Chapter 10
The Ring of Trust Model

C. Kollmitzer and C. Moesslacher

10.1 Introduction

The following chapter deals with a possible application of methods of quantum cryptography to permit secure communication between parties in different architectures by establishing a Ring of Trust. The aim is to solve the problems of key distribution with methods of quantum cryptography without being limited by their transmission range. At the same time, a high level of security is obtained, which is ensured by the use of corresponding cryptographic algorithms. The model is not restricted to certain cryptographic algorithms. Therefore, it is possible to enlarge a preexisting system with new cryptographic algorithms or to replace formerly employed cryptographic algorithms with new ones.

The model presented here limits neither the number of communication parties nor the maximum distance between the different parties. Quantum key distribution (QKD) has now reached a stage of maturity which makes it possible to implement QKD into existing infrastructures, for example, in medical information systems (MIS), and thus enhances their security level significantly. Medical information systems are a critical field because patient-related data and surgery data are both confidential and a subject to legal restraints. Furthermore every kind of medical data has to be highly available.

There also arise new services from this field which can only be implemented if a secure transmission and storage of data can be guaranteed.

C. Kollmitzer (✉)
Safety & Security Department, Quantum Technologies, AIT Austrian Institute of Technology GmbH, Lakeside B01A 9020 Klagenfurt, Austria,
christian.kollmitzer@ait. ac.at; http://www.ait.ac.at

C. Moesslacher
Safety & Security Department, Quantum Technologies, AIT Austrian Institute of Technology GmbH, Lakeside B01A, 9020 Klagenfurt, Austria, christian.moesslacher@gmx.net

Kollmitzer, C., Moesslacher, C.: *The Ring of Trust Model*. Lect. Notes Phys. **797**, 185–210 (2010)
DOI 10.1007/978-3-642-04831-9_10

10.2 Model of the Point of Trust Architecture

Two communication parties who want to communicate can be in two different Trust Zones, as shown in Fig. 10.1. In order to communicate they have to rely on a Point of Trust they are assigned to. Each client is connected to its Point of Trust via a quantum channel. All clients of a single Point of Trust form a Trust Zone. Different Points of Trust are connected to each other either directly or via other Points of Trust using either a public channel or a quantum channel. Also the different clients are connected via a public channel, but in order to have a secure communication beyond their Trust Zone they have to establish a session key via their Points of Trust and the corresponding network.

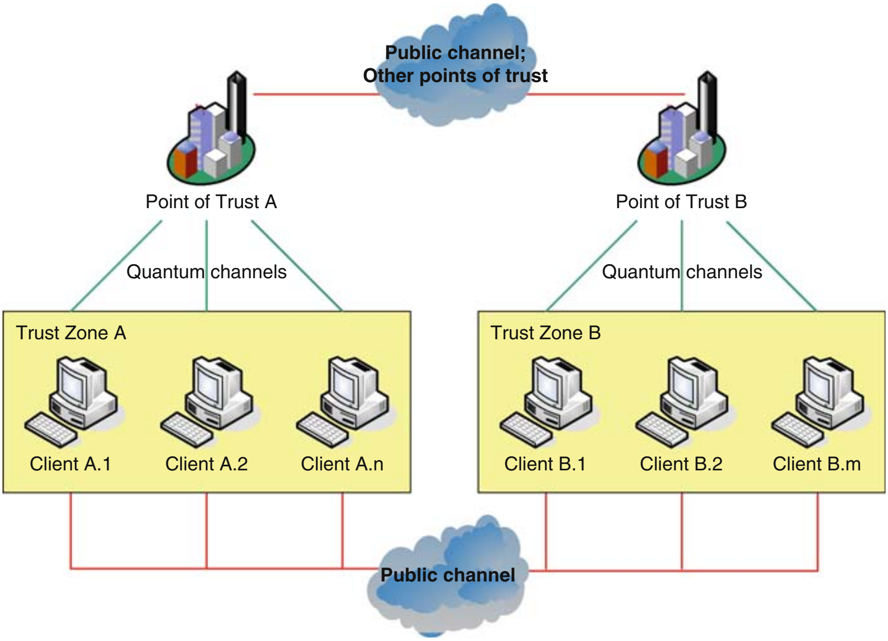


Fig. 10.1 Point of Trust architecture with several Trust Zones

If both communication parties are within one Trust Zone, as shown in Fig. 10.2 (i.e., both are connected to the same Point of Trust) it is easy for them to establish a secure communication via the assigned Point of Trust. But to be able to communicate with both, communication parties inside and outside their own Trust Zone, they can use the Ring of Trust architecture.

10.3 Communication in the Point of Trust Model

The following examples describe the secure communication between two clients. These two clients are either in different Trust Zones, as outlined in 10.3.1.1 and 10.3.2.1, or in the same Trust Zone, as described in 10.3.1.2 and 10.3.2.2. Due to

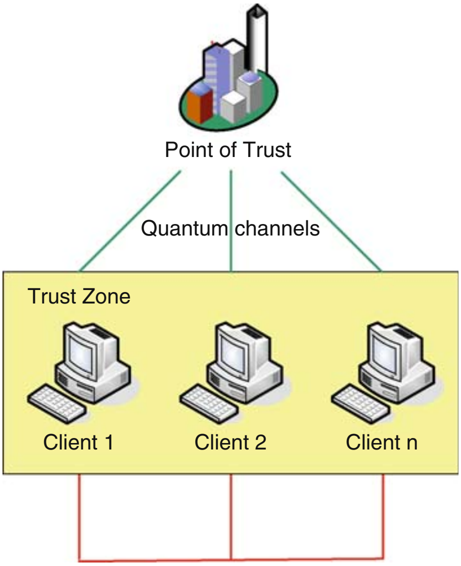


Fig. 10.2 Point of Trust architecture with one Trust Zone

the new architecture presented in this chapter, it is no longer necessary for the two legitimate communication parties to exchange keys over a secure channel. Yet, they can still communicate at a high level of security.

10.3.1 Resource-Oriented Setup of Communication

Contrary to the speed-oriented setup as described in 10.3.2, both steps are triggered by the initiator. Therefore, more steps must be carried out than in the speed-oriented setup.

10.3.1.1 Point of Trust Architecture with Several Trust Zones

In this architecture, communication takes place between clients of different Trust Zones. The participating Points of Trust must be trustworthy, i.e., they must have exchanged a key. Such a network of Points of Trust can be set up in different ways, e.g., in the form of a hierarchical model or a point-to-point model as shown in Figs. 10.3 and 10.4. The form of communication between the respective Points of Trust is not relevant for the function of the Point of Trust model.

Step 1: Initiation of communication

At the beginning of the communication the situation is given by the following conditions. Client A.1 requests client B.2 to communicate and client A.1 and client B.2 are members of different Trust Zones.

The initialization of communication is shown in Fig. 10.5. The communication steps are delineated subsequently.

Fig. 10.3 Hierarchical model

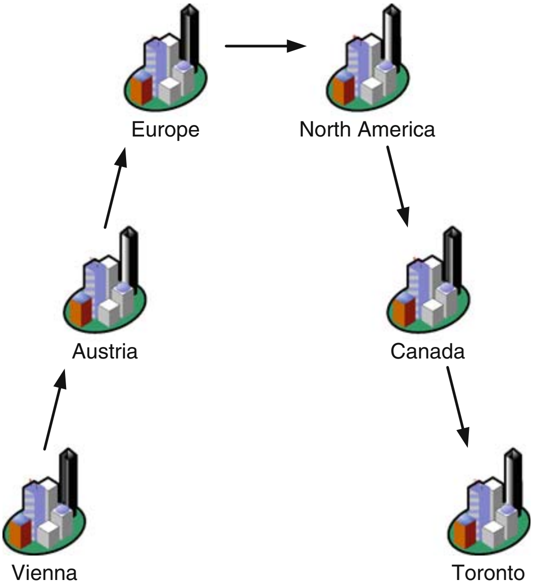
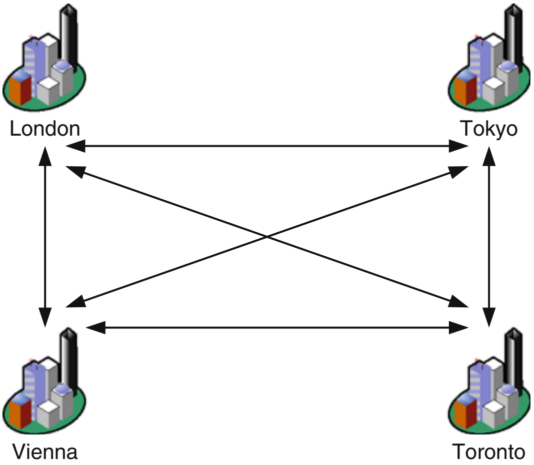


Fig. 10.4 Point-to-Point model



To initialize the communication client A.1 sends a request and transmits its data (authenticity, authorization, accounting information, etc.) to Point of Trust A (*1*) in order to be identified as part of Trust Zone A. Point of Trust A checks the data of client A.1. After positive validation, the request for communication party client B.2 is transmitted to Point of Trust B (*A1*) that is responsible for the target, client B.2. (Points of Trust A and B might be connected directly or via other Points of Trust).

