Towards a secure communication protocol for highly distributed and dynamic eHealth applications

Ola Græsli

Thesis submitted for the degree of Master in
Applied Computer and Information Technology – ACIT

Department of Computer Science
Faculty of Technology, Art and Design

Oslo Metropolitan University - OsloMet

Spring 2022

Towards a secure communication protocol for highly distributed and dynamic eHealth applications

Ola Græsli

Towards a secure communication protocol for highly distributed and dynamic eHealth applications

http://www.oslomet.no

Preface

The subject of this thesis is selected based on interests and a recognized demand in the health care sector. Working as a Paramedic and ICT consultant at Oslo University Hospital over the last years, I have discovered the increasing demand for health care systems. At the same time, I have experienced the need for distributed systems myself. This combination of technical and medical backgrounds gives me an insight into both requirements and opportunities. I wanted to investigate possible solutions for a model that ensures information security at the same time as being easily implementable.

I would like to especially thank my supervisor, Kyrre Begnum, for supporting me through the process of writing this thesis. Thank you for all your academic and technical input and for being a valuable discussion partner when forming the thesis and its content.

Abstract

Demand for electronic health care systems is increasing. In addition to this, more of the systems benefit from being accessible outside of the physical organizations. This is also something that gives users better decision support, which in turn is beneficial for the patients. Health care systems have high demands for information security and are regulated by laws and regulations. Communicating sensitive information forces the systems to prevent unintended data access and unauthorized modifications. Such breaches might be fatal to patients in acute situations. At the same time, there is a demand for availability of data. The thesis focuses on the use case of an ambulance handling situations outside the organization to assess this.

The thesis suggests a model for secure communication of data in health care systems in distributed and dynamic applications. Legal requirements, official standards, and best practices will be evaluated to do this. The suggested model contains central parts of such systems and is intended as a basis for implementation in different types of systems. The options for each of the selected parts in the suggested model are evaluated using an expert review based on the acquired information.

Based on an overview of a general health care system, the selected parts for the suggested model are communication over the different networks, encryption of messages, and authentication and governance of external clients. The expert review of these parts resulted in a socket-based communication directly between the external clients and the central system. To encrypt the messages, AES was selected to ensure the confidentiality of data. A system with private and public keys for the central system and the external clients is used for authentication and governance. By signing the encrypted messages with the receivers' public key, the receiver can verify that the message is from the sender and is not modified. A simple proof of concept implementation tests the combination of the different parts and exchange of messages.

The suggested model creates a platform for possible implementations in both new and existing systems. Parts of the model are according to laws and regulations and follow most

of the suggested standards and best practices. It also seems to fulfill the discovered requirements by the end-users. The model is created based on limited time and resources, which means that more research probably will improve the model further. This might be needed to make this a recognized standard for such communication. Because the model consists of multiple parts, it is possible to adjust some of these and still use many of the suggestions for the rest of the model. At the same time, the suggested model is tested and will work as intended. Therefore, it is possible to implement it in a system and try to get the system approved. Because the model is not created in association with a specific organization, it is not verified that it will be accepted by the responsible for information security in a particular organization.

Table of contents

Table of figures

1 Introduction

Handling of health care information and journal data is strictly regulated by multiple laws and legislations in Norway, as in most countries (Patient Journal Act, 2014). These laws are centered around each health care worker and define what should be documented. They also specify how data should be stored and who should have access to them. Information security is vaguer and specifies that data should not be accessible to unauthorized people. Information security and management of data are regulated in laws on an institutional level and focus on who should have access and options for sharing data (Patient Journal Act, 2014). Locking at the legal aspects of data transfers, these are not that clearly defined. This thesis focuses on transferring data inside the same institution and will therefore not focus on the legal aspect of sharing data between institutions. The laws classify the data as internal data transfers because the data stays inside the same institution. The technical aspects of internal data transfers are not covered directly by laws. The laws say that the data should be secured, but not directly how or a minimum security level.

There are multiple different digital health care systems in most health institutions (Røise, 2016). These are a mix of local installations and more centralized solutions (Røise, 2016). Because many health care institutions have different and some things specialized needs, there are a lot of different applications in use (Røise, 2016). For these to work optimally, they have to communicate and synchronize information. The information in these systems might be stored, owned, and used locally and shared between multiple healthcare institutions. Common for most of these systems is that they are contained inside the institution's secure network, which has secure connections to centralized sources.

Digitalized health care has moved from mainly being handled centralized inside institutions to remote locations and patient homes (Shepperd et al., 2016). This transformation creates the need for more distributed systems that communicate with central systems while still being considered within the same institution. The systems are installed permanently in specific locations and are part of moving health care services. Moving health care services might be nurses coming home to patients or emergency ambulances. This creates a demand for systems that handle communication from different connections with different types of infrastructure available.

Some of the most essential parts of data transfer are to ensure that the correct data (integrity) are transferred in a secure manner (confidentiality) and are available to the right systems or users (Kolkowska et al., 2012). Health systems need to transfer data both from the user to the central system and from the central system to the user. This means that the principles need to be applied in both directions of communication. To do this, the different parties have to trust each other, agree on a secure channel and have a defined protocol. Health care data are often a sensitive matter and should therefore only be accessible to the desired systems and users. At the same time, more advanced systems rely on data from different systems to decide, for example, treatment for patients. This raises the importance of correct data connected to the right patient.

In recent years more and more advanced electronic health registration systems have emerged. Examples of such systems are electronic journals for ambulances, multi-monitors for collecting vital parameters from patients, and patient vital sign chart systems. They are intended for the registration and documentation of health data. This development is also regulated by the health journaling laws, which state that journaling mainly should be done electronically (Patient Journal Act, 2014). The data registered should be transferred in near real-time to ensure updated data across systems and locations. This is because data are used in decision support and remote monitoring. Examples of this are early warning scores and more skilled personnel monitoring from a central or remote location. In addition to the synchronization frequency, the quality of the data is also increasingly more important. This is to ensure the best possible decision support and functionality. Data needs to be transferred both ways. The user enters data and monitors collect data, which are sent to the central system. On the other end, the system may respond to the user with decision support, historical data, and adjusted procedures and guidelines. This generates the need for fast transfers and data processing outside the main site. Managing this gives both increased patient safety and usability.

When transferring critical health information, security and integrity are very important. The security part of this is especially relevant in cases where the data is transferred outside the health institution´s main premises. This might, for example, be to health care workers in an ambulance treating a patient. Security ensures that the data is not accessible to other people and that the users have access to the correct information. This is at least as important concerning integrity because this ensures correct information is connected to the right patient. The integrity of the data is important both ways. When the user accesses data, the information may be a central part of the decision-making regarding patient treatment and monitoring. Data sent to the server must be correct and connected to the right patient. This ensures that incorrect data do not corrupt the data on the server. Users not on the scene, like health care workers at the hospital, will also rely on the data sent to the server to give advice and assess the information; therefore, the integrity of the server will also be important for acute decisions.

In patient information security, it is crucial to ensure that only the intended data about the intended patient is transferred to the right person. Inside a system in a controlled environment, this can be handled by limiting access to networks and inside the application itself. Sometimes patient information has to be transferred out of these secure sones. One of the examples of this is when the incident and patient data have to be transferred to the ambulances, and information is sent from the ambulances to the central system. This creates multiple risks regarding verifying correct data and verification of sender and receiver of the data. Today this is solved by having special channels in the mobile network. Another solution might be to create some kind of persistent VPN connection.

The evolution of health systems and user requirements have created a need for system designs handling issues concerning remote connections, security, large data, and real-time synchronization. It is interesting to investigate different solutions for each part of the system to address this need. These solutions should then be combined in a model that covers the demand according to best practices. Based on the analysis of different technologies and the suggested model, system architects of health care systems can take considered decisions regarding the implementation of such systems. To ensure simplicity and flexibility, this thesis will investigate securing data transfers using the public networks still guaranteeing the security and integrity of the data. The model will then be evaluated according to scalability and performance.

1.1 Problem domain

This thesis will try to identify a suggested model to handle communication between a central system inside an organization and an external device verified by the organization. Based on this, the problem domain for the thesis is:

> *Identify and assess a suggested model for secure communication in highly distributed and dynamic eHealth applications.*

A *model* is needed to describe the suggested parts of a system and their relations. Using the model, different systems can be assessed with it, and it becomes easier to implement the different parts of the model in both existing and new systems.

By using the suggested *model,* systems can benefit from a solution to secure communication that is verified and assessed considering legal aspects, best practices, and available technologies. Having such a model makes it easier for *eHealth* to be developed and made available for users.

The increasing demand of out of hospital health care and more advanced prehospital treatments creates a demand for *distributed eHealth applications*. By having systems available outside of the hospital or institution, health care workers can get more and updated data. This is important to provide the best possible patient care. At the same time, *distributed eHealth applications* increase the need for *secure communication* both between systems and in systems with users physically outside of the institution.

Recent eHealth applications are getting more and more *dynamic*. This means that data flows between the client and the server in both directions, often in real-time. With such data flow, the users get updated information, and centralized systems might provide additional decision support. The *dynamic* data transfer also makes it easier for users to collaborate with each other and see the same data. In health care, this means that specialists can provide assistance to users outside of the institution.

