

## *interNet* Services (BS2000/OSD) Version 3.2 Internet standard products

Issue October 2006

Pages 3

### Internet standard products in BS2000/OSD

The 'open' communications network will mainly be shaped by the Internet Protocol Suite (IPS) of the TCP/IP world. The products FTP, TELNET, DNS, NTP, OpenSSL, OpenSSH and e-Mail of the selectable unit *interNet* Services (short designation: INETSERV (BS2000)) provide functions that support the interoperability of communication partners in 'open' TCP/IP-based networks. The products making up the *interNet* Services selectable unit are ported versions of corresponding internet standard products from the 'open' world, adapted to suit the specific conditions of the BS2000/OSD environment. This guarantees a standardized user interface, as well as administration and interoperability of the products across system boundaries.

TELNET, FTP, OpenSSH and e-Mail are available as both servers and clients.



#### TELNET

The TELNET client runs in interactive mode under TIAM or POSIX and enables connections to be set up to other computers in the network. The TELNET server runs in batch mode, receives connection requests from TELNET clients in other computers, and forwards them to TIAM in the local BS2000 computer.

#### FTP

The FTP client runs in interactive mode under TIAM or POSIX and enables connections to be set up to other computers in the network. The FTP server runs in batch mode, receives connection requests from FTP clients in other computers, and executes their jobs in separate subtasks on the local BS2000 computer.

#### Domain Name Service (DNS)

The motivation for setting up a name service in a data network springs from the desire to increase the performance, scope of services and acceptance of the network. In the internet environment, communication partners are generally addressed on the basis of symbolic names. The DNS server administers the resource records serving to describe the relationships between the names and IP addresses of computers and answers queries in this regard. Socket applications in the BS2000/OSD system can submit queries to DNS servers by means of the DNS Resolver.

#### Dynamic Domain Name Service (DDNS)

The DDNS is based on a protocol that represents an extension to the DNS. This protocol enables dynamic changes to be made to the database during online server operation.

#### Network Time Protocol (NTP)

The Network Time Protocol is based on the client/server concept and permits a reference clock time (Universal Coordinated Time, or UTC) to be distributed within a network. It also handles coordination of the clocks in networks of any size. The implementation of the NTP V3.0 protocol corresponds to RFC 1305.

#### e-Mail

The internet's e-mail system is a complex structure in which a whole series of different protocols and standards interwork. The e-mail system differs in one quite significant respect from other internet applications such as Telnet, FTP or the World Wide Web. All these services and protocols require a direct connection via TCP or UDP between sender and recipient. The situation is different with e-mail. In this case the recipient's computer system does not have to be connected to the network at the same time as that of the sender. The e-mail system is based on the concept of intermediate mail routers which first receive a message and then forward it to the recipient's mail server. A suitable mail program capable of supporting the SMTP (Simple Mail Transfer Protocol) protocol is used for this purpose. The message is read out from the mail server onto the destination computer system using a service that is enabled by the POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) protocol. This closes the loop from the sender to the recipient. The interaction between the instances involved is based on the client/server concept. In this scenario, a PC computer, for example, handles the client part and the BS2000/OSD system including the *interNet* Services products acts as the server part.

## Secure Socket Layer (OpenSSL)

To allow encrypted transfer of user data with the socket applications TELNET, FTP and e-Mail, and also to provide security for accesses to DNS servers, the Open Source product OpenSSL has been ported to BS2000. The OpenSSL interface serves exclusively for internal use by the internet services of the product and consequently is not provided for use by customer applications.

## Secure Shell (OpenSSH)

The Secure Shell (SSH) under POSIX makes possible secured communication over uncertain networks and can the uncertain r-commands (remote shell), telnets and ftp replace, which transfer the entire communication, especially however the passwords, uncoded (unless, they use SSL/TLS-certain connections).

## Functional Description

### TELNET

Connection requests are accepted by the TELNET server at the TELNET port and a DCAM connection is set up to TIAM in each case. As far as TIAM is concerned, an 8103 terminal is emulated. This permits a line-oriented dialog, but no format mode is possible. The TELNET client transfers the connection request to the target system (TELNET server), which receives the connection request at the opposite end and processes it further. If the client is authorized, a virtual connection is set up.

To enable secure use of the TELNET services, the socket application TELNET can also optionally make use of encryption via the SSL/TLS interface. Authentication and data transfer can be performed using encryption. Functional enhancements implemented in the present version include:

- Secure authentication via SSL/TLS
- Secure transfer using SSL/TLS
- Provision of a TELNET client in POSIX
- and various other customer requests.

### FTP

For each connection request received from the network, a LOGON is performed under the required user ID and the program <FTPDC> is started. This program handles the actual file transfer and the local file accesses. This ensures that the usual DMS access rights are observed. Thanks to its restart capability, an interrupted transfer can be resumed from the point of interrupt.

FTP can be supplemented with the FTAC (File Transfer Access Control) functionality of *openFT*. The FTAC function achieves the separation of FTP access authorization and login authorization in order to protect the BS2000 server and thus controls access rights on the basis of users and/or partner systems.

To enable secure data transfer using FTP, the socket application FTP can also optionally make use of encryption via the SSL/TLS interface. Authentication and data transfer can be performed using encryption. Data transfer using SSL/TLS is possible either only for the monitoring connection or for both the monitoring and the data connection.

Functional enhancements implemented in the present version include:

- Secure authentication via SSL/TLS
- Secure transfer of monitoring and user data using SSL/TLS
- 1:1 transfer of files with a homogeneous BS2000 link
- Subprogram interface
- Writing of accounting records
- and various other customer requests

## DNS / DDNS

In the internet environment, communication partners are usually addressed on the basis of symbolic names. As the name of the DNS service itself implies, the name space of the network is subdivided into areas called "domains". The domains are arranged in a tree structure. Information on addressable objects is stored in Resource Records (RRs) and managed by the name server. The syntax in which RRs are held in the name server database is specified in full. The data is coded in ASCII.

