Prototype Military Message Form (P772) and Mail List Agent (MLA) for National MMHS

Col.Dr. Murat UCUNCU
Turkish General Staff. Information Systems Division (TGS IS)
Genelkurmay Bilgi Sistemler D. Bsk.ligi
06100 Bakanliklar
Ankara
TURKEY

murat.ucuncu@tr.net

A. Betul SASIOGLU
National Research Institute of Electronics and Cryptology (TUBITAK – UEKAE)
PK.74
Gebze Kocaeli
TURKEY

betul.sasioglu@uekae.tubitak.gov.tr

Maj. Erdal YILDIZ
Turkish General Staff. Information Systems Division (TGS IS)
Gnkur. MEBS Bsk.ligi
06100 Bakanliklar, Ankara
TURKEY

eyildiz@tsk.mil.tr

ABSTRACT

It is clear that messaging service is the most important part of a joint CCIS infrastructure. Before the development of Internet and computer technologies, most of the allies were using text based messaging systems commonly known as ACP 127 systems. ACP 127 is a messaging protocol and a set of rules and procedures that enable military community to exchange character oriented messages between teletype machines over telegraph circuits. With the advent of e-mail technologies, it is now possible to build flexible, cost effective messaging infrastructures that provide services more closely aligned with the business needs of the military community, which is known as a Military Message Handling Systems (MMHS)

NATO C3 Board Information System Sub Committee (ISSC) Military Message Handling Systems Working Group (MMHSWG) is the responsible body in NATO to develop and publish the official standards for MMHSs and it has developed STANAG 4406, which is a set of extensions to civilian X.400 based Messaging Services required for military messaging, gateway functionality to legacy messaging systems (ACP 127 systems) and a security protocol for the authentication and non-repudiation of the messages in the system

Turkish General Staff, with the intention of having a modern and STANAG 4406 complaint joint MMHS, initiated a project named as MEDAS (which is an acronym for Turkish joint MMHS) as part of an ongoing Turkish Armed Forces CCIS project in 1990s. The technical specifications of the intended system were prepared in accordance with the NATO STANAG 4406 and ACP 123. X.500 based directory services and X.509 based public key infrastructure (PKI) services were also designed as the major parts and core services of MEDAS. The contractor started to establish the system in the second half of the 1999. The project was phased in three main parts and aimed to establish the system in all strategic and operative level (up to brigade level or equivalent) all over the country between 1999-2003.

Ucuncu, M.; Sasioglu, A.B.; Yildiz, E. (2006) Prototype Military Message Form (P772) and Mail List Agent (MLA) for National MMHS. In *Military Communications* (pp. P5-1 – P5-12). Meeting Proceedings RTO-MP-IST-054, Poster 5. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

The system is now operational at Communication Center (COMCEN), Operations Centers (OPCEN) and some special organizational users level in some strategic HQs. for almost two years. After the first year in operational use, several user feedback was received which forced us to develop a new military message (P772) form for the client side applications of the national MMHS and Mail List Agent (MLA) for the handling of address /distribution lists. The new project was named as MAMF (which is am acronym for the project in Turkish and we call it as MAMF for the rest of the paper).

The development phase of the MAMF was started in December 2003 and planned to be finished in June 2005. The result is going to be a "prototype" and after being evaluated in both test bed and in the real time systems, if agreed, it will be populated in MEDAS instead of current client side messaging products. In this paper, the architecture of the joint Turkish Armed Forces MMHS project will be summarized and the design details of the Prototype MAMF project will be fully explained.

1. INTRODUCTION

Since secure messaging has always been one of the most important topics in military environment, nations try to implement their own Military Message Handling Systems (MMHS). As it is well known, MMHS is designed to provide reliable, functional, and secure electronic messaging at military environments. The National MMHS project of Turkish Armed Forces has been developed with a parallel intention. The aim of the project is to have a modern and operational system in accordance with NATO STANAG 4406 [1] and ACP 123 [2].

This paper describes the general architecture of the Joint Turkish Armed Forces MMHS project (MEDAS) and fully explains the design details of MAMF project, which is being developed as a new set of "prototype" software for the client side applications of the National MMHS and a National MLA (Mail List Agent). The major components that constitute the Prototype MAMF project are explained in terms of their functionality, implementation details, and logical state within the whole MEDAS system.

