Proposal of an Authentication Method "SPAIC" using a Non-contact Type IC Card

Changjun Shu* Hidekazu Suzuki† Akira Watanabe‡

Graduate School of Science & Technology, Meijo University
1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502, Japan
Tel: +81-052-838-2406, Fax: +81-052-838-2406,
E-mail: * m0632019@ccmailg.meijo-u.ac.jp
†m0641506@ccmailg.meijo-u.ac.jp ‡wtnbakr@ccmfs.meijo-u.ac.jp

***Abstract*— When important information is exchanged in a client-server system, it is quite essential to perform reliable authentication and encryption. In such a situation, a method using an IC card that stores unique user information has been widely used. Until recently, the security of communication between an IC card and a client has not been a critical concern because contact type IC cards have been used in most cases. However, now that non-contact type IC cards are expected to be spreading in the near future, secure communication between an IC card and a client is considered to become a serious concern. Although there exists a method whereby all IC cards and clients use a common key to realize secure communication, there is a concern that secret information is easily leaked from the client terminal. To solve this problem, we propose in this study a protocol called "SPAIC". Presuming that a non-contact type IC card is used, SPAIC can deliver the important information from a server to a client that has no initial information so that there exists no risk of information leakage.**

I. INTRODUCTION

Along with the development of the Internet, user's demand for exchanging information with a remote server through a client terminal has been increasing. When exchanging important information through a client-server system, secure authentication and encryption are indispensable. From the past, various methods for secure information deliveries by way of authentication and encryption have been studied [1]-[5]. Recently, the needs for having access to the server from different client terminals are increasing, and in this environment, too, secure communication by authentication and encryption is required.

To meet such requirements, the method that a user holds an IC card is paid attention [6], [7]. An IC card can executes simple transaction with its CPU and memory, and can also store the essential information for authentication securely because of its tamper-proof character [8]. Thus it is possible to execute authentication and secure communication without any identification of a user in a client terminal. That means, the user can choose any client terminals freely, and also prevent the leakage of user's information from terminals. In recent years, the non-contact type IC card is attracting much attention because of its convenience that data can be exchanged by just putting an IC card near an IC card reader/writer. It is expected that the market of the non-contact IC card will be increase [9].

As the authentication method using an IC card, user's authentication to identify the owner of the IC card is also required, besides the authentication between the client and the server. The principal of the method is that an IC card checks the user information such as a password received from a client with the one registered in the IC card [10]. In the case of a contact type IC card, the security of communication between the client and the IC card has never been a big concern because they are connected tightly. But, in the case of a non-contact type IC card, cipher communication between the IC card and the client is needed to ensure the authentication safely. As for the cipher communication between the IC card and the client, a conventional method of using a Pre-Shared Key (PSK) is defined in JICSAP [11]. However, since all IC cards and clients possess the same key, there is a risk of information leakage from the side of the client. Moreover, when a leakage occurred, it could affect the entire system.

Since a client does not have tamper-proof character unlike the case of IC card in general, it is expected that a client does not have any secret information at all. Therefore, the purpose of this study is to find out what kind of initial information should be stored in an IC card, a client and a server beforehand, and what kind of procedure should be performed to execute the authentication and encryption safely.

In this paper, we propose a protocol named "SPAIC" (Secure Protocol for Authentication with IC card), which enables deliveries of important information from a server to a client that has no initial information using a non-contact type IC card.

In SPAIC, the massage from the client to the IC card is encrypted by a public key of the IC card. Then the message from the IC card to the server is encrypted by the public key of the server stored in the IC card via the client. Furthermore, the common key is generated with the Diffie-Hellman key exchange between the client and the server, which is used for the secure delivery of the important information [12]-[15].

We describe the conventional system and their associated problems in Chapter 2, our proposed system in Chapter 3, the results of our evaluation in Chapter 4 and the conclusion of this paper in Chapter 5.

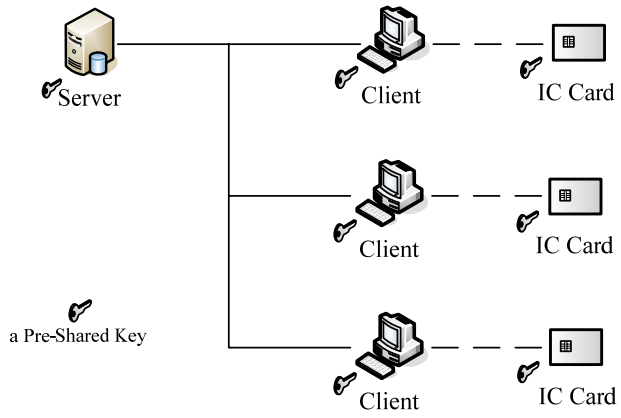


Fig. 1. Conventional authentication method

II. Conventional Systems and its Associated Problems

In most of the conventional systems, contact type IC cards are used in a manner that they are inserted into the client terminal. Then, the IC card and the client are regarded as an integrated unit and consequently, no encrypted communication is usually conducted between them.

However, in the case where a non-contact type IC card is used, encryption becomes necessary because the communication between the IC card and the client is performed wirelessly. To cope with the situation, a Pre-Shared Key (PSK) is possessed by all IC cards and client terminals for encrypted communication in most of the conventional systems (Fig. 1). In this method, an encryption key for the encrypted communication between the IC card and the client is dynamically generated by using this PSK.

However, in the PSK method, it is necessary to have the client possess secret information, and thus, there is a risk that information is leaked from the client. Furthermore, since the same PSK is used in the entire system, if and when this PSK is leaked from any client terminal, the impact could extend to the entire system. Thus, the PSK for all IC cards and clients needs to be periodically updated to ensure the system safety, and as a result, its administrative load becomes quite heavy.

III. Our Proposed Method

In our proposed method, a model in which the client has no secret information is defined. Under this condition, all the important information such as the encryption key (which should be kept confidential to the third party) is delivered from the server to the client safely and securely.

A. System Model Assumed and Conditions

Fig. 2 shows the system model assumed in this study. The user holds an IC card possessing personal information.

Each client terminal is equipped with an IC card reader, which performs user authentication by using the IC card issued to each user. After authentication of the user, mutual authentication is performed between the IC card and the server, and important information is delivered to the client.

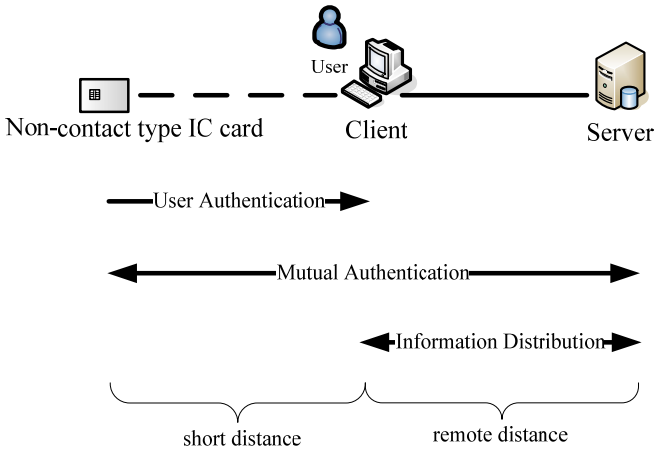


Fig. 2. System model assumed in our proposal

In this system, the following conditions are assumed.

(1) Non-contact type IC card is used, in view of its wide use in future.
(2) The information stored in the IC card will never be leaked because of its temper-proof character.
(3) The distance between the IC card and the client is so short that the user can be easily identified, and no man-in-the-middle attack is possible.

B. User Authentication Method

As the method of user authentication, a password is usually used. In the case where a higher security is required, it is combined with the biological authentication method. There are two types of authentication methods, depending on the difference in the places of storing information. One type is the SERVER-type authentication, which performs authentication by using information stored in the server, and the other type is the CLIENT-type authentication, which performs authentication by using information stored in the IC card (Fig. 3).

The SERVER-type authentication is an end-to-end user authentication, which performs a direct authentication between the user and the server. The authentication information acquired by the client is transmitted to the server through the IC card for the purpose of authentication. This method has an advantage that the processing load of the IC card is reduced because both the user authentication and the IC card authentication are performed on the server side. However, since the information of all users is administered on the server side, the structure for administration of the server is very important. For this reason, adoption of various measures such as a large-scale temper-proof hardware or elaborate equipment is required.

The CLIENT-type authentication is a link-by-link authentication where authentication between the user and the IC card and that between the IC card and the server are performed independently. The authentication information acquired by the client is sent to the IC card, in which user authentication is performed, and thereafter, the IC card authentication is done between the IC card and the server. In

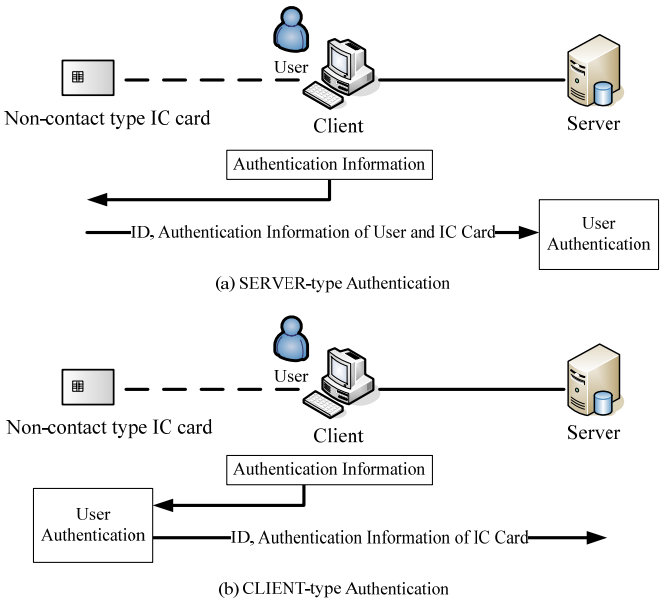


Fig. 3. User authentication methods

this authentication method, the IC card authentication in the server serves also as the user authentication. This method has an advantage that user authentication information such as the password and the biologic information can be safely stored because the IC card has a temper-proof character. On the other hand, the processing load on the IC card gets heavier.

By either of the authentication methods, personal authentication can be performed safely. In this paper, we adopt the CLIENT-type authentication method, in which the user authentication and the IC card authentication can be treated independently and the safety can be achieved more easily.

C. *Relationships of Authentications in SPAIC*

In SPAIC, the client has only the programs related to authentication operation [16] and information deliveries and possesses no secret information required for authentication. Accordingly, there is no possibility of secret information being leaked from the client side.

In SPAIC, the IC card, the client and the server are assumed as independent work units, and a circular authentication is performed among them. Fig. 4 shows the relationships of authentications performed in SPAIC. The arrow indicates the direction of authentication. As the user operates the client, we regard them as an integrated unit. The IC card performs user authentication by using the password and/or biologic information. The server authenticates the IC card by verifying the digital signature created from the private key of the IC card [17]. The client authenticates the server by verifying the digital signature created from the private key of the server.

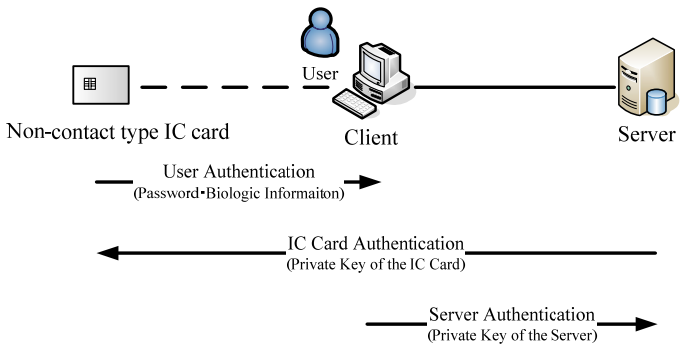


Fig. 4. Relationships of authentications

By implementing the above three paths, the authentication between the client and the server is performed.

