Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Note

Wireless Health and Care Security architecture

The blood glucose demonstrator

Note no DART/09/05

Authors Per Røe, Jon Ølnes, Ole Anders Walseth

Date May 2005

Norsk Regnesentral

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Norwegian Centre for Telemedicine

The Norwegian Centre for Telemedicine (NST), www.telemed.no is a national competence centre for telemedicine research and development activity. NST opened officially in 1993 as a department linked to the University Hospital of North Norway, where telemedicine and e-health services have been in daily use since the 1980s. In 2002 the World Health Organization (WHO) designated the Norwegian Centre for Telemedicine as its first Collaborating Centre for Telemedicine.

The NST is a multidisciplinary organization with 100 employees comprising 32 technologists (1 ass. prof., 4 PhD stud., 20 research scientists), 16 social scientists (1 ass. prof., 1 postdoc, 7 PhD stud), 16 health care professionals (3 MDs), 7 educationalists, 4 economists, 2 legal advisers and some administrative staff.

At present the NST conducts research and development projects that contribute to an understanding of ICT-based health-care services, as a means of promoting equitable treatment for all users and fulfilment of their legal rights to health care. The NST cooperates with trade and industry in the development of new products.

The NST also focuses its research on the primary and specialist health service in Norway, helping to develop efficient telemedicine services and to apply telemedicine in clinical services. The centre gathers, produces and disseminates information about telemedicine nationally and internationally.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
Office address
Gaustadalléen 23
NO-0371 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Title	**Wireless Health and Care** **Security architecture** **The blood glucose demonstrator**
Authors	**Per Røe, Jon Ølnes, Ole Anders Walseth**
Date	May
Year	2005

Abstract

WP 13 of the Wireless Health and Care (WsHC) project covers surveillance of the patient in his/her own home.

As part of this work package NST has implemented a demonstrator where the blood glucose level for a patient is measured. The measured data is first transferred wirelessly by the sensor to the patient's mobile phone using Bluetooth, before they are sent to a server in an SMS message. The data are then finally stored in the patients electronic health record (EHR), where a diabetes nurse can access the data.

This document describes given an analysis of the computer security aspects this demonstrator. A risk analysis is performed; both for small scale testing and for usage on a larger scale, and requirements for the system are established. Based on this we list some recommendations that should be implemented before the system can be used on a larger scale.

Keywords	Security architecture, wireless sensors, Bluetooth
Target group	Participants in the WsHC project.
Availability	Public
Project number	320302
Research field	Computer security
Number of pages	28

Contents

List of figures

List of tables

1 Introduction

This document discusses the security in the demonstrator of work package 13 (WP 13) of the Wireless Health and Care (WsHC) project. The document is built upon the general security requirement [1] and security architecture documents [2] for the project. WP 13 studies the use of wireless sensors in the patients own home, and the reporting of the measured data to a central entity, usually a hospital.

2 Short description of demonstrator

A patient with diabetes has to measure the blood glucose level regularly to manage the level, and to avoid acute medical complications and long-term complications. A person with diabetes has meetings with his/her diabetes nurse where the nurse evaluates the patient's ability to control his/her diabetes. The current method for doing this is for the patient either to write down the measures on paper, use a computer program to print the result or (most usual) give their doctor an approximate estimate at each meeting based on their own memory. These are methods that place heavy demands and responsibility on the diabetes patient.

NST has developed a prototype where the blood glucose level is measured using a sensor. The data is then sent to central server using the patient's mobile phone, before it is stored in the EHR record for the patient, so that the diabetes nurse can access the data.

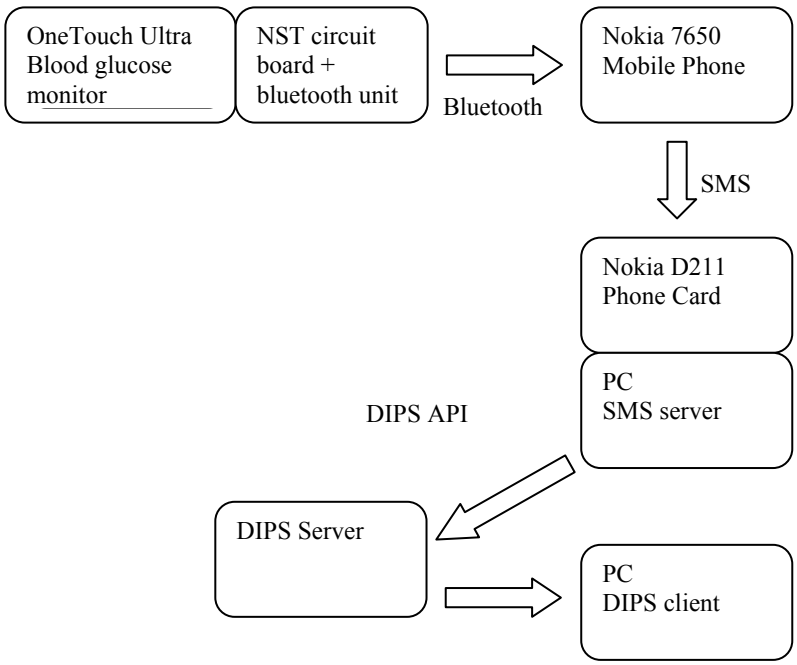

Figure 1: Physical architecture of the demonstrator

2.1 Demonstrator functionality

The diabetes patient measures his/her blood glucose level with the OneTouch Ultra blood glucose monitor. This is the only part of the process that is visible to the user. When the blood glucose monitor is switched off, the NST Bluetooth unit will be switched on and stay active for 3 minutes. If the Nokia 7650 mobile phone is within range a connection will automatically be established, and the last blood glucose measure will be transferred using Bluetooth. If the Nokia 7650 is not within range (or turned off), the blood glucose measures taken will be sent the next time the Bluetooth unit is turned on and the phone is within range.

