非接触型ICカードを用いた認証方式SPAICの提案

束　長俊[†]　鈴木秀和[†]　渡邊　晃[†]

クライアント/サーバ間通信において重要な情報を交換する場合，確実な認証と暗号化が必要となる．このような環境において，ユーザ固有の情報を格納したICカードを利用する方式が注目されている．これまでは，接触型ICカードを利用する場合がほとんどであり，IC カード/クライアント間通信のセキュリティはそれほど重要ではなかった．しかし，今後は非接触型ICカードの普及が見込まれ，IC カード/クライアント間でも暗号通信を行うことが必須になると考えられる．これを実現するために，すべてのICカードとクライアントに同じ共通鍵を所持させるという方法があるが，クライアントから情報が流出するという懸念があった．本論文では，非接触型ICカードを利用し，初期情報を一切持たないクライアントに重要情報を配送することを可能とするプロトコルSPAICを提案する．

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

Changjun Shu,[†] Hidekazu Suzuki[†] and Akira Watanabe[†]

In case where important information is exchanged in a client-server system, it is quite indispensable to perform authentication and encryption. In such an environment, the method using an IC card that stores proper user information is becoming popular. Currently, the security of communication between an IC card and a client is not a critical concern since contact type IC cards are used in most cases. However, it is considered that non-contact type IC cards will be spreading hereafter, secure communication between an IC card and a client will be a serious concern. There is a method that all IC cards and clients possess a common key to realize secure communication, however, it can easily result in the leakage of information from the client sides. To solve the problem, in this study, a protocol called SPAIC is proposed. Presuming that a non-contact type IC card is used, it can deliver the important information from a server to a client that has no secret information in it.

1. はじめに

インターネットの発展に伴い，ユーザがクライアント端末を利用して遠隔地のサーバと情報交換したいという要求が高まっている．クライアント/サーバ間通信において重要な情報を交換する場合，確実な認証と暗号化が必須である．認証と暗号化による情報配送は，従来から様々な方式が検討されている[1)~5)]．近年では，異なるクライアントからサーバにアクセスしたいというニーズが増えており，このような環境においても同様に認証と暗号化による情報配送を行えることが望ましい．

このような要求を満たす方式の一つとして，ユーザがICカードを所持する方式が注目されている[6)~9)]．ICカードは耐タンパ性を有しており、認証に必要な情報を安全に格納することが可能で，クライアント端末内にユーザの情報を保持することなく認証と暗号通信を行うことが可能である．これは，ユーザが端末を選べるという利便性だけでなく，端末からユーザの情報が盗まれるのを防止するという利点もある．近年では非接触型ICカードの発展よって，ICカードの利便性が一層向上することが期待されている．

ICカードを利用した認証方式では，クライアント/サーバ間で行われる認証に加えて，ICカードの持ち主を確認するためのユーザ認証も併せて行う必要がある．ユーザ認証は，ICカード内にパスワードなどのユーザ情報を格納し，クライアントから入力されたユーザ認証情報をICカード内で検証する方法が主流である．接触型ICカードでは，ICカードとクライアントが一体であるため，両者の間の通信に係るセキュリティは大きな問題にはならなかった．しかし，非接触型IC

† 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University

カードを用いる場合，これらの認証処理に必要な情報を安全にやりとりするためには，IC カードとクライアント間の暗号通信が必須である．

IC カードとクライアント間の通信を暗号化する方法として，事前共有鍵を利用する方式が定義されている[10]．しかし，この方式では，すべての IC カードおよびクライアントに事前共有鍵を所持させるため，クライアント側から情報が漏洩する危険性がある．さらに，漏洩した場合，影響がシステム全体に波及する可能性がある．

クライアントは IC カードのような耐タンパ性がないのが一般的であるため，クライアントに秘密情報を所持させない方式が望ましい．そこで，IC カード，クライアント，サーバがあらかじめどのような初期情報を所持し，どのような手順で認証や暗号化を行うべきかについて検討を行った．

本論文では非接触型 IC カードを利用し，初期情報を一切持たないクライアントに対し，サーバから重要情報を配送することを可能とするプロトコル SPAIC (Secure Protocol for Authentication with IC card) を提案する．

SPAIC では，IC カード公開鍵を利用して，クライアントから IC カードへの通信の暗号化を行う．また，サーバ公開鍵を利用して IC カードからクライアントを経由し，サーバまで通信の暗号化を行う．更に，クライアント/サーバ間では Diffie-Hellman 鍵交換[11)~13)]により，動的に暗号鍵を生成し，サーバから安全に重要情報を配送することを実現する．

以降，2 章で従来システムとその課題，3 章で提案方式，4 章で評価，5 でまとめを述べる．

2. 従来システムとその課題

従来システムでは，接触型 IC カードをリーダライタに挿入して利用するような場合がほとんどであるため，IC カードとクライアントが一体のものであるとみなし，IC カード/クライアント間の暗号通信を行っていないものが殆どである．

しかし，非接触 IC カードを利用する場合，IC カード/クライアント間が無線通信になるため，暗号化が必須となる．これを実現するための方式として，暗号通信の種となる共有鍵をすべての IC カード，クライアント端末に所持させる事前共有鍵方式が定義されている（**図 1**）．この方式では，事前共有鍵を用いて IC カード/クライアント間で暗号通信を行うための暗号鍵をダイナミックに生成する．

しかし，事前共有鍵方式では，クライアントに秘密情報を所持させる必要があるため，クライアントからの情報漏洩の危険性がある．更に，システム全体で同じ事前共有鍵を所持しているため，この共有鍵が漏洩した場合，その影響がシステム全体に波及する可能性がある．このため，システムの安全性を確保するためにはすべての IC カード，クライアントの事前共有鍵を定期的に変更する作業が必要であり，管理が煩雑である．

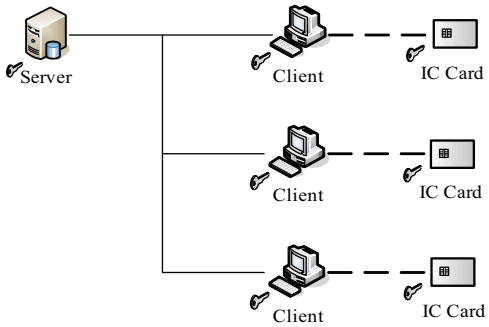


図 1 従来システムの認証方式
Fig. 1 Conventional Authentication Model

3. 提 案 方 式

提案方式では，クライアントに秘密情報を一切所持させないモデルを定義する．この条件のもとで，サーバからクライアントへ暗号鍵など第三者に秘匿すべき重要情報を安全かつ確実に配送することを目的とする．

3.1 想定システムモデルと前提条件

本研究で想定するシステムモデルを**図 2** に示す．ユーザは個人情報を格納した IC カードを所持している．各クライアントには IC カードリーダが搭載されており，各ユーザに発行された IC カードを用いてユーザ認証を行う．ユーザ認証後，IC カードとサーバの間で相互認証を行い，クライアントへ重要情報を配送する．