D. *Definitions of Signs*

Below-mentioned are the definitions of all the signs used to explain our proposed method.

uID: User ID
PW: Password
T: Biological information template
PSK: Pre-shared key (used in a conventional model)
PrI, PuI: Private key of the IC card, Public key of the IC card
PrS, PuS: Private key of the server, Public key of the server
Ni, Nr: Random Number
DH1, DH2: Diffie-Hellman exchange key
K: Common Key
Ci, Cr: Cookie
$E_Y[X]$: X is encrypted with key Y
$S_I(X)$: Digital signature to X with the IC card
$S_S(X)$: Digital signature to X with the server
Key_REQ: Key-Request packet
Key_RES: Key-Response packet
Cookie_REQ: Cookie-Request packet
Cookie_RES: Cookie-Response packet
CertUser_DIST: Distribution packet of user authentication information
SignIC_DIST: Distribution packet of IC card signature information
Info_DIST: Distribution packet of information
SignMS_DIST: Distribution packet of server signature information

E. *Initial Information at Each Terminal*

Table 1 shows the initial information possessed by the PSK method and SPAIC. For user authentication, a password

TABLE I
COMPARISON OF THE INITIAL INFORMATION POSSESSED BY THE PSK METHOD AND THE SPAIC METHOD

	PSK Method	**SPAIC**
IC card	uID PrI PuS PW T ***PSK***	uID PrI PuS PW T ***PuI***
Client	***PSK***	—
Server	uID PrS PuI	uID PrS PuI

and/or biological information is supposed to be used. In the PSK method, ID (uID) unique to each IC card, a private key of the IC card (PrI), a public key of the server (PuS), a password (PW), and a biological information template (T) are stored in the IC card held by each user, whereas ID (uID) of each IC card, a private key of the server (PrS), and a public key of the IC card (PuI) are stored in the server. For the encryption of communication between the IC card and the client, PSK is possessed by all IC cards and client terminals.

In the case of SPAIC, a public key of IC card (PuI) (instead of a common key (PSK) of the PSK method) is stored. All other initial information is the same. The client has no initial information. The server possesses ID (uID) of each IC card, a private key of the server (PrS), and a public key of the IC card (PuI). The initial information shown in Table 1 is created on the side of the server all together and the issuance of the IC card has been done off-line in advance. As the public key (PuI) and the private key (PrI) of the IC card are created simultaneously, the storing of this information in the IC card does not increase the administrative burden.

F. Outline of the SPAIC Operation

Fig. 5 shows the outline of the SPAIC operation. The authentication procedures of SPAIC consist of three steps.

First, the IC card performs user authentication with the following procedures. In order for a user to have access to the server, the user should hold up his IC card near a client. Then, a connection with the client is established, and the public key of the IC card (PuI) and the public key of the server (PuS) are delivered from the IC card to the client. Then, the password input window is displayed on the client side. The user inputs user authentication information such as the password (PW) and/or the biological information (T) to the client. The client encrypts the user authentication information with the public key of the IC card and also generates a Diffie-Hellman exchange key (DH1) and send them to the IC card. The IC card takes out the user authentication information (PW and/or T) by using the private key of the IC card (PrI) and performs user authentication by comparing the information with the secret information stored in the IC card. Through these procedures, the client which the user is using is authenticated indirectly at the same time.

The next step is the authentication of the IC card by the server through the following procedures. The IC card adds a digital signature to the DH exchange key 1 by using the private key of the IC card (PrI) and delivers it together with the user ID (uID) to the server via the client. The server verifies the digital signature by reading out the corresponding public key of the IC card (PuI) from the received uID and authenticates the IC card. Through these procedures, the client which the user is using is also authenticated indirectly, as the IC card has already authenticated the user. The server acquires the DH1 as well.

The last step is the authentication of the server by the client through the following procedures. The server generates a DH exchange key 2, adds to it a digital signature by using the private key of the server (PrS) and delivers it to the client. The client verifies the digital signature by using the public key of the server (PuS) received from the IC card and authenticates the server.

By the above-mentioned three paths (steps), the authentication between the client and the server is completed. Because the DH exchange key 1 and 2 are shared in the above procedures, the client and the server can generate a common encryption key (K). The subsequent communication between the client and the server is performed by using K.

G. Detailed Sequence of SPAIC

Fig. 6 shows the detailed sequence of SPAIC. In the actual authentication system, countermeasures against denial of service (DoS) attacks or replay attacks are important. DoS attacks are dealt with by way of exchanging cookies between the client and the server [18]. The value of Cookie is generated based on the ID of the communication partner, the

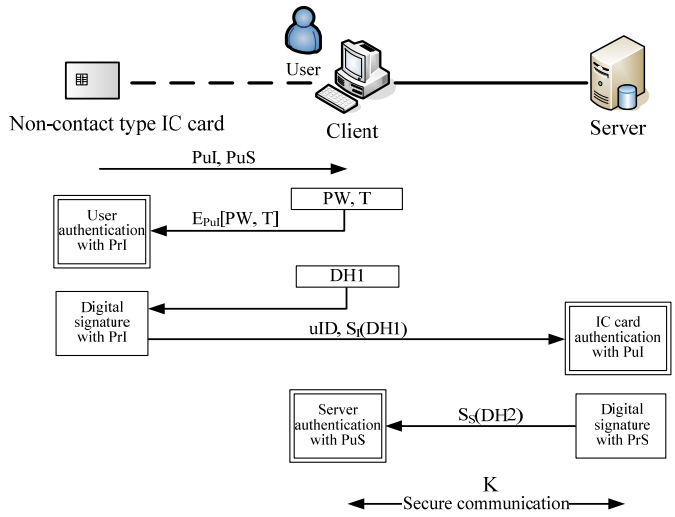


Fig. 5. Outline of SPAIC operation

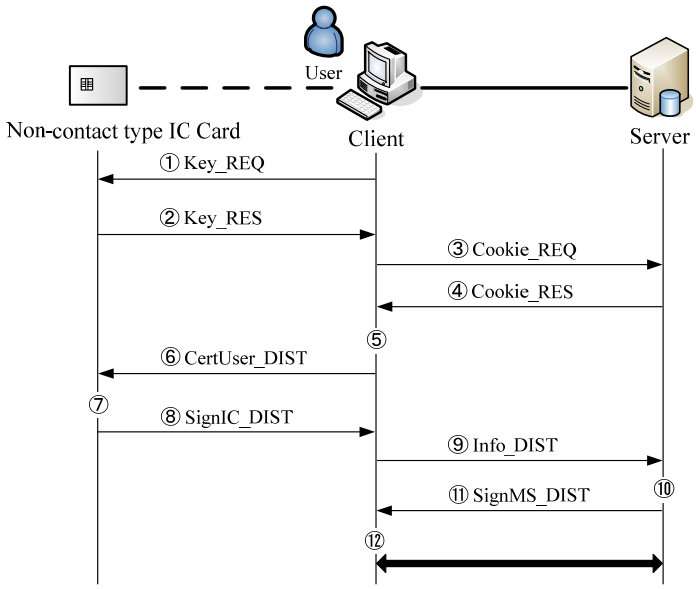


Fig. 6. Detailed sequence of SPAIC

IP address and a random number. Since a different value is generated for each communication, the Cookie can prevent DoS attacks from unrelated terminals by containing it in the packet from a client to a server at the time of IC card authentication.

Replay attacks are dealt with by way of using the random number Ni which the IC card generate and the random number Nr which the server generates and transmits to the IC card at the time of exchange of Cookies. Ni and Nr serve as challenge codes. The random number Nr is also used to check if the IC card authentication information was in fact created at the time of authentication.

(1) Sending of Key_REQ to the IC card:
In order to encrypt user authentication information etc., the client requests the IC card to deliver the information such as the public key of the IC card.

(2) Sending of Key_RES to the client:
The IC card delivers the user ID (uID), the public key of the IC card (PuI), the public key of the server (PuS) and a random number (Ni).
uID, PuI, PuS, Ni

(3) Sending of Cookie_REQ to the server:
The client generates a cookie (Ci) to prevent DoS attacks, and deliver it to the server.
Ci

(4) Sending of Cookie_RES to the client:
The server generates a random number (Nr) and a cookie (Cr). Then deliver them to the client together with the cookie (Ci).
Ci, Cr, Nr

(5) Encryption of user authentication information:
The random number (Ni) and the user authentication information (PW, T) received from the IC card are encrypted by PuI stored in the client. The random number Nr received from the server is simultaneously encrypted by PuS. Moreover, The Diffie-Hellman exchange key (DH1) is generated.
$E_{PuI}[PW, T, Ni], E_{PuS}[Nr], DH1$

(6) Sending of CertUser_DIST to the IC card:
The authentication information created at step (5) is sent to the IC card.
$E_{PuI}[PW, T, Ni], E_{PuS}[Nr], DH1$

(7) User authentication and generation of IC card authentication information:
The IC card takes out PW, T, Ni by using the private key of the IC card (PrI), and performs user authentication. In addition, it compares this Ni with the generated Ni. After the user authentication, the IC card adds DH1 to $E_{PuS}[Nr]$, and creates a digital signature for such information by using the private key of the IC card (PrI).
$S_I(DH1, E_{PuS}[Nr])$

(8) Sending of SignIC_DIST to the client:
The IC card authentication information created at step (7) is delivered to the client together with the uID.
$uID, S_I(DH1, E_{PuS}[Nr])$

(9) Sending of Info_DIST to the server:
The client sends the IC card authentication information received at step (8) to the server together with the cookies Ci and Cr received at step (4).
$uID, S_I(DH1, E_{PuS}[Nr]), Ci, Cr$

(10) Authentication of the IC card and generation of server authentication information and K:
The server confirms the validity of the cookie sent by the client. The server also verifies the digital signature by reading out the corresponding public key (PuI) from the uID and authenticate the IC card. In addition, the server takes out Nr by using the private key of the server (PrS) and compares it with the generated Nr. Thereafter, the server generates a Diffie-Hellman exchange key (DH2) and creates a digital signature to perform the server authentication by using the private key of the server (PrS). Futhermore, the server generates the common encryption key (K) by using acquired DH1 and DH2.
$S_S(DH2), K$

(11) Sending of SignMS_DIST to the client:
The signature information created at step (10) is delivered to the client together with the cookies Ci and Cr.
$S_S(DH2), Ci, Cr$

(12) Server authentication and Generation of K:
The client verifies the validity of the cookies sent by the server. In addition, the client verifies the digital signature by using the PuS received in advance and authenticates the server. Thereafter, the client acquires DH2 and generates the common encryption key (K) by using DH1 and DH2.

The subsequent encryption communication between the client and the server is performed by using this encryption key K.

IV. EVALUATION

Table 2 shows the results of the comparison between the PSK method and SPAIC. The first advantage of SPAIC over the PSK method is that there is no possibility of information leakage from the client side because the client has no secret information.

TABLE Ⅱ
COMPARISON BETWEEN THE PSK METHOD AND SPAIC

	PSK Method	**SPAIC**
Information stored in the client	Operational programs, Pre-Shared Key (×)	Operational programs (○)
Administrative load	Complicated renewal procedures for the common key (×)	Simply adding or deleting users (○)
Encryption between the IC card and the client	Use Pre-Shared Key method (○)	Use Public Key method (○)
Load to the IC card	Middle (○)	High(△)

The second advantage of SPAIC over the PSK method is that the administrative load in the case of SPAIC is quite small because it needs only to add or delete users, whereas in the case of the PSK method the administrative load is heavy because it needs to frequently update the PSK for the sake of system safety.

There is one potential disadvantage for SPAIC, that is that the public key operation performed in the IC card may lead to an increase in the processing load of the IC card. However, it does not seem to give a big impact on its practical application because SPAIC operates only at the time of start-up of the client.

V. CONCLUSION

In the PSK method, there is a possibility of information leakage from the client terminal. Thus, in order to solve this problem, we proposed in this paper a protocol named SPAIC that enables deliveries of secret information from a server to a client in the user environment of non-contact type IC cards without any possibility of information leakage, by defining a model whereby client terminals do not possess any initial information except for operational programs.

In our proposed system, encrypted communication between an IC card and a client can be performed, and secure authentication among the IC card, the client and the server is ensured even if the client does not possess initial information, through the system in which the IC card possesses an IC card public key.

In our system, the communication pathway between the client and the server for safe information deliveries is established by the use of an encryption key created by the exchange of a Diffie-Hellman key.

Although some decrease in the performance is anticipated in the case of SPAIC for the processing of public-key cryptosystem performed in the IC card, we think that the system can be adequately used for authentication at the time of start-up of the system. We are going to evaluate the performance of SPAIC by actually implementing it in the future.

REFERENCES

[1] J. Kohl, Digital Equipment Corporation, C. Neuman, ISI., "The Kerberos Network Authentication Service (V5)," RFC 1510, Sep. 1993.

