Security protocol for a remote user authentication system over unsecure network

Raghad Mohammed Hadi
Iraqi commission for computer and informatics
informatics of postgraduate studies.

Abstract

Security of data communication becomes a crucial challenge due to the rapid development of computer and information technologies. To ensure security of resource transmission, computer engineers have proposed numerous schemes for protection among them, the remote user authentication schemes using smart cards are regarded as very efficient.

Remote user authentication has been adopted as one of the most commonly used solutions in network environments to protect resources from unauthorized access. As a result, smart-card based authentication schemes has become a popular research topic in recent years. So we propose a system about remote user-authentication that aims to achieve more functionality these schemes is secure and works like a close channel because ID user and password is required to authenticate the user, so we fulfill the basic need of authentication schemes. Furthermore, the proposed scheme provides the following properties: establish a session key, mutual verification, easy-of-use, without verification table and based on public key encryption.

Keywords:
Communications, Remote Authentication, Smart card, cryptography, identification, password.

1. Introduction

A remote user authentication scheme is a mechanism that authenticates remote users and allows legitimate users to access network services over an insecure communication network. [1].The control of the access to remote resources has become a crucial challenge due to the rapid development of computer and information technologies. Generally, most of the resources provided on Internet are not free for all users. Often, some services on the remote servers are paid. In other words, the providers of the services/ facilities have to put their resources under appropriate protection. The password authentication schemes are usually considered as the most efficient and practical method to achieve the goal of protecting remote resources. In the password authentication schemes, the user sends his/ her identity (ID) and password (PW) to the server in order to get authentication when he/ she wants to access facilities on the remote system. ID and PW are issued to the user by the remote server in the registration phase. If the user is authenticated successfully, the user will be authorized to access the facilities provided by the remote system; otherwise, the access request will be rejected.[2]

2. Information security concept.

When a user accesses the directory, two critical steps must take place: user authentication and authorization. User authentication is the process of mapping a user to set of identities, which we call credentials. Typically, credentials include the user's name and the list of groups to which the user belongs.[3] Authorization is the process through which a file server checks a user's credentials against an ACL to make an access control decision.[4]

Information security relates to the need to keep information from falling into the wrong hands. Failure to follow good security practices may lead to unauthorized uses of information, to fraud and to identity theft. In contrast, businesses collect and share information about people for a variety of appropriate reasons: improving service, decreasing costs, reducing fraud, and targeting offers of goods and services. This normal flow of information in a business context is not an example of lax security practices and does not lead to the unauthorized use and fraud associated with bad security. The policy issues relating to information security differ markedly from the policy issues relating to information sharing.[5]

3. Smart Cards

Smart cards come in a variety of shapes and sizes, although they look very similar to credit cards in general [6], [7]. A smart card contains an integrated circuit chip (ICC) within its structure. This is a microchip that is able to perform processing and contains some form of non-volatile memory [8]. Within the telecommunications environment, smart cards are predominantly uses as pre-paid telephone cards [9] for public pay phones, and as the Subscriber Identity Module (SIM) card used within mobile phones. Smart cards store information in a file structure within their memory, which can only be accessed through the operating system (OS) stored on each card.

Therefore, the processing ability of smart cards provides better security than other storage mediums, and is therefore, useful in electronic commerce , pre-paid telephone cards [10], and within mobile telephone systems Certain information stored on the smart card requires that the user enter in a PIN value before the information can be

accessed. The access control is controlled by the operating system and cannot be bypassed since it is located on the hardware level. If the user enters a PIN incorrectly several times, the operating system will disable access to the information on the card permanently, or until the user enters in a different, longer PIN value, usually referred to as a PIN2 value. It is important to note, that the user must keep the PIN value secret, or anyone else could make use of the smart card, and hence, impersonate the user.[11]

4. The Proposed System Platform Requirements

The platform is foundation of the software solution and should be presented first. The core component will be indicted, piecing it all together in overall architecture, with some though about communication, figure (1) shows the proposed system's platform, the proposed system content the following parts:

A. User

The propose system is a one of secure system to run must have hardware, the hardware is different types of device, recommendation should run at the following device:

1. Personal computer or laptop with a minimum specific as below:

- Microsoft windows XP
- IIS which provide basic HTTP
- TCP/IP protocol
- HTTP protocol
- Web browser
- LAN Cart
- 512 RAM
- 1.7 CPU

B. Internet

- Internet connection Side: which PC or Laptop sends and receive over an Internet Protocol (IP)-base internet network.

