LAPPEENRANTA UNIVERSITY OF TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

Wireless Authentication and Authorization, case Wireless Access Control System

The subject of the thesis has been approved by the council of the Department of Information Technology on May 14th, 2003.

Supervisors: Professor Jari Porras
D.Sc. (Tech.) Jouni Ikonen

Lappeenranta, April 27, 2004

Arto Hämäläinen
Korpimetsänkatu 10 C 9
53850 Lappeenranta
Finland

ABSTRACT

Lappeenranta University of Technology
Department of Information Technology
Hämäläinen, Arto

Wireless Authentication and Authorization, case Wireless Access Control System

Master's thesis
2004
77 pages, 13 figures, 3 tables and 1 appendix

Supervisors: Professor Jari Porras
D.Sc. (Tech.) Jouni Ikonen

Keywords: authentication, authorization, access control, PKI, Bluetooth

The utilization of short-range wireless technologies enables use of new kind of local services as well as enhancement of old services. Access control is a daily service, and it's been selected as an example application. Several authentication and authorization mechanisms are studied, and public key infrastructure is presented as an example application of public key cryptography. The general information about Bluetooth, Zigbee, RFID and IrDA wireless technologies is presented in the wireless technologies chapter. The structure of Bluetooth, including its security architecture, is studied more carefully.

Bluetooth is used as transfer medium in the designed wireless access control system. A handheld device equipped with Bluetooth technology acts as a personal trusted device, which can be used as a key device of its owner. Authentication and authorization is based on public key infrastructure. Public key certificates, signed by the administration, include information about a user and his rights as well as his public key. Challenge response mechanism based on public and private keys is used to perform authentication at the access controllers. Shortly, handheld Bluetooth devices are used as wireless keys to electromechanical locks.

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto

Tietotekniikan osasto

Hämäläinen, Arto

Langaton käyttäjän tunnistaminen ja valtuuttaminen, case Langaton kulunvalvontajärjestelmä

Diplomityö

2004

77 sivua, 13 kuvaa, 3 taulukkoa ja 1 liite

Tarkastajat: Professori Jari Porras
TkT Jouni Ikonen

Hakusanat: tunnistaminen, valtuuttaminen, kulunvalvonta, PKI, Bluetooth

Lyhyen kantaman radiotekniikoiden hyödyntäminen mahdollistaa uudenlaisten paikallisten palveluiden käytön ja vanhojen palveluiden kehittämisen. Kulunvalvonta on päivittäisenä palveluna valittu työn esimerkkisovellukseksi. Useita tunnistus- ja valtuutustapoja tutkitaan, ja julkisen avaimen infrastruktuuri on esitellään tarkemmin. Langattomat tekniikat Bluetooth, Zigbee, RFID ja IrDA esitellän yleisellä tasolla langattomat tekniikat –luvussa. Bluetooth-tekniikan rakennetta, mukaan lukien sen tietoturva-arkkitehtuuria, tutkitaan tarkemmin.

Bluetooth-tekniikkaa käytetään työssä suunnitellun langattoman kulunvalvontajärjestelmän tietojen siirtoon. Kannettava päätelaite toimii käyttäjän henkilökohtaisena luotettuna laitteena, jota voi käyttää avaimena. Käyttäjän tunnistaminen ja valtuuttaminen perustuu julkisen avaimen infrastruktuuriin. Ylläpidon allekirjoittamat varmenteet sisältävät käyttäjän julkisen avaimen lisäksi tietoa hänestä ja hänen oikeuksistaan. Käyttäjän tunnistaminen kulunvalvontapisteissä tehdään julkisen ja salaisen avaimen käyttöön perustuvalla haaste-vastaus-menetelmällä. Lyhyesti, järjestelmässä käytetään Bluetooth-päätelaitteita langattomina avaimina.

PREFACE

This thesis is a result of my studies and research at the Lappeenranta University of Technology. The thesis has been done at the Department of Information Technology. I got a possibility to write it while working at the Laboratory of Communications Engineering at LUT.

I'd like to thank my supervisors professor Jari Porras and D.Sc (Tech.) Jouni Ikonen for your effort, and all the co-workers, past and present, at the Comlab for advices. Also thanks to my parents who have been worried about my graduation for the last few months. Most thankful I am to Sanna - Your support was essential to my studies and this thesis.

Arto Hämäläinen

TABLE OF CONTENTS

List of figures

List of tables

Abbreviations

CA	Certificate Authority
CoD	Class of Device
dBm	Decibel referenced to milliwatt
FCC	Federal Communications Commission
FHS	Frequency Hop Synchronization
GAP	Generic Access Profile
GTS	Guaranteed Time Slots
ID	Identifitcation
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IrDA	Infrared Data Association
IrLAN	Infrared Local Area Network
IrMC	Infrared Mobile Communications
IrOBEX	Infrarex Object Exchange
IrTran-P	Infrared Transfer Picture
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunications Union – Telecommunications Standardization Sector
L2CAP	Logical Link Control And Adaptation Protocol
LAN	Local Area Networking
LMP	Link Manager Protocol
MAC	Media Access Control
MHz	Megahertz
mW	milliWatt
OBEX	Object Exchange Protocol
PHY	Physical
PIN	Personal Identification Number
PKC	Public Key Certificate
PKI	Public Key Infrastructure

PTD	Personal Trusted Device
RA	Registration Authority
RSA	Rivest Shamir Adleman Algorithm
RSSI	Received Strength Signal Indicator
SDAP	Service Discovery Application Profile
SDP	Service Discovery Protocol
SIG	Special Interests Group
SPP	Serial Port Profile
Wi-Fi	Wireless Fidelity
XML	eXtensive Markup Language

1 INTRODUCTION

Some kind of access control is needed daily. People need to unlock doors to their apartments, cars or workplaces. When they use their computers to access network services like email, access control is needed. In a traditional access control system there are locked doors, keys that match the locks on the doors and a way to manage the key-door combinations. The owner of the building must be able to control the keys for the locks. In practice, for example a janitor provides the people with keys when needed. When applying for a key, an applicant is authenticated somehow and a suitable key is given to him.

Wireless handheld devices, especially mobile phones, have become very common nowadays. People use them on a daily basis, carrying their phones practically all the time with them. The performance and properties of these devices is far better than in "similar" devices a few years ago. Mobile phones were used just to call and write short messages then, but in these days, the latest models have capabilities to install and run users' own applications.

In this thesis, access control systems and the use of wireless handheld devices are combined. A wireless access control system, in which handheld devices are used as keys in a physical access control system, is designed and implemented. Wireless short-range connections are used when transferring information between the administrator and the user and between the user and the controllers, that control the locked doors. Although traditional physical keys are easy to use, they have also their limitations. A slight change of user's rights is difficult to implement. The use of wireless devices may provide versatility in management of users' rights. Users' access can be limited precisely to certain locks and also the duration of rights can be controlled.

1.1 Goal and scope

A goal of this thesis is to study, what kind of advantages and limitations different authentication and authorization methods have, especially when using in an environment like a wireless access control system. This thesis will not study mathematical basis of cryptographic algorithms used in authentication methods, but things like introduction of new users to an authentication system or removing old users from it are considered. The suitability of Bluetooth wireless technology for the wireless technology of the access control system is also studied.

The main goal of this thesis is to design a general architecture of a wireless access control system using known authentication methods and wireless technologies. A demonstration system in accordance to this architecture is implemented and used to control regular electromechanical locks. Security and communication issues are researched and benefits and usability of the system will be evaluated.

1.2 Structure of the thesis

The first chapter introduces the reader to the topic and gives a little bit of background information. It also lists the goals, the scope and the structure of this thesis. In the second chapter issues concerning user authentication and authorization are discussed. Basic information about different authentication and authorization methods are introduced to the reader. Wireless technologies, mainly Bluetooth wireless technology, are presented for the reader in chapter three. A few alternatives for Bluetooth are introduced. This thesis includes also a practical application, which is designed using technologies studied in chapters two and three. This application, a wireless access control system, is described in the fourth chapter. Chapter five, the last part of this thesis covers author’s conclusion after this study.

2 AUTHENTICATION AND AUTHORIZATION

There are three main components in security - *authentication*, *authorization* and *encryption*. Each of these has its special function in a scheme of security. Authentication is used to verify, that a user or a device is really what he or it claims to be. Authorization determines, whether or not a user or a device is allowed to use certain service. Encryption protects the data and the communication parameters between and also in the communicating endpoints.

Depending on the needs of an application, each of those three components can be either enabled or disabled. But still, because authorization depends on the knowledge of the user's identity, authentication must be executed before authorization. There is no reason to even start checking one's authority, if there isn't reasonable proof of his authenticity. Encryption is also advantageous only when the endpoints have authenticated each other successfully.

This chapter focuses mainly on the first two parts of the security toolbox, authentication and authorization. Several ways to authenticate and authorize a user or a device is presented, explaining the advantages and disadvantages in them. Encryption is not handled especially, but some of the presented mechanisms can be used to enable encryption, too.

2.1 Elements in an authentication system

Authentication systems include five elements. An authentication system is created to authenticate a number of *persons*. There has to be a way to distinguish one person from the others. This way is called *distinguishing characteristic*. *A proprietor* is the entity, who administrates the authentication system. The mechanism, on which the proprietor relies when distinguishing a person from other persons, is called *an authentication mechanism*. When the authentication done by the authentication mechanism succeeds, *an access control mechanism* grants the person privileges to use the controlled service or device. [SMI2002]

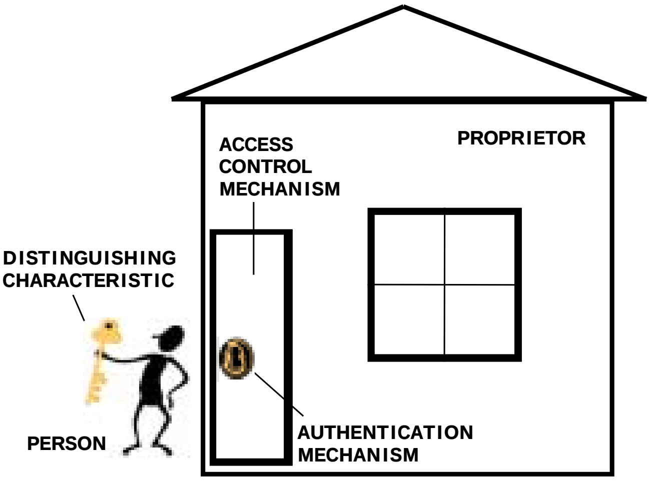


Figure 1 - Elements in an authentication system

The elements of an authentication system are depicted in Figure 1. The whole authentication system is based around a person, who needs to be authenticated and authorized. The person must have a distinguishing characteristic, which differentiates him from the others. In the figure, a key represents the distinguishing characteristic. A regular key is the most used distinguishing characteristic in authentication systems. In computer systems, the most used distinguishing characteristic is a password. Another possible characteristic is personal characteristic: for example a fingerprint, iris or voice recognition. The lock in the door is the authentication mechanism, which uses the distinguishing characteristic to authenticate and authorize entering persons. When a key is given to a user, he becomes authorized to enter the building. The door and the lock together represent the access control mechanism, which provides the access to a building after a successful authentication. The proprietor is the owner of the building, who controls the access to the building.

2.2 Identification and authentication mechanisms

Before accessing a service or a system, a user must be *identified* and *authenticated*. The identification is carried out by simply checking the username or any other user ID. After the identification follows the authentication [MUF1989]. In authentication, the authenticating party verifies, that the user really is who he's claiming to be. Methods of identity verifications can be divided into three or four categories, depending on whether or not the last two are combined. The four categories are [DAV1989]:

- Something that the person knows
- Something that the person has
- Something that the person is
- Something that the user does in his own way

A simple way to authenticate a user is to provide him a username and a password and check them when he's connecting to a system. The passwords usually are reusable, but variable one-time password authentication is possible, too. Tokens like magnetic cards and keys fall into the second category. Personal characteristics like the fingerprint are included in the category three. The last category includes person's involuntary actions like his signature.

2.2.1 Password authentication

An example of authentication based on the user's knowledge is password authentication. Passwords may be in a form of a password, a pass phrase, a PIN (personal identification number), etc., basically something that only the user knows.

Reusable passwords has been used as a security method in a remotely accessed time-sharing systems and computers several decades [MOR1979]. There have been multiple development steps in the security of password systems. In first phase, the system-wide password file included all the user names and their respective passwords in clear text format. This password file had to be heavily protected against being read or re-written by a malicious user or a software error. A first solution to this was to encrypt every password in the system and discard the password in a clear text format. When a user later logs on in to the system, the system encrypts this input and compares the result with the stored encrypted password. If these two passwords match, the login is accepted. The next step was to separate the user information and passwords to separate files, and make only the user information readable for all system programs and services. The password information was not only encrypted, but readable only by the administrating user or a group which was granted an access to it.

Variable o*ne-time passwords* differ from reusable passwords on the fact, that a new password is generated for every login attempt [DAV1989]. One-time passwords have been developed to counter replay attacks. Replay attacks are the kind of attacks, where user account information like user name and password has been captured and used afterwards by an attacker. Internet Engineering Task Force (IETF) has been studying a one-time password system in their One time password authentication working group. The specification, which is derived from Bellcore's S/KEY one-time password system [HAL1994], is presented as a Request for Comments document [HAL1996].

While one-time passwords may seem appropriate replacement for reusable passwords, they require either a pre-generated list of passwords to enter at next few logons or a token, which generates one-time passwords. Another way to verify user's identity using his knowledge is to require him to answer correctly to a *questionnaire* [DAV1989]. This questionnaire includes questions apparently irrelevant like questions about family relations or favorite things. This kind of information is easy to remember, but asking questions like this may involve a lengthy exchange between the user and the authenticator. This makes it inconvenient for several situations. Furthermore, this kind of information could be researched with a sufficient background study of the user by the intruder. Therefore it is not likely to be used in high security systems.