想定システムでは，以下の条件を前提とする．

(1) 今後の普及を考え、非接触型 IC カードを利用

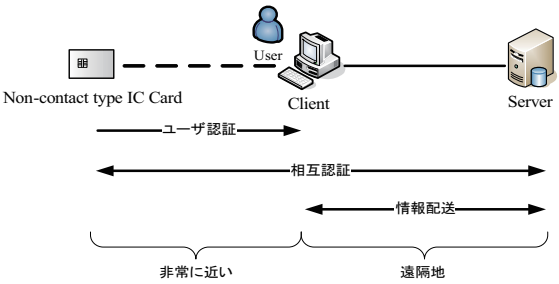


図 2 想定するシステムモデル
Fig. 2 Assumed System Model

する．

(2) IC カードは耐タンパ性を有し，IC カード内部情報が漏洩することはない．

(3) IC カード/クライアント間はユーザが確認できる程の近距離であり，中間者攻撃 (Man-in-the-middle Attack) はできないものとする．

3.2 ユーザ認証方式

ユーザ認証の方法として，一般的にはパスワードが用いられる．より高い安全性を必要とする場合には，生体認証などと組み合わせる．このとき，ユーザ認証情報の格納場所の違いにより，サーバに情報を格納して認証を行うサーバ型認証と IC カード内に情報を格納して認証を行うクライアント型認証に分けられる (**図 3**)．

サーバ型認証は，クライアントで取得した認証情報を，IC カードを経由してサーバへ送信して認証を行う．この認証方式ではサーバ側でユーザ認証と IC カード認証を一括して行うため，IC カードの処理負荷を軽減できるというメリットがある．しかし，ユーザ全員の情報をサーバ側で一括して管理するため，サーバの管理体制が重要となる．このため，大規模な耐タンパハードウェアを用いたり，厳重な設備を準備するといった対策が必要となる．

クライアント型認証は，クライアントで取得した認証情報を IC カードへ送信して IC カード内でユーザ認証を行い，その後 IC カード/サーバ間で IC カード認証を行う．この認証方式ではサーバにおける IC カード認証がユーザ認証を兼ねることになる．IC カードは耐タンパ性を有しているため，パスワードや生体情報などのユーザ認証情報を安全に格納することができるというメリットがある．しかし，IC カードに掛かる処理負荷が大きくなる．

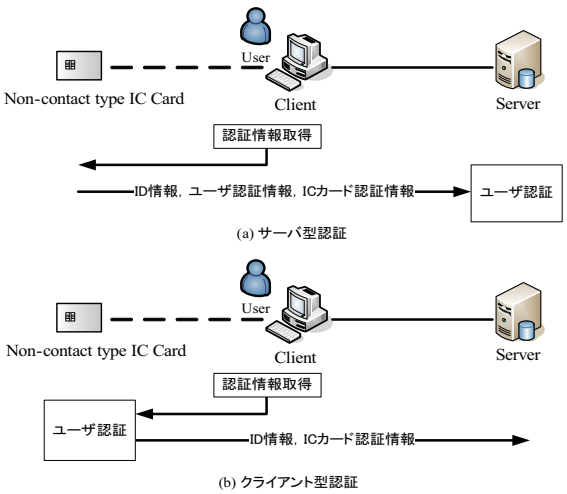


図 3 ユーザ認証方式
Fig. 3 User Authentication Method

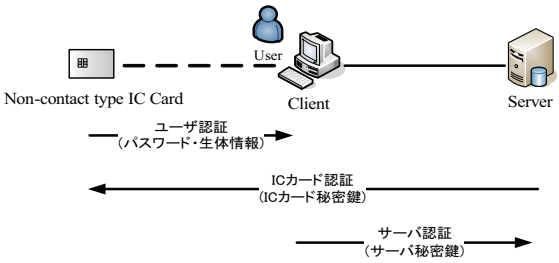


図 4 認証の関係
Fig. 4 Relation of Authentication

本論文ではユーザ認証と IC カード認証を独立して扱うことができ，簡単に安全性が達成できるクライアント型認証を採用する．

3.3 SPAIC における認証の関係

SPAIC ではクライアントには認証動作と情報配送に必要となるプログラムだけを格納し，認証に必要となる秘密情報は一切所持させない．このためクライアントからの情報漏洩の心配がない．

SPAIC では IC カード/クライアント/サーバを独立したものとして環状の認証を行う．SPAIC で行う認証の関係を**図 4** に示す．矢印は認証の方向を示している．ユーザはクライアントを操作しているため，両者は一体のものとみなす．IC カードはパスワードや生体情報を用いてユーザ認証を行うことによりクライアントを認証する．サーバは IC カード秘密鍵から作成されたディジタル署名を検証することにより IC カードを認証する．クライアントはサーバ秘密鍵から作成されたディジタル署名を検証することによりサーバを認証する．

以上の 3 つの経路の認証を実現することにより，クライアント/サーバ間の認証が行われる．

3.4 記号の定義

提案方式の説明に使用する記号を以下のように定義する．

uID：ユーザ ID
PW：パスワード
T：生体情報テンプレート
PSK：事前共有鍵（従来方式）
PrI, PuI：IC カード秘密鍵，公開鍵
PrS, PuS：サーバ秘密鍵，公開鍵
Ni, Nr：乱数
DH1, DH2：Diffie-Hellman 交換値
K：Diffie-Hellman 共通鍵

Ci, Cr:クッキー
$E_Y[X]$：X を鍵 Y で暗号化
$S_I(X)$：IC カードによる X へのディジタル署名
$S_S(X)$：サーバによる X へのディジタル署名
Key_REQ：鍵配送要求パケット
Key_REP：鍵配送応答パケット
Cookie_INIT：クッキー配送要求パケット
Cookie_RESP：クッキー配送応答パケット
CertUser_DIST：ユーザ認証情報配送パケット
SignIC_DIST：IC カード署名情報配送パケット
Info_DIST：情報配送パケット
SignMS_DIST：サーバ署名情報配送パケット

3.5 各端末の情報

事前共有鍵方式と SPAIC が所持する初期情報を**表 1** に示す．ユーザ認証にはパスワードと生体認証を用いるものとする．事前共有鍵方式では，各ユーザが所持する IC カードには，IC カード固有の ID（uID），IC カード秘密鍵 PrI，サーバ公開鍵 PuS，パスワード PW，生体情報テンプレート T が格納されている．サーバには，サーバ秘密鍵 PrS，各 IC カードの ID（uID）と公開鍵 PuI が格納されている．また，IC カード/クライアント間の通信を暗号化するため，事前共有鍵 PSK をすべての IC カード，クライアント端末に所持させる．