C. Remote Server

The recommendation system is a web application so that the proposed system depends and uses web server feature like:

- IIS (Internet Information Services): which provide basic HTTP, FTP and SMTP Service?
- ADO.NET (Active Data Objects): which provide as robust development platform for building web application, which OLE DB provider (ODEDB) and can connect with any Microsoft tools and interface with underlay SMD databases.

5. Implementation toolset

The tools use to implementation proposed system in world web site must use different types of tools, one of the tools is language, web programming language and data manipulation language used to compose a system, the language types are:

- ASP.NET(Active Server Pages) are HTML page, which include scripting and create active web server applications,ASP.NET language is very important to build web application and different from the previews language to have many tools to build site and can used the visual basic or JavaScript .NET language to easy be programming functions, and ASP.NET can be connected with Emulator Smart phone, It has tools for drawing and designing the interface in web applications, when used the ASP or HTML to build the web applications, we need to programming all functions, the preview web design language not have any facility when compare with NET language.

• **Structure query language** is a standard computer language for access and manipulation database system, SQL statements are used to retrieve update data in database and used execute query against database. SQL work with data base programs like MS access, Oracle and DB2.ect

• **Visual Basic.** NET is used to programming algorithm , the visual Basic has many facility as tools web use to build and connect with internet, this language is easy connect with ASP.NET, when programming is debugger Program can easy discover the error by used many windows for watch, and in writing code for programming the debugger work in real time to increase speed.

6. System components

The system can be explained by describing these components:

Certificate authority (CA) and Remote server and Smart card (SC) see **figure (1).**

6.1 Certificate Authority (CA)

The primary role of the CA within the architecture of the proposed system is to issue the user with a smart card. The smart card contains a biometric section as well as a data segment. The biometric section contains the personal and identification information of the user (ID user), while the data segment contains encryption keys (EKs) and identification variables (IDVs), as shown in Figure 2. The proposed system on computer used these two types of keys for authentication and exchange key and the keys are found on the smart card of user who went to connect with remote server and used its services.

• When user registry initializations in system and enter data from proposed system on CA computer, the system used secret key (symmetric key) as password and must unique key this key is (EK1) found in slot1 on data segment of smart card, this key used to encryption data in scenario send and receive to encryption and decryption data.

• In the connection with remote server, the user used smart card to enter the system, to avoid attacker in channel these information encryption by public key for administrator, therefore the system generator public/private keys used for that.

6.2 Start of the Identification Process (Message 1)

To allow a user to make use of a service offered by a remote server, the smart card identifies the user to the remote server by transmitting the user’s ID. However, the proposed system encrypts the user’s ID number with a EK value from the data segment of smart card. Therefore, in addition to the encrypted user

ID, the SN of the card, and the slot index position (a) of the EK (Sa: EK1) used to encrypt the user ID, are also sent to the remote server, i.e. Message (1) = {SN, a, Sa:EK (ID)}.

6.3 Processing the Encrypted Message (Message 2 & 3)

The remote server is unable to identify and authenticate the user. However, the CA is having the EK set stored on the smart card of user who went to connect with Remote server. The remote server can therefore request the EK from the CA using a secure communication channel, such as using RSA encryption. Hence, the remote server sends EK to the CA to identification of user, EK encrypted with the public RSA key of the CA, i.e. Message (2) = {CA PubKey(EK)}. Once the CA has decrypted the message, the CA retrieves the relevant EK. The retrieved EK is encrypted with the remote server's public key and sent to the remote server, i.e. Message (3) = {remote server PubKey(EK)}. The remote server decrypts the message (Message 1) received from the user using the EK. The remote server now has the user ID and EK with the remote server's database of registered users. If the user exists within the remote server's database of resisted users, the user is now authenticated to use the service. This step achieves mutual identification and authentication of the user and the remote server.

7. Installation Algorithm

The installation process is done by administrative

Begin

The user sends to request system.

The CA responses to user's request for sends to user request smart card to enter in system.

The user sends message 1 to Remote server.

The remote server in the system receives message1 and add its information in remote server table.