Point of Trust B receives the request for communication between the communication parties client A.1 and client B.2 and requests the identification of client B.2 to communicate (*A2*). Client B.2 receives the request and sends his data (authenticity,

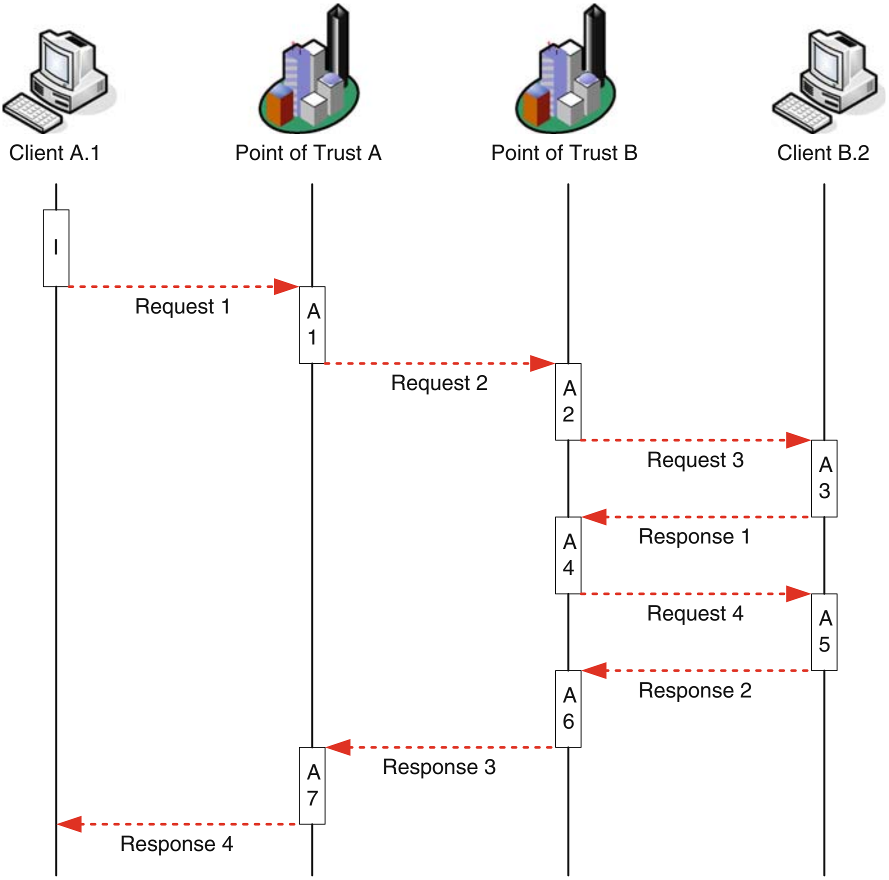


Fig. 10.5 Initiation of communication

authorization, accounting information, etc.) to Point of Trust B as response (*A3*) in order to be identified as part of Trust Zone B. Point of Trust B receives the response and checks the data of client B.2. After positive validation, the information relevant to the communication is sent to client B.2 (*A4*), introducing the requesting communication party, client A.1.

Client B.2 confirms the request for communication from client A.1 and sends his response to Point of Trust B (*A5*). Point of Trust B receives the confirming response and forwards it to Point of Trust A (*A6*). Point of Trust A receives the confirming response and forwards it to the requesting communication party, client A.1(*A7*).

Step 2: Setup of secure communication

The setup of secure communication is shown in Fig. 10.6. The communication steps are delineated subsequently.

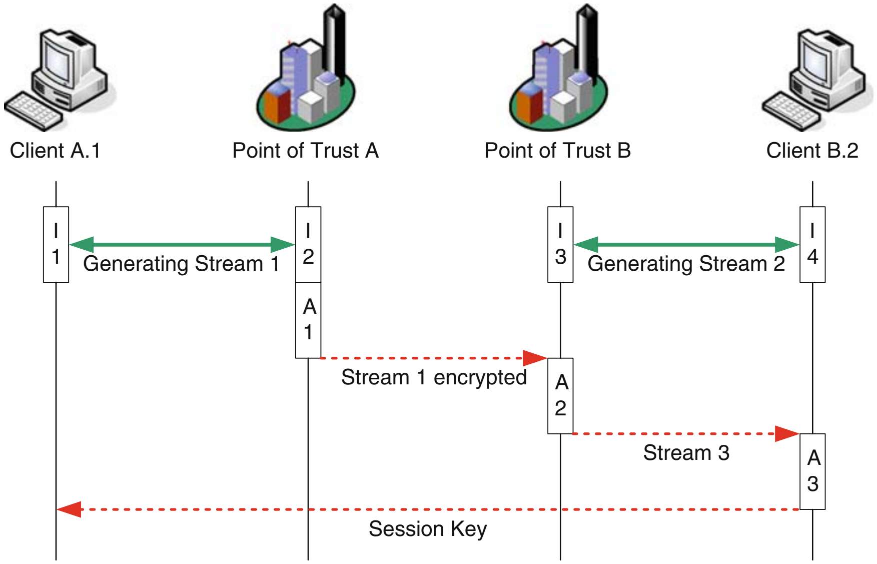


Fig. 10.6 Setup of secure communication

Client A.1 and Point of Trust A are ready to communicate and generate Stream 1, a shared stream generated by using quantum mechanical techniques, over a quantum channel (*I1* and *I2*). Analog, client B.2 and Point of Trust B are ready to communicate and generate Stream 2 (*I3* and *I4*).

Both communication parties have generated streams they share with their respective Points of Trust. Point of Trust A encrypts Stream 1 using a key shared with Point of Trust B generating Stream 1 encrypted and transmits it to Point of Trust B (*A1*). Point of Trust B receives Stream 1 encrypted and uses the key shared with Point of Trust A to decrypt it. The reproduced Stream 1 is then encrypted by Stream 2 generating Stream 3 which is transmitted to client B.2 (*A2*).

Client B.2 receives Stream 3 and uses Stream 2, which is known to him, to reproduce Stream 1. Stream 1 is subsequently established as the session key for the communication parties, client A.1 and client B.2 (*A3*).

10.3.1.2 Point of Trust Architecture with One Trust Zone

Step 1: Initiation of communication

At the beginning of the communication the situation is given by the following conditions. Client A.1 requests client A.2 to communicate and client A.1 and client A.2 are members of the same Trust Zone.

The communication steps for the initialization of communication are delineated subsequently.

To initialize the communication client A.1 sends a request and transmits his data (authenticity, authorization, accounting information, etc.) to Point of Trust A in order to be identified as part of Trust Zone A. Point of Trust A checks the data of client A.1. After positive validation, Point of Trust A requests the identification of client A.2 to communicate.

Client A.2 receives the request and sends his data (authenticity, authorization, accounting information, etc.) to Point of Trust A as response in order to be identified as part of Trust Zone A. Point of Trust A receives the response and checks the data of client A.2. After positive validation, the information relevant to the communication is sent to client A.2, introducing the requesting communication party, client A.1.

Client A.2 confirms the request for communication from client A.1 and sends his response to Point of Trust A. Point of Trust A receives the confirming response and forwards it to the requesting communication party, client A.1.

Step 2: Setup of secure communication

The communication steps to setup secure communication are delineated subsequently.

Client A.1 and Point of Trust A are ready to communicate and generate Stream 1, a shared stream generated by using quantum mechanical techniques, over a quantum channel. Analog, Stream 2 is generated between Point of Trust A and client A.2 which is ready to communicate too.

Both communication parties have generated streams they share with Point of Trust A. Point of Trust A encrypts Stream 1 using Stream 2 to generate Stream 3. Stream 3 is then transmitted to client A.2.

Client A.2 receives Stream 3 and uses Stream 2, which is known to him, to reproduce Stream 1. Stream 1 is subsequently established as the session key for the communication parties, client A.1 and client A.2.