Figure 2: OneTouch Ultra, NST bluetooth unit, Nokia 7650

When the Nokia 7650 receives the blood glucose measure from the patient, the phone will automatically send the measure as an SMS to a preset phone number. In the Wireless Health and Care project the Nokia 7650 is configured to send the measures to a PC equipped with a Nokia D211 phone card. From the PC the measures are sent over the Internet (Norwegian Health net in a real setting), using the DIPS[1] API and are stored on the DIPS server.

The NST developed application running on the SMS server runs the following loop:

1. Check if a new SMS measure has arrived.
   If a new measure has arrived:
   a. Check if the SMS has the correct format.
   b. Start a DIPS session, log on to the DIPS server. Access to the DIPS server is performed using the DIPS COM+ API.
   c. Create a new lab requisition on the DIPS server.
      The phone number of the arriving SMS is used to determine which patient id on the DIPS server the measure should be stored on.
   d. Store blood glucose measure, time and date in the requisition.

[1] DIPS is an EHR system that is used at many of the Norwegian hospitals.

e. Log of DIPS.

2. Return to 1.

Figure 3: Nokia D211 phone card

Once a measure is stored in the DIPS server, any DIPS client connected to the server can view the measure. The DIPS client can also display the data as a graph of measures over time.

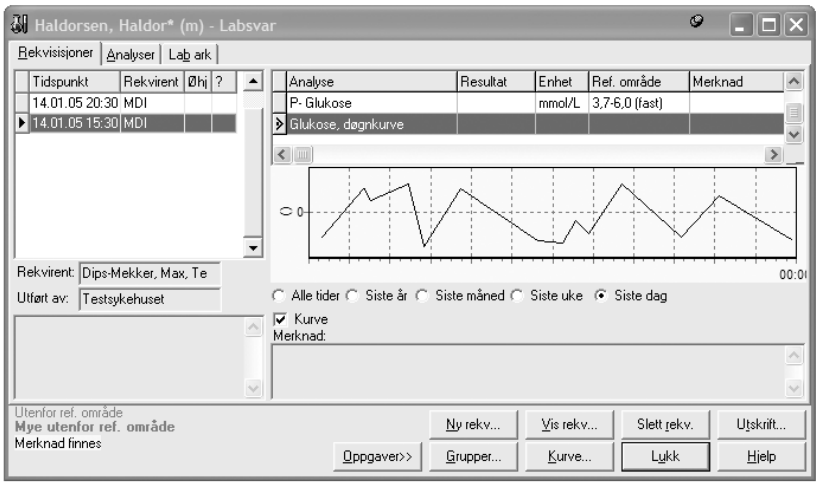

Figure 4: The lab module of the DIPS client, displaying blood glucose data

2.2 Security in the present setup

The connection between the sensor and the mobile phone is set up by a unique pairing of the Bluetooth ID of the Bluetooth chips in the two units. The chip in the sensor must be taken out and configured to be able to accept the ID of mobile phone. The mobile phone is turned on, and a search for Bluetooth devices is performed. Finally a pairing is done and the channel between the sensor and the mobile phone is set up. Note that it is impossible to do the pairing if the Bluetooth chip in the censor does not accept the Bluetooth ID of the mobile phone.

The measurement is transferred unencrypted from the sensor to the mobile phone. An application in the mobile phone generates an SMS containing the measurement, and

sends it automatically to the central server. This SMS is not encrypted. This is justified by that the measurements are not considered to be very sensitive.

The access control to the data stored in DIPS is handled by policies implemented in DIPS. We also assume that the DIPS server is set up and configured in such a way that the probability of an unauthorized person gaining access to the data stored there is very low. Further we assume that the communication between the SMS server and the DIPS server is secured, and that physical access to the SMS server is restricted.

3 System model

The general system model for WsHC is shown in Figure 5.

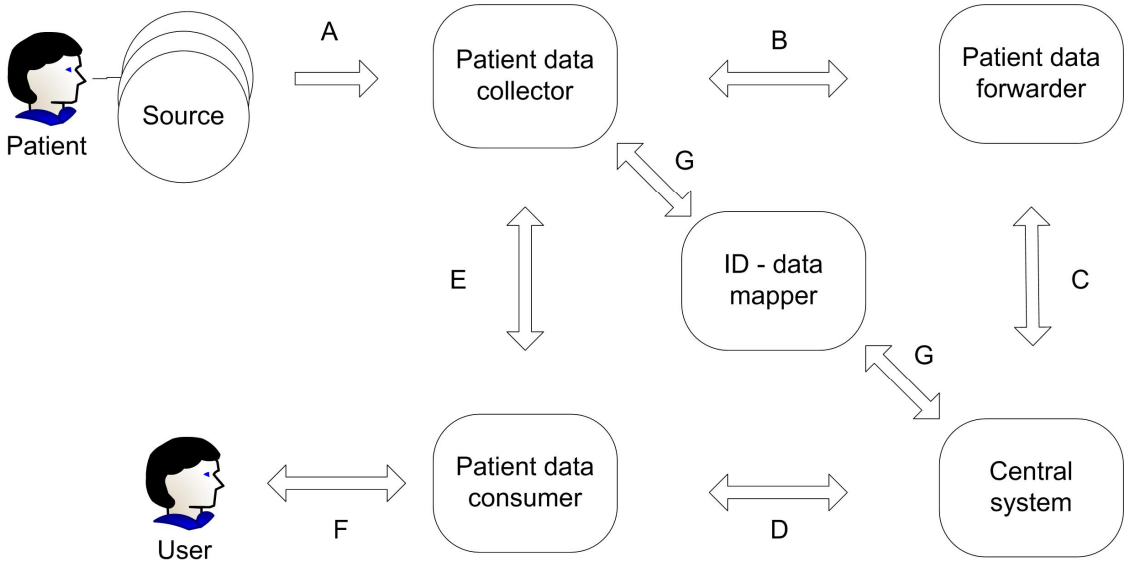

Figure 5: System model for WsHC.