2.2.2 Authentication using tokens

Authentication using tokens fall into a category of "what user has". Incorporated with traditional password authentication, token-based authentication enhances the reliability of authentication. In order an authentication to succeed, one must know the right password and possess the right token. Physical keys or smart cards with magnetic stripes or chips are commonly used authentication tokens. [DAV1989]

Tokens may also be used alone without need for passwords or alternatively as password generators - these approaches take away much memorization. However, in this case the token must be kept extremely safe. Tokens may be protected against theft with a with a PIN (Personal Identification Number) code. PIN codes are usually quite short numerical values, which might seem too poorly designed. However, this kind of tokens incorporate a way to detect guessing attacks. It may delay the guesses or lock the token after a certain amount of trials. [SMI2002]

2.2.3 Authentication by personal characteristics

Authentication by personal characteristics use something that one is - that is unique personal information [SMI2002]. These unique features may be checked in form of a fingerprint or iris scanning or voice recognition. Although the sensor and measurement type used may vary a great deal, all of them use the same fundamental design. Unlike other authentication mechanisms, biometrics match is never 100% the same. Therefore authentication system must be configured to allow a slight imperfection in the match to still accept the authentication.

The fact, that a biometric value can't be changed, is a great advantage and also a disadvantage. If an attacker collects a victim's biometric reading by using false reader or stealing the binary representation during remote authentication, he can use this information in replay attacks. Since it might be hard to alter one's physical appearance, the usage of this method becomes insecure because of compromised identity. For this reason, biometrics should be used only in local authentication and never send binary representation over insecure channel to a remote host. [SMI2002]

2.2.4 Authentication by address

One of the simplest forms of authentication in networks is to check the location of the user's device. When using wireless network architecture with multiple access points, services may be offered to devices, which are physically in a presence of a certain access point. This provides pretty efficient way to offer services to the devices on a certain area. This also brings us to a point, whether the authentication should answer to question "who" instead of "where". Sometimes the where is enough, but sometimes we must know, whose device exactly is on the other side of a connection.

Another way is to authenticate devices with their hardware addresses. For example Institute of Electrical and Electronics Engineers (IEEE) issues a hardware address for every Ethernet interface card and Bluetooth device, and this address may be used to authenticate a device. When a person uses his personal device, also the person can be authenticated in this way. An address-based authentication is widely used non-cryptographic way to authenticate users. However, to be used in user authentication, it requires a device to perform a local authentication of its user in advance.

Although addresses can be built in the hardware, there still might be a chance that someone could falsify an address and pose as someone else. For example some development tools allow developers to choose the address of the device for development purposes. This enables also easier misuse of the posed address, if a malicious person gets hold of this kind of a development device. Therefore address-based authentication may not be adequate for every system.

2.2.5 Challenge response authentication

Challenge response is a general term for mechanisms, in which the person must answer to a mathematical challenge sent by an authentication mechanism with a correct response. The response may be constructed from the challenge in several ways. Naturally communicating participants must know the used construction method.

The response is usually generated with a one-way function from the challenge and user's base secret. The response is impossible to calculate without this secret. The base secret may be user's password or an authentication token. Challenge response has been implemented to many authentication tokens. Server's challenge must be entered into a token, which calculates the correct response. Using a challenge response mechanism, the base secret is not sent over the transmission path. This is an important property in challenge response, especially when its used in wireless environment.

Challenge response is also widely involved in public key authentication and authorization. The requesting server creates a random challenge and encrypts it with the public key of a user. The server then creates its own checksum from the challenge with a one-way function. The server sends the encrypted challenge to the user, who decrypts the challenge with his private key. In this case, the private key is the base secret for the user. The user creates a hash with a one-way function as the response for the challenge and sends it back to the server. The server compares these two hashes, the one it made and the other it received from the user. If the hashes are the same, the user has been authenticated successfully.

2.3 Key-based cryptography and authentication

Key based cryptography can be divided in symmetric cryptography and asymmetric or public key cryptography. In symmetric cryptography, both the encryption and the decryption of a message is done using the same secret key. Public key cryptography introduces a key pair, which includes a public key and a secret private key.

2.3.1 Symmetric cryptography

In symmetric cryptography enciphering and deciphering is done using the same key. This key must be exchanged between the parties before the actual communication. The algorithm can be one of the existing algorithms. In good cryptosystem the security is based on knowledge of the key - not of the algorithm [SCH1996].

Using this kind of symmetric cryptography one can be sure that the no one else than the possessors of the same key can read the message. Symmetric cryptography is somewhat analogous to a situation, where the knowledge of the combination of a lock provides access to the safe. In symmetric cryptography, the secret key represents the combination. In addition to the encryption of the message, this also takes care that the sender of a message is authenticated to be the possessor of the key. No one else than the owner of the key can "open the safe and put message in" - that is encrypt the message. Of course if the key has been stolen, communications encrypted with the key can't be considered secure anymore. [SCH1996]

A prerequisite for a symmetric cryptography is, that there can be a secure link between communicating devices, which is used to exchange the secret key. Therefore it may be not the most suitable approach to public services, where new communication pairs are introduced often. Besides, if one wants to use different key for every connection, the key collection may grow considerably big. A number of users n results a $(n^2 – n) / 2$ potential pairs who wish to communicate privately from other users [DIF1976].

2.3.2 Public key cryptography

Public key cryptography, also known as asymmetric cryptography, allows two participants to communicate with each other securely without prearrangements [MUF1989]. The concept of public key cryptosystem was invited by Diffie and Hellman in 1976. The mechanism of public key cryptography consist of a private deciphering key, a public enciphering key and general mechanisms for enciphering and deciphering. Enciphering key can be distributed publicly without fear of compromising the security of deciphering key [DIF1976].

Public key algorithms have four general properties. Notation k represents the key, E_k and D_k the encrypting and decrypting functions using the key k, respectively. M stands for the message.

1. For every k, E_k is the inverse of D_k, thus $D_k(E_k(M)) = M$.
2. E_k and D_k can be easily computed.
3. For almost every k, D_k or any algorithm equivalent of it is computationally infeasible to derive from E_k. Thus, revealing E_k doesn't mean revealing D_k.
4. It's feasible to calculate inverses E_k and D_k for every k.

Encryption and decryption consist of the general method and the key. Everyone can use the same general method, and the security lies on the security of the key. [DIF1976]

The usage of two keys is somewhat analogous to a locked mailbox with a reasonably safe structure. Anybody can put a letter into the mailbox via a slot in it and encrypt a digital message using a public key. Getting the mail out of the mailbox is generally pretty hard without a physical key for the mailbox - it's like decrypting an encrypted message without a private key. However, with a secret, that is a physical key to a mailbox or private key in a key pair, a letter or message can be acquired easily. Mathematically public key cryptography is based on a trapdoor one-way functions. A trapdoor one-way function is easy to compute in one direction, but hard to compute in another direction without the secret trapdoor. In public key cryptography the secret trapdoor is the private key. [SCH1996]

Public key cryptography can also be used to provide digital signatures. The signature is generated from the message with the sender's secret decryption key. The message and the signature is then sent to the recipient, who verifies the signature with the sender's public encryption key. The signature and the message can be also encrypted with the recipients public key for privacy. In that case, the recipient must first decrypt the message and the signature with his private key and then verifies the signature. [RIV1978]

Since the introduction of the concept of public key cryptography, several public key cryptography algorithms have been proposed. Only few of these are both secure and practical. One of the easiest algorithms to understand and implement is RSA, named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman. RSA relies on the difficult factoring of large numbers [RIV1978]. RSA is also the most popular and there are several implementations of it, both hardware and software ones. [SCH1996]

The private key should be stored in a safe place and it's recommended to encrypt it with a password or other secret known only by the owner of the key pair. The public key can and should be distributed to all other participants. There's no need to secure the channel where public key is transferred [MUF1989]. Therefore one can think of situations, where public key cryptography suits better than the symmetric cryptography. One situation like this is secure ad hoc networking, where a group of devices which are temporarily at the same place at the same time would like to establish a secure communication environment. All they need to do to establish a secure network is to exchange their public keys.

Disadvantage of the public key cryptography compared to the symmetric cryptography is, that encrypting is more complex and requires more computing power. Therefore many applications use so called hybrid cryptosystem, in which both of these two methods are combined. The actual message is encrypted with a random key using symmetric encryption algorithm and this key is further encrypted with the public key of the receiver of the message. This practice brings us both the possibility to exchange the keys and message via insecure channel and the effectiveness of symmetric encryption.

2.4 Authorization methods

After the user has been authenticated, he should be authorized to check, what resources he is allowed to access. While the authentication is straightforward - the authenticated person either is who he's claims to be or not - authorization and access control may be controlled by several rules. Usually a common security policy is set for the organization, and all the authorizations comply with it. In addition, some personalized rules may apply for personal data or configuration. The choice of the access control policy depends on the characteristics of the environment. [SAN1994]

Authorization can be done in several ways. The information can be checked from a database, certificates can be used to prove one's identity and rights or authorization can be done by a specialized service.

2.4.1 Access control lists

Administrator can keep a list of different resources and users, who can use each of the resources. This list can be located in a database or a file. The system which includes the data itself may include some kind of tags for each file or resource. Authorization may be configured to allow access depending on different information. It may be limited for certain users, groups or devices connecting from a certain subnet of the network. Modification of access control rights might be difficult, if centralized database isn't used.

2.4.2 Single sign-on

Retailers, banks and service providers provide services which can be used after logging in with username and password. Users may want to use the same or similar username and password at several different places to help memorize them, which may bring a problem. A malicious service provider may access user’s information on other service, if they happen to have the same or too similar passwords. The need for memorization and use of several logins can be eased with a single sign-on services. Single sign-on is a generalized term for services, which allow user to access several services after a single authentication. Authentication server provides user a proof of his identity, which can be passed to the servers as a replacement for his password. This proof of identity must be encrypted in the manner, that it can be passed to the user without a fear that the user can tamper it in any way. An example of this kind of service is the Microsoft .NET passport [MIC2004].

Kerberos is another well-known system based on the single sign-on idea. It was originally designed for open network computing environments in Project Athena at the Massachusetts Institute of Technology. The servers of a Kerberos system trust in Kerberos server with the identities of the other clients. Kerberos uses *tickets* to securerily pass the identity of a client to a server. The client gets his initial ticket from the Kerberos server by sending his identity to the server and then decrypting the response with his password. This initial ticket, a ticket-granting ticket, is then used with the ticket-granting server to obtain additional tickets for other servers. A Kerberos ticket is encrypted with the private key of a server and it includes the *name of the client*, the *name of the server*, the *address of the client*, a *timestamp*, a *lifetime* and a *random session key*. One ticket may be used to authenticate a client to the one server multiple times during the lifetime of the ticket. When using other servers, a new ticket for them must be obtained from the ticket-granting server. Kerberos software does this automatically, and the users interaction is only needed when getting the initial ticket. [STE1988] [MIL1988]

2.4.3 Certificate authorization

Certificates were originally designed as digitally signed bindings between a *subject* and a *public key*. There are several different certification methods. The most used ones are the X.509 and systems based on it [HOU2002] and PGP [NET2000]. X.509, which uses the hierarchical structure of certificate authorities to issue and verify certificates is called a *directory method*. PGP, which uses "web-of-trust" model is called a r*eferral method*. Both of these methods deal with certification in a different way. With PGP certificates, anyone can back up a claim, that a public key and the key’s owner go together, generating a above mentioned "web-of-trust" model. People need to specify, whose validation they trust. In X.509 validation must be done always by a certificate authority. However, PGP systems recognizes also X.509 certificates, so those can be used as well. [GER2000]

Abovementioned basic certificates which bind a subject and a key are called *ID certificates*. These certificates prove that according to their issuer, the subject of the certificate is holding the private key related to a public key in the certificate. The public key can be used to encrypt confidential information directed to the subject of a certificate. However, sometimes the identity of the owner of a public key not enough. Information about whether or not a subject is authorized or not to some access is needed. IETF Simple Public Key Infrastructure (SPKI) working group addresses this thing. A request for comments document by SPKI working group describes *Attribute* or *authorization certificates*, which can be used for mappings between *authorization* and *subject* or *authorization* and *key*, respectively [ELL1999b].

Since an attribute certificate binds the authorization and the subject together and an ID certificate binds the subject and the key together, attribute certificates can be combined with the ID certificates to complete a binding between authorization and the key. If these certificates are controlled by different issuers, both of them must be trusted with the authorization decision [ELL1999b]. In case of an authorization certificate the permission is mapped directly to a key, which is used as an ID for an individual. The ID mapping between the subject and the key can be left outside of the access control. [ELL1999a]

The X.509 version 3 specification permits extensions to be added to an X.509 certificate. In these extensions, authorization information can be carried. Using these extensions the certificate makes both the direct mapping between an authorization and a mapping between a subject and a key. Issuer of a certificate must be authority on both the subject naming and the authorization. SPKI certificates are another solution which offers also the mapping between an authorization and a key. [ELL1999b]

2.5 Public key infrastructure

Systems, which use public key cryptography and certificates are usually called public key certificate systems or public key infrastructure (PKI). In public key infrastructure, public key cryptography is used to encrypt and decrypt information and certificates are used to bind public keys to their owners. PKI is a collection of organizations, mechanisms, protocols and procedures which can be used to create, certify and distribute public keys. Widely used certificate standard in PKI is the X.509, specified by the International Telecommunication Union-Telecommunications Standardization Sector (ITU-T) and adapted for example by the Internet Engineering Task Force (IETF) in its own specifications [HOU2002]. X.509 based public key infrastructure is meant to be scalable to provide public keys for a small user group, an enterprise or even nationwide. [SMI2002]

2.5.1 X.509 framework

The X.509 framework is a standardized format for certificates. In a system which uses X.509 certificates a trusted authority issues a unique ID and a signed certificate for each user. A certificate includes user's ID and the public key. The fields of a X.509 certificate can be seen in Table 1. [SCH1996]

Table 1 – Fields of an X.509 certificate.

