pd.tvz.hr
POLYTECHNIC & DESIGN Vol. 5, No. 4, 2017.
DOI: 10.19279/TVZ.PD.2017-5-4-18

SMART CARD CONCEPT OF TWO-FACTOR USER AUTHENTICATION AND DATA ENCRYPTION WITHIN A WINDOWS DOMAIN

KONCEPT PRIMJENE PAMETNE KARTICE ZA DVOFAKTORSKU AUTENTIKACIJU I ENKRIPCIJA PODATAKA UNUTAR WINDOWS DOMENE

Ivan Jurinić, Roman Domović

Tehničko veleučilište u Zagrebu, Vrbik 8, Zagreb, Hrvatska

Abstract

Smart cards play an important role in information, financial and mobile industry. In information industry, smart cards are used as safety element within variety of services such as data protection, user identification or providing secure communication over insecure communication environment. In this paper, network infrastructure is created, consisting of server, switch, desktop computer, laptop and router that is assigned by the ISP. Using a blank smart card and reader assigned by Financijska agencija – FINA (eng. Financial agency) and using ActiveClient software, we demonstrate user authentication within domain, data encryption by using Encryption File System (EFS) and connection to internal network over Virtual Private Network (VPN).

Keywords: *smart card, authentication, data encryption, Windows domain*

Sažetak

Pametne kartice igraju važnu ulogu u informatičkoj, financijskoj i mobilnoj industriji. U informatičkoj industriji, pametne kartice koriste se kao sigurnosni element u okviru raznih usluga kao što su zaštita podataka, identifikacija korisnika ili osiguravanje sigurne komunikacije preko nesigurne komunikacijske okoline. U ovom radu kreirana je mrežna infrastruktura koja se sastoji od poslužitelja, preklopnika, stolnog računala i usmjernika kojeg je dodijelio pružatelj internetskih usluga. Koristeći praznu pametnu karticu i čitač kojeg je dodijelila Financijska agencija (FINA) te koristeći ActiveClient programsku podršku, prikazujemo autentikaciju unutar domene, enkripciju podataka koristeći Encryption File System (EFS) i konekciju prema internoj mreži preko virtualne privatne mreže.

Ključne riječi: *pametna kartica, autentikacija, enkripcija podataka, Windows domena*

1. Introduction

1. *Uvod*

Development of smart cards can be traced back to 1970s when technology made it possible to integrate data storage and processing logic on a single silicon chip which can be integrated into a card made of Polyvinyl Chloride (PVC) material [1]. With the expansion of cards in financial industry, some things have become obvious: to protect credit card transactions from the fraud and manipulation it is necessary to expand and improve smart cards functionality and protection. Along with development of the cards, development of cryptography, computer and information systems was carried out. In 1974. Frenchman Roland Moreno patented a card with integrated circuit which improved simple card into the smart card [1]. With the further development of the cryptography and smart cards, new possibilities have appeared for their use. This paper introduces the concept of using smart cards for the purpose of authentication within the domain, encryption of data using Encrypting File System (EFS) and connection to the internal network through a Virtual Private Network (VPN). It came out of the graduate work and the purpose of it is to present simple smart card security method in a short, concise, partially "how to" form. In the „Smart Cards" section we are explaining structure and types of smart cards. In the „Cryptography" section we are explaining basic principles of cryptography.

In the following section there is an overview of digital signature and digital certificates as cryptography tools. Next chapter is a brief explanation of Public Key Infrastructure, followed by chapter about security risks. Finally, we have description of proposed security concept and conclusion. Niz kolega iz struke – projektanata ili drugih – koji nisu profesionalni nastavnici, niti to žele biti, ipak rado prezentiraju svoj rad, te rado dođu pokazati svoje netom završene, omiljene ili nagrađene projekte. Studenti tako imaju priliku vidjeti veći broj raznovrsnih aktualnih izvrsnih projekata, iz prve ruke, što im je veoma zanimljivo i doprinosi dobrom osjećanju na studiju, i ponosu.

