

The military messaging architecture

The Clearswift FlashPoint product is STANAG 4406 (Ed.1 & Ed.2) compliant Military Messaging system, providing a Messaging Client, Message Transfer Agent and Message Store. Its key features are:

- Messages signed and originators authenticated using PCT (Protecting Content Type)
- STANAG 4406 MMHS (Ed.1 & Ed.2) conformant to all mandatory requirements
- Native MAPI client with intuitive Windows GUI (Graphical User Interface)
- Uniquely suitable for use where backwards compatibility is required, since FlashPoint supports both modes of PCT defined in STANAG 4406 (Ed.1 & Ed.2). Support for transparent PCT signature allows a signed message to be read by older systems not supporting PCT, while still conveying a signature that can be verified by clients that support PCT transparent signature.
- Message Stores on server facilitates management and back-up, allows users access from any client workstation anywhere, and enables simultaneous shared access ideal for role mailboxes

Clearswift FlashPoint Client

The FlashPoint client provides composition and reception of Military Messages through an intuitive Windows Interface. It interfaces to FlashPoint server which provides the Message Store and Message Transfer Agent.

- Native Windows messaging client using a MAPI X.400 P7 Service Provider to make a remote P7 Message Store appear as a local MAPI store
- Full support for X.413(1994) P7 in client and server providing folders in the Message Store and powerful Auto-Actions
- By storing both sent and received messages in the Message Store, FlashPoint allows access to one mailbox from clients in different locations, simultaneously if required
- Client can monitor multiple mailboxes simultaneously
- Security Labels are supported in PCT, in the P772 Military Message security label fields including attachment security labels, and in the envelope
- Security label policy schemes are user/administrator configurable, supporting multiple security policies
- User-friendly SIC codes are implemented
- Support for "Address List" and "Exempted" recipients (in addition to Action, Info, Bcc, RSVP and Authorized)

Clearswift FlashPoint Server

- Precedence qualifier giving six levels of precedence. Higher precedence messages always processed ahead of lower precedence
- Server auto-action to forward messages that have not been read within a configurable time period after delivery, with different timeouts for each Precedence level. This enables automatic escalation to a guaranteed action point.
- Option for Address List expansion and Distribution List expansion using ALS/DLs stored in X.500 Directory, including the removal of exempted recipients
- Option for distribution of incoming messages based on SIC codes, using policy stored in X.500 Directory
- Obtains address from X.500 Directory when recipient specified only by Directory Name
- Available on Windows NT/2000/XP/2003 and UNIX platforms
- On Windows NT/2000/XP/2003 runs as a service or in foreground
- Option to support transport of Military Messages over SMTP, in conformance with RFC 3854
- Option to support Strong Authentication

Product Highlights:

- Messages signed and originators authenticated using PCT
- STANAG 4406 MMHS conformant to all mandatory requirements
- Native MAPI client with intuitive Windows GUI
- Option for Address List Expansion
- Option for SIC code distribution
- X.413(1994) fully supported with Auto Actions
- Creation of folders in the Message Store
- Interfaces to X.500 Directory
- Option for Strong Authentication
- Alerts for new messages across security domains
- Option for SMTP message transport

Implementation of PCT

The client implementation of PCT supports both PCT wrapped and transparent modes. The transparent mode allows messages to be signed whilst preserving backwards compatibility, so that each message can be read by older non-PCT aware clients and also authenticated by any PCT aware client supporting this mode.

In wrapped mode a Military Message (MM) or Interpersonal Message (IPM) is wrapped in a Cryptographic Messaging Syntax (CMS) envelope, which is placed in the X.400 message content. In transparent mode, the MM or IPM remains as the X.400 content, while the CMS signature is conveyed in an envelope extension.

The implementation includes full checking of Certificate Path and Certificate Revocation Lists and uses Microsoft Cryptographic Service Provider (CSP).

FlashPoint as NATO Reference Implementation of PCT

The Clearswift FlashPoint product provides the reference implementation of PCT in the NATO MMHS Security Demonstrator Programme (MSDP) at NATO C3 Agency in The Hague. This is in active use by a number of nations to test and verify their implementations of PCT.

STANAG 4406 Compliance

FlashPoint is a full implementation of STANAG 4406 (Ed.1 & Ed.2) military messaging with conformance to all mandatory requirements and mandatory functional groups in the AMH91 profile, including optional Functional Groups: MM Distribution List, MM Use of Directory, Civil IPM Interworking, ACP 127 Interworking. The implementation is in turn based on a very full implementation of the civil X.400 standards conformant to 1994 and 1999 editions.

Other relevant products

Clearswift DeepSecure™

Clearswift DeepSecure is an adjunct security product that offers a Common Criteria EAL4 evaluated Military Messaging Firewall. It is designed to link networks of differing security levels, particularly in a JTF (Joint Task Force) where "Eyes Only" caveats may apply, with assured security against network attack and release of classified material. It incorporates Clearswift's award-winning scalable, high-performance, high-availability e-Policy enforcement product. It performs filtering for viruses, malware (Worms, Trojans, etc.), media and content. Its GUI-based management station is available on Windows and provides high visibility of policy hierarchy and inheritances. It can manage multiple and geographically dispersed servers.

Clearswift Bastion™

Using FlashPoint in conjunction with Bastion enables a user to be alerted to the delivery of new messages in a different security domain. For example, a user may have separate workstations for Secret and Restricted networks and separate mailboxes on each, but on each workstation that user will receive new mail alerts from each mailbox to ensure that notification of arrival of important new messages is not delayed because the user is working in the other security domain.

Clearswift Bastion provides Common Criteria EAL4 assured network separation, but can allow the Message Store access protocol to traverse. It can restrict the use of P7 to Alerts only – thus preventing access to messages between security domains whilst permitting Alerts to traverse between security domains.

