CA Top Secret® for z/OS

Design Guide

r15

CA Technologies Product References

This documentation set references the following CA products:

- CA ACF2™ for z/OS (CA ACF2)
- CA Common Services for z/OS (CA Common Services)
- CA Distributed Security Integration Server for z/OS (CA DSI Server)
- CA LDAP Server for z/OS (CA LDAP Server)
- CA Top Secret® for z/OS (CA Top Secret)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Formulating a Security Policy

This section contains the following topics:

Statement of Goals

Detail your security implementation goals before you set out to achieve them. Your installation's CA Top Secret implementation plan should be based on the following premises:

CA Top Secret is a means to an end

Your environment is not secure immediately after installing CA Top Secret. CA Top Secret is the tool used to build a secure data processing installation.

Implementation requires adequate support

A security implementation does not go quickly and it requires internal support. Security must have support in terms of management direction, manpower, and resources. Take the time to evaluate the environment and plan the implementation. A rushed implementation often requires rework.

Security is a global concern

The corporate area assigned to handle security administration is not the only area that needs to be concerned with security and the security product. Security is not a function that can be restricted to one area. It is an environment consisting of every person involved in the data processing function-from the EDP auditors to the end-users. Without the support of all individuals, it is unlikely that security will be taken seriously within your organization.

Security implementation is ongoing

The security implementation never ends. After implementation of CA Top Secret, you will find that your use of CA Top Secret must be continually adjusted to reflect changes which occur within your installation. Your implementation is just as dynamic as your data processing environment. It will require continual analysis, review, and modification to properly protect your installation.

Management support

Management support is critical during the implementation of security. The proper creation of an attitude throughout your organization that emphatically supports the implementation of security must be encouraged at the highest level. No security software will stop cooperative parties in strategic positions from violating the security software and procedures. Policies must be established that indicate the importance and level of security required for the particular environment. These policies must be communicated to all individuals who use the data processing facilities as part of their job function.

The security policy should address the following areas:

Objectives

The need for security in your environment.

Scope of security

What is to be protected (for example, data, data processing facilities, hardware).

Ownership of resources

Who owns the data processing resources (such as data, facilities, and hardware).

Responsibility for the integrity of the resources

Who is responsible to ensure that resources are being accessed, used, or modified in a secure manner.

Requirements to access the resources

Who needs access. Requirements might also specify those job functions authorized to determine when an individual requires access to a resource.

Statement of intent

How are violations logged and reported.

Accountability

Action to be taken when security is breached.

Account protection requirements

In password-based security systems, this protection could include change intervals, one account per employee, and account assignment for remote users. This approach assumes that:

- Access to data processing facilities and data is company property granted to the employee to perform a specific job function.
- Each employee is responsible for the use of his account.

Responsibility by functional area

What is expected of each functional area in the support and enforcement of the policy. Each user of the data processing facility must understand that he has a role to play in the security scheme and must understand what that role is.

Systems Software Security Policy

Identify those responsible to:

- Maintain the security software in a secure and responsible manner, ensuring that the data processing environment is always protected when it is available for use by the user community.
- Notify the appropriate parties if the security software is disabled
- Limit development and availability of facilities capable of bypassing security to only those situations in which they are absolutely necessary
- Work with the security administration function to ensure that system resources are properly protected
- Design the security requirements for the vendor-supplied system software for which they are responsible, and to work with the security administration area in implementing those requirements

Applications Software Security Policy

Applications areas must interface properly with the security areas to ensure that application resources are properly protected.

Consider assigning responsibilities to:

- Define the security requirements for the application, and to work with the security administration area in implementing security for the application
- Notify the appropriate security administrator of all revisions to the application that affect the security design

Auditor Function Security Policy

The auditors should be responsible for monitoring the effectiveness of the security procedures and controls. Consider assigning responsibilities to them to:

- Monitor all responsible areas to ensure that they adhere to the security policy
- Audit the use of all critical system and application resources
- Periodically monitor user activity
- Monitor the access requirements set by the security administration area

Operations Security Policy

The operations area is responsible for scheduling, controlling, running, and distributing the production processing. Consider assigning responsibilities to them to:

- Handle all responsibilities of production processing in a secure manner
- Access all resources only through the production facilities developed by the systems and applications software areas, and only for the purposes defined by those facilities

All Users Security Policy

General responsibilities can be assigned to all users regardless of functional area. Consider assigning responsibilities to the general users to:

- Keep confidential all accounts used to access data processing resources and facilities
- Revise the password to these accounts at regular intervals
- Notify the appropriate areas if abuse of an account is suspected
- Actively support all security procedures

Corporate Level Security Security Policy

A corporate level of globally acceptable security measures and procedures is the typical level of policy that is issued for general distribution to all users of the data processing facilities.

Application Level Security Policy

There are often applications that require additional measures above the level set by the corporate policy. Specific policies can be developed which detail the additional security requirements necessary for facilities such as accounts payable, human resources, or particularly sensitive facilities. These policies might be distributed to only the necessary functional areas.

Chapter 2: Security Administration Function

This section contains the following topics:

Where to House Security Administration

The security administration function can live anywhere within the organization. The best place is in a security administration area that reports directly to top management. This allows the function to handle its responsibilities without the compromises that can result from loyalties to the functional area which security administration is part of. It can also be advantageous to include all security functions, including physical security activities, within this area.

