E-SRF

**EKC Security
Reporting Facility**

General Information

EKC Inc.
10400 West Higgins Road
Rosemont, Illinois 60018
www.ekcinc.com

(847) 296-8010

E-SRF™ is a proprietary product
developed and maintained by

EKC Inc.
10400 West Higgins Road
Rosemont, Illinois 60018
USA

 (847) 296-8010

Technical Support:
(847) 296-8035

Table of Contents

E-SRF General Information Guide   v

E-SRF Publications

Name	Contents
Installation Guide	E-SRF installation including: installation and maintenance steps, startup and shutdown considerations, and backup and recovery procedures.
Change Summary Guide	Contains all new features and system function changes.
General Information	An overview of E-SRF and its components.
Resource Grouping Facility Guide	Brief overview of the Resource Grouping Facility, its relationship to E-SRF, language command syntax, TSO commands and JCL.
Access Analysis Introduction	An overview of the Access Analysis component.
Access Analysis Reports Guide for ACF2	Brief overview of Access Analysis reports for ACF2 systems, explanation of the DataOwner and LogonidOwner reports, command syntax, utilities necessary for creating input to reports, and JCL.
Access Analysis Reports Guide for RACF	Brief overview of Access Analysis reports for RACF systems, explanation of the DataOwner and UseridOwner reports, command syntax, utilities necessary for creating input to reports, and JCL.
Event Reporting User Guide	A "How To" guide for users of E-SRF Event Reporting.
Event Reporting Facility - Command Reference	Explains the Event Reporting Facility command processor, command syntax, and JCL.
Event Reporting Facility - Masterfile and Data Dictionary Reference	Explains the structure of the E-SRF Masterfile and describes all Masterfile fields.
Event Reporting Facility - Messages and Codes	Lists Event Reporting Facility messages and codes.
Event Reporting Facility - Report Overlays Guide	An overview of the report overlays provided with the Event Reporting Facility.

Trademarks

IBM	is a trademark of the International Business Machines Corporation.
MVS/ESA™	is a trademark of the International Business Machines Corporation.
MVS/XA™	is a trademark of the International Business Machines Corporation.
RACF™	is a trademark of the International Business Machines Corporation.
CA-ACF2™	is a trademark of the Computer Associates International, Inc.
CA-TopSecret™	is a trademark of the Computer Associates International, Inc.

E-SRF Genera formation Guide

Introduction

This document is intended to answer basic questions of what E-SRF is, what it does, and why it would be beneficial in your CA-ACF2 and/or IBM-RACF security environment. There are a number of documents that address how E-SRF does it, but the whats and whys are spread throughout them. Here we will gather some of those thoughts and answer some of the more basic questions.

The anticipated audience is IT managers, internal auditors, risk managers and others who are looking for an understanding of what E-SRF can do for their organization; how it can assist with their daily security reporting, and with their compliance needs.

The EKC Security Reporting Facility (E-SRF) is a comprehensive security analysis and event reporting tool and provides for installation-customized reporting with Resource Grouping. This full spectrum of reporting addresses the primary needs of Risk Managers and Security Analysts when it comes to knowing what is going on and what could go on in their environment, as well as notifying the manager-owners of data and users.

EKC constantly strives to improve its products and add functionality from year to year. To this end, E-SRF has added several minor tools to make life easier for security professionals. Two such enhancements are detailed in this document. The Security Signature Analysis tool finds security programs and exits that may be long forgotten or misplaced. The CKC Analysis Collector helps to identify all of your CICS transactions for inclusion in Access Analysis reporting.

More add-ons will follow as you, the customer, tell us what would help the most. At EKC, customer feedback is very important - it drives tomorrow's products and shows us where we can improve our current offerings. Our mission is to provide the best products and services for the information security community.

Please feel free to contact us regarding your information security needs: reporting, role-based security implementations, or simply keeping your resident security system operating at its best.

Visit us on the Web at: http://www.ekcinc.com
Technical Support: (847) 296-8035, or support@ekcinc.com
Questions/Sales Support: (847) 296-8010, or sales@ekcinc.com

Executive Summary

The long strides of information technology have been both a boon and a bane. They've enabled e-commerce, but also identity theft. They've given the corporate world incredibly simple access to financial information, and yet provided shadows for white-collar crime to hide in. Sarbanes-Oxley, HIPAA and similar legislation provide the impetus and the guidance to remove some of those hiding places and to better secure customer and employee data.