The main purpose of implementing the prototype is the necessity to implement a military message form (having P772 services as defined in STANAG 4406), which can work with the National PKI software [3] product. Additionally, it is planned to improve an efficient, easy-to-use, customer-defined system by means of the new features added to the current system via MAMF project.

The new architecture developed in National MMHS project, which is called "Prototype MAMF project," has two main parts; the first is the new national military message form, which is used to handle the main national messaging task, and the other is the National MLA. This paper intends to summarize the architecture of the new National MMHS project and to explain the full design details of the Prototype MAMF project.

2. THE NEW NATIONAL (THE JOINT TURKISH ARMED FORCES) MMHS ARCHITECTURE

MEDAS is a "Message and Document Distributing System" which contains, STANAG 4406 Military Messaging Standards as a framework. In addition, X.500 [4] / ACP 133 [5] based Directory Services Standards, X.509 [6] based Public Key Infrastructure (PKI) and certificate standards, S/MIME security services [7] and some other messaging services and requirements defined in ACP 123 have been used in the current operational system.

The prototype National MAMF project has several different components and sub-modules used for different functional purposes inside the National MMHS system. National MMHS system with MAMF elements will have the following functional main key components;

User Agent (UA): User Agent is the client side component. In the National MMHS, both Windows 2000 and Windows XP will be used as client side operating system. New Microsoft Exchange-based client side messaging software (P772 Military Form) having the same look-and-feel image as Microsoft Outlook has been developed. Military Form which has been developed in "Microsoft .Net framework" development environment is the graphical user interface to create, send, receive, re-send, forward the messages, and track messages In addition to the GUI component, which realizes the above-mentioned functionalities, National MAMF – directory interface sub-component, the National ACP 127 [8] –P772 Format Converter, the National PKI sub-component and integration of IRIS MFS (Message Formatting System) [9] software are also the key components running within the National MAMF component at client side. PKCS #11 Smartcards and Smartcard readers, which are connected to the S/MIME agent, are also on UA component to provide secure login and to create/read signed/encrypted secure messages. The private key is stored on a smart card and the public key is provided by the directory service.

Message Transfer Agent (MTA): MTA component of National MMHS works as a store and forward message switch. MTA accepts messages from other components in National MMHS and either routes them or delivers them to message stores. Exchange 2003 – W2K3 is used as the MTA component of the system. To implement some features in the National MAMF system, some specific rules have been defined on MS Exchange Server 2003. MTA-to-MTA communication is realized via X.400 [10] protocol.

Directory Services: The Directory is the natural repository for storing the directory object classes and their attached attributes related to MHS users/distribution lists, Public Key Infrastructure (PKI) information such as certificates and certificate revocation lists. In addition to these objects, some other information, which is needed to be distributed and to be used by all UAs, is also stored inside the directory. Attributes attached to object classes are used to provide information identifying the capabilities of the entries belonging to these object classes. In National MMHS system, Critical Path 4.2 – W2K3 software is used as the Directory Services Server

Certificate Authority Server: This server component is one of the main parts of the National PKI system. It has an interface with Directory Server to store, update, and delete the certificates. It is also responsible to keep the certificates up-to-date inside the directory. A National PKI product, which has been developed by National Research Institute of Electronics and Cryptology (TUBITAK – UEKAE) was used in the system.

3. THE PROTOTYPE NATIONAL MAMF ARCHITECTURE

The new national military message form in MAMF project is fundamentally an end-user Client Interface Module used mainly for messaging tasks like preparing, sending, receiving, forwarding, and resending messages within MEDAS. The prototype National MAMF mainly supports P772 military messaging elements.

The main functionalities of the client side application of Prototype MAMF project are summarized as follows:

- Well Known P772 Messaging functionalities such as "Action and Info Addressees, Precedence, Security label, Subject Indicator Code (SIC), Handling Instructions, Message Instructions, Message Type" and etc,
- Alerts based on primary precedence and security classification,
- Advanced ability to track the sent messages,
- Customizable printout facilities regarding fulfilled fields in each message,
- Secure messaging facility interoperable with national PKI software product; S/MIME V3 ESS for both encryption and digital signature services,