The demonstrator consists of a Source that measures blood glucose levels and transfer these data over a Bluetooth channel to a mobile phone acting as a patient data collector. The mobile phone generates an SMS message containing the data and sends this SMS to a server located at a hospital. The received data are imported into the electronic health record (EHR) of the patient. The central system for this demonstrator consists of the server and the EHR. Health personnel can get access to the reported data through clients to the EHR, and these clients will then function as Patient data consumers.

Figure 6 shows the system model where the components in the demonstrator are shown.

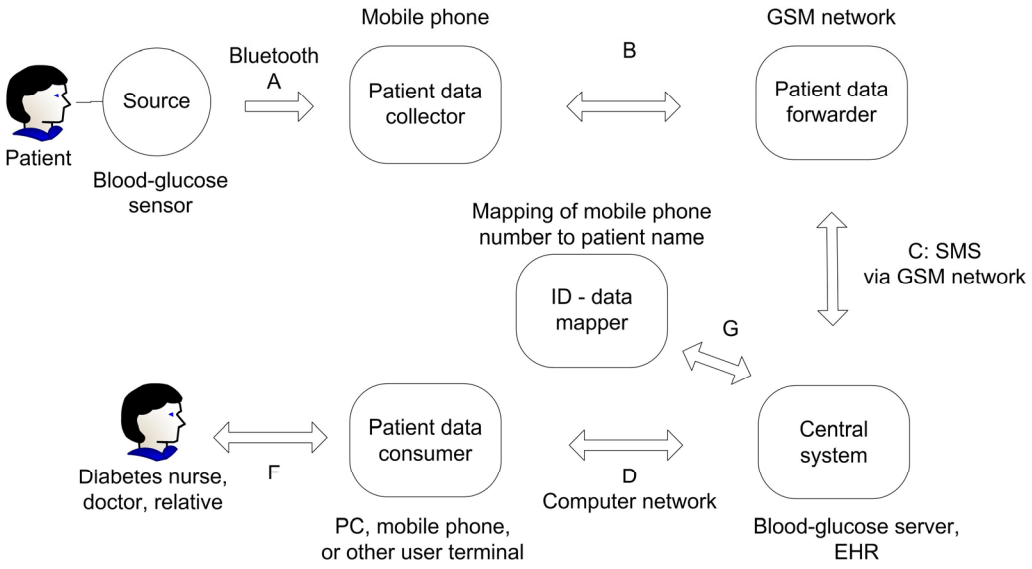

Figure 6: Blood-glucose demonstrator

We have the following use cases:

Use case 1:

1. The patient uses the sensor to perform a blood-glucose test.
2. Results are sent automatically to the mobile phone via Bluetooth.
3. Results are forwarded by the mobile phone via SMS to a server that is connected to a mobile phone card.
4. The results are connected to the patient and stored in the EHR.

Use case 2:

1. The diabetes nurse uses an EHR-client to look at the data for a patient.
2. A diabetes nurse reviews the results to determine whether the treatment plan of the patient needs to be changed.

4 Risk analysis – small scale testing

In the following risk analysis it is assumed that the system is used on a small scale for testing and prototype purposes. The testing is thought to be limited to one hospital with testing on around 100 patients. All the patients are informed about test setup and the risks this setup gives, and have agreed to participate in the test on a volunteer basis.

The data system discussed in this document handles measurements of blood glucose level used for treating diabetes. The data sent over the Bluetooth link only contains the measurements and is not connected to the patient. The SMS contains both the data, and the sender's phone number, and can therefore be traced back to the patient.

These measurements are not highly sensitive, and the measured data might not be of use for others than the patient and the health personnel, but if the system is widely used the measured data could be of interest for e.g. insurance agencies, and manufacturers of medical equipment. The patient may also want to hide from the public that he or she has diabetes. On the other hand it is important that the collected data are correct, since the patient can be treated on basis of the collected data, and wrong treatment can lead to danger for the patient's health. But the long-time blood glucose level HB1Ac is measured during consultations with health personnel, which gives the possibility to detect if the collected data are very incorrect.

In the following a list of risks are given, and each risk is given a probability level and a consequence level. The given probabilities for the risks are for a demonstrator where the security measures mentioned in section 2.2 are implemented.

The consequence levels are defined as following:

Consequence level	**Description**
Catastrophic	Loss of lives.
Large	Danger for patients' life and health. Privacy breach for a large number of patients. Serious economic losses. Serious loss of reputation.
Moderate	No danger for patients' health. Privacy breach for a small number of patients. Moderate economic losses. Moderate loss of reputation.
Small	No danger for patients' health. No privacy breach. Inconsequential economic losses. No loss of reputation.

Table 1: Consequence levels

We use the following probability levels:

Probability level	**Description**
High	The event must be expected to occur several times per year. No security measures or security measures that can be accidentally breached, both by internal personnel and outsiders.
Medium	The event must be expected to occur at least once per year. Security measures can be easily breached by internal personnel, both accidentally or on purpose. Outsiders can't breach the security measures accidentally, and need some knowledge about the system and implemented security measures to attack the system on purpose.
Low	The event must be expected to occur once every 2-3 years.

	Security can be breached by internals on purpose and with knowledge of the system. Outsiders need detailed knowledge about the system and routines and special equipment to be able to attack the system.
Very low	There is a slight possibility for the event but it is not expected to occur. Security can only be breached by internal personnel with special competence. Outsiders can normally not attack the system.

Table 2: Probability levels

4.1 Incorrect data stored for a patient

The data that is stored in the central system may not be the same as the data that is measured for the patient.

This can happen if

- The data is sent from the sensor to the wrong mobile phone, and belongs to another patient.
- An attacker sends fake data on the Bluetooth link.
- An attacker sends SMSs with spoofed sender phone number and with fake measurements.
- The patient modifies his/her own data. This can for example be done by sending an SMS with wrong data to the server.