[2] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, Nov 1998.

[3] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998.

[4] T. Dierks, Certicom, C. Allen, and Certicom, "The TLS Protocol Version 1.0," RFC 2246, Jan. 1999.

[5] A. Watanabe, Y. Koui, T. Ideguchi, Y. Yokoyama, and S. Seno, "Realization Method of Secure Communication Groups Using Encryption and Its Implementation", *IPSJ Journal*, Vol.38, No.4, pp.904-914, Apr.1997.

[6] Y. Isobe, M. Mimura, Y.Seto, and Y. Kikuchi, "A Proposal for Authentication System using a Smart card With Fingerprints," *IPSJ SIG Notes*, *99-CSEC-4*, Vol.99, No.24, pp. 55-60, Mar. 1999.

[7] H. Yoshida and S. Hirata, "Trends in and Problems of Smart Card Technology," *IPSJ Magazine*, Vol.43, No.3, Mar.2002.

[8] Y. Kagei, "Frontiers Trend of Smart Card Technology," *IPSJ Magazine*, Vol.39, No.5, pp. 429-433, May 1998.

[9] M. ITOH, "Contactless IC Card Technology and Application," *IPSJ Magazine*, Vol.43, No.3, Mar.2002.

[10] Y, Sato, "Individual Authentication by Smart Card," *Unisys Technology Review*, No. 73, pp. 137-139, May 2002.

[11] Japan IC Card system application council, "Specification of IC cards," Jul. 2001.

[12] E. Rescorla, RTFM Inc., "Diffie-Hellman Key Agreement Method", RFC 2631, June. 1999.

[13] K. Imamoto and K. Sakurai, "Notes on Dynamic Information Management for Authenticated Key Exchange," *Information Security Group (ISEC)*, pp.91-96, March 2003.

[14] C. Kaufman, Microsoft, "Internet Key Exchange (IKEv2) Protocol," RFC 4306, Dec. 2005.

[15] J. Schiller, Massachusetts Institute of Technology, "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)," RFC 4307, Dec. 2005.

[16] OpenSSL Project. The Open Source toolkit for SSL/TLS. http://www.openssl.org/.

[17] W. Polk, R. Housley, and L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3279, Apr. 2002.

[18] D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC2408, Nov. 1998.

7th International Symposium on Communications and Information Technologies
October 16-19, 2007
Sydney, Australia

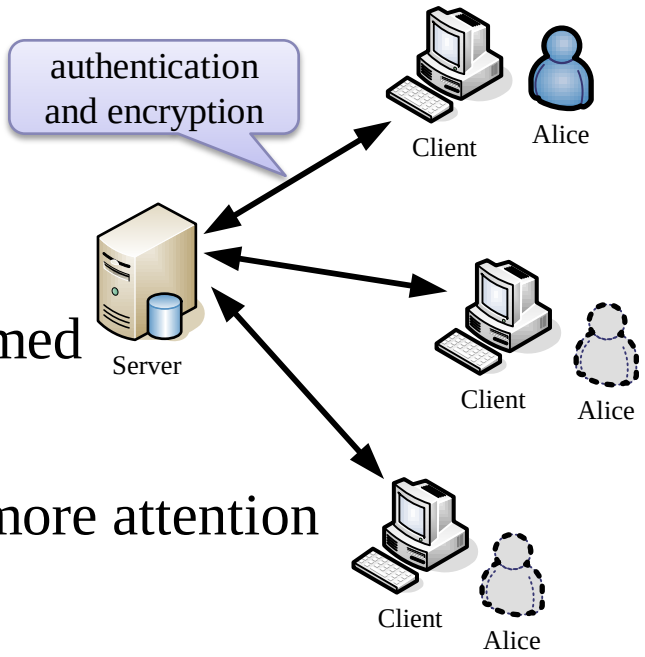
Proposal of an Authentication Method "SPAIC" using a Non-contact Type IC Card

Changjun Shu, Hidekazu Suzuki, and Akira Watanabe
Graduate School of Science and Technology
Meijo University, Japan

Background

- When exchanging important information in a client-server system
  - Secure authentication and encryption are indispensable
- When Accessing the server from different client terminals
  - Secure communication with authentication and encryption is required

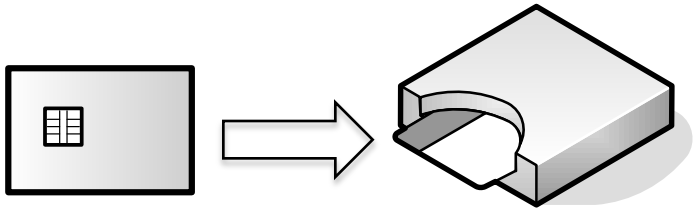
IC cards are paid attention



  - Authentication and encryption are performed in IC cards
  - Tamper-proof character
  - Non-contact type IC cards are attracting more attention

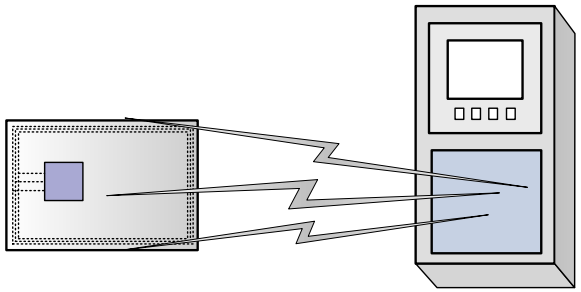
Classification of IC Cards

- Contact type IC card
  - An IC card and a client are connected tightly
  - Cipher communication is not commonly used



Insert

- Non-contact type IC card
  - Wireless communication between an IC card and a client
  - Cipher communication is needed



Wireless Communication

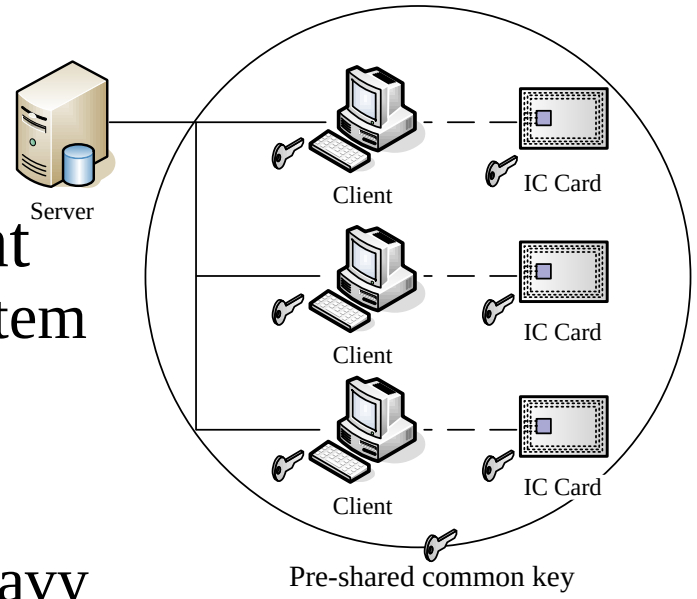
Conventional Authentication Method

- Cipher technology between an IC card and a client
  - Pre-Shared Key Method (PSK Method)

    →Defined by JICSAP (Japan IC Card System Application Council)
- All IC cards and clients have a same common key

ISSUE

- Information leakage from the client
  - Impact could extend to the entire system
- The common key needs to be periodically updated
  - Administrative load become quite heavy

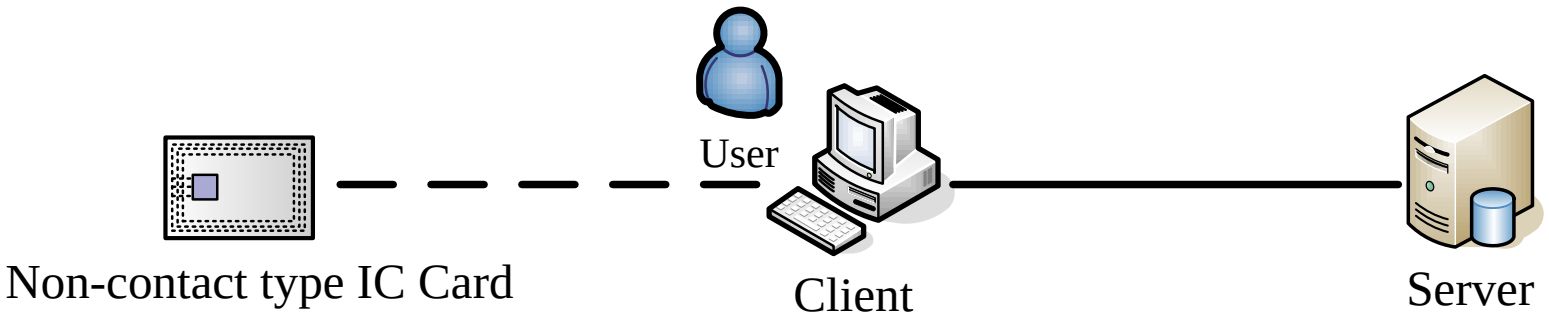


Proposed Method: SPAIC

- SPAIC: Secure Protocol for Authentication with IC Card

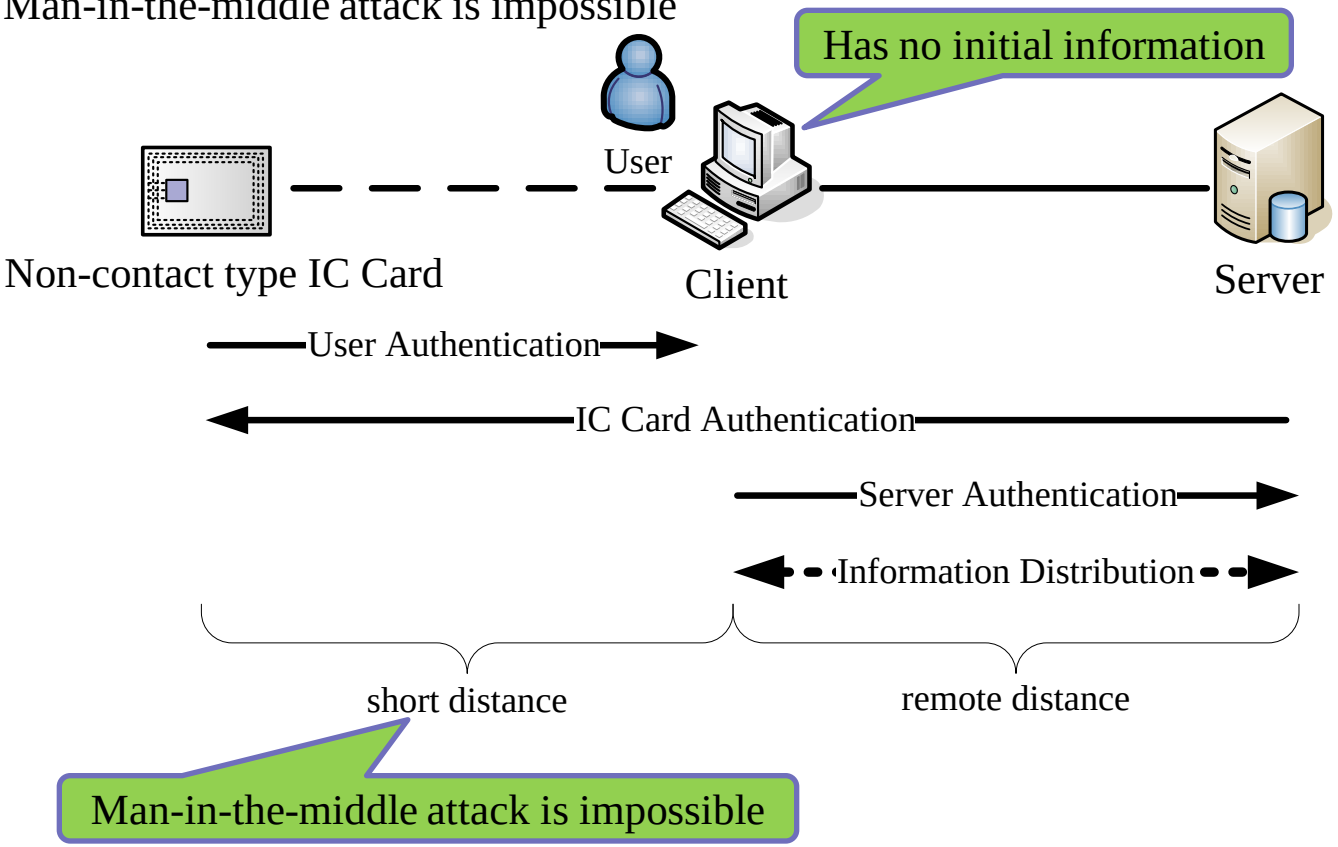
Purpose

- Delivery of important information securely from a server to a client using a non-contact type IC card