2 Background

Based on the intentions of the thesis, different aspects of eHealth communication will be described. Both laws that systems have to follow, developments in the society, and practical needs will be investigated.

2.1 Laws, regulations and standards

Transferring of health information is strongly regulated and is affected by both laws and regulations in Norway. To suggest a model for communicating health data, it is important to have an overview of the laws and regulations. The laws give general guidelines for how such systems should function and what should be considered. Regulations are more specific and include obligatory and recommended standards. The combination of this gives the legal constraints of the model and is also important when the implementation of the model is considered.

2.1.1 Laws

The treatment of personal information is regulated in the Personal Data Act (2018). This states that personal information should be treated with enough security to prevent unauthorized access and illegal usage, integrity and confidentiality (Personal Data Act, 2018, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Article 5, point 1f). The Personal Health Data Filing System Act (2014, §21) states that the data controllers should do technical actions to ensure an appropriate security level, according to the risks of handling the data. This is also reflected in the Health Personnel Act (1999, §22). Both these refer to an article in the Personal Data Act (2018, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Article 32). This article describes security in the processing of data. The system should ensure confidentiality, integrity, availability, and robustness in systems and services. It also states that risks involved in data processing should be considered when deciding the system's level of security. Prevention of unauthorized access, modifications, and data loss is specifically mentioned.

Laws also regulate the availability of data to health care personnel. The Patient Journal Act (2014) is intended to give good health care to patients by making relevant and necessary information available for health care personnel while ensuring that information security is covered. It explicitly states that the data controller shall ensure that relevant and necessary health information Is available for health care personnel when necessary to provide health care (Patient Journal Act, 2014, $19).

2.1.2 Regulations and standards

There are not that many regulations regarding the technical implementation of eHealth systems. The one that covers most of this is the Regulation regarding standards and national eHealth solutions (2015). This states that the department of eHealth can give out mandatory and optional standards (Regulation regarding standards and national eHealth solutions, 2015, §7). These standards cover both specific implementations and general structures.

The mandatory standard regulating the implementation of general eHealth systems is the Norm of information security and privacy in the health and care sector (Normen) (Department of eHealth, 2020). This describes standards for both governance of such systems and technical implementations. It gives an overview of what should be covered but does not give specifics about technologies and physical implementation.

Some of the optional standards and recommendations give more specific details about the usage of different technologies. One that covers many parts of the implementation of eHealth solution with external data transfer is called Reference architecture for data sharing (Department of eHealth, 2018). Looking at different scenarios for data sharing, it describes recommended architectures and technologies. It also discusses some protocols for transferring data between systems. The main focus is communication between a client in one organization to a system in another. An example of this is access to national registers. This makes it similar to the model covered by this thesis in some ways, but it does not have the same focus regarding communication inside the organization. Because of this, many principles can be used, but some considerations will be different.

Another standard describing communication in eHealth solution is the ebXML standard for message exchange between health care systems (Department of eHealth, 2011). This is primarily used for communication between health care systems. It describes the required format of the data packages sent and standards for encryption and certificates. Some of the recommendations are to use the encryption level RSA-SHA256 and public keys for signing messages.

In addition to these standards, the Norwegian National Security Authority has developed recommendations for ICT security (National Security Authority, 2020). This covers both general security and specific recommendation for ICT systems. Regarding data communication, it recommends limiting the access to the internal network as much as possible. It also states that it is important to control data inside the organization and between organizations, especially if this communication is outside of local networks.

2.2 Demand in the health care sector

The demand for distributed systems in the health care sector is steadily rising (Department of eHealth, 2021). There are multiple reasons for this, but there is no doubt that more advanced treatments and assessments are performed outside the hospital (Department of eHealth, 2021). Healthcare professionals, patients, and relatives are using more advanced systems, which are increasingly more integrated with hospital systems. Studies show that this may increase the quality of the care for more patients and help prioritize which patients need more advanced treatment or follow-ups (Sutton et al., 2020). At the same time, as this is taking patients away from the professionals at hospitals, this is part of the process of handling the increased demand for health care services (Department of eHealth, 2021). Used by health care professionals, such systems may also reduce the need for transportation of patients and reduce risks and wait times associated with hospital visits (Department of eHealth, 2021).

The need for eHealth systems is also mentioned in a government report regarding handling emergency situations outside hospitals (NOU 2015: 17, 2015). It states that the health care sector will have a large technological development. Collaboration inside health care institutions and between such is highlighted as important in the further development. This is connected to the usage of new technology and making knowledge accessible to health care workers.

Studies show that clinical decision support gives better patient care and reduces the risks of errors (Sutton et al., 2020). Some of the success criteria for these effects are that the decision support is easy to use and preferably integrated with other systems (Sutton et al., 2020). Decision support may consist of fixed data and scores or dynamic processing of the available data. The latter will benefit from being processed at a central location because of processing power and access to large amounts of data and analyses. Using machine learning and artificial intelligence has become more common in the health care sector (Sutton et al., 2020). These technologies benefit a lot from centralized solutions, and analysis of health data often requires this because of the restrictions on transferring health data.

When treating a patient and deciding on proper plans for further treatments, access to updated and correct data for the patient is hugely beneficial (Slaatsveen et al., 2018). Having all of the information about the patient gives the best possible background for decision-making. This is also true the other way when health care professionals at the patient ask for decision support from someone not present. Giving them the most updated information about the patient and assessments performed in real-time makes their decision based on the best information available. The development of such collaborative systems is already emerging, and existing systems are being updated to support this (South-Eastern Norway Regional Health Authority, 2021).

2.3 Current eHealth systems

There are multiple systems in the health care sector with integrations to devices outside the health institution. Most of these systems probably use different models for their integrations based on the lack of a standardized model for such integrations and studies with suggested models. The systems have different approaches, depending on the health care institution's general system infrastructure. Some of the more common models are VPNs for single applications or the whole organizational network and solutions for secure remote desktops. Typical for these solutions is that they depend on larger configurations in the general infrastructure. At the same time, they often provide greater access than needed for the specified application. Some of them are also dependent on having complete control over the external user's device.

3 Approach

In the later years, more and more systems have started to be moved outside the hospital. This creates a demand for standards and implementation methods. Today there are multiple laws and superficial recommendations. These do not cover the actual implementation and do not give concrete advice. Because of this, each system creates its own solution to handle the transferring of data, and the systems are assessed individually based on the knowledge present at the time. A concrete model would be beneficial to get one step further in standardizing recommendations for such data transfers of data. Having a standardized model thoroughly assessed and evaluated makes it easier to create secure systems that handle transferring of data outside institutions.

Governance of such data transfers and the parties involved are only vaguely described. This makes this topic also in need of a more concrete model. Having a clear model with best practices for governance will make it easier to implement such systems and be sure to have a thoroughly evaluated system. Creating a model based on current best practices, regulations, and research will create a solid platform for this.

This thesis suggests a model for communication with health care systems from outside the institution. The model is developed based on common structures and practices for communication between users and central systems. Only parts of the entire system will be assessed and described in the model to narrow the scope. The focus is on data transportation between the user and the central system. Handling of the data, system-specific functionality, and user authentication will not be discussed. Based on this, the model suggests secure transportation and authentication of data from the user and data to the user from the server.

To relate the use cases to real-world usage, the main focus of this thesis is on communication from ambulances in the field. The model is general and might be used for most situations where health care workers need to communicate with a central system or other users of a central system. It will also be transferable to other use cases. Because health care data might be very sensitive and critical, the model might be overly secure and complex for some use cases. At the same time, a little too much security and verification might not be that negative if the model is standardized, easy to implement, and well documented.

The selected method to suggest such model is to assess general laws, restrictions, and recommendations and combine these with identified best practices and studies of the separate parts of the model. Different parts of the model will be assessed with an expert review of each part and the combination of parts. These reviews will be matched with common practices, literature, studies, and guidelines in the final suggested model. The different choices will be discussed in light of the described need for such a model and the matching of previous work, laws, and regulations. This will create the groundwork for the practical usage of the model and identify further work in the area.

To identify the parts of the suggested model, a broader common model for health care systems will be identified. This model will be created on a high level, based on prior knowledge of this type of system in general and especially health care systems. The model will be based on common use cases and the general requirements for such systems. The main elements of the model will be described briefly to create a common understanding of the parts and their functionality. This makes the basis of further descriptions and discussions regarding selected elements. The elements chosen for the suggested model will be compatible with this general view, and this creates an understanding of a complete system and the usage of the suggested model.

Based on the general model, the components of the suggested model for this thesis will be identified. These elements will be picked based on the goal of the thesis, namely, to suggest a model for communication between an internal system and external devices with dedicated software. The selected elements will be described in detail, and different solutions for these parts will be presented and discussed. The parts will be placed in the context of a suggested model and discussed in the context of each other.

The model’s components will be investigated based on laws, regulations, recommendations, and common practices. This will be based on the identified recommendations and regulations for such systems. At the same time, common practices, studies, and other literature regarding each of the parts implementation will be identified and discussed. This combination of best practices and regulation will be the basis for recommending the usage of the suggested model and may be an important part of the considerations regarding actually implementing the suggested model in a real system.