2. Smart cards

2. *Pametne kartice*

A smart card is a card with an embedded integrated circuit. Smart cards are divided in two ways: by the type of the chip and by the method of data transfer. By the type of the chip smart cards are further divided into shared memory smart cards and microprocessor smart cards, while according to the method of data transmission they are divided into contact smart cards and contactless smart cards. As for the physical structure of the smart cards, most smart cards are the size of bank credit cards, made out of PVC material with a chip containing the processor and memory, and the contact surface consists of eight metal contacts. Today's smart cards are made according to ISO 7810 standard, and there are four basic smart card formats; ID-1 (Identification), ID-00, ID-000 and mini-UICC (Universal Integrated Circuit Card). The chip is the most important and the most sensitive part of the card, and because of its sensitivity it is built into small case within the card, called a chip module. The module is designed to protect the chip from external conditions and has eight metal contacts that enable communication between the card and the terminal. There are three types of module: TAB module (Tape Automated Bonding), Chip-on-flex module and Lead-frame module. TAB module was the standard in the 90s, but today it is not being used because its implementation is too expensive. Implementation of the module in the smart card was not an easy task, and after the issuance of the card it was impossible to remove the module without destroying the card. The advantages of TAB modules are the strong connection with the chip contacts and a small empty space inside the module. Chip-on-Flex module is today's most commonly used module because its implementation on the card is very simple and cheap. But the disadvantage of the chip-on-flex module is in the chip and its connection with the contact area.

To connect the contacts, micro wires are used, that also need the protection, therefore a larger space for the module is required that some cards will not be able to support. Lead-frame module is actually a combination of TAB modules and chip-on-flex modules, i.e. their combined benefits with the lowest cost of production. The contact surface is made in accordance with ISO 7816-2 standard, which determines its size and standing of the contacts. With the development of the smart cards and their increasing prevalence, it was necessary to define specifications for manufacturers. So, various organizations have defined standards. Some of the best known standards are ISO / IEC 7816, Global System for Mobile Communications - GSM and Europay, MasterCard and Visa - EMV. From the IT point of view, the key component of the smart card is microcontroller. It controls, drives and controls all the electrical operations of the card. The main components of the microcontroller are processor and memory (Random Access Memory - RAM, Read-only memory - ROM, Electrically Erasable Programmable Read-Only Memory - EEPROM, and Flash). It has an interface that is connected to the Input / Output (I/O) contact for the communication with the outside world. By using the Central Processing Unit (CPU) on the card itself, a variety of applications can be put on the card for the usage in financial and mobile industries. Standard microcontrollers are larger and more expensive and have more functions that are not needed in the smart card which is why the smart card microcontrollers are made according to the special specifications. These microcontrollers have only certain functions dependent on the type of card, and are smaller and cheaper. ISO / IEC 7816 standard is divided into 14 parts, of which parts 1, 2 and 3 define the physical structure of the contact card, while parts 4, 5, 6, 8, 9, 11, 13 and 15 define the logical structure of the contact and contactless cards. ISO / IEC 14443 and ISO / IEC 15693 standards define the physical characteristics and the interface of the contactless cards, the radio-frequency (13.56 MHz) and communications protocols. These standards are commonly used for public transportation cards and for key cards [1]. ISO / IEC 7501 describe standards for cards that are used for identification such as electronic passports (ePassporte).

3. Cryptography

3. *Kriptografija*

Cryptography is the science of secret writing with the goal of hiding the meaning of a message. It is part of the cryptology – science of the secret communication along with the cryptanalysis – science of breaking cryptosystems, i.e. finding a meaning of the message without knowing the key [2].

