## 原文

未区分说话人 00:02

大家上午好，下面由我来代表编制组向大家介绍量化评估规则这个文件的内容。首先我们看一下这个文件的位置，它是处于我们今天的上午讲的测评的一个评价体系的。量化评估这个位置说白了就是说给评估的结果进行打分。那么我的报告分三部分内容，第一个是关于设计的初衷向大家做一个介绍，第二部分介绍一下主要的规则，最后再强调几个要注意的点。首先在设计量化评估的时候，或者说我们在最开始设计最初的一个评价标准的时候，其实从密码学角度来说，其实密码强调是比较强的安全性，也就是没有像安全普通的安全一样，有很多量化的指标，或者说很多风险评估的内容，所以说密码的一个理论基础是非常深厚的一个内容。

未区分说话人 00:59

那么从密码理论来说，比如说有这些评价指标，从理论上来说，比如密钥有多少的商，对这个密码算法有多大的复杂度，公钥密码算法解决困难问题又有多少的复杂度？比如说我们常数的2s1024，它的破解的安全强度就只有二的80次方，我们又称为80比的安全，这可能就是我们传统密码学理论上的一些量化的指标。那么因此来说从理论上来讲，在我们前面所讲的密钥严格保密的情况下，使用这些已经在用的标准的算法是可以保证实际的实际的安全性能。

未区分说话人 01:37

因此来说传统的密码检测，包括产品检测，除了验证算法的实现的正确性，接口的正确性之外，重点就是检测我们密钥的安全性，检测密钥的全生命周期有没有泄露的风险。如果出现的话，其实在我们执行前产品检测的时候就执行的就是一票否决制。所以说在最初设计密评的一些评价标准的时候，我们执行的也是一票否决制，也是延续了这个理念，但是实际上从密码的安全到密码应用的安全，再到我们系统的安全，其实是有很多的过渡过程的。

未区分说话人 02:15

所以说在密码用起来就可能存在各种各样的应用安全问题。这里我也显示了去年在温州水城报告的时候，李永强老师的一个图，就是说从密码学到网络安全到系统安全，其实是有很多的联系，那么从底层的密钥管理到上层的算法技术，再到更上层的密码的使用，每一个环节出问题，其实都会降低密码应用的安全性。这里之所以强调是降低，就是因为从信息系统安全的角度来说，它指的是一个它一个重要的目标就是说把风险降低到可接受的范围内，这个相当于是一个量化的评价的指向。

未区分说话人 02:58

所以说这里我们讲的是可以降低密码应用安全性，并不是说使密码应用的安全性完全失效。因此来说从系统安全这个角度来说，我们在风险可控的前提下，我们有后面高风险判定指引标准来约束，而且在我们现在国产密码应用在推进，很独盏统在改造的大背景下，系统的密码应用情况要有一个量化的评价指标，也就是说能让信息系统的承建方或者信息系统责任方能看到自己的系统每年在进步，或者说每一步骤在进步，这也是一个量化评价的东西所要呈现的内容。

未区分说话人 03:35

因此来说在这种设计初衷的前提下，我们就给出了量化评估规则的一个设计的一个原则。首先是遵循法律法规和最新的标准指导性文件的总体要求，遵循基本要求，还有测评要求，后面我们还有几个导向，第一个是鼓励使用密码技术，鼓励使用密码记录，第二个是特别鼓励使用合规的密码算法技术产品和服务。所以这两个的评价的一个指标或者评价的一个分值完全是不一样的。然后另外提出了密码应用的两个重要的一个方向，优先在网络和通信安全应用和数据安全这两个层面进行密码技术应用，因为这两个是目前密码产品比较成熟，密码应用也比较成熟的两个领域，所以说优先在这两个层面进行密码技术的应用。

未区分说话人 04:25

因此来说在导向的基础上，我们就开展了后面的量化规则的一个设计，下面跟大家做一个详细的介绍。首先我们先看一下量化评估的步骤，首先给完整体的测评结果之后，就给完符合部分符合或者不符合之后要计算的每一个对象的，也就是我们每一个测评项的测评结果。所以特别每个测评项的测评结果进行汇总之后，得到一个测评单元或者每个测评单元的得分。

