非接触型 IC カードを用いた重要情報の配送方式 SPAIC の提案

Researches on SPAIC: Secure Protocol for Authentication with IC Card

束　長俊　　鈴木　秀和　　渡邊　晃
Changjun Shu　Hidekazu Suzuki　Akira Watanabe

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

１．まえがき

IC カードが幅広い分野で応用されている．近年では非接触型 IC カードの登場によって，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．そのため，IC カードとクライアント間も暗号化されることが望ましい．特に，非接触 IC カードでは，暗号化が必須となる．

このような要望を満たす方法として，すべての IC カード及びクライアントに共通鍵を所持させる方式がある．しかし，この方式ではクライアント側から共通鍵が漏洩した場合，影響がシステム全体に波及する可能性がある．そのため，クライアントは秘密情報を一切所持させない方法が望ましい．

本稿では，非接触型 IC カードを利用し，サーバから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（Secure Protocol for Authentication with IC card）を提案する．

２．SPAIC の概要

SPAIC では，クライアント端末に動作プログラムだけを格納し，認証に必要となる初期情報は全て IC カードが保持すると言うモデルを想定する．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．

SPAIC の動作概要を図１に示す．まず，IC カードは以下の手順によりユーザ認証を行う．ユーザは，ユーザ認証情報となるパスワードや生体情報をクライアントに入力する．IC カードからクライアントへは IC カード公開鍵，サーバ公開鍵を送信する．クライアントではユーザ認証情報を IC カード公開鍵で暗号化し、更に Diffie-Hellman 鍵交換の交換値（DH 交換値１）を生成し，サーバ公開鍵で暗号化する．これらの情報を IC カードへ送信する．IC カードでは IC カード秘密鍵を用いてユーザ認証情報を取り出し，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．

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 カード秘密鍵を用いて，サーバ公開鍵で暗号化されている情報にディジタル署名を付加し，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 IC カード ID から対応する IC カードの公開鍵を用いて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 DH 交換値１を取得する．

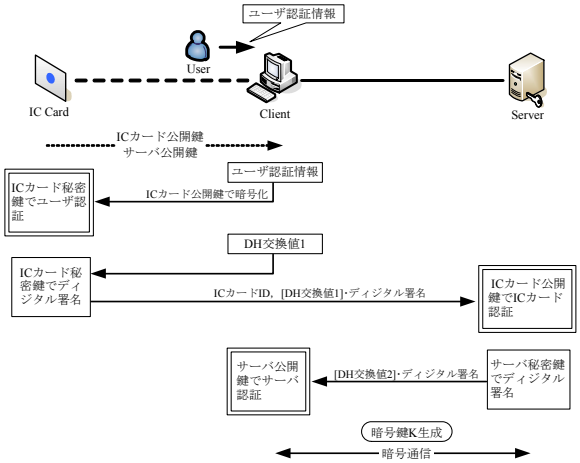


図１　SPAIC の概要

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．サーバは新たな DH 交換値２を生成し，サーバ秘密鍵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を利用してディジ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/サーバ間で確実な認証を行うことができる．

上記手順の中で DH 交換値１，２の共有が行われているため，クライアント，サーバは上記手順で得られた DH 交換値を用いて共通の暗号鍵を生成する．以降のクライアント/サーバ間の通信はこの共通暗号鍵を用いて暗号化される．

IC カード内には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存することなくユーザの認証とクライアントへの情報配送を行うことが可能になる．

３．むすび

本稿では，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．SPAIC は，非接触 IC カードを利用したシステムにおける有効な手段である．

今後は実装を行い，詳細な評価を行う予定である．

文　献

[1] 伊藤政彦，“非接触 IC 技術とその応用”，情報処理学会会誌 Vol.43 No.3　Mar. 2002

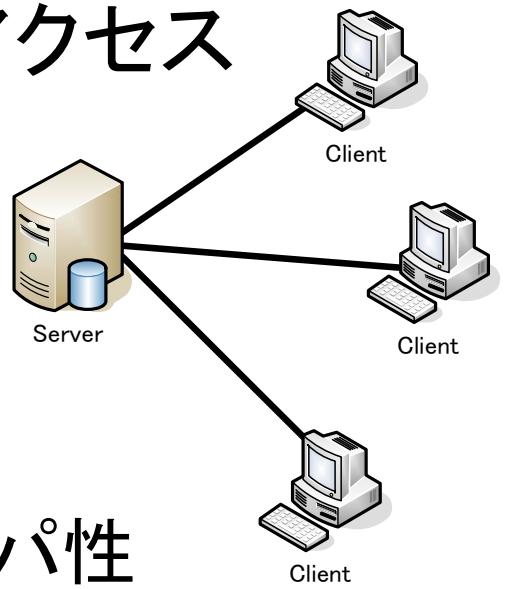
[2] 保母雅敏，渡邊晃，“IC カードを用いた重要情報の配送方式 SPAIC の検討”，DICOMO2005 シンポジウム，Jul.2005