The consequences of such an incident are considered to be large since it may affect the treatment of the patient, and through that the patient's health.

The probability of data being sent to the wrong mobile phone is considered to be very low, since the connection between the sensor and the mobile phone is done on a hardware level, and is not easily modified.

The probability of an attacker actively sabotaging the data by attacking the Bluetooth or SMS communication is also considered to be very low. Sophisticated equipment and some knowledge are needed to performing such an attack. The attacker would also not gain much performing such an attack, especially since there are few users.

In the present setup it would be easy for the patient to modify his/her own data, if he/she wants to do so. In this analysis we assume that the patient cooperates, and that patients who are suspected for wanting to modify his/her own data are treated specially.

4.2 An unauthorized person gaining access to data for one patient

A non-authorized person can gain access to the data if:

- An attacker is able to eavesdrop on communication on the Bluetooth link.
- An attacker is able to eavesdrop on the communication between the mobile phone and the central server and gains a copy of the SMS.

- The application on the mobile phone is not configured correctly so it sends the SMS to the wrong receiver.

The consequences of such an incident are considered to be moderate since it is a small privacy breach, and as mentioned earlier in this section, the data collected is considered to be not so sensitive.

The probability of the mobile phone sending the messages to the wrong phone number is considered to be low given that proper routines for ensuring that the configuration of the application is correct.

The probability of an attack on the Bluetooth or SMS communication is considered to be low since the data sent are not readily useful for an attacker, and since the attacker needs sophisticated equipment to perform the attack.

4.3 An unauthorized person gaining access to data for a large number of patients

This incident may be caused by:

- An attacker gaining access to the EHR system.
- An attacker gaining access to the server receiving the SMS.
- An attacker eavesdropping on all the SMS-communication to the server.

The consequences of such an incident are considered to be large, since the privacy of a large number of patients may be breached.

The probability of an attacker gaining access to the SMS server or the EHR system is considered to be very low, if a sufficient level of access control, both physical and through authentication of the users, is implemented both for the EHR system, the SMS server, and the data channel between these two servers.

The probability of an attacker eavesdropping on all the SMS-communication to the server is considered to be very low, even though the SMSs are unencrypted. The reason for this is that the attacker would need very sophisticated equipment to be able to perform such an attack, and since it is only a small number of patients, the attacker would not gain much on performing such an attack.

4.4 Loss of collected data

The data is lost if the data measured on the sensor for some reason fails to be sent to the server.

This incident may be caused by:

- Error on the Bluetooth channel.
- Accidental jamming of the Bluetooth channel.
- Jamming of the Bluetooth channel done on purpose by an attacker.
- The mobile phone is switched off, or out of range when the sensor tries to send the data.

- Error when sending the SMS.
- Error on the SMS server.
- The patient purposely preventing the data from being sent.

The consequences of such an attack are considered to be small, since it results neither in danger for the patients health, or in loss of privacy, and it is easy to detect that data is lost.

The probability of such an incident is considered to be high, since there are so many ways that the communication can fail. Jamming of the Bluetooth channel requires sophisticated equipment, and the gain of such an attack is considered to be very low. The Bluetooth standard is pretty resistant against accidental jamming.

As with modification of data we assume that the patient cooperates, and does not sabotage his/her own data.

4.5 Software errors and configuration errors

Errors in the software or in the configuration of the software may result in both loss of data, or incorrect data connected to a patient. Error in the configuration of the mobile phone may also cause SMSs with patient data to be sent to the wrong recipient.

Since this risk analysis concerns the testing of a demonstrator system, the probability for such errors should be considered to be high.

However during the testing phase all data should be checked up against original data recorded by the patient to make sure that the collected data are correct, and that data not has been lost. Provided that this is done, the consequences of such an error should be small.

4.6 Summary

Risk ID	Description	Probability	Consequence
R1	Incorrect data stored for a patient	Very low	Large
R2	An unauthorized person gaining access to data for one patient	Very low	Moderate
R3	An unauthorized person gaining access to data for a large number of patients	Very low	Large
R4	Loss of collected data	High	Small
R5	Software errors and configuration errors	High	Small

Table 3: Summary of risks

In the risk matrix we have the following risk levels:

Low risk	Medium risk	High risk

Low risk – Acceptable risk level, however risk reducing measures that are easy to implement should be considered.

Medium risk – Risk reducing measures should be considered from a cost/benefit point of view.

High risk – Not acceptable risk level. Risk reducing measure **must** be implemented.

Consequence: Probability:	Small	Moderate	Large	Catastrophic
Very low		R2	R1, R3	
Low				
Medium				
High	R4, R5			

Table 4: Risk matrix

5 Revised risk analysis – full-scale testing and normal use

In this section the risk analysis is revised to cover full-scale testing, and operational usage. We assume that the system is stable, and that the system is used on a big scale.

5.1 Incorrect data stored for a patient

The probabilities and consequences for storing incorrect data for a patient will be the same as for the small scale testing. That is the probability is very low, and the consequences are large.

5.2 An unauthorized person gaining access to data for one patient

The consequences of an unauthorized person gaining access to data for one patient are still considered to be moderate.

We still consider these attacks to be so sophisticated compared to the value of the information that an attacker can get in this way, that we still consider the probability for such an attack to be low.

5.3 An unauthorized person gaining access to data for a large number of patients

The consequences of an unauthorized person gaining access to data for a large number of patients are still considered to be large.

We still consider the probability of an attacker gaining access to the central system to be very low. However an attacker can gain access to a large amount of data without attracting any notice by eavesdropping on all the SMS traffic to the SMS server. Since the SMSs can be tracked back to the patients using the mobile phone number, and the system is used by a large number of patients, the probability for such an attack will be higher. Sophisticated equipment is still needed however, and we consider the probability of such an attack to be medium.

5.4 Loss of collected data

The probability and consequences for loss of collected data is still the same, independent of the number of patients using the system.