未区分说话人 05:00

测评单元上面就是测评层，就是安全层面再汇总得到安全层面的得分，最后把安全层面之间再进行汇总，得到总体的得分，所以我们要强调一点，就是说量化评估一定是在把所有的整体测评都做完，也就是说把该修正修正完，该弥补的弥补完之后，再进行一个细致的打分。那么首先我们先看一下量化评估的框架，框架的最底层是密钥管理的安全，再上层是密码算法和基础的安全，最上层是密码使用安全，我们也称为Dak的一个模型，我们看一下它跟测评要求里面的各个关系。

未区分说话人 05:41

关于密码使用安全就是最上层的对应的就是测评，要求的里面的测评实施的第三条判定的就是说密码技术有没有被正确有效的使用，那么密码算法和技术的安全对应的就是测评要求的第一条，也就是算法和技术是不是合规。密钥管理的模型的最底层就是密钥管理安全，它对应的侧面要求的第二条就是密钥安全，其实指的就是说密钥管理的全生命周期是否安全，用于密码计算或密钥管理的密码产品和密码服务是否安全，也就是说我们的产品有没有通过认证，这是一个非常重要的指标。

未区分说话人 06:29

那么按照这个模型的基础上， Dak这个模型基础上，我们就有了一个更加详细的测评指标。那么在首先我们先看一下这个表，这个表也在我们这个规则里面有，那么这个表里面分了三列，Dak三列，分别是使用安全，算法的技术合规和密钥管理安全。那么第二部分是第二列，下面一列给出了示例，最后一列给出了分值。首先要说的是这里讲的密码测评要求里面指的密码服务、密码产品，还有密码算法技术，不再单独的评价，而是融合在具体的一个测评指标里面进行评价，跟我们测评要求的整个内容也是一致的。

未区分说话人 07:16

第二个要说明的一点就是对于密钥应用管理要求，不是技术要求的外的管理要求，不针对各个对象的测评结果进行量化评估，而是根据测评要求给出各单元评价的结果，后面我会再举例再进行说明，符合为一不符合0，部分符合0.5就没有更加细致的一个评价了。另外一个如果对于同一个测评对象涉及多个密码算法，产品服务和密钥的，Dak的都按照最低的分值进行给分，前面就是一些总体的原则，后面我逐行进行一个举例的介绍。

未区分说话人 07:56

第一个一分比较好理解，它指的就是测评对象使用了认证合格的密码产品，且使用的密码算法技术，合规正确有效，而且其中的密钥管理都是在密码产品由密码产品来做的。比较典型的事例就是我们 slvpn使用的是标准的sm4sm3算法，而且配置正确使用的是方证书由sm二进行的身份鉴别。二第二行指的是是0.50.5分，有两不同的一个两个不同的情况。第一个情况就是说算法技术的合规性有距离，第二个就是密钥管理的安全性，跟我们这个标准情况有距离，这个先讲第一个是使用认证合格的密码产品，但是使用的密码算法就是不合规，主要指的是我们先期一些认证过的产品，还支持比如说SS2sa等等算法。

未区分说话人 09:00

这时候如果它里面调用了sisc算法，但是这个产品也是被认证通过的，而且这个功能也是被检测通过的，这种情况下我们才会给0.5分。比如说我们一个有认证过的产品，但他自己新加了一个新的算法，这种情况下是不能够给人不能给不能够给分值的，这是第一个0.5分。第二种情况0.5分就是使用未经认证或者不满足安全等级要求的密码产品，但是使用的密码算法技术合规这有两种情况，第一个不满足安全等级的要求，比如说我们要求使用二级的情况下使用了一级，这种情况下就满足了这种情况。

未区分说话人 09:43

第二种情况是产品没有经过认证，但是使用的算法和技术合规，但是我们这里指的是一定是可被命名人员验证的算法和技术，如果命名能力没有能力验证，或者说无法为命名的命名人员提供验证的证据的情况下，这种情况下也是不能够认为是算法和技术合规的。比如我们常见的科学验证手段，比如说我们就用sm三杂凑这种方法，比如说在提供好源代码，提供好测试压力的情况下，逆变人员可以用相应的基准性的工具来验证算法合规，这种情况下是可以得到分值的。

未区分说话人 10:20

其他如果你做一些更复杂的算法，这样的情况下是很难满足这个要求的。再下面一条是关于0.25分这个分值，就是两个情况都不满足，就未经产品未经认证或者不满足安全点的要求，企业使用的算法和技术不合规，这里主要指一下未经认证，但公开的经长期验证无问题的密码算法，比如说就open SSL里面的稳定版本的密码算法，这种情况下且是这种但是实现不合规或者无法验证合规的密码算法技术，可以匹配这种条款，这种情况下就只能给0.

