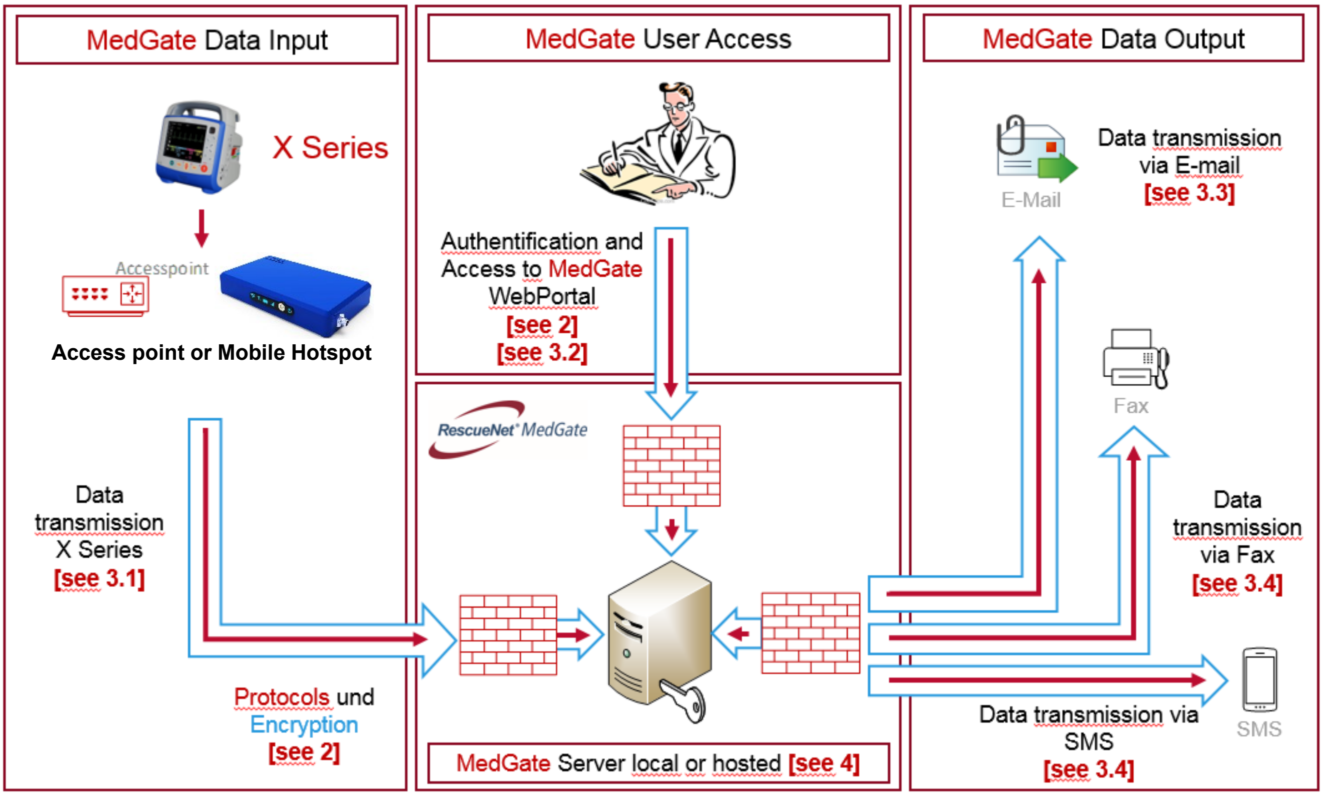
MedGate Dataflow- & Access Architecture

CRS medical

Content

1. MedGate Dataflow & Access Architecture


MedGate Data Input
X Series
Accesspoint
Access point or Mobile Hotspot
Data transmission X Series [see 3.1]
Protocols und Encryption [see 2]
MedGate User Access
Authentification and Access to MedGate WebPortal [see 2] [see 3.2]
RescueNet® MedGate
MedGate Server local or hosted [see 4]
MedGate Data Output
E-Mail
Data transmission via E-mail [see 3.3]
Fax
Data transmission via Fax [see 3.4]
SMS
Data transmission via SMS [see 3.4]

2. Protocols and Encryption

MedGate uses the following Protocols:

- HTTPS
- SMTP

MedGate supports incoming and outgoing the following encryption standards:

- TLS 1.2
- TLS 1.3

3. Data Communication and Security

In general, access to MedGate is HTTPS secured and each login needs to be validated via username and password.