Each part of the model will be investigated and assessed by itself and in combination with the other parts. The combination of the best solutions for each part is important to identify a complete model. Both regarding technical possibilities and recommendations and to ensure that the suggested model will work as intended as a whole. This combined model will also be discussed in the same way as each part, focusing on regulations and recommendations. It will also be evaluated against the actual use cases, and the practical usage will be described. To get to the final suggested model, the outline of the model and identified components will be assessed for improvements and possible extensions. This is important to identify the best combination of solutions for each of the parts of the model. The separation of the model into different parts will, in combination with the complete suggested model, make it easier to make adjustments to parts of the model. This might be relevant in case of new technology, adjustments to the organization´s security policy, or architectural constraints in specific systems. By having assessments of both each part and the complete model, much of the considerations presented will be reusable if something is replaced.

The final model will be implemented in a simplified matter to create a proof of concept and identify possible weaknesses. This will be a very simple implementation, just to verify that the solution for each part is working and that the different parts are working together. To take it a step further, the implementation will also assess some of the requirements identified, like the need for fast exchanges of messages and handling of larger amounts of messages in a short time. Because this only will be a conceptual implementation, it will not be set up to run real-life metrics or load testing. Therefore, the results of the implementation will only give an indication of the functionality of the model and not exact measurements. Based on the test of the implemented model and the theoretical assessments, the final model will be evaluated, and positive and negative sides will be pointed out.

This thesis focuses on a theoretical model, and the model will not be implemented and assessed as part of a real system. Therefore it is difficult to make conclusions on how the model will work in actual systems and if it follows a certain institution´s security policy. Because of this, the suggested model will create a basis for further work, both regarding technical implementation and usage and security considerations. Therefore, the goal is to create a suggested model with a good description of the different parts and the general model.

There are also other methods to assess the model, and they have different positive and negative sides. Some of the possible approaches identified are expert interviews and extensive testing. They are not chosen in this thesis for multiple reasons. The main reason is that they are very time-consuming compared to the selected method. This is a factor in this thesis because it is time-limited and has limited resources. Both expert interviews and testing of options for each solution for the different parts might have given more specific results. The goal is to try to compensate for this by using studies of different solutions to identify the pros and cons of the different solutions while matching this with recommendations and best practices. This will create a combination of knowledge and hopefully a well-described and considered model. The suggested model might be the basis for a more streamlined implementation of such a model by suggesting a testable model with considerations as a basis for risk assessments.

3.1 Ethics

This study does not have any direct ethical impacts. The study only looks at present regulations and best practices and suggests a model based on this. Therefore no one is directly impacted by the study. The ethical impacts will be present if someone starts implementing the suggested model, but this is not part of this study.

4 Results

To define the need for a model for communication with devices outside the institution, the general need will be investigated, and some real-world examples will be used for context. The examples will focus on the electronic assistive systems and describe the use of them, this is based on use cases, and many of the solutions are not currently available. This need and the examples will be the base for the further investigation of a model for handling this communication.

4.1 General use cases for data transfer

There are multiple use cases for data transfer in health care settings. They range from specific data connected to a patient to general information about operational data connected to an incident. The data transfer can be split into two parts; data sent to the field and data sent back from the field.

Data sent to the field consists of information transferred from the central systems to the external client. In the beginning, this is often general information about the situation and the patients involved. If the patient’s identity is known, the data might contain previous medical history and critical medical information, like allergies and current medication prescriptions. This information makes it possible for the health care workers to prepare for the situation and treatment. Further into the situation, information from specialists might also be transferred electronically and easily accessible. By entering information about the patient and the current condition and situation, the system will also be able to give knowledge-based suggestions and advice. Having a centralized system also makes it possible to take advantage of big data and predictions based on these. The personnel can also be presented with updated protocols and treatment plans, both general and for the specific patient. This might increase patient safety by checking the planned treatments with current protocols and recommendations. In complex situations, information about the organizational parts of the situations will provide better decision support. This can include special maps, a real-time overview of the incident site, patients’ positions and information, and dangerous sones because of different hazards. Having this information easily accessible, the health care workers can make decisions based on all information available and get a common understanding of the situation.

In the opposite direction, data is sent from the field to the central system. By sending both manually entered and automatically-collected data from the field, the central system gets a good overview of the situation and can provide decision support. This ranges from documented treatment, assessments, and actions performed to real-time data from patient monitors, including vital signs. The data might be used to create a complete overview of the situation and give this to the parties in need of it. Operational data from the field are also a big part of handling more complex situations. Having personnel in the field enter operational data, like patient positions, the number of patients, and, for example, involved vehicles, gives a better understanding of the situation for involved health care workers. This also makes it possible for personnel in the dispatch centers and personnel at the hospitals to work together with the personnel at the scene to handle the situation in the best way possible.

4.2 Scenario one: The traffic accident

Imagine an ambulance responding to a traffic accident. The initial information to the paramedics[1] is very limited. They probably know that it is a traffic accident, the number, and types of vehicles or pedestrians, and an estimate of the number of involved persons. The amount of information is hugely dependent on the individuals reporting it and the investigations they can do[2]. Because of this, the amount of information might be both more and less detailed. When pulling up on the scene, the paramedics can make their assumptions about the accident and the persons involved. Based on this information, the paramedics will start investigating the scene and estimate the forces involved and the severity of the injuries to the people involved. At the same time, this information is shared, by radio, with other

[1] Paramedics are health care workers specially trained in emergency medicine and operational situations outside of hospitals

[2] In addition to the callers' descriptions, there are now possible for the Emergency Medical Control Centers (EMCC) to ask the caller for real time video. Sometimes the accident is on roads with traffic cameras, which are also made available to the EMCC.

emergency services and health care resources. This is crucial for everyone to have the same understanding, priorities, and an estimate of the resources needed.

The main focus of the paramedic, after securing the scene, is to provide the best possible help for the involved persons. This is initially done by getting an overview of the number of involved persons and their severity. Sometimes there are persons in need of immediate care, and they will then be treated right away. When they are stabilized, the most severe injuries will be prioritized. There are specific protocols for handling mass casualty situations and having too many patients in need of immediate care. These will not be explained here, and this scenario will be centered on a scene where there are enough resources and health care professionals.

When approaching the first patient to treat, time-critical actions are initiated. When they have time, the patient's name and national security number are entered into the tablet carried by the paramedics. This information is then used to find the correct person in the central registers. When there is a match, a summary of important health care information is returned to the tablet. Then the paramedic will be alerted right away about possible hazards associated with this person and their medical history. Based on this, the paramedic can adjust the care appropriately. The paramedic also hooks the patient up to medical monitors to monitor the patient’s vital signs. These measurements are continuously transferred to the central system through the tablet. The patient is in a lot of pain, and the paramedic decides to administer some painkillers. Before administering it to the patient, the drug, administration form, and dosage are entered into the tablet. The tablet automatically informs the paramedic about suggested treatment protocols based on available information. Based on the patient’s medical history, the tablet tells the paramedic to be careful with the drug because the patient has had powerful reactions to the drug previously.

After a while, an incident commander arrives at the scene. The incident commander has time to get an overview of the incident and starts to coordinate the health resources. The commander draws up the scene on a tablet on top of the map provided to make it easier to manage. This map already contains the resources on scene. The map is synchronized to the dispatch center in real-time, which gives them the same understanding of the situation. On the tablet, the commander also has access to resources on the way to the scene and a list of patients connected to the incident. The patients are updated in real-time with data collected from medical monitors and entered by the paramedics treating the patient. This gives the commander a complete overview of the scene. By having this and sharing it with the dispatcher, decisions might be made using all information accessible. The dispatcher can then assess the need for additional resources and help the incident commander on the scene. When discoveries are made and the scene changes, the commander makes changes in the interactive map.

One of the ambulances is transferring a patient to the hospital. Because the patient is critically injured, a specialized trauma doctor in the hospital monitors the patient from the hospital. This is done by assessing the information entered by the paramedics and real-time monitoring devices connected to the patient. Based on this, the doctor might advise on treatment on the way to the hospital. At the same time, the doctor can prepare to receive the patient and give further treatment. Because of the real-time data transfer, the system will also notify the paramedics and the doctor about essential changes in the patient's condition. This makes it possible to identify critical changes early and make adjustments to the patient's treatment as soon as possible.

The hospital will have a complete overview of all incoming patients. This makes it possible for the hospital to be ready to receive the patients. They can then prioritize the patients and get alerted if the patients' conditions change. From the monitor, the assigned doctors might also look into the treatments given and make further adjustments to the planned treatment on arrival, based on the prehospital journal.

4.3 Scenario two: Home health care

Another example of when real-time data synchronization will be beneficial is when the ambulance service treats a patient at home. This is something that the ambulance service is doing a lot of. By having information about the patient, the paramedics can give treatment and make decisions based on the most recent information available.

On the way to the patient, the paramedics might read previous journals associated with the patient, assess the patient´s current medications, and other information about the patient. By doing this on the way to the patient, the paramedics are prepared to help the patient and identify potential important information for treating the patient. Because the system is connected to central systems, the paramedics can also read journals from the hospital and review previous findings.