10.3.2 Speed-Oriented Setup of Communication

Contrary to the resource-oriented setup as described in 10.3.1, the response of the target, when requested to communicate, is not directly transmitted to the initiator. Instead the target responds by taking the initiative in setting up secure communication. In this way fewer steps are necessary, which speeds up the setup of communication.

10.3.2.1 Point of Trust Architecture with Several Trust Zones

In this system, communication takes place between clients from different Trust Zones. The respective Points of Trust must be trustworthy, i.e., they must have exchanged a key. For information on different network models see 10.3.1.1.

Step 1: Initiation of communication

At the beginning of the communication the situation is given by the following conditions. Client A.1 requests client B.2 to communicate and client A.1 and client B.2 are members of different Trust Zones.

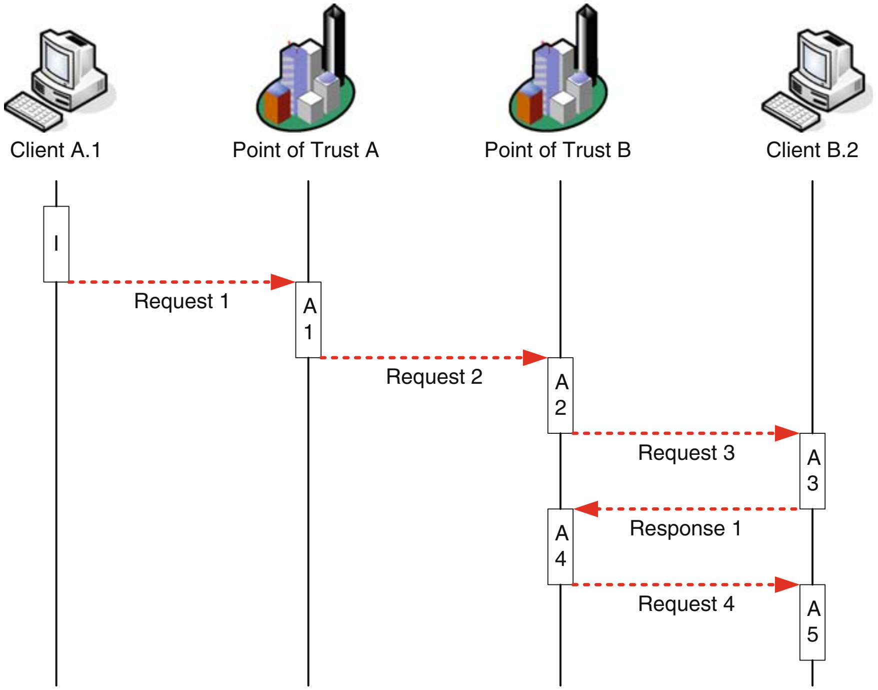


Fig. 10.7 Initiation of communication

The initialization of communication is shown in Fig. 10.7. The communication steps are delineated subsequently.

To initialize the communication client A.1 sends a request and transmits his data (authenticity, authorization, accounting information, etc.) to Point of Trust A (*I*) in order to be identified as part of Trust Zone A. Point of Trust A checks the data of client A.1. After positive validation, the request for communication party client B.2 is transmitted to Point of Trust B (*A1*) which is responsible for the target, client B.2.

Point of Trust B receives the request for communication between the communication parties client A.1 and client B.2 and requests the identification of client B.2 to communicate (*A2*). Client B.2 receives the request and sends his data (authenticity, authorization, accounting information, etc.) to Point of Trust B as response (*A3*) in order to be identified as part of Trust Zone B. Point of Trust B receives the response and checks the data of client B.2. After positive validation, the information relevant to the communication is sent to client B.2 (*A4*), introducing the requesting communication party, client A.1.

Client B.2 confirms the request for communication from client A.1 and takes initiative (*A5*).

Step 2: Setup of secure communication

The setup of secure communication is shown in Fig. 10.8. The communication steps are delineated subsequently.

Client A.1 and Point of Trust A are ready to communicate and generate Stream 1, a shared stream generated by using quantum mechanical techniques, over a quantum channel (*I1* and *I2*). Analog, client B.2, and Point of Trust B are ready to communicate and generate Stream 2 (*I3* and *I4*).

Both communication parties have generated streams they share with their respective Points of Trust. Point of Trust B encrypts Stream 2 using a key shared with Point of Trust A generating Stream 2 encrypted and transmits it to Point of Trust A (*A1*). Point of Trust A receives Stream 2 encrypted and uses the key shared with Point of Trust B to decrypt it. The reproduced Stream 2 is then encrypted by Stream 1 generating Stream 3 which is transmitted to client A.1 (*A2*).

Client A.1 receives Stream 3 and uses Stream 1, which is known to him, to reproduce Stream 2. Stream 2 is subsequently established as the session key for the communication parties, client A.1 and client B.2 (*A3*).

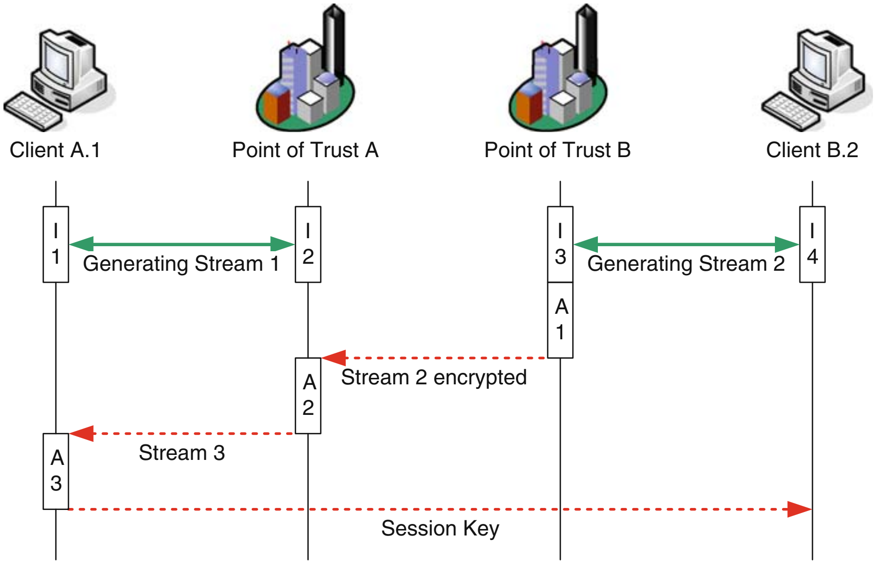


Fig. 10.8 Setup of secure communication

10.3.2.2 Point of Trust Architecture with One Trust Zone

Step 1: Initiation of communication

At the beginning of the communication the situation is given by the following conditions. Client A.1 requests client A.2 to communicate and client A.1 and client A.2 are members of the same Trust Zone.

The communication steps for the initialization of communication are delineated subsequently.

To initialize the communication client A.1 sends a request and transmits his data (authenticity, authorization, accounting information, etc.) to Point of Trust A in order to be identified as part of Trust Zone A. Point of Trust A checks the data of client A.1. After positive validation, Point of Trust A requests the identification of client A.2 to communicate.

Client A.2 receives the request and sends his data (authenticity, authorization, accounting information, etc.) to Point of Trust A as response in order to be identified as part of Trust Zone A. Point of Trust A receives the response and checks the data of client A.2. After positive validation, the information relevant to the communication is sent to client A.2, introducing the requesting communication party, client A.1.

Client A.2 confirms the request for communication from client A.1 and takes initiative.

Step 2: Setup of secure communication

The communication steps to setup secure communication are delineated subsequently.

Client A.1 and Point of Trust A are ready to communicate and generate Stream 1, a shared stream generated by using quantum mechanical techniques, over a quantum channel. Analog, Stream 2 is generated between Point of Trust A and client A.2 which is ready to communicate too.

Both communication parties have generated streams they share with Points of Trust A. Point of Trust A encrypts Stream 2 using Stream 1 to generate Stream 3. Stream 3 is then transmitted to client A.1.

Client A.1 receives Stream 3 and uses Stream 1, which is known to him, to reproduce Stream 2. Stream 2 is subsequently established as the session key for the communication parties, client A.1 and client A.2.

10.4 Exemplified Communications

The following section presents examples of communication models. It shows the difference between the setups for communications between several Trust Zones and within one Trust Zone and the setup for the generation of the bit stream itself.

10.4.1 Communication Between Several Trust Zones

In this system two Points of Trust are involved which are either connected directly or over an arbitrary network structure.