Version
Serial number
Algorithm identifier (Algorithm, parameters)
Issuer
Period of validity (Not before date, not after date)
Certificate holder's information
Certificate holder's public key
Signature

The v*ersion* number field identifies which version of X.509 standard applies to this certificate. The *serial number* is a unique number within the authority, which issued the certificate. The Algorithm, which is used to sign a certificate, is told in a*lgorithm identifier* field. A pair of dates in the *period of validity* field tells, when this certificate is valid and can be used to authorize its holder. After the validity field are *certificate holder's information* and the *certificate holder's public key* fields. Information field identifies the person, who is to be authorized with this certificate. The public key is used in cryptographic operations needed in the authentication and authorization. The last field is the signature of the certificate authority, which has issued the certificate. This signature binds the above information to the public key. [SCH1996]

X.509 version 3 introduced the use of extensions in X.509 certificates. The validity of a certificate may be limited by assigning user or action related constraints to it using the extensions. For example the network address of user's device may be inserted into a certificate and bind the certificate to that particular device. When the user's device connects to a service, the service checks the network address extension from a certificate and compares it with the address of the device, which sent the certificate. The extensions may also carry access control information, which can be used to allow or deny an access to a service.

2.5.2 Architecture of the public key certificate system

The public key certificate system consists of the five main entities, which are figured with their actions in the Figure 2:

- Certificate authority
- Registration authority
- Public key certificate holder
- Public key certificate client
- Certificate revocation lists

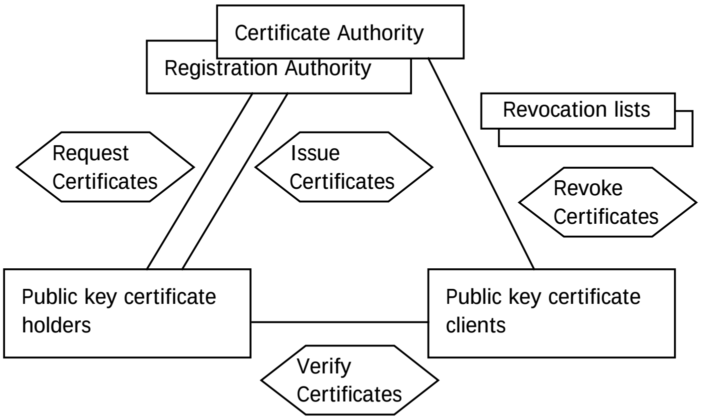


Figure 2 - Parts and functions of a public key certificate system

A certificate authority (CA) is the authority, which issues public key certificates (PKC). Because the CA is sitting at the top of the trust pyramid, its use must be heavily protected. The whole certificate system is depended on the security of this component. It's private key must be kept well safe from intruders. It's suggested that the computer that is hosting the CA should be kept offline all the time. The pass-phrase, which is used to encrypt the private key of the CA, must not be written anywhere and in extreme cases, it should be split between many administrators so that nobody can use it alone. [HON2000]

In a certificate system, there might be several certificate authorities placed in a pyramid structure. This structure is depicted in Figure 3. In the pyramid, a certificate authority has signed the certificate of the CA placed on the lower level. If a CA is trusted in public key infrastructure, every CA on a same branch below it, are also trusted. Likewise, if the secret key of a CA is compromised, every CA on the same branch below it must also be considered as compromised. If a CA is compromised, its public-private key pair must be re-generated, its certificate re-distributed to the lower branches and all the existing certificates signed by it must be voided.

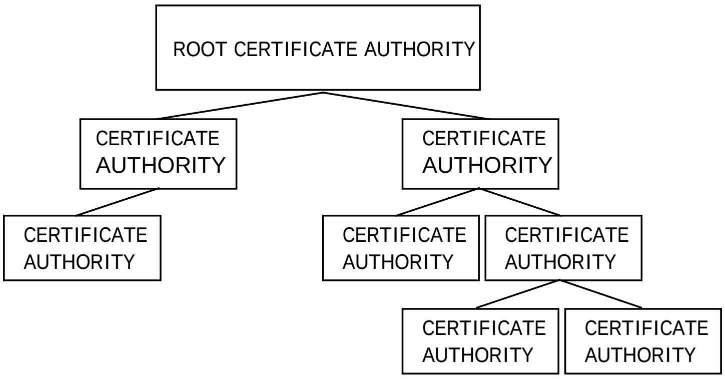


Figure 3 - A pyramid of several certificate authorities

A *registration authority* (RA) processes certificate requests. The RA may be tied in the CA or may be a separate entity. Unlike the CA, the registration authority should be accessible to users, who are requesting certificates [HON2000]. The actions performed by the registration authority include confirming certificate holders' identities, validating that the holders are entitled to have the requested values in their public key certificates and verifying that the holders are possessing the private key associated with the public key.

A *public key certificate holder* is the entity in certificate system, who is issued a certificate and who signs digital signatures and decrypts documents with his private key. To become a certificate holder, one must generate a key pair and request a certificate from the RA which forwards the request to the CA. In short, the whole system is designed to authenticate and authorize PKC holders.

Public key certificate clients validate PKC holders' digital signatures and their certificate paths from a known public key of a trusted CA. They use public keys to encrypt messages that are intented to PKC holders. The PKC clients are the points, where the authentication and authorization take place.

A public key certificate has a certain lifetime, after which it shouldn't have the ability to validate signed data. It's up to the clients, whether or not they accept expired certificates. Sometimes a certificate must be invalidated before the end of its lifetime. This may be necessary in the event that the CA, which signed the certificate, has been compromised, or the owner of the certificate can't no longer be trusted, for example because of an ended employment relationship. Invalidation is also necessary, if user's own private key has been compromised [NAO1998]. For this purpose, a public key certificate system has *certificate revocation lists* (CRL), which include all the revoked certificates. In addition to CRL's, there are another revocation ways, for example certificate revocation system or certificate revocation trees [NAO1998], but basically the idea is to transfer information about revoked certificates to the public key certificate client.

2.5.3 Functions of the public key certificate system

Different actions in a public key certificate system can be categorized into a five main functions:

- Registration
- Certification
- Initialization
- Key generation
- Revocation

Registration is the procedure, in which the subject makes itself known to the certificate authority and provides its common name and other attributes for its public key certificate. Registration may be done directly at CA or via RA. This information is also verified by some means, which are outside the scope of PKI. It's important to know, what is to be certified.

After the registration follows the *certification*, in which the CA issues a PKC to a subject or posts the certificate in a repository. After this, the subject is able to sign documents with his private key and send the certificate to the clients who can then validate the signature and the certificate and encrypt documents with the public keys found in the certificates.

In *initialization* the CA provides the client systems with its own public key or public key certificate. After this step the client systems can validate public key certificates issued by the same CA or a CA belonging to the same CA hierarchy.

Key generation in PKI may take place in user's device or by the CA. If the private and public keys are created in the CA, the private key must be distributed to the user's device using a secure link. If the key pair is generated in the user's device, the certificate request must be sent to CA to provide enough information for the CA to issue and send back the certificate. The certificate request assures the RA or CA that the user holds the private key, because the request can't be created without it.

A public key certificate is expected to be in use for its whole lifetime. However, a certificate must be revoked using the *revocation* procedure, if the private key of a key pair has been compromised or if there are some other reasons why a certificate should be invalidated. Private key may be compromised because someone breaks in the device from the network or steals the whole device in which a private key is stored. Revocation is done for example with Certificate revocation lists (CRL), which are published periodically or when necessary. CRL consist of a chain of the serial numbers of compromised certificates, with a date after which these certificates should not be considered as valid.

2.5.4 Risks in public key infrastructure

The public key infrastructure is widely used, although several threats can be found in it. Some of them are valid for many different cryptographic systems, some of them are targeted mainly to the PKI and some are present because of the human nature. [ELL2000]

Like in all systems based on key based cryptography, private key must be held well protected. Depending on the significance of the key, necessary physical and network security must be ensured. The client of a PKI may need to consider, what does he allow a certain certificate authority to authorize. Even if the certificate is indeed signed by a trusted CA, he may still want to reject this certificate for the certain purpose.

How does CA or RA identify the certificate holder, when he is requesting a certificate? Can the identity be checked face to face or does the holder request a certificate via an online service? In the first case, the identity may be checked from an ID card, but in latter there might not be a definite proof that the requestor of a certificate is the one whose information is listed in the certificate request.

The protection of a verifying computer must be also complete. In PKI, certificate verification is done with public keys, so there's no secrets to be protected. However, an attacker must not be allowed to add his own public key to the list. If the verifier trusts blindly the list of public keys stored on his device, he may accidentally verify also certificates signed by the private key of the attacker.

Subject name in a public key certificate must be composed wisely. The association with only a name is not likely useful in many situations. There must be other information which the verifier can use to uniquely connect the certificate with a certain person.

2.6 Summary

Authentication system includes five elements. *Proprietor* uses *authentication mechanism* to authenticate *persons* based on their *distinguishing characteristics*. After successful authentication, *access control mechanism* provides access to the provided service.

Passwords and PIN codes are widely used distinguishing characteristics. In local authentication passwords are suitable choices – easy to implement and correctly used quite efficient. However, when using them in remote authentication, the secret password should not be send over the transmission path, at least not in clear text format. Authentication tokens can be used alone or in addition to password authentication. A more sophisticated authentication mechanism is to use personal characteristics to authenticate a person. Because this kind of information is difficult, if not impossible, to change, biometric reading must not be send over the transmission path. If a malicious attacker steals a biometric reading, the whole authentication mechanism for that person becomes unusable.

There are two main groups in key based cryptography. In symmetric cryptography, the same key is used to encrypt and decrypt information. In asymmetric cryptography, public key is used to encrypt messages or verify digital signatures and private key is used to decrypt messages and create signatures. Public key can be made public without the fear that the private key is exposed. This enables secure communication without prearrangements.

Public key infrastructure is suitable selection to wireless access control system. X.509 version 3 public key certificates with extensions can be used to bind users public key both to this personal information and his access control rights. Users can be authenticated and authorized with a challenge response mechanism offline without connection to the authority.

3 BLUETOOTH AND OTHER SHORT-RANGE WIRELESS TECHNOLOGIES

Nowadays wireless technologies are widely used in telecommunications. Possibly the best known of these is the family of specifications by Institute of Electrical and Electronics Engineers (IEEE) called 802.11. These standards, known also as Wireless Fidelity or in short Wi-Fi, specify several wireless local area network technologies. These technologies are more and more emerging to challenge fixed networks as a technology for Local Area Networking (LAN). Wireless network technologies have several aims such as to cut down cabling costs and work in permanent or semi-permanent network environments and to allow freedom of movement of ad-hoc networking when using small network terminals like laptops or PDA devices

In this thesis, the Wi-Fi technologies are not studied, because with their longer range, higher bandwidth and higher power consumption their target of application is local area networking (LAN). Instead, Bluetooth and a few other short-range radio technologies, designed mainly for personal area networking (PAN), are inspected. They appear to suit better for the wireless access control system, an application presented in this thesis. The main technology studied is Bluetooth, a radio technology specified by Bluetooth Special Interests Group (SIG). IrDA is an infrared transfer specification designed by Infrared Data Association. Other radio technologies such as ZigBee and RFID are also presented briefly.

3.1 Bluetooth in general

Bluetooth is a short-range radio technology, which provides ad-hoc networking between different devices. It has been developed and specified by the Bluetooth SIG, which also qualifies products before they can to use Bluetooth as their wireless technology. This way Bluetooth SIG tries to ensure the interoperability between devices from different manufacturers.

Although necessary means are included in Bluetooth specification, Bluetooth isn't targeted to replace widely used 802.11 wireless networks as local area networking or Internet access technology. The range and bandwidth of 802.11 Wi-Fi technologies exceed the ones of Bluetooth clearly. Instead, Bluetooth is aimed to be a universal cable replacement technology. Bluetooth devices can be found in several product groups, and additionally there are cable replacement modules for existing systems.

3.1.1 Bluetooth network topology

In a connection between two Bluetooth devices one works as a master and another works as a slave. A Bluetooth *piconet* is a group of one master and up to seven active slaves connected to the master. In addition to active slaves, there can be more slaves in a *parked state*. Parked slaves are not active on the channel, but they are synchronized to the master of a piconet. A *scatternet* is a group of piconets whose coverage areas overlap and which have common devices. A Bluetooth device can be a master only in one piconet at a time, but it can be a slave in another piconets at the same time. Also a device can be a slave in many piconets concurrently. The conceptual picture of Bluetooth piconet and scatternet is presented in Figure 4.

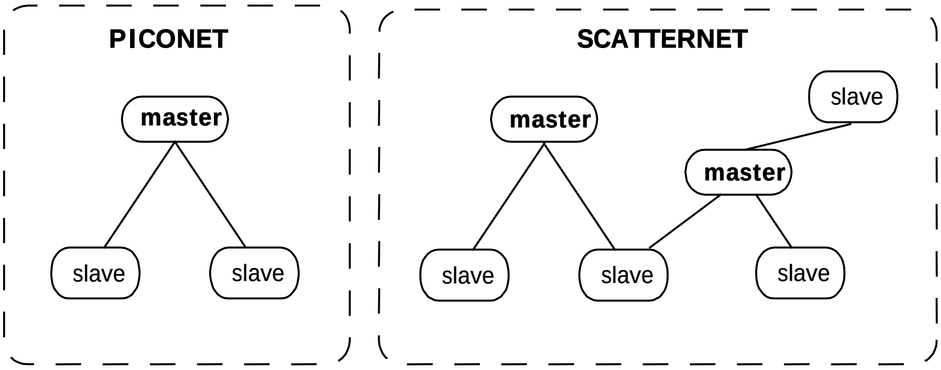


Figure 4 - Bluetooth piconet and scatternet

Still many current applications for Bluetooth use the simplest topology, a piconet with single-slave operation, which is actually a regular point-to-point connection. A single Bluetooth device connects to another device and exchanges information. Applications like wireless headset, file transfer and LAN access profile use simple point-to-point connection.