It is important for a company not only to be vigilant for instances of inappropriate access, but also to be pro-active in this regard and to be able to demonstrate the appropriateness of its computer security implementation. The EKC Security Reporting Facility (E-SRF) provides the necessary reports to help you with both the "before and after" of these aims.

Access Analysis reports examine your current IBM-RACF and/or CA-ACF2 security environment and shows you what **could** happen. People move from one position to another, and sometimes the access rights they accumulate are unintended. Sometimes mistakes are made in setting up a new hire's access rights. In both of these cases, the users with certain access may not even know that they have it. For data owners, it could cause problems from accidental disclosure to intentional sabotage. E-SRF's Access Analysis reports show who has access (and what kind of access) to data and other resources, so these potential problems can be taken care of before they become an event.

Security Event reports are used to report on recent logged events on a scheduled and/or ad-hoc basis. Event Reports tell you "what **has** happened" and are quite flexible. Its well-documented event database provides a wealth of resources to answer questions about what's happening in your environment. It can be set up to monitor general activity on a regular schedule, and you can delve into specific concerns more deeply. You may say "I already get violations reports from CA-ACF2. What do I need this for?" Event Reports provide the same information (and more) that you would find in the standard reports, but in a much easier to read and understand format. In addition, it allows you to put together a set of reports based on your own standards and

specific concerns, such as source of entry, excluding "clutter" loggings, and the like.

Resource Grouping is provided to identify which datasets and resources belong to which group. The dataset or resource names do not need to follow a standard naming convention to be included in the same group. Datasets and resources seldom have common names across the entire environment. The number of acquisitions and mergers taking place these days makes it difficult to keep up with naming conventions as the acquired company's information assets are integrated into your data center. Yet, there are instances where it would be helpful to group information. If this grouping cannot be accomplished using standard naming conventions, EKC Resource Grouping can help.

Companies have often developed their own distribution applications for the standard violation/logging reports that come with IBM-RACF or CA-ACF2. These applications, built to handle data/resource owner notification, can often be replaced by simple-to-maintain selection commands in E-SRF and entries grouped together using ESRF Resource Grouping rules. This decreases your dependence on legacy application expertise.

ESRF includes "minor" tools that expand its capabilities. EKC tries to provide a new utility each year. The Security Signature Analysis tool was added in 2005. SSA is designed to find security software modules in source, object, or load module libraries, based on specific "signatures" or groupings of code. With SSA, you can find exits or home-grown security implementations that have been "misplaced."

The most recent addition is a CICS transaction finder. It's pretty common for transactions to accumulate over the years and be forgotten as developers move on to other things. EKCCAC for ACF2 is a set of programs that read several portions of your CICS and CA-ACF2 environments and generate a list of all CICS transactions for inclusion in Access Analysis reporting.

Section 1 - E-SRF Access Analysis Reporting

E-SRF Access Analysis reporting is unique among security reporting software products. Reports examine your security implementation at a point in time, providing answers for data owners (Who has access to our data?) and for managers (What files does our staff have access to?).   These reports were originally designed to assist with security database maintenance issues – to identify and clean up unintended access - but with the advent of S-OX requirements, E-SRF Access Analysis reports have become an invaluable tool for auditing and compliance reporting.

Separate modules are provided for Access Analysis reporting on ACF2 and for RACF based security implementations. Both of these resident security systems (RSS) have their own ways of doing things, but all RSS applications have to protect access from users to resources. That is basic. In this section, we will discuss the common reports of Access Analysis and their distinctives.

There are four main common reports: two for Data "Owners" (those responsible for specific data and applications, such as payroll or an inventory database), and two for User "Owners" (those who manage staff whose user accounts may have access to those payroll or inventory data and applications).

Each of these owner types has two common reports: one for datasets and one for other resources. Data, while still a resource, is distinct from other resources in that it is the lifeblood of an IT environment, flowing through the other resources such as programs, transactions, and terminals. Both ACF2 and RACF are set up to handle datasets apart from other resources, because by its nature, data requires special treatment.

Access Analysis Reports

Data Owner / Dataset Report

The Data Owner / Dataset report, as its name implies, lists datasets belonging to a data owner, and shows which users have access to that data, and what type of access they have. The data can be selected by dataset high level qualifiers or by predefined grouping. Grouping will be discussed in a later section.

The report will include all USER or LOGON accounts that have any access to the datasets, whether it's for normal processing, for backup purposes, or because the account has attributes such as "READALL" or "Operator."

