

Purpose

Modern business requires instant, reliable, confidential and secure communication between business entities. J42 for Secure Access Direct Link allows you to use the Internet for exchanging messages with your business partners and customers and to be confident that those messages are secure, secret and safe. Direct Link uses simple low cost Web technology to bring you high quality communications for a very small outlay.

J42 for Secure Access Direct Link uses standard technologies such as SSL and PKI and with its flexible interfaces you can transparently integrate it into your existing infrastructure.

Each Direct Link installation is identified through PKI certificates and stores the associated private keys on an HSM (Hardware Security Module). This ensures that each installation has a unique identity. Both ends of all SSL communication links are authenticated through these certificates and all messages are digitally signed. This technique provides legal proof that a message received at one end of the Direct Link is the same original message that was given to the Direct Link at the other end. It also guarantees complete confidentiality of that message over a Direct Link.

A Direct Link communication link is always up and the servers at each end of the link exchange digitally signed “keep alive” messages at specified intervals to monitor the link’s continuous operation. Any problems are immediately logged and optionally e-mails can be automatically sent to the Direct Link administrators. These administration messages also serve to mask the real traffic and provide further security by hiding the level of real activity on your system.

Direct Link servers can be run in parallel linked by replicating databases to provide high availability and fault tolerance. Extensive APIs allow you to add message specific processing and message transformation directly into Direct Link thereby providing transparent integration between applications.

J42 for Secure Access Direct Link provides remote HTTPS based administration with multiple server support allowing a flexible scalable effective solution with easy-to-use control. Each server process is fully parameterized and has a multilevel tracing facility.

The Direct Link is just one component of the J42 for Secure Access product range. The J42 for Secure Access range provides secure communication for host access and message exchange. An extensive set of APIs is built into the architecture of the product making the solutions extremely flexible and adaptable.

Based purely on Java 2 technology, J42 for Secure Access products can be run on any platform which supports Java 2 including HP NonStop, IBM AIX, Linux and Windows NT/2000/XP.

J42 for Secure Access Direct Link is provided with full documentation.

The next page provides an overview of the J42 for Secure Access Direct Link architecture and a summary of the product’s features. For more details please contact us at info@j42.com or via our website: <http://www.j42.com>

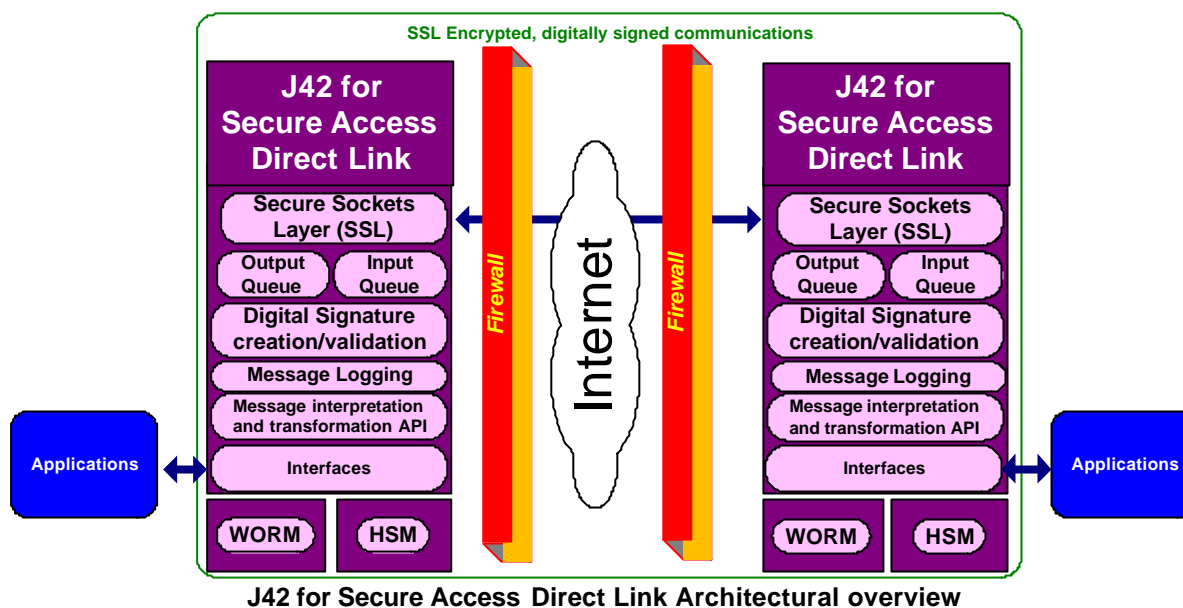
J42 for Secure Access is available from:

J&B Computing Services

e-mail: info@j42.com

web site: www.j42.com

J42 is a registered trademark of J&B Computing Services BV. Java, 100% Pure Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.



J42 for Secure Access Direct Link Features

- *J42 for Secure Access is 100% Java*
- *Runs on any platform:* runs as a Java application on any Java 2 compliant platform.
- *Full Security Package:* with support for
 - *Confidentiality:* using standard SSL technology
 - *Authentication:* through client and server authentication
 - *Non-Repudiation:* all messages are digitally signed and logged, optionally digitally signed receipts may be returned to the sender providing proof of delivery
- *Flexible Interfaces:* the standard package includes interfaces to MQ Series, Java Messaging System (JMS), file & directory based dispatch and reception and an FTP server and client.
- *Strong SSL Encryption:* full strength encryption to ensure confidentiality
- *Authentication through HSMs or other devices:* each Direct Link installation uses an HSM to securely store the PKI private key providing a guarantee against impersonation
- *Digitally Signed Messages:* each message is digitally signed using the HSM and logged for purposes of non-repudiation
- *Message Confirmation:* Signed confirmation of receipts optionally returned to the sender
- *Digitally Signed Receipts:* for specified message types a digitally signed receipt can be automatically generated and returned when the message has been delivered to its destination
- *Interfaces to HSMs:* APIs for interfacing to Hardware Security Modules using the industry standards PKCS#11 and Java JCE.
- *Smart Card as HSM:* Able to use a Smart Card as an HSM providing an efficient low cost option.
- *Extensive tracing facilities:* to identify problem connections or clients
- *Logging facilities:* Logging API to allow you to store signed transactions in files, in a database and/or on a WORM drive.
- *On-line monitoring and control:* the system administrator has web browser access to details of all sessions plus the ability to cancel them
- *Startup and shutdown control:* runs as a service with force and quiesce shutdown options
- *Interoperability:* full support for interoperability with other Web solutions

Technical information

J42 for Secure Access is developed using Java technology and requires a minimum of Java v1.2.

J42 for Secure Access uses industry standard encryption technology and techniques including SSL, Diffie-Hellman, MD5, SHA, RSA, DES and triple-DES.