- Easy connection to X.500 directory via the National Directory Browser Application,
- Easy upgrade the National MMHS product regarding to the changes in configuration values: The parameters used inside National MAMF are not hard-coded. With an additional administrative tool, it is possible to add, delete, and modify almost all configuration values inside National MMHS.
- Offline working facility with Local Address Book and Local Certificate Store,
- ACP 127 / P772 Automatic Message Conversion,
- Possibility to read and prepare formatted messages via IRIS interface,

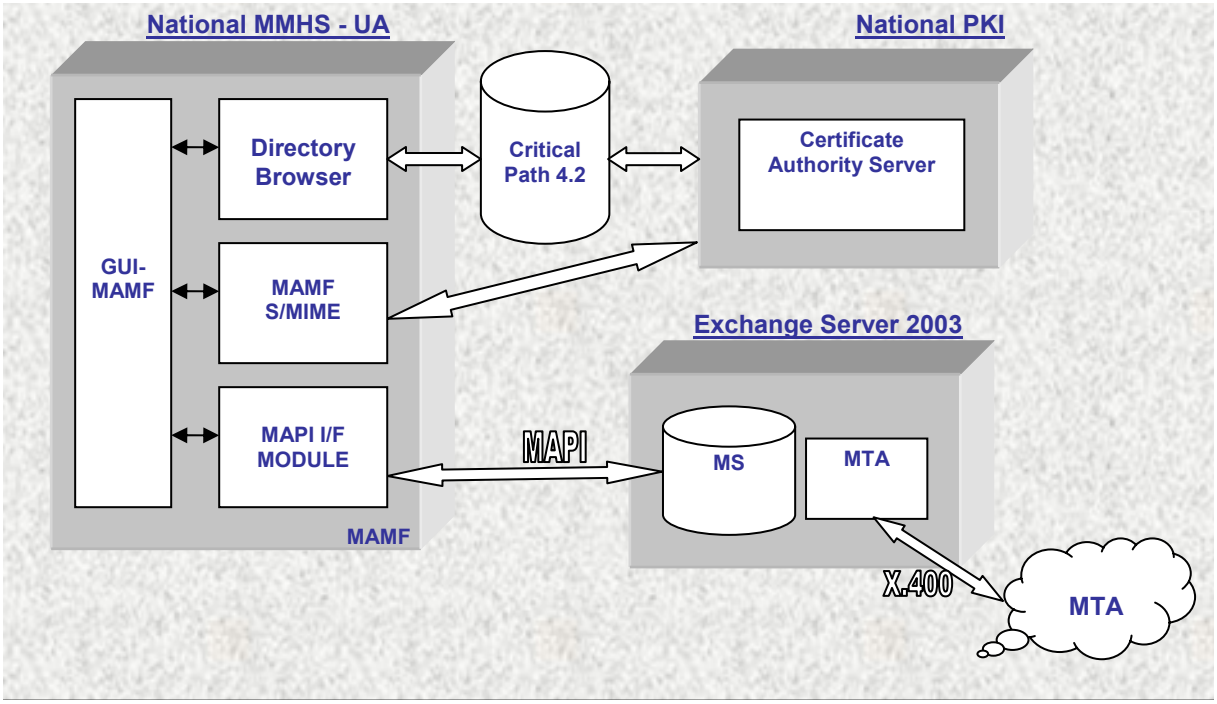

Figure 1: MAMF architecture inside the National MMHS

Although there are many specific modules within National MAMF, the main functional modules that are depicted in Figure 1, are explained as follows:

3.1 MAPI Interface Module

The National MAMF product is a MAPI-based standalone Exchange Mail Client. To handle MAPI protocol between National MAMF and MS Exchange Server 2003, a MAPI Interface Module has been developed within the National MAMF. In order to transfer the full contents of messages (precedence, subject, time, originator, recipients, body etc.) via MAPI protocol, the MAPI Interface Module realizes a conversion mechanism between the fields of a MAPI message and the National MAMF.

MAPI Interface Module, which is an access module between MAMF GUI Module of the National MAMF product and the MTA, is the outer module of the National MAMF.

3.2 MAMF Graphical User Interface (GUI) Module

MAMF GUI Module is an end-user Client Interface Module used mainly for both originating and displaying the military messages. In addition to this responsibility, MAMF GUI Module has an advanced message tracking application.

In order to enter MEDAS environment through National MAMF, the end users are authenticated with their "User Name" and "Password" under the domain of MTA.

