(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112597551 B
(45)授权公告日 2023.08.18

(21)申请号 202011524762.3

(22)申请日 2020.12.22

(65)同一申请的已公布的文献号
申请公布号 CN 112597551 A

(43)申请公布日 2021.04.02

(73)专利权人 南京道熵信息技术有限公司
地址 211100 江苏省南京市江宁区秣周东路9号

(72)发明人 周林

(74)专利代理机构 南京苏高专利商标事务所(普通合伙) 32204
专利代理师 孟红梅

(51)Int.Cl.
G06F 21/80(2013.01)

(56)对比文件
CN 103268435 A,2013.08.28
CN 106936797 A,2017.07.07
CN 109218333 A,2019.01.15
US 2008134178 A1,2008.06.05
US 2014165053 A1,2014.06.12
WO 2012149717 A1,2012.11.08

审查员 罗思异

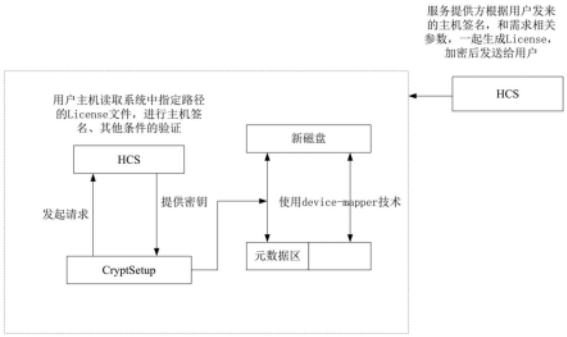
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种使用License可实时更新的磁盘加密方法与系统

(57)摘要

本发明公开了一种使用License可实时更新的磁盘加密方法与系统,该方法根据用户主机的磁盘uuid生成主机签名,再将包括加密时间、主机签名以及容量大小限制在内的用户需求相关信息加入License中,对License进行加密得到密文;在磁盘加密软件请求密钥时对License进行验证,生成主机签名、读取系统时间,和License中信息进行比对以确定能否加密;若验证通过,将与主机签名相关的密钥发送给磁盘加密软件,对需要加密的磁盘进行映射。本发明采用新的加密思路不再局限于固定字符串作为加密密钥,使得磁盘加密过程更加的安全可靠,并且过程全部可控,能够解决遗忘密码的窘境。



CN 112597551 B

1.一种使用License可实时更新的磁盘加密方法,其特征在于,包括如下步骤:

(1)根据用户主机的磁盘uuid生成主机签名,并发送给License提供方;

(2)License提供方将用户需求相关信息加入License中并进行加密,将License密文发送给用户主机,其中用户需求相关信息包括到期时间、主机签名以及容量大小限制;

(3)用户主机将License密文存放在指定的路径,保证用户主机每次启动时能正确读取并解密License信息;

(4)在磁盘加密软件请求密钥时对License进行验证,根据磁盘uuid生成主机签名,并和License中的主机签名进行比对,且读取并记录系统时间,并和License中到期时间和上次记录的时间进行比对,且比对用户需要加密的盘与License中限制的盘大小;若主机签名比对结果为不一致,或系统时间不在到期时间范围内,或系统时间早于上次记录的系统时间,或用户需要加密的盘大小超过License中限制的盘大小,则无法加解密,否则进入步骤(5);

(5)依据设定的字符提取规则将主机签名中的部分字符,或License密文中与主机签名相关的部分字符作为密钥发送给磁盘加密软件,磁盘加密软件根据提供的密钥对需要加密的磁盘进行映射。

2.根据权利要求1所述的使用License可实时更新的磁盘加密方法,其特征在于,License提供方在License中增加标记License密文生成时间的时间戳;在用户主机对License密文进行验证时,根据该时间戳判断License密文是否为最近设定时间范围内产生的,若不是,则无法加解密。

3.根据权利要求1所述的使用License可实时更新的磁盘加密方法,其特征在于,所述步骤(1)中根据预先设定的字符提取规则截取用户主机上所有磁盘uuid设定位置的字符组成主机签名。