非接触型ICカードを用いた重要情報の配送方式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

はじめに

- 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

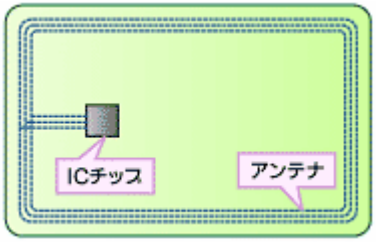


- ICカードを利用した認証方式
  - ICカード内で暗号・認証処理が可能
  - 外部から不正読み取りを防ぐ耐タンパ性
  - 非接触型ICカードの登場による利便性の向上

ICカードモデル

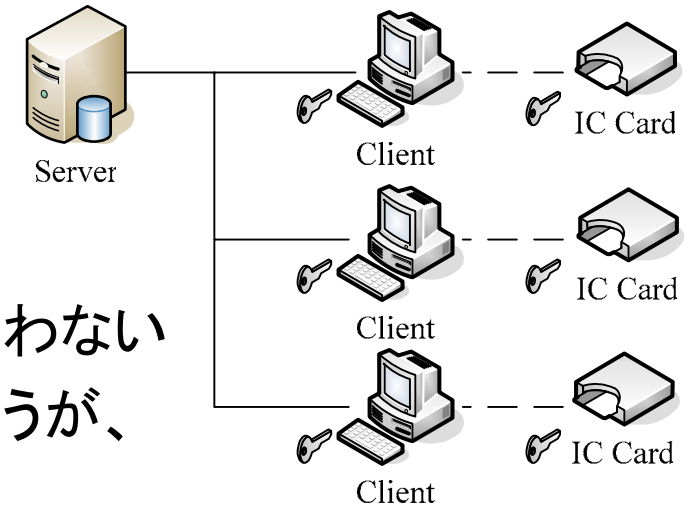
- 接触型ICカード
  - ICカードとクライアントを一体とみなす
  - ICカード/クライアント間暗号通信を行わない

- 非接触型ICカード
  - ICカード/クライアント間で無線通信
  - ICカード/クライアント間で暗号化が必須



従来の暗号・認証方式と課題

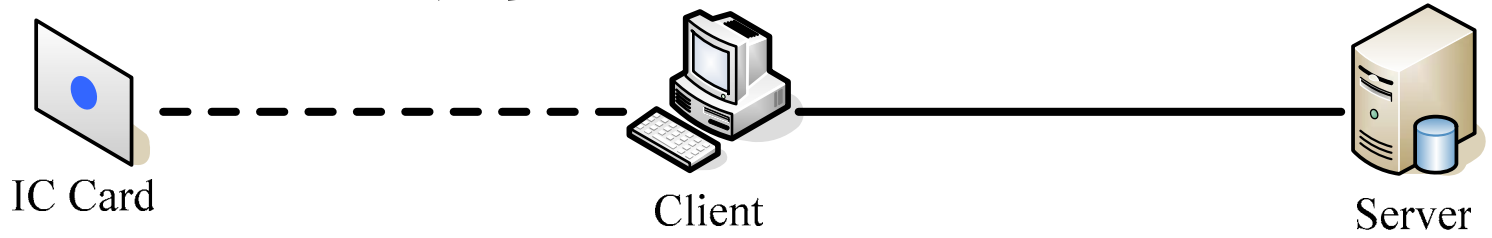
- 事前共有鍵方式
  - 事前共有鍵をすべてのICカード、クライアントに所持する
- クライアントから共有鍵が漏洩する可能性
- 共有鍵を定期的に変更必要



