非接触型 IC カードを用いた認証方式 SPAIC の提案と実装

063432019　束　長俊
渡邊研究室

1.　はじめに

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となる．また，ユーザが自由に移動する環境においても認証と暗号化による情報配送を行いたいという要求がある．

このような要求を満たす方式として，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 カードと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事前共通鍵を利用する方式があるが，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．

2.　既存技術とその課題

従来システムでは，接触型 IC カードを IC カードリーダに挿入し，IC カードとサーバ間で認証プロセスを行う．IC カードとクライアントが一体のものであるとみなせるため，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．一方，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，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日本 IC カードシステム利用促進協議会で定義されている[1].

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．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．

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.　SPAIC の概要

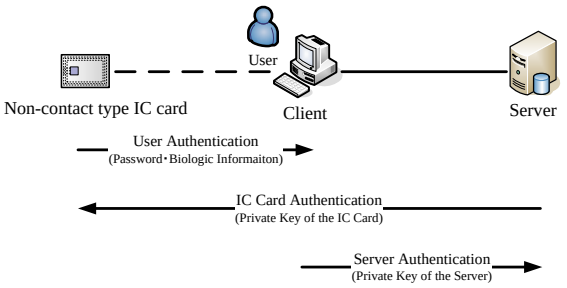


図 1　認証の関係

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．これを実現するために，IC カードに格納する初期情報として，事前共有鍵に代わり，新たに IC カード公開鍵を格納する．

SPAIC で行う認証の関係を**図 1** に示す．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．

3.2.　SPAIC の動作

SPAIC の動作概要を図 2 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 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．クライアントにはユーザ認証情報入力画面が表示される．ユーザは，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[2]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．

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

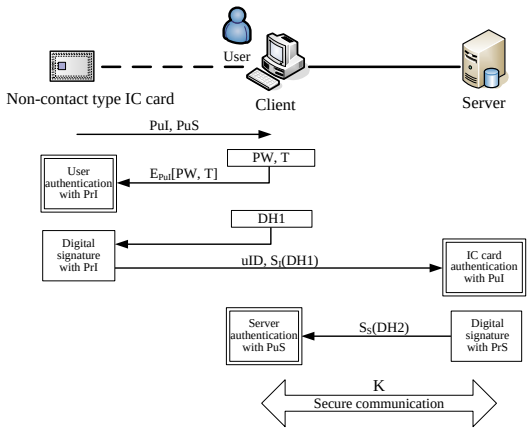


図 2　SPAIC の動作概要

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/サーバ間の通信はこの暗号鍵 K を用いて行う．

4.　実装

4.1.　モジュール構成

クライアントおよびサーバにおける試作システムの実装モジュール構成を図 3 に示す．クライアントの処理は，メインモジュールと，初期処理，認証情報取得，

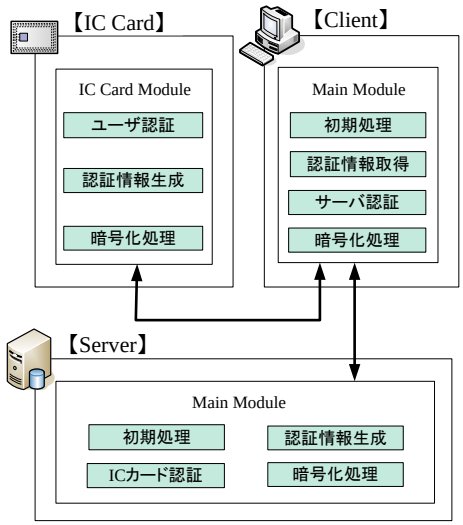


図 3　モジュール構成

サーバ認証，および暗号化処理サブモジュールにより構成される．IC カードの処理は，ユーザ認証，認証情報生成，および暗号化処理モジュールにより構成される．サーバの処理は，メインモジュールと，初期処理，IC カード認証，認証情報生成，および暗号化処理サブモジュールにより構成される．