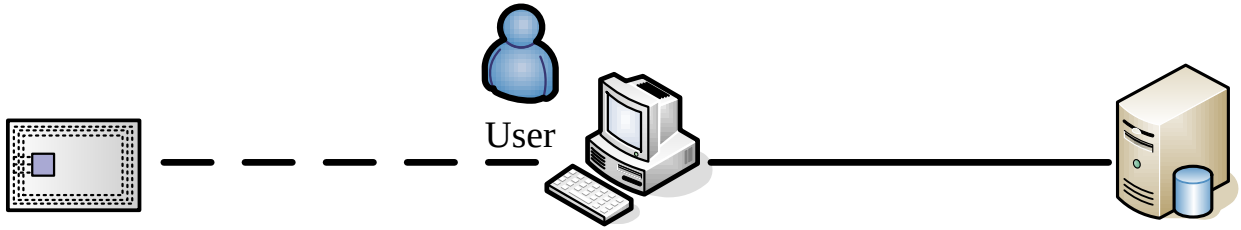


Assumed Model

- A client has no initial information
- A non-contact type IC card is used, in view of its wide use in future
- An IC Card and a Client are separated, but are within a short distance
  - Man-in-the-middle attack is impossible



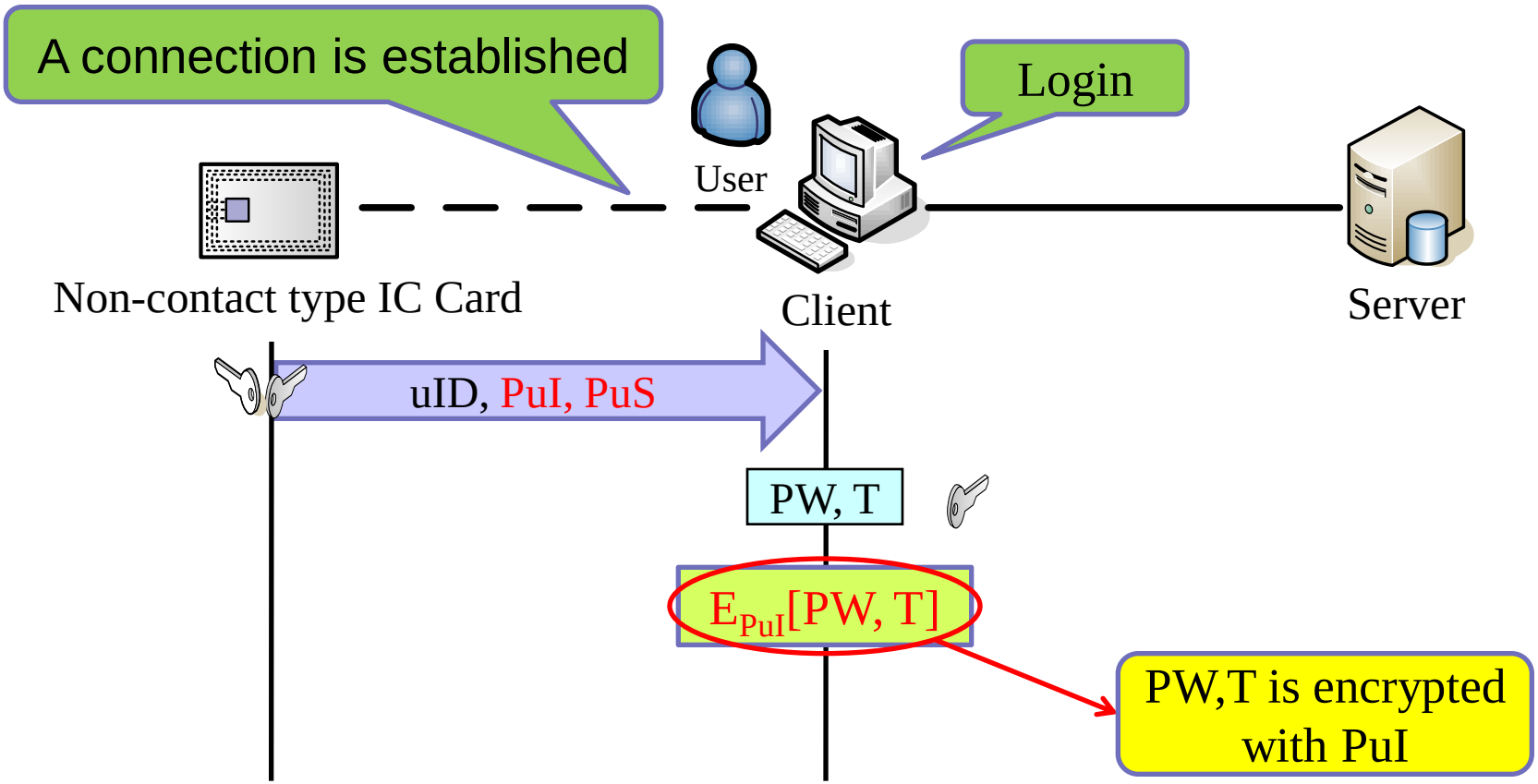
Initial Information in each device



	PSK Method	SPAIC
IC Card	User ID (uID) Private key of the IC card (PrI) Public key of the Server (PuS) Password (PW) Biological information template (T) ***Pre-shared common key (PSK)***	User ID (uID) Private key of the IC card (PrI) Public key of the Server (PuS) Password (PW) Biological information template (T) ***Public key of the IC card (PuI)***
Client	***Pre-shared common key (PSK)***	—
Server	User ID (uID) Private key of the Server (PrS) Public key of the IC card (PuI)	User ID (uID) Private key of the Server (PrS) Public key of the IC card (PuI)

SPAIC Sequences: User Authentication

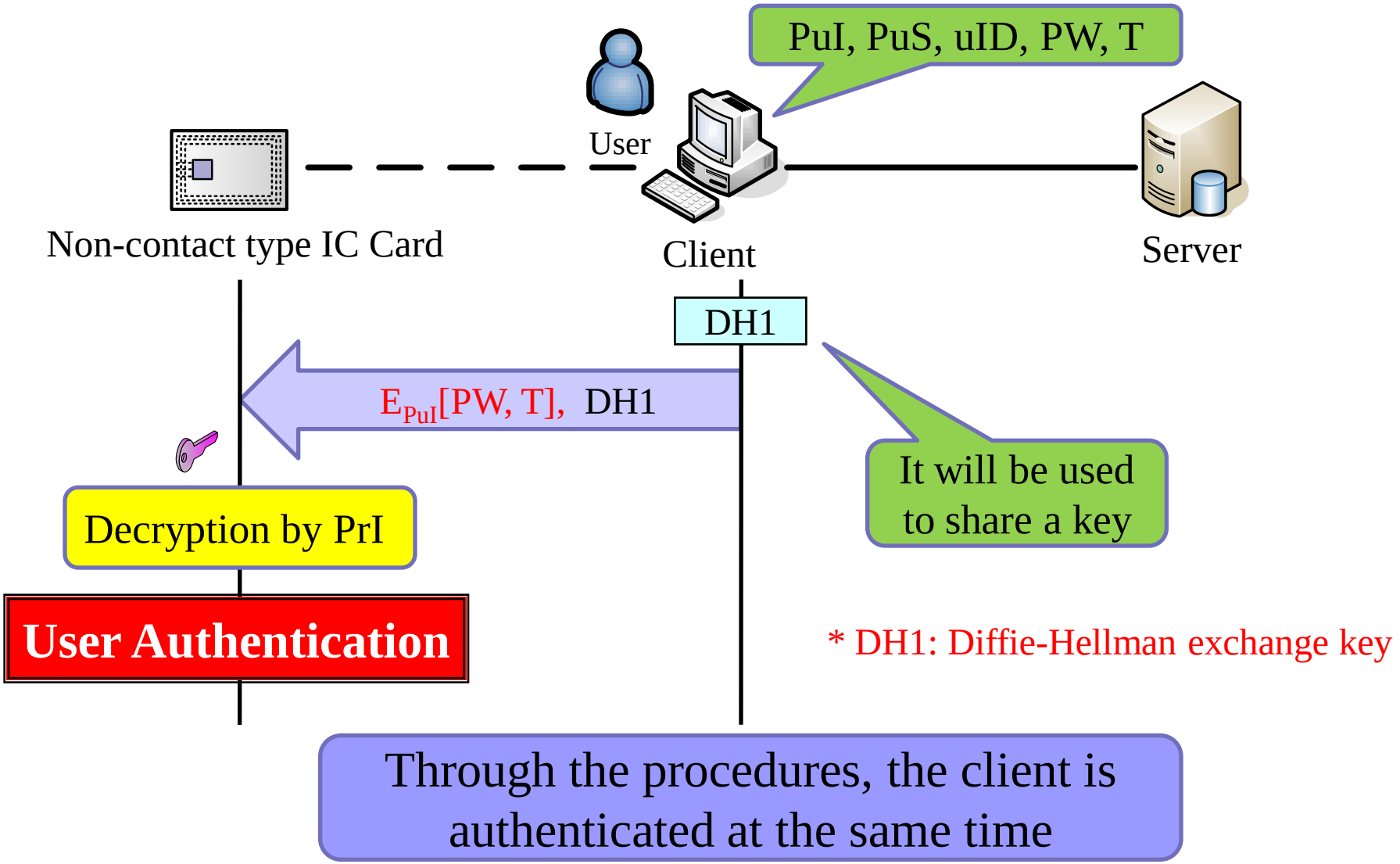
- The IC card performs user authentication by the password and biologic information



