Deutsche Bank
Global Markets

http://autobahn.db.com

Autobahn

Security Overview for Fixed Income, Foreign Exchange and Futures & Options accessed via Autobahn Launcher

What are the security features of the product?

- All connections are made with HTTPS using 128 bit, SSL 3, to provide encryption and server authentication
- The installer has been signed to ensure tamper detection, and to allow connectivity both to the web server and the data server
- User authentication uses RSA SecurID two factor authentication (where available)

What firewall changes do I need to access the product over the Internet?

- Normal web connectivity should be sufficient, i.e. HTTP (port 80), HTTPS (port 443) and Sockets over SSL (port 9001) access either directly, via proxy with HTTPS tunnelling or via NAT

  Note: Poorly performing / heavily loaded proxies and other network devices are the main cause of issues with the product

What alternative is there to Internet Access?

- We use Radianz to provide dedicated communications lines in a virtual private network (VPN) for customers requiring higher bandwidth. A suitably sized Radianz connection with normal web connectivity should be sufficient, i.e. HTTP (port 80), HTTPS (port 443) and Sockets over SSL (port 9001) access either directly, via proxy with HTTPS tunnelling or via NAT
- Further discussion will be required about how the product URLs are presented onto the local network

What security precautions does Deutsche Bank take with their infrastructure?

- All infrastructure is located in Deutsche Bank server rooms. Physical access to the servers is only allowed to authorised infrastructure staff. The access is controlled by proximity cards / fingerprint scans and a list of personnel entered the server room is maintained
- Deutsche Bank has implemented fire suppression systems, UPS power and backup generators to guarantee availability for all core servers
- Deutsche Bank has set-up a state of the art firewall system for any Internet/Extranet based traffic that can be accessed from outside the bank. The set-up is used by all Deutsche Bank e-commerce systems. In general two firewalls are set-up to create an Internet DMZ, one firewall controls the traffic from outside the bank and the other firewall controls the traffic to/from internal systems

What other security procedures does Deutsche Bank have in place?

- Deutsche Bank use IDS which constantly monitor for potential assaults. Each deployment monitors the traffic within the associated DMZs generating alerts which are delivered to a 24x7 monitoring service
- Servers in this environment have security hardened OS, Change control is in place for all operations
- Servers are patched with the latest security patches after they've been tested by our dedicated support team
- An Incident Response/CERT team is in place within Deutsche Bank to respond to potential or actual computer emergency incidents
- Audits are conducted daily on each server through ESM

Has the product been reviewed by an external security consultant?

- Penetration Tests by External Security consultants are conducted yearly or on major releases (whichever is more frequent)
- All the production and BCP servers are subject to a strict Change Management procedure. Every request has to be approved by at least two different groups and a back-out plan has to be provided. Access to production system is granted on a need-to-access basis

Is a Disaster Recovery site available?

- All the systems have built-in resiliency and are configured in High-availability mode. A Disaster Recovery site is also available as part of the Business Continuity Plan