10.4.1.1 Initiation of Communication

At the beginning of the communication, it must be determined whether it is in the interest of the network operator and the two communication parties to set up communication. The request for communication is set up by preparing the required data in a packet.
The content of such a packet could be exemplified by the following:

- *Initiator*: The identification of the initiator, in this example the identification of client A.1, by a unique network address, which can be compared with other network protocols like IP.
- *Target*: Identification of the party who is requested to communicate, in this case the identification of client B.2.
- *Time* when communication is initiated: Determines the desired time of communication. Additionally, a token for an immediate setup of communication could be defined.
- *Conditions for the setup of communication*: Permits the definition of tokens regarding different communication factors. Examples of such tokens are payment (by initiator, target, other accounts, e.g., of a company), responsibility for the transmitted data, priority of communication, level of secrecy.

This request is transmitted over a public channel to the responsible Point of Trust, in this example Point of Trust A. In the first step the data of the initiator is examined. Such a check could include information as to, e.g., the authenticity, the authorization of the initiator to communicate (with the target, the level of secrecy, the point in time, etc.), and accounting information. If the validation fails, the communication is terminated and a response is generated accordingly.

If the identification is valid, then the information relating to the target is checked. The information check could include factors like availability of the target, level of secrecy of the communication. If the check yields a negative result, the communication is terminated and an appropriate message is transmitted to the initiator.

If the check yields a positive result, the request is forwarded to the Point of Trust, which is responsible for the target. This Point of Trust can be contacted in different ways. Examples are a hierarchical organization of the different Points of Trust or a direct connection of all Points of Trust.

The target's Point of Trust receives and processes the request. At this point, the data of the target is checked. Now the accounting information of the target could be checked, as this information may only be known to the respective client. Information regarding the level of secrecy or the ring of authorized communication parties could only be known to the responsible Point of Trust and might also be checked at this stage. If the check yields a negative result, the communication is terminated and an appropriate message is sent.

Additionally, the responsible Point of Trust could request the authentication of the target. At the same time, the target would be informed about the request for communication. Now all the information of the request can be transmitted. Alternatively, the data related to the request is forwarded after the positive identification, as depicted in Fig. 10.9. In this example the data required for communication is transmitted only after a valid identification of the target. This guarantees a higher level of security.

If the identification of the target fails, then the setup of communication is terminated and a response is sent accordingly. Otherwise the request is forwarded to the target. The target then decides whether to accept or reject the setup of communication. The response of the target is then routed to the initiator and to all Points of Trust involved. Depending on the form of communication the participants had previously agreed on (level of secrecy, accounting information, etc.) and the determined time, the required initializations can now be prepared.

In the case of a negative response, e.g., caused by the termination of communication, the initiator can start a new setup of communication. The Point of Trust may employ mechanisms to make use of operation parameters like, e.g., maximal number of attempts to set up communication over a certain period of time, costs per communication attempt.

Note: A higher level of security could be obtained by encrypting all the communication between the respective parties. Symmetric ciphers like block ciphers, stream ciphers, or asymmetric systems based on a central PKI would be suitable for that purpose.

10.4.1.2 Setup of Secure Communication

Once the communication is initiated the next step is to generate the required streams and to set up a secure communication as seen in Figs. 10.9 and 10.10. The initiator of the communication generates a stream with specified quality criteria and a respective key length with its Point of Trust. A key length of 256 bits is agreed upon to work subsequently with an encryption of, e.g., AES (see [2]).

As a next step the generated status is checked. A negative status leads to the termination of the communication. If the generation status is positive, the generated stream is encrypted by the initiator's Point of Trust. Symmetric ciphers like AES or asymmetric systems like PKIs can be used to encrypt the stream.

After receiving the encrypted Stream 1, the target's Point of Trust initiates the generation of a stream (Stream 2) with the target. Again different quality criteria can be agreed on. Depending on the encryption algorithm, that is subsequently used, the Stream 1 and Stream 2 have to be of equal length. Then the status is checked. In case of a negative status the communication is terminated.

If the status proves positive, then the encrypted Stream 1 is decrypted. As a next step Stream 1 is encrypted by Stream 2 to produce Stream 3. A One-Time-Pad cipher