Message tracker module, which has two different sub-modules within the National MAMF, is processed in MAPI Interface Module and MAMF GUI Module. The first sub-module tracks each sent message one by one by automatic handling of delivery and read receipts. The second one tracks the messages, which are sent between two specific times; the start and finish time are selected by the end user. MAPI Interface Module collects the reports and reports them to the MAMF GUI Module. After receiving the reports from MAPI Interface Module, MAMF GUI Module displays the results.

The messages and message tracker reports may easily be printed-out. To customize the printout regarding to fulfilled fields in each message is also possible in National MAMF.

English/Turkish user interfaces upon user selection are also possible in this product.

There is an IRIS interface module within the MAMF GUI Module for handling formatted messages. It is possible to prepare messages within IRIS environment and transfer them inside National MAMF easily and to transfer the received formatted messages into the IRIS environment by pressing a single button on the MAMF GUI Module.

3.3 National S/MIME Agent

Both encryption and digital signature services are implemented via National S/MIME component (or National S/MIME Agent), which is also interoperable with National PKI product. This component uses S/MIME V3 ESS (Enhanced Security Services). The application layer message security services including Authentication of Origin, Non-Repudiation, and Message Integrity are provided by this component. The message security services are implemented through the combination of generating a single digital signature wrapper over the P772 content type with the Cryptographic Message Syntax (CMS) for authentication of origin and message integrity. One of the main tasks of National S/MIME Agent is to provide Message Privacy; S/MIME scrambles or encrypts messages to help ensure that only the sender and the intended recipients can read them. The identification of a message sender is done through a digital signature.

PKCS #11 smart cards and smart card readers which are connected to the National S/MIME agent provide secure login function and because the private key is stored on a smart card while the public key is provided by the directory service, signed/encrypted secure messages are also processed by using the personal smart card.

3.4 National Directory Browser Module

National Directory Browser Module is mainly an interface module between MAMF GUI sub-module and the X.500 Directory. This module connects to the directory in order to get only the email addresses and their other necessary properties recorded in the Directory. Connection to Directory for getting certificates is the responsibility of National S/MIME Agent.

- The National Directory Browser Module has the following main features:
- Works as if an LDAP browser,
- Easy selection of user/distribution list message receivers for TO, CC, and XMT,
- Connection to X.500 directory to access SIC tables,
- Easy-to-use advanced search facilities,

- Storing search results facility,
- Easy address transfer to Local Address Book facility.

3.5 Message conversion between MMHS and ACP127 domains

In order to provide compatibility between message terminal units (MTUs) using ACP 127 format (such as MTU's communicating with ships via radio systems) and National MMHS end-user terminals, an interconnection module was developed which will work on the client side. System works as described below.

Client side messaging software has two modules for ACP 127/P772 conversion; the port-access and ACP 127 monitor, which realize the conversion from ACP 127 to P772 format. The port-reader sub-module of the port-access is a service program to listen to the specified port via which the messages are received in ACP 127 format. The ACP 127 monitor is a GUI module, which is used to view and/or edit the received ACP 127 messages, convert them to P772 format and lastly transfer them to the National MAMF environment.

In other direction, the conversion from P772 format to ACP 127 format is also realized by the same sub-modules, but with different functionalities. The messages received or prepared in P772 format are converted to ACP 127 format by clicking a conversion button on the National MAMF. The messages transferred into ACP 127 format may be viewed and/or edited inside the ACP 127 monitor module and then the ACP 127 messages are sent to the specified port via the port-writer sub-module of the port-access.

4. THE NATIONAL MLA DESIGN

The Mail List Agent (MLA) component of National MMHS is used to manage and expand Address Lists (AL). An Address List is commonly used where either a large number of recipients have to be represented as a group or where the members of a group can change frequently.

In our MMHS, there are two different send-processes for encrypted messages to Address Lists; the first approach lets the messages to be sent directly to each member of the group by encrypting with the key of each end-user. Moreover, in the second approach, encryption is done with the key of the National MLA, which is responsible to that Address List, and the message is sent through the National MLA.

Although it is always possible to use the first approach as an option, the second is recommended for effectiveness. In this session, only the details of the second approach will be given.