Data Owner / Resource Report

The Data Owner / Resource report could have been called the "resource owner resource report," in that it does not list datasets, only the "other" resources. Which users can execute which CICS or IMS transactions? Which users can get in using Remote Job Entry from another system? Which users can access the system through the internet or dialup connections?

This report can answer these questions, but be aware that in many cases the "Data Owner" is an IT manager responsible for those application or access environments. For instance, if the CICS transaction is a "debug type" that can listen in on data from other transactions, it's important for the access to be highly restricted.

Logonid (Userid) Owner / Dataset Report

The Logon ID (ACF2) or User ID (RACF) Owner / Dataset Report provides department managers with a view of what datasets their direct reports have access to. This is especially useful in limiting a department's accountability (thereby limiting risk to the organization) to a "need to do" basis.

Logonid (Userid) Owner / Resource Report

This report provides department managers with a view of which resources (such as CICS or IMS transactions) their direct reports can access.

All of the above common reports include information about what type of access is being permitted, whether the access is logged, if it is permitted by access rules or by a userid attribute such as Security, Auditor, Operator, Non-cancel or the like. Both summary and detailed reports are available, so in addition to the general audiences indicated by the report names, all of these reports would be of interest and use to an internal auditor, security manager, etc.

Resident Security System Specific Reports

Some Access Analysis reports are RSS Product specific. In the following paragraphs, we will identify and describe these product-specific reports.

RACF Data Owner / Open Edition / UNIX System Services Report

This report provides the data owners with an overview of which users can access their Open Edition files, and what types of access are allowed. This would apply, for example, to RACF secured logons via TSO or started task to UNIX from MVS environments using Open Edition services.

RACF Userid Differences Report

This report is an aid to grouping and/or role modeling. It reads exported output from the two Userid Owner reports – Dataset and Resource – and analyzes access patterns, groups together users with identical access permissions, and itemizes the changes that would be needed to make the access identical. This makes an excellent tool for developing RACF group profiles. It is also helpful to auditors or managers when looking for questionable additional access.

ACF2 System Differences Report

This report, for ACF2 secured systems, analyzes the differences between two versions of the ACF2 databases. As such, it can be used to show the effect of rule changes from one month to the next, or it can be used to show the effects of proposed rule changes. This report would be helpful to an auditor, for example, to ascertain that a proposed rule change doesn't result in inappropriate access.

ACF2 Database Differences Report

This report may sound similar to the one above, so let's clarify. The System Differences Report shows the <u>effect</u> of changes, while the Database Differences Report shows the changes themselves. With this report, changes to access or to rules will be listed, highlighting to a security manager or auditor the old and the new values. It may also prove useful in debugging a major change to the security definitions.

ACF2 Database Comparison Report

As if we weren't tongue-tied enough! Another similar sounding report, but this time, the databases are assumed to be as close as possible, such as synchronized databases on two systems. In the Database Comparison Report, differences between the two images of the security file sets are shown, along with timestamps for those changes, to highlight possible problems with synchronization links. The time stamps will also aid in determining how long the two images have been out of synch.

In General…

Both Access Analysis and Event reports can use E-SRF Resource Grouping to aid in data selection, report distribution, and report bundling, putting all of an owner's reports together. Resource Grouping will be discussed in Section 3.

All E-SRF report programs can export their results into a format suitable for loading into PC spreadsheets, SAS® procs, database programs and the like. This can be useful for reporting on multiple disparate platforms, modeling the effects of a data center consolidation, or just e-mailing notifications to appropriate parties.

Section 2 - E-SRF Event Reporting

E-SRF Event Reporting provides a much better way of reporting security events than what is available with the Resident Security System. All RSS systems – CA-ACF2, IBM-RACF, CA-TopSecret – provide a means of logging events. There are two basic reasons for an event being logged…

- Something didn't happen, but if it had, it would have been a problem, and
- Something did happen, and it's not necessarily a problem, but someone should know.

The first type we'll call "Violations", and the second is just "Loggings". The reasons that these events are logged is that someone should know, and E-SRF Event Reporting is a tool that lets people know better than anybody else's tool.

An important note is that unlike Access Analysis, Event Reporting does not distinguish between datasets and other resources (at least in naming of reports). They're all resources, and "dataset" is just another class of resource, like Source (e.g. VTAM LU) or CKC (CICS transaction).