Cryptography itself splits into two main branches:

a) symmetric cryptography (or secret-key cryptography) where parties in communication process share the same key by which message can be encrypted and decrypted. The key must be known only to sender and receiver of the message and must remain secret to everyone else.

b) asymmetric cryptography (or public-key cryptography) where parties in communication process have two different keys: public key for encryption which can be published to everyone and private key for decryption which must be known only to receiver of the message.

Cryptography is often asked to provide these goals:

a) confidentiality – service used to keep the information secure from everyone except those authorized to have it,

b) authentication – service which addresses the origin of a message. It should be possible for a receiver of the message to ascertain its origin, where intruder should not be able to mask himself as an original sender.

c) integrity – service which addresses the unauthorized alteration of data. It should be possible for a receiver of the message to verify that it has not been modified in transit and to detect data manipulation by unauthorized parties. An intruder should not be able to substitute a false message for a legitimate one.

d) nonrepudiation - a service which prevents an entity from denying previous commitments or actions. A sender should not be able to falsely deny later that he sent the message [3][4].

4. Digital signature and digital certificates

4. *Digitalni potpis i digitalni certifikati*

Digital signature is asymmetrically encrypted message digest and it is used for the purpose of authentication of the sender, to preserve the integrity and nonrepudiation of sending messages. The sender first calculates the message digest by conducting the plaintext through some hash algorithm. Message digest is then encrypted by using a private key of the sender, which forms a digital signature. When used for the purpose of authentication, asymmetric cryptographic algorithm uses a private key for encryption and public key for decryption. Then the original message and the digital signature together are sent over the network to the recipient, who is also calculating message digest by conducting the plaintext through the same hash algorithm as the sender. By using the sender's public key, the recipient decrypts digital signature which leads to the message digest created by the sender. If a message digest calculated by the recipient is equal to the one created by the sender, digital signature is valid and the message is unchanged.

To ensure the credibility of a public key to verify a digital signature, digital certificate was introduced. Digital certificate is actually a certificate issued by the certification authority and it confirms that the owner of the certificate has a private key corresponding to the public key contained in the certificate. It binds identity with a public key and properties of public/private keys along with some protocols assure the ownership of private key. There are several types of certificates, but the best known and most widely used is the X.509 v3 standard [5].

5. Public key infrastructure

5. *Infrastruktura javnog ključa*

Public Key Infrastructure or simply PKI provides a secure binding of public keys and users. The objective of establishing PKI was to find out how to design an infrastructure that allows users to establish certification paths which contain more than one key. The purpose of PKI is to establish trust in public keys and therefore enable and support secure exchange of data, documents and values (such as monetary instruments) in unsecure environments (such as internet) between entities. PKI enables the establishment of the confidential hierarchy and risk management.

Creation of certification paths, commonly called chains of trust, is established by Certification Authorities or CAs. A certification path is a sequence of CAs. CAs issue, revoke and archive certificates. In the hierarchical model, trust is delegated by a CA when it certifies a subordinate CA. Trust delegation starts at a root CA that is trusted by every node in the infrastructure. Trust is also established between any two CAs in peer relationships (cross-certification) [6].

6. Security risks

6. *Sigurnosni rizici*

In the process of authentication of a person on a computer or information system, confidential information is transmitted between that person and the authentication system, over some communication channel. This opens up the possibility of several attack vectors:

a) identity of the person who authenticates,

b) confidential data that is being transmitted during the authentication process,

c) insecure communication channel through which data is transmitted.

Regarding the environment and primarily due to the weakness of unprotected authentication infrastructure, it is necessary to analyze the attack vectors and devise possible solutions.