4.根据权利要求1所述的使用License可实时更新的磁盘加密方法,其特征在于,所述步骤(2)对License中信息进行加密后,再进行ASCII码移位得到License密文。

5.根据权利要求4所述的使用License可实时更新的磁盘加密方法,其特征在于,在进行ASCII码移位之前,对加密算法得到的字符串对与时间相关的整数取余。

6.根据权利要求1所述的使用License可实时更新的磁盘加密方法,其特征在于,对License进行验证时,记录失败次数,进行延时验证或锁住磁盘;被锁住的磁盘需要新的License密文才能解开。

7.根据权利要求1所述的使用License可实时更新的磁盘加密方法,其特征在于,在生成主机签名时,若用户主机为虚拟主机,则生成的主机签名的位数少于实体主机的主机签名位数。

8.根据权利要求1所述的使用License可实时更新的磁盘加密方法,其特征在于,所述磁盘加密软件对磁盘进行分区,将磁盘分为元数据区和数据区,只对元数据区进行映射。

9.一种使用License可实时更新的磁盘加密系统,其特征在于,包括用户主机密钥管理模块、磁盘加密模块以及License提供方密钥管理模块;

所述用户主机密钥管理模块,用于根据用户主机的磁盘uuid生成主机签名,并发送给License提供方,接收License提供方发送的License密文,并将License密文存放在指定的路径,保证用户主机每次启动时能正确读取并解密License信息;

所述License提供方密钥管理模块，用于将用户需求相关信息加入License中并进行加密，将License密文发送给用户主机，其中用户需求相关信息包括加密时间、主机签名以及容量大小限制；

所述磁盘加密模块，用于根据提供的与用户主机签名相关的密钥对需要加密的磁盘进行映射；

所述用户主机密钥管理模块，还用于在磁盘加密软件请求密钥时对License进行验证，根据磁盘uuid生成主机签名，并和License中的主机签名进行比对，且读取并记录系统时间，并和License中到期时间和上次记录的时间进行比对，且比对用户需要加密的盘与License中限制的盘大小；若主机签名比对结果为不一致，或系统时间不在到期时间范围内，或系统时间早于上次记录的系统时间，或用户需要加密的盘大小超过License中限制的盘大小，则无法加解密，否则在磁盘加密模块请求加密密钥时，依据设定的字符提取规则将主机签名中的部分字符，或License密文中与主机签名相关的部分字符作为密钥发送给磁盘加密模块。

10.根据权利要求9所述的使用License可实时更新的磁盘加密系统，其特征在于，所述License提供方密钥管理模块，还在License中增加标记License密文生成时间的时间戳；所述用户主机密钥管理模块对License密文进行验证时，根据该时间戳判断License密文是否为最近设定时间范围内产生的，若不是，则无法加解密。

一种使用License可实时更新的磁盘加密方法与系统

技术领域

[0001] 本发明涉及磁盘加密方法,具体涉及一种能够对安全性要求高的磁盘进行灵活加解密的使用License的磁盘加密方法与系统,属于软件加密认证领域。

背景技术

[0002] 当前磁盘加密技术主要采用device-map技术,在磁盘进行映射时,对其进行加密,主要技术是DriveCrypt,虽然加密程序提供了异常可靠的实时加密功能,可以确保数据安全,避免数据丢失。但是加密所采用的随机字符,难以记忆;且我们使用加密磁盘时,当加密的字符串丢失或遗漏,只能依靠专业的技术人员到现场恢复,甚至专业人员操作也可能出现丢数据的风险;并且现有加密技术的字符串都是随机生成的,无法涵盖一些有用信息,这是一个技术瓶颈。

[0003] 当前磁盘加密具有很多的不足之处,不够灵活且安全系数低,这对于安全系数极强的用户(如军队/银行/政府)是不安全的;不足之处主要有如下几个方面:1、磁盘加密无法限制时间,加密之后就一直是加密盘,这对只需要某个时间段加密的场景不友好,可能只需要一定时间段内对数据盘进行加密;2、磁盘全盘加密影响效率,每次读写都需要加密之后才能落盘,不适合于高安全高性能的场景。3、无法限制磁盘大小和类型进行加密;针对不同的盘进行不同的加密方法,如虚拟盘的加密;4、无法定时更新,理论上可以使用穷举法暴力破解;5、都是采用固定字符串作为加密密钥,一旦忘记,无法再打开旧的加密盘,密码忘记了,就无法再解密,只能格式化。