- 実際の運用
  - ICカード/クライアント間暗号通信を行わない
  - ICカード/クライアント間暗号通信を行うが、共有鍵を変更しない

SPAICプロトコルを提案

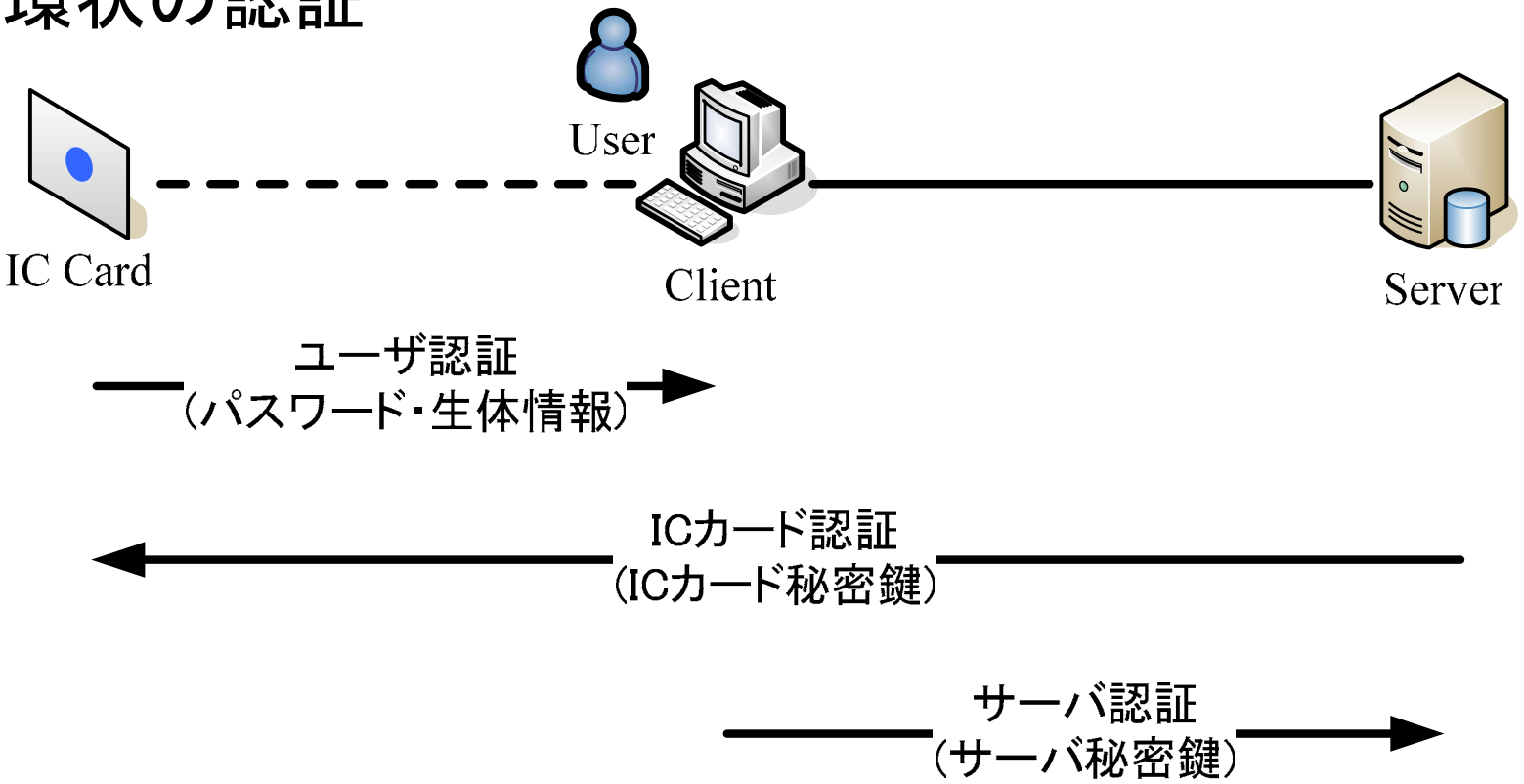
SPAICの概要



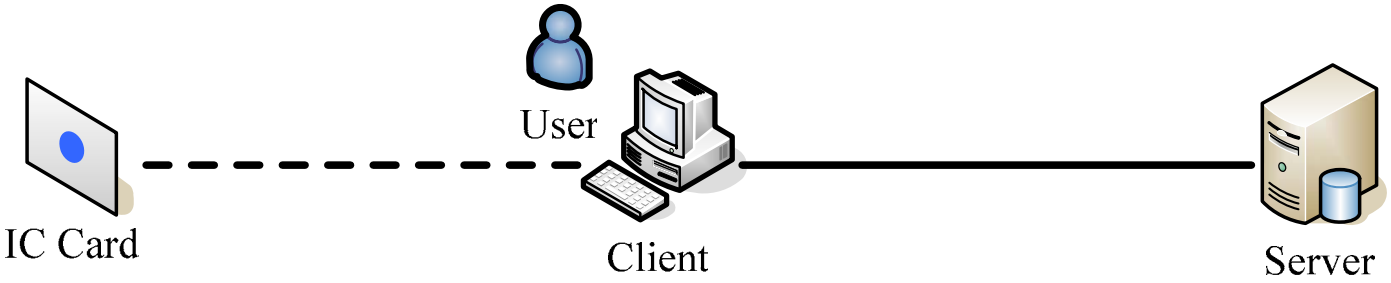
- SPAIC：Secure Protocol for Authentication with IC Card
- 非接触型ICカードの利用を前提
- クライアントに初期情報を一切所持しない
  - 情報漏洩の防止
- ICカード/クライアント間の認証にはICカード公開鍵を利用
- クライアント/サーバ間の重要情報の配送にはDiffie-Hellman鍵交換による暗号鍵生成

