

SDoT[®] Security Gateway 6.0i

Secure Information Exchange Between Networks with Different Protection Requirements

Background

Topics such as Command & Control (C2), Knowledge Management and Network Enabled Capability are critical to all military areas.

Only the immediate availability of relevant information across network boundaries enables a comprehensive assessment of the particular situation and has a decisive influence on the management process. Compliance with the strict requirements relating to security protection at the domain transition interfaces must therefore be ensured. In other words, the information to be transferred needs to be verified exactly.

SDoT[®] Security Gateway Connects Networks

The product Secure Domain Transition SDoT[®] Security Gateway provides the appropriate solution for this purpose. It is installed at a highly sensitive interface between two differently classified security domains. The SDoT[®] Security Gateway guarantees that all data objects will be monitored, blocking all those which do not meet the confidentiality requirements.

If, for instance, a secret network is connected to a restricted one using the SDoT[®] Security Gateway, the secure filter mechanism ensures that only data objects with a confidentiality level of “restricted” or “unclassified” may flow from the secret domain to the lower classified one. At the same time, and if needed, all data may pass from the restricted network to the secret domain. An additional firewall protects the higher classified domain against potential attacks from the lower classified network.

The SDoT[®] Security Gateway thus provides bidirectional information exchange between networks of different protection requirements.

Approval up to SECRET

Only trustworthy security systems may be used at the high-

ly sensitive network interfaces. As of April, 26th 2017, the German Federal Office for IT Security (BSI) has approved the security and reliability of the SDoT[®] Security Gateway up to GERMAN SECRET. This is a „general approval“ and is therefore not limited to a specific project. It is valid for all use cases and covers NATO CONFIDENTIAL and EU CONFIDENTIAL as well.

The process to achieve a NATO/EU SECRET approval has been started by the BSI and is ongoing.

Content Filtering Made in Germany

The SDoT[®] Security Gateway executes a comprehensive and precise content inspection, and controls the complete information flow at the gateway of two different security domains. The content inspection can be performed automatically as well as manually. Automatic content inspection involves a parser that checks all data concerning structure and content based on a set of rules. Examples for structured data are status information and position coordinates in XML files, nautical data in NMEA 0183 format, radar data in ASTERIX format or Link 16 messages.

Filtering based on security labels

For data that cannot be automatically filtered based on a set of rules, the SDoT[®] Security Gateway provides a service to check an externally generated security label. Instead of performing a content inspection, the confidentiality level enclosed in the security label and the validity of its digital signature will be verified. Because of a strong cryptographic binding, a manipulation of the data object or the security label would be detected immediately.

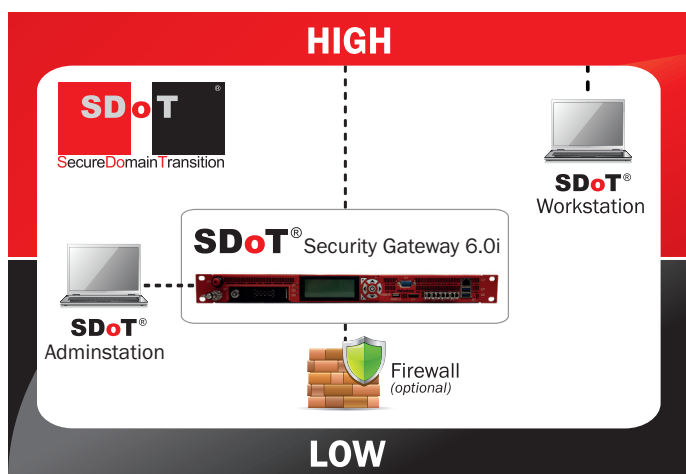
The SDoT[®] Security Gateway supports NATO compliant XML security label. INFODAS GmbH provides a network based system to create such security labels with its product SDoT Labelling Service[®].

Improved Security Architecture

The **SDoT**® Security Gateway 6.0i introduces an all new architecture and achieves an additional improvement of security by implementing a new operation system providing a strong separation. The critical filter mechanisms of **SDoT**® Security Gateway 6.0i are effectively separated from other function by so called “compartments”. The new architecture is based on a fully evaluated version of the microkernel operating system L4, which was specifically modified for the high security needs of **SDoT**®.

Filter mechanisms and all cryptographic functions are separated from the network interfaces by the separation kernel of the operating system. Thus, all critical functions are effectively protected from a direct access by a potential attacker from the lower network as well as from the higher security domain.

The usage of a microkernel operating system enables complete evaluation of the platform and reduces the amount of needed hardware. Our newly introduced special hardware for **SDoT**® Security Gateway 6.0i comprises of a single 19”-server hardware with a height of only one unit.



New Cryptographic Component

SDoT® contains a dedicated hardware component providing cryptographic security functions and an access controlled memory.

Range of Functions

Basics Features

- Supported communication protocols: HTTP, SMTP, TCP, UDP, FTP (with **SDoT**® Data Store)

- Restriction of IP targets possible
- Protection against attack from the LOW network by use of an optional firewall
- Virus checking of transmitted data and filtering of active content by optional firewall
- Comprehensive logging and auditing
- Sending of alarms in case of security violation or incidents
- Remote administration of all components via a comprehensible web interface
- Error protection: An unwanted leakage of classified information is always effectively prevented in case of a faulty configuration, faulty operation, or malfunction.
- Optional high availability variant with failover
- Bandwidth control
- Separation by evaluated microkernel

Data Transfer from HIGH to LOW

- Supported formats using automatic filtering: XML, ADEXP, NMEA0183, ADatP-3, ASTERIX, Link 16, as well as practically all types of structured data
- Supported formats using manual filtering via the Secure Viewer software of the **SDoT** Workstation: ASCII, XML, ADatP-3, monochrome bitmaps, RTF with reduced instruction set, and further formats on request
- All types of files are supported using automated filtering based on externally generated security labels (e.g. with the **SDoT** Labelling Service®)
- Publishing of filtered documents on the **SDoT**® Data Store in order to be accessible by other systems in the lower classified network (HTTP or FTP)
- Online access to web services
- Download lower classified data into the HIGH domain

Data Transfer from LOW to HIGH

- Transmission of all kinds of data using the supported protocols (including SNMP)
- Controlled download via HTTP (**SDoT**® Data Store)
- Controlled data exchange via HTTP (HTTP response is checked)
- Automatic generation of security labels based on the classification of the lower domain. This enables later transmission back into LOW, as long as data remains unchanged.

Summary

Today, INFODAS GmbH provides a flexible and approved solution for the data exchange in cross domain scenarios with the **SDoT**® Security Gateway.