发明内容

[0004] 发明目的:针对上述现有技术磁盘加密的不足,本发明目的在于提供一种使用License可实时更新的磁盘加密方法与系统,采用新的加密思路不再局限于固定字符串作为加密密钥,使得磁盘加密过程更加的安全可靠,并且过程全部可控,能够解决遗忘密码的窘境。

[0005] 技术方案:为实现上述发明目的,本发明采用如下技术方案:

[0006] 一种使用License可实时更新的磁盘加密方法,包括如下步骤:

[0007] (1)根据用户主机的磁盘uuid生成主机签名,并发送给License提供方;

[0008] (2)License提供方将用户需求相关信息加入License中并进行加密,将License密文发送给用户主机,其中用户需求相关信息包括到期时间、主机签名以及容量大小限制;

[0009] (3)用户主机将License密文存放在指定的路径,保证用户主机每次启动时能正确读取并解密License信息;

[0010] (4)在磁盘加密软件请求密钥时对License进行验证,根据磁盘uuid生成主机签名,并和License中的主机签名进行比对,且读取并记录系统时间,并和License中到期时间和上次记录的时间进行比对,且比对用户需要加密的盘与License中限制的盘大小;若主机签名比对结果为不一致,或系统时间不在到期时间范围内,或系统时间早于上次记录的系

统时间,或用户需要加密的盘大小超过License中限制的盘大小,则无法加解密,否则进入步骤(5);

[0011] (5)依据设定的字符提取规则将主机签名中的部分字符,或License密文中与主机签名相关的部分字符作为密钥发送给磁盘加密软件,磁盘加密软件根据提供的密钥对需要加密的磁盘进行映射。

[0012] 进一步优选,License提供方在License中增加标记License密文生成时间的时间戳;在用户主机对License密文进行验证时,根据该时间戳判断License密文是否为最近设定时间范围内产生的,若不是,则无法加解密。

[0013] 进一步优选,所述步骤(1)中根据预先设定的字符提取规则截取用户主机上所有磁盘uuid设定位置的字符组成主机签名。

[0014] 进一步优选,所述步骤(2)对License中信息进行加密后,再进行ASCII码移位得到License密文。

[0015] 进一步优选,在进行ASCII码移位之前,对加密算法得到的字符串对与时间相关的整数取余。

[0016] 进一步优选,对License进行验证时,记录失败次数,进行延时验证或锁住磁盘;被锁住的磁盘需要新的License密文才能解开。

[0017] 进一步优选,在生成主机签名时,若用户主机为虚拟主机,则生成的主机签名的位数少于实体主机的主机签名位数。

[0018] 进一步优选,所述磁盘加密软件对磁盘进行分区,将磁盘分为元数据区和数据区,只对元数据区进行映射。

[0019] 一种使用License可实时更新的磁盘加密系统,包括用户主机密钥管理模块、磁盘加密模块以及License提供方密钥管理模块;

[0020] 所述用户主机密钥管理模块,用于根据用户主机的磁盘uuid生成主机签名,并发送给License提供方,接收License提供方发送的License密文,并将License密文存放在指定的路径,保证用户主机每次启动时能正确读取并解密License信息;

[0021] 所述License提供方密钥管理模块,用于将用户需求相关信息加入License中并进行加密,将License密文发送给用户主机,其中用户需求相关信息包括加密时间、主机签名以及容量大小限制;

[0022] 所述磁盘加密模块,用于根据提供的与用户主机签名相关的密钥对需要加密的磁盘进行映射;