*PW: Password

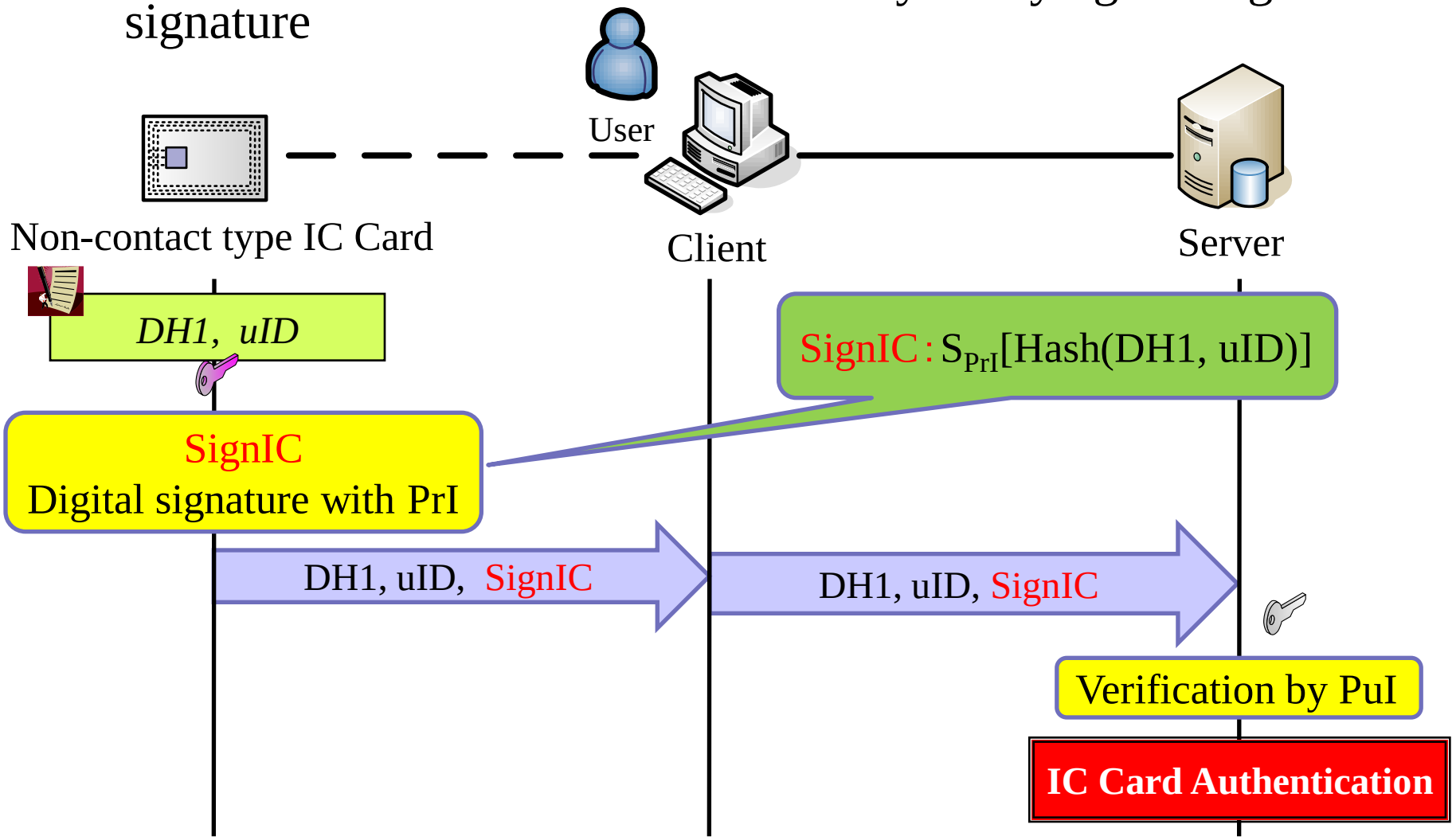
*T: Biological information template

SPAIC Sequences: User Authentication

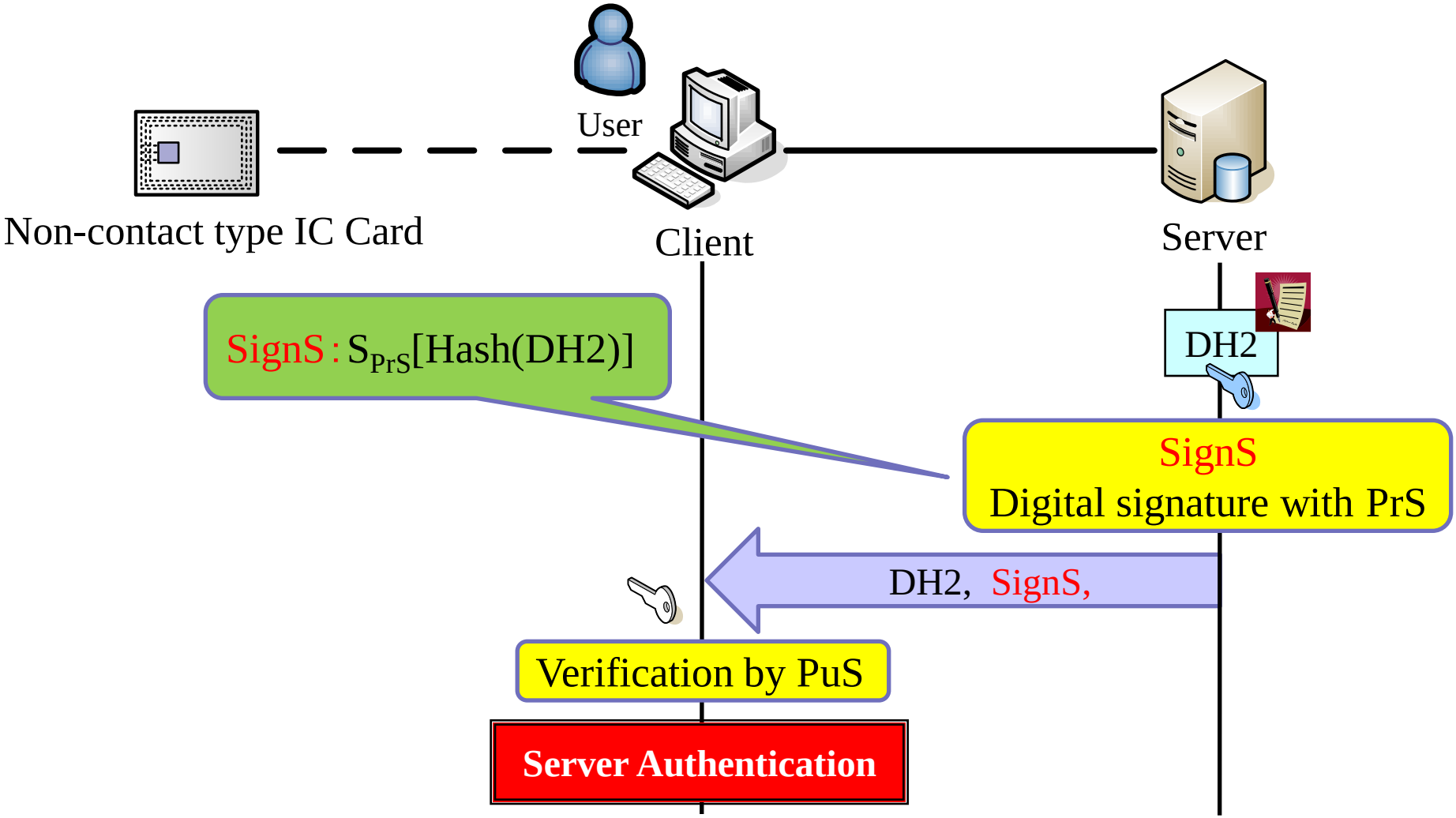


SPAIC Operation: IC Card Authentication

- The server authenticates the IC card by verifying the digital signature

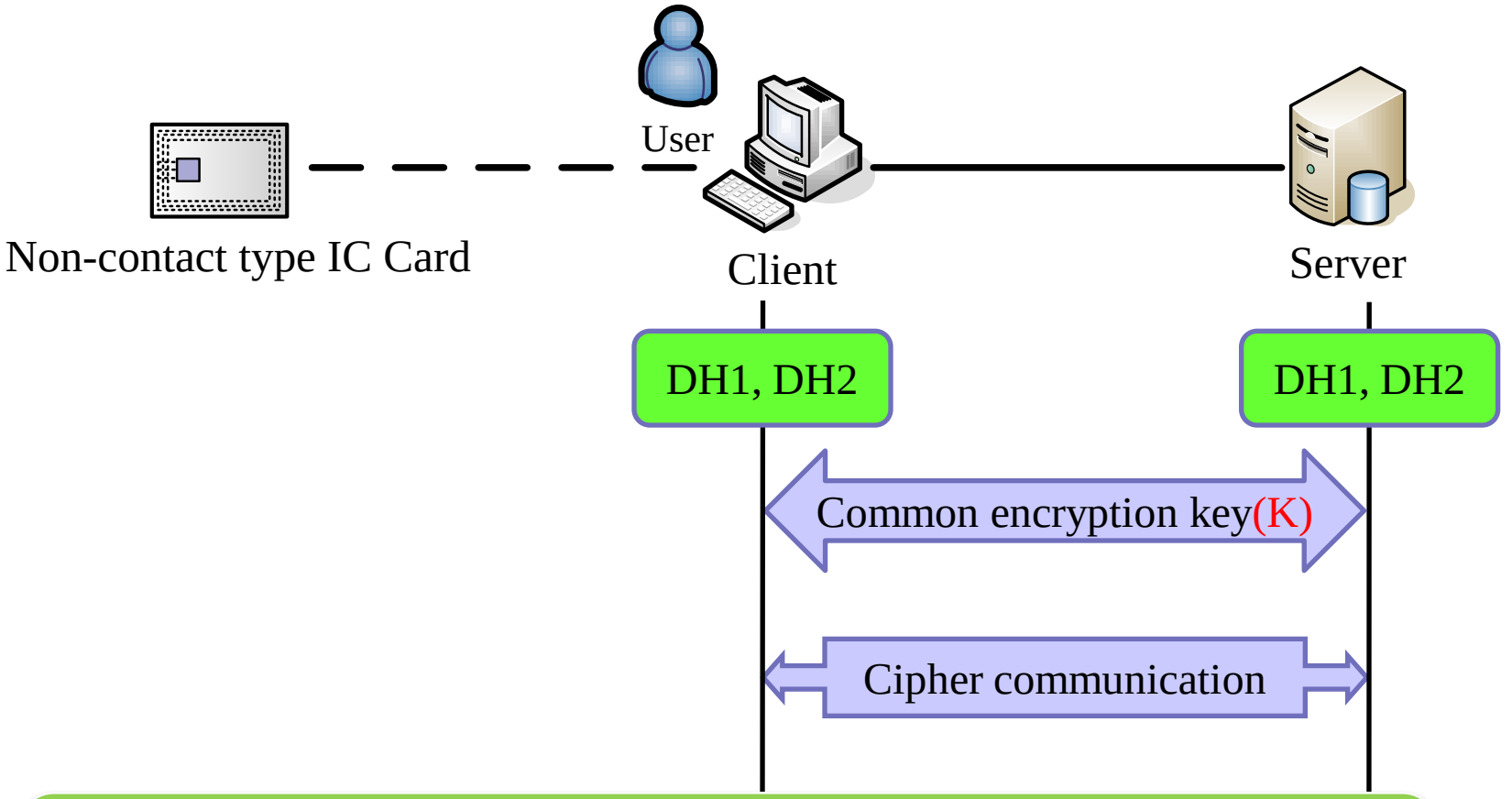


SPAIC Sequences: Server Authentication



* DH2: Diffie-Hellman exchange key

SPAIC Sequences: Encryption Key Generation



The subsequent cipher communication between the client and the server is performed by using the key, K

Evaluation

	PSK Method	SPAIC
Information stored in the client	Operational programs, Pre-Shared Key (×)	Operational programs (○)
Administrative load	Periodical update of a common key (×)	Simply adding and deleting users (○)
Encryption between the IC card and the client	Utilize the Pre-Shared Key (○)	Public Key of the IC card (○)
Load to the IC card	Middle (○)	High(△)

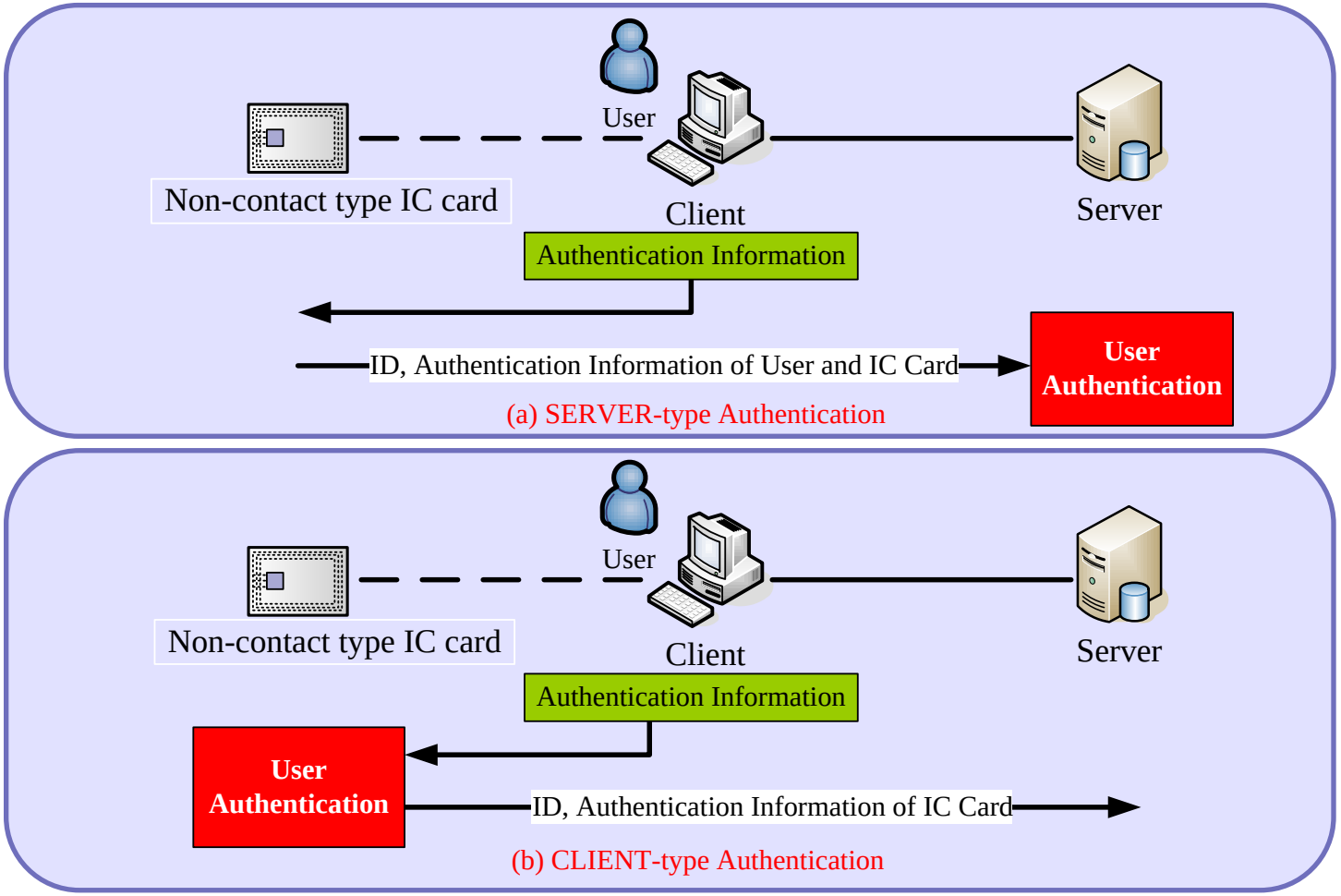
Summary and Future Works

- Summary
  - A model that clients do not have any initial information is defined
  - An authentication method “SPAIC” using a non-contact type IC card is proposed
  - Secure Communication between the client and the server is established
- Future work
  - Implementation of SPAIC
  - Performance evaluation

