White Paper
FUJITSU Software BS2000 SECOS

Security with BS2000

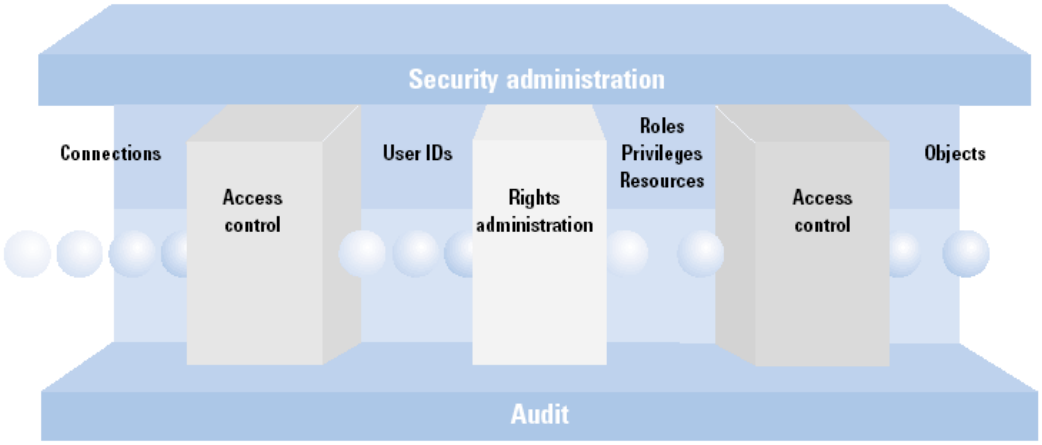
The security risks attending commercial data processing are manifold. They range from errors in the use and operation of IT-systems to premeditated computer crime. Possible consequences include the loss of data availability, integrity and confidentiality. It is therefore imperative to combat these risks and institute security measures to administer and monitor access rights, anticipate potential threats and counter them if they actually materialize.
In this sea of insecurity there is still an impregnable island – the mainframe with its approved security mechanisms: applications and data are still nowhere as secure as on the mainframe. For the BS2000 platform FUJITSU Software BS2000 SECOS and its procedures guarantee cutting-edge levels of system security, which can even be scaled to the requirements of individual users.

Contents

Product description

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 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.



Comprehensive and seamless security is vital for commercial data processing.

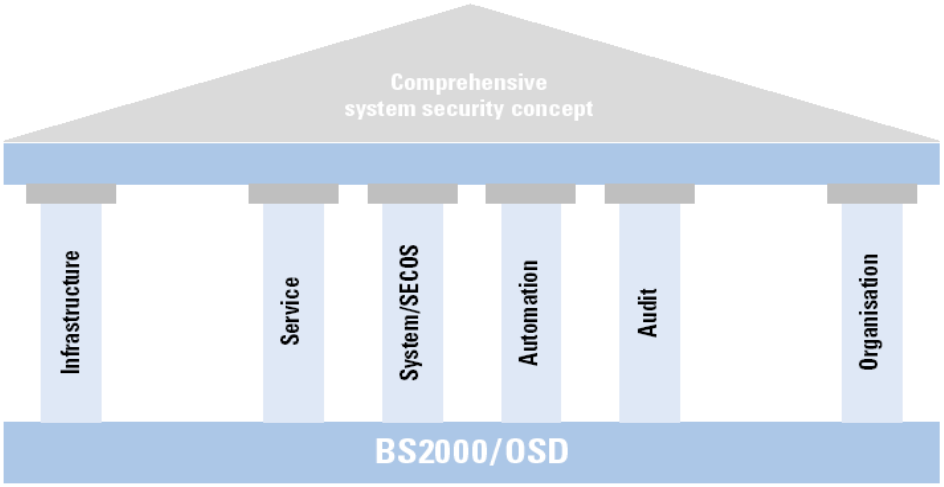
SECOS – the security lock for BS2000 system security

The BS2000 platform provides the keys to custom-built security solutions:

- openSEAS opens up cross-platform transaction security, right down to mobile client level.
- *open*Networking opens up comprehensive network security, and
- SECOS (SEcurity COntrol System) is the security lock for scalable system security for BS2000 servers.

SECOS enables authorized users and user groups on BS2000 systems to keep their data, activities, processes and programs hidden from unauthorized users and prevent them from being manipulated. At the same time it guarantees that the attempted misuse of the system will be instantly detected and logged in detail by privileged system operators with special access rights.