Remote server generates message 2 and send it to the CA. This step achieves mutual identification and authentication of the user and the remote server.

End

8. Send/ Receive Scenario Algorithm

Begin

The user can login to his account by using smart card.

The systems will encryption the some information of smart card by public key and sends them to the remote server.

The last (remote server) receives information of smart card to decryption by the private key of remote sever.

The CA check these information in login table, if the user is registry then the service retrieved to the user account in the account table.

End

9. System Services

The actual operator of proposed system consists of two services confidently and authentication. They will summarize in turn:

Confidently: it is the most important basic service, which is provided by encryption message to be transmitted, the proposed encryption is used.

Authentication: The encryption algorithm used in proposed system is of secret key type therefore the user authenticity is determined by the owner of the secret key.

10. Conclusions

1. In this paper we consider the condition of user's identity format in away that is making it to work well.
2. Furthermore, we proposed several ways that enable an attacker to obtain a really valid identity as well as its corresponding password.
3. This scheme is secure and works like a close channel. Because user ID is required to authenticate the user, so we fulfill the basic need of authentication schemes.
4. To achieve the authenticity process to reach data in the proposed System, the secret key is encrypted by the RSA public key method so to get a high level of key management security.

11. References

[1] Huei-Ru Tseng, Rong-Hong Jan and Wuu Yang, " ***A Bilateral Remote User Authentication Scheme that Preserves User Anonymity***".

[2] Chin-Chen CHANG and Jung-San LEE," ***An efficient and secure remote authentication scheme using smart cards*** ", information & security. An International Journal, Vol.18, 2006, 122-133.

[3] Amit K Awasthi," ***Comment on 'A Dynamic ID-based Remote User Authentication Scheme***",Transaction on Cryptology@ Copyright GFCR, 2004 Aug 2004, Vol. 01, Issue 02

[4] Michael Kaminsky," ***User Authentication and Remote Execution Across Administrative Domains***", Massachusetts Institute of Technology, 2004.

[5] Alan W., "***Prepared Statement before the House Subcommittee on Commerce***", Trade and Consumer Protection, For a good summary of these surveys May 8, 2001. ***www.cdt.org/privacy/ccp/security1.shtml***

[6] S. Petri, "***An introduction to smart cards***," Messaging Magazine, September 2003. www.opengroup.org/comm/the message/magazine/mmv5n5/SmartCards.htm

[7] D. Everett, "***Smart card tutorial***," www.smartcard.co.uk, Tech. Rep., 1994.www.smartcard.co.uk/tutorials/ sct-itsc.pdf2

[8] M. Baker, "***Non-volatile memory for fast, reliable file systems***," Proceedings of the Fifth International Conference on Architectural Support for Programming Languages and Operating Systems, October 2002.

[9] G. Chew, "***Smart cards, systems using smart cards and methods of operating said cards in systems***," United States of America Patent 5,901,303, May, 1999.

[10] E. Turban and D. McElroy, "***Using smart cards in electronic commerce,***" International Journal of Information Management, vol. 18, no. 1www.sciencedirect.com/science/article/B6VB4-3SX7008-6/ 2/33984f67ec3985a4e3c39bde70f3f791.

[11] P. Martineau, "***Prepaid smart card in a gsm based wireless telephone network and method for operating prepaid cards,"*** United States of America Patent 5,915,226, June, 2005.

