An analysis of required authentication of user traffic across networks

Ole-Erik Hedenstad

Norwegian Defence Research Establishment (FFI)

28 September 2012

FFI-rapport 2012/00801

1174

P: ISBN 978-82-464-2157-5
E: ISBN 978-82-464-2158-2

Keywords

Informasjonssikkerhet

Autentisering

Sikkerhetsdomene

Brukstilfeller

Samhandling

Approved by

Ole-Erik Hedenstad	Project Manager
Anders Eggen	Director

English summary

The analysis documented in this report identifies and assesses use cases that require authentication of user traffic across networks. The purpose of the analysis is to show that there exist several use cases where such authentication is needed. The analysis covers remote exchange of user information and also users' access to remote applications. The authentication of user information refers to authentication of various types of information objects, e.g. messages.

Authentication is the process of verifying identities. The identity is proven through something which the entity *is*, *has*, or *knows*. Typical examples are fingerprints, cryptographic keys and passwords. It is usually used in conjunction with authorization and access control.

The following use cases are described and assessed:

a) Civil-Military Cooperation; coordination between coalition units and NGO cells when the coalition forces escort an NGO convoy
b) Military cooperation in multi-domain environment; cooperation between national and coalition units in two security domains (*Mission secret* and *National secret*)
c) Collaboration between coalition units at combat level and tactical level; collaboration in three separate security domains (*Mission unclassified*, *Mission restricted* and *Mission secret*)
d) Cross domain information exchange; extension of use case b
e) Multilevel security (MLS); use case c extended with MLS.

For each use cases we describe collaboration requirements between various actors at the operational level. The actors collaborate in order to perform common tasks, and to complete the tasks they need information and applications that are accessed through the network. Further, for each use case we assess the required authentication, both for remote access to applications and for remote exchange of user information. The assessment gives the required type of authentication and the identities to be authenticated. Why verification of these identities is required is also stated in the assessment.

Sammendrag

I denne rapporten identifiserer og vurderer vi brukstilfeller (use cases) som krever autentisering av brukertrafikk over nettverk. Hensikten med analysen er å vise at det fins flere brukstilfeller hvor slik autentisering er nødvendig. Analysen dekker utveksling av brukerinformasjon og brukerens tilgang til applikasjoner over nettverk. Brukerinformasjon er ulike typer informasjonsobjekter, som for eksempel meldinger.

Autentisering er prosessen for å verifisere identiteter. Identiteten blir bevist ved noe som entiteten *er*, *har* eller *vet*. Typiske eksempler er fingeravtrykk, kryptografiske nøkler og passord. Autentisering brukes vanligvis sammen med autorisering og tilgangskontroll.

Følgende brukstilfeller blir beskrevet og vurdert:

a) Sivilt-militært samarbeid; koordinering mellom koalisjonsenheter og NGO celler når koalisjonsstyrkene eskorterer en NGO konvoi
b) Militært samarbeid mellom nasjonale enheter og koalisjonsenheter; i to separate sikkerhetsdomener (*Mission secret* and *National secret*)
c) Samarbeid mellom koalisjonsenheter på stridsteknisk og taktisk nivå; i tre separate sikkerhetsdomener (*Mission unclassified*, *Mission restricted* and *Mission secret*)
d) Informasjonsutveksling mellom sikkerhetsdomener; utvidelse av brukstilfelle b
e) Flernivåsikkerhet (MLS); brukstilfelle c utvidet med flernivåsikkerhet.

For hvert brukstilfelle beskriver vi behovet for samvirke mellom ulike aktører. Aktørene samvirker for å utføre felles oppgaver, og for å kunne gjennomføre disse trenger de informasjon og tilgang til applikasjoner over nettverk. Vi vurderer dessuten krav til autentisering. Vurderingen angir hvilken type autentisering som kreves og identitetene som må autentiseres. Vurderingen fastslår også hvorfor det er nødvendig å verifisere disse identitetene.

Contents

1 Introduction

The analysis documented in this report identifies and assesses use cases that require authentication of user traffic across networks. The purpose of the analysis is to show that there exist several use cases where such authentication is needed. The analysis covers remote exchange of user information (e.g. messages) and also users' access to remote applications.

It is well known that authentication is required when a user logs on to a local node and that management data and management operations needs authentication. However, the report does not cover these aspects. Authentication of local logon and management aspects have been omitted in order to focus on the need for authentication of user traffic.

Authentication refers to the verification of identities [1]. The identity is proven through something which the entity *is*, *has*, or *knows*. Typical examples are fingerprints, cryptographic keys and passwords. Authentication is usually used in conjunction with authorization and access control.

The work documented in this report supports the FFI project 1174 GISMO's research on authentication, Public Key Infrastructure (PKI) and exploration of new distributed infrastructures for authentication. This research offers scalability analysis and optimization techniques for a PKI [2] and also an alternative to the traditional PKI [3]. Further, the research offers a survey on existing authentication technologies and a comparison of their potential usage in an army tactical setting. GISMO's research in this area also includes a three-level framework for authentication in NBD tactical ad hoc networks [1].

An overview of the use case analysis is given in chapter 0. This chapter starts with describing the threat model adopted for the analysis. Then the method for use case description and assessment is introduced. Chapter 2 also gives definitions and terms. Five use cases are assessed in the next chapters (chapter 3 to 7). Chapter 8 gives a summary of the report.

The following use cases are assessed:

a) Civil-Military Cooperation
b) Military cooperation in multi-domain environment (Mission/National)
c) Collaboration between coalition units at combat level and tactical level
d) Cross domain information exchange – extension of use case b
e) Multilevel security (MLS) – use case c extended with MLS

2 Use case analysis overview

In the use case analysis we identify use cases that require authentication of user traffic across networks. The intention is not to provide a comprehensive study of all possible use cases of this type. It is more to provide a set of good examples showing that several such authentication use cases exist.

For each use case we describe collaboration requirements between various actors at the operational level. Note that the collaboration use cases are at the operational (business) level, not at system or technical level. The actors of a use case collaborate in order to perform common tasks. To complete the task they need information and applications that are accessed through the network. Thus, for each use case the information and applications needed are described.

The actors have one or more communication nodes that are connected to a tactical network. Figure 2.1 illustrates the communication nodes and the tactical network they are connected to. Actor A has a communication node that is directly connected to the tactical network, and actor B (e.g. a military unit mounted on a vehicle) has a local network that is used to connect the actor's communication nodes to the tactical network.