[0023] 所述用户主机密钥管理模块,还用于在磁盘加密软件请求密钥时对License进行验证,根据磁盘uuid生成主机签名,并和License中的主机签名进行比对,且读取并记录系统时间,并和License中到期时间和上次记录的时间进行比对,且比对用户需要加密的盘与License中限制的盘大小;若主机签名比对结果为不一致,或系统时间不在到期时间范围内,或系统时间早于上次记录的系统时间,或用户需要加密的盘大小超过License中限制的盘大小,则无法加解密,否则在磁盘加密模块请求加密密钥时,依据设定的字符提取规则将主机签名中的部分字符,或License密文中与主机签名相关的部分字符作为密钥发送给磁盘加密模块。

[0024] 进一步优选,所述License提供方密钥管理模块,还在License中增加标记License

密文生成时间的时间戳;所述用户主机密钥管理模块对License密文进行验证时,根据该时间戳判断License密文是否为最近设定时间范围内产生的,若不是,则无法加解密。

[0025] 有益效果:与现有技术相比,本发明具有如下优点:1、本发明使用License加密,可以选择某个时间段内对磁盘加密,这个时间段内的数据就是封装加密的,比如设置某个日期之前的文件是加密的;2、本发明使用License加密,可以限制磁盘大小,对类型进行区分,不同的磁盘类型可进行不同的加密,采用不同的加密算法方法和策略;3、本发明使用元数据分区加密,可以只选择加密元数据分区加密,无需全盘加密,提高数据读写效率。4、本发明中不需要用户记住密码,即使丢失,可以向提供商购买新的License,对磁盘进行解密,无需毁坏数据,解决了遗忘密码的窘境。5、本发明可以实现License的实时更新,能够适用于安全性要求高的场合。

附图说明

[0026] 图1为本发明实施例的原理示意图。

[0027] 图2为本发明实施例中采用的分区加密形成新的逻辑盘架构示意图。

具体实施方式

[0028] 下面将结合附图和具体实施例,对本发明的技术方案进行清楚、完整的描述。

[0029] 本发明实施例基于新的加密思路采用License对磁盘进行加密映射,通过本发明开发的专用软件HCS(HorebCryptSetup,软件主要职责是生成主机签名、解读、验证、传送License等),结合现有的磁盘加密软件CryptSetup实现本发明的功能。如图1所示,本发明实施例公开的一种使用License可实时更新的磁盘加密方法,先根据用户主机的磁盘uuid生成主机签名,并发送给License提供方;然后License提供方将用户需求相关信息加入License中并进行加密,将License密文发送给用户主机,用户主机将License密文存放在指定的路径,保证用户主机每次启动时能正确读取并解密License信息;在磁盘加密软件请求密钥时对License进行验证,若验证失败则无法加解密,提取与用户主机签名相关的字符作为密钥发送给磁盘加密软件,磁盘加密软件根据提供的密钥对需要加密的磁盘进行映射。具体操作如下:

[0030] 1、用户需要生成单独主机签名,使用HCS软件的接口sig_pc_gen,根据用户主机上面的所有磁盘,生成一串字符,这个字符串是截取所有磁盘uuid的特定位置(例如截取所有uuid的质数位字符)字符组成,如果用户主机更换磁盘,那主机签名就会变。用户将整个唯一的签名发给License的提供方。在生成主机签名之前,可检查环境,判断是否是虚拟化的,如果是虚拟环境,生成策略会考虑一些性能因素,生成的主机签名会较实体主机的短一点。

[0031] 2、根据用户需求,将加密时间(到期时间)、主机签名以及容量大小限制等因素加入License中,软件可以根据这些信息,使用加密算法,调用lic_gen接口,生成一个唯一的字符串,其中加密算法可以是现有加密算法(如国密SM4、openssl等)或自定的加密算法,具体算法选择不公开,并在其基础上进行ASCII码移位,移位规则不公开,所生成的字符串对用户来说不是明文的(License信息加密的密钥和规则HCS软件中用户主机和提供方预先已有约定)。License文件信息中包含有License版本号lic_ver、附属信息extra-data、到期时间valid-to、生成时间戳gen_date(用于支持实时更新的场景)、主机签名sig等信息;其中