5.5 Software errors and configuration errors

When the software is used on a larger scale it should be tested very carefully, so that the probability for software errors should be low. There should also be clear routines for installation and configuration of the software to prevent configuration errors.

Software errors could lead to that incorrect data is stored for a patient, or that the privacy for a large number of patients is breached. The consequences of software or configuration errors are therefore large.

5.6 Summary

Risk ID	Description	Probability	Consequence
R1	Incorrect data stored for a patient	Very low	Large
R2	An unauthorized person gaining access to data for one patient	Low	Moderate
R3	An unauthorized person gaining access to data for a large number of patients	Medium	Large
R4	Loss of collected data	Medium	Small
R5	Software errors and configuration errors	Low	Large

Table 5: Summary of risks

Consequence: Probability:	Small	Moderate	Large	Catastrophic
Very low			R1	
Low		R2	R5	
Medium			R3	
High	R4			

Table 6: Risk matrix

6 Requirements

6.1 Security requirements

The requirements below are the same as in the general requirements document [2].

(Requirement numbers correspond to those of the logical system model. Requirements that are not applicable for the demonstrator are left blank.)

No.	*Actor(s)*	*Requirement*	*Requirement fullfillment*
Sec13.1	Source	**Limited storage**. Sensor shall not store sent data longer than necessary (confidentiality)	The data is not considered sensitive, and is stored on the phone.

No.	*Actor(s)*	*Requirement*	*Requirement fullfillment*
Sec13.2	Channel A	**Short-range communication.** Source and Patient data collector shall only communicate with each other short range (confidentiality and integrity)	OK. The communication between the sensor and the mobile phone is short range.
Sec13.3	Channel A	**Confidentiality protection.** Patient data should be protected from eavesdropping when transmitted to Mobile phone. (Note: communication is short range, which reduces the need for strong communication encryption)	This is considered to not being necessary, since the data are not considered to be sensitive for the patient, and since an attacker would not gain much performing such an attack.
Sec13.4	Channel A	**Integrity protection**. Patient data should be integrity protected when transmitted to Mobile phone. (Note: this includes protection from interference)	OK, a reliable Bluetooth channel is used.
Sec13.5	Channel A	**No automatic roaming**. The connection between Sensor and Mobile phone shall be manually initiated, i.e. a human actor determines (at some point in time and through a defined procedure) which Sensors and Mobile phones that shall talk to each other (integrity)	OK, the setup of the connection between the mobile phone and the sensor is done manually.
Sec13.6	Patient data collector	**Verify Sensor identity**. Mobile phone shall verify correct identity of the Sensor (integrity and accountability)	This is done when the connection is set up.
Sec13.7	Patient data collector	**Data integrity verification**. Mobile phone shall verify the integrity[2] of patient data (integrity)	The channel between the sensor and the mobile phone is assumed to be reliable.
Sec13.8	Patient data collector	**No data modification.** Mobile phone shall not modify patient data, except possibly for aggregation or other defined transformations (integrity)	OK. Data is not modified at the mobile phone.

[2] "Integrity verification" refers to the verification that data has not been altered during transmission from the Source; it does not imply a "sanity check" on the data. Such a sanity check should be implemented somewhere in the system; at least in the Central system before storage of the data.

No.	*Actor(s)*	*Requirement*	*Requirement fullfillment*
Sec13.9	Patient data collector	**No unauthorised data access.** Mobile phone shall not give unauthorised actors access to patient data (confidentiality and integrity)	The data is not more sensitive than other data the patient will have stored on his mobile phone, and no extra access control is implemented.
Sec13.10	Patient data collector	**Limited storage.** Mobile phone shall not store data longer than necessary to ensure successful transmission of patient data (confidentiality)	In the present demonstrator the message is stored as an SMS, and all sent SMS are stored on the phone.
Sec13.11	Channels B, C, D and E	**Confidentiality protection.** Personally identifiable patient data shall be protected from eavesdropping when transmitted across open networks.	Channel B and C, from the mobile phone to the server is not protected in the present demonstrator. Protection should be implemented before the system is set in normal use.
Sec13.12	Channels B, C, D and E	**Integrity protection.** Patient data shall be integrity protected when transmitted across open networks.	The data is sent over reliable channels, but in the present demonstrator it is possible to inject false data into the system so that the integrity is compromised.
Sec13.13	Central system	**Data integrity verification.** Central system shall verify the integrity of patient data.	This is done at import into DIPS.
Sec13.14	Central system	**Data origin authentication.** Central system shall authenticate the Mobile phone or the user of the Mobile phone (integrity and accountability)	The central system checks the origin using the senders mobile phone number.
Sec13.15	Central system	**No unauthorized access**. Central system shall not give unauthorised actors any type of access (view, insert, transform, delete) to patient data in the central system (confidentiality and integrity)	Access control to the stored data is handled by DIPS.
Sec13.16	Central system	**Patient identity.** Central system shall know the identity of the patient to whom the patient data pertains (integrity)	The central system gets the identity of the patient from the mobile phone number.

No.	*Actor(s)*	*Requirement*	*Requirement fullfillment*
Sec13.17	Central system	**Source type**. Central system shall know the type of sensor used to produce the patient data (integrity)	The server provides information about the source when storing in DIPS.
Sec13.18	Channel D	**Authenticate User.** Central system shall authenticate the User (confidentiality and accountability)	Access control handled by DIPS.
Sec13.19	Channel D	**Authenticate Central System.** PC, mobile phone, or other user terminal shall authenticate the Central system (integrity)	Authentication of the central system is handled by the DIPS client.
Sec13.20	Channel E		
Sec13.21	Patient data consumer	**Data integrity verification.** PC, mobile phone, or other user terminal shall verify the integrity of patient data	The channel between the DIPS server and the DIPS client is reliable.
Sec13.22	Patient data consumer	**No unauthorized access.** PC, mobile phone, or other user terminal shall not give unauthorised actors any type of access (view, insert, transform, delete) to patient data from the PC/mobile phone/user terminal (confidentiality and integrity)	Access control is implemented in the DIPS client.
Sec13.23	All components	**Emergency access.** Where emergency access functionality is available, invocation of emergency access shall override any restriction on read access (availability)	Emergency access is handled by DIPS.
Sec13.24	All components except Source	**Emergency access monitoring**. Emergency access shall trigger extended monitoring of relevant events to enable detection of unnecessary access (confidentiality and accountability)	Emergency access is handled by DIPS.