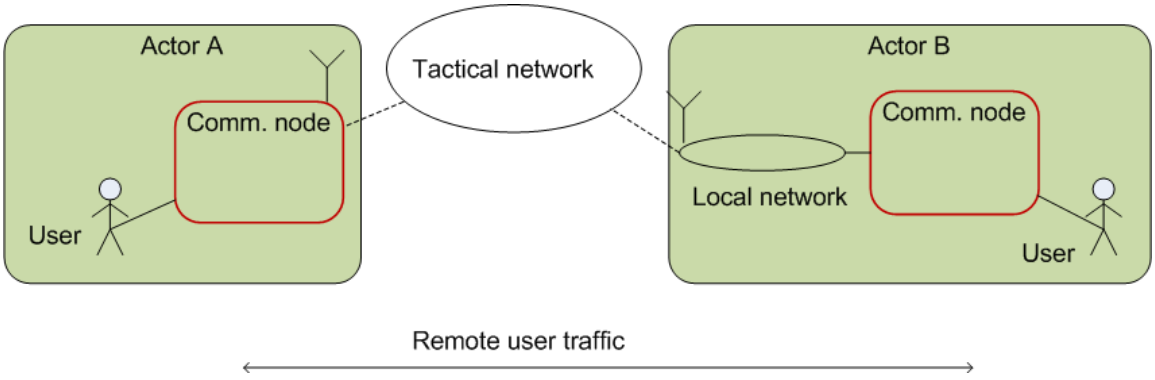

Figure 2.1 Communication nodes and the tactical network

Local user traffic takes place over a short range connection to the communication node or through the local network to another communication node of the actor. *Remote user traffic* refers to exchange of user information (e.g. messages) and users' access to applications through the tactical network.

Authentication refers to the verification of identities. As the objective of the analysis is to assess use cases that require authentication of user traffic across networks, we denote for each use case the types of authentication required and also explain the reason it is required. We distinguish between authentication of remote exchange of user information and authentication of remote access to applications. Authentication of user information refers to authentication of various types of information objects, e.g. messages.

The authentication framework described by Hegland et al. in [1] proposes a three-level framework for authentication in tactical ad hoc networks. Network level hop-by-hop authentication provides the basic protection. It prevents external attackers from being included in the tactical network. The second level is end-to-end application level authentication, which is included only when finer resolution is needed. The third level of authentication relates to physical node access, i.e. the entity authentication of a user that logs on to the local node or remote application.

We use the authentication framework proposed by Hegland et al. as foundation for our analysis. The network level hop-by-hop authentication is used as the basic authentication of user information. Note that an identity at this level can either represent a single network entity or a group of network entities. The second level, end-to-end application level authentication, is used for authentication of user information when finer resolution than provided by the network level authentication is required. At this level all identities represent a single application entity (e.g. single role or application process). We use the third level (physical node access) for authentication of remote access to applications.

The analysis is limited as follows:

- Local logon to a node is not addressed. Only remote user traffic that takes place over the tactical network is addressed
- Management data and operations are not addressed. We only address remote user traffic through the tactical network. It is well known that management data and operations needs authentication. However, these aspects have been omitted to focus on the need for authentication of user traffic
- Use of voice is not addressed
- Key authentication mechanisms, which are needed when public key schemes are used, are not addressed.

2.1 Threat model

The enhanced Dolev-Yao threat model described in [1] is adopted for the use case analysis. The basic Dolev-Yao threat model [4] assumes an active external intruder that can read, modify and redirect all messages, but not decrypt or forge a signature without the correct cryptographic key. In the enhanced model the threat can also originate from insiders with legal physical access to the communication nodes, but who tries to access applications other than those she is authorized to access.

2.2 Use case description and assessment

A use case is described by the following elements:

- **Actors**. The set of actors that participate in the collaboration
- **Tasks**. The common tasks the actors collaborate on
- **Means**. The information and the applications (e.g. short messages, position reports) the actors need to perform the common tasks. Use of voice is outside scope of the analysis
- **Communication infrastructure**. The networks used.

For all use cases the enhanced Dolev-Yao threat model is assumed.

The use case description is followed by a two-stage authentication assessment. First the required authentication of remote access to applications is assessed, and subsequently the required data origin authentication of user information is assessed. The authentication assessment is summarized in one table for each stage.

Remote access to applications require mutual entity authentication. Otherwise the parties cannot be sure who is in the opposite end. Both the client (user, role, client application) requesting remote access and the application itself must be authenticated. Client authentication is needed to establish the client's access privileges and to enforce access control based on these privileges, while application authentication is needed to determine the authorization of the application.

Mandatory access control is required to protect military classified information objects. The mandatory access control will ensure that only authorized subjects get access to an object, because the system controls the access and no individual user can alter that access. We assume the mandatory access control policy is expressed in terms of confidentiality labels attached to subjects and objects. The label contains a security policy identifier and a classification level. We also use this confidentiality label structure to denote the security policy and classification level[1] that applies to the nodes of a security domain.

Mandatory access control is required for remote access to applications when communication nodes of multiple security domains use the same network infrastructure. The mandatory access control will ensure that the client requesting access is authorized to connect to the actual application. This means that both the client and the application must be authenticated so that theirs confidentiality labels can be determined.

For user information two types of authentication can be used. These are data origin authentication and transaction authentication. See section 2.3 for definition of the two types of authentication. Transaction authentication is preferred over message authentication where resilience to replay and other denial-of-service (DoS) attacks are important. In this report we only assess the need for data origin authentication.

[1] More than one classification level if the security domain is MLS.

2.3 Terms and definitions

Terms and definitions from the authentication framework [1]:

- The basic authentication challenge is; *verification of identities of trusted entities communicating in a non-trusted environment that includes entities with different access rights and varying trustworthiness, and where one or more of the trusted entities controls access to a protected resource.*
- The trusted entities are communication nodes communicating over a network, applications inside the communication node or a user communicating with a trusted communication node.
- *Entity authentication* refers to the traditional two or three step protocol where the supplicant convinces the authenticator that he is currently communicating with the identity claimed by the supplicant. Then the protocol terminates. The *authenticator* controls access to a protected resource. The supplicant tries to get access by being authenticated by the authenticator through an authentication protocol.
- *Data origin authentication (message authentication)* assures the receiver (authenticator) that the message at some point in time originated from the claimed source (supplicant). The two main effects of data origin authentication are verification of the originator and verification of the binding between the originator and the content – including integrity protection of the message content.
- *Transaction authentication* is parallel to data origin authentication, but includes time-variant parameters that enable the receivers to detect the timeliness of the message.
- *Identity and identifiers*: The *identity* specifies a unique entity, for instance a user, a role, an application or a host. The identity is represented by one or more *identifiers* – for instance a number or a text string. An entity can also be a *group* of entities referred to by a single identifier.

Mandatory access control [5]: When a system mechanism controls access to an object and an individual user cannot alter that access, the control is a *mandatory access control*.

A *security domain* is defined as a collection of entities to which a single security policy enforced by a single authority [6] applies.

Publish/subscribe communication is where one application (the publisher) “publishes” a message on a particular topic, and all the applications that have “subscribed” to this topic receive the message.

The Transport Network concept from the The CoNSIS (Coalition Network for Secure Information Sharing) project [7]: The transport network (TN) is a network that connects coloured enclaves. The coloured enclaves are plaintext networks or individual communication nodes where users connect. They are separated from the TN by encryption devices. Access control is enforced on all connections and the TN only includes authenticated nodes.

The protected core network concept [8] uses the terms protected core network (PCN) for TN and coloured clouds for coloured enclaves. Access control is enforced on all connections and the PCN only includes authenticated nodes, as for TN. The CoNSIS terms are used in this report.

