A Smart Card Mediated Mobile Platform for Secure E-Mail Communication

Geylani Kardas
Ege University International Computer Institute, 35100, Bornova, Izmir, TURKEY
geylani.kardas@ege.edu.tr

Ebru Celikel
University of Texas at Dallas, Richardson, TX 75083, USA
ebru.celikel@utdallas.edu

Abstract

We introduce a mobile e-mail communication platform which employs smart card to provide authentication and confidentiality for e-mail exchange. The security of the system is incorporated by PGP based asymmetric encryption. Smart card is used to store the mail account information, as well as PGP private key of each user to offer further security, authentication and mobility to the system. The real contribution of our scheme is the absorption of all the complexity of PGP to a PIN based smart card by causing no compromise on the security of PGP. We use JavaCard technology in real life implementation of the proposed platform.

1. Introduction

In this study, we introduce a mobile platform in which smart cards are employed to provide secure e-mail communication in client/server architecture based IT systems. The platform we design incorporates PGP (Pretty Good Privacy) [3] cryptographic privacy and authentication tool to implement message transmission. To achieve a high level of security, our scheme also utilizes the mobility, flexibility, reasonable data storage and ability to provide user authentication facilities of the smart card.

Although strong in some aspects, none of the similar studies [1 and 4] provides a concretely defined and fully-implemented smart card system considering requirements of the distributed messaging systems. We believe that the smart card mediated platform we propose provides realization of such secure messaging systems by specifying all architectural components needed, providing the concrete software infrastructure which includes those predefined components and utilizing state of the art smart card and security technologies.

2. System Architecture

The overall architecture of the system we introduce is given in Figure 1. Architecture includes components such as smart card media, CADs (Card Acceptance Devices), card terminals, e-mail and encryption key servers. Functionality of each component is logically unique. However, some of them may reside in the same hardware in real-life implementations.

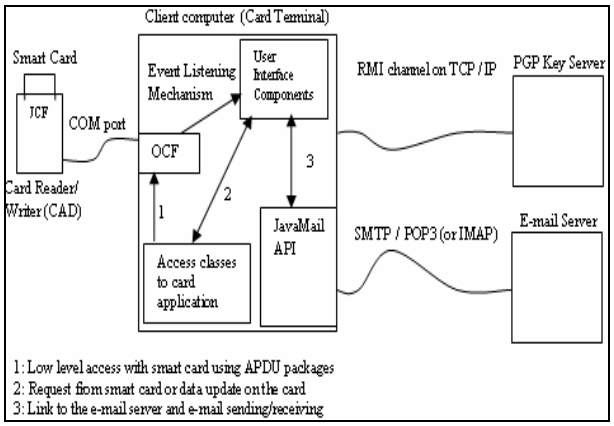

Figure 1. The architecture of the platform

An e-mail client computer is also a smart card terminal and is connected to a card reader / writer unit via COM port. E-mail client software of this machine utilizes the OCF (OpenCard Framework) [2] library to control smart card applications. OCF utilization provides off-card programs to communicate with smart cards over APDU protocol. APDU (Application Protocol Data Unit) [5] is a low-level protocol and it requires card application programmers to deal with primitive and limited packet structure of the smart card communication model. For this reason, we designed and implemented a smart card client software which prepares the card environment on computer, manages secure card sessions and communicates with smart cards via APDU protocol for high-level applications. Smart cards that we use in our system are JavaCards

and they store personal mail account information (user id, password and other connection parameters) and user PGP private keys. On-card system software is developed by using JCF (Java Card Framework) [5].

Smart card terminals act as clients in system's Java RMI (Remote Method Invocation) based protocol. The RMI makes it possible for an object running on a Java VM (Virtual Machine) to call and use the methods of an object on another Java VM. In here, related remote objects reside in encryption key servers (e.g. PGP servers) within the system. When a user wants to send an encrypted e-mail to another system user, he should access the PGP public key of the receiver. Requested keys are obtained from these key servers over RMI channel. Employing the public key through a public key ring of the PGP service would add enhanced security to the system defined. Card terminals communicate with RMI remote components to retrieve those keys over serialized structure of the RMI protocol. The protocol uses parameter marshalling so public key object is transmitted over the network as serialized and protected against interfering third persons.

The e-mail client software in our design utilizes JavaMail API (Application Programming Interface) to send and receive e-mails. User interface components provide a user friendly GUI (Graphical User Interface) to use the e-mail client software. SMTP and POP3 (if the e-mail server uses IMAP, then IMAP) are used for encrypted message sending and receiving, respectively.

A user requesting to download e-mails from an e-mail server and read them places the smart card containing the PGP private key into the card terminal. Event listening mechanism triggers the e-mail client program together with APDU to initiate the communication with smart card. The user is requested to enter a PIN (Personal Identification Number) to initiate the secure card session. After successful PIN entry, smart card authentication is ensured and connection information to the e-mail server is transferred from the card.

Then, incoming e-mail(s) are downloaded from the server. Since each e-mail was previously encrypted with PGP public key of the corresponding user, they now need to be decrypted. For decryption, PGP private key of the user is required. At this point, the e-mail client initiates a new transmission session with the smart card to request the user's private key from the card. Since the authentication was already ensured in the previous session with the card, the card transfers the requested private key in APDU packages to the client. Upon obtaining the PGP private key, incoming e-mails are decrypted to be open to the receiver.

E-mail sending itself can also be performed in this card session. For that, the user encrypts his message using the PGP public key(s) of the receiver(s) and sends the encrypted message via the related protocol. The e-mail server then sends the encrypted message to the appropriate user(s).

Smart cards, we employed for our real life implementation, are GemXpresso 211/PK model JavaCards manufactured by Gemplus. Our card software and permanent data objects (such as PGP private key) needed approximately 10K EEPROM of smart cards. Gemplus GCR410 serial, card read/write unit has been used as CAD. We used JCF 2.1 in smart card software development and OCF 1.2 library for smart card communication.

3. Conclusion and Future Work

In this study, we introduce a mobile e-mail communication platform where smart card is employed to provide authentication and confidentiality for e-mail exchange. Employing smart card in our scheme is useful in two ways: The storage capacity of the card is large enough to allow us store the PGP session keys securely. Furthermore, the mobility feature provided by the card is the source of portability for our system.

Our studies continue for the addition of new features (such as secure file transfer and use of digital signature) to the current implementation.

4. References

[1] J. Rees, and P. Honeyman, "Webcard: A Java Card Web Server", *IVth CARDIS*, Bristol, 2000.

[2] OpenCard Consortium, *OpenCard Framework 1.2 Programmer's Guide*, IBM, Germany, 1999.

[3] P. R. Zimmermann, *The Official PGP User's Guide*, MIT Press, USA, 1995.

[4] R. Brinkman, and J-H. Hoepman, "Secure Method Invocation in JASON", *5th Smart Card Research and Advanced Application Conference*, USA, 2002.

[5] Z. Chen, *JavaCard Technology for Smart Cards Architecture*, Addison - Wesley, USA, 2000.