IBM Systems MEDIA

Trusted Key Entry Policy Wizards

Do you have IBM Z host crypto modules and want to manage them using the most secure tool and processes available? TKE has a set of wizards for you to use to help uncomplicate things.

By Garry Sullivan

03/01/2019

Do you have IBM Z host crypto modules and want to manage them using the most secure tool and processes available? Do you find the thought of using Trusted Key Entry (TKE) overwhelming? Well, don't worry. TKE has a set of wizards for you to use to help uncomplicate things.

IBM Z host crypto modules must be managed according to strict policies established by the client. These policies are based on client preferences that are influenced by various legal, regulatory and compliance requirements. In many cases, the final policies must include dual control management and hardware-based master key part protection to pass internal and external security audits. TKE is the only feature that allows you to manage IBM Z host cryptographic modules running in Common Cryptographic Architecture (CCA) or IBM Enterprise PKCS#11 (EP11) mode, using compliant-level hardware-based key management techniques.

To help you define your security policies, TKE provides six wizards that work together to implement a comprehensive set of security policies for managing access to the TKE workstation and managing host crypto modules and their domains. These security policies require that something is stored on a smart card. Therefore, the first wizard (the TKE Smart Card Wizard) creates the smart cards that the other five wizards need. The five additional wizards set up the minimum recommended security policies for managing administrators responsible for specific tasks.

Identify What Needs to Be Managed

Before we get started, it's important to identify everything that needs to be managed from TKE. There are two categories:

1. The TKE workstation: An access policy must be created for administrators that manage the TKE workstation and a policy must be created for administrators that access TKE to manage host crypto modules. This is covered by the TKE Workstation Logon Policy Wizard.
2. Host crypto modules: Host crypto module management is broken down into these four categories:
    - CCA host crypto module-wide settings and normal mode domain-specific settings
    - CCA host crypto module domains in Imprint mode and PCI-Compliant mode
    - EP11 host crypto module-wide settings
    - EP11 host crypto domain-specific settings

There is a TKE policy wizard for managing access to the TKE workstation and a TKE policy wizard for establishing a management policy for host crypto modules in each of the four module categories. You only need to use the wizards you require. In addition, each of the TKE policy wizards expect something to be stored on smart cards, which the TKE Smart Card Wizard creates.

An Overview of the New Wizards

1. TKE Smart Card Wizard

The first wizard in the TKE policy wizard family is the TKE Smart Card Wizard. All TKE policy implementation wizards use smart cards. This wizard creates the smart cards the other five TKE policy implementation wizards need. You can also use this wizard to create a new TKE zone and enroll your TKE workstation in a TKE zone.

2. TKE Workstation Logon Profile Wizard

The TKE Workstation Logon Profile Wizard helps you create a set of individual and group TKE local crypto adapter profiles, conforming to your policy definition for managing access to your TKE workstation. Your administrators are sorted into two categories:

- Administrators that manage the TKE workstation
- Administrators that need access to the TKE to manage host crypto modules

The TKE Workstation Logon Profile Wizard requires that the individual local adapter profile logon keys are stored on TKE or EP11 smart cards that have descriptions beginning with specific values. The best way to create these smart cards is with the TKE Smart Card Wizard found in the Smart Card Utility Program (SCUP). There are two kinds of TKE workstation logon policies for two different kinds of administrators:

- **TKE Workstation Logon Policy for TKE Workstation Administrators:** The TKE Workstation Logon

Profile Wizard implements a TKE workstation access policy for the administrators that manage TKE. The wizard's policy requires two individual TKE local crypto adapter smart card profiles for the administrators responsible for managing the TKE workstation. These profiles must be members of a TKE local crypto adapter group profile. The wizard does the setup for you. There are two kinds of TKE workstation logon policies for two different kinds of administrators:

- **TKE Workstation Logon Policy for Host Crypto Module Administrators:** The TKE Workstation Logon Profile Wizard implements a TKE workstation access policy for the administrators that manage host crypto modules. The wizard's policy requires individual TKE local crypto adapter smart card profiles for administrators responsible for managing host crypto modules.

When you look at the list of local profiles the TKE Workstation Logon Profile Wizard can create for the host module managers, the process of deciding how to manage access to the TKE workstation can be overwhelming. Most administrators prefer one of these two policies:

- Create individual profiles for a small number of administrators and make the individual profiles members of a group profile that require all the individuals to present during a TKE workstation logon. This provides a level of TKE access approval for administrators that do not have their own TKE workstation logon profiles.
- Create individual profiles for your host module administrators. This provides maximum individual accountability but increases the number of local profiles to manage.

3. CCA Setup Module Policy Wizard

The CCA Setup Module Policy Wizard creates a set of host crypto module roles and authorities that your administrators use when managing module-wide and normal mode domain-specific settings. The CCA Setup Module Policy Wizard creates four roles that places host module administrators into two categories:

- Administrators responsible for managing all settings except master and operational keys. One role only allows the administrator to start (issue) commands while the second role only allows the administrator to approve (cosign) commands.
- Administrators responsible for managing master and operational keys. One role only allows the administrator to load a first key part while the other role only allows the administrator to load additional or last key parts.

4. CCA Setup PCI Environment Wizard

The CCA Setup PCI Environment Wizard is similar to the CCA Setup Module Policy Wizard, but helps you create a set of domain-specific host crypto module roles and authorities that your administrators use when managing domain-specific settings for domains that are configured to run in PCI-Compliant mode. The CCA Setup PCI Environment Wizard is only available when a domain is in IMPRINT MODE. This is the state that a domain must be in order to do the initial PCI-Compliant domain configuration before you can move the domain to PCI-compliant mode. The CCA Setup PCI Environment Wizard creates four roles that place host domain administrators into the same two categories listed above, in the CCA Setup Module Policy Wizard overview section.

5. EP11 Setup Module Policy Wizard

The EP11 Setup Module Policy Wizard is only available when an EP11 host crypto module is in its initial state, which is called imprint mode. While the module is in this state, you add the administrators that manage the module once it's taken out of imprint mode. The EP11 Setup Module Policy Wizard creates and adds the module-wide EP11 administrators you need to manage your module. After the wizard has added the administrators, it takes the module out of the initial state by changing the signature threshold and revocation

signature threshold value from zero to two.

6. EP11 Setup Domain Policy Wizard

The EP11 Setup Domain Policy Wizard is only available when an EP11 host crypto domain is in its initial state, which is called imprint mode. While the domain is in this state, you add the administrators that will manage the domain once it’s taken out of imprint mode. As you would expect, the EP11 Setup Domain Policy Wizard is like the EP11 Setup Module Policy Wizard, with a focus on EP11 domains. The EP11 Setup Domain Policy Wizard creates and adds the domain-specific EP11 administrators you need to manage your domain. The wizard also takes the domain out of imprint mode for you after the administrators have been added to the domain.

Reducing Complexity

TKE is the only feature that allows you to manage IBM Z host cryptographic modules running in CCA or EP11 mode using compliant-level hardware-based key management techniques. With the help of the TKE policy wizard family, setting up the management policy for the TKE workstation and the host crypto modules that you manage is simple and straightforward. The TKE wizards reduce the time you spend, and simplify the process of setting up policies for managing your cryptographic environment.

About the author
Garry Sullivan is the team leader of the Trusted Key Entry development team.