Many organizations cannot set up a separate security area. In this case, the security administration function should reside in an area where it will have the power to enforce security. This power should be granted and actively supported by the top management of the organization. The area should also have the manpower available to staff the function. Under these circumstances, the security administration function can live virtually anywhere within an organization.

The classic functional areas chosen to harbor the security function include:

Systems Software

Because it is very involved with the security software itself.

Database Management/Data Administration

Because requests for access to corporate data are usually made to this area.

Operations

Because it is responsible for all processing.

Auditing

Because it is responsible for ensuring proper access to resources in accordance to policy.

Centralization or Decentralization

After setting up the central security administration function, consider whether to centralize or decentralize the security function:

- Centralized security will:
  - Give concentrated control over changes in security and will possibly strengthen security enforcement.
  - Provide one point for security administration.
  - Make policies and procedures simpler to develop, enforce, and monitor.
  - Provide a higher level of security by limiting the number and distance of individuals authorized to change security definitions.
  - Allow for more flexible reporting.
  - Require fewer security staff members than would be required by a decentralized organization.
- But centralized security might:
  - Be less responsive to the user because of logical and physical distance from the user's environment.
  - Involve longer response times to react to maintenance requests.
  - Require a higher maintenance workload.
- Decentralized security will:
  - Allow more sensitivity to user requirements, since the administrator is more familiar with the resources being protected and with the users than is possible at the central level.
  - Allow faster response to maintenance requests.
  - Require a lower administration workload per administrator since security maintenance is delegated among several decentralized sites.
- But decentralized security might:
  - Require more complex policies and procedures.
  - Provide a lower level of security since the authority to modify security definitions are performed in many disassociated locations.
  - Require more time to implement.
  - Require additional overhead at the central level to monitor the activities of the decentralized administrators.

Many installations successfully use the central security administration approach and later decentralize the function wherever maintenance requirements make it practical. This allows the central level staff to become the security system experts before they are required to train and monitor administrators and staff on a decentralized level.

Set-up and Maintenance Dependencies

In any decision regarding who is to handle security administration, consider the amount of setup and maintenance activity required. This activity depends on:

- The number of corporate entities, such as departments, divisions, applications.
- The number of defined users, as well as employee turnover requirements.
- The number of data processing resources to be protected.
- The existence of standards; standards are discussed later in detail.
- The different kinds of facilities to be protected, and the extent of security required on each.
- The number of hardware entities to be protected. For example, if terminal protection is used heavily and regular network reconfiguration is a fact of life, security maintenance based on terminal ID revisions are heavy.
- The application development activity. If heavy development is being pursued, the security requirements for maintenance activity and security review activity must be considered for new and revised application segments.
- Auditing requirements and frequency of change to them.
- The number of special routines requiring user-defined resources, and the maintenance activity against them.

Chapter 3: Implementation Considerations

This section contains the following topics:

Introduction

Planning and scheduling the security implementation can help set proper direction and keep the implementation on course.

It might also require cooperation and contribution from the other affected areas in the organization. Many organizations create a security implementation project team with individuals from:

- Security Administration
- Systems Software
- Applications Software
- Operations
- Auditors
- End users

Develop a Security Policy

The initial assignment of the security implementation project team might be to develop and recommend the security policy and objectives. The team is an ideal committee to develop this document, because the concerns of each area can be taken into account.

If the security policy or document of security objectives has already been developed, the implementation team can use this document as its mandate.

Construct a Flexible Schedule

The implementation team should draft a flexible schedule. If at all possible, avoid setting a final implementation date until the inventory and design phases are completed. Plan to take care of the emergency requirements first and then phase in the remainder of the organization.

It is not as important to put timeframes on each phase of the implementation plan as it is to be certain that the implementation attends to all requirements.

Create a task list showing all tasks that must be accomplished to implement security at your site. This allows you to determine which tasks must be done as part of a step-by-step procedure, and which are independent.

Chapter 4: Planning Emergency Procedures

This section contains the following topics:

Security File Backup

CA Top Secret has an automatic backup feature that is set to copy the Security File to a DASD backup at 1:00 a.m. daily. This Backup File is critical to the built-in recovery capability. You can change the time of backup or deactivate the automatic backup through the BACKUP control option. A backup can be taken at any time from the console using the BACKUP modify command.

CA Top Secret also includes a recovery mechanism based on the DASD backup and the Recovery File. This procedure should be installed and tested before serious security maintenance begins so that all Security File updates can be recovered.

Off Site Storage

All of the CA Top Secret files should be backed up to tape or cartridge daily for off site storage:

- Security File
- Security File Backup
- Recovery File
- Audit/Tracking File
- CPF Recovery File
- Parameter File

CA recommends that the Security File reside on a different volume and string than that of the Backup and Recovery Files. This allows you to use the Backup and Recovery files to quickly and easily circumvent minor hardware problems which affect access to the Security File.

Emergency ACIDs

Establish procedures for emergency ACIDs when production problems occur that require the assistance of the systems or applications programmers when the security staff is unavailable.

The operators can assign an emergency ACID to the abending job which allows the job to process and records the access activity of the job.