SPAICの認証関係

- 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

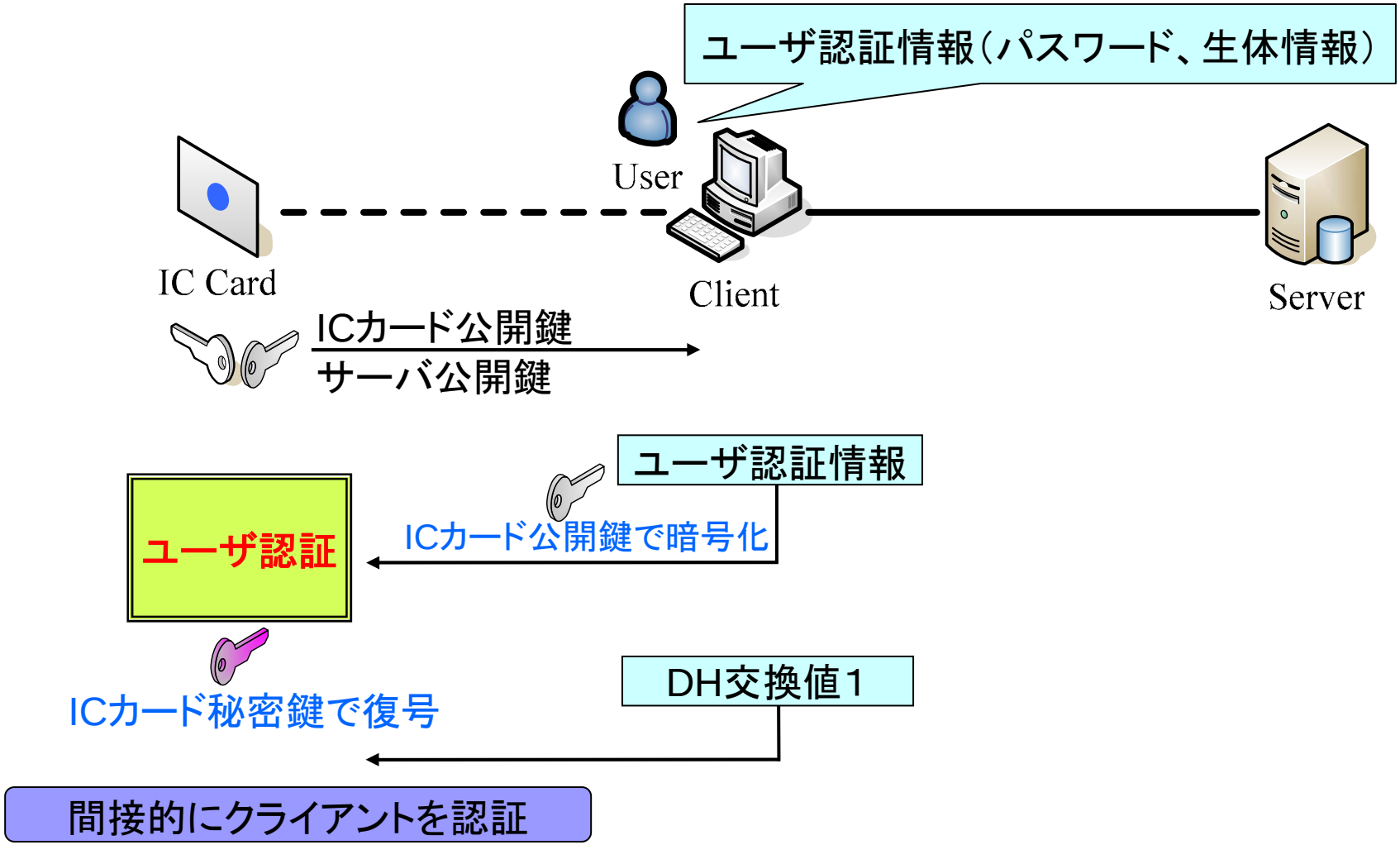


SPAICの初期情報