7. Proposed security concept

7. *Predloženi sigurnosni koncept*

7.1. Network infrastructure

7.1. *Mrežna infrastruktura*

The server which we used has Microsoft's virtualization tool Hyper-V installed, which allows multiple operating systems to be installed on one physical computer. Two virtual servers are created, running Windows Server 2012 R2. The first one has Domain Controller (Active Directory Domain Controller - ADDC) installed, Domain Name System (DNS) and Certification Authority (Active Directory Certificate Services - ADCS), and the other one has Remote Access installed. Laptop and desktop computer are running Windows 7 Professional. Connecting all computers into one network has been enabled with a switch which has eight ports, and to go out to the internet a router is used that is assigned by ISP. ActiveClient version 6.2 software has been installed on all computers, which can read, write and delete certificates on the card. Network infrastructure can be seen in Figure 1.

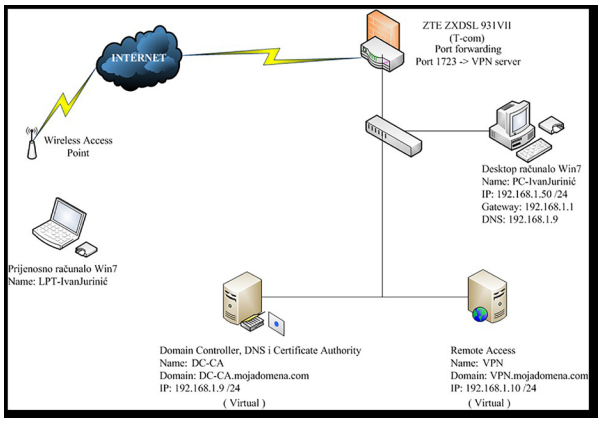

Figure 1 *Network infrastructure*

Slika 1 *Mrežna infrastruktura*

On the server that we called DC-CA, domain "mydomain.com" has been created and two users - one of which has administrative and the other one has limited rights. For users who have limited rights under "Account Options" option "Smart card is required for interactive logon" is set and is marked with the option "Allow Access" under "Network Access Permission". This stipulates that the user must have a smart card to enter the computer. Access is given via remote access. In Group Policy Management Editor under "Public Key Policies" option "Certificate Services Client - Auto-Enrollment" is enabled which enables automatic allocation of certificates to clients who are in a domain environment. Certification Authority has been configured via ADCS service with root CA certificate, which allows the signing of all other certificates. Routing and Remote Access service has been installed on the VPN server and then through the Remote Access Wizard a VPN access has been defined, and the router has been configured to forward the Point-to-Point Tunneling Protocol (PTTP) towards VPN server on port 1723.

7.2. Writing certificate on the card

7.2. *Zapisivanje certifikata na karticu*

For the certificates to be able to be written on the card, Personal Identification Number (PIN) needs to be created on the card. When the card is first inserted into the reader, a pop up window pops out requesting PIN registration to be used for further authentication. After entering the PIN, a card is ready to read, write and delete certificates. On the CA service, certificates based on the templates "Enrollment Agent" and "Smartcard Logon" need to be created. "Enrollment Agent" allows an administrative user to write the certificate on the card for other users, and "Smartcard Logon" enables user authentication via smart card. To create the certificate that will allow an administrative user to write on the card, user needs to right-click on "Certificate Templates" and choose "Manage". In the new window "Certificate Templates Console" it needs to duplicate template "Enrollment Agent" and set it as follows:

- In the "General" tab enter the name of a new template "SmartCard Logon User" and select the option "Public certificate in Active Directory",
- In the "Request Handling" tab under "Purpose" select "Signature and Encryption",
- In the "Cryptography" tab choose "Requests must use one of the following providers:" and select "ActiveClient Cryptographic Service Provider",
- In the "Security" tab add administrative user and mark the Read, Write, and Enroll option,
- In the "Extenstions" tab add "Encrypting File System" and "Server Authentication",
- In the "Issuance Requirements" tab mark "This number of authorized signatures" and under "Application policy 'in the drop-down menu select" Certificate Request Agent ".