Appendixes

User Authentication Methods

- Two types of authentication methods
  - Depending on the difference in the places of storing information
  - Server-type authentication and Client-type authentication

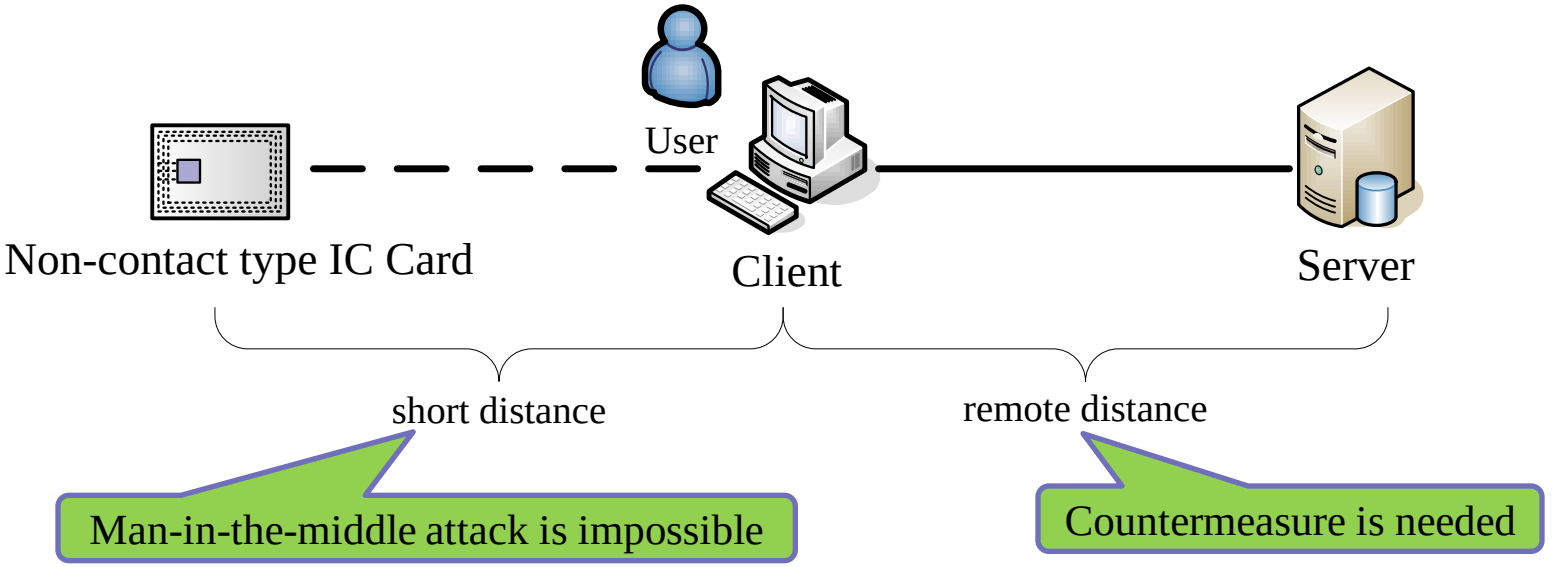


Load to the IC Card

- Storing the public key of the IC card
  - Dose not increase the administrative burden because the public key(PuI) and the private key(PrI) of the IC card are created simultaneously
- Performing the public key operation
  - Lead to an increase in the processing load of the IC card
  - Not a big impact on its practical application because SPAIC operates only at the time of start-up of the client
- Evaluation of processing load of the IC card
  - The implementation of SPAIC is not finished
  - The detailed evaluation will be given in future

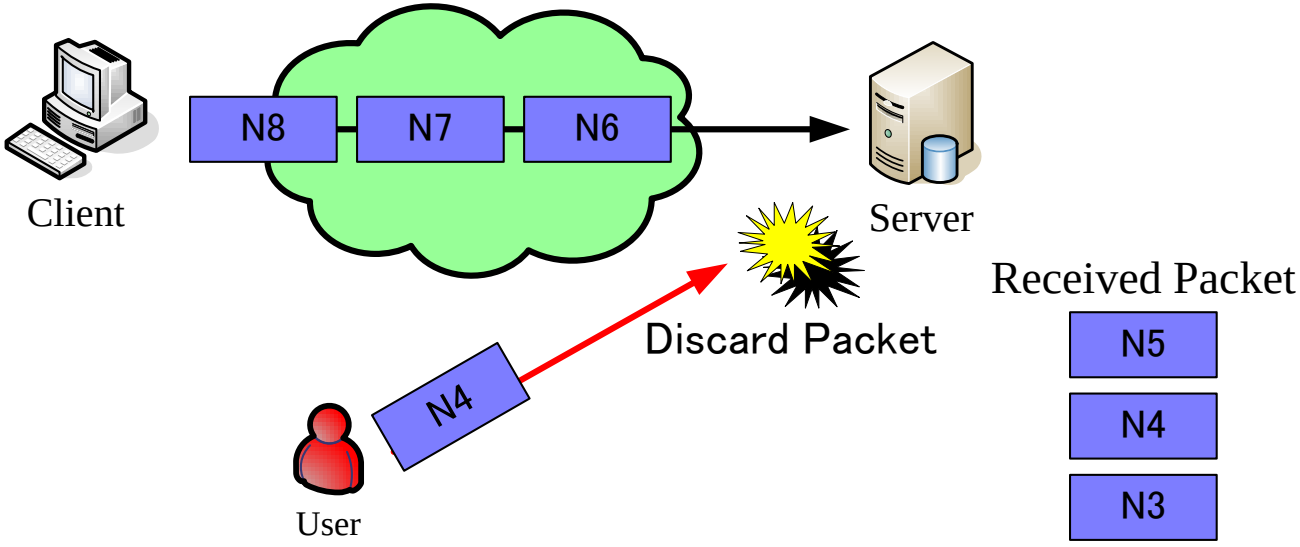
Countermeasure against Man-in-the-middle Attack

- Man-in-the-middle Attack
  - An attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised
- Countermeasure
  - Use digital signature to defense against the attack



Countermeasure against Replay Attack

- Replay Attack
  - A form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed
- Countermeasure
  - Use random numbers to check for duplicate
  - Discard the packet if duplicate

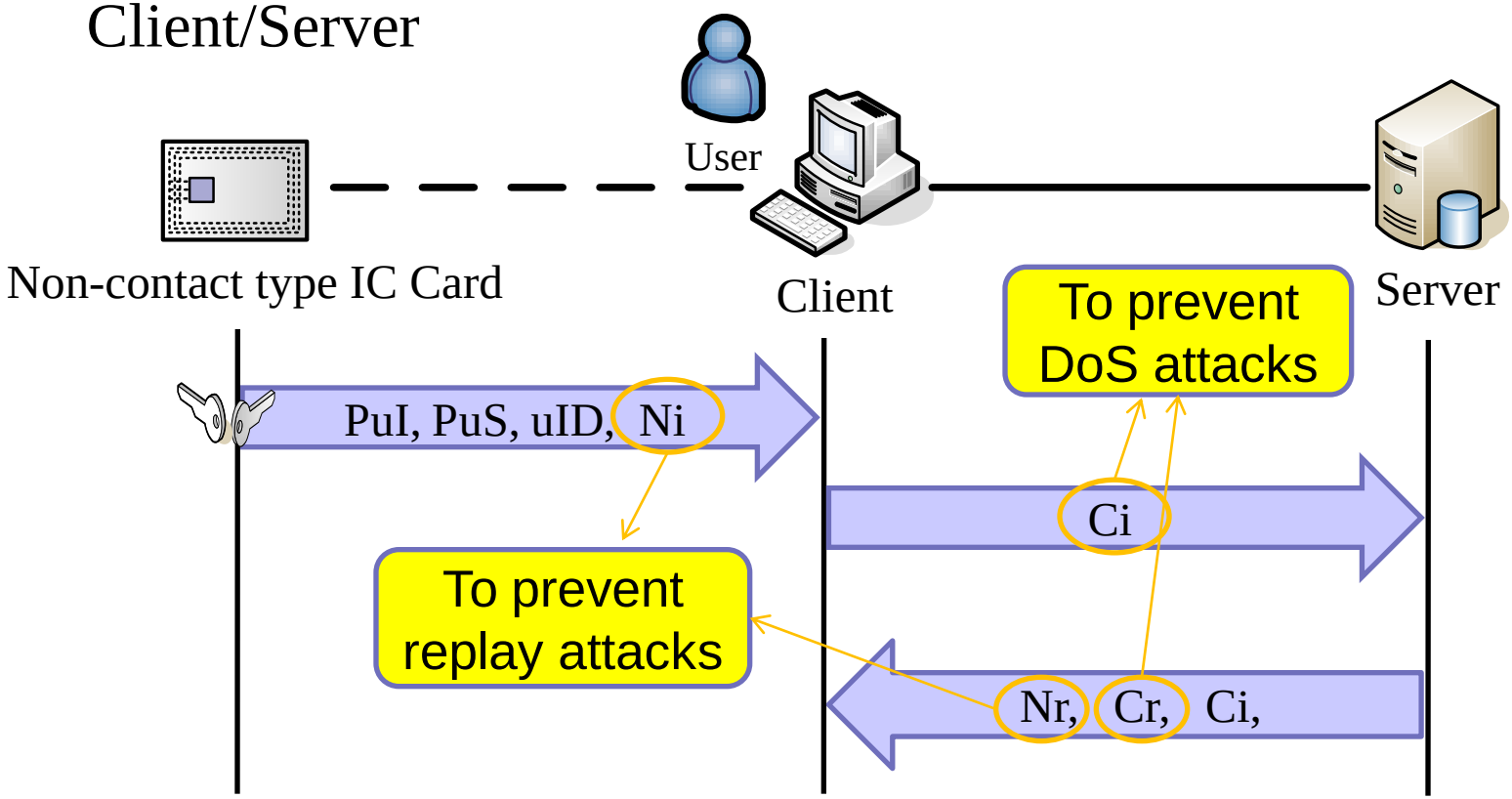


Countermeasure against DoS Attack

- DoS Attack（Denial of Service Attack ）
  - A type of network attack that is designed to bring the network to its knees by flooding it with useless traffic
- Countermeasure
  - Avoid by exchanging Cookie between Client/Server
  - The value of Cookie is generated based on the ID of the communication partner, the IP address and a random number.

