Datasheet

Fujitsu Software BS2000 SECOS V5.6

Security Control System

Reliable data protection is a key requirement for the use of systems in commercial data processing. Mission-critical data must be effectively protected against intentional and above all against negligent modification or destruction. SECOS is a software product that is designed to implement security solutions for BS2000 systems to meet all requirements, from simple concepts to complex, according to customer-specific security policies.

The security risks attending commercial data processing are manifold. They range from errors in the use and operation of IT-systems to premeditated computer crime. Possible consequences include the loss of data availability, integrity and confidentiality. It is therefore imperative to combat these risks and institute security measures to administer and monitor access rights, anticipate potential threats and counter them if they actually materialize.

The basic security functions in BS2000 and the SECOS product combine to offer comprehensive, scalable security options for BS2000 operation in interactive and batch operating modes, as well as for the POSIX environment and POSIX-based procedures and applications. The product is also supported by an extensive array of services, ranging from security analyses through turnkey SECOS solutions for BS2000 installations.

Given their security functions (in particular SECOS), BS2000 business servers can be successfully included in security audits and with it contribute to certification of the security management of a company.

Features and benefits

Main features	Benefits
Extended access control	
• Rules for passwords (limitation of lifecycle, minimum complexity) • Barricade and observe of user IDs/terminals (dependent on time, after n failed attempts) • Personal LOGON (additional authentication on common used user IDs) • Assignment of an access class for each user ID • Support of Single Sign On-functions with Kerberos	• No illegal access by trial and error of passwords • Check on access paths • Logon without specification of password in the sense of single sign on possible
Rights Management System	
• Decentralization of system administration by means of privileges • Introduction of customer-specific role-concepts • Introduction of user groups	• Decentralization of the tasks of the system administration • Privileges for customer specific security roles • Mapping of org. unities or projects to user groups with common administration
Extended access control for objects	
• Definition of access control conditions independent of the object via GUARD • Default protection • Co-ownership for files and JVs • Restricted Co-owner-facility for TSOS	• Complete protection of objects • Defining access rights common for several objects • Defining access rights on the level of single users
Auditing	
• Selective logging of security-relevant events • Archiving and evaluation of auditing data for revision and security analysis	• Recognition of penetration tests and violation of safety policy • Complete survey of accesses to objects • Backtracking of security-relevant events to the responsible person

Topics

Extended access control

Extended access control improves password protection in BS2000 by introducing measures which effectively prevent systematic attempts to crack LOGON passwords during normal operation. In addition to existing options (e.g. password encryption), SECOS provides the following mechanisms:

- Specification of a minimum password length forces users to keep to a certain length for their passwords in order to prevent them working in the system without passwords or with only trivial passwords.
- Introduction of a minimum complexity for passwords is intended to prevent users defining overly simple passwords.
- Limiting the lifecycle of a password forces the owner of a user ID to change his or her password after a certain length of time, thus increasing security in the use of passwords.
- Support for an initial password: When issuing a new password, the system administrator not only specifies the lifecycle of the first password, but also has the option of immediately flagging the new password as expired. This obliges the user to define a new password when logging on for the next interactive session.
- Password history
  Passwords that have already been used (the number can be specified) are archived to prevent the same password being used again. This enables the period of validity of a password to be precisely traced.

Barricade and observe of user IDs/terminals

- Limiting the lifecycle of a user ID is appropriate in situations where it is possible to anticipate that a certain user identification should be valid for a specific period of time only.
- Information function detailing last LOGON access
  Following successful terminal logon, users receive information relating to the security of their user ID. Users can use this information e.g. to determine the last time their user ID was used or how many failed logon attempts have been made between the current and the last successful access. This information is intended to meet the security needs of users and make them independent of the attention of the security administrator.
- User IDs / terminals can be barred after n failed attempts (previously, failed attempts during password input were sanctioned with time penalties or connection clear-down; even automated intrusion attempts could be prevented in this way, however). User IDs that have not been used for n days can also be barred.

Restriction of interactive access based on the **"personal LOGON"** function. To authenticate interactive dialog jobs, the personal LOGON can be specified in addition to the user ID to allow unique identification of a specific individual, particularly for auditing purposes.

Differentiation of access classes

- It is possible to specify permitted access methods (e.g. interactive, batch, POSIX rlogin) separately for each user ID. This enables the different access paths to be controlled. It is also possible to impose restrictions on partners in the network, particularly terminals.
- A number of access classes have been implemented to support POSIX. This enables e.g. access by cross-computer POSIX commands to be administered independently of the POSIX rlogin. A further access class allows selective activation of user IDs for POSIX server tasks.

Kerberos for cross-platform Single Sign On

By supporting Kerberos-based authentication in BS2000, SECOS enables BS2000 users to log on without specifying a password (in terms of a single sign-on). A Kerberos client has been implemented in BS2000 and will use the Windows Primary Domain Controller (PDC) that (usually) exists in the BS2000 environment as the server (Key Distribution Center). Support for the Kerberos authentication function has been implemented on the client side in the **MT9750** terminal emulation (starting with V6.0) as well as in other emulations from software partners.

The Kerberos authentication functionality is also available for TU applications. First time users are OMNIS, OMNIS-MENU and openUTM.