到期时间可以限制磁盘在哪个时间之前进行数据加密,明文如下:

[0032] [HOREBCHECK]

[0033] lic_ver=200

[0034] extra-data=5N200T

[0035] valid-to=2021-12-30

[0036] gen_date=1608088796

[0037] sig=wGYdtC9dYnVj9EeptiTE+6bB8wIhw69Dm8tx62bc4/wX/+VvcFj8OfNJbse8dAIz3Ydjt1BDR7UoYaQ/+1zpnhG/9O2G+7CWmsnnlYzoCMNLJ4WxulmeWjrQhRmOvGrmjEkeYg2SkAhhQGCOOXD4utXC9e8yaoVkycA1JnU2PKE=

[0038] 密文如下:

[0039] U2FsdGVkX1+iYEZaT7chWjCOhPFBv949AhyHzkVHLKOJuj8nhp+mmI13Mejh6NRoOAvwO/OEngslWT1OwthvfilY1aaAJpzH1/uZdMOMQKzmt/U+22UwbzHLs+OyZS+9nN/fiArC3ClzdfKavwFN9p86hQ+j1s76Qx4MbBxEj65//3F+ywVuVf8mKACdH/W6I+/K7gADuOtDEpnCASd8YSRqKIlELOnG7wRwrE/9BxigQMrOm65l/jReOdbEYGM2tefTsY6ToJRf2aASixobipPhPLAF8cACqndzQUlBOsnPQigNlj2LBhxOEwlxVaRorCzC6PJJitywXWPCftOAEWhu8g8RIHSrfkyDqUwVjN4OQLjk1nNw3xyqrN9t739weMIxu7D3AvTAC6ShfFwFtw==

[0040] 3、License的密文放置在系统的某个位置,需要将其路径写在/etc/rc.local中(比如/etc/license),以保证每次服务器重启的时候,HCS软件能正确读取到License信息。

[0041] 4、主机重启时,HCS软件也会调用sig_pc_gen接口,根据当前磁盘uuid生成主机签名,和License中的主机签名进行比对,生成规则已经编译到HCS中,且会读取系统的时间,和License中有效时间进行比对,记录此次比对的时间戳,如果用户串改系统时间,下次比对是系统时间戳就会比上次保存的时间戳小,HCS程序会报错;且会比对用户需要加密的盘是否小于License中限制的盘大小,超过则无法加密。若用户丢失了License,只需将主机签名(含有磁盘uuid信息)发给提供方,提供方根据主机签名和其他限制信息生成新的license,发给用户,HCS软件只要在License中检测到uuid即认为这个License是正规的。

[0042] 支持实时更新的场景中,在HCS检查license密文之前,会读取License密文中的一段gen_date字段,这个字段是对当前时间戳(可以通过date获取)的前六位数字进行加密,时间戳的前6位在三个小时之内是不会变的,就是说HCS检查License时,会提前验证这个License密文是不是最近三小时之内产生的,如果不是,拒绝验证。

[0043] 5、对磁盘进行加密映射时,CryptSetup和HCS软件结合,HCS软件保存了License和磁盘uuid信息,以及他们之间的对应关系。

[0044] 6、如图2所示,CryptSetup对磁盘进行分区,将磁盘分为两个区,元数据区和数据区,本发明只对元数据区进行映射,携带磁盘uuid,向HCS发起请求,HCS将其对应的License字符串返回,如果是第一次加密,直接将磁盘的uuid存入信息表,返回License密文信息。磁盘加密的字符采用主机签名的某些位字符串。例如,主机签名是:sig_pc=ABCDEFGHIJKLMSNIJK;用户需求等其他信息:other_info=UJKLOGINKSDF;提供方拿到ABCDEFGHIJKLMSNIJK之后和UJKLOGINKSDF,假设使用ASCII码移位加密形成:U2FsdGVkX1+3gv1bZFOGUQ8u8OcvR/OOkhkt8xRFYhlpI8k5TxOZW1uheX4FjZ1fIRN/aUChk2IWjjSA69oOCeAi6yBpOguEh++2dHLtycbchOnGkltUoVTmdWvG