There are two approaches you can use to design emergency ACID procedures:

- Create an emergency ACID with authority to access production resources. All production resources are permitted to this ACID. When defining an emergency ACID in this manner:
  - Audit this ACID at all times, so that your report shows when it is used and what the emergency ACID is accessing.
  - Do not use any of the security bypass attributes when creating the emergency ACID as an easy way of defining access to all production resources.
  - In an emergency, you can use a modified BYPASS(jobname).
  - The security bypass attributes turn off auditing for the resource class selected for that ACID.
- Create an emergency ACID in WARN mode with limited authority to access production resources. Only globally available production resources not defined in the ALL record should be permitted to this ACID. This includes resources such as production load libraries or global production programs. When using an emergency ACID in this manner only the violations are recorded.

Multiple Super ACIDs

You can define a series of emergency ACIDs, possibly by production application, or you can define just one for all production emergencies. The more precisely you define your emergency ACIDs, the easier it is to monitor the abnormal, audited, or violation activity.

- Clearly define and explain all appropriate emergency ACIDs to your operations staff so that they are prepared for any production emergency.
- Restrict the use of these ACIDs to off-hours through date and time controls. This discourages misuse of the emergency ACIDs for non-emergency situations.
- Monitor the emergency ACID reports to determine whether the use of the ACID is legitimate.
- Research the cause of the unexpected violation to ascertain that it was not a deliberate attempt by someone outside of the operations area to bypass CA Top Secret. This is possible if the use of production emergency ACIDs is common knowledge.
- Operations staff should be responsible for the use of these ACIDs and should be held accountable for their misuse.
- Do not allow a user who is disgruntled or near termination to use an emergency ACID.

Software Problems

Loss of CA Top Secret files or major operating system errors can cause system failure. CA Top Secret protects itself from attack, and will, if necessary, disable the operating system before allowing unauthorized security bypasses to occur.

The following points may be useful in such a situation:

- CA Top Secret has secure means of bypassing selected parts of, or the entire, security system. Be familiar with them and test their operation occasionally. Be aware of the behavior the various facilities will show when bypasses are in effect and be prepared for them. For example, when being bypassed TSO signons revert to the use of the UADS password.
- CA Top Secret recovers all internal errors. Be sure that procedures exist for printing snap dumps taken by CA Top Secret and delivering this information to the proper systems areas in a timely fashion. A growing problem, such as a failing DASD controller assigned to the CA Top Secret files may go unnoticed because the dumps generated from CA Top Secret recovery are ignored.
- Most problems with CA Top Secret involve security authorizations not working in the manner expected. Have the *Troubleshooting Guide* available and a terminal present so that you can use CA Top Secret diagnostic tools when contacting customer support.
- If CA Top Secret has completely failed, a system IPL without CA Top Secret may be in order. IPL processes to accomplish this should be set up, but should only be known to a select group of trusted employees. If there is more than one CPU in your complex, this may be unnecessary if the unaffected CPU can be used to address the problem.
- Since any problem can occur off-hours, contact lists and phone numbers of your security personnel and for CA emergency support should be available.

Disaster Recovery

Modify your disaster recovery plan to include procedures to bring CA Top Secret to the disaster recovery site.

If your disaster recovery site permits you to install your own version of the operating system, plan to bring the CA Top Secret load library and files to the site. CA Top Secret should be brought up after IPL.

If the site provides you with an operating system, be sure that you can install CA Top Secret at that site as part of your disaster recovery operation.

Install the CA Top Secret version of the IBM module ICHSEC00 at your disaster recovery site if:

- You do not wish to include CA Top Secret in your disaster recovery plans
- Any part of your z/OS operating system is not using z/OS alwayscall logic
- Protection of some or all of your data sets is dependent on RACF bits

This allows z/OS to ignore the RACF bits so that your disaster recovery operation runs smoothly.

Chapter 5: Resource/User Inventory and Exposure Analysis

This section contains the following topics:

Introduction

A user and resource inventory and exposure analysis is often too large to be handled all at once. Address the analysis on a user group basis, targeting implementation a group at a time. It is often helpful to solicit the support of the various user groups in doing the inventory, since each group is the best source of information on the resources required for their own needs.

CA recommends that you address the inventory in manageable segments.You can further segment the effort by z/OS facility, since the nature of the resources differs among facilities.

Note: Be aware of the different resource types used in each facility and should carefully determine appropriate controls on each resource type.

Objectives of the Inventory

The inventory and exposure analysis should answer the following questions:

- Who are the users?
- What are the resources? Must they be classified?
- Who is responsible for the resources?
- Which users are accessing which resources?
- Which users must access which resources to accomplish their job function, and at which access level?
- Which operations and procedures leave critical resources exposed?

Prioritize Users, Resources, and Facilities

Prioritize the facilities to be protected, the users to be defined, and the resources to be protected. This allows you to implement security for the most critical facilities, users, and resources first. As each inventory phase is completed, input the results into your Security File design and implementation strategy before continuing with the next inventory phase.

Note that inventory information is dated. Since environments change and grow quickly, you might have to reanalyze the segment if you do not quickly implement the results of your research.

Organize Users into Groups

Group the users together by corporate entity and job function. This organization might have already been accomplished for you as part of z/OS subsystem assignment, such as the standard TSO, CICS, IMS or additional facility user tables. You might also have user and group USS assignments with security assignments to consider.