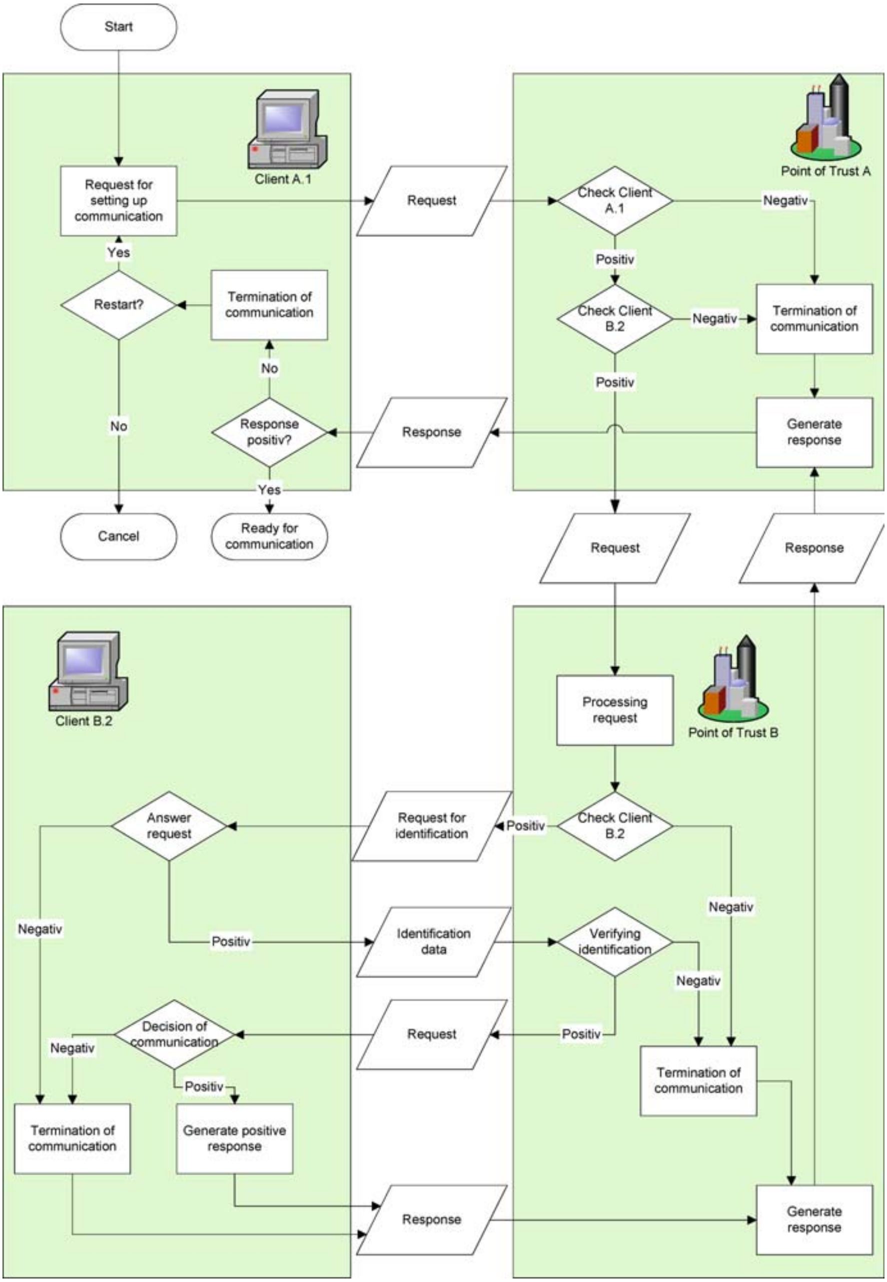


Fig. 10.9 Request for communication setup

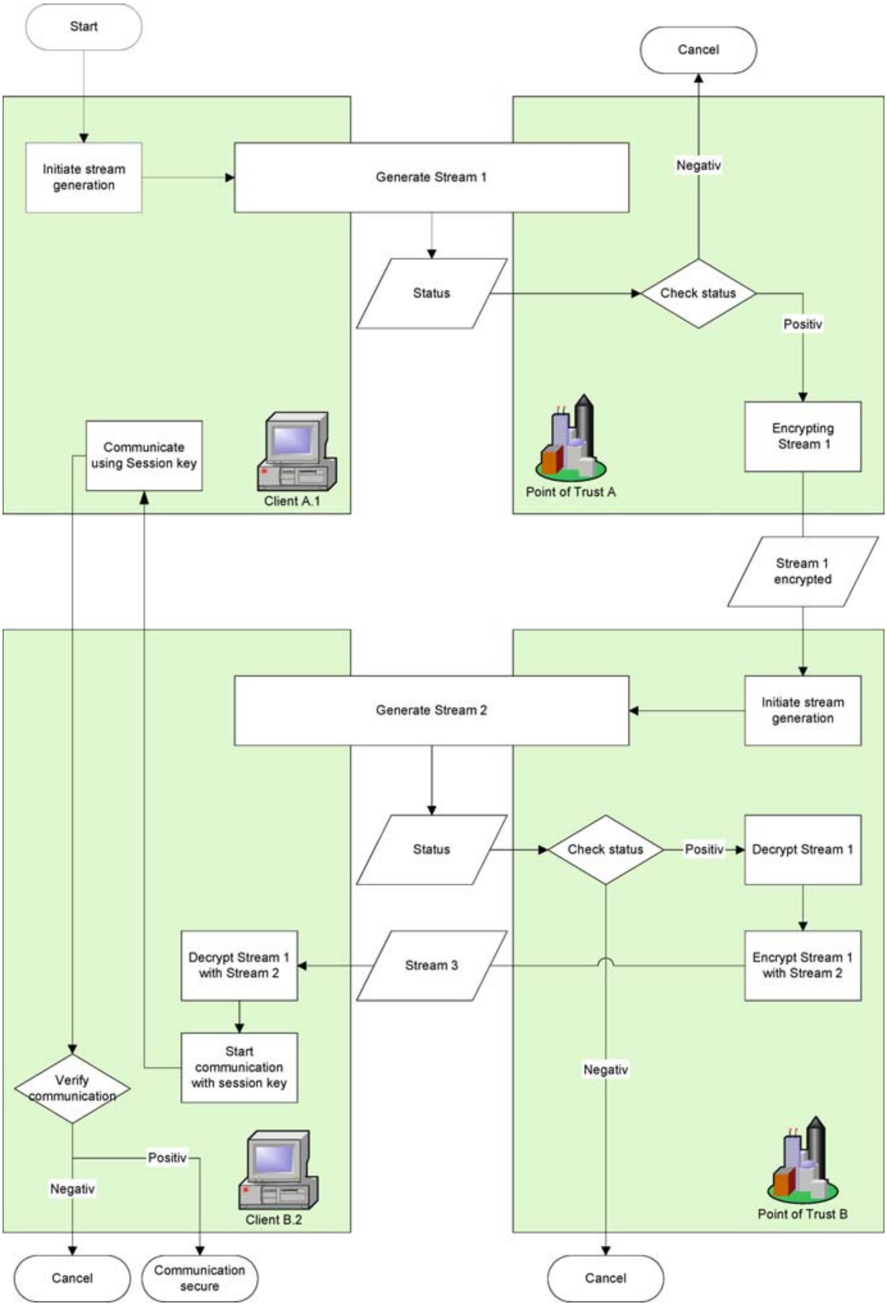


Fig. 10.10 Setup of secure communication

using the two streams is an example of a possible encryption. In this case, it is necessary that the streams are of equal length and fulfil predefined quality criteria.

Stream 3, which has been generated in this manner, is then transmitted to the target. The target decrypts Stream 3 using Stream 2. The result of the decryption (Stream 1) is subsequently referred to as the Session key.

The target now sets up communication with the initiator. Algorithms like AES or IDEA could be employed. Next, the setup of communication is checked. If the communication check yields a negative result, then the communication is terminated. If the result is positive, the communication is secure in the framework of the method.

Note: After the communication has been terminated, an appropriate message is sent to all of the participating communication parties. It is up to the system operator to define further steps in the event of the termination of a communication and to, e.g., repeat failed attempts. Whether a repeated attempt is permissible could depend on the requirements defined in the first step of the communication setup or on the prearranged time.

10.4.2 Communication in One Trust Zone

10.4.2.1 Initiation of Communication

At the beginning of the communication, it must be determined whether it is in the interest of the network operator and the two communication parties to set up communication. The request for communication is set up by preparing the required data in a packet.

The content of such a packet could be exemplified by the following:

- *Initiator:* The identification of the initiator, in this example the identification of client A.1, by a unique network address, which can be compared with other network protocols like IP.
- *Target:* Identification of the party who is requested to communicate, in this case the identification of client A.2.
- *Time when communication is initiated:* Determines the desired time of communication. Additionally a token for an immediate setup of communication could be defined.
- *Conditions for the setup of communication:* Permits the definition of tokens regarding different communication factors. Examples of such tokens are payment (by initiator, target, other accounts, e.g., of a company), responsibility for the transmitted data, priority of communication, level of secrecy.

This request is transmitted over a public channel to the responsible Point of Trust, in this example Point of Trust A. In the first step the data of the initiator is examined. Such a check could include information as to, e.g., the authentication of the initiator, authorization of the initiator to communicate (with target, the level of secrecy, the point in time, etc.), and accounting information. If the validation fails, the communication is terminated and an appropriate response is generated.

If the check yields a positive result, the information related to the target is examined. The check could include factors like, e.g., availability of the target, authorization to communicate with the initiator, accounting information of the target, level of secrecy. If the check yields a negative result, the communication is terminated and an appropriate message is forwarded to the initiator.

Additionally, the Point of Trust could request the identification of the target. At the same time, the target would be informed about the request for communication. Now all the information of the request can be transmitted. Alternatively, the data related to the request is forwarded after the positive identification, as depicted in Fig. 10.11. In this example the data required for communication is transmitted only after a valid identification of the target. This guarantees a higher level of security. If the identification fails, then the setup of communication is terminated and a response is sent accordingly.

Otherwise the request is forwarded to the target. The target then decides whether to accept or reject the setup of communication. The response of the target is then routed to the initiator and to the Point of Trust. Depending on the form of communication the participants had previously agreed on (level of secrecy, accounting information, etc.) and the determined time, the required initializations can now be prepared.

In the case of a negative response, e.g., caused by the termination of communication, the initiator can start a new setup of communication. The Point of Trust may employ mechanisms to make use of operation parameters like, e.g., maximal number of attempts to set up communication over a certain period of time, costs per communication attempt.

Note: A higher level of security could be obtained by encrypting all the communication between the respective parties. Symmetric ciphers like block ciphers (AES, IDEA, etc.), stream ciphers (one-time-pad, SEAL 2.0, etc.), or asymmetric systems based on a central PKI would be suitable for that purpose.

10.4.2.2 Setup of Secure Communication

Once the communication is initiated the next step is to generate the required streams and to set up a secure communication as shown in Figs. 10.11 and 10.12. The initiator of the communication generates a stream with specified quality criteria and a respective key length with his Point of Trust. For example, a key length of 256 bits is needed to work subsequently with AES (see [2]).

As a next step the status of the generation is checked. A negative status leads to the termination of the communication. If the status of the generation is positive, then the Point of Trust initiates the generation of a stream (Stream 2) with the target. Again, certain quality criteria (like [1]) can be agreed on. Depending on the encryption algorithm that is subsequently used, Stream 1 and Stream 2 have to be of equal length. Then the status is checked. In case of a negative status the communication is terminated. If the status proves positive, Stream 1 is encrypted by Stream 2 to

