

Nexor Centurion 2.0

In the current military climate of coalition based operations, the requirement to exchange information between different Military Message Handling Systems (MMHS) both nationally and internationally has been widely accepted. CCEB nations are working together to define new standards for secure, trusted communications between one another. These technology standards can be applied both within and between messaging domains to facilitate secure communications between disparate systems.

Nexor has been tracking the emergence of the ACP145 standard and leading the market with a compliant solution. Based upon proven and resilient Nexor technology, Nexor Centurion provides ACP145 functionality at the border, enabling message protocol translation and security between diverse military messaging systems.

Nexor Centurion is a secure messaging gateway that enforces the flow of messages in and out of the organisation using a defined policy allowing different message processing for different domains. As communication agreements are established with different partner organisations, the appropriate policy can be applied for messages to and from those organisations.

The Solution

Nexor Centurion protects messages through the use of digital signatures that are applied and verified on behalf of the domain it protects. These provide three distinct services:

- Content integrity to allow the detection of a message that has been tampered with in transit;
- Authentication providing proof of the originating domain;
- Non-repudiation of origin, preventing the originating domain from denying that the message came from them.

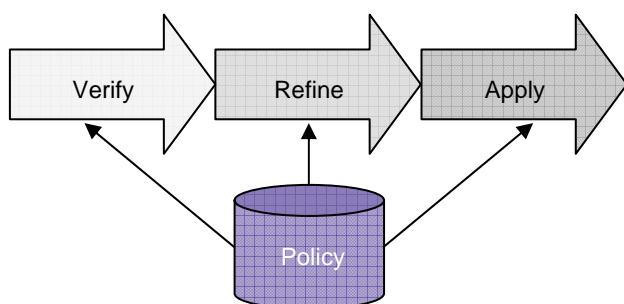


Diagram 1: Message processing

Processing of the messages through Nexor Centurion consists of three distinct steps and is performed in consideration of the security label which indicates how the message should be handled:

- Verify - determines that the policy applies to the message and verifies the message content, including digital signature if present;
- Refine - removes any components (e.g. Digital Signature) that should not be transferred into the destination domain;
- Apply - implements the appropriate security for the destination domain.

In performing these operations a directory service is consulted for appropriate information such as Certificate Revocation Lists (CRLs) and Security Policy Information Files (SPIFs).

Benefits

Interoperability:

- Compliant to emerging ACP145 standard for international interoperability.

Lower total cost of ownership :

- Support of multiple domain policies in one gateway;
- Support for mapping multiple domain label formats, including CCEB, NATO, and North America, additional to ACP145;
- Security-enabling existing infrastructures.

Reduced risk:

- Allows application of centralised security policy;
- Support for controlled transition to secure messaging infrastructure;
- Extends existing, proven Nexor technology.

Platforms

Nexor Centurion is available on:

- Windows 2003 / 2008 Server

Other platforms, including trusted operating systems, may be supported on request.

connect transform protect

NEXOR®

Standards Compliance

- ACP 145 (V1.0 May 2003)
- P772 STANAG 4406/ ACP123
- X.411 Message Transfer System
- X.420 Interpersonal Messaging System
- RFC 2630 Cryptographic Message Syntax
- RFC 2634 Enhanced Security Services
- RFC 2251 LDAP
- Draft RFC Securing X.400 Content with S/MIME
- Draft RFC Transporting S/ MIME Objects in X.400
- X.841 Security Information Objects for Access Control
- SDN.801 Access Control Concept and Mechanisms
- PKCS#12 Personal Information Exchange Syntax
- PKCS#11 Cryptographic Token Interface Standard
- CAPI Microsoft Cryptographic API

Deployment Scenarios

Nexor Centurion provides a means of gatewaying messages as they traverse between two domains that have differing policies and is flexible enough to support a wide range of deployments; from operating as a national boundary to 'security enabling' a speciality product.

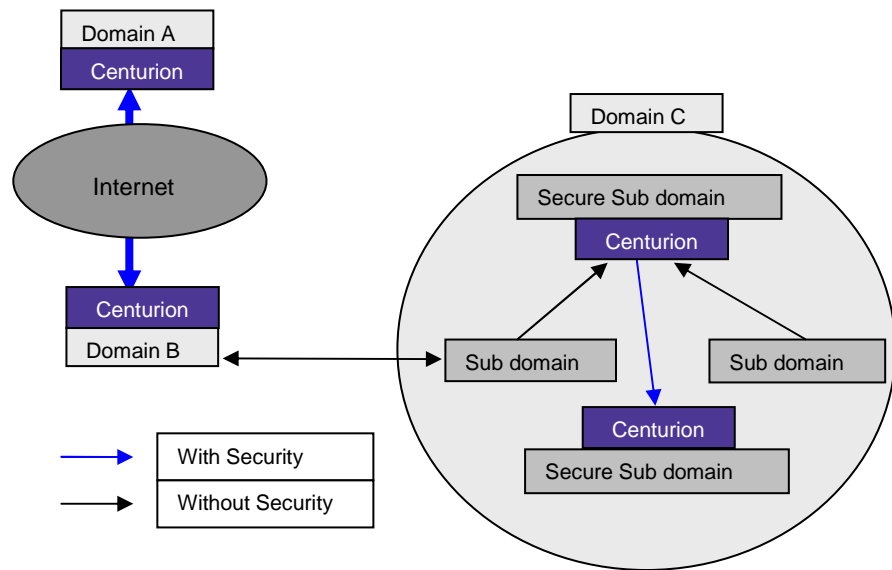


Diagram 2: Deployment Scenarios

Typical scenarios include:

- Security that has been applied to a message within Domain A may not be appropriate for an external Domain B as it may not understand or trust the security. The Nexor Centurion can be used at Domain B to verify the message security, refine the message to simple content and then apply security that Domain B does understand and trust.
- A non-security aware domain may start receiving secure messages from Domain B. In the best case these messages will result in recipients in that domain seeing confusing security dialogues, and in the worst case prevent the recipient from viewing the message at all. By deploying Nexor Centurion, the message security can be verified and then removed for the domain recipients.

Policy Driven Security

Nexor Centurion enables processing of the message to be dependent upon the destination domain. For example, a secure message leaving an internal domain could be:

- Verified, but the security left intact for a recipient domain that understands / trusts the security;
- Verified and refined to simple content for non-security aware domains;
- Verified and the security replaced with the security that the recipient domain understands / trusts.

Labelling

Nexor Centurion provides security label services that can be applied to messages as they cross between domains. These include mapping between security label;

- Locations e.g. from ESS to P1;
- Policies e.g. from NATO to UK;
- Encodings e.g. from SDN.801 to X.841.