Take Inventory of Resources

Use existing automated records of resources that already exist in your site, such as:

- JCL libraries, VTOC listings, and SMF information for data sets and volumes
- Load library directories for programs
- CICS tables for CICS resources
- VTAM tables for available terminals
- USS file system directories
- USS user, group and security designations

Organize Resources

Detail each resource or set of resources as to:

- The type of resource
- Who owns or is responsible for the resource
- Where the resource is recorded
- The purpose of the resource

CA Top Secret supports data set masking as well as full resource prefixing, so you might not have to detail each resource specifically if you can easily detail a resource group by masking or prefixing.

Assign Access Levels to Users/Resources

After you have decided which resources are candidates for protection, assign these resources to the appropriate user group at the appropriate access level. This information is specific input to resource ownership decisions and design of profiles.

Record Assignments Online

Recording your inventory results in an automated fashion, possibly using an online editor such as TSO/ISPF, might serve you in later converting this information into the required TSS commands. It saves time to record the results of your inventory in TSS command format. The results are easily revised for last-minute adjustments and can be directly input to the batch TMP to update the CA Top Secret Security File. It is important that this inventory be carefully restricted to avoid security pilferage or tampering.

Chapter 6: Developing Procedures and Standards

This section contains the following topics:

About Naming Standards

If your organization has successfully designed and enforced standards prior to the security implementation, you are able to use CA Top Secret's resource prefixing or masking capabilities to define resources.

If you are implementing security in an organization that has not enforced standards you will have to create more resource definitions or alter your current naming standards.

Resource Naming Standards

You can design or enforce the standards when:

- The resource/user inventory has been completed
- You have a good feel for what resources the organization owns and who is responsible for them

CA Top Secret can allow users to read or update resources that currently exist, and which do not follow the standard, but not allow users to create resources that do not follow the standard.

User Naming Standards

CA Top Secret (without customization) uses a user ID of eight characters because the ACID is restricted to eight characters. Use one user ID (ACID) across facilities, so that a single identifier can identify a user no matter which facility they are using.

Common Naming Standards

Some theories on the development of user IDs are:

Unique User IDs

Each user is assigned a unique ACID to establish accountability for the use of the ACID. This lets you trace violations and audited events back to the correct individual.

CA recommends that this ACID not be reused when the user transfers to another department or terminates employment. This allows you to trace the events associated with this user historically.

Static User IDs

The user ID can remain unchanged for the user's full term of employment, even if the user transfers to a different department. The type of ACID usually chosen to follow this theory is a unique ACID which identifies the employee, such as employee name or number.

Dynamic User IDs

An ACID which identifies the department or location of the user by ACID prefix and identifies the user with a unique ACID suffix. This ACID is changed when the user transfers to another department, because the prefix of the ACID determines the department and the general responsibilities of the user. This type of ACID allows security administrators and even computer operators to quickly determine when, for example, a user outside of the Payroll Department is attempting to access a payroll resource.

Secret IDs

A common theory is to obscure the user ID so that it cannot be easily guessed by an interested third party. While this can be an effective measure to deter unauthorized users from getting into unauthorized accounts, it can be very difficult to administer, since it is just as difficult for the administrator to determine the owner of the ACID without listing the ACID from the CA Top Secret Security File. This can make auditing and violation monitoring more difficult. Although this is an often-used and viable approach, it might be better to depend on strong password controls and possibly user authentication devices to deter unauthorized access to accounts without obscuring the user ID.

Determine your approach before you begin to build your Security File and define your users.

Security File Standards

CA Top Secret uses ACIDs to define the functional entities within the Security File. The ACID names used in the file should also follow a standard, to simplify maintenance and to allow the definitions to be readily located for research and analysis. For example, you should be able to determine by the ACID name if the ACID is a user, a profile, a department, a division, a zone, or a CA Top Secret security administrator.

Procedures for Handling Violations

A pattern of unauthorized access attempts by a user (or group of users) could indicate that these users are looking for a loophole in your security definitions. If they find the loophole, this will not show up as a violation. Therefore, a pattern of attempts might indicate a potential breach of security and should not be ignored or taken casually.

If employees sense that no one is monitoring violation attempts, they might be encouraged to try to access resources that they should not.

To handle excessive violations:

- Carefully monitor your regular violation reports to determine patterns of excessive violations by specific users or groups of users
- If you identify suspicious users or groups of users, consider doing further research on access patterns by auditing the suspected ACIDs
- Use TSSUTIL to produce regular reports on these users, showing violations and all audited activity
- Use TSSTRACK to monitor the suspected users as they are working, and later produce reports on your observations
- If the attempts are made against a specific set of resources, consult with the owner of the resources to determine the sensitivity of this information
- If you feel that these patterns should be formally reviewed, meet with the user to determine the cause of the access activity
- If the activity was malicious or destructive in nature enforce an agreed upon action
- Continue to monitor the user's activity

Security Maintenance Procedures

Maintenance takes the form of updates to the CA Top Secret Security File, as well as maintenance to the CA Top Secret software itself. It is important that your maintenance procedures are in place before receiving the first request.

If you have chosen a gradual approach to security implementation (implementing functional areas and facilities one at a time), maintenance will become a requirement before the implementation is completed.

CA Top Secret Security File Maintenance

As your environment changes you are required to revise your security definitions to reflect these changes. Determine that the changes to security definitions are both necessary and legitimate. Have a CA Top Secret Security File maintenance procedure which lets you ensure that the requested revisions are correct and authorized.