Table 7: Security requirements

7 Security recommendations

This section lists some security recommendations that should be implemented before the system can be used in an operational setting.

7.1 Storage of data at sensor and mobile phone

The data is the user's own data, and it might be useful for the user to have her own data stored locally on the sensor or mobile phone. The data should not be stored locally without the user's knowledge and consent, and it should be possible for the user to prevent this, or to remove the stored data.

The measurements are not considered to be very sensitive, and it is sufficient that the access to the mobile phone is controlled by normal means, e.g. physical access control and with a PIN-code.

7.2 Communication between sensor and mobile phone

We do not recommend any further security measures on this communication link since, as noted earlier, the information sent between the sensor and the mobile phone is not very sensitive, and a potential attacker would gain very little by attacking this link.

However, if it is deemed necessary that this communication link should be protected from eavesdropping, this could be done by the means of standard Bluetooth encryption functionality. This would also provide authentication of the sensor. The use of the encryption functionality requires that a key is installed on the sensor and on the mobile phone. This key is used as a basis for the encryption and to make this encryption strong enough we recommend that the full key-length (128 bit) is used. For more information about Bluetooth security, see [3].

7.3 Communication between mobile phone and blood glucose server

Since SMS is not a reliable channel, and also only provides one-way communication, we recommend that the SMS channel is replaced with communication over IP using GPRS, EDGE, 3G or similar technologies. This will ensure that the application on the mobile phone will be notified if the communication with the server fails.

Communication over IP together with an encryption scheme can also provide two-way authentication. This ensures that it is only mobile phones running the developed application that can send data to the server, and also prevents data from being sent to the wrong recipient.

To prevent attackers from eavesdropping on the communication between the mobile phone and the server, and to provide two-way authentication we recommend that encryption is implemented. To further enhance the security the mobile phone could sign the messages before sending them to the server, but in general it is enough that the server is able to authenticate the mobile phone.

There exist several possible encryption schemes, Public Key Infrastructure (PKI), or that the mobile phone and the server share a secret key, either symmetric or a private/public key pair. The key used for the authentication and encryption can be installed together with the blood glucose application. Since the sensor shall initiate the sending of the message to the server and the message shall be sent automatically without the user

needing to accept, the key used for authentication and encryption must be accessible from the software running on the phone.

One possibility is the use of the key embedded in the SIM-card. All SIM-cards from Telenor Mobile (except some very old ones) are equipped with public key cryptography functionality. However, at present this can only be used to sign an SMS received from Telenor's mHandel service platform, returning the SMS to the same service platform. Although it is possible to utilize this to achieve authentication of the user and integrity protection of the blood glucose measurement, the user interaction is deemed to be too awkward for the purposes of this demonstrator. See Appendix A for a description of Telenor's mobile PKI in the context of the demonstrator.

Another possibility is the use of another PKI, for example a general purpose PKI for healthcare. This PKI is planned, but not yet implemented [4]. Other options include that the server share a secret key with each of the mobile phones. If the there is one secret key for each mobile phone, the server has to store the complete list of keys. The same key can be used for all the mobile phones, but this would reduce the security, and there would be a large task to change the key on all the mobile phones, if the key was compromised.

7.4 Software and configuration maintenance

Careful routines for installation, configuration and maintenance of the software should be implemented. All software should be carefully tested to ensure that there are no bugs that could affect to integrity of the collected data before the software is used in an operational setting. Further when installing the software on the patients mobile phone, the software and the configuration of the software should be tested to make sure that the data is sent to the right place, and that the data is associated with the right patient when they are imported into the EHR system.

8 Conclusion

The security of the blood-glucose demonstrator implemented by NST was analyzed. We found that the security was sufficient for a small-scale test, but that there should be implemented additional security before the system can be used on a larger scale.

The most important issue is that the confidentiality of the communication between the mobile phone, and the central server should be protected. To do this we recommend that the communication is done over IP, and that an encryption scheme is implemented.

9 References

[1] R. Arnesen, J. Danielsson, J. Ølnes and J. I. Vestgården. *WsHC Security Architecture*. NR Technical Report 1006, January 2005.

[2] R. Arnesen, J. Danielsson, J. Ølnes and J. I. Vestgården. *WsHC Security Requirements*. NR Technical Note DART/01/05, January 2005.

[3] H. J. Rivertz, *Bluetooth Security*. NR Technical Note DART/05/05, March 2005.
[4] A. Vestad. *Anbefalinger og standarder for PKI i helsesektoren*. KITH rapport nr. 13/04, 19.10.2004.

10 APPENDIX A: Use of Telenor Mobile's PKI in the demonstrator

10.1 Telenor Mobile's PKI in short

All SIM cards issued by Telenor Mobile are equipped with software for public key cryptography. A key pair is created for each SIM card. This software is used for Telenor Mobile's "mHandel" services (mobile e-commerce). A Telenor Mobile subscriber must explicitly activate access to the mHandel services, and the activation process includes issuing of a certificate for the subscriber's public key. The certificate is issued by ZebSign and is a qualified certificate according to the EU Directive on electronic signatures.

Only the user's private key exists on the SIM-card. The public key and the certificate are only stored in Telenor Mobile's mHandel service platform.