To realize the second approach, a National MLA component has been developed. The P772 messages prepared for an Address List in National MAMF at client side are transferred to the National MLA in order to be executed. The National MLA is a software application responsible for the expansion of address lists stored in the X.500 directory. Its primary objective is to off load the per recipient encryption from the User Agent (UA) to a more powerful and dedicated processor. The National MLA also ensures that only authorized users send mail to a given Address List (AL). To achieve this goal, the National MLA only accepts delivery of secured messages with signatures (signed only, or signed and encrypted), which allows the National MLA to verify the originator identity by checking his/her signature.

In National MMHS, an end-user sends a message to an Address List by addressing the message to the responsible MLA of that particular AL. The message is encrypted with the session key first and this session key is encrypted with the MLA's public key which is responsible for that AL. Compared to the encryption directly with the public keys of all the members in AL in MAMF, the only encryption with the MLA's public key is one of the major advantage of this architecture design.

The signed/encrypted addressed-to-AL scenario which is depicted in Figure 2, starts by forming a secure message with an AL address on its "TO" or "CC" field; After matching AL to MLA in Directory Browser, MAMF S/MIME Module completes its signing and encryption processes. The message prepared in MAMF is sent to all the members of that AL through the MTAs (Exchange Server 2003) on the way and through the responsible MLA.

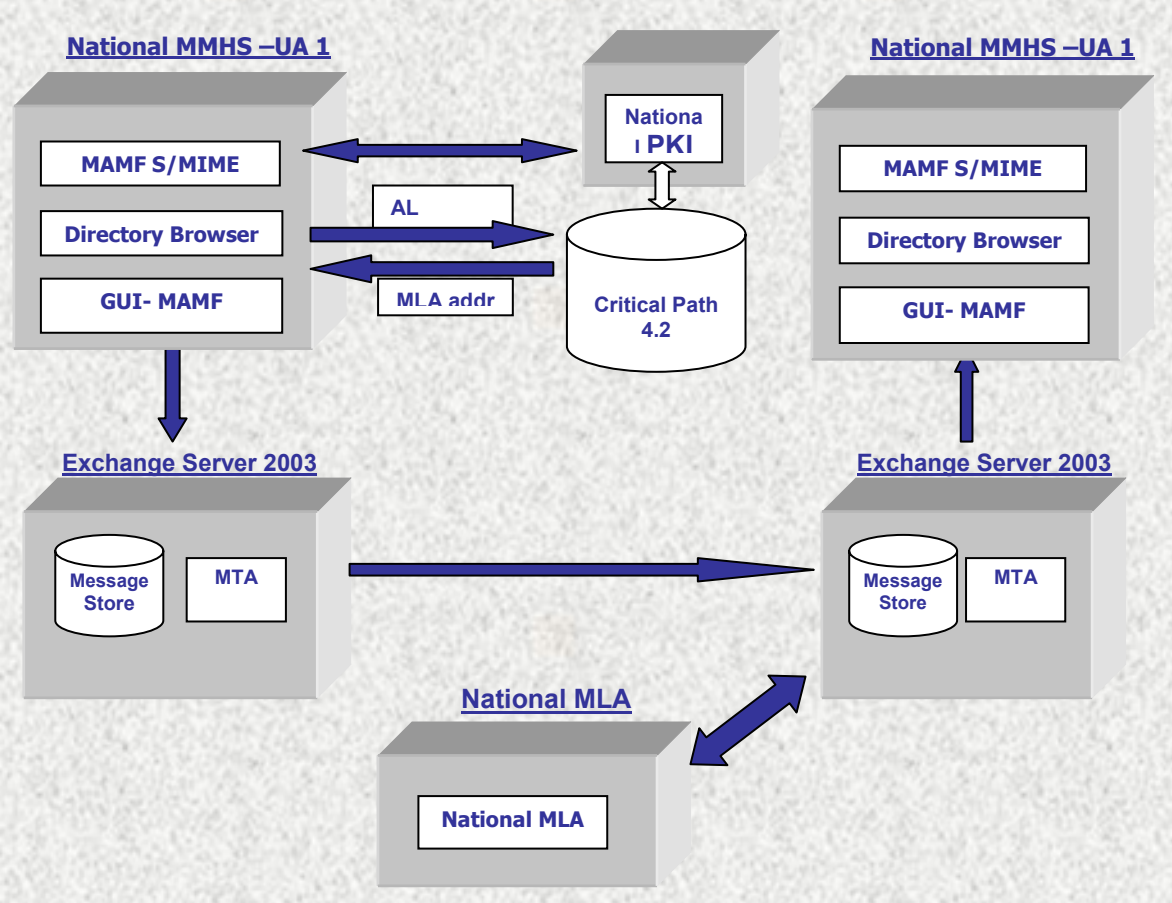

Figure 2: Message distribution through the National MLA in the National MMHS working scenario