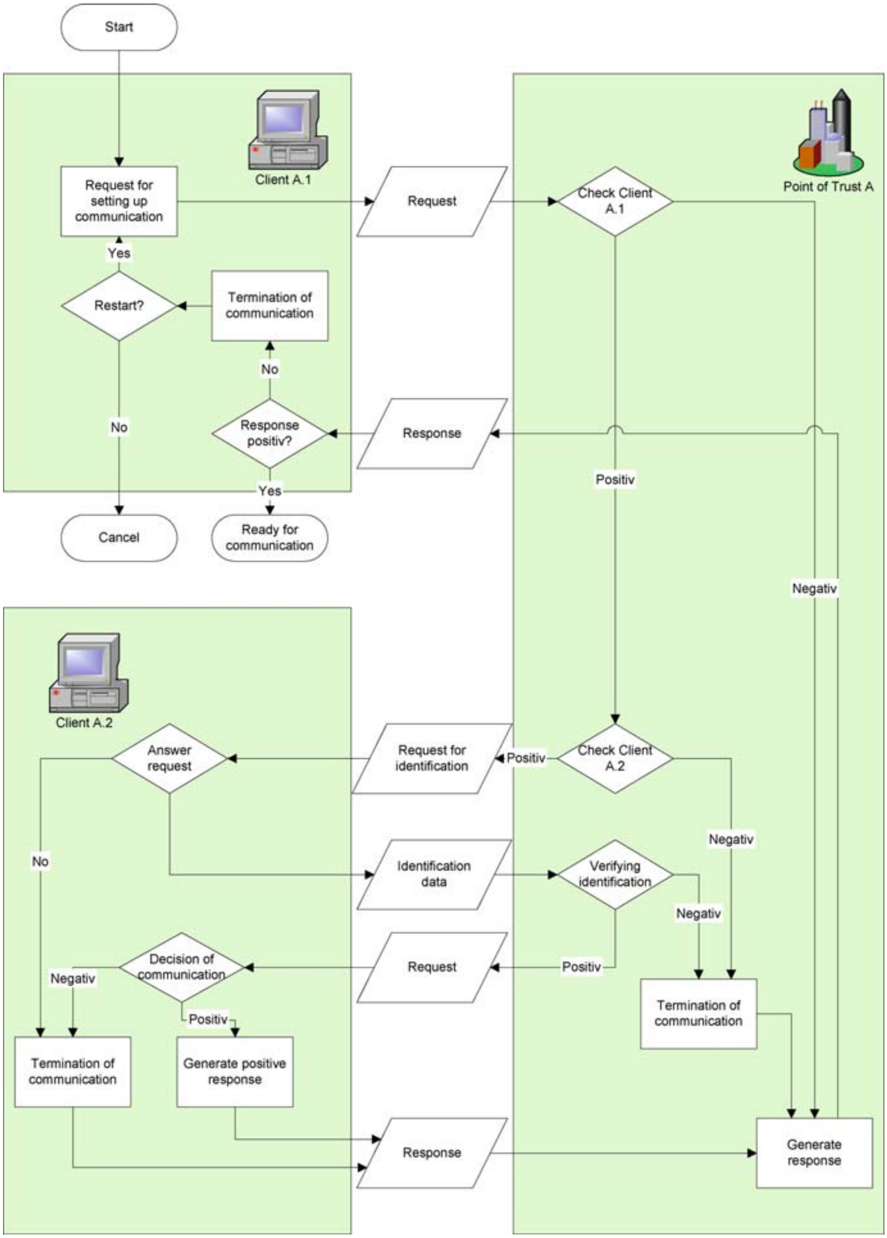


Fig. 10.11 Request for communication setup

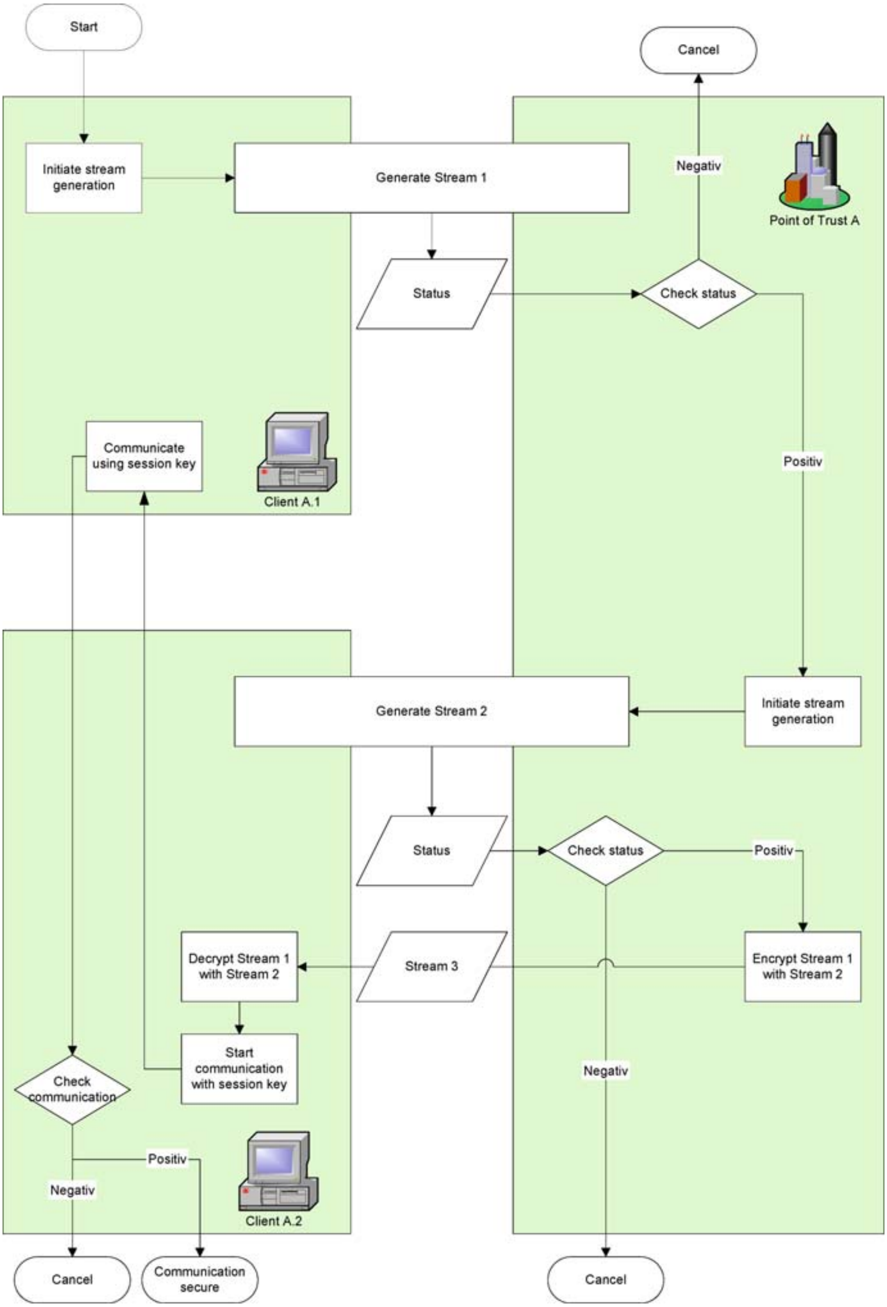


Fig. 10.12 Setup of secure communication

produce Stream 3. A One-Time-Pad cipher using the two streams is an example of a possible encryption. In this case, it is necessary that the streams are of equal length and fulfil predefined quality criteria.

Stream 3, which has been generated in this manner, is then transmitted to the target. The target decrypts Stream 3 by using Stream 2. The result of the decryption (Stream 1) is subsequently referred to as the Session key.

The target now sets up communication with the initiator. Algorithms like AES or IDEA could be employed. Next, the setup of communication is checked. If the communication check yields a negative result, then the communication is terminated. If the result is positive, the communication is secure in the framework of the method.

Note: After the communication has been terminated, an appropriate message is sent to all of the participating communication parties. It is up to the system operator to define further steps in the event of the termination of a communication and to, e.g., repeat failed attempts. Whether a repeated attempt is permissible could depend on the requirements defined in the first step of the communication setup or on the prearranged time.

10.4.3 Generation of a Stream

At the beginning of the generation process, the initiator prepares a detailed request as seen in Fig. 10.13. This request could include different tokens like the length of the stream that is to be generated, the quality criteria of the stream, e.g., FIPS 140-2 [1], criteria according to Golomb [9], linear complexity [9].

The request is forwarded to both communication parties and serves to initiate respective steps such as the preparation of the system (adjustments, self test, etc.), logging.

The participating communication parties generate a stream using a respective protocol, e.g., BB84 [3].

Once a stream with the specified length is generated, it is checked by one of the communication parties involved. In this check, the quality criteria specified in the request can be checked. If the test leads to the rejection of the generated stream, an appropriate error message is generated and sent to the second communication party.

If the stream is approved, a positive status message is generated. This message confirms that both communication parties now share a key, which has been generated by both parties.

It could be up to the initiator to make another attempt at generating a key if one try results in an error message. In this case, the system operator could interfere by, e.g., limiting the number of attempts over a certain period of time, charging each attempt separately.

If the attempt is not repeated, a negative status message is generated. It confirms that no shared key could be generated.