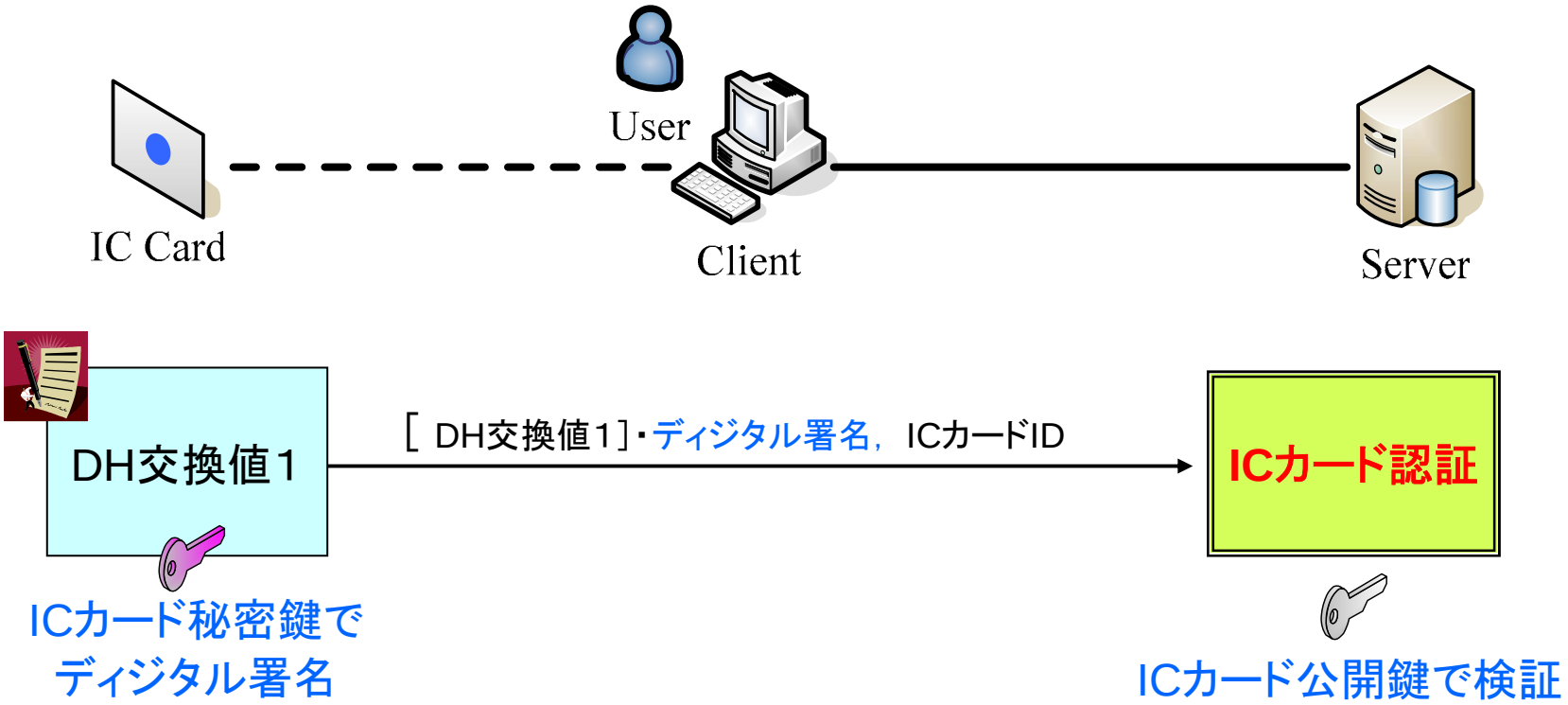


ICカード	ICカードID ICカード秘密鍵 サーバ公開鍵 パスワード情報 生体情報テンプレート ~~事前共有鍵~~ ~~ICカード公開鍵~~
クライアント	~~事前共有鍵~~
サーバ	サーバ秘密鍵 ICカードID ICカード公開鍵