Change Request Verification

If the organization is small, and the security administration staff can easily identify and control all users and resources, then the central administrators might be able to verify the requests for changes.

If the organization is large, it is difficult for the central staff to know all users and resources. They will have to depend on other individuals to verify change requests. In large organizations, or even in small ones, it is recommended that the representatives of the functional area that owns the resource(s) be responsible for verifying the necessity and accuracy of change requests. Requests should be made in writing with the proper authorization.

Many installations design security maintenance request forms that are completed by the appropriate functional area and are approved by the appropriate functional authority. The forms are submitted to the appropriate administrator for revision of the Security File. The forms are then filed as a permanent record of the request. These forms should contain all of the information necessary for the revision, including effective date, resource name and level of access required, user or profile name, and expiration date if the request is for temporary access.

Be sure that your maintenance activity follows your original Security File design. Be careful that your profile structure is not compromised by numerous requests for update to user ACID records. Review each request to ensure that the request falls in the appropriate place in the Security File. It is possible that the requestor is unfamiliar with the structure and has requested an update for an inappropriate ACID. You might have to review the request with the requestor and modify the request before the update is actually made to the Security File.

Procedures for Quick Turnaround

Your CA Top Secret Security File maintenance procedure should be designed for quick response. If quick response is not practical, then the turnaround time for requests should be communicated and understood by all user areas so that they can effectively plan for timely Security File revisions. Emergency procedures should be available for immediate response when required.

The ability of a central security administration staff to respond quickly to maintenance requests can determine whether you choose to decentralize CA Top Secret security maintenance. If certain areas require more timely response than is possible at the central level, you might choose to decentralize maintenance for those areas.

z/OS Security Interface

CA Top Secret works through the z/OS Standard Security Interface and is rarely impacted by z/OS maintenance. If you receive early releases or special releases of z/OS maintenance which revise these interfaces, take care in applying and testing this maintenance with CA Top Secret. Testing procedures for operating system software changes and upgrades should always include a verification of basic security system functions as part of the plan.

Ensure that maintenance to interfaces of other vendor products still function properly with CA Top Secret.

Develop Testing Procedures

Initial testing and testing after revision are important tasks in ensuring that the software is functioning as required. Develop test plans for CA Top Secret that you can use throughout implementation and whenever CA Top Secret maintenance is applied. Test the significant interfaces whenever vendor maintenance is applied.

All accesses to a particular resource are handled in the same manner. To CA Top Secret there is no difference between data set access through batch and data set access through TSO (other than facility limitations). All checks are done out of the standard interfaces that are part of the z/OS operating system and its access methods.

Check all access to resource combinations. Once tested in one environment, it is not necessary to check other environments that use the same resources. An exception is different environments run in different modes.

An effective test plan has:

- Batch jobs accessing programs, data sets, and combinations of access characteristics that are appropriate to the controls in your organization. There should be a set of jobs that always fail, with documentation describing the expected failures in the JCL, and another series that must successfully execute.
- Application simulating procedures for special applications (such as CICS) which attempt access to all resource types used in your organization. Functions should be set up to fail for documented reasons, and others must succeed.

The processes should be run by both normal users, administrative ACIDs, and undefined users to cover all possibilities.

By segregating the tests into resource types (for example, TSO/Batch versus CICS versus IMS), useful tests are available to quickly and effectively evaluate specific system changes such as a new release of CICS, or a newly installed CA Top Secret interface to an existing IMS region.

Save the test results for comparison with those saved from prior tests and for comparisons with the next series of tests, in case there is any question of correct system performance.

Chapter 7: Designing a Security File

This section contains the following topics:

General Guidelines

When designing the Security File.

- Keep the file structure simple. The structure can follow your organization's functional areas of responsibility.
- Standardize the Security File names
- Use a consistent approach and style.

Department, Division, and Zone ACIDs

The CA Top Secret departments, divisions, and zones give you:

- A reference point to establish ownership based on corporate responsibility
- A logical grouping of users based on their position within the organization

Even if you initially choose to centralize security, you are able to easily respond to decentralization requirements when they arise for administration, auditing, or reporting purposes.

Note: Division and zone grouping is optional.

Organization ACIDs Provide Structure

It is not necessary to have a one-to-one relationship between the zones, divisions, and departments in your organization and CA Top Secret zones, divisions, and departments. These organizational ACIDs are provided to form structure and scope within your file. Think of these ACIDs as providing levels of control.

In a large sales-oriented company, CA Top Secret zones might be used to differentiate the Research and Marketing Divisions in the East coast office from the same divisions in the West coast office. In a service company, CA Top Secret divisions might represent client companies. In a small organization, CA Top Secret divisions might represent corporate departments and CA Top Secret departments might represent units within each department.

Resource Ownership

Plan to define ownership of resources to the selected department, division, or zone. Ownership should be defined at this level because:

- Ownership of resources at the user or profile level equates to default access levels that cannot be overridden. Therefore, fine-tuning of access requirements for a specific resource cannot be done for the user or profile that owns the resource. Ownership at the department, division, or zone level does not equate to any default access for the users defined within that department, division, or zone.
- If ownership is defined at the user level, ownership must be transferred to another ACID if the user terminates. This can become a maintenance problem.