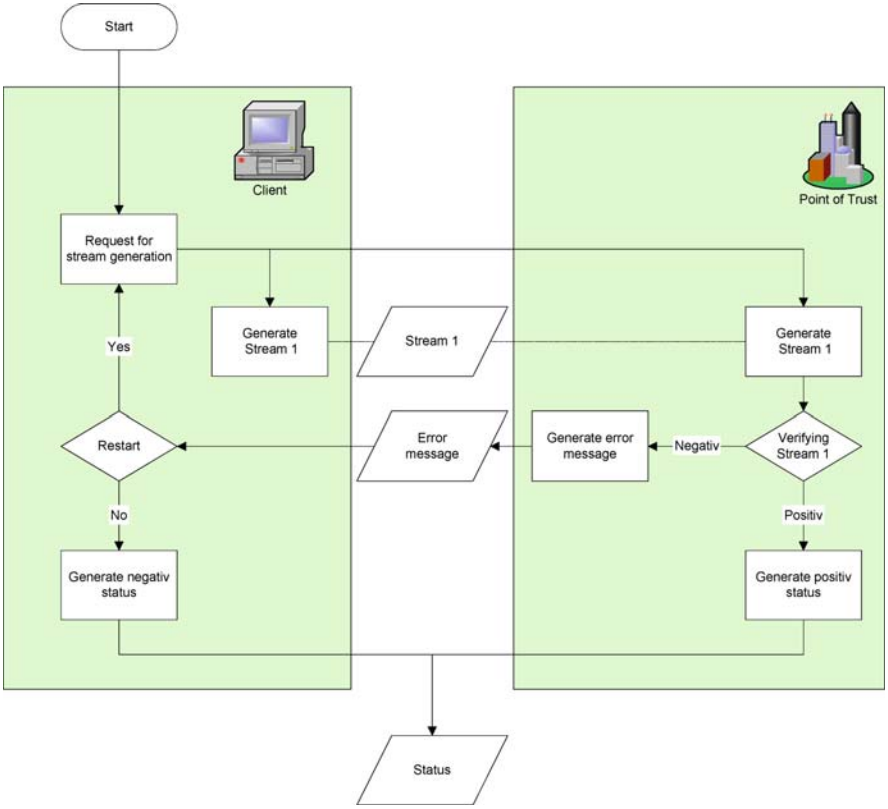


Fig. 10.13 Generation of a stream

10.5 A Medical Information System Based on the Ring of Trust

10.5.1 Field of Research

10.5.1.1 Availability on Demand

Besides the distribution of high-quality keys in an adequate amount also the storage of these keys is very important. In large data-processing centers it is possible to securely store such sensitive data since the required environment (access control, backup structure, hardware architecture) is present. But most of the commercial and private users do not have this kind of environment at their disposal. Thus we can state the requirement: keys should be generated on demand and not on supply to overcome the problems of their secure storage.

10.5.1.2 Scalability

Today we have different requirements about the security level of transmitted data. The data which gets transmitted during an online surgery over the Internet needs a much higher security level than most other data. Therefore it is necessary to draw a distinction between certain security levels for data to optimize speed and reduce the amount of needed resources.

Within a medical information system there exists data which could be encrypted with a classical algorithm for an adequate security level. There also exists data that is subject to legal requirements and hence needs to be encrypted with a certain algorithm. Further kinds of data need to be encrypted with predefined security algorithms to allow the use within existing environments or already used protocols like VPN. But beside this, most companies today have to maintain huge databases and transmit huge amounts of highly critical data, which needs high-level security.

10.5.1.3 The Problems of Distance and Speed

In our opinion it is another basic aspect that keys of adequate quality need to be available over long distances and with the according quality. QKD provides high-quality keys but today it is not possible to generate keys over very long distances. Within QKD systems increasing distance between Alice and Bob leads to decreasing transmission speed. So the deployment of classical QKD-based networks is limited.

10.5.2 Requirements

Medical Information Systems (MIS) [6, 8, 11] consisting of data-processing units like Radiology Information System (RIS), Lab Information System (LIS) [8], Digital Imaging and Communications in Medicine (DICOM), Health Level 7 (HL7) [10, 5], Picture Archiving and Communicating System (PACS) [6], ORBIS (MIS powered by GWI AG), International Statistical Classification of Diseases and Related Health Problems (ICD-10) [8] database or any other kind of digital information system are essential components of modern medical data processing units.

It is commonly known that patient-related data is highly sensitive. This kind of data needs to be stored for a longtime and its privacy has to be guaranteed for the whole time of storage. Only to a selected group of people like doctors or the nursing staff the access to the patient-related data should be granted. To prevent an intervention of an adversary it is essential to encrypt patient-related data during the transmission. Here it does not matter whether this information contains recipes, radiology reports, or any other kind of medical data.

Telemedicine is part of telematics-related surgeries [7] where a surgeon operates on a patient over a long distance – maybe even in another country. The surgeon's physiological transaction data is transmitted, for example, from Vienna to the operating theatre in Klagenfurt over a public channel. This highly sensitive data (e.g., heart surgeries over the Internet via triggering ”da Vinci” surgery robot) needs to be protected against any adversary. Other important aspects besides high level of security are transmission speed and independence of the amount of transmitted data.

Manipulation of data is a severe threat and especially in medicine it could result in devastating consequences. Thus it is necessary to implement modern cryptographic methods into existing infrastructures. Additionally, techniques are needed which are easy to implement and also provide a high level of security and fulfil the requirements for transmission speed and long-range communication.

10.5.2.1 Results of the Survey

The survey [4] shows that the participants (medical technicians, commercial service providers, exc.) are very well informed about the state-of-the-art Medical Information Systems (cf. Fig. 10.14).

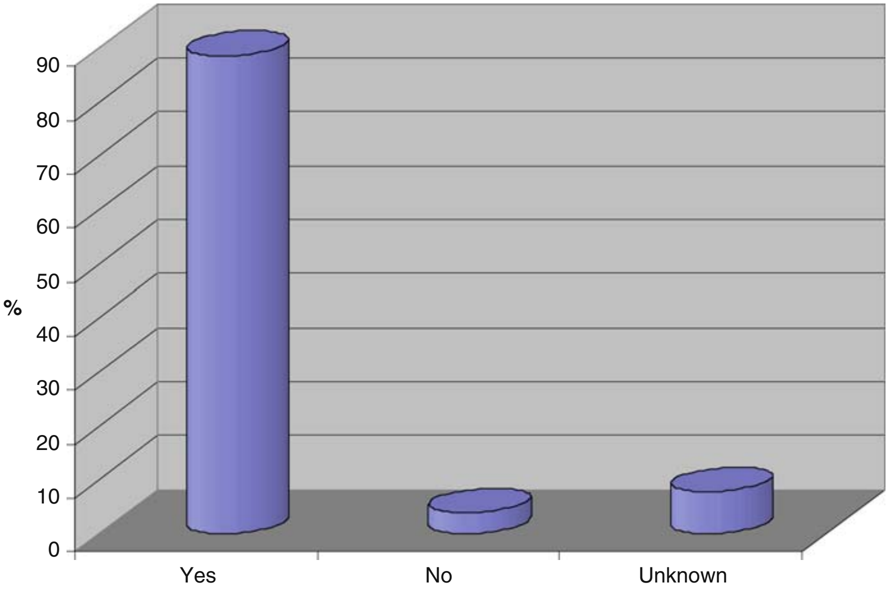


Fig. 10.14 Awareness about state-of-the-art Medical Information Systems

Regarding the privacy of transmitted data about 40% agreed that more than 75% of the communication has to be encrypted. Almost two-thirds say that more than 50% of the transmitted and stored data is sensitive (cf. Fig. 10.15).

As a result of the survey about 90% of the participants agreed that in medical data processing the need for high-quality security solutions is given. About 60% of the participants stress that current architectures could not meet the requirements stated in Sects. 10.5.1.1, 10.5.1.2, 10.5.1.3. They stated that modern solutions are needed to protect the patient's privacy to reach a high level of security (cf. Fig. 10.16).

QKD is a solution to these problems. It provides high-quality keys and fulfils the requirements from Sects. 10.5.1.1 and 10.5.1.2. A drawback of quantum key distribution is the range in which it is operable since it is rather low (about 20 km). But certain models like the Ring of Trust are able to solve also these problems.