After creating templates, in CA service, by right-clicking on the "Certificate Templates" choose "New" and "Certificate Template to Issue", and then "Enrollment Agent SmartCard" template and "SmartCard Logon User" template. When templates are created, it needs to request those certificates from client computers, so that they can be issued to users. On the domain computer, it needs to be enrolled as an administrative user and ask "Enrollment Agent SmartCard" certificate. Then Microsoft Management Console (MMC) starts and adds Certificates snap-in for the current user. Using Certificates - Current User tools, all certificates that are stored on the computer for certain user can be seen. For the certificate to be requested from a CA, there must be right mouse click on the "Personal", then "All Tasks" and "Request New Certificate". Certificate "Enrollment Agent SmartCard" needs to be selected and installed on the computer.

After installing certificates, administrative user can request certificates for other users and write them down on a smart card. In the MMC tool Certificates - Current User > right mouse click on the "Personal" > "Advanced" > "Enroll On Behalf of ...". Certificate that has the ability to sign certificates must be selected i.e. certificate that is just created. After selecting administrative certificate, choose a certificate that will be written on a card or "SmartCard Logon User". Then select the user for whom the certificate is issued, and finally enter the PIN number of the card.

7.3. User authentication

7.3. *Autentikacija korisnika*

For the user to be able to log in to his account, ActiveClient must be installed on the computer, which allows reading the certificate from the smart card. When applying to the account a new icon appears and below it requests "Insert a smart card." (Figure 2).

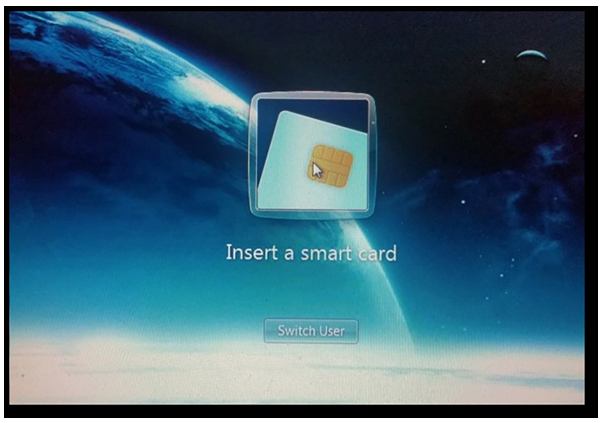

Figure 2 *"Insert a smart card" request*

Slika 2 *Zahtjev za umetanjem pametne kartice*

When the card is inserted into a reader, PIN that is set on the first usage of the card is required (Figure 3).

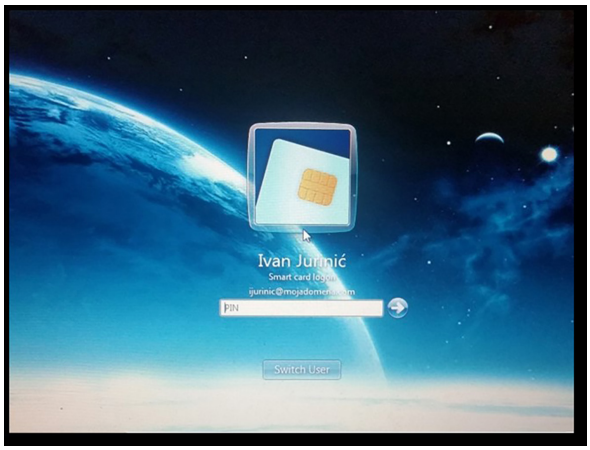

Figure 3 *Entering PIN number*

Slika 3 *Unos PIN-a*

7.4. Data encryption by using Encrypting File System

7.4. *Enkripcija podataka korištenjem sustava Encrypting File System*

Data encryption is performed by using the Encrypting File System or EFS, built into Microsoft operating systems from Windows 2000 system further on. Some of the main features of EFS are:

a) control: user has control over permissions to read the document,

b) practicality: data is encrypted when not in use, but is automatically unlocked when owner opens it,

c) simplicity: to remove the encryption from a document or folder "Encrypt contents to secure day" needs to be marked in the settings.