Data transmission from mobile devices to MedGate as well as the access to the MedGate portal is HTTPS secured. The Backend for incoming transmissions and access to the website is an Apache2 server which provides services via Apache Tomcat.

3.1 Data Transmission from Defibrillator (e.g. X Series)

Data transmission from mobile defibrillators to MedGate is realized via HTTP POST (secured via TLS) request in which a JSON document is transmitted. For the POST request, the defibrillator needs to sign in on the MedGate server with login details created by the MedGate system. The login credentials are accessible for authorized personnel only.

3.2 User Access

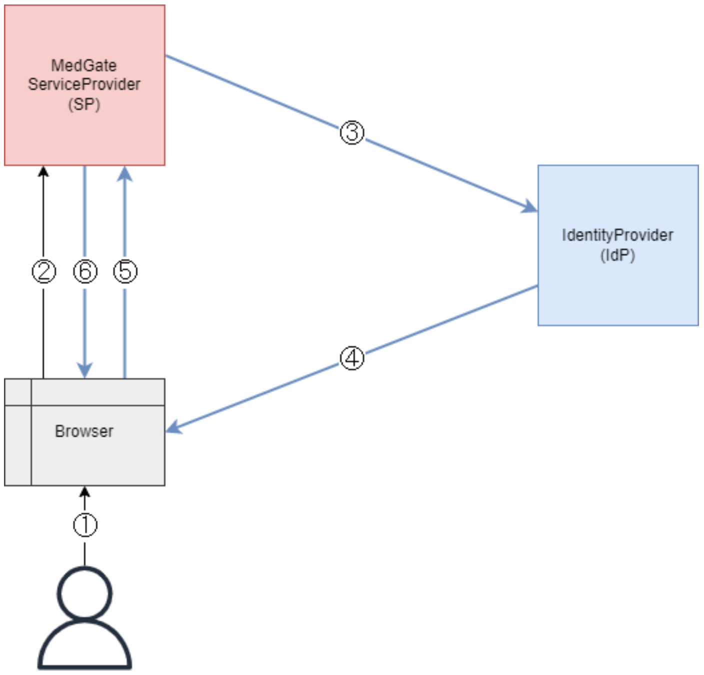
Access on the MedGate website and the personal data is browser-based and secured by username and related password. After 3 invalid login attempts, the account will be blocked for 15 minutes. The user passwords are not accessible in the system and are stored encrypted in the MedGate database.

New accounts can be created by the users with the corresponding rights. Initial password will be set by the system and can be changed when the user logs in himself for the first time.

3.2.1 User Access via SAML

Users can be managed and authenticated via SAML.

Authentication/Authorization



① User opens Browser

② Request to access MedGate(SP)

③ SAML Authorization Request to IdP

④ If user is authenticated, SAML Tokens are returned to Browser

⑤ The Browser redirects the tokens to MedGate

⑥ MedGate(SP) validates the SAML tokens and returns the secure page to the Brower/User.

The IdentityProvider(IdP) must be provided and configured by the customer.

User management

If an Active Directory (AD) is used as IdentityProvider (IdP) AD Groups will be mapped to a MedGate Accounts (e.g. for a hospital) and AD Users will be mapped to MedGate Logins (e.g. for a doctor). If you move an AD User to another AD Group the MedGate Login will be moved to this other MedGate Account. This will also change the permissions of the MedGate Login, because the Logins inherit the permissions from the respective MedGate Account.
Deactivated or deleted users will not be able to login into MedGate.

SAML Attributes

MedGate represents the user's unique ID in the SAML Attribute Subject.NameID. Mapping to the appropriate Active Directory attribute for the user ID must be done on the SAML server (IdP) using the SAML claims configuration.

3.2.2 User Access via OpenID

OpenID is currently not supported by MedGate directly. However, it is possible to use OpenID via okta-Authentication-Services (https://www.okta.com/)

3.3 E-Mail Dispatch

MedGate has the functionality of generating and sending E-Mails automatically. A PDF file including the requested data is attached to the outgoing E-Mails. E-Mails are send via SMTP to a mail server defined by the customer. E-mails can be encrypted with the TLS standard.