When at the patient, the paramedics wish to discuss further treatment with a doctor at the hospital. Because the system transfers all the data, the doctor at the hospital can review the available data about the patient, assessments noted by the paramedics, treatments given, and current vital signs. This gives the doctor important decision support and a common understanding of the situation with the paramedics.

4.4 The need for a model

The latest years, the usage of mobile systems has increased steadily (Meingast et al., 2006). This has led to the development of different types of software and systems for communication between central systems and users physically outside the institution. These systems use different types of technologies to achieve this communication (Meingast et al., 2006). Some of them use a specialized connection to the internal network. This might have both positive and negative effects. Some of the negative effects of this are that the organization needs to manage the external devices and maintain these strictly. At the same time, such devices pose different forms of risks to the internal network if the user is allowed to add applications and have freedom. Other systems use communication on a per-application approach. This creates a demand for specialized integrations for each application. Common for such systems is that different systems and software use different methods, and it is difficult and time-consuming to verify the security of all the systems. When it comes to health care applications, the complexity of these security evaluations becomes even more demanding. Because of the sensitivity of the data and the consequences of data escaping from the system or wrong data. To simplify this process, a model for such communication would possibly make it easier and more secure to develop and improve health care systems with the ability to communicate with external devices.

Health care outside institutions is getting increasingly complex. There are multiple different usages, and they have a wide range of requirements. One thing that has a positive effect on such systems is the ability to communicate with centralized systems. There might be just a collection of data from a medical monitor but also real-time synchronization and collaboration. The common need is a secure method for transferring data from external devices. Many patients are sent home with medical monitors, both for general monitoring and more extensive monitoring for a shorter period. In these cases, data is most often transferred to a central system, where they are either manually or automatically monitored. With increasingly more complex monitoring devices, the data’s sensitivity and importance are rising.

Looking at the ambulance services, the positive effects of accessible data are gradually discovered. In these settings, there is a demand for transferring data to the central system and acquiring relevant information from the central system. These data might be used in critical situations, which increases the importance of authenticity and integrity in communication. This comes in addition to the general need for confidentiality when dealing with sensitive information.

There is a clear need for medical information and communication of such data in the ambulance service. At the same time, the ambulance service also needs operational data. This includes information about the whole situation, including patients, hazards, and for example, information about an accident site, a multi-story building, or an overview of a remote area. In more complex situations, this operational information might be essential to handle the situation in a good way. Having this information accessible and synchronized gives even better opportunities to handle situations. This makes it possible to have remote parties giving advice and reacting to changes in the condition. Health care workers on scene can easily document and access information and get both manual and automatic recommendations based on the available data. Therefore, operational data might be critical for handling the situation, at the same time as it might contain sensitive information regarding the specific situation and involved parties.

When dealing with sensitive and critical information, the importance of verification and authorization of the sender and receiver of data is highly important. The sender of the data has to be sure that the data can only be read by the desired receiver. At the same time, the receiver must ensure that data received are from a known sender and that the integrity of the data. The content of the data and verification of correct incident and patient are also important but will not have focus in this thesis because that is highly software dependent.

Health care systems, in general, have a quite large backlog when it comes to technical systems (Meingast et al., 2006). Especially when it comes to communication across systems and outside of the physical institutions. There might be multiple reasons for this, like strict budgets, concerns for security vulnerabilities, and limited knowledge between health care workers about what is possible to achieve. It is probably a combination of all these and more factors that have landed the health care sector where it is. The increased focus on technology and electronic communication in the health care sector in the latest years is a step in the right direction (Meingast et al., 2006). Standardizations and predefined models make it easier and faster to develop existing systems and create new systems to meet the further demand and lift the technology used in health care.

In health care, the focus on information security has a large focus, and therefore the basic principles of information security become very important. The basic principles of ICT information security are commonly referred to as confidentiality, integrity, and availability (CIA-triad) (Kolkowska et al., 2012). They are not meant to cover all the information security needs but create a good basis and starting point. Looking at the requirements for health care systems and communication in them, these principles are some of the most important. The confidentiality of health care data is very important and one of the most regulated requirements for such systems. Patients need to trust the systems to handle their data securely and protect it from those who should not have access. This is also an important part of the trust between health care workers and the patients. When using the data given by the system in acute situations, the integrity of the data is important. Acting on the wrong information might be fatal or cause a lot of damage. Along with the development of electronic health care systems, the demand for data availability has increased. This is also reflected in laws and regulations requiring the data controllers to make data available.

Availability of data is also important in acute situations, giving the health care providers the best possible basis for decisions.

4.5 General structure

To make an overview of the field, a general figure of central components in a system with users outside the institution is created (FIG).

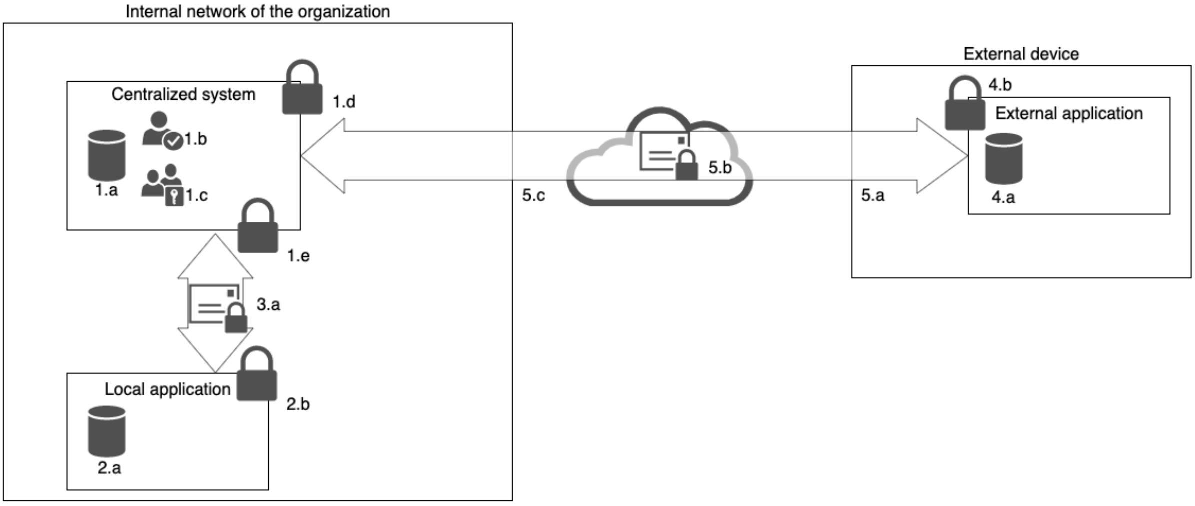

Figure 4.1 General overview

The overview contains the most important part of such system. These parts might then be separated further and implemented using different methods. The components will be described briefly, and these descriptions will be used as a basis for selecting the main parts of the model suggested in this thesis. Because this thesis focuses mainly on communication between the central system and clients physically outside the institution, parts supporting this will be investigated as part of the suggested model.

4.5.1 Local application

The local client represents the client used to communicate with the central system. This client will access data from the central system and is defined as inside the institution’s local network. This means that it is inside the firewalls and other protective measures of the local network.

4.5.2 Central system

The central system represents the server-side of the system. This part is often used as a hub for data transfer and processing. At the same time, it is responsible for providing endpoints to clients for communication. Because of this, it also needs a system to authenticate and authorize clients and users. The specific methods for this might vary between different systems. Because it will receive data from different clients, it also needs a system to handle data integrity.

4.5.3 User authentication in the central system

There are two main types of authentication if we look at the central system in general. The most obvious is the authentication of users in the system (1.b). Secondly, there is sometimes a need to authenticate the client device or the application running on a specific device (1.d, 1.e). Authentication of users is widely used in many systems. There are many common practices and standards for implementing this. The authentication of clients is not that common and is often only needed in some systems. Such systems are, for example, applications that contain or handle data that needs specialized protection, and the server should be able to verify each application. It is also relevant in systems where data is communicated on a per device mode, even if each user is authorized in the application. For example, the application might fetch data before the user is authorized, or the application can access sensitive data, which should only be accessible and handled by original applications.

4.5.4 User authorization in the central system

Authorization of users handled by the central system (1.c). It is assumed that the central system will handle user authorization in the system. This might be done using local or centralized authorization solutions.

4.5.5 Data storage

Data storage is handled on multiple levels. In this structure, there are data storages in the local client (2.a), the central system (1.a), and the external client (5.a). It is assumed that each of the data storages can be separated from other applications and, therefore, might store information connected to the structure’s information security, such as private keys. There are different solutions for this based on the technology used and technical platform.

4.5.6 Data transfer protocol

There are different methods to transfer data between systems (3.a, 5.b). For example, HTTP and sockets. The structure has data transfer from the central system to both the local and external clients. It is not required that these two use the same protocol. Based on general security recommendations, protocols should be used with encryption.

4.5.7 Local client to the central system

The communication between the local client and the central system is handled inside the organization´s local network (3.a). Because of firewalls and other security features normally in an internal network, this communication will be hard to intercept in general.

4.5.8 External client

The external client consists of both the external physical device and the specific application running on the device, which communicates with the central system. In general, the device might be of any standardized type. The requirement is that it supports standard security protocols and is based on a platform with common security features available.