SPAIC の場合は，IC カードには，事前共有鍵方式における共有鍵 PSK に代わり，IC カード公開鍵 PuI を格納する，その他の初期情報は同様である．クライアントは初期情報を一切所持しない．また，サーバには，サーバ秘密鍵 PrS，各 IC カードの ID（uID）と公開鍵 PuI を所持する．表 1 に示す初期情報はサーバ側で一括して作成し，IC カードの発行はあらかじめオフラインで実施しておく．IC カード公開鍵 PuI は IC カード秘密鍵 PrI と同時に生成するものであり，この情報を IC カードに格納することによって管理負荷が増えることはない．

表 1 事前共有鍵方式と SPAIC の初期情報
Table 1 Initial Information of PSK Method and SPAIC

	事前共有鍵方式	SPAIC 方式
IC カード	uID	uID
	PrI	PrI
	PuS	PuS
	PW	PW
	T	T
	PSK	PuI
クライアント	PSK	—
サーバ	PrS	PrS
	uID	uID
	PuI	PuI

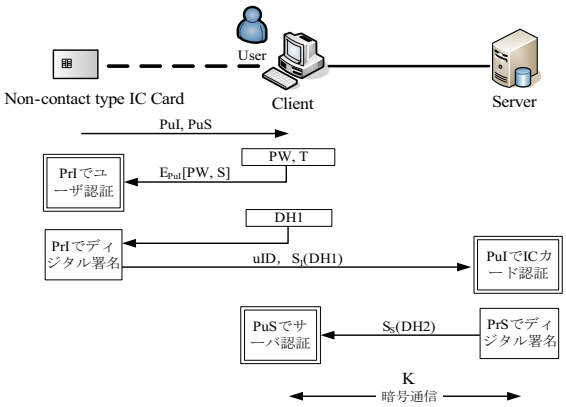


図 5 SPAIC の動作概要
Fig. 5 Outline of SPAIC

3.6 SPAIC の動作

SPAIC の動作概要を**図 5** に示す．SPAIC の認証動作は三段階ある．まず，IC カードは以下の手順によりユーザ認証を行う．ユーザがサーバへアクセスするために，IC カードをかざすと，クライアントとの間にコネクションが確立され，IC カード公開鍵 PuI，サーバ公開鍵 PuS がクライアントに送信される．クライアントにはパスワード入力画面が表示される．ユーザは，ユーザ認証情報となるパスワード PW や生体情報 T をクライアントに入力する．クライアントではユーザ認証情報を IC カード公開鍵 PuI で暗号化し，更に Diffie-Hellman 鍵交換の交換値（DH1）を生成する．これらの情報を IC カードへ送信する．IC カードでは IC カード秘密鍵 PrI を用いてユーザ認証情報（PW や T）を取り出し，内部に保持している秘密情報と照合することによりユーザ認証を行う．上記手順により，間接的にユーザが使用しているクライアントを認証したことになる．

次に，サーバは以下の手順により IC カードを認証する．IC カードは IC カード秘密鍵 PrI を用いて，DH1 にディジタル署名を付加し，ユーザ ID（uID）とともにクライアント経由でサーバへ送信する．サーバでは受信した uID から対応する IC カードの公開鍵 PuI を読み出し，ディジタル署名の検証を行い，IC カードを認証する．IC カードはユーザを認証済みなので、間接的にユーザが使用しているクライアントを認証したことになる．サーバは同時に DH1 を取得する．

最後に，以下の手順によりクライアントはサーバを認証する．サーバは DH 交換値（DH2）を生成し，サーバ秘密鍵 PrS を用いてディジタル署名を行いクライアントへ送信する．クライアントでは，IC カードから受信したサーバ公開鍵 PuS を利用してディジ

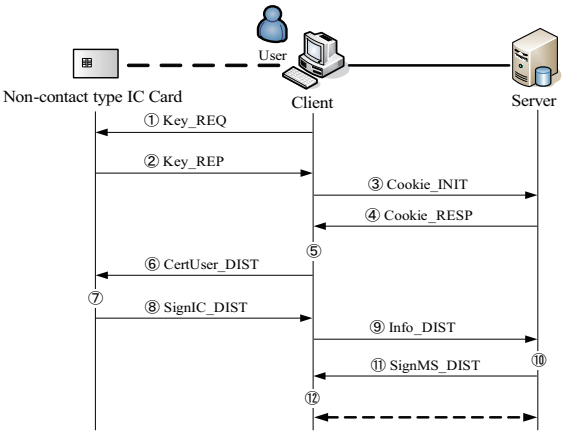


図 6 SPAIC の詳細シーケンス
Fig. 6 SPAIC Sequence in Detail

タル署名の検証を行い，サーバを認証する．

以上の 3 つの経路の認証により，クライアント/サーバ間の認証が完了する．上記手順の中で DH1，DH2 の共有が行われているため，クライアント，サーバは共通暗号鍵 K を生成できる．以降のクライアント/サーバ間の通信は K を用いて行う．

3.7 SPAIC の詳細シーケンス

SPAIC の詳細シーケンスを**図 6** に示す．

実際の認証システムにおいては，サービス不能攻撃（DoS 攻撃）やリプレイ攻撃への対応が重要となる．

DoS 攻撃に対しては，クライアント/サーバ間でクッキー交換することにより対応する．クッキーの値は，通信相手の ID，IP アドレスと乱数をもとに生成される．クッキーは通信ごとに異なる値が生成されるため，IC カード認証時にクライアントからサーバへのパケットに含むことにより無関係な端末からの DoS 攻撃を防止することができる．

リプレイ攻撃に対しては，IC カードが生成する乱数 Ni とクッキー交換時に送信される乱数 Nr を利用することで対応する．乱数 Nr は，IC カード認証情報が認証時に作成されたものであるかどうかを確認するためにも利用する．

(1) IC カードへ Key_REQ を送信
クライアントはユーザ認証情報などの暗号化を行うために，IC カードへ公開鍵等の情報配送を要求する．

(2) Key_REP を送信
IC カードはユーザ ID(uID)，IC カード公開鍵 PuI，サーバ公開鍵 PuS，乱数 Ni を送信する．
uID, PuI, PuS, Ni

(3) Cookie_INIT を送信
クライアントは DoS 攻撃を防止するためのクッキー Ci を生成して，サーバへ送信する．
Ci

(4) Cookie_RESP の送信
サーバは乱数 Nr とクッキー Cr を生成する．また，クッキー Ci と共にクライアントへ送信する．
Ci, Cr, Nr

(5) ユーザ認証情報の暗号化
クライアントでは IC カードから受け取った乱数 Ni とユーザ認証情報 (PW, S) を PuI で暗号化する．同時にサーバから受け取った乱数 Nr を PuS で暗号化する．また，Diffie-Hellman 交換値 DH1 を生成する．
E_{PuI}[PW, S, Ni], E_{PuS}[Nr], DH1

(6) CertUser_DIST の送信
（5）で作成した認証情報を IC カードへ送信する．
E_{PuI}[PW, S, Ni], E_{PuS}[Nr], DH1