3.1.2 Bluetooth radio specification

Bluetooth operates in the 2.4GHz band for Industrial, Scientific and Medical (ISM) use. The Bluetooth specification defines requirements for Bluetooth transceivers working on this unlicensed ISM band. The band is limited to frequencies 2400 - 2483.5 MHz. This includes also 2 MHz lower guard band and 3.5 MHz upper guard band. Bluetooth devices use frequency hopping scheme which uses the whole band. This results 79 radio frequency channels. at frequencies

$$f = 2402 + k \ MHz, k = 0,...,78$$

Bluetooth specification defines three power classes. The lowest power classes has maximum output power of 1 milliwatt or 0 dBm. This is the maximum transmit power in the ISM band without spread spectrum operation, permitted by the

Federal Communications Commission (FCC). Since Bluetooth uses frequency hopping, it's able to operate at up to 20 dBm, allowing ranges up to 100 meters. The range and maximum power consumption for each one of the classes are listed in Table 2. The ranges 100, 10 and 1 meters are defined to Bluetooth Power Classes 1, 2 and 3, respectively. These are just nominal ranges, an actual range depends on environmental factors. In an ideal environment the range may be few times bigger than the nominal range, and vice versa, in an environment with a lot of interference the range could be just a fraction of the nominal range. Still, the nominal ranges give us a fair view of suitability for different applications. [BLU2001a]

Table 2 – Bluetooth power classes

Power class	**Maximum power *[1]**	**Range**	**Power Control *[2]**
Class 1	100 mW (20 dBm)	100 meters	M: +4 dBm to 20 dBm O: -30 dBm to 4 dBm
Class 2	2,5 mW (4 dBm)	10 meters	O: -30 dBm to 4 dBm
Class 3	1 mW (0 dBm)	1 meter	O: -30 dBm to 4 dBm

[1] dBm = decibel referenced to one milliwatt (mW)
[2] M = mandatory, O = optional

The Bluetooth specification defines mandatory power control to devices which are working in Power class 1. In Power classes 2 and 3 power control is optional. Power control is operated by receiver which monitors the Received Signal Strength Indication (RSSI) and sends Link Manager Protocol (LMP) commands to the transmitter, if the transmit power is higher than strictly necessary or too low. Transmitter then reduces or increases the transmit power, which is necessary at the moment. [BRA2001]

3.1.3 Bluetooth connection establishment

To establish Bluetooth connection between devices, the Bluetooth device address of another device must be known. This could be inquired using the *Bluetooth device discovery* procedure. However, this inquiry phase takes several seconds to complete, and it's not very suitable in some applications. The Bluetooth specification [BLU2001a] defines a time of 10.24 seconds, which should guarantee responses from every device in an error-free environment. If the users should do this every time they want to unlock a door, it causes big delays in operation. But then again, creating the actual connection, when a Bluetooth device address is known, takes much less time. The Bluetooth specification [BLU2001a] defines a maximum time of 2.56 seconds for this. The typical time taken in this *paging* step is usually shorter, usually less than two seconds. Therefore preprogramming addresses to the device could be a better approach for several applications.

Both the discoverability and the connectability can be either enabled or disabled. If discoverability is disabled, the device doesn't answer to device discovery inquiries sent by other devices. This helps the device stay hidden from other devices. However, if the device is in connectable mode while nondiscoverable, the connection can be established to it, if the connecting party knows the Bluetooth device address.

3.1.4 Bluetooth protocols

Bluetooth specification includes protocols from the lowest hardware and firmware layers to the levels in Bluetooth software, which are located just below the application layer. Bluetooth consists of the following general protocols:

- Link Manager Protocol
- Logical Link Control and Adaptation Protocol
- Service Discovery Protocol
- Radio Frequency Communication

Link Manager Protocol (LMP) is used to create and control links between Bluetooth devices. Link manager is also responsible for filtering incoming packets and stopping all unsuitable packets while propagating applicable packets to upper layers

Logical Link Control and Adaptation Protocol (L2CAP) is layered over Baseband layer and resides with in data link layer with aforementioned link manager protocol. L2CAP provides upper layers with connectionless and connection-oriented data services. L2CAP handles data multiplexing, segmentation and reassembly operations and group abstractions.

Service Discovery Protocol (SDP) is designed to provide means for searching and browsing services on other devices and offering services on own device to others. Service discovery responses include information about the types of services as well as information how to access the services.

Radio Frequency Communications (RFCOMM) protocol provides serial port emulation over L2CAP protocol. Several Bluetooth usage profiles are specified to use serial port emulation enabled by the RFCOMM, and therefore RFCOMM is widely supported in Bluetooth software stacks. Using RFCOMM most of the applications, which use wired serial port transfers, can be altered to use Bluetooth technology.

3.1.5 Service discovery

Service discovery is needed when a networked device needs to find services in a nearby network. This network may be a fixed or an ad-hoc wireless network. The service discovery makes it possible to have zero configuration networks, where user doesn't need to configure the network to reach services [KAM2002]. In Bluetooth, the service discovery is done with Bluetooth Service Discovery Protocol (SDP). SDP offers means to search or browse services or list own services to others. Having this kind of a service discovery method is very important because of a non-existent infrastructure for the service discovery. Directory services with semi-permanent service lists are not the suitable solution to Bluetooth service discovery, because the devices, even the service provider, can move in and out of the network. [KAM2002]

Bluetooth service discovery may be short-circuited with help of the Bluetooth device discovery procedure. The low-level Frequency Hopping Synchronization (FHS) packet is exchanged between devices during the inquiry process, and this packet has a Class of Device (CoD) value. The CoD is a 24-bit value, which has three parts: Major Device Class, Minor Device Class and Major Service Class. The application may choose only those devices that have the appropriate device or service class defined in this CoD value. This makes the service discovery much more efficient, because the device doesn't need to connect to all the neighboring devices for complete service discovery. Bluetooth SIG controls the values for these three classes. [BLU2001a] [KAM2002]

3.2 Bluetooth Profiles

A thing worth mentioning in Bluetooth is the use of profiles. When the standard Bluetooth specification defines clearly, what the Bluetooth technology is, the profiles provide straightforward and complete instructions, how to use the technology in several real world situations or usage models. [MOR2002]

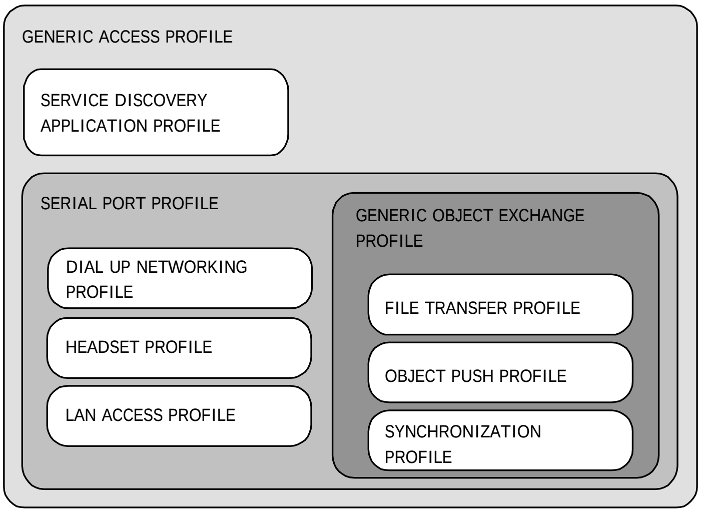


Figure 5 – Main Bluetooth profiles

Bluetooth profiles are divided in general profiles, which define the general principles and operation modes, and more specific ones, which define exact operations in certain situations.

As seen in Figure 5, *Generic Access Profile* (GAP) applies to all the usage models. It defines the procedures related to the discovery, link management and the security levels. The GAP specifies three *discoverability* modes: *Non-discoverable, limited discoverable* and *generic discoverable*. Two *connectability* modes are specified: *non-connectable* and *connectable*. *Pairing* is divided to *non-pairable* and *pairable*. The GAP also lists several procedures related to device discovery, which are called idle mode procedures. These consist of *general* *inquiry*, *limited inquiry*, *name discovery*, *device discovery* and *bonding* modes. Security modes were already presented in chapter 3.3.4. These various modes, specified in the GAP are addressed in each Bluetooth profile with their implementation requirements: mandatory, optional, conditional support, excluded and not applicable. [MOR2002]

In addition to the GAP, two other generic profiles are specified: Service Discovery Application Profile (SDAP) and Serial Port Profile (SPP). SDAP specifies the use of Service Discovery Protocol and supports browsing of the services on a device and searching for services on other devices by service class or service attributes. Serial Port Profile defines the requirements for setting up emulated serial port connection using RFCOMM. [BLU2001b]

The more specific profiles define usage scenarios. These set their own requirements for the GAP, SDAP and SPP procedures. The *Dial-up networking*, *Local area network access* and *Personal area networking* profiles provide ways to use network access in different situations. Also a few profiles exist for exchanging files and objects like calendar and phone book information. In addition to these, several miscellaneous profiles are specified for different communication situations. [BLU2001b][MOR2002]

3.3 Bluetooth security

Bluetooth has security architecture, which is quite suitable for personal use. But using the security architecture in a wider environment brings some problems. Bluetooth security uses the PIN code as a shared secret and semi-permanent link keys as authenticating keys. In the wireless access control system, this may become a problem. Only the users of the system and nobody but them should know the PIN code, which may become difficult when users come and go. This is the main reason, why Bluetooth security is not suitable for the Wireless access control system. In the Wireless access control system, the security is left completely to the application layer where public key cryptography provides authentication mechanisms.

3.3.1 The keys used in Bluetooth security

There are four types of 128-bit *link keys* defined in Bluetooth specification. *Unit key*, K_a, is created at the installation or first use of Bluetooth device. A *Combination key*, K_{ab}, is derived from two units A and B. Therefore this key is different for each pair of devices. The *Master key*, K_{master}, is used when transferring secure information to several devices at once. The Initialization key, K_{init}, is used in initialization process to protect the initialization parameters. [KAM2002]

3.3.2 Pairing

Bluetooth security is enforced using permanent and temporary link keys and user's input. *Pairing* is the procedure invoked when a link key hasn't been created for the connection between devices. Connecting devices are called the *verifier* and the *claimant*, the verifier being the one who's trying to verify the claimant's authenticity. The verifier calculates a temporary Initialization key, K_{init}, from a PIN code, a random number and a Bluetooth device address. The random number is transferred to the claimant, which calculates the same initialization key using the received random number, same PIN code and the same Bluetooth device address. K_{init} can be used then to encode the semi-permanent link key (K_a or K_b) while distributing it to the other device. Either the verifier's key K_a or the claimant's key K_b or a combination of them, K_{ab}, may be used as a semi-permanent link key. When the other device stores the agreed key, pairing procedure is over. [KAM2002]

3.3.3 Authentication, authorization and encryption

After the pairing is finished, verifier sends then a randomly generated challenge to the claimant, which responds with a response calculated using the link key. The verifier does the same calculations and compares the results. If the same PIN code has been entered on both sides, the results match and the *authentication* is successful. The whole process of pairing, authenticating, link key creation and storage is called *bonding*. [KAM2002]

Authorization requires the authentication to be successfully completed. Authorization may be done by asking the user through a man-machine interface or by searching for the device in the trusted devices list, which includes a list of devices that the user has previously marked as *trusted*.

Bluetooth *encryption* is enforced with Bluetooth *encryption key*. It's derived from the current link key every time the encryption is wanted. The encryption key can be between 8 and 128 bits long. Separating authentication and encryption keys weaker encryption can be used and still apply stronger authentication.

Encryption is used to prevent the transmitted data to be so easily understood by a malicious party. Transmitted data is encoded using an encryption key generated from the stored link key. On the receiving end, the same key is used to decode the data. [KAM2002]

3.3.4 Bluetooth security modes

Bluetooth Generic Access Profile has specified three security modes. Mode 1 is actually not a security mode at all - because it has no security whatsoever. Mode 2 enforces security, when a higher layer protocol or service is requested or used. Mode 3 invokes security mechanisms already when another device is connecting to the device. [KAM2002]

Bluetooth Security Mode 1

Bluetooth has a mode for non-secure connections, and this has been labeled Bluetooth Security Mode 1. Of course, this implies only, that the connection is non-secure, as far as Bluetooth stack is concerned. The service itself may request its own authentication, authorization or encryption methods before service is granted.

Bluetooth Security Mode 2

Bluetooth Security Mode 2 is the most common and useful of Bluetooth security modes. When a creation of peer-to-peer connection is attempted to L2CAP or RFCOMM layers, Bluetooth stack informs the *security manager* which carries out pre-defined security measures. The security manager can be configured to do the following things upon a connection attempt. [KAM2002]

- Make no action and allow the connection to be established
- Authenticate and authorize the connecting device or user
- Request encryption between the devices before connection establishment

These security choices may be configured for each service independently. For example a connection attempt to Dial-up networking service on a mobile phone could trigger authentication and authorization, meanwhile incoming Object Push can be accepted without checks.

Bluetooth Security Mode 3

The Bluetooth Security Mode 3 is the strictest of these three modes. When a device is in this security mode, the security measures are carried out immediately after any radio connection, incoming or outgoing. The first phase for Security mode 3 is authentication, and after successful authentication, encryption may be applied to the data link.

3.4 Other short-range technologies

3.4.1 Infrared standard by Infrared data Association (IrDA)

Infrared standard by the Infrared Data Association (IrDA) is a short-range data transfer technology, which uses infrared as a physical network layer. The fact, that IrDA needs a visual communication to transfer data is both an advantage and a disadvantage compared to a radio technology like Bluetooth, which uses radio network as a physical layer. The direction and range of IrDA data transfer is far more limited than in Bluetooth, which makes eavesdropping, if it can be said about light, more difficult. That makes also reaching of services more difficult.

