INGOLD SOLUTIONS GMBH

Key Management Policy
(Ref No: - ISMS/IS/5.2/5)

A key management policy (KMP) is a high-level set of rules that are established by an organization to describe the goals, responsibilities, and overall requirements for the management of cryptographic keying material used to protect private or critical facilities, processes, or information. These statements include authorization and protection objectives, and constraints that apply to the generation, distribution, accounting, storage, use, and destruction of keys. Key Management Policies are implemented by systems administrators through a combination of security mechanisms and procedures.

Varieties of security policies

There are several types of policies that are needed before a key management system (KMS) can be implemented and put into use. Different organizations may have different policies related to the security levels needed for their particular product or service. Policies can also vary within an organization for different applications and types of data. The KMS must be designed to handle and support the requirements of individual business units within each organization. The various types of policies can be very difficult to sort through and understand unless some form of simplification can be made.

Organizing policies in layers

To address the requirements, organizations often use a hierarchy of policies, in a layered fashion. The functions that oversee and control the actions of the policies in general are placed in the top level (or top layer). The top layer is usually the information-management level that provides the basic requirements and desired control actions for the lower levels. The lower and intermediate levels provide the details of the actual implementation and enforcement procedures for a particular type of security protection defined in an upper layer. So each layer in this hierarchy handles a particular subset of key management system functions and tasks related to security, and passes other specific requirements down to the next lower level, which is designed to handle them.

Assigning tasks for each policy layer

Each layer performs its set of functions and tasks in the form of “outputs” based on certain “inputs” related to the type of security provided. Each layer also interacts with the next higher policy level to make sure policy is in accordance with the overall requirements. Although this can vary between organizations, the layers (in terms of the tasks they handle) are typically arranged from top to

bottom as: information management, data security, physical security, computer security, communications security, and cryptographic key security. For the purpose of this article, these multiple layers can be reduced to just three layers, as described below:

Functions of the top policy layer (Information Management)

The top policy layer (Information Management) sets the foundation for the overall management based on established set of standards, which include industry standards, legal requirements, and organizational goals regarding its needs for data protection. This policy usually sets the goals for assuring information security, and also establishes the types of authorization and management roles for a select group of people. The specifications provided in this layer are passed down to the next lower level (Information Security), and provides information on the protection levels needed for the various categories of sensitive data and information. This information includes specifications for the levels of confidentiality, integrity, availability, and source-authentication protections.

Functions of the second policy layer (Information Security)

The next lower level (Information Security), is designed to specify more details on the basic information received from the information management layer. Details are provided on the protection needed for the various kinds of threats, and how that protection should be implemented for each data type. This layer is provided with additional inputs to determine how and what information should be protected, which include a list of the potential threats to the security of the organization's information, and the risks associated with the unauthorized disclosure, modification, and destruction or loss of the information. From these inputs, the information security layer can determine the degree of protection for the various categories of data, and rules for implementing this protection. This policy may also include the guidelines of a Data Security policy, which provides rules for protecting electronic information, governs the use of computers, applications, and communication networks. In relation to the cryptographic techniques that should be defined in the first two policy layers, outputs are provided to the next layer (KMS Security Policy) that defines the use and protection of the additional mechanisms that provide security protection for the cryptographic keys and associated metadata.

INGOLD SOLUTIONS GMBH

Functions of the third policy layer (KMS Security Policy)

The next lower level (KMS Security Policy), is created to establish and specify the details on protecting keys and metadata, which maintain confidentiality, integrity, availability, and source authentication throughout a key's life cycle. The KMS Security Policy should state the specific protections applied to each key type and its metadata, and the length of time that keys and metadata are to be retained based on the sensitivity of the data they protect. All cryptographic mechanisms and protocols that can be used by the KMS are specified by this policy. This policy must also be consistent with the higher level policies. It is often required that a Security Policy be encoded so that an automated system can enforce it. In this case, a KMS Security Policy would be converted to electronic format, so that a firmware program will enforce the policy requirements. Such systems may be able to check themselves for proper functioning, diagnose problems, report the problem, and even automatically correct the problem.

Other Related Security Policies

Sometimes other external policies are required for proper and secure operation of the key management systems. These should be included in the key management policy. These policies are layered just below the KMS Security Policy, and it directs their actions by providing inputs based on their assigned functions. These policies would also return outputs to the higher levels to verify their compliance with the system requirements. These external policies would also include inputs related to the more advanced technical factors, such as security standards and possible threats to data. An example of an external policy is a document stating how physical protection and access control is provided to assure protection of the key management system itself. The key management system could be designed and implemented to provide these features, or they could be provided by the facility in which the key management system is installed and operated.

Domain Security Policy

One of the more important policies layered below the KMS Security Policy is the Domain Security Policy. This policy provides the rules and restrictions that allow computers, networks, applications, and users in the same domain to exchange and process data, keys, and metadata with the given protection stated in the policy. If the domains of two entities are different, they can communicate only if certain conditions are satisfied. For example, if a certain subset of the provided protections satisfy both domain security policies, communication can take place between the two entities, but it is limited according to the equivalent portion of the policies.

INGOLD SOLUTIONS GMBH

Using a key management system designed for a market segment

Normally, a standard off-the-shelf key management system design will not have the capabilities or features in its design that would satisfy the requirements of all organizations. They are usually designed to support the market segment which the key management system is meant for. An organization looking to utilize a key management system should consider the capabilities and features documented by the designer of the key management system. These documents should be reviewed by the organization, and modified to develop a KMS Security Policy to suit the needs of the organization.