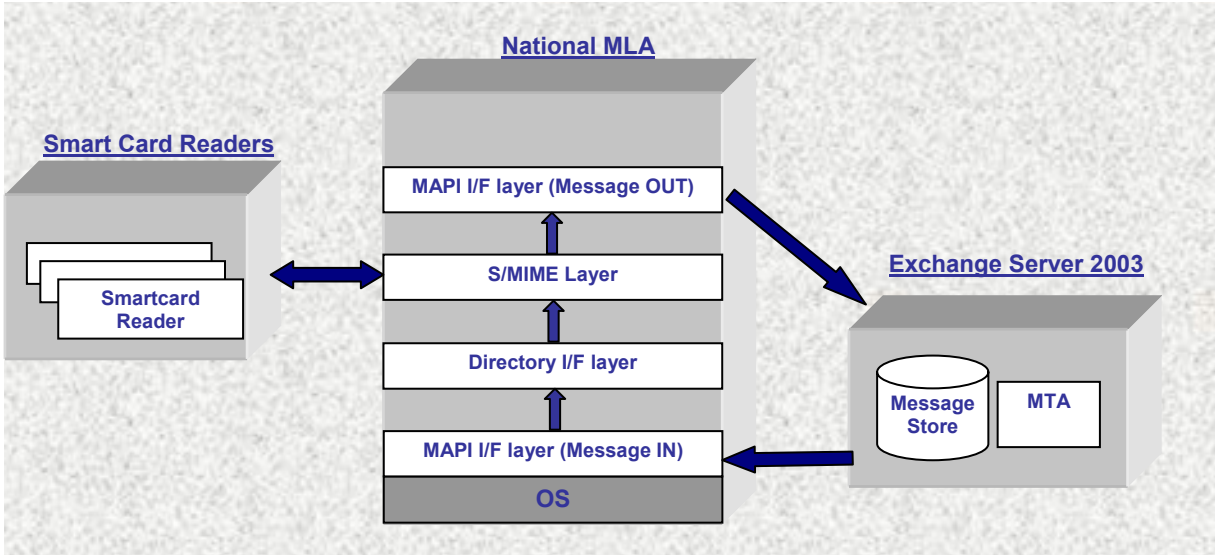

Figure 3: National MLA working process

The National MLA architecture which is depicted in Figure 3, has mainly four functional modules; MAPI Interface Module, Directory Browser Module, S/MIME Agent Module and Management Module

4.1 MAPI Interface Module

The MAPI Interface Module is the sub-module of the National MLA where the messages are received and sent by using MAPI protocol. MAPI Interface Module has also two sub-modules; MLA Message Receiver Module and MLA Message Sender Module.

The messages sent to the National MLA, come to the Message Store of the National MLA at first, from where they are transferred to a queue by receiving the related events. The MLA Message Receiver Module is responsible for listening to the message events. This mentioned queue allows fetching at most five headers of the received messages. By searching the header information, whether a report message or a P772 message was received is decided and later it is transferred to an in-report queue or to an in-message queue. In in-message queue, the message, which has a higher priority, is processed earlier.

Only the delivery and non-delivery notifications are received by the National MLA and are firstly sent to the in-report queue. Receipt and non-receipt notifications are directly sent from the receiver UA to the sender UA. The number of the synchronous report processing is configured via the Management Module of the National MLA. After extracting all the information of the received report in the MLA Message Receiver Module, matching the report to the related message is done by the Database Module of the National MLA. Later on, the report is sent back to the first message sender after the necessary arrangement on the report is completed.

P772 message processing starts by receiving the incoming P772 message to the in-message queue. The number of the synchronous message processing is also configured via the Management Module of the National MLA. After receiving the message from the in-message queue, the necessary information of that message is extracted first from Exchange Server in the MLA Message Receiver Module, and then is transferred to the Directory Browser Module for AL extraction and to the S/MIME Agent Module for signature verification, decryption and encryption processes respectively. Last module to be executed in the National MLA is the MLA Message Sender Module for distributing the message to all the members of the AL by submitting it into their MTAs (the connected Exchange Server 2003 in this implementation).

