



Fujitsu Siemens Computers

*open*CRYPT™-SERV (BS2000/OSD)

Version 1.2A

January 2005

Release Notice

Copyright (C) Fujitsu Siemens Computers 2005
All rights reserved

Release Notice *openCRYPT™*-SERV V1.2A

1	General	2
1.1	Ordering	3
1.2	Delivery	3
1.3	Documentation	4
2	Software extensions	5
2.1	Limiting the number of sessions per user	5
2.2	Long runner	5
2.3	Additions for file encryption	5
2.4	Performance measures	5
3	Technical information	6
3.1	Resource requirements	6
3.2	Software configurations	6
3.3	Product installation	6
3.4	Product use	7
3.5	Obsolete functions (and those to be discontinued)	7
3.6	Incompatibilities	7
3.7	Restrictions	7
3.8	Procedure in the event of errors	7
4	Hardware support	8

1 General

This Release Notice is a summary of the major extensions, requirements and operating information with regard to *openCRYPT™*-SERV V1.2A which runs under the BS2000/OSD *) operating system.

The release level is that of January 2005.

This Release Notice is supplied as a file in uppercase and lowercase. Customers will receive an updated version of this file should any subsequent changes be made.

To print the file, use
/PRINT-DOCUMENT FROM-FILE=SYSFGM.OCRYSERV.012.E, -
/ DOC-FORM=*TEXT (LINE-SPACING=BY-EBCDIC-CONTR)
(English version).

This Release Notice is also available online
<http://manuals.fujitsu-siemens.com> or under
http://its.siemens.de/lobs/its/its_sc/fgm_en/bs2000/index_en.htm

If one or more previous versions are skipped when this product version is used, the information from the Release Notices (and README files) for BS2000/OSD-BC of the previous versions must be noted.

The use of names, trademarks, etc. in this Release Notice does not entitle readers to assume that these names/designations may be used without restriction by anyone; often the names / designations are protected by law or contract, even if this is not indicated here.

Security notice:

LIABILITY EXCLUSION!

If you implement a security architecture as part of your project, you must configure and use the selectable functions and systems according to their actual requirements.

Fujitsu Siemens Computers will not accept any responsibility for any type of problem or damage that occurs as a result of wrongly set parameter values or incorrectly used mechanisms or functions of the *openCRYPT™* interfaces.

openCRYPT™ products use standardized open interfaces for encryption and decryption

openCRYPT™-SERV is based on the PKCS#11 interface and provides BS2000/OSD applications with a function interface for accessing cryptographic functions.

*) BS2000/OSD (R) is a registered trademark of Fujitsu Siemens Computers

S-server

openCRYPT™ BOX offers for BS2000/OSD-systems together with *openCRYPT™*-SERV cryptographic basis functions. As a canal-coupled external Co-processor it is available for the encoding orders.

SX-server

openCRYPT™-SOFT is an optional integrated solution for cryptographic functions on SX-systems. It supports, the PKCS#11 based application interface of *openCRYPT™*-SERV. For SX-systems *openCRYPT™*-SOFT prepares functions, that are offered for S-server through the *openCRYPT™*-BOX.

Highlights of *openCRYPT™*-BOX or *openCRYPT™*-SOFT are

- High processing performance thanks to external coprocessor for S-Server or dedicated CPU for SX-Server and therefore relief of the BS2000-CPU
- BS2000 application interface (*openCRYPT™*-SERV)
- secure encryption thanks to use of proven and recognized algorithms and long keys

1.1 Ordering

The delivery unit *openCRYPT™*-SERV V1.2A can be ordered from your local distributors and is subject to the general terms and conditions of the software product use and service agreement.

1.2 Delivery

The *openCRYPT™*-SERV V1.2A files are supplied via SOLIS.