The functionality offered is very limited. The mobile phone receives an SMS from the mHandel service platform, this SMS is signed (cannot be altered) and returned to the mHandel service platform. The signature is checked by means of the certificate, and the result is logged in what Telenor Mobile calls a "notary log" (refers to a notary third party service for electronic commerce).

The primary use of this functionality is to sign an SMS containing an "order" (confirming that the user buys something to a certain price). Telenor Mobile has close to 40 different services on the platform, with cinema tickets and refill of mobile phone cash cards as the two mot popular ones. Apart from this, the services range from airplane tickets with Norwegian and tickets for the airport express train in Oslo to beer (or any other order) at certain pubs and soft drinks at some vending machines. The procedure is explained below.

Some third-party software suppliers have implemented both authentication for access to company internal systems and signing of electronic documents based on the solution. This is explained briefly below but is not really of interest to the wsHC demonstrator.

It is not possible to write and sign an SMS, to sign an SMS received from anyone else but the mHandel service platform, or to send a signed SMS to anyone else but the service platform. The solution has one key pair, used only to sign SMSs. There is no encryption functionality. According to Telenor Mobile, these limitations are due to the software used as basis for the solution (SIM toolkit based, Entrust software for the service platform).

However, one may also suspect that Telenor Mobile does not really want a more open solution. Telenor Mobile has to pay for the extra functionality on the SIM cards, a cost that the company must gain back (with a profit) from use of the service platform. If the key pair and the certificate were allowed for more general use, other service providers could capitalise on the investment without paying a share of the costs.

10.2 NetCom's mobile PKI

NetCom is in the process of introducing similar functionality in the company's SIM cards. Several hundreds of SIM card key pairs and certificates have been issued and are used for pilot services. Certificates are issued by NetCom's owner, Telia (in Sweden) and are reputedly at a qualified level (although NetCom has refrained from using the qualified term as long as the system is used only in pilot operation, to avoid the obligations that are imposed on issuers of qualified certificates according to Norwegian law).

The service platform is provided by Buypass (a joint venture by ErgoGroup/Posten and Norsk Tipping), and the primary service is betting on Norsk Tipping's different games.

NetCom operates a mobile eCommerce platform but it is not clear if this will be enhanced to take advantage of the mobile PKI.

NetCom's solution is based on the same software platform as Telenor Mobile's solution but both parties have modified and done further development. Making the services of the Telenor Mobile's mHandel service platform available to subscribers of NetCom's mobile PKI, or the other way around (Buypass/NetCom services available to Telenor Mobile subscribers) may be rather straightforward from a technical perspective. However, the commercial aspects may be more challenging. As a minimum, certificates and revocation information must be made available to the other party.

10.3 SMS service provider Interface to mobile PKI

The steps taken in accessing an SMS-based service by means of Telenor Mobile's PKI solution are shown in Figure 7 below. Telenor Mobile provides an API (application program interface) to all service providers on the service platform. Communication between the service provider and the mHandel service platform is typically over Internet protected by SSL or a VPN solution. The API is extensible. Functionality may be added for particular service providers.

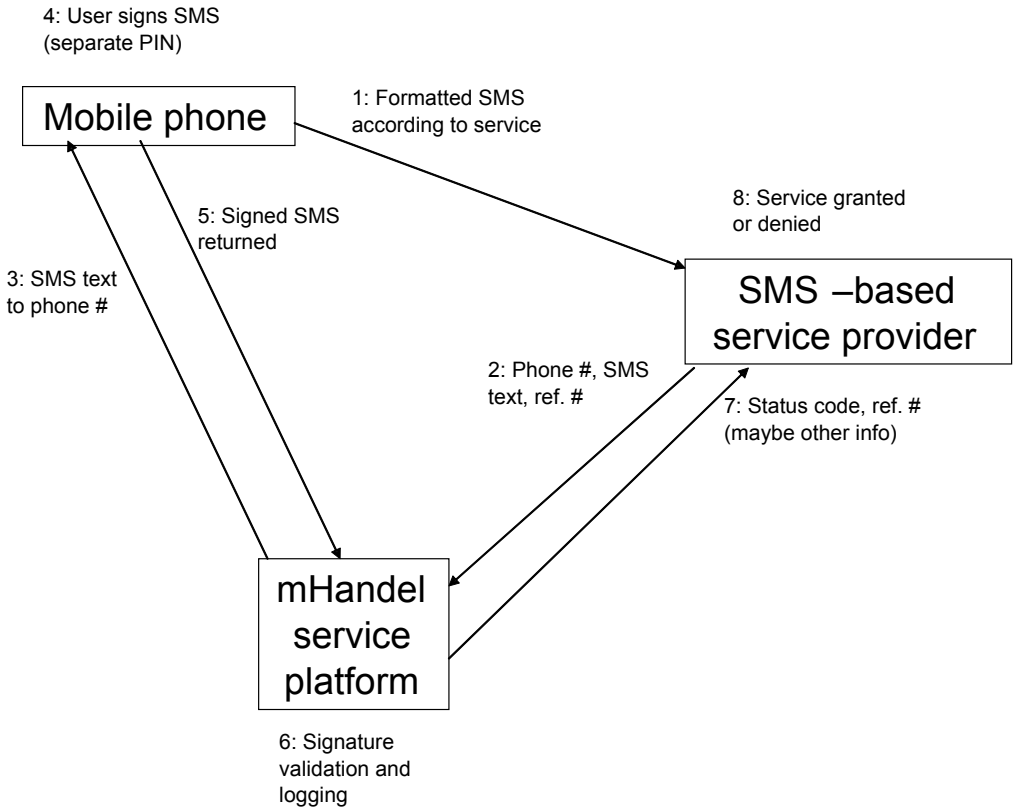

Figure 7: Steps in service access by Telenor Mobile mHandel

The eight steps are carried out as follows:

1. The user is instructed to send a formatted SMS to the service provider. The service provider is in charge of reception and processing of this SMS, which must identify the service requested.
2. A call is made over the API to the mHandel service platform. The service provider supplies the text for the SMS that is to be sent to the user (anything goes, within the limits of a single SMS), the phone number, and a unique reference number. Possibly, other parameters can be supplied (extensible API).
3. The mHandel service platform sends the SMS to the phone number specified, following a check that the user has activated access to mHandel services.
4. The user signs the SMS on the phone, using a separate PIN code (not the one used to access the SIM when the phone is turned on) to access the private key.
5. The signed SMS is returned to the mHandel service platform.
6. The mHandel service platform verifies the signature by means of the user's certificate and logs appropriate information in the "notary log". (Probably, only hash value and signature is logged, not the entire SMS, but we do not have authoritative information on this.)
7. A status code ("OK" or "not OK" at a minimum) is returned to the service provider together with the reference number. Due to the extensibility of the API, further information may be returned. The signed SMS and the certificate are not

returned by default, which means that the service provider cannot itself verify the signature.