"Comprehensive" security means recording and evaluating all potential threats to a system or from within a system. This depends not just on the system but also on individual organizational conditions and on how the IT infrastructure of the enterprise concerned is intermeshed with its suppliers and customers.



SECOS – the flexible security management solution

User identification

The password mechanism is the standard method employed for user management. SECOS supports "coarse" and "fine granular" specifications of usage profiles. Access to definable resources can be restricted to precisely defined client groups and to definable time windows.
The standard method of proving identity is based on the use of passwords, so to support this SECOS permits the time limited definition of password validity and requires a minimum degree of password complexity to prevent known forms of attack (e.g. dictionary attack).
SECOS enables BS2000 to be integrated into a datacenter-wide, cross-platform, single sign-on concept using user-friendly proofs of identity.

The benefits of fine-granular access control are clear from the following security scenarios:
- Access to server resources from outside the organization must be controllable in order to defend against attacks.
- Access to server resources from inside the organization must be controllable, particularly access by privileged users.

Strategies: Security by role assignment

Security management is centralized in BS2000. A security coordinator specifies who is allowed to execute which privileged actions, as well as the scope of the logging function.

The coordinator's tasks include assigning the following security management roles:
- User management
- System-wide management of access rights
- Control of security-relevant event logging
- Management of file transfer access control

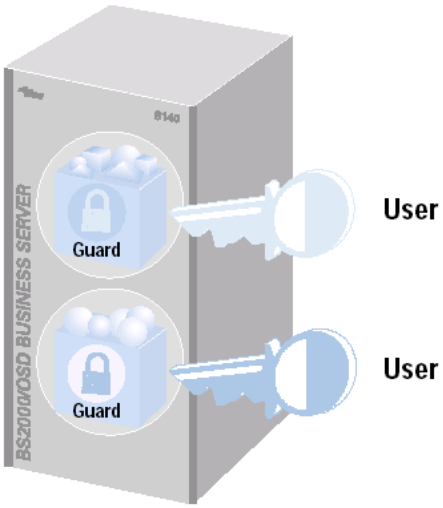
The user management function can, in turn, empower all users to administer their own passwords. Each user can then manage access rights to his or her objects (i.e. objects owned by his or her user ID).

Object-oriented security management

SECOS provides a standardized access control method for files, libraries, job variables and process communication (FITC ports).

With this method, access control profiles are defined independently of the objects and object types requiring protection. These access control profiles are called "guards". Each guard can be linked with an unlimited number of objects of the same or different types.

Guards are used to specify access:
- Which user or which user group is allowed access
- What privileges an accessing user must possess
- At what time access is allowed or prohibited
- What programs may be used for access



Collecting proof

A security system which detects security violations but cannot accurately identify those responsible is worthless. That is why SECOS responds to any security relevant event by recording the time, the user ID of the offender, the consequences of the action, and – if available – the offender's personal ID.

Tracing the person responsible can also be guaranteed even in cases where, for technical or organizational reasons, a number of users are working under the same user ID.

Details of recorded events include:

- Logon, POSIX remote login, batch job start
- Modification of a file or library member
- Assignment of privileges
- Assignment of an operator role
- Processing of data media (tapes, disks)
- Activation of subsystems

Human operators or automatic programmed operators are automatically alerted when major, potentially threatening events occur. "Alarms" are also logged, of course.

The security logs can be analyzed according to security and auditing criteria and saved to long-term archival storage. The security coordinator, system administrators and support staff and individual users can also check the security settings relevant to them at any time.

Comprehensive security management with Fujitsu know-how

Achieving a high level of system security is only possible by in-depth analysis of the security risks ahead of any rollout of security measures. Fujitsu Technology Solutions offers its customers comprehensive support for such an analysis.

Summary

- The scalability of the functions guarantees security tailored to the customer's individual requirements.
- The comprehensive security framework provided by SECOS ensures that even the exacting requirements of auditors (data protection officer, bank auditors, etc.) are complied with.

Kontakt:
Fujitsu
Barbara Stadler
Mies-van-der-Rohe-Straße 8, 80807 München
Germany
Telefon: +49 (0)89-62060-1978
E-Mail: barbara.stadler@ts.fujitsu.com
Website: de.fujitsu.com
31. August 2015 EM EN