The following delivery groups belong to the delivery scope of *openCRYPT™*-SERV V1.2A:

OCRYSERV V1.2A

SYSFGM.OCRYSERV.012.D	Release Notice (German)
SYSFGM.OCRYSERV.012.E	Release Notice (English)
SYSRME.OCRYSERV.012.D	README file (German)
SYSRME.OCRYSERV.012.E	README file (English)
SYSSII.OCRYSERV.012	Structure information for IMON
SYSSSI.OCRYSERV.012	Subsystem information file

CRYPT V1.2A

SIPLIB.CRYPT.012	TPR macro/include library
SPMLNK.CRYPT.012	Load module library (SX-server)
SPMLNK.CRYPT.012.150	Load module library (OSD/XC V2.0)
SPUOML.CRYPT.012	Adapter module library (SX-server)
SYSLIB.CRYPT.012	Macro/include library (S-server)
SYSLNK.CRYPT.012	Load module library (S-server)
SYSLNK.CRYPT.012.150	Load module library (OSD-BC V6.0)
SYSMES.CRYPT.012	Message file
SYSPRG.CRYPT.012	Program library
SYSRME.CRYPT.012.D	README file (German)
SYSRME.CRYPT.012.E	README file (English)
SYSSDF.CRYPT.012	SDF syntax file
SYSSII.CRYPT.012	Structure information for IMON
SYSSSC.CRYPT.012	Subsystem catalog statements
SYSSSC.CRYPT.012.150	Subsystem catalog statements

The current file and volume characteristics are listed in the SOLIS2 delivery cover letter.

1.3 Documentation

The following documentation is available for *openCRYPT™-SERV* V1.2A

openCRYPT V1.1 Sicherheit mit Kryptografie Benutzerhandbuch	U41238-J-Z125-2
---	-----------------

openCRYPT V1.1 Security with Cryptographic User Guide	U41238-J-Z125-2-76
---	--------------------

There are also additional README files for these manuals. They contain any changes and extensions made to the manual.

SYSRME.OCRYSERV.012.D	(German)
SYSRME.OCRYSERV.012.E	(English)
SYSRME.CRYPT.012.D	(German)
SYSRME.CRYPT.012.E	(English)

When printing the files, the CONTR-CHAR=EBCDIC operand should be specified in the PRINT-FILE command.

In addition to the above, the BS2000 basic configuration manuals are required to operate *openCRYPT™-SERV*.

The BS2000/OSD documentation is also available under the title BS2000/OSD SoftBooks in German and English on CD-ROM.

The documentation is available as online manuals under <http://manuals.fujitsu-siemens.com> or can be ordered in printed form at extra cost under <http://FSC-manualshop.com>

2 Software extensions

Only the changes and extension with respect to the previous version *openCRYPT™*-SERV V1.1A are described in the following sections.

2.1 Limiting the number of sessions per user

The number of sessions that a BS2000/OSD user can open simultaneously is limited. As of BS2000/OSD V6.0, the upper limit can be specified with the CRYPTO-SESSION-LIMIT operand of the MODIFY-USER-ATTRIBUTES or ADD-USER command. In versions earlier than BS2000/OSD V6.0, 128 parallel sessions per task are possible.

2.2 Long runner

Extension of the CSESSION macro with the CGENKPR operand. It assigns a process to all calls in the session to the *openCRYPT™*-BOX/SOFT that may run for either a very long time or only a short time.

2.3 Additions for file encryption

As of BS2000/OSD V6.0, files can be encrypted.

2.4 Performance measures

Preparatory actions have been taken to enhance performance in conjunction with openFT and IPsec.

3 Technical information

3.1 Resource requirements

The following resources are required for *openCRYPT™*-SERV V1.2A:

BS2000 disk storage space:

approx. 4,7 MB (S-Server)

approx. 5,5 MB (SX-Server)

Virtual address space:

approx. 2.6 MB (static)

approx. 0.3 MB (dynamic)

The dynamic memory requirement increases for each task by approx. 1.6 MB.

These are minimum values that may be higher depending on the encryption algorithm.

3.2 Software configurations

The runtime environment for *openCRYPT™*-SERV V1.2A is as follows

<u>Product</u>	<u>Version</u>
BS2000/OSD-BC	as of 5.0
OSD/XC	as of 2.0
with X2000	as of 3.0
openNet Server	as of 3.0
SINIX-2000-Z	8.1 K818.20 (BOX)

3.3 Product installation

The product is installed using the installation monitor IMON. The information concerning installation in the delivery cover letter and in the product documentation must be followed as well as the information in this Release Notice.