4.5.9 External communication to the central system

Communication between the external client and the centralized system is central in this structure. The communication path consists of multiple steps. First, the communication goes from the application on the external device to the device’s communication ports (5.a). From the device, the communication passes through public networks before it reaches the organization’s network (5.b). From the organization’s network, the communication is sent to the central system (5.c). Communication from the central system to the application on the external device follows the same path in reverse.

Along this path, multiple steps require special attention regarding security. Some of the most important are the communication of sensitive data from the central system and external device´s application and communication between the organization's network and external networks, including the internet. Sending data out of the system means that other applications on the server, devise, or local network might try to read and modify the data. The communication between the internal network and external networks provides a possible vulnerability. The security of this has to be assessed to ensure that malicious communication cannot intrude the internal network and the centralized system.

4.6 Selected elements

Based on the general model, the most important parts for communication between external clients and the central system are selected for the model in this thesis.

The main elements for the model are (highlighted in green and red in Figure 4.2):

1. Communication between the external client and the central system
2. Encryption of the messages
3. Authentication of the external client

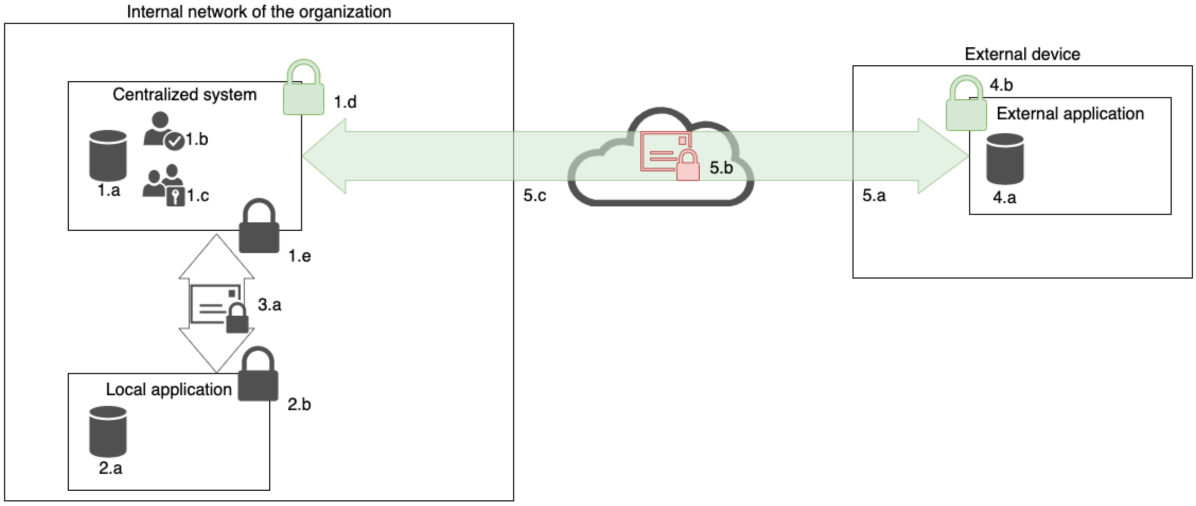

Figure 4.2 Selected elements of the structure (highlighted in green and red)

Some parts are also relevant in such communication, which is not covered in the suggested model. Most notable is the authorization of the user and the specific data transferred. The reason for this is that this is often application-specific and will therefore limit the usage of the model. At the same time, this can be done in the same way for users on external and local clients. As long as the model ensures that the external client is authorized and that the data and commands are correct from the expected client.

4.6.1 General principles

The suggested model is limited to the communication between the central system and the external client. It will not provide solutions for application-specific features like user authentication and management. The focus is to provide a secure way to communicate between the central server and the external client. This includes the protocol for data transfer, the authentication of external clients, and the integrity and confidentiality of data.

4.6.2 Data transfer

There are multiple different methods to transfer data between client and server. When deciding which method to choose, multiple factors should be considered. Some of the most common are HTTP (TCP) and sockets (Yokotani & Sasaki, 2016). All the protocols have options with encrypted communication. It will be natural to use this encryption by default, as recommended.

HTTP is one of the most used web-protocol and supports a wide variety of usages (Yokotani & Sasaki, 2016). In this case, it is an option for communication between the server and the client. The HTTP protocol is good when a continuous connection is not needed. This means that each request is treated as a new connection, which has both positive and negative effects. Some positives are that there is only a connection when there is a need for communication, and periods of time without a connection between the client and server are easier to handle. Only establishing a connection in the event of communication makes sense when there are periods of time without communication because it does not continuously keep the connection between the client and server open. On the negative side, there is some overhead if there is a lot of communication between the client and server. In modern systems, this is normally not noticeable.

Sockets are something that is getting more popular (Yokotani & Sasaki, 2016). They allow the client and server to have a persistent connection. This means they only have to establish the connection one time and, after that, might send data back and forth through the established channel. Some of the concerns regarding this method are that it uses some resources holding the connection open and might have trouble with reconnection in conditions with an unstable connection between the client and server. Most of these concerns have been addressed and handled in standardized libraries for using sockets. This means that error handling and reconnections often are implemented or easy to handle. At the same time, the cost of having a connection open is very limited in today's internet availability. One of the biggest advantages of sockets is the fast communication between the different parts. This means that a lot of communication might be done in a short time.

One of the most established standards for communication using sockets is MQTT or, more specific, AMQP (Yokotani & Sasaki, 2016). This technology is also recommended by the department of eHealth in Norway (Department of eHealth, 2019).

4.6.3 Encryption

Even if the channel used for communication is encrypted, it is good practice also to encrypt sensitive data in addition to this. This limits the risk of sensitive data being accessed by others. At the same time, it might also be an extra layer of security to ensure that the data is only decryptable by the designated receiver. By using keypairs for encryption and decryption, one can encrypt the message based on the receiver's keys. This ensures that only the designated receiver might decrypt the message. One of the disadvantages of encryption is the extra processing power it takes to encrypt and decrypt messages. Having a system with frequent communication this is added to the processing time for both parties of the communication. Both encryption and decryption are relatively fast in modern software, which means that this is a limited problem in most situations.

There are multiple different encryption methods. One of the most commonly used is AES. AES is also recommended in multiple studies comparing the security and usability of encryption methods (Akhil et al., 2017; Boonyarattaphan et al., 2009). AES is also the recommended encryption standard in the government recommendation for message encryption in communication between health care systems (Department of eHealth, 2011).

4.6.4 Authentication and authorization

In a system, authentication and authorization might be handled on multiple levels. Most common is the direct authentication and authorization of a user in a certain system. This can be handled both by local user management in the system or by using a central user management system. Because this is specific to the application, this level will not be discussed further in this thesis.

Authentication and authorization on the server level are interesting in multiple different settings. For example, when sensitive or valuable information is being transferred and when data is transferred without a logged-in user. This means that the server and the client device have authenticated and authorized each other. They might exchange keys or other proof that they are whom they say when communicating to accomplish this. It is important that this identification is hard to forge and can't be picked up and used by third-party systems. Suppose the server is communicating with an external client. In that case, the server or system must ensure that the client application is valid and not some software trying to intercept the communication. This method might both be used on a client device or a certain software on the client device. The latter is highly relevant if the client device is not fully controlled by the organization, which means that the organization has control of all the device's content.

Some systems also use authentication and authorization on the network level. This is most commonly done through VPN (Virtual Private Network) or whitelisted IP-addresses. Sometimes special networks are also used, like local communication lines between businesses or separate mobile networks. The goal of these methods is to limit access to the server. Limiting the allowed traffic or client connections to the server limits the possibilities for malicious third parties to access the server. Some of the downsides of these systems are that they often authorize the whole device to access the server and the network. This might be a problem if the organization does not control the devices connecting fully because malicious software on the device might listen to the communication and try to use the secure channel for communication. At the same time, each device has to be configured in a certain way to make the connection, and the organization has to have a system handling authorization of the connected devices centralized for the network.

When it comes to authentication and authorization of important data, multiple of the above methods are often combined to ensure the security. The user-level is almost always included in some way. This also ensures that the system has control of which users have done what in the system. Users or groups of users are also often used to control authorization in the specific system on a lower level. This means that there is not a choice between different methods regarding this, but rather a choice of combination. Both the server and network-level are often only used to ensure that the client is allowed to talk to the specific server or system. Then the more specific access to parts of the system is handled on the user level.

4.6.5 Governance

Having set up a method for authentication and authorization is only the initial part of the process. The more complex part is to ensure that the system is up to date with both authenticated and authorized clients and users. This is important to handle both devices that are not used anymore, lost, or should be banned. There are multiple approaches to handling these situations. Central systems for handling governance of users in the organization are now part of the standard in health care applications (Department of eHealth, 2020). At the same time, the methods to handle this might vary between the different methods.