未区分说话人 10:58

5分。所以说当你上面这种情况对于使用标准的sm算法，但是无法提供验证合规的证据的情况下，那么仍然给0.5分，所以说对于0.5分的给出的分值也需要非常慎重，非常慎重，这种情况下比较好理解，比如说密码使用也不安全，或者说算法和技术，算法和技术和密钥管理这种情况都我都是什么情况都可以，所以说只要是密码使用不安全这种情况下就直接给0分，就判定不符合。这种比较好理解，那么下面我们看一下再给出每个对象的得分情况下，来怎么进行给我们具体给一个事例。

未区分说话人 11:50

那么我们随便举个例子，这个例子不是真实的案例，下面会有人讲真实的情况，这里我们只是举个例子，那么对于每个对象都按照Dak给出一个具体的情况的判定是勾还是画叉，然后最后给出了一个相应的分值，这是每个对象的一个得分的情况下面，在这个基础上我们要给出每个测评单元的情况，其测评单元其实就是把所有的测评对象进行汇总求平均，所有的测评对象的得分进行汇总求平均，就是测评单元的得分情况，但是到了安全层面，这个里面就有一些变化，那么这是给的是各个测评单元的得分的奖励，也就是把这个里边对象的得分都做一个平均，到了测评单元之后就有一些变化。

未区分说话人 12:43

那么里面首先我们先看一下对于管理方面的测评单元，对于管理方面的测评单元，我们前面讲过了，只有一分和0.5分或者0分三三个档，只要是部分符合就给0.5，而且测评对象没有区分。测评对象都是我们被测系统的一个管理体系，里面包括了各种文件。下面再讲下午再讲测评报告的时候还会详细讲解。下面就到了这个层面，主要是对各个测评单元给出了一个权重，我们最开始也讲了，我们设计原则里面有一个就是说对于不同的层面，或者说对于不同的指标要给一个不同的权重，我们优先在网络层和应用层推进密码应用。

未区分说话人 13:31

因此来说在我们规则的一个正文里面也是给出了一个权重表，那么对每一个指标都给出了一个权重，从1分0.7分0.4分等等都给出了一个权重，那么并且对比较重要的一的权重进行了提升。本来我们这个权重是按英一可来给的，如果是英的就给一分，一的话给0.7分，可的话就给0.4分。那么对于一些重要的仪的权重也进行了相应的提升，比如说对物理和环境安全的身份鉴别，对应用和数据层面的数据传输和存储完整性，还有对于安全管理方面的制度相关的要求也进行了相应的提升。

未区分说话人 14:11

那么这里我们也举个例子，比如说我们从网络层来看，对于网络层的得分之后，就是每个测评单元得分之后，来进行一个权重的相乘和平均，最后得到一个分值，那么这里主要说一下不适用的情况。如果这个指标不适用这个特殊的指这个指标不适用的话，就是不计入整体的分值，相当于说0.4就不带进去来算，这样的话它的权重也没有在里面进行一个体现。还有就是对于特殊指标，特殊指标的话也是不计算到统一的分值里面的单独进行判定的，这是对于管理层面的一个事例，管理层面它的权重只有第一个是一分，那么其他的都是0.