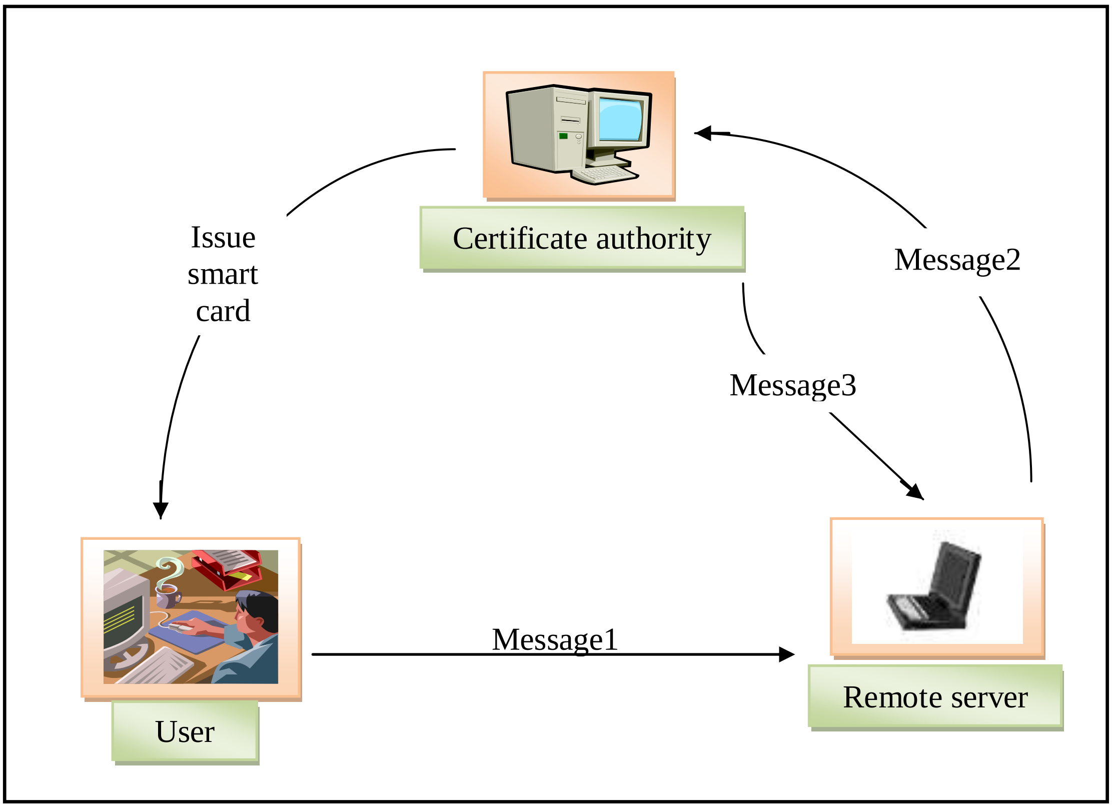
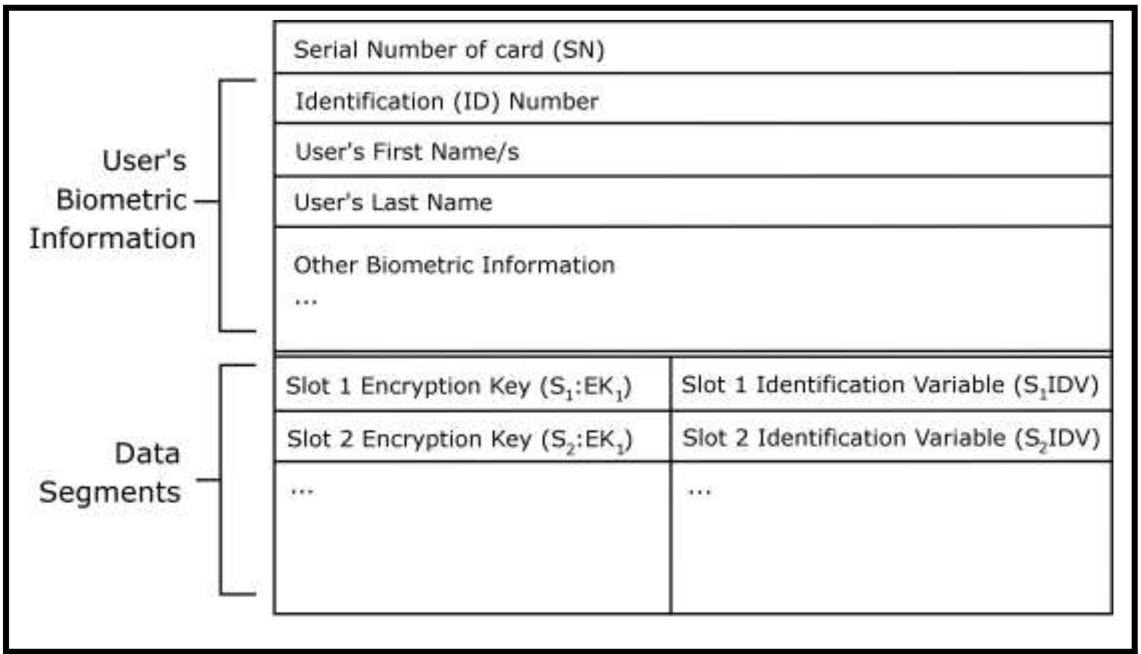


Figure 1: the architecture of proposed system.



