



Security Document

NMS security features

01	2018-03-15	General characteristics	mja	jeg	alx	
Rev.	Date	Reason for issue	Prep.	Check.	Appr.	Client Appr.


Customer (if applicable):		Document status: DRAFT	
Company/Contractor:  Nebb Solutions DOOEL Partizanski Odredi 14 Skopje, 1000 Republic of Macedonia		Document classification CONFIDENTIAL	
Project no.: 1210001	Project title: NMS Nebb Messaging System		
Document type: Security Document	Contract no.: N/A	Quotation no.:	Customer ref. no.:
Document title: NMS security features			
Document no.: DOC-1210001-01		Rev.: 01	Page: 1 of 6

TABLE OF CONTENTS

1 INTRODUCTION 3

2 DESIGN AND DEVELOPMENT PROCESS 3

3 ENDPOINT SECURITY 3

 3.1 Secure Endpoint Provisioning 4

 3.2 Authentication 4

4 CONNECTION SECURITY 5

5 SECURE PROCESSING AND STORAGE 5

 5.1 Authentication and Authorization Authority 6

TABLE OF FIGURES

Figure 1 Microsoft Security Development Lifecycle 3

Figure 2 NMS AAA Scenario 6

1 INTRODUCTION

The following document emphasizes the main security aspects that were considered while designing and developing Nebb Messaging System (NMS). For functional overview of Nebb Messaging System, please consult the product datasheet document or visit the official NMS site.

The process of how NMS has been designed and developed is elaborated in the following chapter. The rest of the chapters focus on different parts of the architecture: Endpoint Security, Connection Security, and Secure processing and Storage. Endpoint Security elaborates the security on endpoint (device) level. The connection security elaborates the communication between the endpoints (for example your production facilities) and the Nebb Messaging System cloud component. The Secure Processing and Storage chapter emphasizes the main security aspects of the data storage and data processing.

2 DESIGN AND DEVELOPMENT PROCESS

Nebb Messaging System, as any other successful product, has been designed and developed in an agile fashion, which guaranties small and functional upgrades in appropriate iterations. Next to the agile development, Nebb Messaging System has been designed and developed as a security-first product. Security-first product is a product that puts the security of the end users and their data as top priority. To provide a security-first product, Nebb follows the Microsoft Security Development Lifecycle (SDL) as an industry-leading software security assurance process, that combines a holistic and practical approach, and introduces security and privacy early and throughout all phases of the development process.

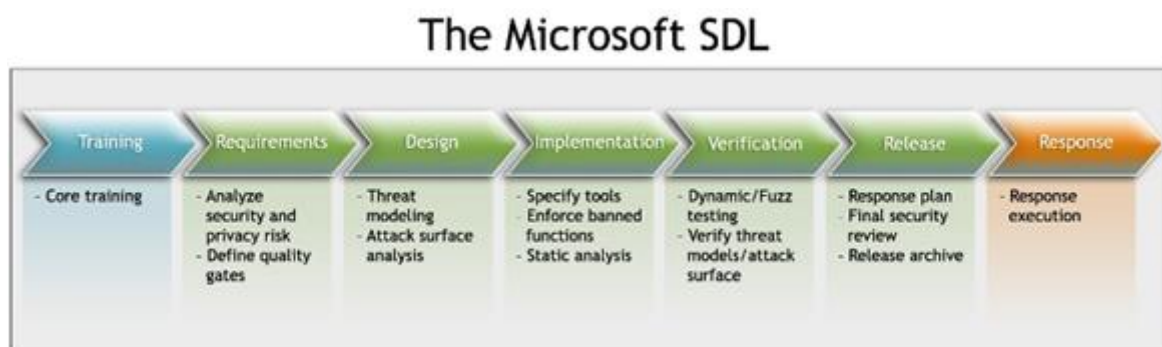


Figure 1 Microsoft Security Development Lifecycle

3 ENDPOINT SECURITY

This chapter elaborates the basic aspects of the security of the Nebb Messaging System on endpoint level. Nebb Messaging System secures endpoints by the following two methods:

- By providing a unique identity key (security tokens) for each endpoint, which can be used by the endpoint to communicate with the Nebb Messaging System Cloud Component.
- By using an on-endpoint X.509 certificate and private key to authenticate the endpoint to the Nebb Messaging System Cloud Component. This authentication method ensures that the private key on the endpoint is not known outside the endpoint at any time, providing a higher level of security.

The security token method provides authentication for each call made by the endpoint to Nebb Messaging System, by associating the symmetric key to each call. X.509-based authentication allows authentication of an endpoint at the physical layer as part of the TLS connection establishment. The security-token-based method can be used without the X.509 authentication which is a less secure pattern. The choice between the two methods is based on security requirements that our customers have.

3.1 Secure Endpoint Provisioning

Nebb Messaging System secures endpoints while they are out in the production environment by providing a unique identity key for each endpoint, which is used to communicate with the device as it is in operation. The generated key with a user-selected endpoint ID forms the basis of a token used in all communication between the device and the Nebb Messaging System. The endpoint ID must be unique for each endpoint for a customer. Duplicate endpoint IDs are not allowed for a single customer since they are the basis of the authentication process.