未区分说话人 15:03

7分，所以说权重是这样来计算的。最后得到各个层面之后，还有一个东西对于整体的得分情况的介绍，对于整体的情况，其实这里也有一个权重，就对层面也有个权重。其实这个指的除了权重的含义，还有一个就是固定得分的含义。这里主要是约束什么？主要是约束，可能对于有的系统或者有的这个情况下，可能某一个层面它都可能出现不适应的情况，对于这种情况也得进行考虑，也在进行考虑。

未区分说话人 15:39

因此来说对于每个测评安全层面其实是给了一个总分，其实给了一个总分，就是说如果当一个层面只有一个指标的情况下，这个指标就代表整个层面的得分，所以说给了每个测评单元的分之后，每个层面的分之后，还要根据每个层面的权重来进行一个加权平均，这里也是按照100分的分值来给出一个每个层面的得分，分别是物理和环境安全十分，网络和通信安全15分，设备和计算安全15分，应用和数据安全30分，管理人员建设都是8分，最后应急处置是6分，通过这个之后进行加权平均之后就得到了最终的分值。

未区分说话人 16:23

我们得到最终分值的整体的情况，这里延续了一个概念，就是我们所有的技术的层技术的要求的一个加分总分总共是70分，那么管理的是总共30分，也体现了一个7分技术3分管理的概念。那么如果某个安全层面的所有指标都不适用，除了跟安全层面不参与量化评估不参与，比如说某一个层面都不适用，那么这个层面也都不参与量化评估，所以说当某个层面不适不适用的情况下，这个层面的分并不会完全的去扣掉，而是会把它给平均掉，平均到其他层面里面去，这个不用做特地的分摊，在我们做加权平均的时候，它就会自动考虑这个事情，最后得到总分之后有一个测评结论的形成过程。

未区分说话人 17:14

刚刚肖老师已经讲过了，我们有三个条件，三种条件。最后再强调几点内容，第一个是关于我们最终结论的形成，一定要结合高风险的判定指引，如果有高风险得到0.5分或者0.25分，对最终结论其实也是没有影响的。所以说不要只看到分值，还要看到每一个分值背后的有没有高风险。第二个事情其实我刚才也强调过了，就是说对于技术层面的部分符合的判定要慎重，这里对测评人员的要求就很高了。

未区分说话人 17:52

测评要非常深入的细致，而且证据要非常的严谨和充分。比如说我们要判定一个使用一个非没有认证过的产品，但是实现了一个合规的算法，这时候判定就非常的慎重。这里我们强调的是专业的事情要有专业的人来做，鼓励大家去使用专门的密码产品已经通过了认证的密码产品，也鼓励我们现在密码产品去做简单认证，这样的话密钥还有产品的安全性才有基本的保证。

未区分说话人 18:19

我们在密评的时候，其实对产品的测评或者对方的测评远达不到产品进行测评的一个深度和广度，而且严谨程度还有标准的符合性，其实都差得很远。虽然我们这里给出了0.5分0.25分的阈值，实际上我们还需要测评人员去做一个非常详细的判定，那么在测评的时候要有这么一个导向，也就是说要用认证合格的产品要鼓励的我们的厂商要去做密码产品的检测认证，那么还有一些条款，条款的不适用并不是不去测评，而是要去验证不适用的条件，还有替代性措施是否真实存在。

未区分说话人 18:57

这个情况下主要体现在我们关于密码应用方案里面的应合一的条款，那么对于一的条款可以进行不适用的判定，但是不适用要有条件，而且要有相对替代性措施。那么在测评的时候就要去验证这些条件和提升措施是否真正存在。如果它不存在的话，这时候我们就要把它视作是为这个条这个指标就要作为试用，然后进行判定，可能很有可能情况下得0分。所以这个也需要测评人员去仔细的判定。还有一个情况就是说我们在测评的时候，不像以前如果是一票否决的话，大家给这个不符合可能就很随意，就发现没有用密码或者用了国外密码直接给不符合也不用做任何的判定，或者不用做任何的分析，有了量化评估之后就要求大家在做一些比如说使用国外的算法或者使用自己实验算法，由大家去做很详细的判定，所以说要大家去做一些有深度的测评，真正的去发现一些问题，大家为用户去解决一些问题。

未区分说话人 20:04

最后要说的是我们这个文件现在目前来说是给大家来试用一段时间，那么适时的话也会进行修订，这个文件也不打算做成标准里面的阈值，也会随着密码应用的情况来逐渐提高。这里我们在报告里面给出了60份，后面有可能进行调整，那么这个工作也需要大家一起去推进，就是我。