(7) ユーザ認証，IC カード認証情報の生成
IC カードでは IC カード秘密鍵 PrI を利用して PW，S，Ni を取り出しユーザ認証を行う．更に，生成した Ni と比較する．ユーザ認証後，E_{PuS}[Nr] に DH1 を付加して，これらの情報に IC カード秘密鍵 PrI でディジタル署名を作成する．
S_I(DH1, E_{PuS}[Nr])

(8) SignIC_DIST の送信
（7）で作成した IC カード認証情報を uID と共にクライアントへ送信する．
uID, S_I(DH1, E_{PuS}[Nr])

(9) Info_DIST の送信
クライアントは（8）で受信した IC カード認証情報を（4）で受信したクッキー Ci, Cr と共にサーバへ送信する．
uID, S_I(DH1, E_{PuS}[Nr]), Ci, Cr

(10) IC カード認証，サーバ認証情報の生成
サーバではクライアントが送ってきたクッキーの正当性を確認する．また，uID から該当する IC カード公開鍵 PuI を読み出し，ディジタル署名の検証を行い，IC カードを認証する．同時に，サーバ秘密鍵 PrS を利用して Nr を取り出し，生成した Nr と比較する．その後，Diffie-Hellman 交換値 DH2 を生成し，サーバ秘密鍵 PrS を用いてサーバ認証を行うためのディジタル署名を作成する．更に，取得した DH1 と

DH2 を利用して共通暗号鍵 K を生成する．
S_S(DH2), K

(11) SignMS_DIST の送信
（10）で作成した署名情報とクッキー Ci，Cr をクライアントへ送信する．
S_S(DH2), Ci, Cr

(12) サーバ認証
クライアントではサーバが送ってきたクッキーの正当性を確認する．また，あらかじめ受信した PuS を利用しディジタル署名の検証を行い，サーバを認証する．その後 DH2 を取得する．更に，DH1，DH2 を利用して共通暗号鍵 K を生成する．
K

以降のクライアント/サーバ間の暗号通信はこの暗号鍵 K を用いて行う。

4. 評　　価

事前共有鍵方式と SPAIC の比較を**表 2** に示す．SPAIC ではクライアント端末に格納する情報が動作プログラムのみであるため，クライアントからの情報漏洩の心配がないという利点がある．

事前共有鍵方式では，システムの安全上事前共有鍵を頻繁に更新する必要があるため，運用時の管理が煩雑になる．一方 SPAIC ではユーザの追加，削除程度の作業で済むため，管理負荷の低減が見込まれる．

SPAIC では，IC カードで公開鍵演算を行うため，IC カードへの処理負荷の増加が懸念される．しかし，SPAIC が動作するのはクライアントの立ち上げ時のみであるため，実用上大きな影響を与えるものではないと考えられる．

5. おわりに

本論文では，事前共有鍵方式においてクライアント端末からの情報漏洩の問題を解決するために，クライアント端末が動作プログラム以外の初期情報を一切所持しないというモデルを定義し，非接触型 IC カードを用いてサーバからクライアントに重要情報を配送することを可能とするプロトコル SPAIC の提案を行った．

表 2　事前共有鍵方式と SPAIC の比較
Table 2　Comparison of PSK method and SPAIC

	事前共有鍵方式	SPAIC
クライアントに格納する情報	動作プログラム，事前共有鍵（×）	動作プログラムのみ（○）
管理負荷	共有鍵の変更が面倒（×）	ユーザの追加、削除程度（○）
IC カードへの負荷	中程度（○）	高い（△）

IC カード公開鍵を新たに IC カードに所持させることにより，クライアントが初期情報を持たなくとも IC カード/クライアント間の暗号通信を行い，IC カード/クライアント/サーバ間での確実な認証を可能にした．更に，クライアント/サーバ間で Diffie-Hellman 鍵交換で作成した暗号鍵を利用することにより，安全に重要情報を配送するための通信経路を確立した．

本方式では，IC カードで行う公開鍵暗号方式の処理のため，パフォーマンスの低下が予想されるが，立ち上げ時の認証において十分に利用できると考えられる．今後実装を行い，性能評価を行う予定である．

参　考　文　献

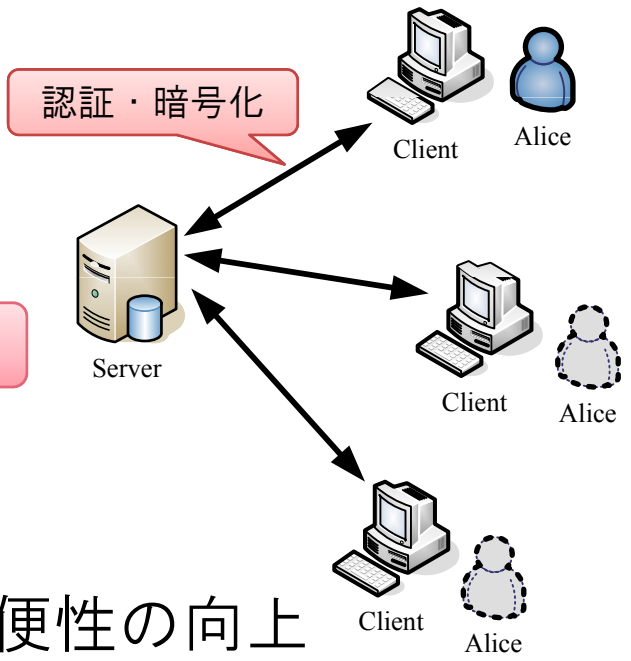
1) Maughan, D., Schertler, M., Schneider, M. and Turner, J.: Internet Security Association and Key Management Protocol (ISAKMP), RFC2408, IETF (1998).
2) 渡邊　晃，厚井裕司，井手口哲夫，横山幸夫，妹尾尚一郎 : 暗号技術を用いたセキュア通信グループの構築方式とその実現，情報処理学会論文誌，Vol.38, No.4, pp.904–914 (1997).
3) 渡邊　晃，岡崎直宣，朴　美娘，井手口哲夫，笹瀬　巌 : イントラネット閉域通信グループの構築に適した安全な鍵配送方式とその運用管理方式，電気学会論文誌 C，Vol.121, No.9, pp.1429–1438 (2001).
4) 瀬戸洋一 : ユビキタス時代のバイオメトリクスセキュリティ，日本工業出版 (2003).
5) 今本健二，櫻井幸一 : 認証付き鍵交換における動的情報管理に関する考察，電子情報通信学会技術研究報告，Vol.102, No.74, pp.91–96 (2003).
6) 磯部義明，三村昌弘，瀬戸洋一，菊地良知 : 本人認証 IC カードによる高セキュリティシステムの構築，情報処理学会コンピュータセキュリティ研究報告，Vol.99-CSEC-4, No.24, pp.55–60 (1999).
7) 影井良貴 : IC カードの動向，情報処理学会会誌，Vol.39, No.5, pp.429–433 (1998).
8) 吉田　壱，平田真一 : IC カード技術の現状と課題，情報処理学会会誌，Vol.43, No.3, pp.296–303 (2002).
9) 伊藤雅彦 : 非接触 IC カード技術とその応用，情報処理学会会誌，Vol.43, No.3, pp.304–307 (2002).
10) IC カードシステム利用促進協議会 : JICSAP IC カード仕様書 V2.0 (2001).
11) Rescorla, E.: Diffie-Hellman Key Agreement Method, RFC2631, IETF (1999).
12) Kaufman, C.: Internet Key Exchange (IKEv2) Protocol, RFC4306, IETF (2005).
13) Schiller, J.: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), RFC4307, IETF (2005).