The endpoint provisioning is implemented by downloading and installing a preconfigured installation and provisioning software that securely self-registers the endpoint with a unique ID within the customer workspace in the Nebb Messaging System. The Nebb Messaging System identity registry provides secure storage of endpoint identities and security keys for a solution. Individual or groups of endpoint identities can be added to an allow list, or a block list, enabling complete control over device access

Additional endpoint security features include the following:

- Endpoints do not accept unsolicited network connections. They establish all connections and routes in an outbound-only fashion. For an endpoint to receive a command from the backend, the endpoint must initiate a connection to check for any pending commands to process. Once a connection between the endpoint and Nebb Messaging System is securely established, messaging from the cloud to the endpoint and endpoint to the cloud can be sent transparently.
- System-level authorization and authentication use per-endpoint identities, making access credentials and permissions near-instantly revocable.

3.2 Authentication

Based on the security pattern selected, the endpoint authentication can be implemented by using security tokens or X.509 certificates.

3.2.1 Security Tokens

Each of the supported communication protocols in the Nebb Messaging System such as MQTT, AMQP, and HTTPS, transports tokens in different ways. When using MQTT, the CONNECT packet has the EndpointId as the ClientId, in the Username field, and a SAS token in the Password field. When using AMQP, SASL PLAIN and AMQP, Claims-Based-Security are supported. If AMQP claims-based-security is being used, the standard specifies how to transmit these tokens. HTTPS implements authentication by including a valid token in the Authorization request header.

3.2.2 Supported X.509 certificates

Any X.509 certificate can be used to authenticate an endpoint with Nebb Messaging System. Certificates include:

- **An existing X.509 certificate.** An endpoint may already have a X.509 certificate associated with it. The endpoint can use this certificate to authenticate with Nebb Messaging System.

- **A self-generated and self-signed X-509 certificate.** Nebb Messaging System customers can use self-generated certificates and store the corresponding private key (and certificate) on the endpoint. Tools such as OpenSSL and Windows SelfSignedCertificate utility can be used for this purpose.
- **CA-signed X.509 certificate.** To identify an endpoint and authenticate it with Nebb Messaging System, use of X.509 certificate generated and signed by a Certification Authority (CA) is supported. The Nebb Messaging System only verifies that the presented thumbprint matches the configured thumbprint. The certificate chain is not validated.

4 CONNECTION SECURITY

Durability of messaging is an important feature of Nebb Messaging System. The need to durably deliver commands and/or receive data from endpoints is underlined by the fact that endpoints are connected over the Internet, or other similar networks which can be unreliable.

Efficiency is important to ensure conservation of resources and operation in a resource-constrained environment. HTTPS (HTTP Secure), the industry-standard secure version of the popular http protocol, is supported by Nebb Messaging System, enabling efficient communication. Advanced Message Queuing Protocol (AMQP) and Message Queuing Telemetry Transport (MQTT), supported by Nebb Messaging System, are designed not only for efficiency in terms of resource use but also for reliable message delivery.

Additional connection security features include the following:

- The communication path between endpoints and Nebb Messaging System, is secured using industry-standard Transport Layer Security (TLS) with Nebb Messaging System authenticated using X.509 protocol. Nebb Messaging System supports TLS 1.2, TLS 1.1 and TLS 1.0, in this order. Support for TLS 1.0 is provided for backward compatibility only. It is recommended to use TLS 1.2 since it provides the best security.
- To protect endpoints from unsolicited inbound connections, Nebb Messaging System does not open any connection to the device. The endpoints initiate all connections.
- Nebb Messaging System durably stores messages for endpoints and waits for the endpoint to connect. These commands are stored for two days, enabling endpoints connecting sporadically, due to power or connectivity concerns, to receive these commands. Nebb Messaging System maintains a per-device queue for each device.

5 SECURE PROCESSING AND STORAGE

Nebb Messaging System contains different components for data aggregation, data processing, and data storage. Moreover, there are UI components to present the data in the preferred format to the end user. In general, the components are divided in two groups based on their purpose: components for secure processing and components for storage. Both types of components are designed and developed with the latest security patterns to provide optimal protection for our customers and their data

First, Nebb Messaging System can be accessed only if the user is authenticated and authorized by central authentication and authorization authority (AAA). Without valid token generated from the AAA, the user cannot be authenticated and authorized to access any of the Nebb Messaging System resources.

Second, all the keys that Nebb Messaging System needs to access certain processing and storage components are safeguarded by secure key management component, that encrypts keys and small secrets like passwords that use keys stored in hardware security modules.

Third, Nebb Messaging System provides a way to monitor and audit all access to the data to alert of any intrusion or unauthorized access.

5.1 Authentication and Authorization Authority

Nebb Messaging System end users can use the functionalities by accessing the Nebb Messaging System portal. Access to the portal, which is a web application, is completely controlled by Authentication and Authorization Authority (AAA). Figure 2 depicts a simple scenario when a user wants to access Nebb Messaging System. In case the user is not authorized, the user will be redirected to AAA Sign-In page. If the user successfully logs in AAA, the user will get valid token (depicted with a pentagon on Figure 2 NMS AAA Scenario) that can be used to access Nebb Messaging System.



Figure 2 NMS AAA Scenario