的安全。

## 多平台接口支持

拥有USB、TYPE-C、TF卡、蓝牙等多种接口方式，满足不同设备的接入需求。同时支持WINDOWS、LINUX、Android等多种平台，支持适配X86、龙芯、飞腾、兆芯等多种处理器架构。

# 服务架构

“密盾+量子”密码服务架构如下图所示。根据架构要求，系统主要分为量子密钥分发/生成层、量子密码基础服务层、应用安全密盾服务层。其中量子密钥分发/生成层为系统提供量子密钥，由量子密钥分发网络（光纤和卫星），以及量子随机数发生器组成；量子密码基础服务层为系统提供基础密码服务（密钥管理平台、密码机、密码模块等），包括密钥全生命周期管理、加解密算法和协议等；应用安全密盾服务层，包括应用身份认证、加解密服务、签名验签服务、摘要运算服务。应用安全密盾服务层将量子密钥/密码技术，与实际用户业务系统进行融合，从而提高信息系统的安全性。



“密盾+量子”密码服务架构图

# 性能参数

|  |  |
| --- | --- |
| 序 号 | 主要性能参数 |
| 1 | 采用TYPE-C/USB接口； |
| 2 | 128KB高速智能密码钥匙； |
| 3 | 金属旋转式外壳；提供定制外壳标识； |
| 4 | 可增加自定义API，满足量子密钥的存储、更新等； |
| 5 | Windows标准的CSP，可以存储数字证书； |

# 公司介绍

深圳科盾量子信息科技有限公司是深圳比特耐特信息技术股份有限公司和海南国科量子通信网络有限公司共同成立并控股的技术型高科技公司，是国内最先致力于将量子通信技术和经典密码技术进行融合的网络信息安全创新公司，主要从事商用密码产品及信息安全产品的研发与销售，并提供网络信息安全整体解决方案与专业信息安全服务，在密码与信息安全领域具有雄厚实力。

公司研发的“量子增强密钥管理系统”是国内首个通过国家密码管理局测评的基于量子密钥的加密产品。已获得7项国家专利，20余项软著，并成功为多个政府单位提供定制化数据加密解决方案。是中国密码学会会员单位，深圳市商用密码行业协会会员单位。

目前，公司服务的客户群体主要集中在8个领域，分别是政府、公安、应急、电力、水务、医疗、军队、教育；随着公司的发展以及业务的需求，公司将在更多领域与用户单位开展深度合作，提供优质的量子加密及信息安全服务。

科盾量子以经典密码技术为基础支撑，通过与国内量子网络龙头企业深度合作，将量子密码技术创造性地与对称密码体系融合，提供专业、合规、标准、安全的量子增强安全产品和解决方案。在信息技术互联网化，移动化和云化的发展趋势下，公司形成的一系列功能完善、稳定可靠的密钥管理产品，将为“数字产业化、产业数字化”提供一流的量子安全级别信息安全保障。