The governance of devices is more complex because they are not necessarily connected to specific users. This is, for example, the case in ambulances where the device follows the resource and not the users. In such cases, there is a need for a special system for governance of the devices. The easiest is just to have this done manually, but that leaves the system open for manual errors, and the probability of devices not being removed at the correct time is high. This might be prevented by adding systems to help administrators in the revision process. One of the simpler checks that can be added is a time limitation of the registration. This ensures that each device is reviewed at every fixed interval. By using a system like this, the possibility of devices being forgotten is limited, at least in each revision. One might argue that this process might be time-consuming and that the users will find shortcuts in the process, like renewing all devices without reviewing this. This is a negative effect of such a system. The extent of this will probably vary based on the number of devices and resources used to review them.

A more sophisticated method for the governance of devices is to have a central authority. Because the model in this thesis is supposed to cover a single application in a more or less unknown environment, this might be more complex. At least if the organization implementing this does not have a storage and management of keys for devices. A hybrid solution to cope with this is to have the keys stored in the system itself but check the device id with a central management solution. By using a trusted central system to check for allowed devices, the system can almost instantly indicate or even revoke devices that should no longer have access.

4.7 Suggested model

Some general decisions are made to create a suggested model for this communication. Based on these decisions, each component will be discussed and evaluated. The suggested model will be based on the considerations made in the sections for selected components for the model.

4.7.1 The components

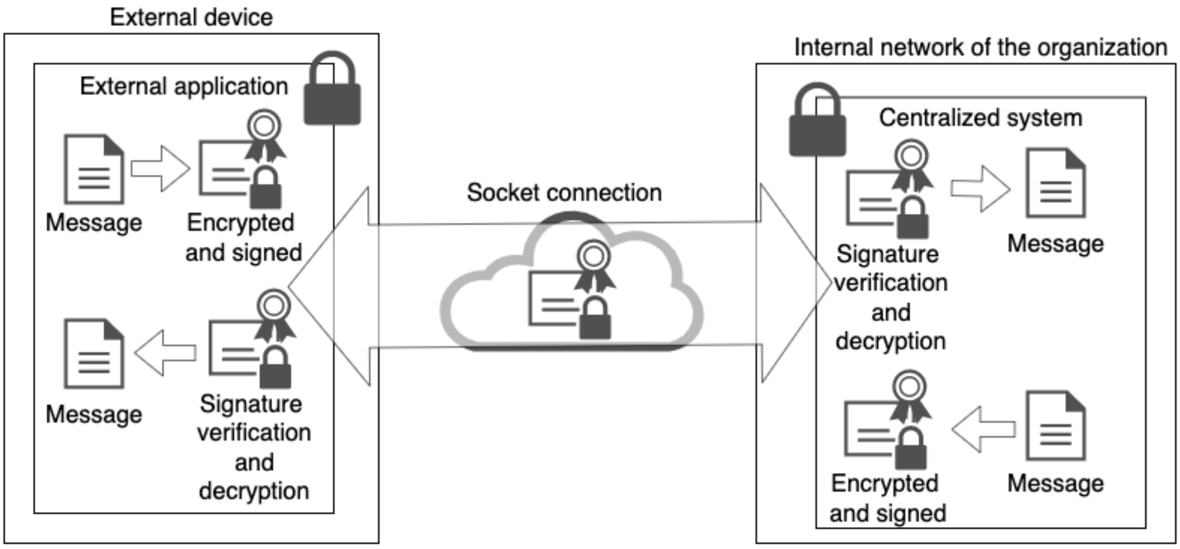

Figure 4.3 Overview of selected suggested model

Based on the context and practical usage used as background for this thesis, the selected communication method for the final model is sockets (Figure 4.3). This is mainly because of the fast communication regarding an incident when it is active. It ensures fast communication and makes it easier to transfer data in real-time. The protocol is also verified in government recommendations and research.

To ensure encryption of the data, AES encryption will be used. This is a standardized and widely used method. The suggested model does not cover user authentication in the application but covers the authentication and authorization of devices. This will be handled by having a system where the server only accepts messages from clients that are previously authorized. The same will be for the clients where they only accept messages from the correct server.

Governance of the devices and certificates will primarily be handled in the system itself, but with a hybrid approach where the devices might be checked against a central system. This ensures that the model requires minimal of general setup in the organization, at the same time as it covers the increasing demand for central authentication and authorization.

4.7.2 Usage of the model

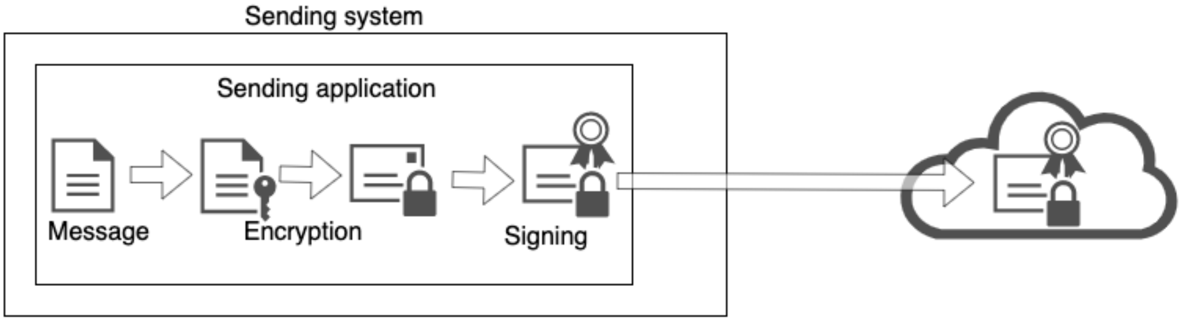

Figure 4.4 The system sending a message

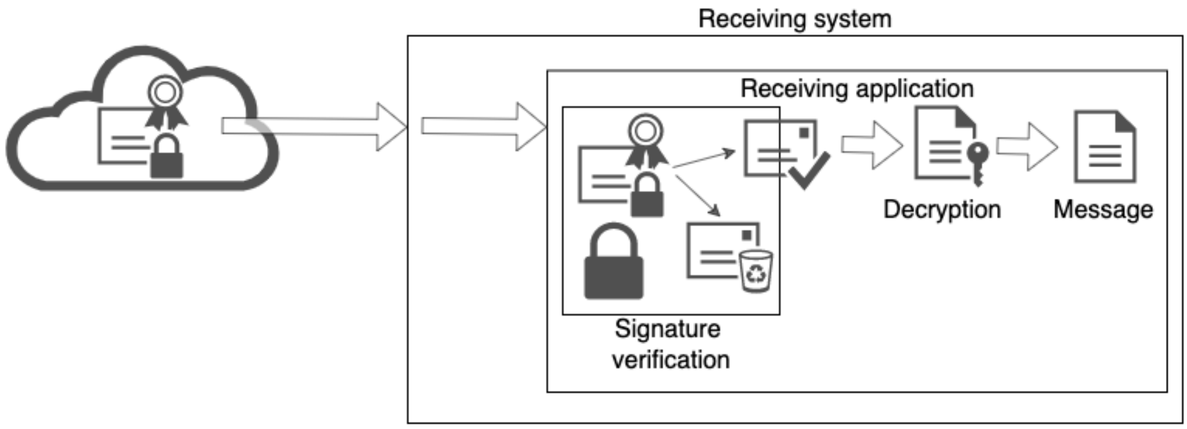

Figure 4.5 The system receiving a message

Having the components for the model figured out is a good start, but to make a complete model, a specification for implementation is also needed. To describe this, the implementation of each part will be presented. First with a technical focus and then practical usage of the model.

One of the first obstacles in the system is the communication between the external client and the internal server. Having openings to external systems from an internal server is a possible security risk. This risk increases when the data communicated and available on the server is sensitive. At the same time, one of the goals of the suggested model is to make it easy to implement with minimal configuration of the general systems. Therefore it is suggested to open a port on the server for external communication. To prevent malicious usage of this port, it is important to strictly control the data being transferred over it. This will be handled by using one of the security mechanisms of the messages transferred. The measure is to sign all the messages with the private key of the client (Figure 4.4). When the server receives a message from an external device, it can then check if the message’s signature matches the client sending the message (Figure 4.5). This ensures that the server can ensure that only messages from allowed clients will be processed. The rest of the messages will be discarded. Al the communication will, as suggested, also be using the basic SSL encryption provided by the socket protocol.