4.2 Directory Browser Module

After the process in the MLA Message Receiver Module is completed, the messages are forwarded to the Directory Browser Module. In this module, the AL addresses that have already resolved in the sender MAMF environment to get an E-tracker string are resolved once again to get all the member addresses of the received ALs. In this module, the member addresses are extracted regarding their precedence ("TO" or "CC" fields) after the loops are prevented.

4.3 S/MIME Agent Module

After the processes are completed in the MLA Message Receiver Module and the Directory Browser Module, the messages are forwarded to the S/MIME Agent Module. The triple-wrapping mechanism of S/MIME, which is defined in S/MIME's Enhanced Security Services specification [*11*, *12*, *13*], is used in this sub-module; a triple-wrapped message is a message that has been signed, then encrypted, then signed again. Triple wrapping is used when a message must be signed, and then encrypted, and then have signed attributes bound to the encrypted body. Outer attributes may be added or removed by the message originator or intermediate agents, and may be signed by intermediate agents or the final recipient.

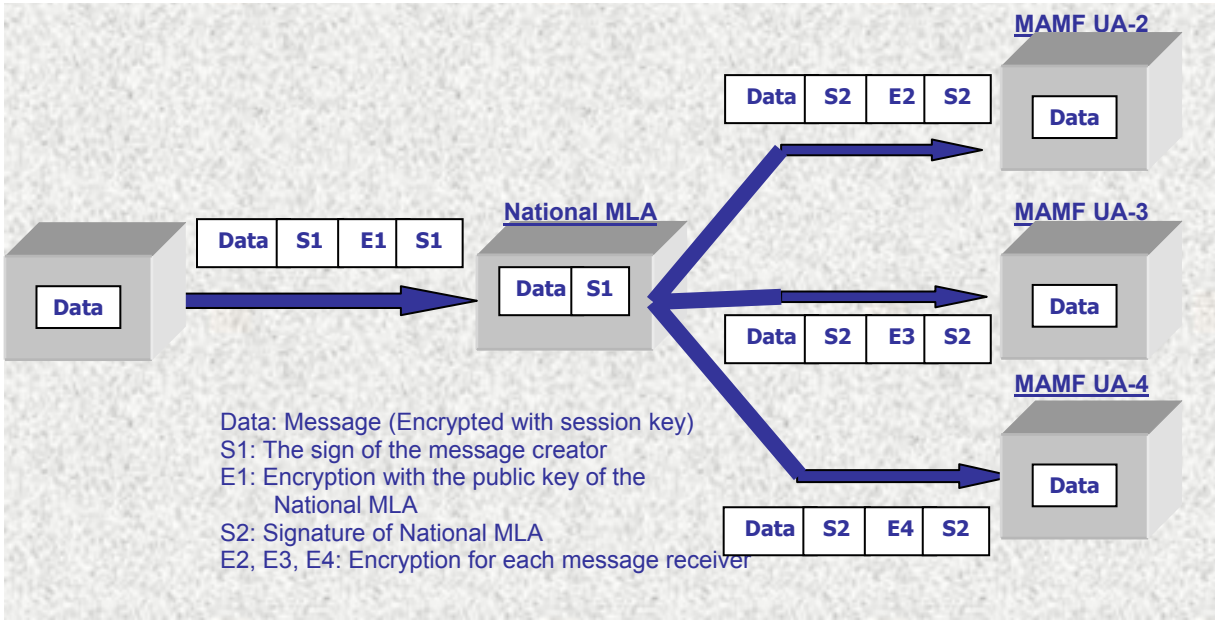

Figure 4: The National S/MIME Agent Working Process

In this architecture, as we have mentioned above, the S/MIME message is prepared using triple-wrapping mechanism in the sender MAMF. The received S/MIME message has four layers in at all; the message, which has been encrypted with the session key, which is called Message Encryption Key (MEK), is the first layer. This layer has been wrapped first with the signature of the sender to constitute the second layer, which is responsible to provide the authentication and the message integrity. These first two layers are end-to-end transferred structures without any process in National MLAs. Then, MEK has been encrypted with the public key of the responsible National MLA for the constitution of the third layer. At last, the signature of the National MLA has constituted the outer signature layer, in order to provide the encryption header integrity.

