

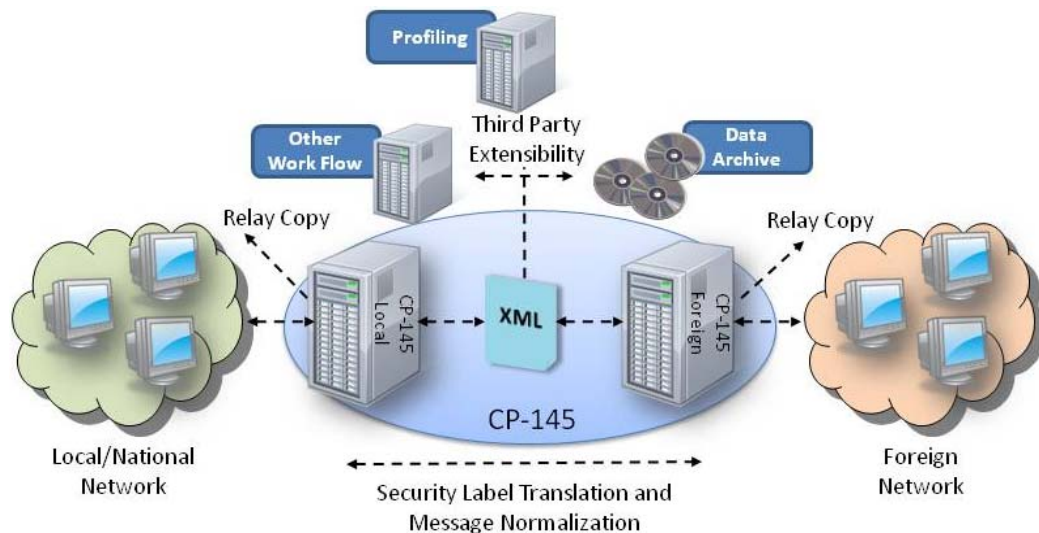


... Provides nation-to-nation connectivity including seamless security policy translation.

The CP-145™ Gateway is an X.400/SMIME-ESS based nation-to-nation gateway per the ACP145 standards set forth by the CCEB (Combined Communications Electronics Board) that facilitates the secure transfer of e-mail between disparate security domains.

CP-145 consists of two subsystems, or 'Elements', each of which offers a discrete X.400/P1 network interface: The Local Element of the CP-145 provides connectivity to the local, national network, whereas the Foreign Element of the CP-145 connects to the external network of the foreign nation. Messages received and transmitted on each network interface are processed in full per the security policy that governs the domain represented by that interface.

Configuration driven and fully audited security label translation services and message normalization are performed to ensure the seamless transfer of messages between the local and foreign domains.



## CP-145 Features . . .

### Message Encryption/Signature Services

- Full SMIME-V3 and/or ACP120 message decryption, encryption, and signature validation processing (incl. CRL checks)

### Security Label Translation

- User configurable Security Policy Translation Tables (SPTTs) define the security label translation rules for message import/export.

### Message Normalization

- Import/export translation rules can be defined for individual message elements-of-service (add, delete, translate).

### Message Virus Scanning

- Message attachments within clear and/or encrypted messages are checked for viruses.

### Message Relay

- All received messages can be relayed to designated external systems for archival/record-management purposes.

### Extensibility

- The internal XML coupling of the gateway supports countless configurations including support for third party modules.



Communications & Power Engineering, Inc.  
Contact: [productinfo@commpower.com](mailto:productinfo@commpower.com)  
[www.commpower.com](http://www.commpower.com)

Message Flow within the CP-145 begins with the reception of an X.400 message on one of its interfaces (local or foreign). For locally originated messages, the CP-145 gateway receives the message at its Local Element X.400 interface. Here the message is validated in full per the local security policy. Once validated, the security label is translated to an exportable version that contains equivalent, mapped values that can be processed by the receiving foreign organization. Also performed, is element-of-service (EOS) mapping to “normalize” unique local e-mail values into standard values that likewise can be processed by the receiving foreign organization.

Once translated, the message is rendered into XML and passed to the Foreign Element of the CP-145 where it is reconstituted into X.400/P772 and SMIME protected using certificates/keys that have been coordinated with the receiving foreign organization. Lastly, the resulting SMIME/X.400 message is transmitted to the foreign organization via an X.400 P1 link.

For foreign to local data flows, identical processing as described above is performed.

Message flow between the Gateway’s discrete Local/Foreign Elements is accomplished via XML services that promote standardization, commerciality, and extensibility within the product.

### **Security features supported by the CP-145 include:**

- **Supported Security Standards.** Two security standards are fully supported within the CP-145 Gateway: SMIME-ESS (Extended Security Services), and ACP120. For each security domain (local/national and foreign), compliant certificate path validation, CRL (revocation) processing, and encryption/decryption services are provided.
- **Security Policy Definition.** Security Policy Information Files (SPIFs) can be created for each supported security domain that define the security policy(s) in effect and the access controls to be enforced.
- **Security Label Translation.** User configurable Security Policy Translation Tables (SPTTs) are used within the Gateway that define the security label translation rules between differing security policies. These tables are signed to prevent unauthorized/undetected tampering and thus can be posted with confidence to the X.500 directory for use by multiple CP-145 Gateways.

### **Other core features of the CP-145 include the following:**

- **Virus Checking.** Third party anti-virus products can be invoked by the CP-145 to scan in-transit messages and their attachments for malicious content.
- **Relay Services.** All received messages can be relayed in X.400 format to designated external systems for archival/record-management purposes.
- **Message Services.** As with all CommPower Military Messaging products, the CP-145 offers full protection, accountability, and recovery for all messages within the Gateway.
- **Third Party Services.** Third party capabilities such as profilers can be installed “in line” to perform additional processing on the XML message as it passes through the Gateway.
- **Extensibility.** Because of the Gateway’s modular architecture, a host of configurations can be realized to allow connectivity to one or more nations, each with a separate security translation policy.

### **CP-145 Status**

The CommPower CP-145 product is a core certified and operational component within the U.S. DMS Program.

### **CP-145 is available directly from CommPower and also via our partners:**

- Lockheed Martin (U.S. DMS)
- Compuat Research Pty Ltd. (Australia)