Research Paper - Smart Cards

Due on August 25th, 2019

Computer Organization & Programming

CS550WS—Summer I

Ed Banduk

Daniel Kadyrov

1 Introduction

Smart cards, also known as, chip cards, and integrated circuit cards are physical devices with integrated circuitry that allows for electronic authorization. The embedded electronics, different and more secure than the magnetic strip found on a credit card, transmit information through contact or without for their respective use. The most popular applications are for credit and debit cards, financial applications, public transportation cards, personal identification and authentication, as well as mobile phones (SIM cards).

2 History of the Smart Card

The first patents for an electronic identification device were filed by Helmut Gröttrup and Jürgen Dethloff in 1968 and 1969. Gröttrup is credited for developing the principals behind the smart card while participating in creating identification switches for German petrolium stations. In 1974, Roland Moreno began developing a microchip integrated in a plastic card which he called *la carte à puce*, translated as the chip card, and demonstrated its potential for electronic financial transactions in 1976.

It took almost a decade for the smart card to be first adopted - mainly due to high initial costs. The first implementation of the smart card was in 1983 by France Télécom as a payphone payment card, the Télécarte. In 1992, French banking institutions integrated a microchip into the Carte Bleue, or blue card, which required users to insert the card into a merchant's point of sale and then enter a personal identification number, PIN, before the transaction could commence. At the same time, smart cards were adopted for subscriber identity modules, SIM, to be used in mobile-phone equipment on global system for communications, GSM, network. Now, smart cards are widely available in a variety of applications (Davison, 2012).

3 Technology

The contact method of the contact card uses gold-plated contact pads that provide electrical connectivity when inserted into a reader. The power is supplied by the card reader. The standards ISO/IEC 7810 and ISO/IEC 7816 define the physical characteristics, the electrical characteristics, the communication protocols, and the basic functionality for contact cards (Rankl, 2003).

The contactless method is used through radio frequency, RF, induction which uses a magnetic field to transfer energy through electromagnetic induction.The RFID data is alphanumeric but can also provide graphical images, photographs,

and even video (Englander, 2014). The contactless interface is standardized in ISO/IEC 14443-4. Hybrid cards are also manufactured that feature both contact and contactless methods.

A USB protocol was also developed to allow a smart card to be used a security token in authentication and encryption applications. The protocol is defined by the chip card interface device, CCID, and sometimes contains a SIM card in addition to the USB dongle (USB, 2019). Some CCID providers include Yubico and Advanced Card Systems.

The smart card management system, SCMS, and the credential management system, CMS, are the systems for managing smart cards. These systems have protocols to register and unregister a card, issue a card to a holder, initiate the card, activate and deactivate the card, lock and unlock, revoke, retire, back up, restore, and delete. They also oversee connection and transfer of information from the smart card and the smart card reader (Rankl, 2003).

4 Applications

Within finance, the Europay MasterCard Visa, EMV, became a payment standard used with contact cards. Although the three companies created the standard, it is now managed by EMVCo and is used by other financial companies like American Express and Discover. The United States adopted the ENV standard for its credit and debit cards in 2014 because of increased identity theft culminating in the Target credit card leak.

Some smart-cards utilize electronic purse systems, also known as stored-value cards, SVC, which store and transmit monetary value offline. Unlike debit or credit cards, which require deposit or credit with an issuer and an account holder, stored-value cards operate with prepaid funds and the information is stored in a closed loop system within the card as binary. Beyond the use of stored-value cards in laundry mats and gift cards, the stored-value smart card method is also used on a variety of public transportation systems including the New York and New Jersey Path Train.

Smart cards are used heavily in identification purposes since they are secure, tamper proof, and can provide a volume of information during use. The United States Department of Defense uses the Common Access Card, CAC, that is a smart-card featuring a public key infastructure, PKI, which is a digital encrypted certificate issued by a PKI provider. Countries such as Turkey, Argentina, Estonia, Belgium, Spain, and Pakistan all have implemented smart-card systems within their government issued identification.

Smart cards are found in cellphones that operate on GSM networks.

5 Benefits and Disadvantages

The benefits of the smart-card lie in ability to store and transmit a variety of information in a portable, replaceable, reliable and secure method. The size of the smart-card contact has been standardized but its applications range from the size of a SIM card chip to a credit card. Since the chip is integrated into a plastic card, they are relatively cheap to manufacture and replace if lost. The security of the card is the main reason why it has been heavily adapted by financial institutions and governments. The variety of information held on the card is encrypted and does not need online access to be decrypted. With the adoption of contactless technology on the cards, a smart-card can be programmed to only allow transactions in the vicinity of another paired device such as a mobile phone.

There are also disadvantages of the smart-card. Although the plastic material used to manufacture the card makes it cheap and replaceable it is a brittle material that susceptible to breaking and the integrated chips may demagnetize or erode over time. The production, use, and disposal of plastic is also environmentally unfriendly. Although smart-cards have been adopted for their security, there are still security attacks on the systems that manage them. Government use of smart-cards for identification or authentication purposes also have raised flags for privacy and right issues.

6 Conclusion

Smart-cards, first developed in 1968, have become widely adopted in a variety of industries for their ability to store and communicate a large amount of data in a cheap, replaceable, and secure device. The standardized size is found in credit-cards and mobile phone SIM cards and the information is transmitted to a receiver by contact through gold-plated contact pads or contactless through RFID technology. Since the data is encrypted and transmitted offline, the technology has been widely adopted for financial transactions, identification, and authentication.

References

[1] Davison, P. (2012, May 04). Roland Moreno: Inventor who missed out on global recognition for his. Retrieved from https://www.independent.co.uk/news/obituaries/roland-moreno-inventor-who-missed-out-on-global-recognition-for-his-computer-chip-smart-card-7715617.html

[2] Rankl, W., Effing, W. (2003). *Smart card handbook*. Chichester: Wiley.

[3] Englander, I. (2014). *The architecture of computer hardware, systems software, & networking: An information technology approach* (Fifth ed.). Hoboken, NJ: John Wiley & Sons.

[4] Specification for Integrated Circuit(s) Cards Interface Devices. Retrieved from https://usb.org/sites/default/files/DWG_Smart-Card_CCID_Rev110.pdf