IrDA standards include physical signaling layer, link access, link management as a mandatory features. Optional features include Tiny TP for flow control, IrCOMM providing serial port emulation, IrOBEX for object exchange services. IrDA Lite provides methods of reducing the size of IrDA code while maintaining compatibility. IrTran-P specifies image exchange protocol. IrMC specifies the way, that mobile telephony devices can exchange information like calendar and phone book. IrLAN describes a protocol used to support IR access to local area networks. [IRD2003]

3.4.2 Radio Frequency Identification (RFID)

Radio frequency identification is a technology based on three components: An antenna or a coil, a transceiver and a transponder (a radio frequency tag) containing unique information. The antenna and the transceiver form a reader device, which is used to read the information from the tags. Tags include some kind of an antenna also. The constant transmissions of the reader activates RFID tags coming into the range of the reader, and the information inside the tag is transferred to the reader. After decoding the information, the reader sends it further to its host system for processing. [AIM2003]

The tags may be either active or passive. Passive tags operate without separate power source, because they obtain all the necessary power from the electromagnetic waves sent by the reader, whereas active ones need a battery or a similar source of power. Passive tags have a virtually unlimited operating lifetime, but this advantage comes with the disadvantage of shorter operating range and the need for higher-powered readers. Read-only tags are typically passive and programmed with unique data from 32 up to 128 bits. Programmed data can't be modified. [AIM2003]

RFID tags can be considered as a radio frequency equivalent to bar codes. Bar codes have their application areas, where the most cost-effective identification is needed. RFID support is growing on application areas, where optical technologies are difficult to use.

3.4.3 ZigBee

Zigbee is a wireless radio technology designed by the ZigBee Alliance to address the need for a low cost, standards based solution that supports low data rates and low power consumption as well as security. Requirements like this are essential for sensors or control devices, which don’t need high bandwidth but need low latency and a long battery life. ZigBee has been designed for several types of traffic. Typical traffic types for ZigBee device are *periodic data* used in sensors, *intermittent data*, for example light switches and *repetitive low latency data* used for example in computer peripherals. [KIN2003]

Abovementioned traffic types, power consumption limits and other requirements set challenges for the physical and media access layers. The ZigBee Alliance has adopted the physical layer (PHY), the media access control layer (MAC) and a part of the data link layer from the IEEE. Those have been specified in IEEE’s 802.15 Task Group 4. Protocol stacks on top of the data link layer are controlled by the ZigBee Alliance. Zigbee uses two bands as a PHY layer. The 868 MHz band is in use in Europe, whereas for example in North America, Australia the substitutive band is at 915 MHz. 2,4 GHz band, however is recognized as a global band, because it’s accepted in almost all the countries. IEEE 802.15.4 MAC layer is flexible enough for the three traffic types. Periodic transfer can be handled with beaconing system, where the sensor wakes up for the beacon, checks if there's messages and goes back to sleep. For intermittent data transfer the device can be in disconnected state, and it only attaches to the network when it needs to communicate. Repetitive low latency applications can use guaranteed time slots option (GTS), which is a quality of service method for operation without contention and latency. [KIN2003] [ZIG2002]

3.5 Summary

Bluetooth wireless technology is the most popular short-range technology in handheld devices. It's mainly used in mobile phones to exchange phone book or calendar information and different kind of media files between two phones or a phone and a computer or in mobile headsets. However, there's no reason not to try using Bluetooth in any other application. In March 2004, there were nearly 500 Bluetooth enabled products available in more than 15 different product areas. Furthermore, some of these products are Bluetooth adapters which can be used to make number of other devices Bluetooth enabled. [BLU2004]

Along with Bluetooth, Infrared-based IrDA is another very common technology in handheld devices. When comparing the usage and applications of these technologies, Bluetooth can be seen as a successor of IrDA in many instances. They have several similarities, like the use of Object Exchange Protocol (OBEX). IrDA, however, needs the line of sight between communicating devices. This may complicate the deployment of devices compared to the Bluetooth based solution. Zigbee is a promising technology, whose biggest advantages are the low power and quick transitions between different working modes. These kind of properties are important for example in sensors and control devices. If the technology keeps up its promises, it may be one of the most common short-range wireless technologies with Bluetooth.

After considering Bluetooth application requirements and surveying the present day market of handheld devices, Bluetooth wireless technology has been selected for the wireless technology in the Wireless access control system, the application designed and presented in the next chapter of this thesis. RFID is highly efficient way to pass simple identification information, but in this access control system, intended authentication and authorization methods require data processing properties from the key device also. Therefore RFID based solution is left outside the architecture.

4 WIRELESS ACCESS CONTROL SYSTEM

People carry their mobile phones with them practically all the time. Therefore the mobile phone with a wireless short-range connectivity would be a suitable platform to install applications, which could be used to access daily services. Unlocking and controlling doors is one of those services. An architecture designed by the author of such access control system is presented in this chapter.

The wireless access control system enables users to unlock doors using their handheld Bluetooth devices. Bluetooth connection is made to an access controller, which controls the electromechanical locks and two way authentication is done between the entities. Bluetooth was selected as a wireless technology because of its availability and also because of the author's background knowledge of it. Widely known authentication and authorization methods are used in user authentication. Every user is issued a public-private key pair. The public key is bound to their personal data using public key certificates, digitally signed by the administrator of the system. General challenge response authentication mechanism is used to verify the possession of the private key. The certification is done also via Bluetooth technology. The architecture is designed so, that the secret of a user, that is the private key, is never sent over the Bluetooth connection. Furthermore, it can be encrypted with a password when stored.

4.1 Related Work

There are several different access control systems based on proximate technologies. A small token, which is read using a reader device, acts as a key device in these systems. The token may be read from a magnetic stripe or using a proximity technology such as Wiegand pulse [DLU1998]. The result of the reading is transferred to the database, where the rights for that particular token is checked. The results of the authorization is then transferred back to the door, which remains either locked or unlocked, depending on the result of the authorization. There are also Bluetooth modules available which can be used to expand existing access control systems to the places, where installing wired readers is difficult. [INT2003]

4.2 General requirements for a Bluetooth application

Before designing and implementing an application which is based on Bluetooth wireless technology, some requirements must be considered. There are six requirements for a Bluetooth based application. [KAM2002]

1. The application adds usability.
2. Interference and latency don't affect primary function of the application.
3. Bluetooth connection time overhead must be tolerated.
4. Bluetooth bandwidth is limited, so must be the need for bandwidth in the application
5. The components of a Bluetooth based application must be equipped with power supplies compatible with Bluetooth specification.
6. The range of a Bluetooth radio transmitters must be adequate for the application.

How these requirements are met in the wireless access control system? Requirements one, three and five from the abovementioned list are the biggest issues in the Wireless access control system. Does it add usability compared with existing access control systems? How is the delay of Bluetooth device discovery and connection handled between personal trusted device and access controller which is handling the lock? One reason for building a wireless access control system is likely to avoid difficult cabling between different elements. Power supply will then definitely become an issue to be solved.

There can be many opinions about usability. Some think that regular keys are easy to use, and the introduction of new technologies is difficult and problematic. On the other hand, binding the key functionality to a Bluetooth enabled handheld device cuts down the amount of things you have to carry in a pocket. Many people carry a suitable device, a mobile phone, anyway. One or two keys is not a problem, but a janitor or a security person may need several. Still a few mobile phone models have Bluetooth functionality, but it’s becoming more and more common all the time. When a portable Bluetooth device is used as a key, usability depends much on the implementation of opening mechanism. Does the user need to press different buttons for different doors or do all the doors open pressing the same button? An optimal functionality from an usability point of view would be, that the correct door opens when user walks nearby. There are still some things like the slow device discovery in Bluetooth that prevent or at least make this last possibility more difficult.

Interference and latency will affect the operation the most, if the application must perform in a most reliable way. Communications that depend on a radio link, such as Bluetooth, have certain characteristics. A connection can’t be ensured every time, because interferences caused by neighboring devices and structures will make the signal weaker. Therefore, Bluetooth should not be used in applications in which the success of a connection is imperative. In an access control system a failure in connection may take a few extra seconds in a user’s daily routine, but it’s not that fatal.

There are two delays in setting up a Bluetooth link. Bluetooth device must first discover other devices in the neighborhood. After that, the connection establishment itself, including encryption and authentication, causes another delay. The first of these, the device discovery takes usually more time than the connection establishment. Application should prevent this delay from happening or at least diminish its effect somehow. In access control application Bluetooth device discovery can be avoided, if the Bluetooth device addresses of access controllers are stored in the user's terminal. The addresses can be downloaded to user's terminal when creating a certificate for a user.

A theoretical maximum transfer speed of an asynchronous Bluetooth link is 723.2 kbps. After considering necessary headers and possible error correction, the actual data rate left for the application is even lower. This may be insufficient for some applications, but for access control system it's more than enough. Packets which are sent during unlocking requests are between one and two kilobytes, and transferring them takes only fractions of a second.

One possible problem when creating a wireless Bluetooth terminal is the power consumption. With wired terminals power supply is rarely a problem, because power cables are usually installed alongside network cables. Power consumption and the range of a radio link are bound to each other. The Bluetooth specification defines three different power classes, which were described in Table 2.

In wireless access control system, the most suitable power class is class 2 with a nominal range of 10 meters. Ten meters is enough for opening a lock. With power class 3 devices and one meter range, users have to walk right to the door and open it there. With a bit more powerful device, the user can send the opening request from a few meters away and walk to door while access control terminal processes the request. Class 1 devices consume a lot more power, and in an access control application, too long range introduces also insecurity. User may open unintentionally a door, which is located far away from the intended door.

4.3 Architecture of the Wireless access control system

The wireless access control system includes three logical entities - an *administration point*, a *personal trusted device* (PTD) and an *access controller*. These parts and their functions are depicted in the Figure 6. The Administration point defines the computer system, from which the authorization and authentication information is granted to users in form of certificates. The administration point uses a database to store information. The personal trusted device is a handheld device, which a user carries with him and uses to unlock the doors. The access controllers are connected to electromechanical locks, and these controllers authenticate and authorize the users.

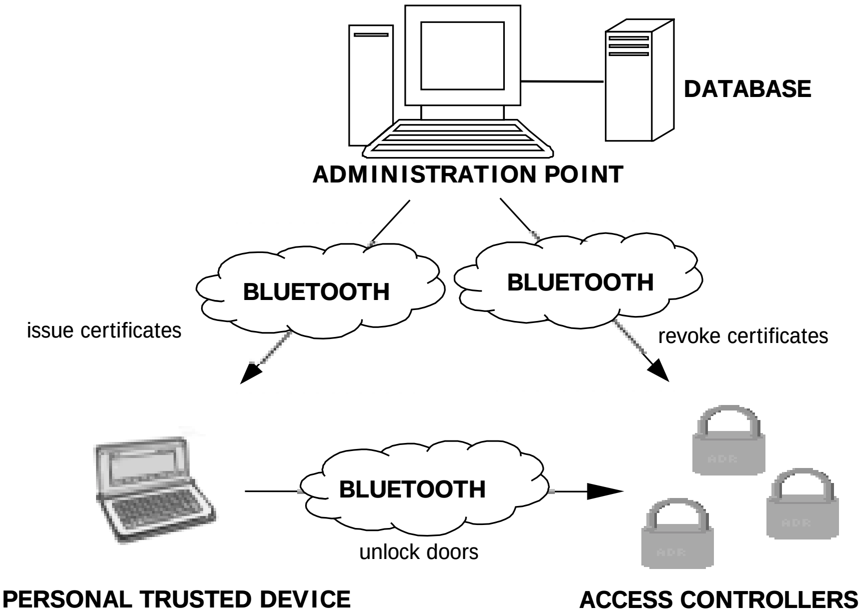


Figure 6 - Parts and functions of the Wireless access control system

Elements of an authentication system were explained in chapter 2.1. The mapping of the elements of an authentication system and the components of the Wireless access control system is provided in Table 3. The authenticated *persons* are naturally the persons who need to unlock the doors. The locked doors are located within a building, whose owner or at least administrator is the *proprietor* of the authentication system. Persons are supposedly bound to the proprietor via employment or any other relationship. A private-public key pair is created for each user. The public key is included in user's certificate and these together form the *distinguishing characteristic*. The software in users' personal trusted devices and in access controllers form the *authentication mechanism*. Access controllers and locked doors are the *access control mechanism*, which provide access upon a succeeded authentication and authorization by unlocking a door.

Table 3 - Authentication elements in Wireless access control system

Authentication element	Wireless Access control system
Person	The user who needs to unlock doors
Distinguishing characteristic	The public key in a certificate
Proprietor	The organization owning the building
Authentication mechanism	Certificate verification and challenge response authentication software
Access control mechanism	Mechanism which unlocks the door

4.3.1 Administration point

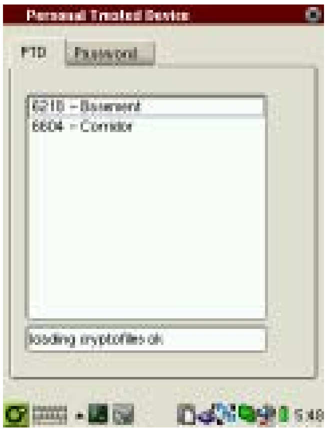
The administration point is an entity which includes a terminal for the administrator and a database. A database is used to store the information about users, their personal trusted devices and locks in the system. The administration point has Bluetooth adapter, which is used to exchange information with users' devices while upgrading certificate information.

The administration point and its operator act as a certificate authority and a registration authority in a certificate system hierarchy for the access control system. It issues the certificates for the users after it has verified their identity. The general hierarchy for the public key certificate system was presented in chapter 2.5.2.

The administration point manages also all the locks and the access controllers of the system. It stores the Bluetooth addresses and other information about the access controllers to its database. When lock information is needed, for example when issuing certificate to a user and sending the list of locks to the user's device, administration point fetches the information from database and uploads extensive markup language (XML) coded file into the user's device. The format of this list of locks is presented in the Figure 10 in chapter 4.6.2.

4.3.2 Personal trusted device

The personal trusted device (PTD) is the device, which acts as a user's key device in this system. It's a handheld Bluetooth device, which becomes personal trusted device when a public-private key pair is generated and authentication and authorization information is transferred to it. The PTD can be for example personal digital assistant (PDA), a cellular phone featuring Bluetooth or any other device capable of handling and transferring authentication information.



6210 – Basement
6604 – Corridor

loading cryptofiles ok

Figure 7 - Screenshot of a personal trusted device

In Figure 7, an explanatory user interface of the personal trusted device application is shown. It's running on a PDA device and Open Palmtop Integrated Environment (Opie) graphical user environment [OPI2004]. The desired lock can be selected from the list of locks presented on the main screen. Under the list of locks is the status field, which tells the user the current status of the program and the unlocking procedure. Password tab is needed when the password for the private key is input. This is the default operation when the program is started. When password tab is selected, the virtual keyboard pops up. When the password is entered, the main screen becomes active again and the status field informs the user about the decryption of the private key.