Once the file is encrypted, in "Advanced Attributes" window, by clicking on "Details", option appears to set who has the access to the file which can be defined by the document owner.

7.5. User authentication through VPN

7.5. *Autentikacija korisnika preko VPN-a*

In order to enable connection between the remote client computer and VPN server, VPN connection needs to be set up on the client laptop, and Computer certificate needs to be installed on the VPN server with which the client checks the server certificate before establishing a connection.

Over MMC console on the VPN server Certificates tool for the local computer (Certificates-Local Computer) needs to be added and a CA Computer certificate needs to be requested. On a laptop in the "Network and Sharing Center" set up a new connection via "Set up a new connection or network". By clicking this option, a wizard starts which makes it easy to set up VPN on computer. In the new window select "Connect to a workplace". In the next window, select the connection method "Use my Internet connection (VPN)" and then set the basic settings to establish a connection. In the "Internet address" field enter the public address that is on the router and mark "Use a smart card" and "Do not connect now; just set it up so I can connect later". After setting the basic settings via the wizard, VPN advanced settings in "VPN Connection Properties" needs to be set up. In the "Security" tab, by clicking on the "Properties" open a new window "Smart Card or other Certificate Properties", which defines certificate that authenticates VPN server. In "Connect to these servers:" field, the name of the server with its domain has to be given, in this case VPN.mydomain.com, and in the "Trusted Root Certification Authorities," select domain root certificate "MYDOMAIN-DC-CA-CA". When starting VPN connection, system requires cards' PIN to be able to begin establishing connection and after the entry of the PIN, VPN connection should be established.

8. Conclusion

8. *Zaključak*

On the newly built network infrastructure, by using a smart card, concept of double authentication is demonstrated, i.e. the user requires smart card reader and a PIN code for authentication and encryption of data. The procedure of writing the certificate on the card, and the usage of a smart card on the computer has been described in detail. A procedure of adjusting the VPN on a computer is also described. This concept provides a certain level of security with regard to authentication and data security, but it is weak to certain attacks such as „evil maid“ attack.

9. REFERENCES

9. *REFERENCE*

[1] W. Rankl and W. Effing , "Smart Card Handbook,“ 4th ed., John Wiley & Sons, 2010.

[2] C. Paar and J. Pelzl, „Understanding Cryptography“, Springer, 2010., pp3.

[3] A. Menezes, P. Van Oorschot and S. Vanstone, „Handbook of Applied Cryptography“ CRC Press; 1st ed., 1996., pp. 4.

[4] B. Schneier, „Applied Cryptography“, 2nd ed., New York : John Wiley & Sons, 1996.

[5] Technet.microsoft.com, „Understanding Digital Certificates“. URL:
https://technet.microsoft.com/en-us/library/bb123848%28v=exchg.65%29.aspx.

[6] M.Y. Rhee, „Internet Security : Cryptographic Principles, Algorithms and Protocols,“ John Wiley & Sons, 2003., pp.201.

AUTORI · *AUTHORS*

Ivan Jurinić
M.I.T. has attended Zagreb University of Applied Sciences where he got his master of information technologies, computer network design and implementation. His main interest focus is on computer networking and information security. He was working as the senior IT technical support officer at the Central Registry of Affiliates (REGOS), at the Department of information and technical support. He is currently working as a system administrator at IDE3.

Correspondence
ivan.jurinic989@gmail.com

Roman Domović
Prof. is a senior lecturer at the Zagreb University of Applied Sciences at the Department of Information Technology and Computing. He went to X. mathematical gymnasium where he graduated physics, after which he attended University of Zagreb and graduated in the field of Information sciences and Phonetics. At the same university he earned his doctoral degree in the field Information and Communication sciences. His research interests are applied cryptography, classical cryptography and information warfare.

Correspondence
rdomovic@tvz.hr