Serial Number of card (SN)	
Identification (ID) Number	
User's First Name/s	
User's Last Name	
Other Biometric Information ...	
Slot 1 Encryption Key (S_1:EK_1)	Slot 1 Identification Variable (S_1IDV)
Slot 2 Encryption Key (S_2:EK_1)	Slot 2 Identification Variable (S_2IDV)
...	...

Figure 2: The sections and layout of the information stored on the smart

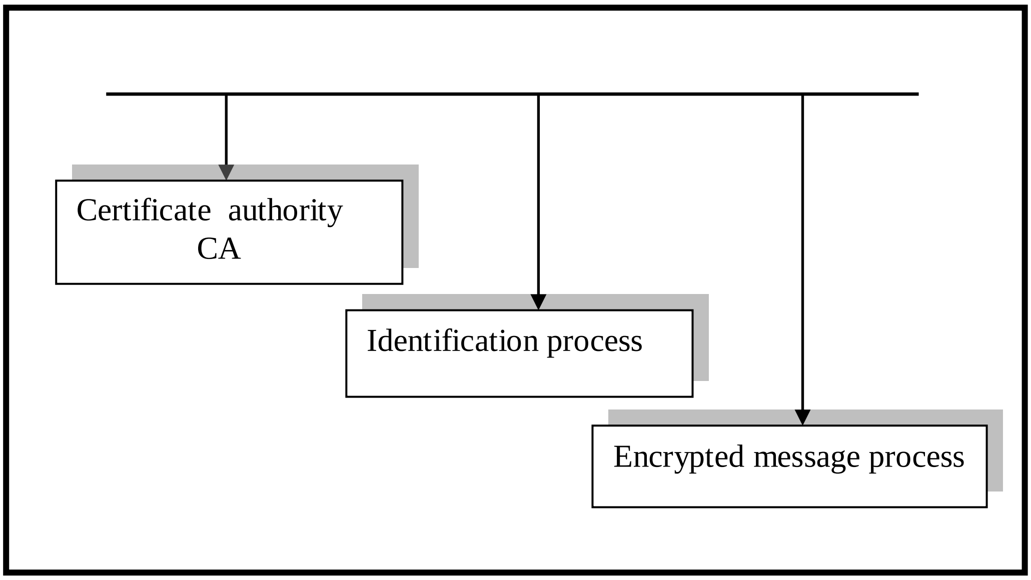


Figure 3: System Component

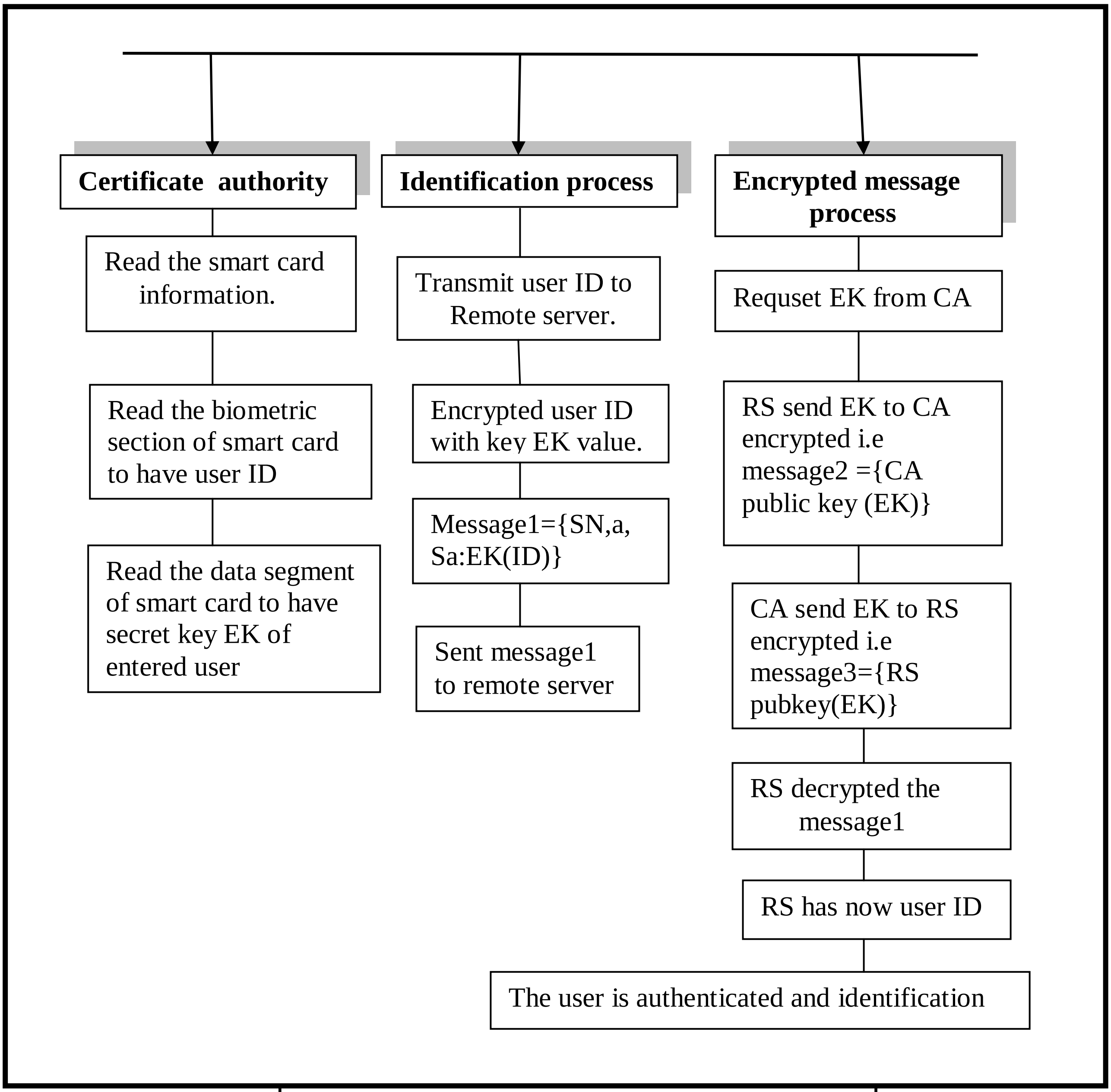

Certificate authority
Read the smart card information.
Read the biometric section of smart card to have user ID
Read the data segment of smart card to have secret key EK of entered user
Identification process
Transmit user ID to Remote server.
Encrypted user ID with key EK value.
Message1={SN,a, Sa:EK(ID)}
Sent message1 to remote server
Encrypted message process
Requset EK from CA
RS send EK to CA encrypted i.e message2 ={CA public key (EK)}
CA send EK to RS encrypted i.e message3={RS pubkey(EK)}
RS decrypted the message1
RS has now user ID
The user is authenticated and identification