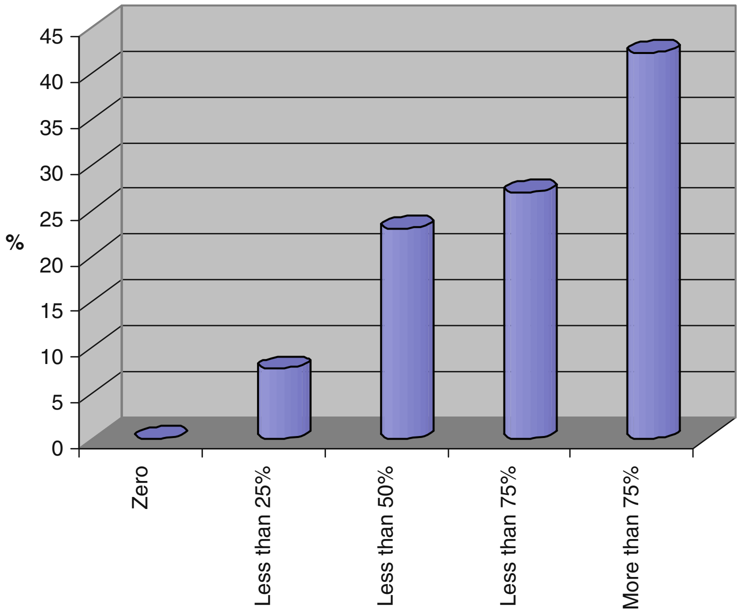


Fig. 10.15 The amount of sensitive data in Medical Information Systems

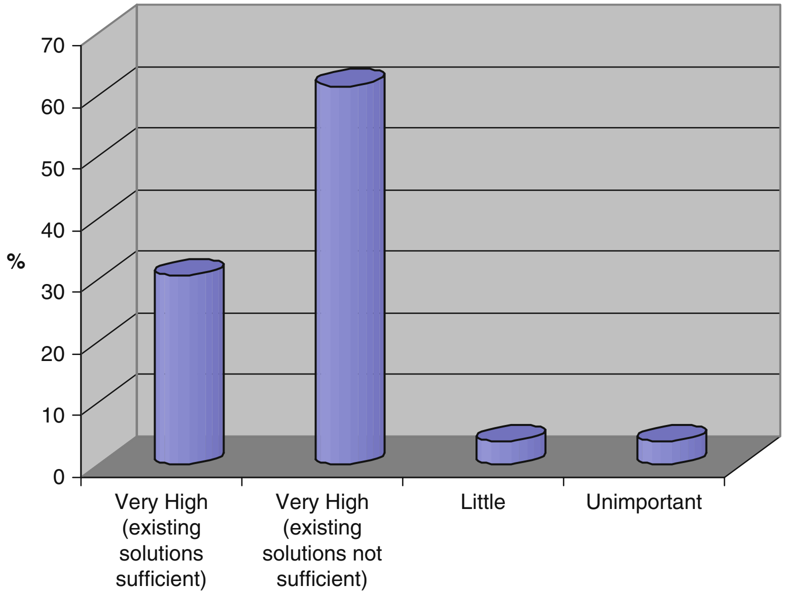


Fig. 10.16 The need for high-level security in Medical Information Systems

10.5.3 Enhanced Ring of Trust model

We can see that there is high demand within medical information systems, not only on generating shared secrets for communication but also to store information in a high secure way. It is absolutely necessary to get access to this highly protected information from any place at any time but only under certain circumstance. To enable this we present an enhanced Ring of Trust model with a special client by introducing a storage client as shown in Figs. 10.17 and 10.18.

10.5.3.1 Storage Client at a Foreign Point of Trust

To access the information on the storage client of a foreign Point of Trust a client A.1 has to take the following steps:

1. Client A.1 generates a key K_A with his Point of Trust. Client A.1 is a member of Trust Zone A and therefore assigned to Point of Trust A.
2. The key K_A is transmitted on a secure channel to the Point of Trust where the storage client is located, the Point of Trust B.
3. Point of Trust B generates key K_B with the storage client, encodes K_A with K_B to K_C (for example, by using the XOR operation) and sends this key either using the secure environment of Point of Trust B if the storage client is located within this secure environment or using a public channel.

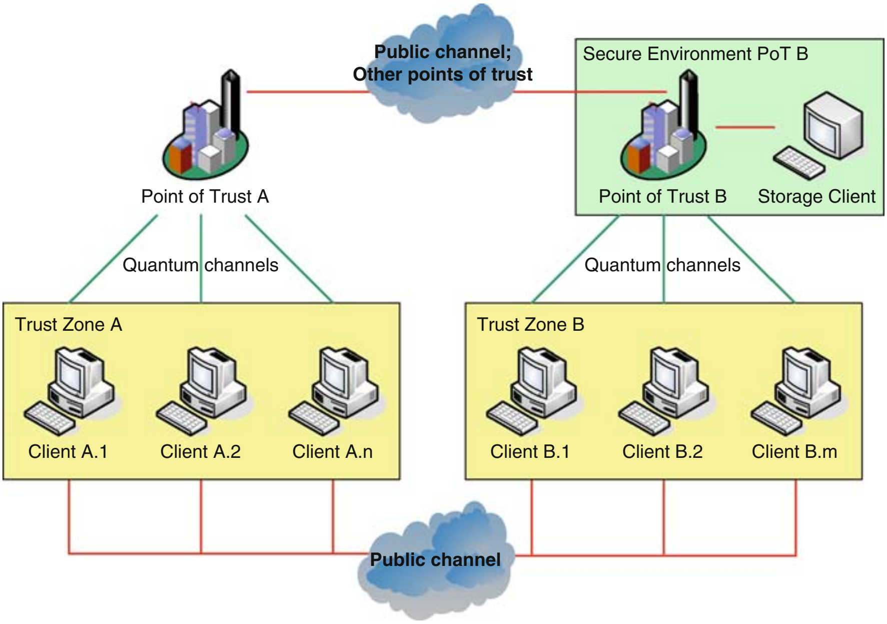


Fig. 10.17 Enhanced ring of trust model with storage client at a foreign point of trust

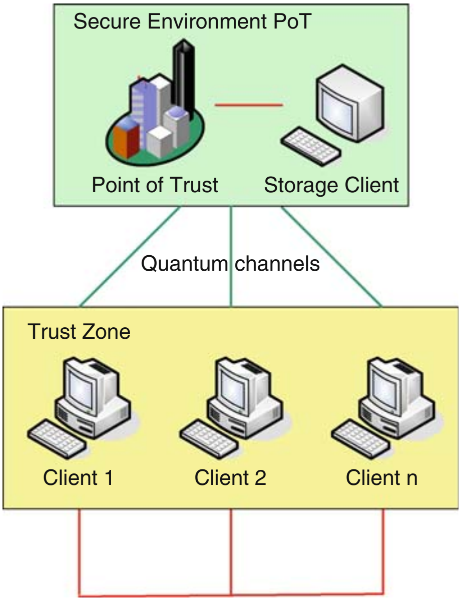


Fig. 10.18 Enhanced ring of trust model with storage client at the home point of trust

4. As the storage client knows K_B he is able to obtain K_A from K_C by calculating $K_A = K_C \oplus K_B$.

With K_A the storage client is now able to establish a secure connection to client A.1. If the storage client is located within the secure environment of the Point of Trust, it would be possible to transmit K_A directly to the storage client without the generation of K_B.

10.5.3.2 Storage Client at the Home Point of Trust

To get access to the information on the storage client at the same trust center, a client has to take the following steps:

1. Client A.1 generates a key K_A with his Point of Trust. Client A.1 is a member of Trust Zone A and therefore assigned to Point of Trust A.
2. If the storage client is located within the secure environment of Point of Trust A, key K_A could be transmitted directly to the storage client.
3. If the storage client is not located within the secure environment but within the Trust Zone of Point of Trust A a key K_B can be generated by the Point of Trust and the storage client.
4. The Point of Trust encodes a new key K_C by calculating $K_C = K_A \oplus K_B$ and sends this key to the storage client by using a public channel.
5. As the storage client knows K_B he is able to calculate K_A from K_C.

Using K_A the storage client is now able to establish a secure connection to client A.1.

References

1. F.I.P.S.P. Security Requirements for Cryptographic Modules. NIST, 140-2 200, 203
2. F.I.P.S.P, 197: Announcing the Advanced Encryption Standard (AES). NIST 196, 200
3. Bennet, C.H., Besset, F., Brassard, G., Salvail, L., Smolin, J.: Experimental Quantum Cryptography. J. Cryptology **5**, 3(1992) 203
4. Dissauer, G.: Security requirements of modern medical information systems. Master's thesis, Vienna University of Technology, Austria (2007) 206
5. Dolin, R.H., Aschuler, L., Boyer, S., Beebe, C., Behlen, F.M., Biron, P.V., Shabo, A.: Medical Informatics Europe. J. Am. Med. Inform Assoc. (2006) 205
6. Haas, P.: Medizinische Informationssysteme und elektronische Krankenakten. Springer Verlag, Berlin, Germany (2004) 205
7. Iakovidis, I.: Towards a Health Telematics Infrastructure in the European Union. European Commission, Brussels, Belgium (2000) 205
8. Lehmann, T.M.: Handbuch der Medizinischen Informatik. Carl Hanser Verlag, Munchen, Germany (2005) 205
9. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press Boca Raton (1996) 203
10. Smith, B., Ceustersc, W.: Medical Informatics Europe. Maastricht, Netherlands (2006) 205
11. van Bemmel, J., Musen, M.A.: Handbook pf Medical Informatics. Springer Verlag, Heidelberg, Germany (1997) 205