Cryptographic requirements

Because authentication and authorization of a person is done using public key certificates and public key cryptography, PTD functionality requires asymmetric cryptography functions and support for the X.509 public key certificate system. The device must allow user to generate and store a private-public key pair in a personal trusted device. The stored private key is encrypted with a password or PIN code known only by the user.

Bluetooth requirements

In this architecture, Bluetooth has been chosen as a transfer technology. Therefore the personal trusted device must be able to establish Bluetooth connection to the administration point and the access controllers. L2CAP protocol is used to transfer certificates and unlock requests and responses. L2CAP is the basic data transfer protocol in Bluetooth and is implemented in every Bluetooth device and stack.

General requirements

The PTD functionality requires a user interface from the device. User input is needed in several phases.

- Creating and handling a key pair
- Inputting personal information
- Requesting certificate updates from the administration point
- Selecting a lock to be unlocked

These operations require a display to show current settings and information and a input devices to select desired operation and to enter information. For displaying information a display of a PDA or a modern mobile phone is adequate. The personal information is input only when requesting a certificate, so its fluency is not a big issue either. The most important issue concerning the handling of the PTD is the way, how the select to lock to be unlocked, because in this architecture, this must be done every time a lock needs to be unlocked. User initiated unlock process has been selected to avoid time taking device diescovery. Therefore a dedicated buttons for selecting a lock and launching the unlock process is recommended.

4.3.3 Access controller

The access controller has a Bluetooth wireless connection and a connection to electromechanical locks. The choice of connection between the access controller and a lock is left outside the scope of this thesis, and it can be done in any possible way. In the test configuration the locks are attached to the access controller via parallel port. A picture of this system can be found in Appendix 1. Eight electromechanical locks can be controlled via relays attached to the parallel port of a computer acting as an access controller. Other mechanisms and electronics can be used to increase the amount of controlled locks.

The access controller must be able to verify certificates sent by personal trusted devices. A digital signature of the administration point must be checked when a unlocking request arrives. If the certificate in the request is valid, the access controller must generate an encrypted challenge using the public key of the PTD owner. When the response, a hashed form of the decrypted challenge, comes back from the PTD, the access controller uses the same hash algorithm to encrypt its challenge. The arrived response and the hashed challenge is then compared.

Bluetooth requirements for the access controller are similar to the other parts of the access control system. It listens for connections on L2CAP protocol layer, and when a connection is established, it must exchange the information needed in unlocking request and challenge response mechanism.

4.4 Authentication and authorization in Wireless access control system

The authentication and authorization of personal trusted device include 11 separate phases. The first four phases cover the assigning and issuing of new certificates. This is done when a new person becomes a user of the system, or when an existing certificate must be renewed. The rest of the phases belong to the actual unlocking. All the phases concerning authentication and authorization are depicted in Figure 8.

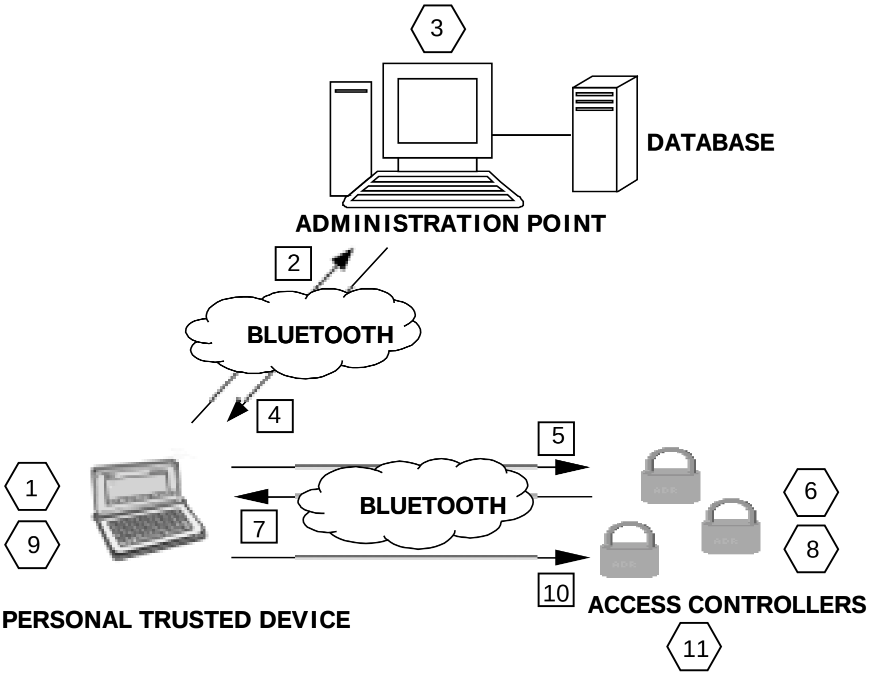


Figure 8 - Authentication and authorization phases

In phase 1, a public-private key pair is generated in the personal trusted device. Using the private key a certificate request is generated and sent to the administration point (phase 2). The owner of the personal trusted device, that is a person who should be authenticated, is then identified by an administrator (phase 3). Identification method is out of the scope of this thesis, but it could be done by checking the personal identification card of the person or any other proof of his identification. The administrator then chooses all the doors this person is allowed to unlock and generates the certificate for him with the selected rights. The certificate is sent to the PTD (phase 4). During these phases, administrator binds the user's identification card with the key pair, that is used to generate the certificate request.

In phase 5, the user sends a unlock request with his PTD. Unlock request includes his certificate and the lock ID signed with his private key. The access controller verifies the certificate with the CA certificate of the administration point (phase 6). The user's certificate includes his public key, and the access controller extracts it from the message to encrypt a random challenge. The encrypted challenge is sent to the PTD (phase 7). Immediately after this, the access controller creates a hash from the challenge (8). After the user's PTD has decrypted the challenge with its private key (9) and responded with a hashed response (10), the challenge and the response are compared (11). If they match, the access is granted and the access controller signals the electromechanical lock. As long as the certificate is valid, there's no need to repeat phases 1-4, just the phases 5-11.

When the certificate becomes invalid either because its duration ends or it's been revoked, the verification in phase 6 fails. In this case, a new certificate must be acquired from the administration point. If the certificate has been revoked because of compromise of private key, a new key pair must be generated in the PTD.

4.5 Bluetooth operation in Wireless access control system

The access controllers are set in nondiscoverable mode. This means that other devices can't discover them using the Bluetooth device discovery. They are naturally in connectable mode, so the connection establishment is possible if Bluetooth device address is known. The list of the controllers and their addresses is downloaded in the personal trusted devices, and the connections are made based on this list of addresses.

Communication is based on Bluetooth L2CAP protocol layer. This provides more than good enough communication properties for this kind of application. L2CAP is an underlying protocol layer used by all Bluetooth data communications, therefore it exists practically in every Bluetooth device and protocol stack.

The unlock request includes the lock ID signed with the private key and a X.509 certificate, which in turn includes user's information and his public key. The signature is used to check, that the lock ID in the packet is verifiably coming from the correct person and is not falsified by an outsider.

The challenge packet sent from the access controller to a personal trusted device includes random number generated by access controller and encrypted with the user's public key. The packet can't be decrypted and random number can't be found out in clear text format without the user's private key. Therefore the access controller can be sure that the response is coming from the correct user.

Response packet includes MD5 checksum of decrypted random challenge. Applying MD5 function to challenge before sending it as a response makes it almost impossible for eavesdropper to compute the challenge. Using MD5 or any other sophisticated one-way function, it's easy to compute a hash *h*, a checksum, from a certain message - but it's difficult to find a message *M* which provides the given *h*. It's also hard to find another message M' so that its hash and the hash of M are the same.

Although it's not impossible to find a message M' which results the same checksum as M, MD5 is good enough for this application. The access controller waits for the response only a short time after sending challenge, and it's not enough for eavesdropper to perform time taking calculations to find out the challenge message.

4.6 Operation sequences

There are four general operation sequences in the Wireless access control system. Two of these, *issuing and renewing certificates* and *updating lock configuration* are carried out between the administration point and the personal trusted device.

The unlocking procedure is naturally performed by the personal trusted device and the access controller. In addition to these, The administrator needs to *update access controllers* sometimes. These procedures are explained in the following chapters.

Removal of users is done when updating access controllers. A certificate revocation list is sent to access controllers, which discard all the requests coming with certificates, that are listed in a certificate revocation list. There's no need to actively remove old users from the system, because their certificates become invalid when they expire.

4.6.1 Certificate issuing and renewing

The user's certificate in his PTD can be updated via Bluetooth connection at the administration point. The administrator generates a certificate according to the information in the user's certificate request. If the user hasn't used the Wireless authentication system before, a certificate request must be created in his PTD and sent to the administration point. Prior to that, also a key pair must be generated in the user's PTD, because the certificate request is created using the private key. The certificate includes the general information of a X.509 certificate, which is presented in chapter 2.5.1. The certificate includes also two extensions. As the first extension, it includes the Bluetooth address of the user's PTD. This extension binds the certificate to the personal device of the user. The second extension is the list of the locks, which this user may open. This extension provides a binding between authorization and the user's public key. When the user has been identified and certificate has been generated, the certificate can be transferred to the PTD using Bluetooth connection. This whole situation as well as renewal of a certificate is described on the left hand side in the Figure 9.

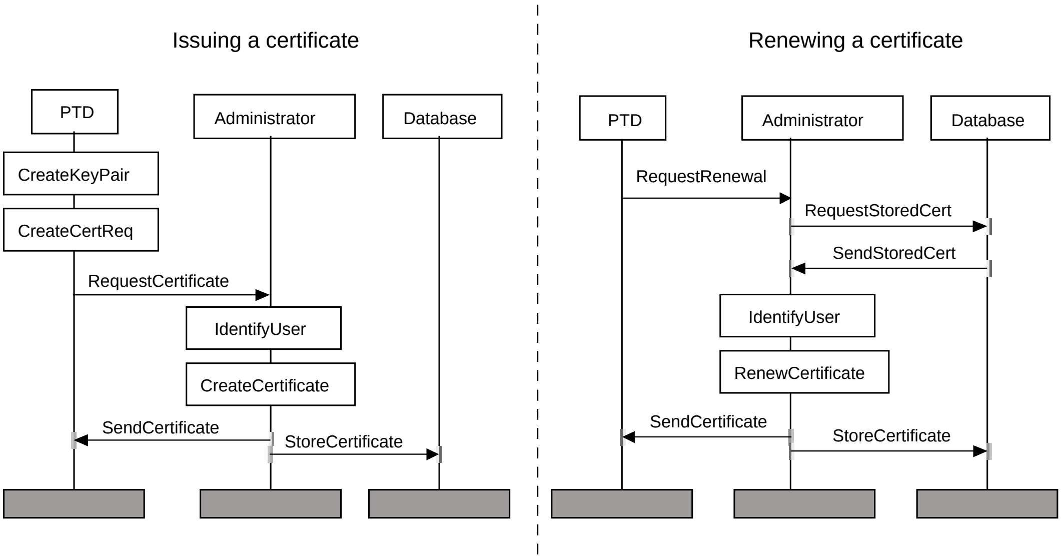
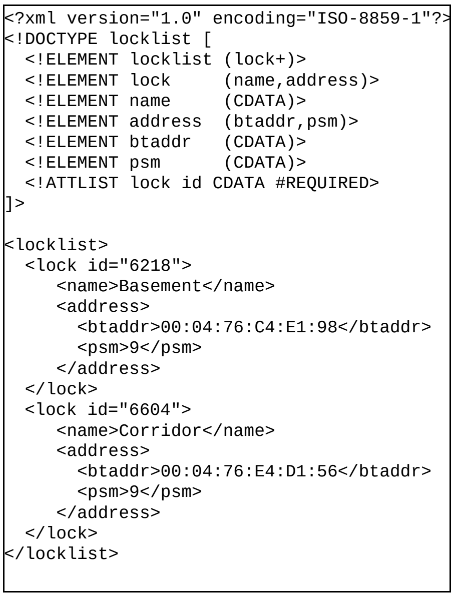


Figure 9 - Message sequence charts for issuing and renewing certificates

If a certificate has been issued to a user earlier, his certificate is found in the database which is part of the administration point. This certificate may be then renewed in the similar way than a new certificate is generated from a request. The new certificate includes the same information than the previous one, but with updated validity period.

4.6.2 Updating lock configuration

When acquiring the certificate, also the lock configuration can be updated. The user can request the updated lock list from his PTD. The PTD sends lock list request to administration point, which replies with the updated lock list configuration. This list is presented in a XML format, and it includes necessary information to present lock identity to the user and to connect to related access controller via Bluetooth. The lock list format is presented in Figure 10. The name of the door or room, marked with a <*name*> tag, is shown to the user and Bluetooth address <*btaddr*> and the Protocol Service multiplexor <*psm*> are used to connect to an access controller.



```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE locklist [
  <!ELEMENT locklist (lock+)>
  <!ELEMENT lock     (name,address)>
  <!ELEMENT name     (CDATA)>
  <!ELEMENT address  (btaddr,psm)>
  <!ELEMENT btaddr   (CDATA)>
  <!ELEMENT psm      (CDATA)>
  <!ATTLIST lock id CDATA #REQUIRED>
]>

<locklist>
  <lock id="6218">
     <name>Basement</name>
     <address>
       <btaddr>00:04:76:C4:E1:98</btaddr>
       <psm>9</psm>
     </address>
  </lock>
  <lock id="6604">
     <name>Corridor</name>
     <address>
       <btaddr>00:04:76:E4:D1:56</btaddr>
       <psm>9</psm>
     </address>
  </lock>
</locklist>
```

Figure 10 - Lock list format

4.6.3 Unlocking procedure

There are two possible choices for the initiation of the unlocking procedure.