Figure 4: described for system parts

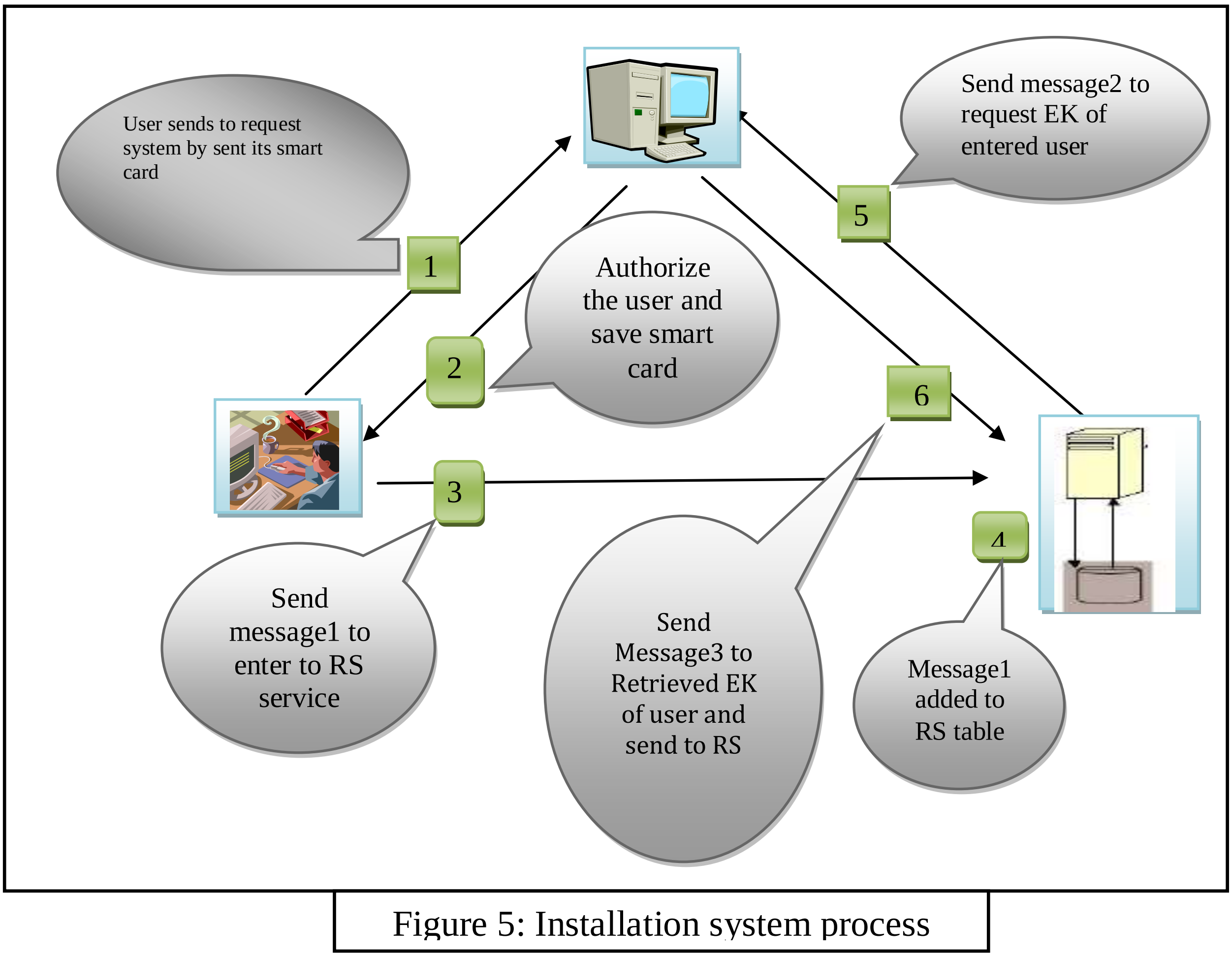

User sends to request system by sent its smart card
1
Authorize the user and save smart card
2
Send message2 to request EK of entered user
5
6
3
4
Send message1 to enter to RS service
Send Message3 to Retrieved EK of user and send to RS
Message1 added to RS table

Figure 5: Installation system process

بروتوكول امني لتخويل المستخدم عن بعد في شبكة غير أمينة.

رغد محمد هادي

الهيئة العراقية للحاسبات والمعلوماتية-معهد المعلوماتية للدراسات العليا.

الخلاصة

أصبح أمن نقل البيانات تحديا حاسما بسبب التطور السريع لتقنيات الحاسوب والمعلومات لضمان أمن نقل الموارد ،واقترح العديد من المهندسين الحاسبات خطط للحماية من بينها تخويل كلمة المرور عن بعد باستخدام البطاقات الذكية والتي اعتبرت فعالة جدا. ونتيجة لذلك أصبحت أنظمة التخويل باستخدام البطاقة الذكية موضوع مهم للبحث في السنوات الأخيرة. لذا تم اقتراح نظام تخويل المستخدم عن بعد و الذي يهدف إلى تحقيق المزيد من الوظائف من هذه المخططات الغير آمنة وتعمل مثل قناة قريبة ولأنه ID وكلمة المرور مطلوبة للمصادقة او للتحقق من تخويل المستخدم فإننا بذلك لبينا الحاجة الأساسية لأنظمة التخويل وعلاوة على ذلك، فإن الخطة المقترحة توفر الخصائص التالية :التحقق المتبادل ، وسهولة الاستخدام ، من دون التحقق من الجدول وعلى أساس وظيفة في نظام التشفير العام.

الكلمات المفتاحية:

الاتصالات, تخويل المستخدم, البطاقة الذكية, التشفير , التحقق, كلمة المرور.