非接触型ICカードを用いた認証方式SPAICの提案

名城大学大学院　理工学研究科
東　長俊　鈴木秀和　渡邊　晃

研究背景

- クライアント/サーバ間通信
  - 重要な情報を交換時、認証と暗号化が不可欠
- 異なるクライアントからサーバへアクセス
  - 認証と暗号化が必要

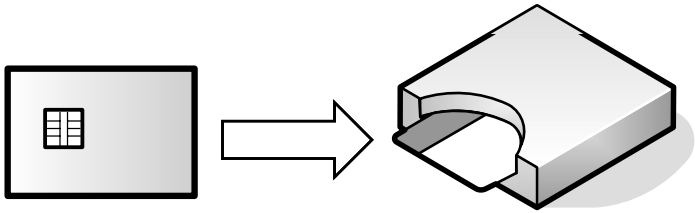


ICカードを利用する方式が注目

- カード内部で暗号・認証できる
- 情報漏洩を防ぐ耐タンパ性
- 非接触型ICカードの登場による利便性の向上

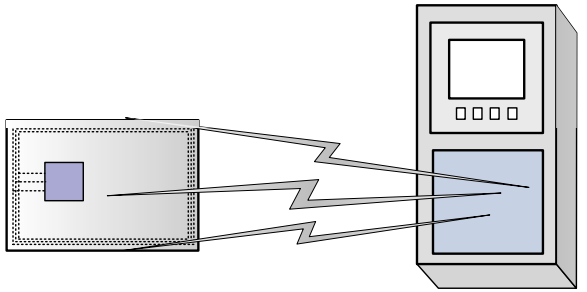
ICカードの分類

- 接触型ICカード
  - IC CardとClientを一体と見なせる
  - IC Card/Client間で暗号通信を行わない



ICカードをリーダライタに差し込む

- 非接触型ICカード
  - IC CardとClient間で無線通信
  - IC Card/Client間で暗号化が必須



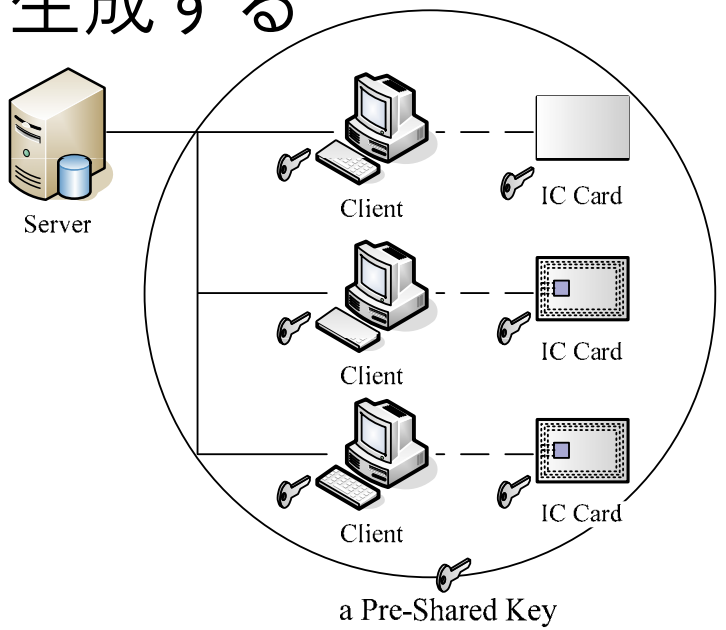
ICカードを差し込む必要がない

既存技術と課題

- IC Card/Client間の暗号化技術
  - 事前共有鍵方式（Pre-Shared Key Method）
    →JICSAPで定義
- 事前に共有鍵を全てのIC Card、Clientで共有する
- 共有鍵を用いて暗号化キーを生成する

課 題

- Clientから共有鍵が漏洩
  - 漏洩時の影響が全体に波及
- 共有鍵を定期的に変更必要
  - 管理が非常に煩雑となる



*JICSAP：日本ICカードシステム利用促進協議会

提案方式：SPAIC

目 的

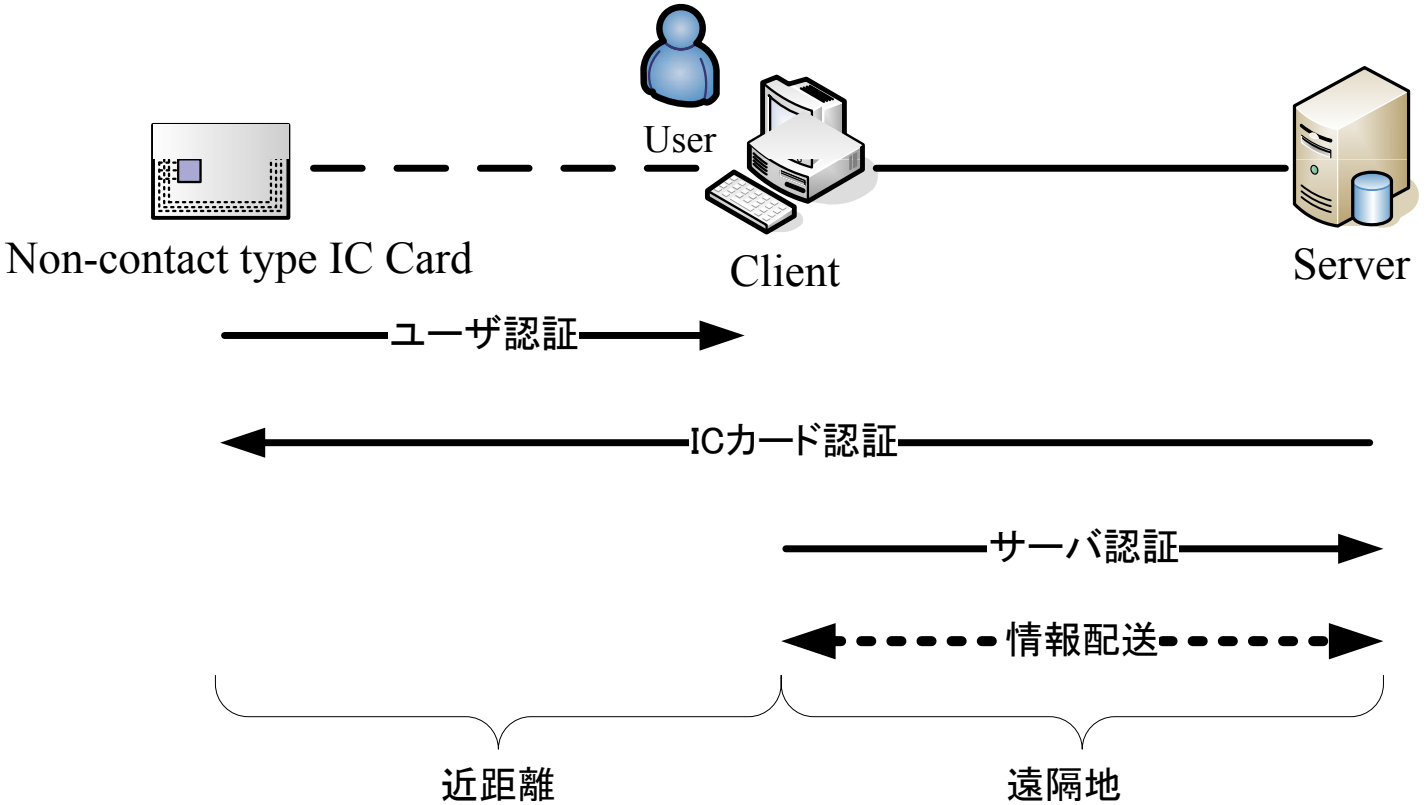
- 非接触ICカードを用いてServerからClientへ重要情報を安全に配送するための通信経路の確立