[0045] 用户拿到License之后，进行ASCII码反移位，解密并定位获得sig_pc；判断和本地生成的主机签名是不是一致的，检验是否过期、是否超过容量等，如果都满足之后，截取主机签名中的某一些特定位为磁盘加密的字符，如(BDGHKNDNCDSHI)。当然，若License密文中能区分出主机签名的密文，也可以截取主机签名密文中的字符作为磁盘加密的密钥。

[0046] 7、CryptSetup获取到密文字符串时，根据此密文对磁盘进行映射；形成一个新的虚拟的device；即在磁盘的两个分区中，一个加密，一个不加密，两者联合再新建逻辑卷，成为一个完整的虚拟OSD(Object Storage Device)。

[0047] 8、在新的虚拟device上面数据开始进行读写。如果磁盘被拔走，上面的数据都是密文，无法读取，且需要HCS和CryptSetup软件协助。所以数据是绝对安全的，无法暴力破解。

[0048] 9、当License丢失之后，可以使用新的License进行解密，因为License是融合了主机签名、用户需求的一段字符串密文；所以当旧的License丢失，客户需要将主机签名发给提供方，提供方根据该主机签名融合其他信息，生成一个新的License；HCS读取到License之后，会先进行解密，读取其中sig那一段字符，如果和本机的主机签名一致，那么久认为该License是合法的。

[0049] 此外，对于安全性更高的场合，本发明加密方法可定时更新License之间的某一段值，例如：早上8点，取所有字符串的ASCII码，对8取余，然后都移位随机数组位置；9点钟就对9取余；等等。如果有人破解磁盘加密，超过20次，就直接开启延时验证，半个小时后才可以再试；如果直接锁住，就必须采用新的License才能将磁盘解开。

[0050] 本发明实施例公开的一种使用License可实时更新的磁盘加密系统，包括用户主机密钥管理模块、磁盘加密模块以及License提供方密钥管理模块；用户主机密钥管理模块，用于根据用户主机的磁盘uuid生成主机签名，并发送给License提供方，接收License提供方发送的License密文，并将License密文存放在指定的路径，保证用户主机每次启动时能正确读取并解密License信息；License提供方密钥管理模块，用于将用户需求相关信息加入License中并进行加密，将License密文发送给用户主机，其中用户需求相关信息包括加密时间、主机签名以及容量大小限制；磁盘加密模块，用于根据提供的与用户主机签名相关的密钥对需要加密的磁盘进行映射；用户主机密钥管理模块，还用于在磁盘加密软件请求密钥时对License进行验证，根据磁盘uuid生成主机签名，并和License中的主机签名进行比对，且读取并记录系统时间，并和License中到期时间和上次记录的时间进行比对，且比对用户需要加密的盘与License中限制的盘大小；若主机签名比对结果为不一致，或系统时间不在到期时间范围内，或系统时间早于上次记录的系统时间，或用户需要加密的盘大小超过License中限制的盘大小，则无法加解密，否则在磁盘加密模块请求加密密钥时，依据设定的字符提取规则将主机签名中的部分字符，或License密文中与主机签名相关的部分字符作为密钥发送给磁盘加密模块。在安全性较高的场合，License提供方密钥管理模块，还在License中增加标记License密文生成时间的时间戳；用户主机密钥管理模块对License密文进行验证时，根据该时间戳判断License密文是否为最近设定时间范围内产生的，若不是，则无法加解密。