8. Service is granted or denied according to the status code, e.g. tickets are reserved or the vending machine is instructed to release one bottle of soft drink.

10.4 Payment

Both service providers and users must be registered with the mHandel service platform. In addition to the steps outlined above, the platform serves as a clearinghouse for accounting and billing for use of services. Since Telenor is not a bank, the Norwegian bank DNB-NOR is brought in as a partner.

Users may select method of payment. The amount may be charged on the telephone bill, drawn from a prepaid account at the mHandel service platform, or from the user's credit or debet card as registered in the service platform.

10.5 Internet-based service provider interface to mobile PKI

The steps taken are exactly the same as outlined above, except that step 1 is carried out over (typically) a web-interface instead of by SMS. A formatted email may of course also be used. The user must explicitly supply the phone number in step 1.

Internet-based includes services on the GPRS or UMTS platforms.

10.6 Log-on to systems by mobile PKI

Several third-party software suppliers (notably Tieto Enator and Efactory) demonstrate use of mobile PKI to log on to a system (e.g. company internal, as used by Tieto Enator itself).

In this scenario, the user enters the phone number in a web logon page. The "service provider" (the logon service) initiates an SMS to be sent via the mHandel service platform to the user, who signs and returns it. If status code is "OK", the user is allowed access.

Some solutions add one further step where the signing of the SMS results in a one-time password being sent to the user by SMS. The user enters the one-time password in the web interface to log on to the system.

10.7 Signing a document by mobile PKI

Solutions for signing documents have been developed by e.g. Tieto Enator and Efactory. Solutions are server-based in that the document to be signed must be available through a web-server (the Service provider in Figure 7, with a web-interface instead of SMS). The document may be created on the server (e.g. some kind of form) or it may be uploaded from the user (or somewhere else) to the service.

The user requests signing and supplies the phone number. The document is assigned a reference number. The service performs the hashing and presents both reference number and hash to the user on the web-interface.

The reference number and hash value is passed to the mHandel service platform as SMS text and sent to the user's phone. The user compares reference number and (preferably)

hash value with the values in the web-interface and signs the values on the phone. In this case, the signature value (from the signed SMS) must be returned to the service provider along with the status code in step 7 in Figure 7.

When receiving the signature value, the service provider creates a signed data object. This is necessarily a non-standard data structure. The document is hashed by the service provider, and this hash value is actually itself hashed (as part of the SMS) on the mobile phone. Thus, the signature is a cryptographic operation on a "hash of a hash". The signed data object must have placeholders for both the original hash and the signature obtained from the mobile phone.

10.8 Use in the blood glucose demonstrator, SMS case

Authentication of source (mobile phone is indicated, but user should be even better) and integrity protection are listed as key requirements for the demonstrator. Telenor Mobile's PKI solution can answer these requirements at the expense of additional user involvement and more SMS traffic.

Since it is not possible to sign arbitrary SMSs, the signature must be created by the user on an SMS received from the mHandel service platform. The process can work as follows:

1. The blood glucose measurement is sent by SMS to the Central system as usual.
2. The Central system calls the mHandel service platform, passing along the phone number and an SMS text like "Blood glucose measurement at time xx is yy. Please sign and return if this is correct."
3. The user must explicitly check the reported measurement value against the original SMS sent to the Central system (or a display on the sensor, if available).
4. If OK, the user signs the SMS and sends it back to the mHandel service platform, and the Central system receives an "OK" status code.
5. If something is wrong, a particular procedure should be initiated in order to declare the measurement as void, and the user should perform a new blood glucose measurement.
6. In this case, only the mHandel service platform stores the actual signatures. If the Central system wants to log more detailed information itself, this information must be provided over the API to the service platform.

The main disadvantage is that the user must be explicitly involved in the process, as opposed to the automated SMS procedure that is described for the original demonstrator. Also, several SMSs are needed, which implies a greater risk of loss of SMSs or delays.

10.9 Use in the blood glucose demonstrator, GPRS case

Since Telenor Mobile's PKI solution cannot be used for authentication at session establishment time, the SMS signing procedure must be used to provide authentication and integrity protection of the blood glucose measurement even in this case. The scenario can be regarded as equal to the Internet case described in 10.5.

The user establishes a GPRS connection/session to the Central system, or the connection is automatically established by the mobile phone when the measurement is

received from the sensor. The measurement is reported, and the Central system initiates an SMS signing procedure to the user's phone as described earlier.

Again, the authentication and integrity protection is provided at the expense of extra user involvement and extra SMSs.

10.10 Conclusion

While it is clear that Telenor Mobile's PKI solution can provide authentication of source and integrity protection for blood glucose measurements, the security gained should be weighted against the extra user involvement and the extra SMSs needed.

Integration towards the mHandel service platform is fairly straightforward, and with Telenor as the lead partner in wsHC, access at favourable terms should be possible in case one wants to test this as an alternative in the demonstrator. Some manpower is needed, but, as stated, integration is fairly straightforward.

This decision is left to the responsible party for the demonstrator (NST) and the wsHC project management.