概 要

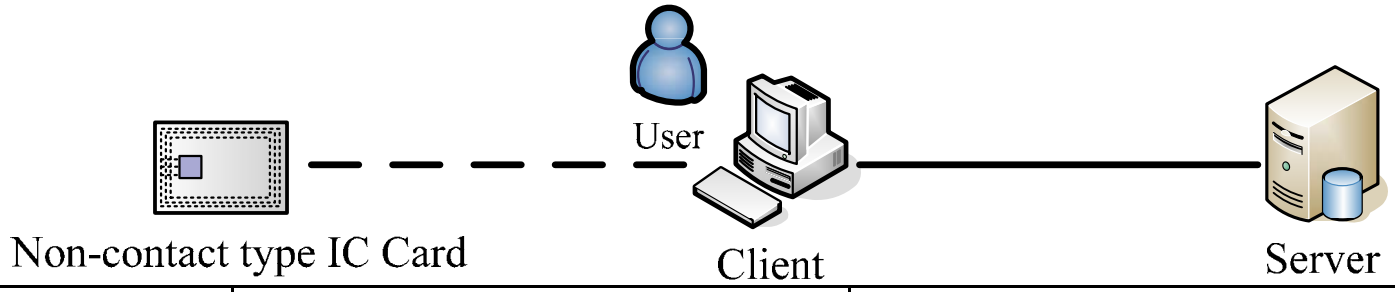
- SPAIC: Secure Protocol for Authentication with IC Card
- IC Card/Client間の認証には
  - IC Card公開鍵を利用
- Client/Server間の重要情報の配送には
  - Diffie-Hellman鍵交換による暗号鍵を生成

