

MULTI-PROTOCOL GATEWAY

PROVIDING SECURE TRANSFER AND VALIDATION OF
INFORMATION BETWEEN SECURITY DOMAINS AND SYSTEMS

/// FACT SHEET



The EDS Multi-Protocol Gateway is a security product, enforcing secure policy controlled transfer of information between strategic, tactical and coalition networks within a secured processing environment.

KEY COMPONENTS

- Secured MPG system environment - hardware and software
- TCP/IP Break
- Data Normalisation (XML)
- Information Integrity
- FIPS 140-2 Level 3 Hardware Security Module (HSM) Key Storage
- Integrated EDS Content Verification
- COTS Anti-Virus Support
- Dominance checking
- Security Label checking
- SMTP, ESMTTP and X.400 support
- Hardened Windows 2003 Server Deployment
- Data Assurance
- Comprehensive Auditing
- Remote Management capability

Overview

The EDS MPG is a security product, enforcing validation and integrity of information passing between security domains. The design offers a flexible and highly configurable modular architecture, enforcing deployment-specific policy-based filtering on transactional data passing between systems.

The MPG will facilitate the exchange of operational information in a secured and controlled manner, between strategic, tactical and coalition systems.

Additionally, the MPG can be used as an integration point between disjoint systems, offering data conversion and integrity checking between them.

Information passes through the EDS MPG via a trusted Data Validation Pipeline (DVP), an EDS software component which enforces validation processing on all information passing through each of its configured modules. A pluggable architecture has been adopted within the DVP, allowing both the installation and configuration of validation modules to be tailored on a per deployment basis, including the use of anti-virus, content verification, dominance and security label components.



The DVP has been developed to meet the operational security requirements of hostile environments, and addresses a number of key security objectives. The product has been accepted into the United Kingdom Common Criteria Evaluation Scheme for evaluation to EAL4 product certification.

The MPG is offered as a multi-box Windows 2003 solution, providing separation of policy validation functions from protocol-enabling services via the use of a TCP/IP network break. The modularised solution permits and enforces uni-directional or bi-directional flow and processing of information.

FEATURES

- Windows Server 2003 Operating System
- Data Integrity
- Protection against information leakage
- Protection against software attack
- Integrated COTS products to enhance functionality
- Transaction signing via Integration into a PKI
- Bi or Uni Directional information flow
- Manual transaction release
- Transaction Quarantine

FUTURE CAPABILITY

- Tactical Data Link (Link-16 forwarding and data conversion and fusion, such as Link-16 to Link-11)
- Radar
- ACP145 and STANAG 4406 support
- Web, FTP
- SMS, Chat
- Archiving
- SNMP Trap Generation
- Mixing and data fusion

POINT OF CONTACT

Chris Abbott

CBRN Business Relationship Manager

T: +44 (0)1256 742043

F: +44 (0)1256 742480

E: chris.abbott@d.edl.uk.eds.com

Security

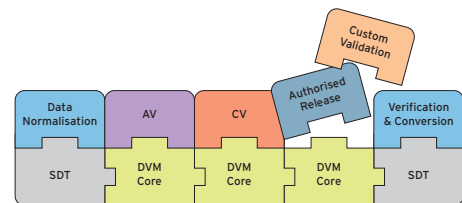
The MPG design is based on using HMG and commercial best practice, and aligns with CESG memorandums and advice. The security design encapsulates:

- Secure Data Transport (SDT), a custom protocol component providing an IP Break (Network Break) within the DVP, breaking end-to-end TCP/IP.
- Data Normalisation (Protocol Break) from the native protocol to a custom extensible MPG XML schema.
- Internal data signing and verification of transactions passing through the MPG, offering data integrity.
- Process signing to assure every transaction has been validated by each security check.
- Secure key protection using tamper resistant FIPS 140-2 Level 3 HSM, using approved encryption and signing techniques.
- Custom MPG Security Lockdown, applicable to both hardware and software.
- Use of COTS products to enhance system security of hardware, system accounts, ports, system files and memory.
- Full auditing of all processing and movement of information through the pipeline.
- Protection against attack via privilege escalation.
- Protection against attack via buffer overflows, execution of unauthorised code, stack pointer manipulation.
- Authorised modifications of transactions permitted, controlled through DVP components.

EDS Data Validation Modules

The DVP consists of a pluggable Data Validation Module (DVM) architecture, offering validation checks on transactions passing through the MPG. Each DVP contains a tailored set of DVMs per deployment, which currently includes (but not limited to):

- Virus scanning using integrated COTS products (McAfee and CA E-Trust currently supported).
- Content Verification filtering of all attachments, including file analysis and white/black list support at a domain level, using EDS' Content Verification Suite.
- Dominance checking of transaction originators and recipients, including cleared to send/receive, support for clearances hosted in directory services.
- Label Mapping between nation policies, plus support for multiple label locations.
- Address Mapping of transaction originator and recipient addresses.
- Customisable validation module functionality for specific deployment needs.



Contact

EDS Defence, 1-3 Bartley Wood Business Park
Bartley Way, Hook, Hampshire RG27 9XA
phone: +44 (0)1256 742000
fax: +44 (0)1256 742612
visit: www.edsdefence.com
visit: www.eds.com



EXPERTISE. ANSWERS. RESULTS.