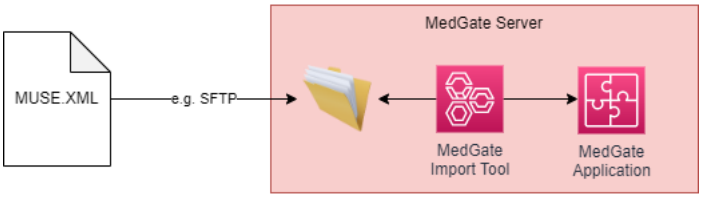
3.4 SMS and Fax Dispatch

User can define numbers in MedGate to which SMS and FAX messages will be send according the configured notification management. External service provider need to be defined by the customer. SMS and Fax service is realized via HTTPS. In case of Fax a tiff file is transmitted and SMS messages are send as text.

3.5 GE MUSE® Import/Export

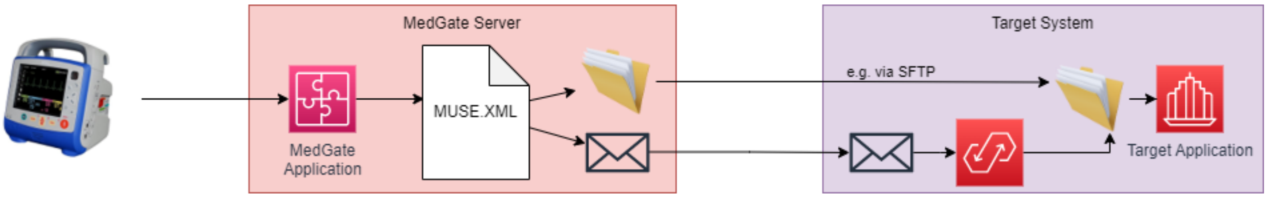
3.5.1 Import

The MUSE.XML file can be placed inside a local folder on the MedGate server (e.g. via SFTP). The MUSE-Import-Tool regularly scans this folder and uploads to MedGate using REST services of MedGate.



3.5.2 Export

ECGs are sent from the X-Series to MedGate. MedGate will generate a MUSE.XML and stores it on the server's local file system (file will be readable by GE MUSE). Access to this folder can be provided by SFTP. No third-party software needed.

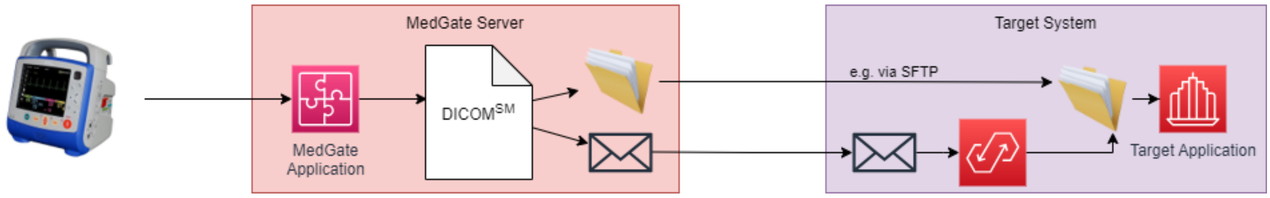


The MUSE.XML file can also be sent by e-mail. A tool is required on the target system to automatically extract the MUSE.XML file from the e-mail to the local file system.

3.6 DICOM^{SM} Export

3.6.1 Export

ECGs are sent from the X-Series to MedGate. MedGate will generate a DICOM^{SM} file and stores it on the server's local file system. Access to this folder can be provided by SFTP. No third-party software needed.



The DICOM^{SM} file can also be sent by e-mail. A tool is required on the target system to automatically extract the DICOM^{SM} file from the e-mail to the local file system.

4. Server Requirements

4.1 Operating System (MedGate Local)

MedGate supports the following operating systems

- Ubuntu 24.04 LTS 64 Bit or newer LTS version **(highly recommended)**
- Windows Server 2022 64 Bit or newer
- Not recommended for new installations but currently supported
  - Ubuntu 22.04 LTS 64 Bit
  - Windows Server 2019 64 Bit

4.2 Operating System (MedGate Hosted)

MedGate Hosted is installed on Ubuntu 22.04 LTS 64 Bit.

4.3 Software Requirements

For normal operation MedGate requires the following software

4.2.1 Apache Tomcat

Apache Tomcat is required for processing MedGate Web application.

MedGate requires Tomcat version 9 or higher.

4.2.2 Apache HTTP Server

Apache HTTP server is needed as backend and central access point from outside.

MedGate requires Apache HTTP server version 2.4 or higher.

4.2.3 PostgreSQL

PostgresSQL 14 or higher is required to store all data.

4.2.4 Java 17

Java 17 is required for running the MedGate web application.

Supported are OpenJDK and Eclipse Temurin.