3 Civil-Military Cooperation

The use case assessed in this section is civil-military cooperation between NGO (Non Governmental Organization) units and military units of a coalition force. The civil-military cooperation takes place within a Civil-Military Cooperation (CIMIC) security domain. At the same time the military units collaborate in a separate coalition security domain in order to coordinate the military operation.

3.1 Case description

Actors: The actors involved are NGO cells mounted on civilian vehicles and coalition units mounted on military vehicles. The vehicle-mounted military units are at the combat level (platoon, squad) and belong to a coalition manoeuvre group. A headquarter staff at the tactical level is also involved.

Tasks: The task addressed in this use case is coordination between the coalition units and the NGO cells when the coalition forces' operations are executed. In addition all the coalition units manage and coordinate the military operation within the coalition security domain.

Means: A distinctive feature of this use case is that communication nodes of two security domains use the same communication infrastructure. We use the confidentiality label structure to denote the security policy and classification level that applies to the entities of the security domains. The relevant labels in this use case are *Mission restricted* and *CIMIC unclassified*. The *Mission restricted* label applies to the communication nodes in the coalition security domain and the *CIMIC unclassified* label applies to the nodes in the CIMIC security domain. Note that each node belongs to only one security domain.

The use case is illustrated by three units in Figure 3.1. The HQ staff and the coalition unit mounted on military vehicle have two nodes each, one for each security domain. The NGO cell have one node that belongs to the *CIMIC unclassified* domain.

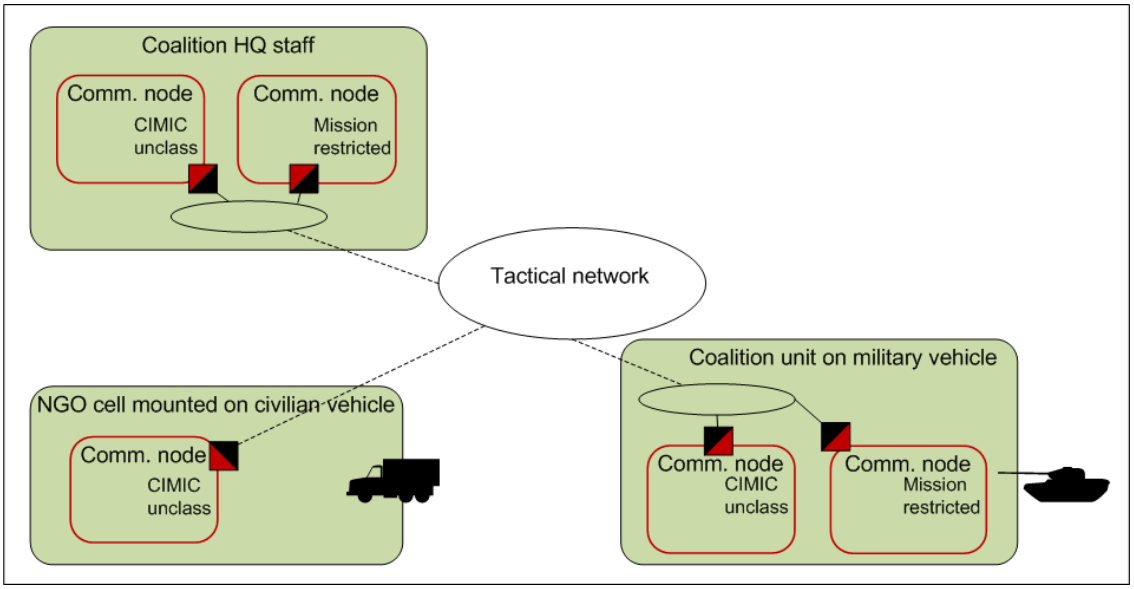

Figure 3.1 Civil-Military Cooperation

The use case is based on the scenario developed in the CoNSIS project [7]. This scenario takes place in a country torn by civil war, and an international coalition is involved in this conflict to protect civilians and initiate the peace process. In one part of the scenario coalition forces escort an NGO convoy to a disaster area.

The applications offered to the actors are:

- Messaging services (e.g. coordination and status messages) in both security domains. The services supports formal, informal and short messages
- Position report service; publish/subscribe type of service in both security domains
- Alert/warning service at combat level; publish/subscribe type of service in both security domains

Communication infrastructure: A coalition tactical network is used for secure information sharing between the actors. The network is managed by the coalition, and the NGO cells are allowed to connect to the network for the purpose of civil-military cooperation. The NGO cells use a civilian wireless network that is connected to the coalition network via an access point located at one of the military vehicles of the convoy.

There are local networks at the coalition HQ staff and at the coalition unit on the military vehicle. The tactical network and the local networks are all segments of a protected transport network (TN). As described in section 2.3, the TN concept is to connect coloured enclaves to the transport network. The coloured enclaves are either plaintext networks or individual communication nodes where users connect. In this use case all coloured enclaves are communication nodes because the two local networks are segments of the TN.

Each coloured enclave (i.e. communication node in this case) is separated from the transport network by an encryption device. This applies to both the *Mission restricted* and the *CIMIC unclassified* coloured enclaves. The encryption device provides confidentiality protection of data before the data enters the transport network.

3.2 Assessment

In this section we assess the required authentication, both for remote access to applications and for remote exchange of user information. Note that authentication of user information refers to authentication of various types of information objects, e.g. messages. The assessments are summarized in Table 3.1 for remote access and in Table 3.2 for remote exchange of user information. The required type of authentication and the identities to be authenticated are denoted in the *Auth. required* and *Identities* columns respectively. The *Reason/comment* column states why verification of the identities denoted in the *Identities* column is required.

We assume the basic hop-by-hop network authentication is used by the transport network so that only authenticated nodes are included in the network. This means that NGO traffic is the only civilian traffic that will be forwarded in the transport network.

Table 3.1 shows that authentication is required for all three application services in order to determine the communicating peer's security domain (denoted by its confidentiality label). For the two publish/subscribe services authentication is also required to determine the subscriber's additional access privileges and to determine the service provider's authorization.

Note that encryption devices provide confidentiality protection before the data enters the transport network. If the security policy permits, the implicit authentication achieved through the possession of the correct key, can be used to determine the security domain of the peer. It is the proper encryption and decryption of the messages that shows that the sending and receiving party possesses the correct key.

We assess that formal messages exchanged in the *Mission restricted* security domain require data origin authentication at application level, see Table 3.2. This fine-grained authentication is necessary because the consequences of forged information is assessed to be serious (can cause serious damage to the ongoing operation). However, the other user information types may be authenticated at the network level. Network level authentication is assessed to be sufficient for these information types, because the consequences of forged information is assessed to be medium (can delay processes of the ongoing operation).

