Secure information sharing at the Tactical Edge

TacEdge IEG secures information sharing for the digital battlefield. It is the first of a new generation data-centric Information Exchange Gateways to provide secure bi-directional information sharing between security domains of equal or different security levels to enable NATO-led missions for enhanced situational awareness.

Information Exchange Gateways, IEGs, are designed to protect their own domain, and only information and services that need to be exchanged are allowed across the IEG to the other security domain.

TacEdge IEG supports any land, naval and air/AEW scenario to enable cross domain communication and MDO tactical missions. The product supports secure sharing of in-formation according to NATO IEG NCS and DCS functionality for central and distributed systems up to NATO Secret, Mission Secret and Svensk Hemlig.

TacEdge IEG software is built from cu-rated open source as well as in-house de-veloped software providing flexibility in what functionality can be offered to Saab's customers. The data plane supports Trusted Domain Separation with strict separation of ports and isolation of virtual machines for secure IEG fucntionality.

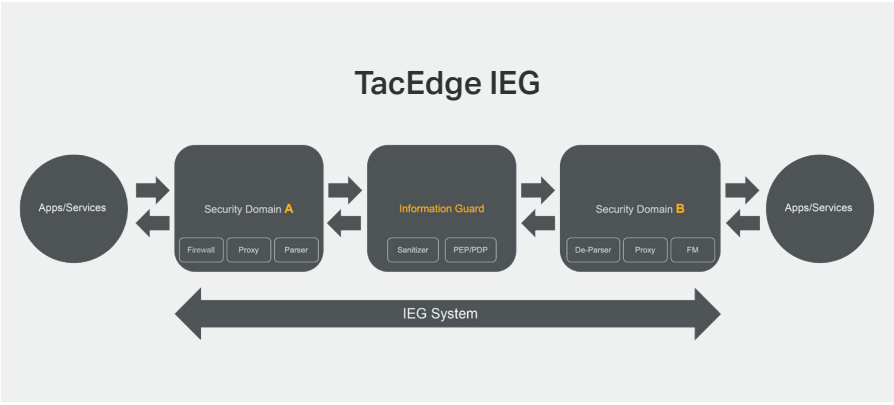
High Assurance

TacEdge IEG is designed for high assurance. Code and processes can be reviewed by customer or governmental authorities for accreditation processes.

TacEdge IEG is being accredited for Common Criteria EAL4+.

Future Proof

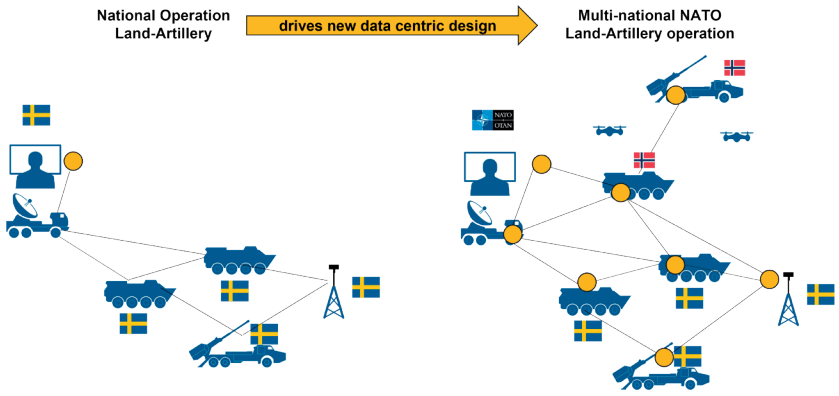
The flexibility of the TacEdge IEG offers customers a path to introduce new features into a trusted and verifiable controlled environment. Future capabilities may include new communication functions and defence against emerging security threats in the digital battlefield.



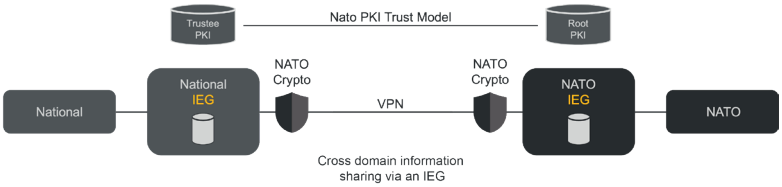
Applications

TacEdge IEG is used where you need to separate two (or more) security domains ei-ther in central solutions between opera-tional and strategic level or at the tactical level in various domains such as air, naval, land, space or combinations in multi-domain use cases.

IEG between two security domains:



An example of a central solution for a nation connecting to NATO:



Key features

- **Designed for NATO IEG and Swedish MoD requirements for an IEG**
  - Enabler for MDO on the tactical level
  - Central solution to connect various Nations/NGO to NATO
- **Federated Mission Networking (FMN) compliant (up to SP5)**
  - FMN functional services
  - FMN core services
  - FMN communication services
- **Data Centric IEG and Network Centric IEG**
- **Key FMN Functional Services**
  - Stateful firewall
  - Proxies
  - Parser and classification of applications
  - Information Guard
  - Sanitizer
- **Key FMN Core services**
  - Chat and instant messaging (XMPP, Jchat)
  - Email (SMTP, Mime, Outlook)
  - Documents (PDF, Excel, Word)
  - MIP, FFT (C2 Land protocols)
  - NATO CSI, NEC CCIS, RAP, JREAP (C2 Air protocols)
  - Voice (SIP, RTP, Tacticall, Skype)
  - Video
  - Web (HTTP, HTTPS, Java-scripts)
  - Sensor data
- **Full suite of Data Centric IEG**
  - Up to Maturity Level 3
  - Data Labelling (STANAG 4774)
  - Data Binding (STANAG 4778)
  - Data Confidentiality and Encryption
  - Data Access Control
  - Meta-data model (STANAG 5636)
  - Security Policy Information Framework (SPIF)
  - Zero Trust Compliant
- **Integrated Trust model with NATO PKI**
  - Root PKI NATO Server and National Trustee PKI Server
- **Trusted domain separation/isolation**
  - Red and black network separation
  - Encryption of transport of data over untrusted/black networks
- **High Assurance**
  - EAL4+

Key benefits

- **Bi-directional protection prevents malware being infiltrated from the inbound security domain and un-authorized information leakage to the outbound security domain**
- **Low latency suitable for tactical use**
- **Tampering protection**
- **Robust denial of service**
- **Up to NATO secret and Svensk Hemlig in the same solution**
- **Software developed by register controlled personnel**
- **NATO CC accreditation**
- **Trusted secure hardware**
- **Formal mathematical proven verification for high assurance and control of the attack surface**
- **Secure hardening**
- **Galvanic separation**
- **Embedded Trusted Linux**
- **Secure and Trusted Hypervisor**
- **Trusted domain separation**
- **Cloud ready environment**

OSL security levels

NATO	Sweden
NATO SECRET	Hemlig (H)
NATO CONFIDENTIAL	Konfidentiell (K)
NATO RESTRICTED	Begränsat hemlig (BH)
NATO UNCLASSIFIED	Sekretessklassificerad (SK)
	Ej Sekretess (ES)

saab.com

SAAB TECHNOLOGIES

SAAB