SettleNET links financial institutions with Euroclear UK and Ireland’s CREST system for the electronic settlement of UK, Irish and international securities. It has been providing benefits to its users since CREST went live in 1996. SettleNET offers a flexible, one-stop-shop approach for BT’s customers. All elements of equipment installation, communications lines, service set-up, support for live running and consolidated billing are handled by BT.

SettleNET was designed from the outset to provide a flexible and scalable solution for CREST connectivity. It has supported changing requirements, and continues to provide a high-capacity, resilient and secure service.

**Added value**

Additionally, BT offers as standard a range of services that might otherwise be costly extras. These include:

- **free support** during initial CREST trialling for new SettleNET users
- **no charge for CREST test and trial traffic**
- **no extra charge for additional (and unlimited) customer workstations** connecting to SettleNET gateways for CREST connectivity via the CREST GUI.

**Customers**

SettleNET’s scalability means that it is suitable for all sizes of Euroclear users. The diverse SettleNET customer base extends across the UK, Ireland and mainland Europe and contains some of the largest CREST users. BT’s customers include many registrars, the majority of brokers and investment managers, and a number of investment banks and CREST payment banks.

**Contingency**

As well as being the CREST connectivity service of choice for a significant proportion of CREST users, SettleNET also provides a simple, low-cost solution for organisations requiring contingency capabilities for business continuity purposes.

**BT SettleNET benefits**

- fully-managed, fast, reliable and efficient service for CREST secure connectivity
- choice of maintenance service levels
- pro-active service management
- 24x7 call reception through BT Service Centre Help Desk for support
- dedicated customer relationship manager as a single point of contact
- small-footprint, server-based solution
- IP connectivity via the BT Network
- user-site configuration options to meet customers’ live-running and business-continuity requirements
- simple file transfer and MQ interfaces for back-office connectivity
- monthly usage reports
- consolidated quarterly billing for all elements of the service
- full range of security features ensure confidentiality, integrity, authenticity and non-repudiation
- supports both CREST DEX and CREST ISO services.
Technical specifications

BT SettleNET is designed around a highly secure and resilient central infrastructure with substantial redundancy and is managed through dual management centres, providing comprehensive network management tools and automatic alerts and escalations. Security is based upon an underlying Public Key Infrastructure (PKI), with BT as the Certification Authority providing online certificate services to the SettleNET community, including certificate request, issue and revocation.

The BT SettleNET gateway is the secure interface to the customer’s systems. It uses well-defined interfaces to send and receive messages, providing extensive error reporting and recovery mechanisms. BT manages these gateways remotely and provides automatic software updates. A customer-configurable facility enables users to specify the level of remote access allowed.

BT SettleNET security includes originator authentication, message confidentiality, message integrity and non-repudiation.

Users have a choice of maintenance service levels and resilience for BT SettleNET. A dedicated helpdesk provides a single point of contact for problem reporting and resolution. The support team is co-located with the operational team to ensure timely resolution of problems.

Security attributes

Authentication of originator: Cryptographic techniques are used to prove the identity of the originator of messages sent across the network.

Message confidentiality: Messages can be encrypted as they pass over the communications network, preventing unauthorised disclosure of message content.

Message integrity: Message authentication codes are calculated and added to messages being transmitted. These codes are checked on reception to verify that the message has not been altered in transit.

Non-repudiation: This provides the ability to confirm that a given transaction took place at a given time. Copies of messages and associated security data are logged and maintained (for a period of 13 years) within a secure central audit facility. This enables re-verification at a later date to prove that a specific transfer of information did or did not take place.

Hardware acceleration: Cryptographic operations are performed with hardware acceleration implemented in an isolated, protected, tamper-resistant device.

Network security: In order to access the infrastructure, participants require BT-supplied gateway equipment configured with valid, authorised network information. Only gateways suitably configured can send messages onto the network.

Replay attack: Each message is supplied with a unique reference to prevent the message being sent more than once. Further transmissions of the same message are rejected.

Certificate validity checking: Prior to receiving message security keys the user’s security certificate is checked as being both active and valid. A certificate may be revoked if it is suspected that it has been handled in an unauthorised manner or has been compromised in some way. Attempts to use a revoked certificate are rejected.

If you’d like to discuss how SettleNET can help your organisation, please get in touch with your BT account manager or email us at settlenet@bt.com.