Services	Auth. required	Identities	Reason/comment
Publish/subscribe services (in both domains): - position report service - alert/warning service	Provider's authentication of subscriber	User/Role /Appl	Needed to determine the subscriber's domain (to verify that the subscriber's security domain is the same as the provider's). Also needed to determine the subscriber's additional access privileges.
	Subscriber's authentication of service provider (publisher)	Role/Appl	Needed to determine the service provider's domain (to verify that the provider's security domain is the same as the subscriber's). In addition needed to determine the service provider's authorization.
Messaging service (in both domains)	Authentication of sender and receiver entities	Appl	Needed to determine each entity's security domain (to verify that the security domain of the entities is the same).
Appl = Application (refers to a specific process) User = Specific operator Role = User in specific role Note: Confidentiality protection is provided by encryption devices. If the security policy permits, the implicit authentication achieved through the possession of the correct key, can be used to determine the security domain of the peer.			

Table 3.1 Assessment of remote access –use case Civil-Military Cooperation

User information object	Auth. required	Identities	Reason/comment
Formal messages (orders, status reports); used in *Mission restricted* domain	Data origin authentication at application level (end-to-end)	Role	The consequences of forged formal messages is assessed to be severe (can destroy the ongoing operation). Authentication with finer resolution than provided by the network level authentication is needed.
Informal messages (e-mail) for coordination; used in both domains	Data origin authentication at network level (hop-by-hop)	Host/Appl	The consequences of forged information of these types is assessed to be medium (can delay processes of the ongoing operation). Network level authentication is assessed to be sufficient.
Position Reports; used in both domains			
Alert messages from combat level; used in both domains			
Short messages; used in both domains			
Appl = Application (refers to a specific process) Host = Communication node or hardware device Role = User in specific role			

Table 3.2 Assessment of user information–use case Civil-Military Cooperation

4 Military cooperation in multi-domain environment

The use case assessed in this section is military cooperation in a multi-domain environment. Coalition partners from different nations collaborate in a *mission* security domain. At the same time the coalition units collaborate with their national units in separate *national* security domains. Note that only the Norwegian national domain is explicitly included in the use case.

4.1 Case description

Actors: The actors involved are a coalition staff at the battalion level, a coalition unit #2, a Norwegian battalion staff and a Norwegian HQ. The two battalion staffs take part in a coalition operation.

Tasks: The task addressed is coordination between the Norwegian battalion staff, the coalition partner staff and coalition unit #2 when executing the coalition operation. In addition the Norwegian battalion staff coordinates with the Norwegian HQ. The use case is illustrated in Figure 4.1.

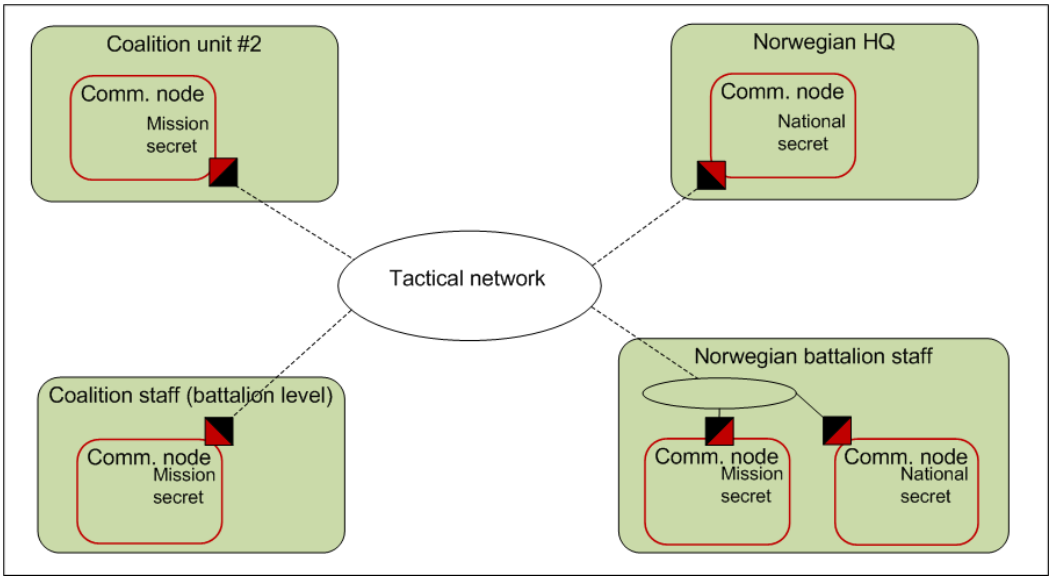

Figure 4.1 Military cooperation in multi-domain environment

Means: In this use case communication nodes of two security domains use the same communication infrastructure. The two security domains are denoted by the confidentiality labels *Mission secret* and *National secret* (Norwegian "Hemmelig"). The *Mission secret* security domain is used for coalition information exchange between the coalition staff, the Norwegian battalion staff and coalition unit #2, while the *National secret* security domain is used for information exchange between the Norwegian battalion staff and the other national unit.

Note that in this use case each node belongs to only one security domain. An alternative is that a communication node provides separate partitions (virtual machines), which enable the same node to host both a *Mission secret* and a *National secret* partition. Partitioned mode of operation with

cross domain information exchange is another alternative for controlling access to information, and this option is introduced in the use case described in section 6.

Applications offered to the actors:

- Messaging services (orders, status reports, coordination) in both security domains. The services supports formal, informal and short messages
- Coalition shared database (CSD) service; pull type of service in *Mission secret* domain
- Situation picture service; publish/subscribe type of service in both domains
- Position report service; publish/subscribe type of service in *Mission secret* domain
- Sensor (observation) service; publish/subscribe type of service in *National secret* domain

Communication infrastructure: A coalition tactical network is used for secure information sharing between the actors. All network segments, including the local network at the Norwegian battalion staff, are part of a protected transport network (TN). As noted earlier, the TN concept is to connect coloured enclaves to the transport network. Also in this use case all coloured enclaves are communication nodes because the local network at the Norwegian battalion staff is part of the TN.

Each coloured enclave (i.e. communication node in this case) is separated from the transport network by an encryption device. This applies to both the *Mission secret* and the *National secret* coloured enclaves. The encryption device provides confidentiality protection before data enters the transport network.

4.2 Assessment

In this section the required authentication is assessed, both for remote access and for remote exchange of user information. The basic hop-by-hop network authentication is used by the transport network so that only authenticated nodes are included in the network, which is the same assumption as for the other use cases.

The assessment of remote access to applications is shown in Table 4.1. The confidentiality labels given in brackets denote the security domain of the services.

All five services require authentication in order to determine the communicating peer's security domain. The publish/subscribe and pull services also require authentication to determine the client's additional access privileges and to determine the service provider's authorization. The assessment of this use case is in principal the same as the assessment of the CIMIC use case (section 3.2). The difference is that the CIMIC use case has fewer services and does not include pull services.

We assess that formal objects require data origin authentication at application level, see Table 4.2. These are formal messages and objects stored in the situation picture and the coalition shared database. The other user information types may be authenticated at the network level. Compared

to the CIMIC use case assessed in section 3.2, fewer user information objects require application level authentication in the CIMIC use case.