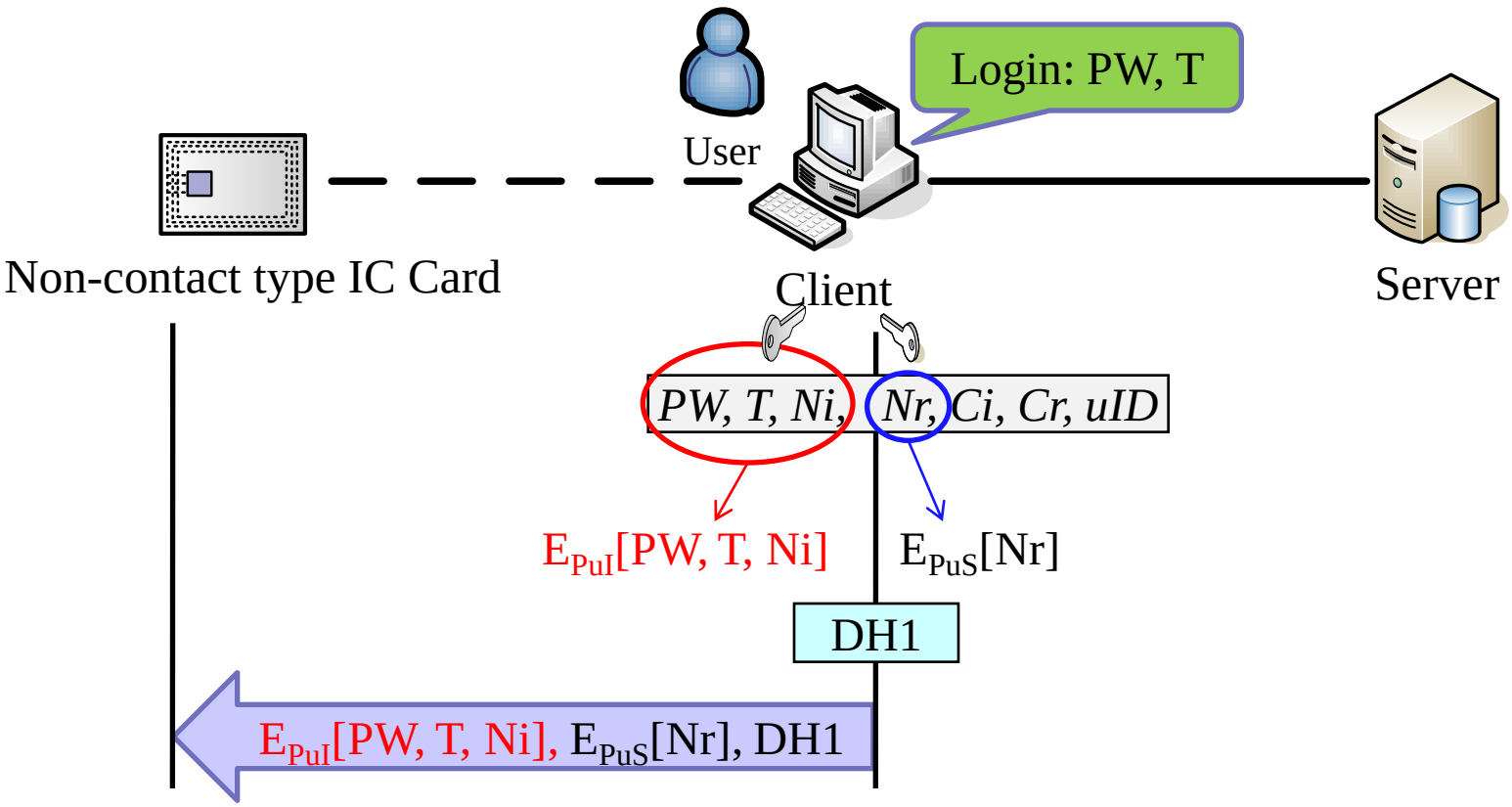
SPAIC Sequences: User Authentication

- Avoid Replay Attacks by using the random number Ni and Nr
- Avoid DoS Attacks by exchanging cookies Ci, Cr between Client/Server



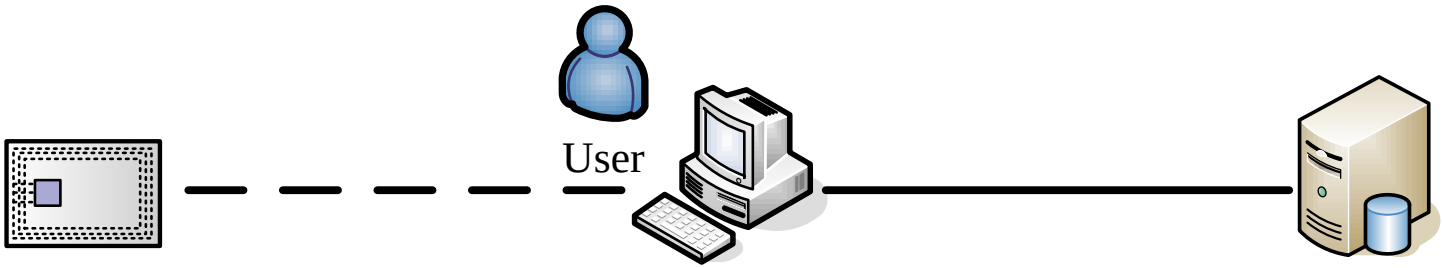
*Ni, Nr : Random Number
*Ci, Cr : Cookie

SPAIC Sequences: User Authentication



* E_{PuI}[PW, T, Ni]: PW,T,Ni is encrypted with key PuI
* E_{PuS}[Nr]: Nr is encrypted with key PuS
* DH1: Diffie-Hellman exchange key