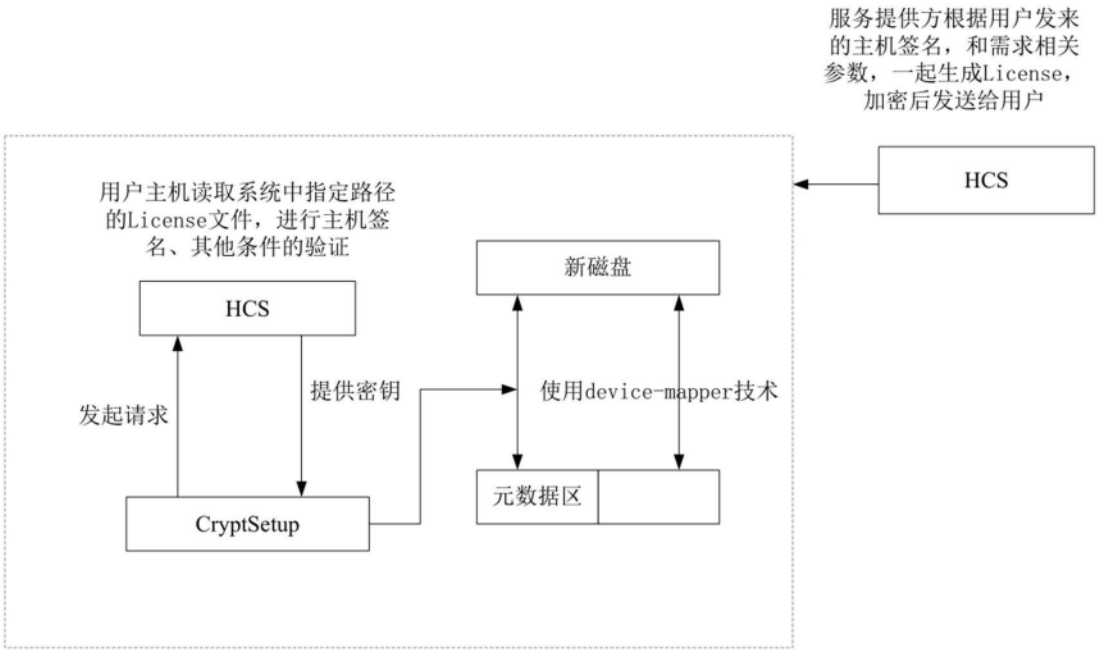

服务提供方根据用户发来的主机签名，和需求相关参数，一起生成License，加密后发送给用户
HCS
用户主机读取系统中指定路径的License文件，进行主机签名、其他条件的验证
新磁盘
HCS
提供密钥
使用device-mapper技术
发起请求
元数据区
CryptSetup

图1

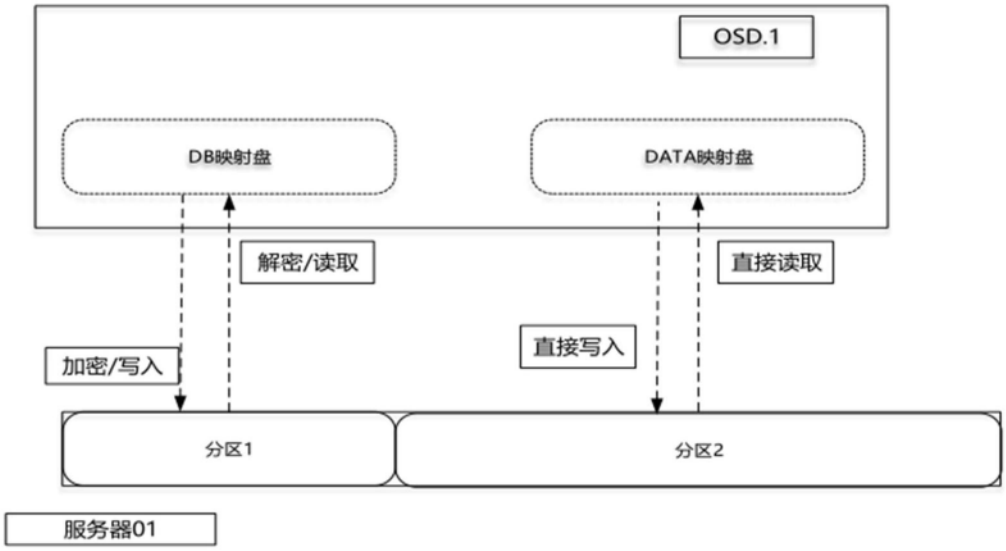

OSD.1
DB映射盘
DATA映射盘
解密/读取
直接读取
直接写入
加密/写入
分区1
分区2
服务器01

图2