E-SRF Event Reporting has both standard "Specific" reports and open-ended "ad-hoc" reports. In this section, we will concentrate on the specific reports because they are specific for a reason: they are the ones you will find most useful in day-to-day operations. There are a lot of specific reports, and we will not spend a lot of time on any one report unless its importance mandates it.

The first eight reports are "ranked" reports. These are summary reports that are listed from high occurrence to low, and, by default, are limited to the top 20 rankings. You can specify another depth if you wish, or remove the limit altogether.

The last three are summary reports, summarizing all violations and loggings. Unlike the Ranked reports, these reports are ordered by USERID, by resource, and by resource class respectively.

Ranked Report Overlays

Ranked Daily Resource Events Report (RDRE)

This report lists the top 20 resources offended, and may be used to count all events, allowed but logged events, or denied by Violations events. This report can help find problems such as a production dataset not having appropriate access specifications.

Ranked Daily User Events Report (RDUE)

This report lists the top 20 offending users - again by all, allowed, or denied counts. This report can help find inappropriate access attempts or insufficient authority for a user to do the job.

Ranked Security Loggings by Resource (RLR)

This report ranks the top 20 resources accessed and logged. It would include access by an account with the "Security" or "Special" attribute, or using a resource rule that specifies LOG. It could help in tuning your logging requirements in the resource ruleset. (e.g., if you're logging access to a dataset or CICS transaction that everybody uses, you're just cluttering up the logs.)

Ranked Security Violations by Resource (RVR)

This report ranks the top 20 resources where access was denied. It would include logon attempts (Source class) attempts to access datasets, etc. This report could help in identifying hacking attacks, or point out access that needs to be granted. (e.g., a new application is rolled out before security adds the rules.)

Ranked Security Loggings by User (RLU)

This report ranks the top 20 Users where resources are accessed and logged. It would include access using a resource rule that specifies LOG, or by an account with the "Security" or "Special" attribute. It could help in identifying users in need of training or insufficient authority for a user to do the job.

Ranked Security Violations by User (RVU)

This report ranks the top 20 Users where accesses to resources are denied. It would include logon attempts (Source class), dataset access attempts, etc., where the access was not allowed. Like the RLU report above, this report could help in identifying training opportunities or insufficient authority for a user to do the job.

Ranked Source Signon Errors (RSSE)

This report ranks the top 20 Entry points (Terminals) where signon errors occurred. It could include hacking attempts, logon misskeys, password problems, wrong time of day, etc.

Ranked User Signon Errors (RUSE)

This report ranks the top 20 USERIDs where signon errors occurred. It could include logon misskeys, password problems, wrong time of day, etc.

Non-Ranked Summaries

The remaining "Specific Report Overlays" list all loggings or violations in their report output, and rather than being ranked, they are ordered by their "by" fields, as in "by USERID".

Count of Violations/Loggings by USERID (UVLC)

This report lists all USERIDs where violations and/or loggings occurred, and summarizes the count of events. It is ordered by USERID, provides a count of each type of event, and for loggings, a count by reason for the log entry, such as specified in rule, or read-all privilege.

User Violations/Loggings by Resource (UVLR)

This report lists all Resources where violations and/or loggings occurred. It is ordered by Class of the resource and by resource name. It provides a count of each type of event, and for loggings, a reason for the log entry, such as specified in rule, non-cancel privilege, or by user exit.

Count of Violations/Loggings by Resource Class (VLCS)

This report lists a summary of resource classes (types) where violations and/or loggings occurred. It quickly (on one page) identifies anomalies such as over-use of the log specification in rules or problems with rules for a CICS region.

Ad-Hoc reporting – ESRFLIST

The full power of Event Reporting can be accessed using the ESRFLIST report overlay. In this report, you specify the fields you want to print, the conditions you want to examine, the order of the report, etcetera. The E-SRF command processor includes an easy yet powerful selection technique to simplify report setup. With almost 400 fields of event data to choose from, you can describe in an easy to read report format just about anything you ever wanted to know about your security environment and what's happening in it.

Formatting your output – CTLCHAR command and ESRFDXD

E-SRF reports can be formatted for mainframe printers, LAN or PC printers (ASCII), HTML pages, partitioned datasets and more. Alternatively, the ESRFDXD report overlay will format your report data for export to spreadsheet programs, databases, or report applications such as SAS® or Crystal Reports®.