想定システムモデル

- 非接触型ICカードの利用を前提
- Clientに初期情報を一切所持しない
- IC Card/Client/Serverを独立したものとして環状の認証

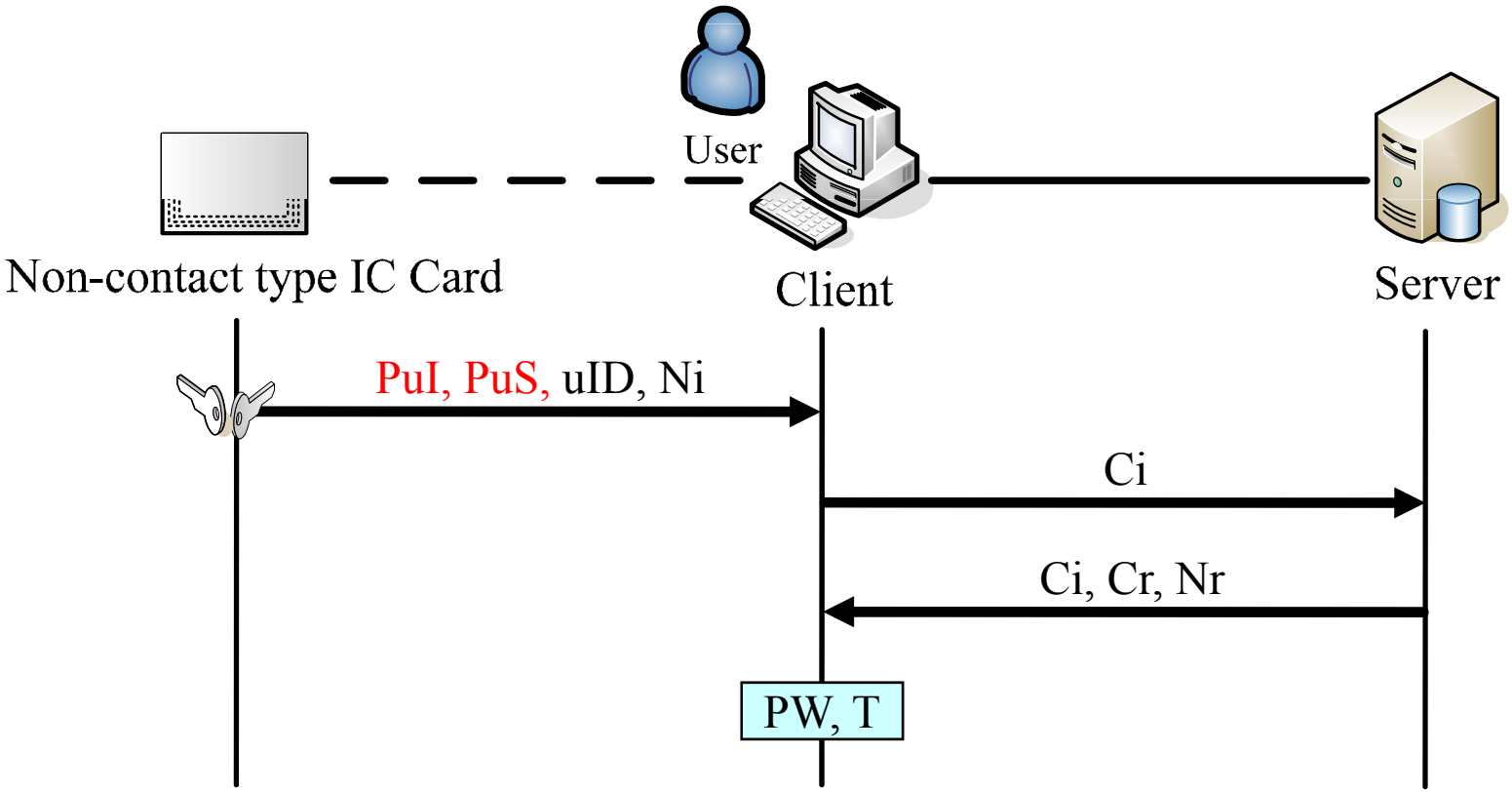


SPAICの初期情報



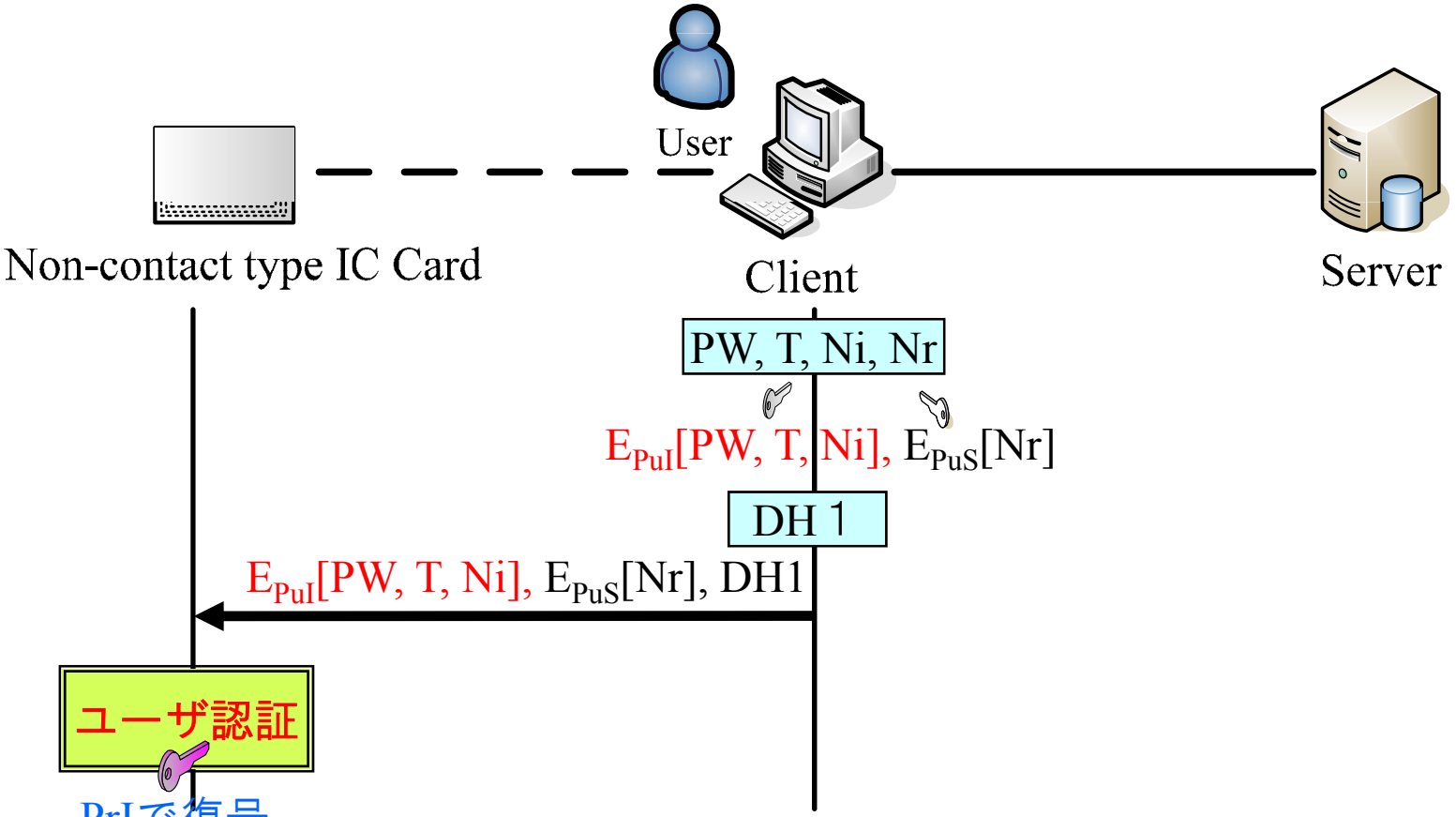
	事前共有鍵方式	SPAIC方式
IC Card	ユーザID（uID） ICカード秘密鍵（PrI） サーバ公開鍵（PuS） パスワード情報（PW） 生体情報テンプレート（T） ***事前共有鍵 （PSK）***	ユーザID（uID） ICカード秘密鍵（PrI） サーバ公開鍵（PuS） パスワード情報 （PW） 生体情報テンプレート（T） ***ICカード公開鍵 （PuI）***
Client	***事前共有鍵 （PSK）***	*なし*
Server	サーバ秘密鍵（PrS） ユーザID（uID） ICカード公開鍵（PuI）	サーバ秘密鍵（PrS） ユーザID（uID） ICカード公開鍵（PuI）

SPAICの動作：ユーザ認証(1)



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

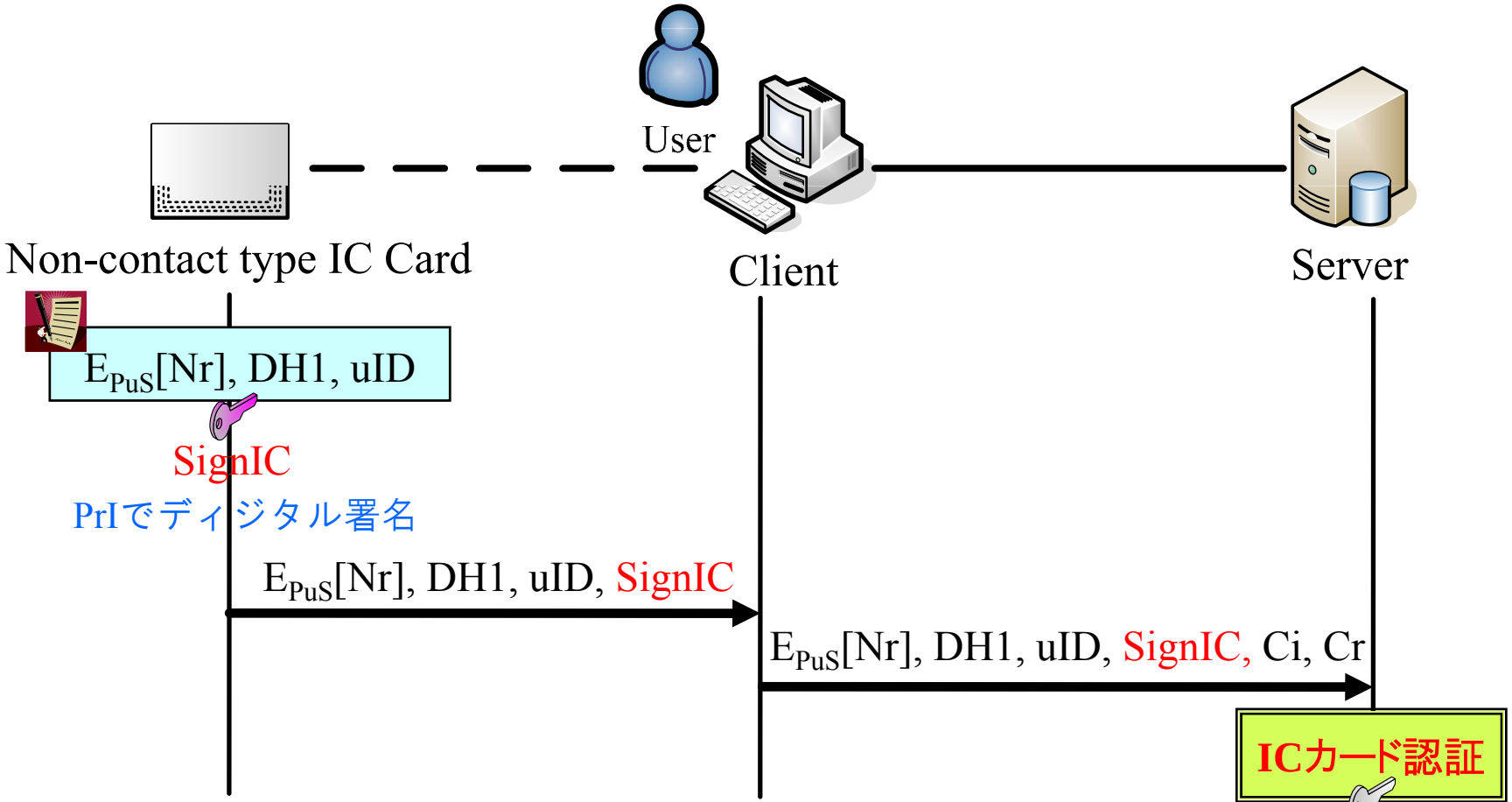
SPAICの動作：ユーザ認証(2)