Services	Auth. required	Identities	Reason/comment
Publish/subscribe services: - situation picture (in both domains) - position report (*Mission secret*) - sensor (*National secret*) Pull service: - coalition shared database (*Mission secret*)	Provider's authentication of client (subscriber, consumer)	User/Role /Appl	Needed to determine the client's domain (to verify that the client's security domain is the same as the provider's). Also needed to determine the client's additional access privileges.
	Client's authentication of service provider (publisher)	Role/Appl	Needed to determine the provider's domain (to verify that the provider's security domain is the same as the client's). In addition needed to determine the service provider's authorization.
Messaging service (in both domains)	Authentication of sender and receiver entities	Appl	Needed to determine each entity's domain (to verify that the security domain of the entities is the same).
Appl = Application (refers to a specific process) User = Specific operator Role = User in specific role Note: Confidentiality protection is provided by encryption devices. If the security policy permits, the implicit authentication achieved through the possession of the correct key, can be used to determine the security domain of the peer.			

Table 4.1 Assessment of remote access – Military cooperation in multi-domain environment

User information object	Auth. required	Identities	Reason/comment
Formal messages (orders, status reports); used in both domains	Data origin authentication at application level (end-to-end)	Role	The consequences of forged information of these types is assessed to be severe (can destroy the ongoing operation). Authentication with finer resolution than provided by the network level authentication is needed.
Formal objects in the situation picture (both domains) & coalition shared database (*Mission Secret* domain): – Recognized situation picture – Recognised reports on own operational status (combat status) – Recognised reports providing logistics assessments – Warnings providing assessments of the CBRN situation			
Informal messages (e-mail) for coordination; used in both domains	Data origin authentication at network level (hop-by-hop)	Host/Appl	The consequences of forged information of these types is assessed to be medium (can delay processes of the ongoing operation). Network level authentication is assessed to be sufficient.
Position Reports; used in *Mission Secret* domain			
Sensor observations; in *National secret* domain			
Short messages; used in both domains			
Appl = Application (refers to a specific process) Host = Communication node or hardware device Role = User in specific role CBRN = Chemical, Biological, Radiological and Nuclear			

Table 4.2 Assessment of user information- Military cooperation in multi-domain environment

5 Collaboration between units at combat and tactical level

In this section the use case assessed is military collaboration between coalition units at combat and tactical level. The coalition partners collaborate in three separate security domains. These are the *Mission unclassified*, *Mission restricted* and *Mission secret* domains.

5.1 Case description

Actors: The actors involved are two vehicle mounted infantry units at combat level, a HQ staff at tactical level and a reconnaissance unit. The vehicle mounted units belong to a coalition manoeuvre group.

Tasks: Two tasks are addressed in this use case. One task is the command and control of combat units when executing the coalition operation. The other task is management of unmanned sensors. A reconnaissance unit is responsible for the unmanned sensors and their communication equipment. The HQ staff collects and analyses information from the unmanned sensors that the reconnaissance unit has placed at various locations along roads. The use case is illustrated in Figure 5.1.

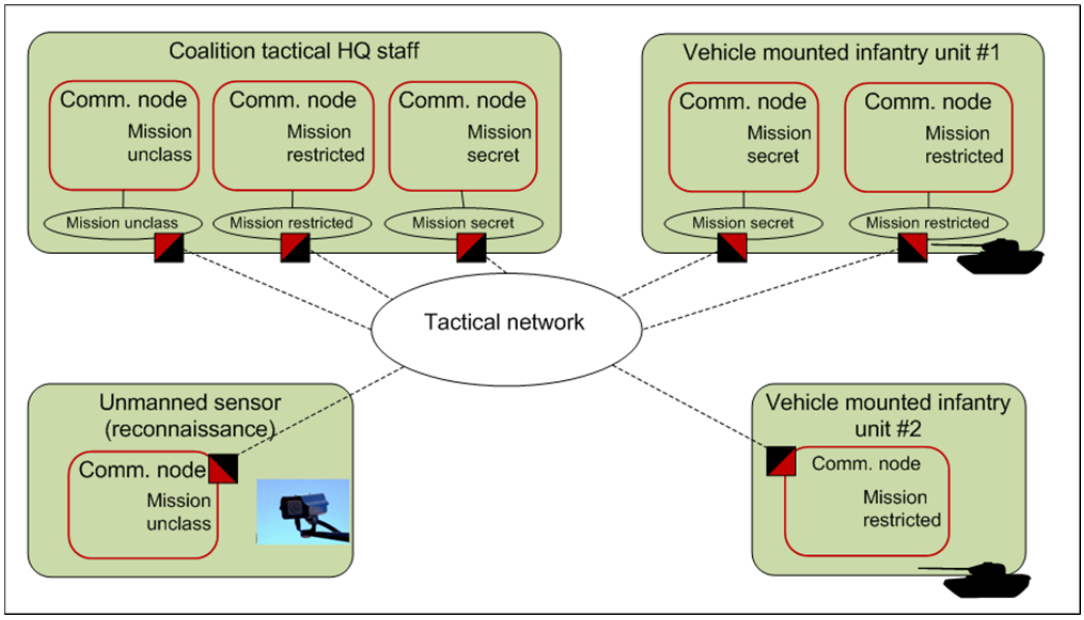

Figure 5.1 Collaboration between units at combat and tactical level

Means: A distinctive feature of this use case is that communication nodes of three security domains use the same communication infrastructure. The three security domains are denoted by the confidentiality labels *Mission unclassified*, *Mission restricted* and *Mission secret*. Command and control information is exchanged in the *Mission restricted* and the *Mission secret* security domains. The *Mission unclassified* security domain is used for remote control of the sensors and for collecting sensor data.

Note that also in this use case each node belongs to only one security domain. As mentioned in section 4.1, an alternative is that a communication node provides separate partitions (virtual machines), which enable the same node to host one partition for each security domain. Multilevel mode of operation is another alternative for controlling access to information, and this option is introduced in the use case described in section 7.

Application support:

- Messaging services (orders, status reports, coordination) in the *Mission restricted* and *Mission secret* domains. The services supports formal, informal and short messages
- Situation picture service; publish/subscribe type of service provided by the tactical HQ in the *Mission secret* domain
- Coalition shared database service; pull type of service provided by the tactical HQ in the *Mission restricted* and *Mission secret* domains
- Position report service; push type of service in the *Mission restricted* domain

- Alert/warning service (both from infantry units at combat level to higher level and the other way around); push type of service in the *Mission restricted* domain
- Sensor data collection service; publish/subscribe type of service provided by the unmanned sensors in the *Mission unclassified* domain
- Remote control service provided by the unmanned sensors in the *Mission unclassified* domain.

Communication infrastructure: A coalition tactical network is used for secure information sharing between the actors. This tactical network is part of a protected transport network (TN). As noted earlier, the TN concept is to connect coloured enclaves to the transport network. There are three local networks at the coalition HQ staff, one for each of the three security domains, and two local networks at the vehicle mounted infantry unit #1. All these local networks are coloured enclaves (i.e. plaintext networks) and are not part of the transport network. In addition we have coloured enclaves at the infantry unit #2 and at the unmanned sensor. Both these coloured enclaves are communication nodes. This means we in this use case have coloured enclaves of two types; both the *plaintext network* and the *communication node* types.