When an S/MIME message is received by the S/MIME Agent Module, this module first determines and verifies the signature of the sender MAMF user in" outer" signed data layer. After the verification of the

signature, in order to ensure that the members of the AL can read the encrypted message; the S/MIME Agent Module decrypts the Encrypted Message Encryption Key (EMEK) to gain the Message Encryption Key (MEK) and re-encrypts it for each new recipient using the directory to obtain the public certificates of each recipient. At last, these provided layers are signed by the signature of the National MLA.

In this architecture, to speed-up the execution, it is possible to process more than one message in parallel; to realize this feature, more than one Smart Card (all keeps the private key of the National MLA) and Smart Card Readers may be used. Each encryption process in the S/MIME Agent Module is realized by one of the smart cards. The messages are received in this module through a queue.

4.4 Management Module

The Management Module of the National MLA may be functionally separated into two sub-modules; Audit and Logging Module, Configuration Module

All processes in National MLA are controlled and are logged by the Management Module in order to recover the detected faults. This module has advanced audit and logging capabilities. Delivering the messages is repeated until the expiration of the related timer. In the case of a failure in the delivery of a message or a report, the management module sends a non-delivery notification to the originator of the message. The different time-out values based on different criteria (priority of the message, a report mail) may be configured inside National MLA.

Another task of the Management Module is to log the details (information on sender, precedence, message Nr, sent time, received time, status of message in each step) of all messages and all reports passed through the National MLA and prepare the statistics for a requested interval. In this module, all the events occurred in National MLA are also logged.

The Management module has a user-interface window called “National MLA Management.” There are two main functionality of the “National MLA Management” window; in the first one the statistics and the logged information are displayed, whereas in the second one the configuration items are listed below and may be displayed/modified via this window.

- Application starting the condition of the National MLA,
- Show/Hide the application Tray Icon,
- MTA selection of the National MLA,
- Logon condition,
- Simultaneous message processing limit,
- Simultaneous report processing limit,
- Quantity of the Smart Cards in process,
- Time-out values,
- Database backup period,
- The lifetime of the old records (deletion period).

5. CONCLUSION

In Military Message Handling Systems, there are two main topics that must be taken into consideration; security and reliability of the overall system, and well-defined functionality.

In order to integrate the security and high-performance needs of end-users, nations require a model or framework that can both provide the secure messaging in military environment and answer the end-users' needs. NATO intends to define the requirements of a Military Message Handling System in STANAG 4406 standard for NATO Nations.

Creating a prototype National MMHS product in accordance with NATO STANAG 4406 and ACP 123, and meanwhile developing an efficient easy-to-use customer-defined system, is a considerable experience. In order to implement both secure and a flexible modern system, the user needs have always been taken into consideration during both design and development phases and the system has been developed with an easy-to-upgrade software approach. However since the product described in this paper is only a prototype, the Prototype National MMHS will be tested in real environment to see its usability and its effectiveness from the viewpoint of the security, reliability and functionality. So that, the future final version of National MMHS will provide all MMHS needs mentioned in this paper.

6. REFERENCES

[1] NATO, STANAG 4406, "Military Message Handling System"

[2] ACP 123, "Common Messaging Strategy and Procedures"

[3] MA3 ASYA, "PKI Software Developed by Turkish TUBITAK UEKAE"

[4] ITU-T X.500, "Data Communication Networks Directory Recommendations"

[5] ACP 133, "Common Directory Services and Procedures"

[6] ITU X.509, "The Directory: Public Key and Attribute Certificates Framework"

[7] NATO, STANAG 4631, "Profile for the Use of S/MIME Protocols Cryptographic Message Syntax (CMX) and Enhanced Security Services (ESS) for S/MIME"

[8] ACP 127, "Communication Instructions Tape Relay Operations"

[9] Systematic Software Engineering A/S, IRIS "IRIS/MFS Presentation Forms"

[10] ITU-T X.400, "Series, Information Processing, Text Communication – Message Oriented Text Interchange System (MOTIS)"

[11] P. Hoffman, Internet RFC 2634 "Enhanced Security Services for S/MIME"

[12] B. Ramsdell, Internet RFC 2633 "S/MIME Version 3 Message Specification"

[13] B. Ramsdell, Internet RFC 2632 "S/MIME Version 3 Certificate Handling"