Rights Management System

Privileges - decentralization of administration

SECOS implements a rights management system enabling the different administrative tasks associated with the TSOS user ID to be shared among a number of other user IDs. The aim of this approach is to move away from the all-inclusive rights previously enjoyed by the system administrator ID toward a distributed system administration more in keeping with real-world conditions.
Individual privileges can be combined into a "collective privilege" and assigned a role specific to the individual computer center. This allows areas of activity comprising several individual privileges to be created.

Introduction of user groups

The advantage of setting up user groups is that the large number of users present on the system can be structured more clearly. It also enables organizational units or projects represented by certain persons with specific user IDs to be simulated with the corresponding resource allocation in the system. The aim of this is to delegate certain well-defined management functions to the local group administrator and so relieve the load on the system administrator.
To improve user group management, group administrators have the option of selecting their own naming schemes. This is done with the aid of character patterns for the specification of unique names for user groups and group members.
Besides the basic relevance of the group on the administration of resources, the group also plays a role when accessing files and job variables.

Extension of group access

In principle, a user ID always can be assigned to one single user group. Problems arise, if an employee acts in several groups at the same time and therefore needs access to the appropriate data.
In such cases, when accessing to files and job variables, which are protected by simple access control lists, the same access rights can be admitted further users, additionally to the real group members.

The same user in multiple user groups

In the real world, user groups are required to enable employees to be assigned to a specific procedure or project. In the past there were potential problems if an employee was simultaneously involved in a number of procedures. With SECOS, a user can be assigned to several user groups so that file accesses can be more easily checked. This allows better mapping of the customer's practical requirements.

Extended access control for objects

Access control options for objects

Existing and new mechanisms are available for protecting files in BS2000. These mechanisms regulate file shareability and access rights in different ways.

- Standard access control can be used as before to specify whether the file can be accessed only by its owner or by all user IDs defined in the system.
- The Basic Access Control List permits more fine-grained protection. Possible access types include read, write and execute. Access rights can be defined separately for the owner, the members of the owner's user group (Group) and all other users (Others).
- The GUARDS subsystem provides an independent, user-definable access control mechanism for objects of different types, such as files, library elements, FITC ports and programs. Here, the protection criteria are administered centrally in the system and the protection definitions, relating to a specific object, are combined in a container called a "guard". Guards are suitable for universal use and are implemented in the system as object-independent entities.
  This has the advantage of providing a simple means of granting the same access rights to multiple objects, and also an easy way of dynamically changing access control for multiple objects.
  A guard can also be used to specify conditions which are to be evaluated when the object is accessed. Conditions may include user privileges a point in time or a time period or a system condition.

Default protection

The use of the default protection function greatly increases access protection for objects (files and JVs). This function gives the user the opportunity to set defaults for protection attributes on an object-specific basis and so provide effective protection for objects from the time they are created. This setting can be made for file namespaces on a user ID or pubset-specific basis. Explicit user specifications override the default settings.

Co-owner protection

The co-owner functionality enables co-ownership of files and JVs (already familiar from TSOS) to be also set up for other user IDs.
The same procedure can also be used to withdraw the co-ownership privilege assigned by default to the TSOS user ID.

Auditing

For auditing purposes in a secure system, the SAT subsystem (Security Audit Trail) is approved for use in BS2000 as a component of the SECOS product. This subsystem supports selective logging of security-related events in specially protected files (SAT logging files). By analyzing these files, duly authorized users can thus obtain a complete overview of which user accessed a specific object in what way and at what time. It is also possible to obtain a trace of special processing steps and actions by specific user IDs in order to discover any misuse of the system or unauthorized access to stored data.

As well as the logging function, an ALARM function is also offered. The security coordinator has the option of defining conditions which trigger an alarm when certain events are called. If an alarm occurs, a message is issued at the main console and the event is written to the logging file.

An offline output of SAT statistical data is used for a preliminary analysis. There are various output options, such as SAT statistics on critical event types or summaries of event types.

In the pre-selection, a filter can be specified with conditions in a similar way to alarm definitions. If one of these conditions is true, the type of filter set determines whether logging is performed (positive filter) or not (negative filter). The full parameter list can be logged in addition to the event to allow more detailed analysis of security violations.

Technical details

Requirements	
Technical requirements Hardware	Fujitsu Server BS2000 SE Serie
Technical requirements Software	BS2000 OS DX V1.0 - SDF-P for the use of function CONVERT-KEYTAB
Requirements for the user	Knowledge of BS2000
Installation and operation	
Operating mode	Dialog and batch operation
Implementation language	C, Assembler
User interface	Commands in English, Message texts in German/English (optional)
Installation	According to the user guide
Documentation and training	
Documentation	The Manual and Release Notice for SECOS are available on the manual server.
Training	See course offer (German)
Reference and delivery	
Conditions	This software product can be leased by the customer in accordance with the conditions for the use of software products.
Ordering and delivery information	The software product can be obtained from your local Fujitsu regional office.

Contact

Fujitsu
BS2000 Services
Email: bs2000services@fujitsu.com
Website: www.fujitsu.com/emeia/bs2000
2022-06-30 EM EN