- User launches the unlocking sequence from user interface on his device
- Device searches for locks and tries to unlock the doors automatically

In this application the first option is selected, because the latter one involves time-taking Bluetooth device discovery. This can be avoided in the first choice using pre-programmed list of locks, from which the user may choose the desired lock. Besides, this way the access controllers can be used in a non-discoverable mode hidden from the other Bluetooth devices.

Unlocking sequence starts when a user selects a lock ID on the user interface of his personal trusted device. The device creates an unlock request and sends it to the access controller, which verifies the certificate and checks the unlock request. If everything checks fine, the access controller creates a random challenge, encrypts it with user's public key and sends it back to the PTD. PTD then decrypts the challenge with user's private key stored in the device. The response is sent back to the access controller, hashed with MD5 one-way function. During this phase when the user's device is generating the response, access controller creates the response using the same function. When user's response reaches the access controller, it's compared against the one which the access controller created itself. If the responses match, the access controller unlocks the lock and allows the user to enter the room. The message sequence chart for the procedure is depicted in Figure 11.

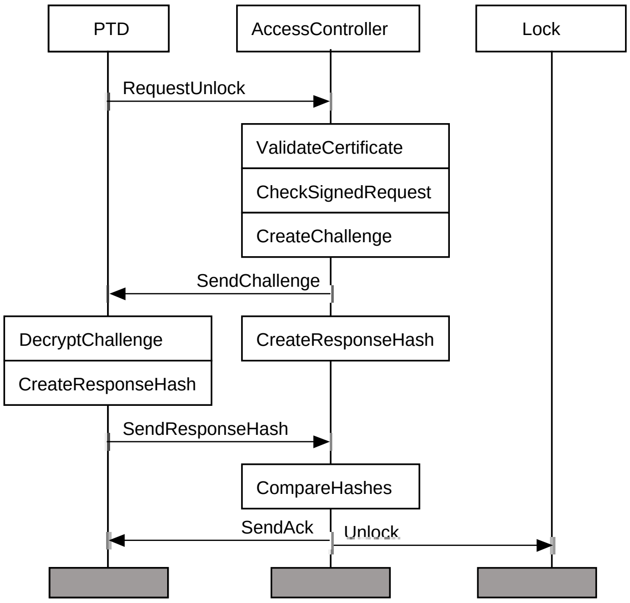


Figure 11 - Message sequence chart for unlocking procedure

This whole procedure, including connection establishment, exchanging the needed messages and executing cryptographic functions takes a few seconds. Timing of a test environment can be found in chapter 4.9.

4.6.4 Updating access controllers

In initial installations of access controllers the certificate of the certificate authority, the Administration point in this system, is installed to access controllers as well as list of locks related to particular access controller. Further updates are needed when the certificate for the administration point is changed, controlled locks are updated or user certificates need to be revoked.

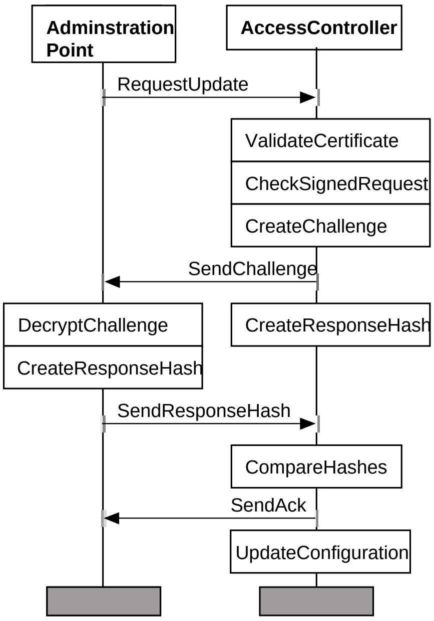


Figure 12 - Message sequence chart for updating access controllers

The first update becomes necessary, if a private key for the administration point has been compromised. In this case, the update must be done physically, because remote connections can't be authenticated anymore. Possible ways to do this is to install the new certificate to the access controllers using a serial port console. The lock list or the certificate revocation can be done remotely. Update in a general level is depicted in Figure 12. The updated information is signed with the private key of the administration point, and this signature is checked before the information is updated. Challenge response mechanism is used to prevent replay attacks.

4.7 Security issues

There are several different risk factors concerning the use of public key infrastructure (PKI). Some of them are common to all PKI applications but some arise when using PKI in certain situations. The most common risks and disadvantages according to [ELL2000] are explained in chapter 2.5.4. This chapter explains, how these would affect the use of the Wireless access control system.

The security of a verifying computer, the access controller in this case, must be taken care of. Since it verifies the incoming unlock requests using CA's public key in CA's certificate, no one must not be able to switch his own certificate in place of a CA's official certificate. The only way to do this is to make the access controller invulnerable to hostile access removing all the unnecessary connections from it and place it in place where it can't be physically tampered.

Many risks in PKI derive from the actual authority level of CA. Is it an authority on the things which are contained in certificates. In the Wireless access control system, those risks are eliminated, because this kind of access control system is based on a single authority, which controls the whole system. Therefore the first point, where the use of certificate may go off, is the part where CA or the Registration authority is supposed to identify the holder of an issued certificate. In this Wireless access control system, the administrator of the administration point must identify the user by checking his ID card. CA must also check that the user holds the private key corresponding the public one in the certificate. This is done using the certificate request, which can't be done without the particular private key.

4.7.1 Compromise of the private key

Since this system uses public key cryptography, a compromise of a private key leads to a relatively threatening situation. A malicious attacker may try to find the correct pass phrase to decrypt the private key and pose as the genuine holder of the key.

When a user notices, that his device has been stolen or the private key has been compromised in any other way, he should immediately contact system administration. The certificate bound to the public counterpart of the compromised private key must be revoked from the system. A list of revoked certificates needs to be distributed to the access controllers. The way how this is done, depends whether or not an access controller is reachable directly from the administration point. If the administration point can reach the access controller directly, it can send the revocation list to it. If not, then someone has to transfer the information to the access controller with a handheld service device.

If the private key of the certificate authority is compromised, that's a wholly different case. If the CA is the root CA, the certificates and keys of the entire system have to be changed. In a case of a non-root CA, all the keys and certificates under the area of influence of the particular certificate authority have to be changed.

4.7.2 Interference and denial of service

Sometimes a malicious person may want to interfere with the operation of a system or deny the user the access to that system. Also other allowed devices operating in the same ISM band may interfere with the operation. Bluetooth has means to attenuate the affect of the interfering devices. [MOR2002]

In addition to the countermeasures in Bluetooth radio specification, there is not much to do to prevent interference and denial of service from happening. The access controllers should be located so, that they can be used only from the neighborhood of the controlled locks. The access controllers should be set to non-discoverable mode, so that they don't respond to service discovery or the device discovery requests. The performance is not affected because of the handling of these requests.

4.8 Usability and the benefits of the system

This system provides a different way of creating an electronic access control system. Traditionally, all the intelligence is located in the main component to which the reader device is connected. The key provides just the identification of the user. In this application, also the authentication and authorization information is located in the device. An accurate offline authentication and authorization can be carried out without connection to main database. The private-public key pair is the distinguishing characteristics of a user. This system can be used effectively to offer a visitor the right amount of rights for the exact time of his visit – as long as he has a suitable handheld device. There is no need for the visitor to return any token or key at the end of his visit.

The ease of use is heavily limited by the usability of the handheld devices. This kind of multipurpose devices are nearly impossible to design as good as single-use traditional keys, whose use is pretty straightforward. However, If there are many different places, where similar access control is needed, or the access control can be used together with another service, the use of wireless handheld appliance as a *personal trusted device* may be a good approach. This makes a handheld device a versatile key to different services.

4.9 Efficiency and test measurements

The efficiency of the access control system was tested with a test environment, where Compaq iPAQ PDA was used as a personal trusted device, a laptop computer and a personal computer acted as access controllers for four electromechanical locks. The locks were attached to the parallel port of the computers.

In a test application the decrypting of the private key is done every time the program is started. This is the most time taking part of the whole situation. However, if a program is running in background, it can be raised to foreground with a shortcut button, and the application is ready to use.

The measurement was carried out by recording the sounds of the unlocking sequence and analyzing the timestamps in the audio file with an audio analyzing software. The sound of the unlock button on the PDA describes the start of the opening sequence, and the sound of the electromechanical lock shows the actual unlocking timestamp. The timestamps were manually sampled from the visual representation of the audio file.

The test was carried out as a series of 31 unlock tries, and it took approximately 5 minutes. The quickest unlocking took 1,2 seconds, and the longest measurable unlocking took 15,6 seconds. Generally the times were between 1,5 seconds and 2,5 seconds. Two times the Bluetooth connection time took more than 10 seconds, and of the 31 tries the unlocking failed once. Electromechanical locks used in the test environment stay open for 3 seconds before they lock again. Therefore the door can be opened no sooner than 1,5 - 2,5 seconds and no later than 4,5 - 5,5 seconds after the unlock request, as far as regular operation times are considered. The results from the test can be shown in the Figure 13 and the individual measurements are listed in the Appendix 1.

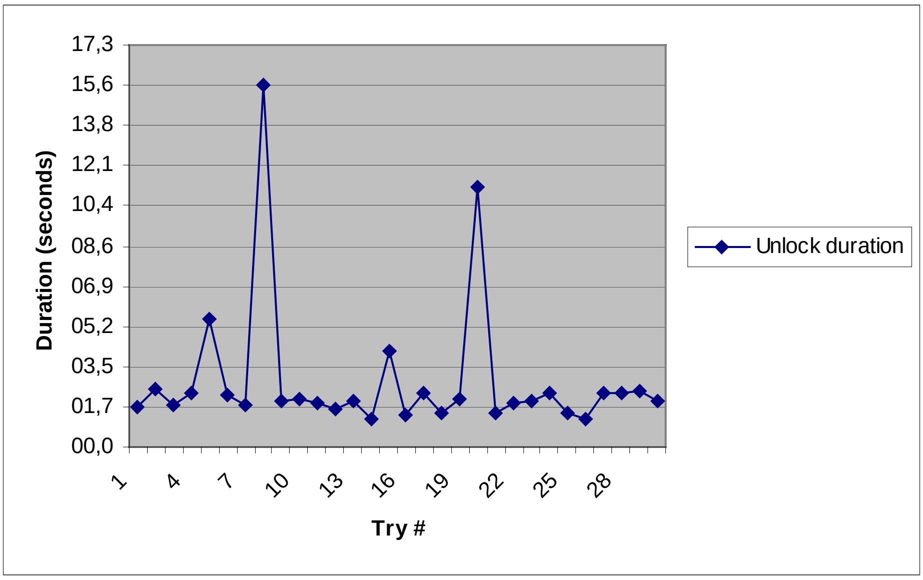


Figure 13 - Unlock durations in the test environment

4.10 Problems

What kind of problems have arisen in implementation of Wireless Access Control System? Originally, the Compaq iPAQ implementation was going to be just a temporary solution, and the main target platform was supposed to be a Symbian Operating System based mobile phone. However, there weren't suitable cryptography libraries available, and there were no resources to build or port one to Symbian OS ourselves. Therefore Compaq iPAQ PDA is the current platform for the Personal trusted device implementation.

4.11 Further development

The installation and initialization process of the implementation for Compaq iPAQ PDA hasn't received much concentration, and currently it involves a few command line programs to get necessary information in and out of the personal trusted device. It is certainly a thing to consider when developing the application further.

When a suitable cryptography library appears for the Symbian OS, the natural development is to build personal trusted device functionality to a Symbian OS based mobile phone. Symbian OS based phones are becoming more and more common, and the suitability of this kind of system is much bound to the number of possible devices to use. Symbian OS based phones are more likely to be the only handheld device for a person than a bigger Compaq iPAQ without any phone features.

The unlocking procedure in the current application begins from the user’s action. User has to select a particular lock from the list to send a unlock request to that particular access controller. If a way to search for access controllers effectively is found, a much more user-friendly approach is possible. The user interface may list a access controllers nearby at the begin of the list, and it’s easier for the user to select a correct lock. He doesn’t need to search for it through the whole list of locks. The ultimate step for the user friendliness is to manage the unlocking request without any user interaction. In addition to effective searching, this involves also a strong limitation of the operating range, which may be not the desired direction for the versatility point of view.

When new technologies emerge, a more suitable radio technology for this application may be found. It may have a faster device discovery and connection establishment than Bluetooth. A possibility to modify the application to use new technologies will be considered when needed.

4.12 Summary

The wireless access control system is an access control system, in which handheld Bluetooth devices are used as key devices. A key device may be for example a mobile phone or a PDA. Connections are made using general L2CAP protocol, which is available in every Bluetooth protocol stack. Therefore from the connectivity point of view, any Bluetooth device can act as a key device.

Public key certificate system is used as an authentication and authorization mechanism. So device must support public key cryptographic functions and public key certificates. The rights for a user are given at the *administration point*. User creates a public-private key pair in his *personal trusted device,* which is a more general term for the key device, and requests a certificate from the administration point. The administrator issues a certificate for the user, binding his personal information to his public key. Also the allowed locks are presented in the certificate providing authorization information.

When the user wants to unlock a lock, he selects the lock from the list in his device, and an unlock request including the certificate is sent to the *access controller*. The access controller verifies the certificate, and if it's authentic and includes the desired lock, the access controller verifies the possession of the private key with challenge response mechanism. Challenge is encrypted with the user's public key, and it can only be decrypted with the corresponding private key. If the user succeeds to respond with a correct response, access is granted and the lock unlocked.

5 CONCLUSION

The main goal of this thesis was to design a wireless access control system, where a generally available multipurpose handheld devices can be used as a key devices and the communication between the parts of the system is wireless. Bluetooth was selected as a wireless technology, mainly because of its popularity in mobile phones and other small devices. Furthermore, there were no known restrictions, why it shouldn't be selected.

After preliminary study on authentication and authorization methods public key cryptography and public key certificates were selected as an authentication and authorization method for the access control system. The introduction of new users is easy to arrange and authentication at the access controllers can be done offline without connection to the certificate authority. When the authentication is done with a challenge response mechanism, the possession of the private key can be verified without sending the secret over the transmission path. Most of the risks of public key infrastructure are related to the trust of other parties, and they can be avoided in a closed system like the wireless access control system. The certificate authority and the public key certificate clients belong to the same organization and administration area.