Not to mention Grouping…

In addition to the above-mentioned distribution and formatting options, EKC Resource Grouping can be used to logically group both Access Analysis and Event reports, as well as automatically distribute Event reports, based on rules that identify data and user "owners". So let's talk about Grouping.

Section 3 – Additional Tools

Resource Grouping

Datasets and resources seldom have common names across an entire enterprise. Even if your organization follows naming conventions, the number of acquisitions and mergers taking place these days makes it difficult to keep up with those naming conventions as the acquired company's information assets are integrated into your data center. Yet, there are instances where it would be helpful to group information. If this grouping cannot be accomplished using those naming conventions, EKC Resource Grouping can help.

EKC Resource Grouping produces a rules-based database for use in selecting resources to be used in Access Analysis or Event reporting, as well as Event report distribution. Grouping is an option, not a requirement. You don't have to set up grouping schemes to run the product, but it will help in simplifying the processes and improving performance as you learn more about your security implementation.

Integral to Access Analysis reporting is its grouping of similar user and resource "profiles". As it analyzes the access permissions, it groups like accesses together. For instance, in the User-Owner Dataset Report, userids with identical access patterns are combined unless you specify otherwise. After a period of getting used to these "natural groupings," you will be better able to specify the grouping rules necessary to distribute reports.

Once you have the grouping database set up, Event report selection and distribution by group is an easy way to automate your periodic security reporting.

With EKC Resource Grouping, you specify group names for resources and the rules by which they are connected to that group. For ACF2 users, it's very similar to resource rule writing; just add a default group name for the key, and a group name for each rule line that you specify. For RACF users, you may want to get a quick start by using the group names and their owners as currently defined in your RACF database.

These may not give you a finished report distribution tree, but experience will help you refine the group definitions in the Resource Grouping database.

EKC Security Signature Analysis

As in all areas of life, clutter in an organization tends to happen over time. Many of the people that have contributed to that clutter have moved on to other opportunities years ago. Now you need to know, for instance, "What user exits are we still using?" or "Where is the source code for the exit?" The Security Signature Analysis tool is designed for that purpose. SSA works in a way similar to virus scanning software: it looks for some basic signatures of security software routines, and it finds them whether they are in load, object, or source format.

In addition to SSA's built-in catalog of security signatures, you can specify your own text to scan for. The simple-to-use command structure allows you to scan for signature bearing modules at three levels. A quick scan will identify all modules in the specified libraries that have at least one occurrence of a security signature. This helps identify which libraries to look at more closely. A "medium" scan will find each signature that it can at least once in a module. The medium level is useful in finding modules with a specific type of security signature. A full scan will find every occurrence of all signatures in a module. This last scan is more comprehensive, and when you get to this point, you probably want to find out where you need to make changes to the code.

CICS Transaction Locator

The CICS transaction locator is a tool for ACF2 Access Analysis reporting. Access Analysis for ACF2 has always printed reports on the rules governing resources such as CICS transactions. However, in many cases, the system administrator is not aware of all the transactions and the possible ways to have set security. For example:

- Transactions that are on the SAFELIST will always be unprotected by ACF2 even if rules are subsequently written.

- Transactions can also be added to the list using masks. For instance, C*** will allow all transactions starting with a C to be unprotected unless a follow-up transaction like CEDF is placed on the PROTLIST. In this case, all other transactions starting with C are unprotected.
- There may be a sense that some transactions are protected when, in fact, because of the use of the SAFELIST and masking - *a transaction may not have security at all*.

The CICS transaction locator uses logging information from your CICS systems to identify all transactions, whether covered by rules or not, and whether they are on the SAFELIST or PROTLIST. The output is formatted for the Access Analysis Resource reports so that all transactions are included in the "final analysis."

System Requirements for E-SRF

The current release of E-SRF is designed with the following Operating System (OS) and Resident Security System (RSS) software in mind.

- IBM z/OS 1.0 and above
- IBM OS/390 1.0 and above
- CA-ACF2 6.5 and above
- IBM-RACF 2.2 and above
- More will be coming in the future.

Contact EKC

For more information, please visit us on the web at
http://www.ekcinc.com/.

To talk to someone about our products, or if you have questions,
please give us a call or write to us.

EKC, Inc.
10400 W. Higgins
Suite 200
Rosemont, IL 60018
USA

Technical Support: (847) 296-8035, or support@ekcinc.com
Questions/Sales Support: (847) 296-8010, or sales@ekcinc.com