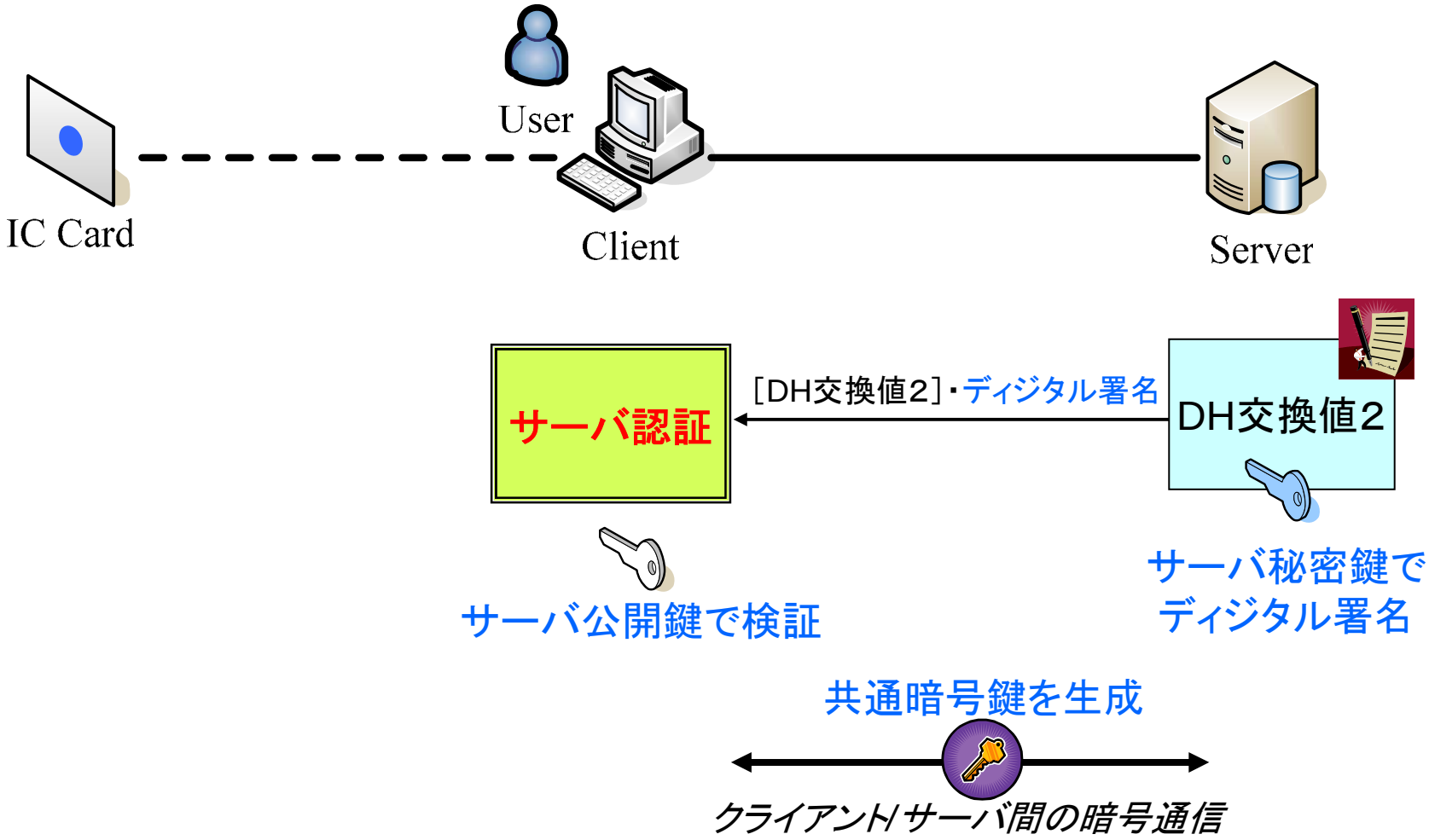
SPAICの動作1：ユーザ認証



SPAICの動作2：ICカード認証



SPAICの動作3：サーバ認証



評価

	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/クライアント間の暗号	○ 事前共有鍵を利用	○ 公開鍵方式を利用
ICカードへの負荷	○ 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カードを用いた新しい情報配送プロトコル
- 今後の課題
  - 実装による詳細な評価を行う