Bluetooth wireless technology is suitable for the access control system, if the time taking device discovery can be avoided. As can be seen in chapter 4.9, the unlock request and the challenge response authentication takes approximately 2 seconds for most of the tries. The device discovery has been bypassed by storing a list of access controllers into the personal trusted device. The usability of the system is highly dependent of the design of the handheld devices.

References

[AIM2003] AIM Global Network. What is RFID? [www-document] Updated September 16, 2003. [Retrieved: April 27, 2004]. From: http://www.aimglobal.org/technologies/rfid/what_is_rfid.htm

[BLU2001a] Bluetooth Special Interests Group. Specification of Bluetooth system, version 1.1, 2001.

[BLU2001b] Bluetooth Special Interests Group. Specification of Bluetooth system, Specification Volume 2: Profiles.

[BLU2004] Bluetooth Special Interests Group . Bluetooth enabled products. [www-document]. [Retrieved: April 27, 2004]. From: http://www.bluetooth.com/products/

[BRA2001] Bray, Jennifer, Sturman, Charles. Bluetooth: connect without cables. Prentice Hall PTR, 2001. ISBN 0-13-089840-6.

[DAV1989] Davies, D.W., Price, W.L. Security for computer networks: an introduction to data security in teleprocessing and electronic funds transfer, 2nd edition. John Wiley & Sons Ltd., 1989. ISBN 0-471-92137-8.

[DIF1976] Diffie, Whitfield, Hellman, Martin E. New Directions in Cryptography. IEEE Transactions on Information Theory, IT-22, 6, 1976, pp.644-654.

[DLU1998] Dlugos, David J. Wiegand effect sensors, theory and application. Sensors, May 1998. [www-document] [Retrieved:April 27, 2004]. From: http://www.sensorsmag.com/articles/0598/wie0598/index.htm

[ELL1999a] Ellison, Carl M. The Nature of Usable PKI. Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 31, Issue 9 (April 1999) pp. 823-830.

[ELL1999b] Ellison, Carl, et al. SPKI Certificate Theory. IETF Request for Comments: 2693. 1999 [Retrieved: April 27, 2004]. From: http://www.ietf.org/rfc/rfc2693.txt

[ELL2000] Ellison, Carl, Schneier, Bruce. Ten Risks of PKI: What You're not Being Told About Public Key Infrastructure. Computer Security Journal, Volume XVI, Number 1, 2000, pp. 1-7.

[GER2000] Gerck, Ed. Overview of Certification Systems: X.509, CA, PGP & SKIP, 2000. [Retrieved: April 27, 2004] From: http://citeseer.ist.psu.edu/252354.html

[HAL1994] Haller, Neil M. S/KEY One-time Password System, Proceedings of the ISOC Symposium on Network and Distributed System Security, pages 151-157, San Diego, CA, February 1994. [Retrieved: April 27, 2004] From: http://citeseer.ist.psu.edu/haller94skey.html

[HAL1996] Haller, N., Metz C. One-Time Password System. IETF Request For Comments: 1938. Updated: May 1996. [Retrieved: April 27, 2004]. From: http://www.ietf.org/rfc/rfc1938.txt

[HON2000] Hontañón, Ramón J. Keeping PKI Under Lock and Key. Network Magazine, October 2000, pp. 58-62.

[HOU2002] Housley, R. et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF Request for Comments: 3280. Updated: April 2002. [Retrieved: April 27, 2004] From: http://www.ietf.org/rfc/rfc3280.txt

[INT2003] Integrated Magnetics. BlueWire Wireless Card Reader Interface. [pdf document]. 2003. [Retrieved: April 27, 2004] From: http://www.integrated-magnetics.com/pdf/BlueWire.pdf

[IRD2003] Infrared Data Association. IrDA Standards. [www-document]. Updated September 9 2003. [Retrieved: April 27, 2004] From: http://www.irda.org/standards/standards.asp

[KAM2002] Kammer, David, McNutt, Gordon, Senese, Brian, Bray, Jennifer. Bluetooth Application Developer's Guide: The Short Range Interconnect Solution. Syngress Publishing, Inc., 2002. ISBN 1-928994-42-3.

[KIN2003] Kinney, Patrick. ZigBee Technology: Wireless Control that Simply Works. Updated: October 2, 2003. [Retrieved January 9, 2004]. From: http://www.zigbee.org/resources/documents/ZigBee_Technology_Sept2003.doc

[MIC2004] Microsoft Corporation. Microsoft .NET Passport Q&A [www-document]. [Retrieved: April 27, 2004]. From: http://www.passport.net

[MIL1988] Miller, S.P., Neuman, C., Schiller, J.I. and Saltzer, J.H. Kerberos Authentication and Authorization System. Project Athena Technical Plan, Section E.2.1, Massachusetts Institute of Technology. October, 1988. [Retrieved: April 27, 2004] From: ftp://athena-dist.mit.edu/pub/kerberos/doc/techplan.PS

[MOR1979] Morris, Robert, Thompson Ken. Password Security: A Case History. Communications of the ACM, Vol. 22, No. 11, November 1979, pp. 594-597.

[MOR2002] Morrow, Robert. Bluetooth Operation and Use. The McGraw-Hill Companies, Inc., 2002. ISBN 0-07-138779-X.

[MUF1989] Muftic, Sead. Security mechanisms for computer networks. Ellis Horwood Limited, 1989. ISBN 0-13-799180-0.

[NAO1998] Naor, Moni, Nissim, Kobbi. Certificate Revocation and Certificate Update. Proceedings of the 7th USENIX Security Symposium (San Antonio, Texas), Jan 1998. [Retrieved: April 27, 2004] From: http://citeseer.ist.psu.edu/naor98certificate.html

[NET2000] Network Associates, Inc. An Introduction to Cryptography. [pdf document] Updated: September 2000. [Retrieved: April 27, 2004]. From: ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf

[OPI2004] Open Palmtop Integrated Environment project homepage. Overview. [www-document]. [Retrieved: April 27, 2004] From: http://opie.handhelds.org/overview.php

[SAN1994] Sandhu, R., Samarati, P., "Access Control: Principles and Practice", IEEE Computer, September 1994, pp. 40-48.

[SCH1996] Schneier, Bruce. Applied cryptography: protocols, algorithms, and source code in C, second edition. John Wiley & Sons, Inc., 1996. ISBN 0-471-11709-9.

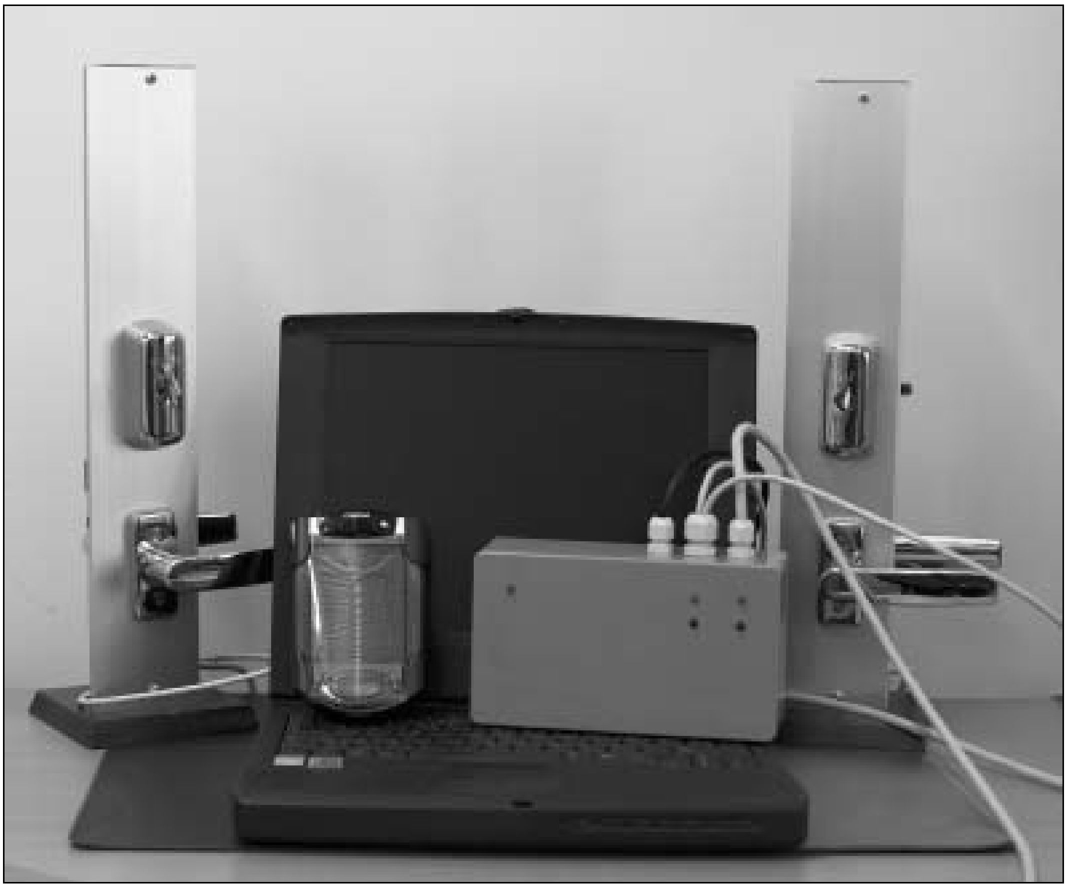
[SMI2002] Smith, Richard E. Authentication: from passwords to public keys. Addison-Wesley, 2002. ISBN 0-201-61599-1.

[STE1988] Steiner, Jennifer G., Neuman, Clifford, Schiller, Jeffrey I. Kerberos: An Authentication Service for Open Network Systems. [Retrieved: April 27, 2004] From: http://secinf.net/uplarticle/2/kerberos.ps

[ZIG2002] The Zigbee Alliance. ZigBee overview. [pdf-document]. Updated September 2002. [Retrieved: April 27, 2004]. From: http://www.zigbee.org/resources/documents/ZigBeeOverview4.pdf

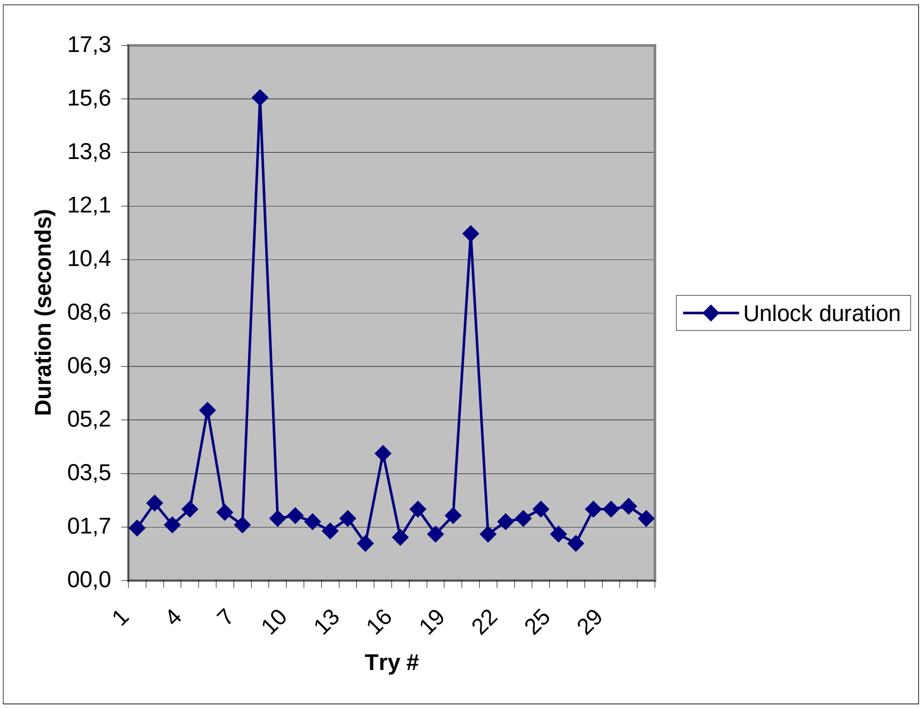
Appendix 1 - Test environment and unlocking results

In the test the durations of unlock requests were measured in a test environment pictured below. A laptop and a personal computer were used as access controllers, and two electromechanical locks were attached to them via an implemented relay box attached to the parallel ports of the computers. Compaq iPAQ handheld computer was used as a key device. Connections were made from it to the access controllers and electromechanical locks were unlocked.



The table lists the durations of individual unlock tries. The durations are depicted also in the chart below.

#	Click	Unlock	Duration	#	Click	Unlock	Duration
1	00:03,4	00:05,1	01,7	17	02:33,8	02:36,1	02,3
2	00:11,6	00:14,1	02,5	18	02:41,9	02:43,4	01,5
3	00:20,8	00:22,6	01,8	19	02:49,3	02:51,4	02,1
4	00:29,7	00:32,0	02,3	20	02:57,9	03:09,1	11,2
5	00:38,0	00:43,5	05,5	21	03:18,1	03:19,6	01,5
6	00:48,9	00:51,1	02,2	22	03:25,4	03:27,3	01,9
7	00:59,3	01:01,1	01,8	23	03:32,7	03:34,7	02,0
8	01:07,3	01:22,9	15,6	24	03:40,1	03:42,4	02,3
9	01:30,1	01:32,1	02,0	25	03:47,6	03:49,1	01,5
10	01:37,5	01:39,6	02,1	26	03:55,3	03:56,5	01,2
11	01:45,3	01:47,2	01,9	27	04:02,1	04:04,4	02,3
12	01:53,3	01:54,9	01,6	29	04:35,4	04:37,7	02,3
13	02:00,8	02:02,8	02,0	30	04:42,7	04:45,1	02,4
14	02:10,3	02:11,5	01,2	31	04:51,1	04:53,1	02,0
15	02:17,9	02:22,0	04,1				
16	02:26,7	02:28,1	01,4	28	04:09,7	00:00,0	Failed


Duration (seconds)
Try #
Unlock duration