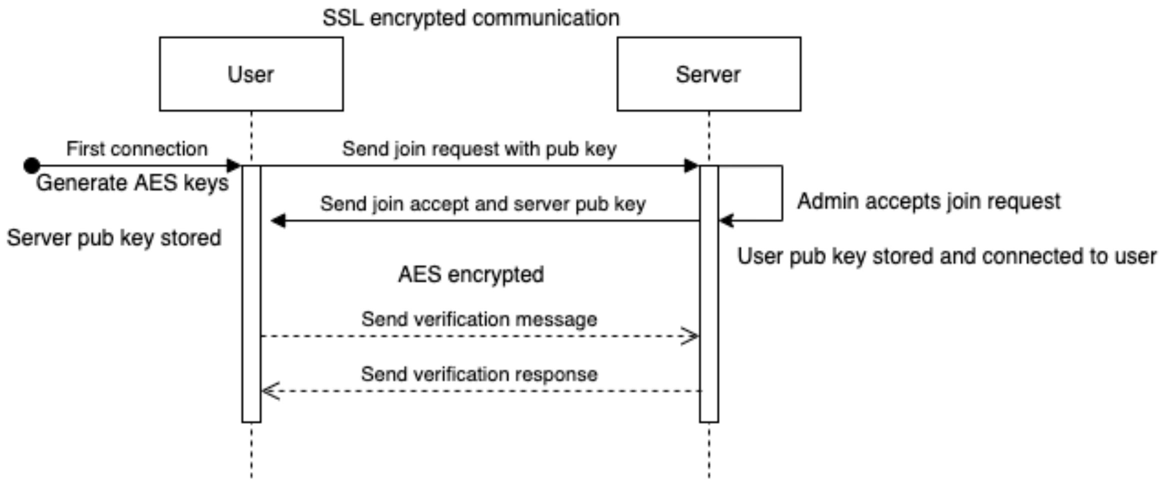
SSL encrypted communication
User
Server
First connection
Generate AES keys
Send join request with pub key
Send join accept and server pub key
Admin accepts join request
Server pub key stored
User pub key stored and connected to user
AES encrypted
Send verification message
Send verification response

Figure 4.6 First connection flow

To manage devices and authentication and authorization of these, it is important to have a secure and efficient system. In the suggested model, this will be administered manually. The main reason for this is that this ensures that each device trying to connect is evaluated and accepted only if it should. In the suggested use case, where devices are shared between multiple users, the inclusion of new devices is limited. This justifies the manual process and makes it possible to have a strict management of devices. The device will send an inclusion request to the server, including its public key (Figure 4.6). This prompts the administrator to review the device. When the device is accepted, it will receive an acceptance notification in addition to the server's public key. At the end of this process, the server has a connection between the device and its public key, and the device has the correct key for the server. If the server is connected to a central device register, the device and public key might be linked to this. This makes it possible to manage devices centrally, and changes to the devices in the central system can be used in this system.

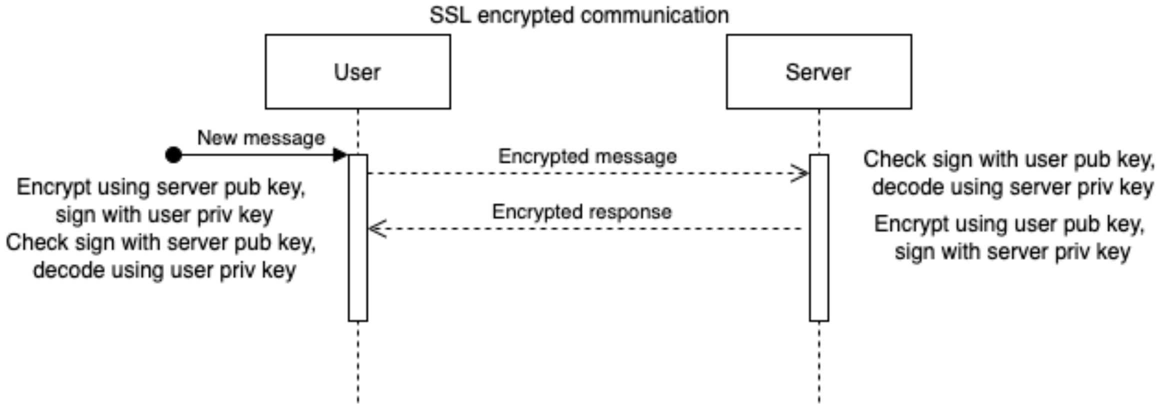
SSL encrypted communication
User
Server
New message
Encrypted message
Encrypted response
Encrypt using server pub key,
sign with user priv key
Check sign with server pub key,
decode using user priv key
Check sign with user pub key,
decode using server priv key
Encrypt using user pub key,
sign with server priv key

Figure 4.7 Sending and receiving messages flow

Ensuring that each message between the device and the server is properly encrypted is important. At the same time, it is important that messages are from whom they say they are from. To ensure this, two different methods will be used. First, the message will be encrypted with the receiver’s public key (Figure 4.7). This makes the content only accessible for the part having the corresponding private key. If the message gets intercepted or read by someone on the way between the dedicated software on the client and the server, it will not be possible to extract the content. A signing process will be used to handle the second part, which is to ensure that the message is from an accepted sender. The encrypted message will be signed with the private key of the sender. This makes it possible for the receiver to check the signature against the public key register of accepted devices on the server and servers on the device.

To govern the accepted devices, there will be a few options. The main functionality will be inside the system, where administrators can manage accepted devices. A periodic review of all devices will be possible to ensure that the list of accepted devices is updated. This means that all devices will be scheduled for periodic review and might be automatically removed or disabled if they are not renewed. Another possibility is to connect the system to a central management of devices, where each device in the system is mapped to the central system and, therefore, might be managed from the central device register. This makes the suggested model work by itself, at the same time as it facilitates the usage of centralized authorization.

4.8 Analysis

The laws and regulations in Norway clearly state that protecting sensitive information is essential. At the same time, they state that information should be accessible and available through the whole health care system, as long as the information is needed for patient care. Looking at prehospital situations, especially in the ambulance service, the patients might have illnesses or injuries that require acute care. In these situations, the need for correct and updated information about the patient is important.

In addition to the laws and regulations, there are also some recommendations that are used in the health thrusts in Norway. One of these is Normen (Department of eHealth, 2020). This recommendation describes high-level guidelines and recommendations for information systems. Because the recommendation does not contain specific descriptions of technologies and methods, this is missing from the ecosystem. Some organizations might have internal implementations, but there is not identified any such on a general basis, describing best practices and scientific-based implementation suggestions.

There is a well-documented need for eHealth systems and the usage of such outside of health care institutions. Even if some models and architectural recommendations are available, a general model for communicating information with external devices inside the same system is not discovered. The suggested model is also based on recent studies and recommendations.

The suggested model described in this thesis covers the communication between software running on an external device and software running on an internal server. Separating the model into parts gives a highly flexible model where the different parts might be changed based on new knowledge and regulations. At the same time, each part is discussed and assessed by itself and in combination with the rest of the parts. This gives the model a transparent architecture, and each decision might be evaluated by itself and in the context of the complete model.

Parts of the suggested model are selected based on an expert review of the available implementations and standards. These are evaluated based on the legal constraints, recommendations, best practices, and an expert evaluation of the technologies themselves and as part of the final model. Based on these, the suggested model consists of parts that are compatible and possible to implement as part of a more extensive system. Integration with central systems like authentication and authorization is also considered.

One of the main concerns in the suggested model is the direct communication between the external device, through external networks, to the central system. This exposes the central system to external networks, which increases the risk of malicious attacks against the server. The positive side of this is that the external devices do not have to be controlled entirely by the organization, even if it is recommended. It also enforces an end-to-end encryption scheme, which protects the messages from unauthorized access by other systems on the server and devices. Other software on the external device does not have more access to the organization's network, which might have been the case if the device was connected through a VPN. Therefore, the exposed system enforces strict security mechanisms and verification of all connections. By checking the signature of the messages on arrival in both the central system and the external application, malicious data is filtered out before the message is opened. Using a private-public key scheme for signing the messages, attackers won't be able to decode the content of the messages, change the content or send malicious messages.

A simple proof of concept is created to verify that the suggested model is possible to implement and that the identified needs will be solvable using the model. This is not a full implementation of the model but is designed to test the parts of the model together. The implementation shows that the model is implementable and handles the identified high-level needs of such a model. Even if this implementation is not created to benchmark the model, it shows that the model can handle relatively large amounts of data in a short amount of time.

5 Discussion

Looking at the suggested model, it follows much of the recommendations and standards described. It is also according to laws and regulations concerning this, even if these are formulated in very generalized terms. Each part of the suggested model is discussed regarding standards and research. This means that the different parts at least are evaluated against these. One decision that is not entirely according to all the recommendations is the decision to have communication over an open network. This exposes the messages and access points of the parties to the open network. Most recommendations say that communication should be done through secure channels like VPN. This decision makes the model easier to implement, and it does not require the configuration of such secure channels between the server and external clients. It also does not create the requirement of a setup on the external client. This thesis argues that this is handled sufficiently because of the suggested model's security mechanisms. Using the recommendations regarding key pairs and signatures, the content of the messages is secured, and the signatures ensure that the messages are sent from a valid part and not modified. This approach is also commonly used in other secure systems available on open networks. Examples of this are online government information about citizens and banking applications. These use technologies like this and are considered secure enough.

The potential impact of the suggested model is somewhat unclear. Multiple factors affect how significant an impact it will get. Potentially it might be the groundwork for a standardized communication in health care systems using open networks as a message carrier. This might make it easier for more health care systems to be easily available to users outside the organization’s network. It can also reduce the need for specialized and managed devices, reducing hardware and technical costs. At the same time, the thorough evaluation of each part and the model as a whole might be used as documentation that the approach is acceptable regarding information security. This is important to make the suggested accepted by the health care organizations and then be used by software providers.

The results and analysis of this thesis suggest a defined model with specific technologies and parts. The suggestion is made based on the information discovered in each topic and is set in context using an expert review. Based on this, the suggested model should be seen as a suggestion on the way to the best possible model for this use case. Each part might have improvements, and organizations might have specific reasons to make adjustments. Therefore, this is also a groundwork and analysis of different possible components. The suggested model is verified and will work but is, first and foremost, a suggestion of a development direction.