Each coloured enclave (both the *plaintext network* and the *communication node* types) is separated from the transport network by an encryption device. This applies to the *Mission unclassified*, the *Mission restricted* and the *Mission secret* coloured enclaves. The encryption device provides confidentiality protection before the data enters the transport network.

5.2 Assessment

In this section the required authentication is assessed, both for remote access and for remote exchange of user information. The basic hop-by-hop network authentication is used by the transport network so that only authenticated nodes are included in the network, which is the same assumption as for the other use cases.

The authentication requirements for remote access to applications are assessed in Table 5.1. The confidentiality labels given in brackets denote the security domain(s) of the services.

Services	Auth. required	Identities	Reason/comment
Publish/subscribe service: - situation picture (*Mission secret*) Pull service: - coalition shared database (*Mission restricted & secret*)	Provider's authentication of client (subscriber, consumer)	User/Role /Appl	Needed to determine the client's domain (to verify that the client's security domain is the same as the provider's). Also needed to determine the client's additional access privileges.
	Client's authentication of service provider (publisher)	Role/Appl	Needed to determine the service provider's domain (to verify that the provider's security domain is the same as the client's). In addition needed to determine the service provider's authorization.
Services provided by unmanned sensors (*Mission unclassified*): - Remote control - Sensor data collection	Provider's authentication of client	User/Role /Appl	Needed to determine the client's access privileges. Will prevent that unauthorized clients modify the settings of the sensors or read sensor data. May also be needed to verify that the client's domain is *Mission unclassified*.
	Client's authentication of service provider	Role/Appl	Needed to determine the service provider's authorization. Will prevent that false sensors are introduced.
Messaging service (*Mission restricted & secret*) Position report service (*Mission restricted*) Alert/warning service (*Mission restricted*)	Authentication of sender and receiver entities	Appl	Needed to determine each entity's domain (to verify that the security domain of the entities is the same).
Appl = Application (refers to a specific process) User = Specific operator Role = User in specific role Note: Confidentiality protection is provided by encryption devices. If the security policy permits, the implicit authentication achieved through the possession of the correct key, can be used to determine the security domain of the peer.			

Table 5.1 Assessment of remote access - collaboration between actors at combat and tactical level

We assess that formal messages (including warning messages from higher levels) and formal objects stored in the situation picture and the coalition shared database require data origin authentication at application level, see Table 5.2. The other user information types may be authenticated at the network level.

User information object	Auth. required	Identities	Reason/comment
Formal messages (orders, status reports); used in *Mission restricted* and *Mission secret* domains	Data origin authentication at application level (end-to-end)	Role	The consequences of forged information of these types is assessed to be severe (can destroy the ongoing operation). Authentication with finer resolution than provided by the network level authentication is needed.
Alerts from higher level; used in *Mission restricted* domain			
Formal objects in the situation picture & coalition shared database: – Recognized situation picture – Recognised reports on own operational status (combat status) – Recognised reports providing logistics assessments – Assessments of the CBRN situation			
Informal messages (e-mail) for coordination; used in *Mission restricted* and *Mission secret* domains	Data origin authentication at network level (hop-by-hop)	Host/Appl	The consequences of forged information of these types is assessed to be medium (can delay processes of the ongoing operation). Network level authentication is assessed to be sufficient.
Position Reports; used in *Mission restricted* domain			
Alert messages from combat level; used in *Mission restricted* domain			
Short messages; used in *Mission restricted* and *Mission secret* domains			
Sensor data; used in the *Mission unclassified* domain			
Appl = Application (refers to a specific process) Host = Communication node or hardware device Role = User in specific role CBRN = Chemical, Biological, Radiological and Nuclear			

Table 5.2 Assessment of user information - collaboration between actors at combat and tactical level

6 Cross domain information exchange

The use case assessed in this section extends the use case described in section 4 with cross domain information exchange.

6.1 Case description

Actors: The actors that participate in the collaboration are the same actors as described in section 4.

Tasks: The tasks the actors collaborate on are also the same as described in section 4.

Means: The relevant confidentiality labels for this use case are *Mission secret* and *National secret*, which are the same labels as described in section 4. The new aspect introduced in this use case is that the communication node at the Norwegian battalion staff performs controlled information exchange between the *Mission secret* and the *National secret* security domains. This node is the only one that handles both the *Mission secret* and the *National secret* confidentiality labels. The other Norwegian node and the two *coalition* nodes handle one confidentiality label, respectively *National secret* and *Mission secret*. The use case is illustrated in Figure 6.1.

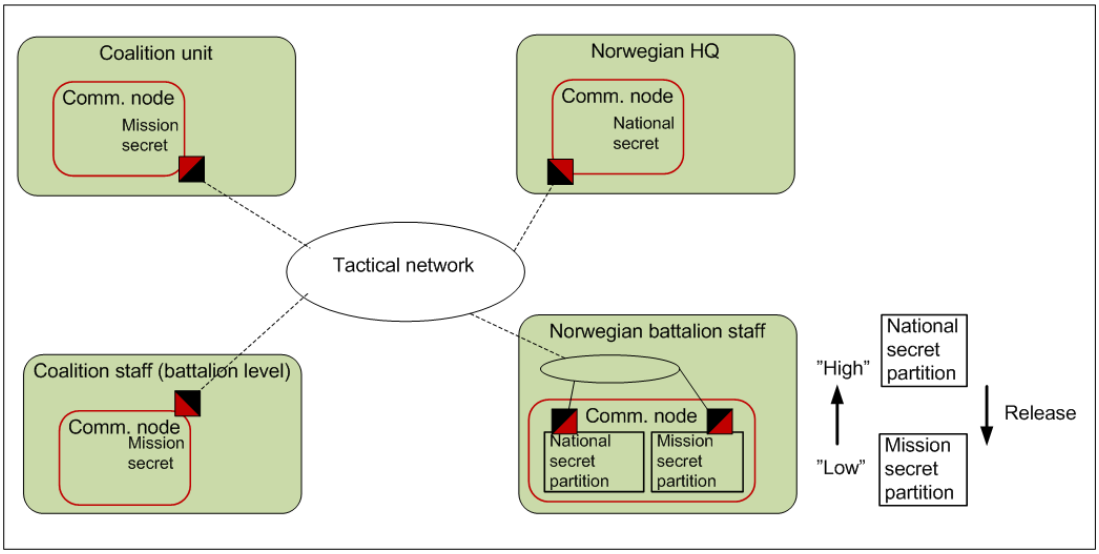

Figure 6.1 Cross domain information exchange

The *system high* mode of operation [9] is applicable for the *coalition* nodes and for the node at the Norwegian HQ, as these nodes handle one confidentiality label and all users of the system are authorized for this confidentiality label. However, this mode of operation is not applicable for the node at Norwegian battalion staff. This node handles multiple confidentially labels and the applicable mode of operation is *partitioned* [9]. In this mode the authorization of users must be controlled before access to data is granted.

We assume that the node at the *Norwegian* battalion staff runs in *partitioned mode of operation*. This *partitioned mode* node will have two partitions:

- *National secret* partition. The users in this partition are authorized for both *National secret* and *Mission secret*. This partition will handle (1) *National secret*, (2) *Mission secret* and (3) *Secret information released to National and/or Mission*.
- *Mission secret* partition. The users in this partition are authorized for *Mission secret* only. This partition will handle (1) *Mission secret* and (2) *National secret information released to Mission*.