Define Resource Ownership

Ownership of a user's own scratch pad data sets (for example, TSO user ID data sets) is a situation where it might be useful to define ownership at the user level. This approach can help to enforce cleanup of work data sets as well as CA Top Secret Security File definitions when an employee terminates. Ownership of a user's personal data sets can still be defined at the department, division, or zone level if desired.

Ownership at the profile level is not recommended.

There are special cases when CA recommends that ownership be defined to the MSCA. These cases include ownership of MODEs and ownership of prefixes which include masking characters.

When establishing ownership of resources, plan to define ownership at as high a level (as short a prefix) as possible. For example, for data sets, try to define ownership by the high level prefix; for programs, by program prefix. This simplifies and reduces the number of required CA Top Secret ownership definitions.

For the data set name SFT1.MASTER.FILE, assign ownership of SFT1. not of the full data set name.

Profile ACIDs

Profile ACIDs are used to group together access requirements that are common to more than one user. The most common use of profiles is to define job position requirements in access definitions. These requirements can be defined in one profile or in a series of related profiles. Use the results of your resource inventory that detail which users require access to which groups of resources as input to your profile design.

You can design your profiles:

- With all users assigned to a department are attached to profiles which are attached to that same department. Profiles must be attached to departments. For example, the Application Department requires access to system resources. PROFILEX, attached to the Application Department, contains the access requirements for the system resources. To allow all Application Department users to access system resources, attach PROFILEX to the user ACID of each user via a TSS ADDTO or CREATE command.
- With the profiles attached to a department define access to resources that are owned within that department. Users in any department who require access to these resources can then be attached to these profiles. For example, PROFILEZ, which is attached to the Systems Department, contains the access requirements for the system resources used by the Application Department users. To allow Application Department users to access the systems resources, attach them to PROFILEZ via an ADDTO or CREATE command.

Department/Division and Department/Zone Level Profiles

Design department and division (optional) level profiles for each user. Even if you initially do not have department or division level requirements, attach these profiles to your users as the users are created and are associated with specific departments. When later requirements surface that affect users on the department or division level, you can fulfill these requirements by updating the appropriate department or division level profile.

Profiles cannot be attached to divisions or zones. To effect higher level profiles, for instance, create a divisional department to which no users are attached, and create your divisional profile within this department.

Profiles by Facility

Profiles can be defined so requirements for a given facility are defined within the profile. TSO and batch requirements, for example, can be defined in one profile while CICS requirements are defined in another profile.

Profiles by Application

The payroll CICS system requirements, for example, can be defined in one profile and the personnel CICS system requirements can be defined in another. A user requiring access to both payroll and personnel applications can be attached to both profiles.

Profiles by Job Description

You can choose to use a single profile per job description.

A payroll clerk's job will always be defined by PROFILEP while the payroll manager's job is defined by PROFILEM. Although the payroll clerk and the payroll manager might share common access requirements, they will nonetheless have individual profiles. This approach makes it very simple to determine the access requirements for a new user assuming the job of payroll clerk or payroll manager.

Note: Profiles are recommended even if the job description profile is only applicable to one user. When a new user assumes that job position, you can simply attach the profile or series of profiles to the new user, eliminating the need to redefine all of the required access definitions for that user.

Number of Profiles

The number of profiles you can attach to each user is limited to 254. CA recommends that you limit the number of profiles attached to each user as much as possible. You should not require more than five or six profiles per user.

Override Strategy

If you use the default options of the AUTH control option, you can use override strategy in designing your profiles.

PROFILEA can be defined to allow READ access to system data sets. PROFILEB can be defined to allow UPDATE access only to a critical subset of data sets defined by PROFILEA. A user attached to PROFILEB and PROFILEA, in the following order, will have UPDATE access to the critical data sets, and READ access to the remaining data sets where the access has not been overridden by PROFILEB. Additionally, other users who only require READ access to system data sets can simply be attached to PROFILEA.

Record All Universal Access Requirements

The ALL record is used to record all access requirements which are effective for all users, both defined and undefined, to CA Top Secret. The ALL record is a powerful implementation tool which lets you protect and define resources, but still allows undefined users to access those resources at a specific level as defined to the ALL record.

Your Security File design for FAIL mode, when all users are defined to CA Top Secret, should indicate limited use of the ALL record. Only truly global requirements should be defined to the ALL record. For example, use of the corporate phone number application or electronic mail system might legitimately be defined in the ALL record.

User Definition

The results of the user inventory are input to the creation of users. Departments to define users into and the existence of profiles to define access requirements for the users simplifies the actual definition of users to CA Top Secret.

ACID Description

The NAME field allows for a 32-character description of the ACID. If this is not enough space for a meaningful description, develop a Security File dictionary that details each ACID by name, its purpose, and the nature of its use.

The installation data (INSTDATA) field can be used for auxiliary security information.

To store specialized information about your users beyond the 32-character limit, add descriptive fields and segments to your ACID structure through the CA Top Secret Field Descriptor Table (FDT).

Security File Organization View

Use TSSCHART to document your Security File design. It flowcharts the organization of your Security File at any level, and indicates the levels at which resource ownership is defined.

Chapter 8: Refining the Security Administration Structure

This section contains the following topics:

Who Administrates Security?