This thesis uses an expert review to identify a suggested model for handling external communication in an eHealth system. There are both pros and cons in regards of using this approach. The background gives a broad base for further decisions regarding technology and use cases. For each of the suggested model parts, there is an evaluation of different alternatives and research supporting this. More aspects and research might be discovered in a more extensive or more specific assessment of components. At the same time, the selected approach makes the evaluation transparent and easy to extend. The final decision on components and suggested model is made using an expert review. This lets practical experience and knowledge affect the different choices. These decisions might be questioned, but most decisions are also supported by standards and research in the suggested model.

Part of the intention of the suggested model is to create a generalized framework. The proposed components are standardized technologies available in most development frameworks. This means that the model is not limited to specific architectures or setups. All the proposed parts are also open-source technologies that are accessible to everyone. This is important to have a model that might be used in as many systems as possible. The structure with different parts evaluated separately makes it possible to make adjustments to the model at the same time as most of the considerations are valid. This might be relevant if organizations have specific requirements for some technologies or standards. In the selection of components to include in the suggested model, most application and organization-specific components were not added. This is also part of making the model generalized. Each organization and software provider can use different technologies together with the suggested model. For example, user authentication and authorization, and message formats do not affect the suggested model. This is also part of making the suggested model easier to implement in existing systems.

This thesis has some limitations regarding the research method and collected information. Because of the timespan and available resources in the project, the information collected and analyzed is limited. This also means that the evaluations might have missed research and best practices. To compensate for this, government standards and recommendations are part of the analysis and used in the different decisions. This does not mean that these are the best solutions, but these suggestions are at least performed by specialists and based on actual implementations in health care systems. The expert review might also be affected by the expert’s previous experience and experiences.

With more time and resources, the suggested model would probably have benefitted from evaluations performed by multiple experts and more research. More practical testing of the different components and performance analysis might have affected the model. These are methods that might be relevant if the suggested model should be developed further and made a more generalized standard. Additionally, the model should be evaluated by information architecture experts and information controllers at different organizations. This will highlight concerns regarding the model and its actual usage.

Based on the discovered needs and use cases, the suggested model seems to fulfill these. Because this is just some part of a complete system, it is not just to implement it in production. It depends on a complete system handling the users’ requirements and necessary functionality. The model also has to be accepted by the responsible for information security in each organization. Having a defined model will make it easier to develop and get acceptance for external usage of the organization´s systems. This will, in turn, give the users and possibly patients better information and decision support.

Looking at a broader usage of the suggested model, there are multiple possible extensions and use cases. Some of the identified possibilities are using the model in server-to-server communication and device-to-device communication. These extensions can also be combined with the primary use case and, for example, be used for communication between multiple devices before communicating with the server. This will be kind of a hybrid solution. By having a verified and accepted model, such extensions become much easier.

6 Conclusion

The suggested model proves to be a good model for handling communication with external devices. There is still some work left before the model can be used in an actual system, but much of the groundwork is in place. The considerations presented will provide a solid decision basis for the selection of technology, actual implementation, and security assessments. Even if the suggested model has specific components, there are multiple similar components. Therefore, some adjustments might be needed or give better solutions based on the specific system. Overall, the suggested model covers the main goal of being a model supporting secure communication in distributed and dynamic eHealth applications.

To take the suggested model further, it needs to be implemented as part of an actual system and approved by information security specialists.

Each component might be tested and optimized further and therefore possibly tuned to create more security and better communication. The model might be developed and improved further by including more research, multiple experts, and testing different components.

7 References

Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017, 23-24 June 2017). Enhanced cloud data security using AES algorithm. 2017 International Conference on Intelligent Computing and Control (I2C2),

Boonyarattaphan, A., Yan, B., & Sam, C. (2009, 28-30 Sept. 2009). A security framework for e-Health service authentication and e-Health data transmission. 2009 9th International Symposium on Communications and Information Technology,

Department of eHealth. (2011, December 2020). *ebXML Framework*. https://www.ehelse.no/standardisering/standarder/ebxml-rammeverk-v1.1

Department of eHealth. (2018). *Reference architecture for data sharing* (HITR 1215:2018). https://www.ehelse.no/standardisering/standarder/referansearkitektur-for-datadeling/_/attachment/inline/33e8a3a6-2061-47db-bfd2-08b0e09bb108:d812f427533dfb987463cc459b35b981f5096505/Referansearkitektur%20for%20datadeling.pdf

Department of eHealth. (2019). *Recommendations regarding usage of AMQP against national systems* (HITR 1224:2019). https://www.ehelse.no/standardisering/standarder/anbefaling-om-bruk-av-amqp/_/attachment/inline/28987aae-45ff-465b-b2e5-406199cbdf2d:6f16fabdd94b05a3ba50b93f4ddf0573ba5b84e2/Anbefaling%20om%20bruk%20av%20AMQP%20mot%20nasjonale%20l%C3%B8sninger.pdf

Department of eHealth. (2020, 13th April 2021). *Norm of information security and privacy in the health and care sector*. Retrieved 14th May 2022 from https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

Department of eHealth. (2021). *Development trends 2021*. https://www.ehelse.no/publikasjoner/utviklingstrekk-2021/_/attachment/download/fa9c435e-c091-4ed5-a317-d371e7c53e91:64107c00782cb9b24db8d7c8b235fe592c3880de/Utviklingstrekk%202021%20E-helsetrender%20oppdatert%20versjon.pdf

Health Personnel Act. (1999). *Act of 2 July 1999 No. 64 relating to Health Personnel etc.* . Lovdata. https://lovdata.no/dokument/NL/lov/1999-07-02-64

Kolkowska, E., Hedström, K., & Karlsson, F. (2012). Analyzing information security goals. In *Threats, countermeasures, and advances in applied information security* (pp. 91-110). IGI Global.

Meingast, M., Roosta, T., & Sastry, S. (2006, 30 Aug.-3 Sept. 2006). Security and Privacy Issues with Health Care Information Technology. 2006 International Conference of the IEEE Engineering in Medicine and Biology Society,

National Security Authority. (2020). *General principles for ICT security 2.0*. N. S. Authority. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0

NOU 2015: 17. (2015). *First and foremost - An comperhensive system for handling acute medical and trauma situations outside of hospitals*. D. o. h. a. care. https://www.regjeringen.no/no/dokumenter/nou-2015-17/id2465765/

Patient Journal Act. (2014). *Act of 20 June 2014 No. 165 relating processing of data concerning health in connection with the provision of healthcare* (LOV-2014-06-20-42). Lovdata. https://lovdata.no/dokument/NL/lov/2014-06-20-42

Personal Data Act. (2018). *Act of 15 June 2018 no. 38 relating to the processing of personal data* (LOV-2018-06-15-38). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38/

Personal Health Data Filing System Act. (2014). *Act of 20 June 2014 No. 43 on Personal Health Data Filing Systems and the Processing of Personal Health Data* (LOV-2014-06-20-43). Lovdata. https://lovdata.no/dokument/NL/lov/2014-06-20-43

Regulation regarding standards and national eHealth solutions. (2015). (FOR-2015-07-01-853). https://lovdata.no/dokument/SF/forskrift/2015-07-01-853

Røise, M. B. (2016). 17 000 forskjellige mennesker bestemmer hvilke systemer som skal brukes. Det har skapt store, uheldige problemer. *Digi.no*. https://www.digi.no/artikler/17-000-mennesker-bestemmer-hvilke-systemer-sykehusene-bruker-det-har-skapt-store-problemer/349244

Shepperd, S., Iliffe, S., Doll, H. A., Clarke, M. J., Kalra, L., Wilson, A. D., & Gonçalves-Bradley, D. C. (2016). Admission avoidance hospital at home. *Cochrane Database Syst Rev*, *9*(9), CD007491-CD007491. https://doi.org/10.1002/14651858.CD007491.pub2

Slaatsveen, I., Stavnesli, I., Halsetrønning, J., & André, B. (2018). Elektroniske omsorgsmeldinger gir bedre og sikrere dokumentasjon. *Sykepleien forskning (Oslo)*(70599), e-70599. https://doi.org/10.4220/Sykepleiens.2018.70599

South-Eastern Norway Regional Health Authority. (2021). *Safer and easier to collaborate about the patient inside and outside hospitals*. Retrieved 15th May 2022 from https://helse-sorost.no/seksjon/nyheter/Sider/Tryggere-og-enklere-%C3%A5-samarbeide-om-pasientene-i-og-utenfor-sykehus.aspx

Sutton, R. T., Pincock, D., Baumgart, D. C., Sadowski, D. C., Fedorak, R. N., & Kroeker, K. I. (2020). An overview of clinical decision support systems: benefits, risks, and strategies for success. *NPJ Digit Med*, *3*(1), 17-17. https://doi.org/10.1038/s41746-020-0221-y

Yokotani, T., & Sasaki, Y. (2016, 12-14 Dec. 2016). Transfer protocols of tiny data blocks in IoT and their performance evaluation. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT),

8 Appendix A

See attachment “Appendix A – Poster.pdf”.