Information can now flow from the *Mission secret* partition to the *National secret* partition, because the *Mission secret* label is considered to be “lower” than the *National secret* label. Information may also flow in the other direction from the *National secret* to the *Mission secret*

partition. However, such information flow can only be initiated by users that are authorized to release *National secret* information objects to the *Mission secret* domain. These information objects are labeled "*National secret information released to Mission*".

The *partitioned* mode of operation allows users of the *National secret* domain to access both *National secret* and *Mission secret* information from the same application. This feature, which is not provided by the use case described in section 4, facilitate users' access to information.

An implementation of a *partitioned mode* node will include one or more applications that are *partitioned mode* capable, i.e. support allowed information flow between the two partitions. We assume, for information flow in the direction from the *Mission secret* to the *National secret* partition, that the Norwegian battalion node implement the following *partitioned mode* capable applications:

- Messaging (supports formal and informal messages)
- Coalition shared database
- Situation picture
- Position report

In addition we assume that the *partitioned mode* implementation provides an application that is used by authorized users to release information objects from the *National secret* to the *Mission secret* partition.

Communication infrastructure: The communication infrastructure is the same as described in section 4.

6.2 Assessment

The communications within the National secret domain and within the Mission secret domain have been assessed in section 4 and are not further discussed. In the following only user information that cross the two partitions are addressed.

Mission secret information objects can flow to the *National secret* domain, and we assess that these objects need to be authenticated as shown in Table 6.1. In addition *National secret* information can be released by authorized users and written to the *Mission secret* domain. We assess that these objects need to be authenticated as shown in Table 6.2.

User information object	Auth. required	Identities	Reason/comment
Mission secret formal messages (orders, status reports)	Data origin authentication at application level (end-to-end)	Role	The consequences of forged information of these types is assessed to be severe (can destroy the ongoing operation).
Mission secret formal objects in the situation picture & coalition shared database, as detailed in Table 4.2			
Mission secret informal messages (e-mail) for coordination	Data origin authentication at network level (hop-by-hop)	Host/Appl	The consequences of forged information of these types is assessed to be medium (can delay processes of the ongoing operation).
Mission secret position Reports			
Appl = Application (refers to a specific process) Host = Communication node or hardware device Role = User in specific role			

Table 6.1 Assessment of user information– from Mission secret to National secret domain

User information object	Auth. required	Identities	Reason/comment
National secret formal messages (orders, status reports)	Data origin authentication at application level (end-to-end)	Role	The consequences of forged information of these types is assessed to be severe (can destroy the ongoing operation).
National secret formal objects in the situation picture services, as detailed in Table 4.2			
National secret informal messages (e-mail) for coordination	Data origin authentication at network level (hop-by-hop)	Host/Appl	The consequences of forged information of these types is assessed to be medium (can delay processes of the ongoing operation).
National secret sensor observations			
Appl = Application (refers to a specific process) Host = Communication node or hardware device Role = User in specific role			

Table 6.2 Assessment of user information– from National secret to Mission secret domain

7 Multilevel security (MLS)

This use case enhances the use case described in section 5 (Collaboration between units at combat and tactical level) with multilevel functionality.

7.1 Case description

Actors: The actors that participate in the collaboration are the same actors as described in section 5. We assume that multilevel functionality is needed for the HQ staff and for some of the units at the combat level.

Tasks: The tasks the actors collaborate on are also the same as described in section 5.

Means: In this use case we introduce the confidentiality label *Mission MLS* to denote a security domain that can handle multilevel functionality. The communication nodes of a *Mission MLS* domain are all MLS capable and can handle the three classification levels *unclassified, restricted* and *secret*. The *multilevel* policy expressed by the Bell-LaPadula security model [10] will regulate the allowed read and write operations. This policy allows information to flow from low to high classification level. The *multilevel mode of operation* described in [9] is applicable for the nodes of the *Mission MLS* security domain.

In this use case we still have communication nodes both at the HQ and combat level that handle a single confidentiality label. These single level nodes either belong to a *Mission secret, Mission restricted* or *Mission unclassified* security domain (as described section 5). The application support for the single level nodes is as described in section 5. The use case is illustrated in *Figure 7.1*.

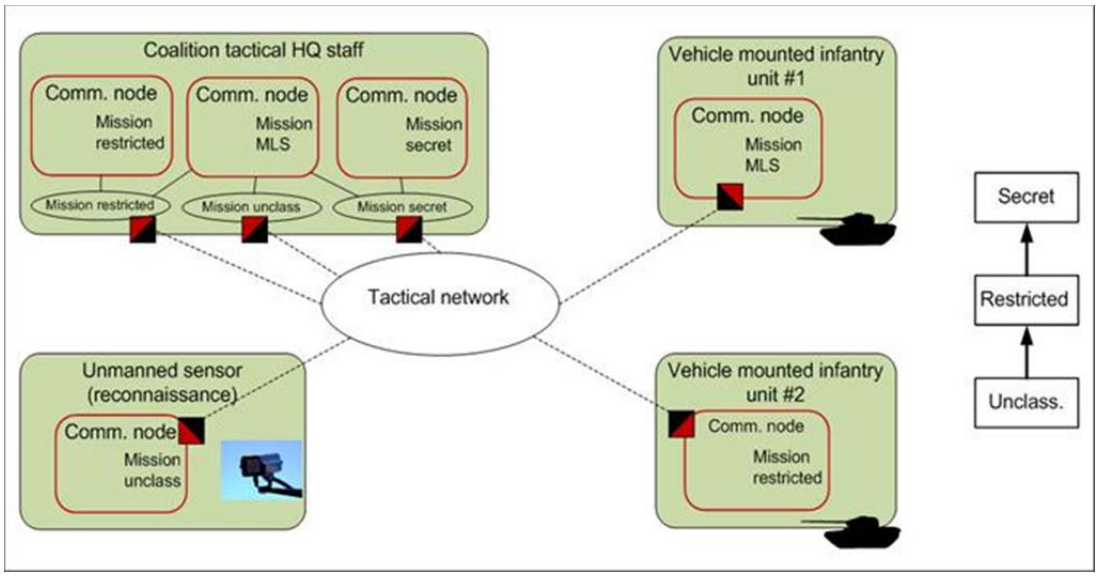

Figure 7.1 Multilevel security

The multilevel mode of operation allows users of the *Mission MLS* nodes to read lower classified information from an application at a higher classification level. This feature, which is not provided by the use case described in section 5, facilitate users' access to information.

An implementation of an MLS node will include one or more applications that are MLS capable, i.e. support allowed information flow between the three classification levels *unclassified, restricted* and *secret*. We assume that the MLS nodes implement the following MLS capable applications:

- Messaging (supports formal and informal messages)
- Coalition shared database; provided by the tactical HQ
- Position report
- Alert/warning
- Sensor data collection

Communication infrastructure: The communication infrastructure is with one exception the same as described in section 5. The exception is that the two local networks (*Mission restricted* and *Mission secret*) at the vehicle mounted infantry unit #1 are not part of the infrastructure any more.