SPAIC Sequences: User Authentication



$E_{PuI}[PW, T, Ni], E_{PuS}[Nr], DH1$

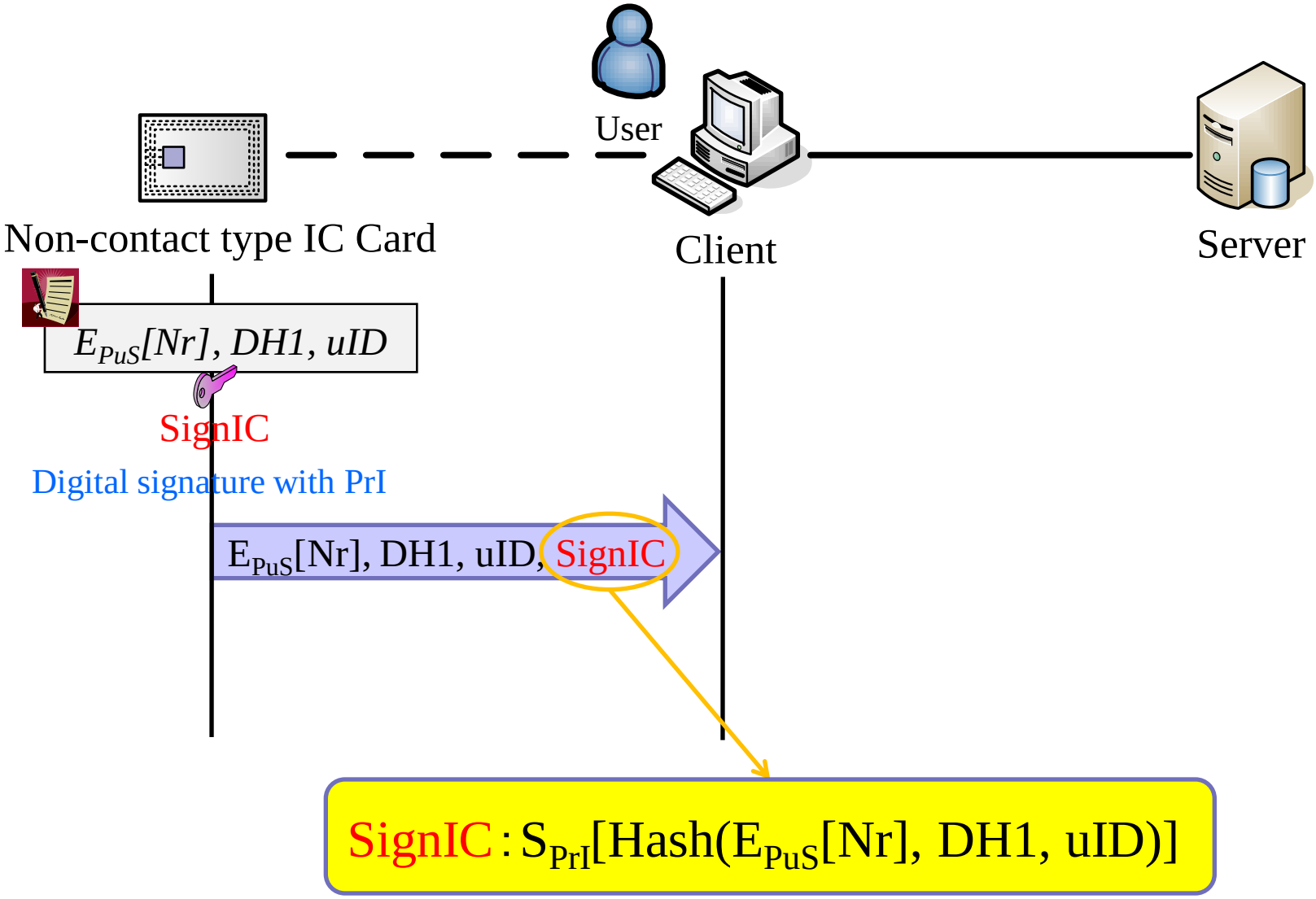
Decryption by PrI

Compare Ni

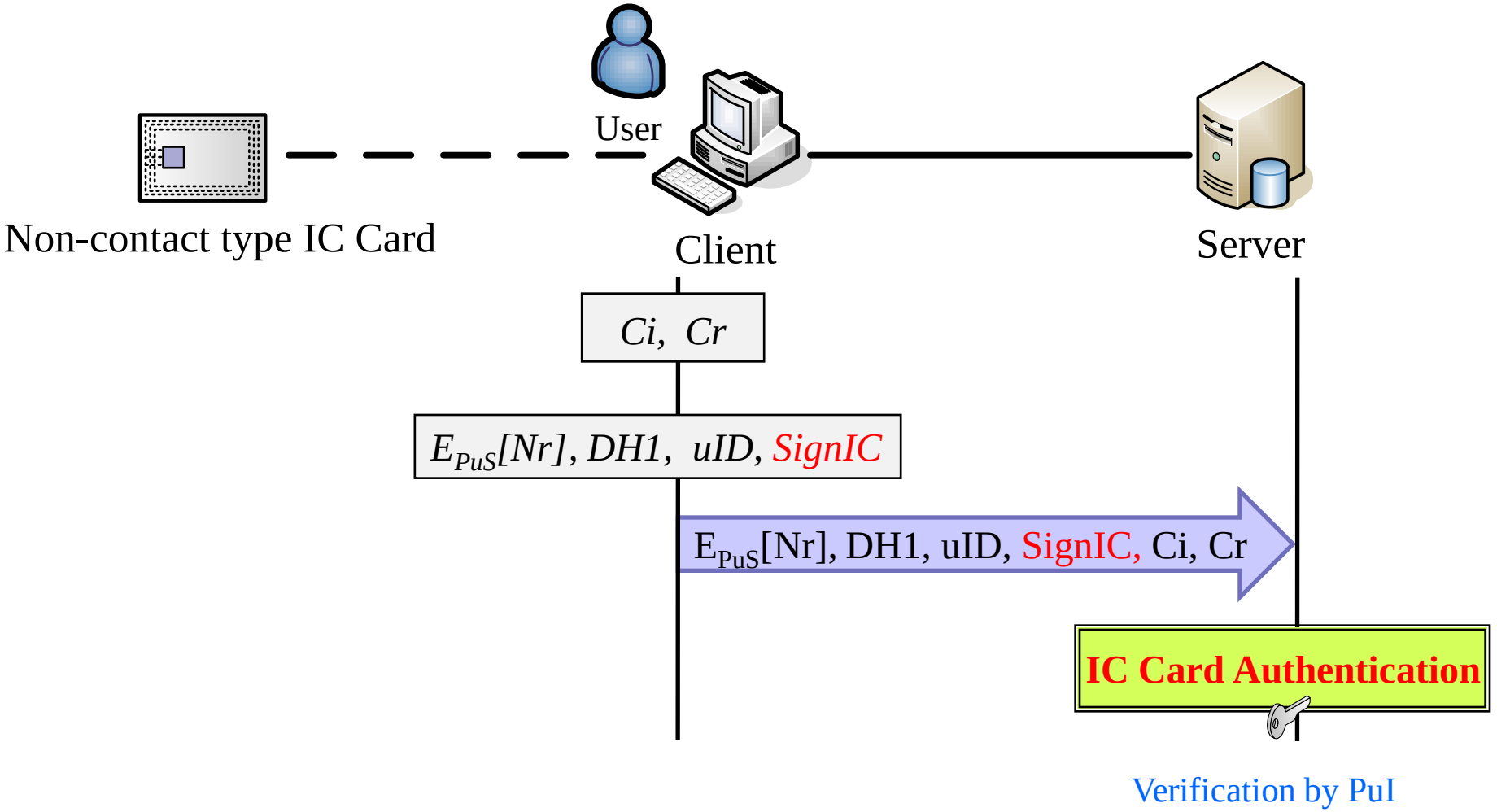
User Authentication

The client is authenticated at the same time

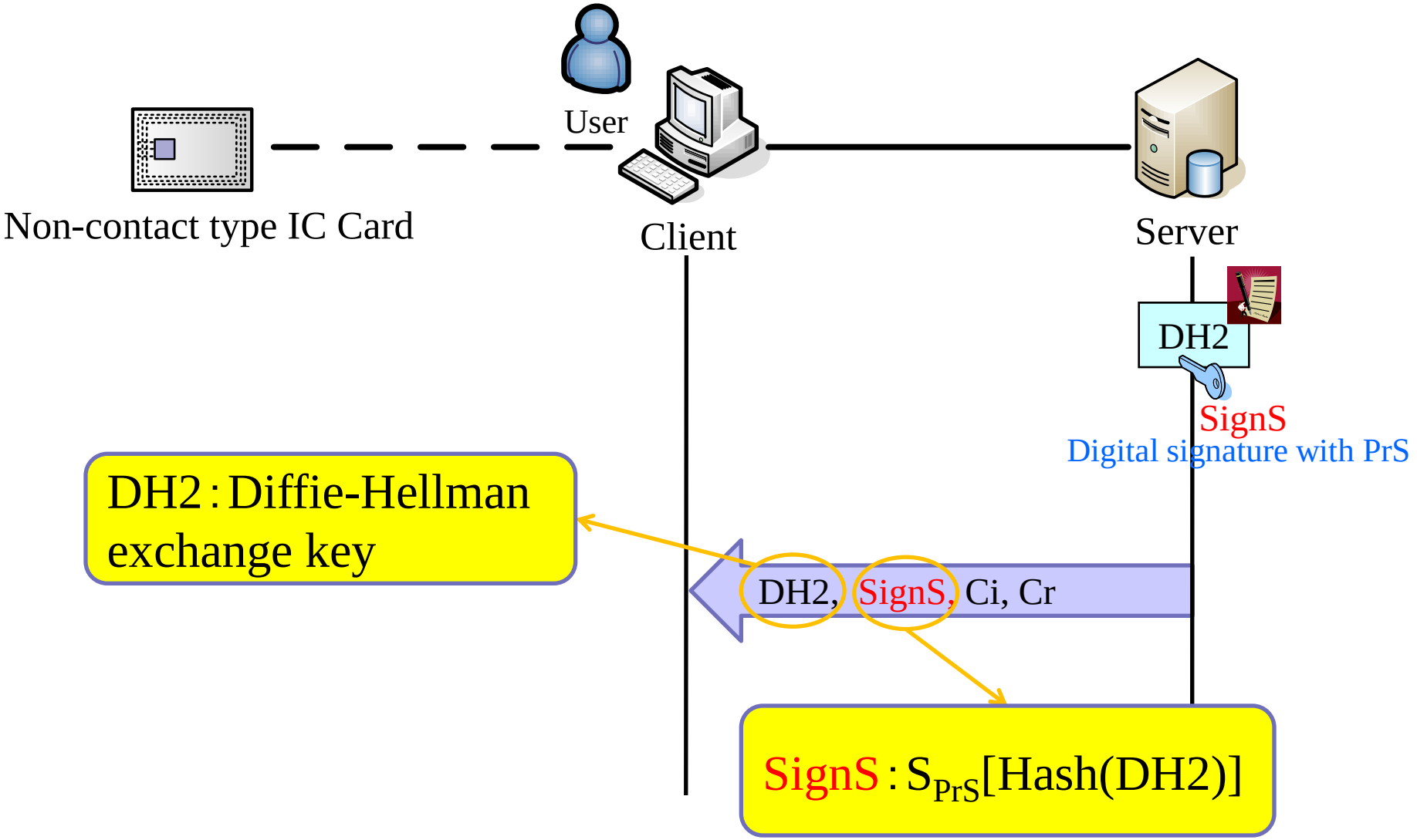
SPAIC Operation: IC Card Authentication



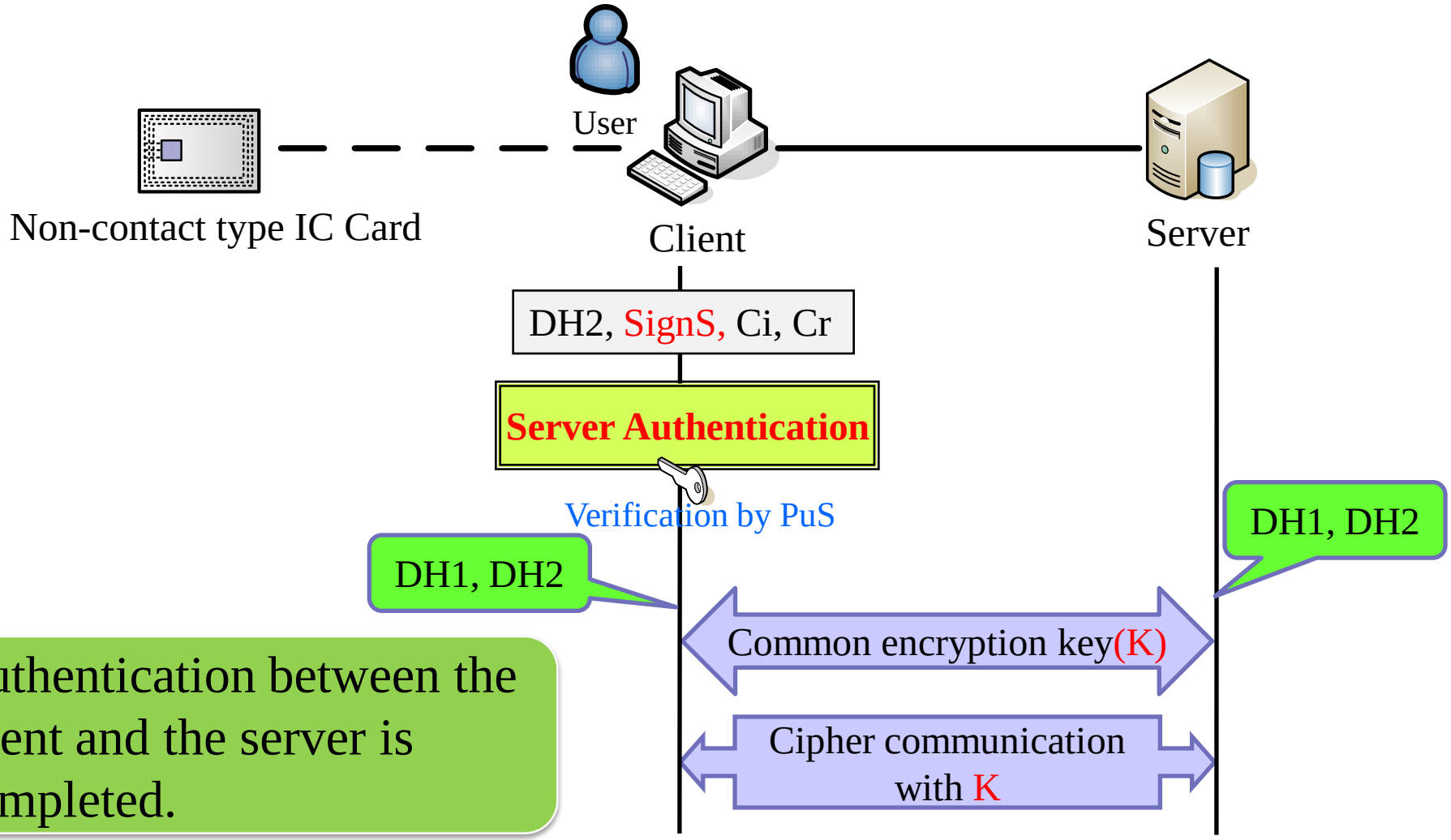
SPAIC Operation: IC Card Authentication



SPAIC Sequences: Server Authentication



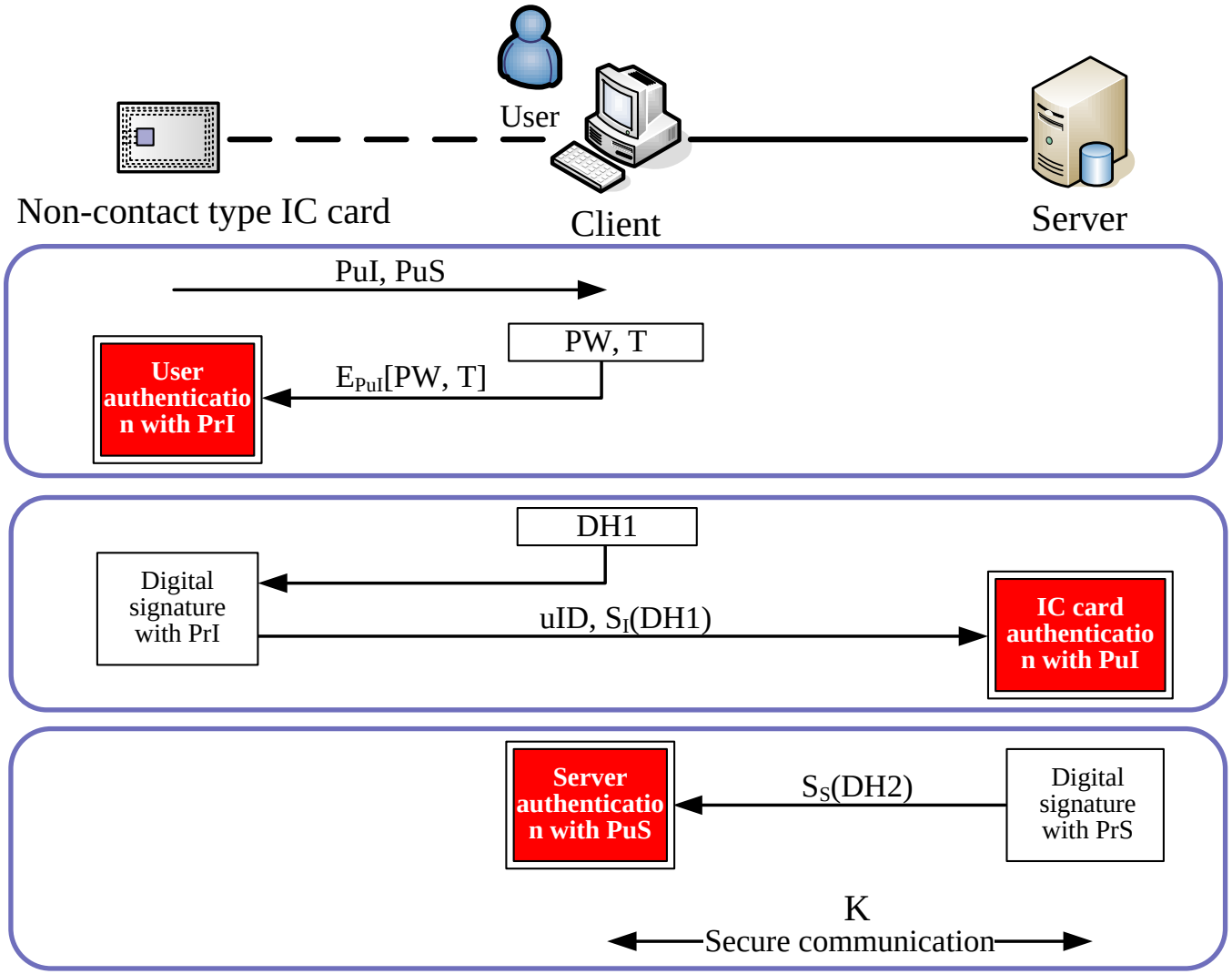
SPAIC Sequences: Server Authentication



Authentication between the client and the server is completed.

Outline of SPAIC operation

- The authentication procedures of SPAIC consist of three steps



Detailed Sequence of SPAIC