A central individual should be responsible for CA Top Secret Security File creation and maintenance. The corporate security administrator does not have to be the same person as the CA Top Secret security administrator. This is most often true in large organizations where the security administration function is handled by a security administration group headed by a security officer. In this type of situation, the CA Top Secret administration might be handled by security analysts or, if the Security File is well defined and simple to maintain, by security administration clerks.

The MSCA's ACID and Password

Keep the MSCA's ACID and password confidential and locked in a safe place so that they can be retrieved in an emergency. The MSCA account should not be used for routine CA Top Secret maintenance. It should be used only when required. For example, to create SCAs or LSCAs.

Suspension of MSCA

By default, the MSCA account cannot be suspended because, if all else fails, the MSCA account can be used to handle maintenance, control option requirements, or emergency procedures. To make the MSCA account suspendable because you fear potential sabotage through password guessing from an outside source, use the MSUSPEND control option.

Additional Central Security Administrators

At least one SCA should be created as the ACID used to perform routine maintenance. There is no limit to the additional SCAs or LSCAs that you can create as required by your organization. The scope of an SCA is all users and resources defined within the CA Top Secret Security File. The scope of an LSCA, which is essentially a limited SCA, is determined by the MSCA and can include other LSCAs. This characteristic might make an LSCA more useful in a security environment that is decentralized or a mixture of centralized and decentralized.

Suggested SCA Authorities

An SCA is not required to have full administrative authority. Tailor your use of SCAs to conform to the requirements of your organization. When planning your use of SCAs:

- Additional SCAs might be required to perform routine maintenance. Especially if you have centralized security maintenance and have heavy maintenance requirements.
- SCAs can be created with auditing capabilities to allow the auditing staff to monitor the implementation and maintenance of CA Top Secret.
- Special purpose SCAs can be created with reduced authority to handle specific environmental requirements. For example, some organizations create an SCA with the authority to only suspend and unsuspend users. This ACID is assigned to an operator with appropriate procedures for unsuspending ACIDs which have been accidentally suspended.

The LSCA Option

The administrative authority of an LSCA can be tailored by the MSCA. The LSCA's scope is subject to modification and need not extend to all CA Top Secret defined users and resources.

Example: LCSA option

In this example:

- LSCA02 has authority over ZONE01 and ZONE02
- LSCA03 has authority over ZONE03 and ZONE04
- LSCA01 has full administrative authority over LSCA02 and LSCA03

This allows LSCA02 and LSCA03 to “function” as SCAs for their respective zones and yet subjects them to the administrative authority of LSCA01.

Decentralized Security Administrators

Decentralized security is set up through zonal (ZCAs), divisional (VCAs), and departmental (DCAs) security administrators. It is not necessary to define an administrator for every department. Decentralized administrators can be defined selectively as required.

One of the advantages to designing and implementing a Security File structure is that decentralized administrators can be assigned wherever and whenever it is appropriate. As long as your structure is well designed and ownership has been assigned along appropriate lines of corporate responsibility, creating a DCA, VCA, or a ZCA at the selected level effectively decentralizes CA Top Secret security administration.

ZCA, VCA, or DCA Considerations

Consider the following when planning to decentralize CA Top Secret security administration:

- ZCAs, VCAs, and DCAs are most often created to perform routine maintenance.
- Temporary or permanent ZCAs, VCAs, and DCAs can be created with auditing capabilities which allow the auditing staff to perform routine or periodic audits on corporate zones, divisions, and departments.
- As with SCAs and LSCAs, special purpose ZCAs, VCAs, or DCAs can be created with reduced authority to handle specific environmental requirements.
- You can choose to assign administrative authorities to user ACIDs. For example, you might wish to allow a user to permit access to the resources that he owns to other users.

Decentralize administration only when and where it is necessary. Valid reasons for decentralization include heavy maintenance activity at the central level and remote user sites which require more responsive administration than can be provided at the central level. Selective decentralization where appropriate can be the most effective way of decentralizing administration.

Monitor Decentralization via TSSAUDIT

If you decentralize, CA recommends that you put the appropriate manual and automated controls in place to monitor the decentralized activity. Use the CHANGES function of TSSAUDIT to regularly monitor all changes made to the Security File by administrators.

Chapter 9: Developing Security Awareness Programs

This section contains the following topics:

About Security Awareness Programs

Security implementation is best handled as a psychological implementation as well as a technical one. The proper psychological environment for security must be created along with the technical procedures. Without the active support of all involved areas, security in an installation can be at best ignored and at worst tampered with.

Awareness Program Goals

The major goals of a security awareness program are:

Cooperation

It is more effective if every individual in your organization monitors the security program in their own area, than if the security administration area or security project team is solely responsible for this activity. You also have a better chance of a solid security implementation if the entire organization is behind it. There are a number of functional areas involved in the use of the security product, and it is an important step to create willing users of the product. The functional areas include:

Systems software area

This is the area most likely to consider breaking or bypassing the security system a challenge. They are often opposed to the security system because they fear that it will get in the way of doing their job. Cooperation should be cultivated in this area because maintenance will probably be the responsibility of this area and this group often uses facilities capable of bypassing security.

Applications area

These individuals develop the business software required within the corporate environment. As part of their function, they are required to access only those resources making up their application and some globally accessible system resources. CA Top Secret provides an applications interface that allows the applications areas to use the security system to provide additional application security needs. This gives the applications area a tool to simplify design wherever additional security is required. This also gives the security administration area the opportunity to eliminate the homegrown application security systems and to centralize all security requirements, as well as to standardize security administration.