間接的にクライアントを認証

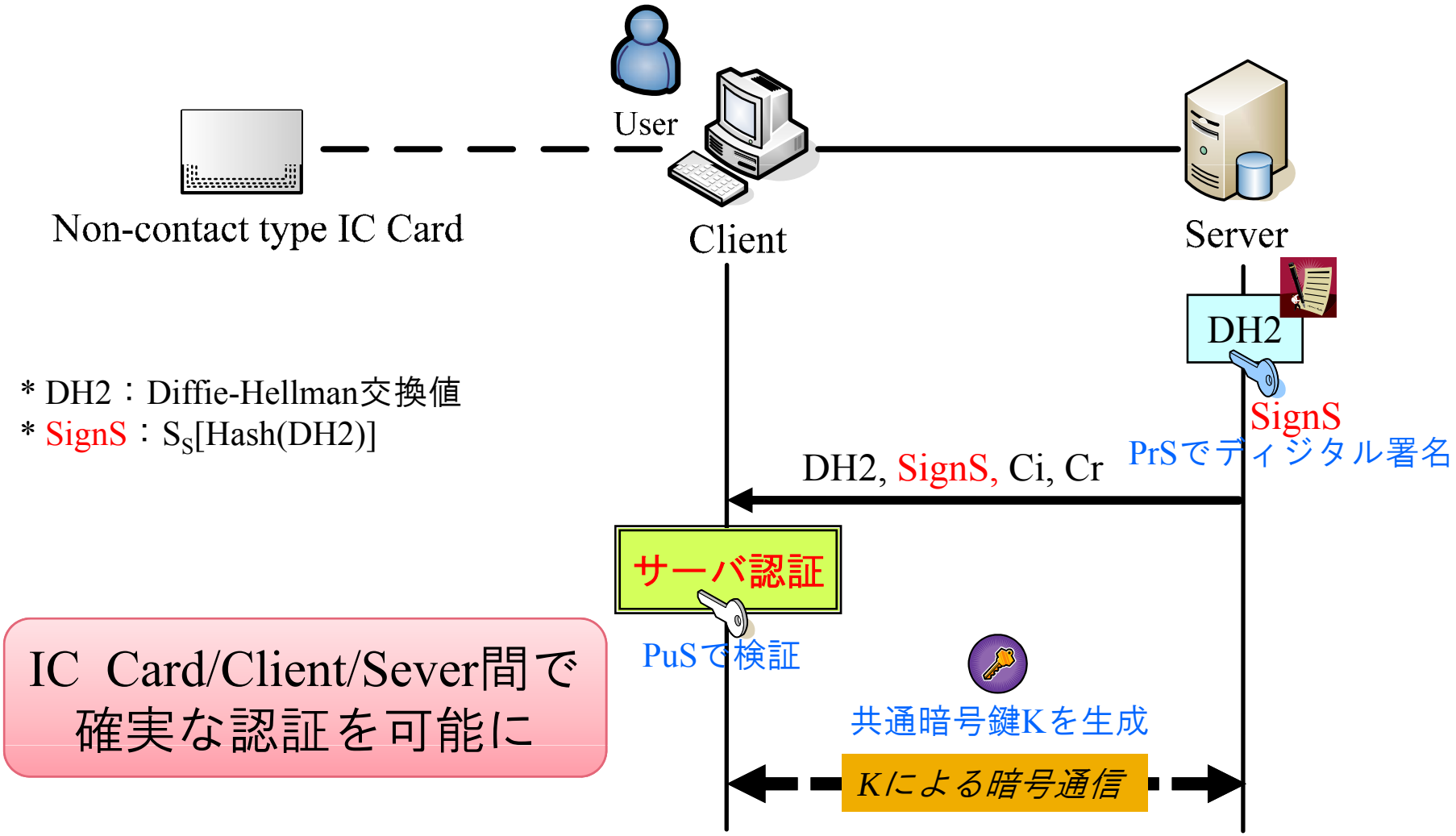
* E_{PuI}[PW, T, Ni]：PW, T, NiをPuIで暗号化
* E_{PuS}[Nr]：NrをPuSで暗号化
* DH1：Diffie-Hellman交換値

SPAICの動作：ICカード認証



* SignIC：S_I[Hash(E_{PuS}[Nr], DH1, uID)]

SPAICの動作：サーバ認証



* DH2：Diffie-Hellman交換値
* SignS：S_S[Hash(DH2)]

IC Card/Client/Sever間で
確実な認証を可能に

評価

	事前共有鍵方式	SPAIC方式
Clientに格納する情報	× 動作プログラム、事前共有鍵	○ 動作プログラムのみ
管理負荷	× 共有鍵の変更が面倒	○ ユーザの追加、削除
IC Card/Client間の暗号	○ 事前共有鍵を利用	○ 公開鍵方式を利用
IC Cardへの負荷	○ 中程度	△ 高い

まとめ

- SPAICの提案
  - クライアントが初期情報を所持しないというモデルを定義
  - 非接触型ICカードを用いた認証方式
  - 重要情報を配送するための通信経路を確立
- 今後の課題
  - 実装による詳細な性能評価を行う