7.2 Assessment

In this section we assess the authentication requirements for the MLS use case.

The authentication requirements for remote access to applications are assessed in Table 7.1. Note that both MLS capable applications and single level applications are part of this use case. In Table 7.1 the possible confidentiality label(s) of the services are given in brackets. The confidentiality label *Mission MLS* denotes that a service is MLS capable. The other labels (*Mission secret, Mission restricted* and *Mission unclassified*) give the classification of single level services.

Services	Auth. required	Identities	Reason/comment
Publish/subscribe service: - situation picture (*Mission secret*) Pull service: - coalition shared database (*Mission MLS*)	Provider's authentication of client (subscriber, consumer)	User/Role /Appl	Needed to determine the client's label, to enforce mandatory access control. In addition needed to determine the client's additional access privileges.
	Client's authentication of service provider (publisher)	Role/Appl	Needed to determine the provider's label, to enforce mandatory access control. In addition needed to determine the service provider's authorization.
Services provided by unmanned sensors: - Remote control (*Mission unclassified)* - Sensor data collection (*Mission unclassified)*	Provider's authentication of client	User/Role /Appl	Needed to determine the client's access privileges. Will prevent that unauthorized clients modify the settings of the sensors or read sensor data. May also be needed to determine the client's label.
	Client's authentication of service provider	Role/Appl	Needed to determine the service provider's authorization. Will prevent that false sensors are introduced.
Messaging service (*Mission restricted, secret or MLS*) Position report service (*Mission restricted* or *MLS)* Alert/warning service (*Mission restricted* or *MLS)*	Authentication of sender and receiver entities	Appl	Needed to determine each entity's label. The label is used by each entity to enforce mandatory access control.
Appl = Application (refers to a specific process) User = Specific operator Role = User in specific role			

Table 7.1 Assessment of remote access – MLS nodes and single level nodes

The authentication requirements for user information that is exchanged at the same classification level (i.e. single level exchange) have been assessed in section 5 and are not further discussed. In this section we discuss the new multilevel functionality that allows information objects to flow

from low to high level. Our assessment of authentication requirements for information objects that flow from lower (unclassified and restricted) to secret level is summarized in Table 7.2.

Note that our assessment shows that lower classified information objects, not only *secret* information, require data origin authentication at the application level. One example is *restricted* reports on operational status.

<table>
<tr><th>User information object</th><th>Auth. required</th><th>Identities</th><th>Reason/comment</th></tr>
<tr><td>Formal messages (status reports); classification restricted</td><td rowspan="3">Data origin authentication at application level (end-to-end)</td><td rowspan="3">Role</td><td rowspan="3">The consequences of forged information of these types is assessed to be severe (can destroy the ongoing operation). Authentication with finer resolution than provided by the network level authentication is needed.</td></tr>
<tr><td>Warnings from higher level; classification restricted</td></tr>
<tr><td>Formal objects in the situation picture & coalition shared database (classification restricted):
– Recognised reports on own operational status (combat status)
– Recognised reports providing logistics assessments
– Assessments of the CBRN situation</td></tr>
<tr><td>Informal messages (e-mail) for coordination; classification restricted</td><td rowspan="4">Data origin authentication at network level (hop-by-hop)</td><td rowspan="4">Host/Appl</td><td rowspan="4">The consequences of forged information of these types is assessed to be medium (can delay processes of the ongoing operation). Network level authentication is assessed to be sufficient.</td></tr>
<tr><td>Position Reports; classification restricted</td></tr>
<tr><td>Alert messages from combat level; classification restricted</td></tr>
<tr><td>Sensor data; classification unclassified</td></tr>
<tr><td colspan="4">Appl = Application (refers to a specific process)
Host = Communication node or hardware device
Role = User in specific role
CBRN = Chemical, Biological, Radiological and Nuclear</td></tr>
</table>

Table 7.2 Assessment of user information - information flow from lower (unclassified and restricted) to secret level

8 Conclusions

The analysis has identified and assessed five use cases that require authentication of user traffic across networks. These are:

a. Civil-Military Cooperation; coordination between coalition units and NGO cells when the coalition forces escort an NGO convoy
b. Military cooperation in multi-domain environment; cooperation between national and coalition units in two security domains (*Mission secret* and *National secret*)
c. Collaboration between coalition units at combat level and tactical level; collaboration in three separate security domains (*Mission unclassified*, *Mission restricted* and *Mission secret*)
d. Cross domain information exchange; extension of use case b
e. Multilevel security (MLS); use case c extended with MLS.

For each use cases we have described collaboration requirements between various actors at the operational level. The actors collaborate in order to perform common tasks, and to complete the tasks they need information and applications that are accessed through the network. We have assessed the required authentication, both for remote access to applications and for remote exchange of user information. The assessment gives the required type of authentication and the identities to be authenticated. Why verification of these identities is required is also stated in our assessment.

For all use cases mutual entity authentication is required for remote access to applications. Client authentication is needed to establish the client's access privileges, while application authentication is needed to determine the authorization of the application. Further, mandatory access control is required when communication nodes of multiple security domains use the same network infrastructure. This means that both the client and the application must be authenticated so that theirs confidentiality labels can be determined.

We also assess that formal objects (e.g. formal messages and objects stored in a database) require data origin authentication at application level. This fine-grained authentication is necessary because the consequences of forged information are assessed to be serious. The other user information types may be authenticated at the network level. We observe that data origin authentication at application level is required in all use cases. In particular our assessment shows that lower classified information objects, not only *secret* information, require data origin authentication at the application level. One example is *restricted* reports on operational status.

References

[1] Hegland A. M., Winjum E., and Hedenstad O.-E. (2011), "A framework for authentication in NBD tactical Ad Hoc Networks", *IEEE Communications Magazine*, vol. 49, no. 10, pp. 64-71.

[2] Fongen A. (2010), "Optimization of protocol operations in a Public Key Infrastructure", FFI-rapport 2010/02499.

[3] Fongen A. (2010), "Identity Management Without Revocation", *SECURWARE 2010*.

[4] Dolev D. and Yao A. (1983), "On the security of public key protocols", *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198-208.

[5] Bishop M. (2003), *Computer Security: Art and Science*, Addison-Wesley Professional, p. 103.

[6] National Institute of Standards and Technology (NIST) (1994), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2.

[7] Coalition Networks for Secure Information Sharing (CoNSIS) (2011), "System and Experimentation Architectures", CoNSIS/Task 5/DL/002, Version 1.0.

[8] Hallingstad G. and Oudkerk S. (2008), "Protected Core Networking: An Architectural Approach to Secure and Flexible Communication", *IEEE Communications Magazine*, vol. 6, no. 11, pp. 35-41.

[9] NSM (2006), "National Security Authority - General Infosec guidance no. 2B draft", G-02B, (Mar. 2006).

[10] Bell D. E. and La Padula L. J. (1975), "Secure Computer Systems: Mathematical Foundations", Technical Report MTR-2547, Mitre Corporation, Bedford, MA.