Each application design should be evaluated for effective protection. Involve the affected application area in the security definition process.

Operations

Operations can easily view security as just another headache that can get in the way of completing production.

Production security must be carefully designed and tested to avoid security abends. If security abends occur, the operations area must have procedures available that will allow them to get production through with minimal delay. Operations staff can be the most seriously impacted by CA Top Secret. Ensure that production runs with the proper protection but without being impacted by the security implementation.

Auditors

In addition to requesting their input on the security design, set up procedures for the auditing staff which allow them to take advantage of the auditing features provided in CA Top Secret. These procedures should be developed early in the security design phase to allow the auditors to monitor activity as the implementation progresses.

End users

This group is the most dependent on the facilities provided by the applications and systems areas to perform their specific job function. The end users will support the use of security, but not if it becomes something that prevents them from simply doing their job. Security for this group should be defined so that it is as transparent as possible.

Education

Individual training programs can be developed for each functional area, or training can be organized by subject. The training should be repeatable so that it can be presented to new users at regular intervals.

The most significant point to be made as part of the education process is that security does not hurt and can in many cases improve the effective use of data processing resources in your organization.

Communication

For the security policy, or document of security objectives, to be understood and accepted within the organization, it must be effectively communicated to all users. It is recommended that you use a combination of the following methods of communication:

Global Distribution

Distribute the physical document to all users. The document could be included with your organization's personnel policies and procedures manual.

Formal Presentations

Formally present the security objectives to all users. This could be included with CA Top Secret training.

Performance Review

Include adherence to security policy in the job performance review checklist. Make clear to each user the position the organization takes on security issues and the responsibilities of each user toward the security program.

Security Seminars

Many organizations develop security awareness seminars where they present the necessity for security, what the organization is doing about security, and what the user is expected to do about security. These seminars are usually quite effective in communicating the corporate attitude toward security.

Security Films

There are a number of good security awareness films available for purchase or rental for security seminars. Contact your CA Top Secret user groups or security organizations for information.

Subject Matter

Some of the subjects that should be addressed and the intended audiences are:

Systems Software Personnel

CA Top Secret installation and information on how it interfaces with the operating system.

Systems Software and Application Development Personnel

Information on how CA Top Secret can be used to assist in the design of new or existing system and application facilities through the CA Top Secret Application Interface.

Auditors or Any Auditing Area

Information on how to use CA Top Secret to monitor the data processing environment without impacting the operation of the site.

Users

Information on ACID and password requirements, including:

- How often the password should be changed, and the procedure for revising it.
- Under what circumstances an ACID can be suspended, and what to do about it.
- What kind of violation messages they might encounter, and what action is required for each.
- The nature of the CA Top Secret Last Used Message and instructions on how to verify that the last use of their ACID was legitimate.

Chapter 10: Additional Considerations

This section contains the following topics:

Common Reasons for Customization

Customization is often used with:

Facility Interfaces

Standard IBM macros are often used to interface CA Top Secret with a facility that is currently not supported by CA.

CA Top Secret is SAF-compatible at the IBM RACF macro level. It is upward compatible with interfaces developed using the standard IBM RACF macros.

Customization that is not based on the use of these macros or CA Top Secret supplied interfaces might require rewriting, or might become totally unusable in subsequent releases of CA Top Secret.

CA Top Secret Installation Exit

The installation exit provides initiation, validation, logging, message, CA Top Secret Security File change, and other exit points for user routines. The exit has been used to:

- Translate messages into different languages
- Keep multiple CA Top Secret Security Files in synchronization across CPUs
- Provide interfaces for second level authentication devices
- Log additional information to SMF or to the Audit/Tracking File

Customization using the installation exit is not limited to the examples detailed. CA recommends that the installation exit not be used to bypass security or to change CA Top Secret behavior to behavior that does not complement documented CA Top Secret features.

CA Top Secret Application Interface

Customization is used to modify system or application programs to call CA Top Secret through the CA Top Secret Application Interface for specialized security checking. Use of the interface does not change CA Top Secret behavior. It lets you perform additional security checks for user-defined requirements.

Use the Application Interface to:

- Eliminate in-house application security systems in online systems (such as CICS or IMS)
- Provide further levels of security beyond file level protection
- Control access to online functions within online applications
- Control use of job class and accounting information

Conversions from Other Security Software

CA Top Secret can live concurrently with many of the controls used by other security products.

The objective is to replace your existing security software with CA Top Secret while minimizing the impact on your environment and your user community. Depending on the security product currently installed, certain CA Top Secret capabilities can be activated. Regardless of the security product in place, you can build the CA Top Secret Security File completely without obstructing the security mechanisms of your current security software.

Although systems programming support is necessary to uninstall your existing security software, systems programming support or modifications are typically unnecessary to convert to CA Top Secret.

The scope of this task depends on how thoroughly you have implemented your existing security product and the size and complexity of your organization.

Ongoing Evaluation

Even after your CA Top Secret security implementation has been completed, do not stop monitoring and evaluating the effectiveness of the implementation. Your implementation of CA Top Secret must be as dynamic as your environment.

Index

S

T

U

W

Z