In the DNS client/server architecture, the Resolver handles the client part. The Resolver instance, represented by the corresponding product in the INETSERV selectable unit, handles queries to the name server on behalf of the application program and hence of the user. These DNS queries can optionally be signed.

The product provides access to the DNS service for the Socket applications running in the BS2000/OSD environment (DCAM (BS2000) and POSIX(BS2000)). A DNS server can also be deployed in order to manage the RRs of the local computers.

The DNS is enhanced by the DDNS functionality, which enables dynamic changes to be made to the database during online server operation. With these zone transfers, the data transfer is always encrypted for security reasons. In the present version of INETSERV, the DNS service in BS2000 is based on the ported version of the Open Source product Bind 9 .

### NTP

BS2000/OSD uses the NTP functionality as a client. The client requests an NTP message with the relevant time stamps from the server and then synchronizes its own clock. The system time in BS2000/OSD is set via the function *adjtime*, which is offered as a privileged TPR interface. The *adjtime* function is used by a number of privileged users. An internal precedence relationship or on the basis of the quality parameter of the time information are specified to determine which jobs to synchronize the clock time are executed.

The system time is available to the user via the GTIME and GDATE interfaces, as well as via the runtime routines of high-level languages.

The Network Time Protocol function may not be used simultaneously with the product DCE.

Note on the VM2000 operational environment:

Every system (monitor or guest systems) participating in an NTP network must have the NTP function installed.

### e-Mail

The e-mail services in the *interNet* Services product include the components:

- SMTP Mail Server
  - The SMTP server is responsible for the transfer and delivery of e-mail messages in the network. It coordinates the transport of e-mails in the network and stores received e-mails in mail inboxes.
- POP3 Server and
  - IMAP Server
    - enable access by a remote e-mail client to the received e-mails in inboxes.
- Mail Sender
  - consists, in BS2000/OSD, of a subsystem with SDF-command and macro interface that permit e-mails to be created and passed to an SMTP Mail Server.
- Mail Reader
  - In BS2000/OSD, the Mail Reader enables automated retrieval and further processing of e-mails by means of POP3 or IMAP. A procedure and a program interface are provided as options in BS2000/OSD for this

purpose. The message headers, message bodies and attachments of an e-mail can be accessed via these interfaces.

To the secure transfer of e-mails, the e-mail services can use in the BS2000/OSD optional also an encryption by means of SSL/TLS between the involved mail servers and between the mail servers and the mail clients. The e-mails themselves can sign and/or encrypt with S/MIME additionally.

The previous mail sender from the version 3.1 (TU program) is with-delivered additional and last again for reasons of the compatibility. From the next version becomes this no longer delivered.

### OpenSSL

The set of functions provided with the ported version of OpenSSL includes a command line tool, the SSL/TLS library and a cryptography library.

OpenSSL is used by the FTP, TELNET, e-Mail and DNS services and provided with these with the level of functionality required in each case. Consequently OpenSSL is not released as a separate product for general customer use.

### OpenSSH

SSH encrypt the entire connection in order to stop eavesdropping, connection hijacking and similar network-attacks. Furthermore, additional possibilities are offered for authentication. With SSH, one can lead further application protocols through a certain tunnel via port-forwarding. With SSH, one marks both a kryptografisches protocol as well as a concrete implementation of this protocol.

## Technical requirements

### Hardware

*interNet* Services V3.2 runs on all servers released for BS2000. This can be seen from the BS2000 assignment matrix.

HNC III (91851),  
HNC III-R ( 91852) or  
HNC IV (91853).

LAN channel adapter 9632-3 or 9632-2 (Type2) with 9632-HST 2 is supported in restricted mode only (BCAM V13.0).

### Software

BS2000/OSD V5.0, V6.0 or V7.0,  
*openNet* Server V2.0 or higher for S- and SR-servers,  
*openNet* Server V3.0 or higher for SX-servers,  
TIAM V13.1 or higher.

With the use of the services under POSIX is required additionally:

POSIX-BC V5.0 or higher with at least correction-version A35.

In following case, a higher correction version is necessary:

Improved installation procedure: A37 .

The products *openFT* V7.0 or higher and *openFT-AC* V7.0 or higher are a requirement for use of the FTAC functionality.

The product JV V13.0 or higher is an additional requirement for use of FTP command monitoring by means of job variables.

The product SDF-P V2.1 or higher is an additional requirement for use of FTP command monitoring by means of SDF-P variables.

### Installation

See documentation and release notice.

### Documentation

Administrator and user guide

The documentation is also available as online manuals, see <http://manuals.fujitsu-siemens.com/mainframes.html> , or in printed form which must be paid and ordered separately at <http://FSC-manualshop.com>.

### Download and Internet

Additional information to the product finds you also in the Internet under the WWW-address

<http://bs2000.fujitsu-siemens.com/INetServ/index.en.php3>. There, you also find a link to our Goody-Side, on which we offer additional software without fee to the download. That are additionally programs to APACHE and mail, just as a mighty editor, a comfortable shell and much more that conversions of Open Source software are on BS2000/OSD.

### Demands on the user

BS2000/OSD knowledge

### Training

See course offer at:

<http://www.fujitsu-siemens.com/training>

### Conditions

This software product is supplied to the customer under our conditions for the use of software products against a single payment or installments.

### Warranty

Class: A  
Delivery format: Machine language

### Ordering and delivery

This software product may be obtained from your local Fujitsu Siemens Computers GmbH regional office.

### License notice:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)).