The subsystem information file SYSSSI.OCRYSERV.012 is stored in the system under the name SYSSSI.CRYPT.012.

The subsystem information file (SYSSSI.CRYPT.012) describes how an *openCRYPT™*-BOX/SOFT is connected to BS2000. It contains an example for defining the interface.

```
PORT PORT-NAME=CRYPOR1,WRITE-DEVICE=????,READ-DEVICE=????
```

Enter the actual values for WRITE-DEVICE and READ-DEVICE prior to startup. Select a free PORT-NAME.

For information about linking the *openCRYPT™*-BOX to BS2000 systems, consult the *openCRYPT* manual and the user manual "SINIX-2000 - Setup, Operation & Administration". The value for the number of processes must be set to "1" and max to "2".

From the viewpoint of BS2000, *openCRYPT™*-BOX is a device that consists of a read and write device. However, in contrast to other channel-linked devices, a dual connection with two included paths is possible.

With a link via a type S connection director, make sure that the devices are assigned to the systems individually since devices cannot be shared by two systems.

Please refer to the *openCRYPT* manual for additional information about device configuration.

3.4 Product use

If it becomes apparent during the subsystem initialization that connection to the *openCRYPT*[™]-BOX or *openCRYPT*[™]-SOFT (dedicated CPU) is not possible, the subsystem startup is aborted with an error.

RECOMMENDATION

It is advisable to shut the subsystem down prior to carrying out administrative activities on the *openCRYPT*[™]-BOX.

3.5 Obsolete functions (and those to be discontinued)

none

3.6 Incompatibilities

none

3.7 Restrictions

none

3.8 Procedure in the event of errors

If an error occurs, a detailed description of the condition is required for diagnostic purposes, as well as information as to whether and how the error can be reproduced.

You will find further information in the *openCRYPT* manual in section "Creating diagnostic documentation".

4 Hardware support

openCRYPT™-SERV V1.2A

All CPUs that are supported as of BS2000/OSD V5.0A are supported in native mode.

openCRYPT™-SOFT V1.2A

For *openCRYPT™-SOFT* an individual CPU (payable) is necessary for the SX-System (beside SX100).



Information on this document

On April 1, 2009, Fujitsu became the sole owner of Fujitsu Siemens Computers. This new subsidiary of Fujitsu has been renamed Fujitsu Technology Solutions.

This document from the document archive refers to a product version which was released a considerable time ago or which is no longer marketed.

Please note that all company references and copyrights in this document have been legally transferred to Fujitsu Technology Solutions.

Contact and support addresses will now be offered by Fujitsu Technology Solutions and have the format *...@ts.fujitsu.com*.

The Internet pages of Fujitsu Technology Solutions are available at <http://ts.fujitsu.com/...>

and the user documentation at <http://manuals.ts.fujitsu.com>.

Copyright Fujitsu Technology Solutions, 2009

Hinweise zum vorliegenden Dokument

Zum 1. April 2009 ist Fujitsu Siemens Computers in den alleinigen Besitz von Fujitsu übergegangen. Diese neue Tochtergesellschaft von Fujitsu trägt seitdem den Namen Fujitsu Technology Solutions.

Das vorliegende Dokument aus dem Dokumentenarchiv bezieht sich auf eine bereits vor längerer Zeit freigegebene oder nicht mehr im Vertrieb befindliche Produktversion.

Bitte beachten Sie, dass alle Firmenbezüge und Copyrights im vorliegenden Dokument rechtlich auf Fujitsu Technology Solutions übergegangen sind.

Kontakt- und Supportadressen werden nun von Fujitsu Technology Solutions angeboten und haben die Form *...@ts.fujitsu.com*.

Die Internetseiten von Fujitsu Technology Solutions finden Sie unter <http://de.ts.fujitsu.com/...>, und unter <http://manuals.ts.fujitsu.com> finden Sie die Benutzerdokumentation.

Copyright Fujitsu Technology Solutions, 2009