4.2.　USB トークンによる試作

SPAIC では非接触 IC カードを利用することを前提としているが， IC カードにプログラムを組み込むのは現時点では困難である．そこで，試作システムの実装には，IC カードの代わりに USB トークンを利用することとした．

試作システムでは，IC カード内で実現すべきプログラムの一部が PC 上での開発となる．将来的には，この部分をそのまま IC カードへ移植することが可能である．

5.　評価

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．

6.　むすび

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．

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．

参考文献

[1] 日本 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”，Jul. 2001

[2] Diffie, W. and Hellman, M.: New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp.644-654 (1976).

非接触型ICカードを用いた認証方式SPAICの提案と実装

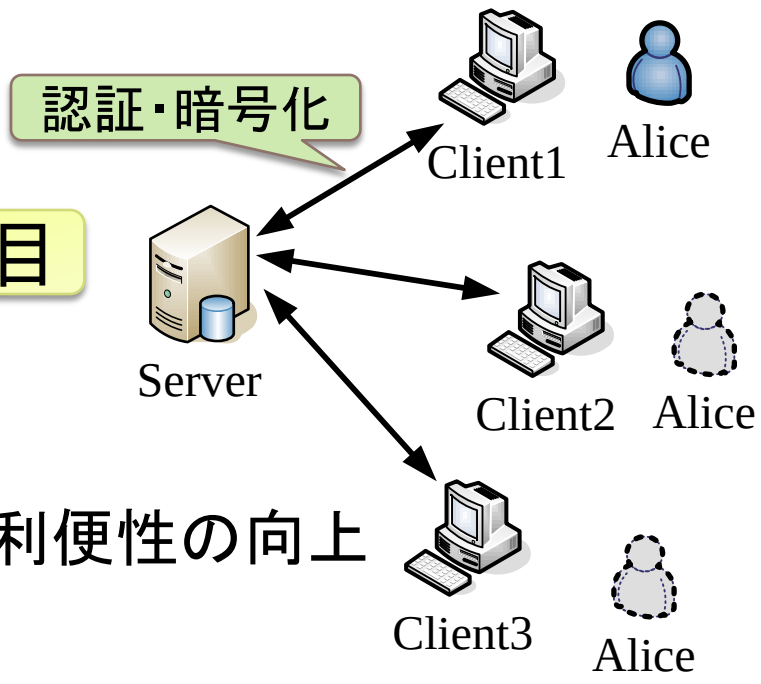
渡邊研究室
063432019
束　長俊

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

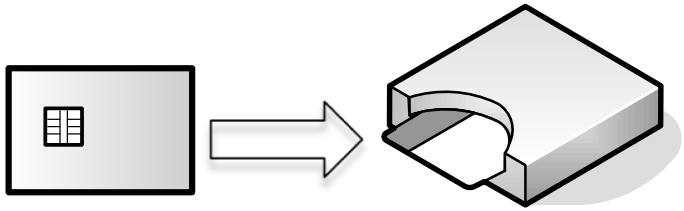
ICカードを利用する方式が注目

- カード内部で暗号・認証可能
- 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



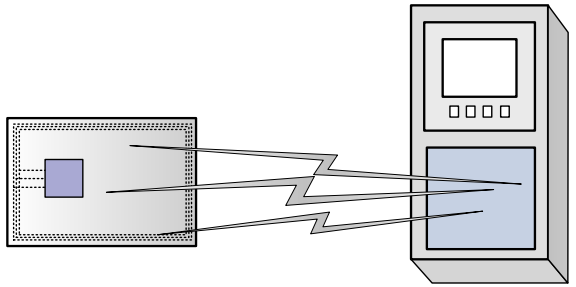
ICカードの分類

- 接触型ICカード
  - IC CardとClientを一体と見なせる
  - IC Card/Client間で暗号通信は不要



Insert

- 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



Wireless Communication

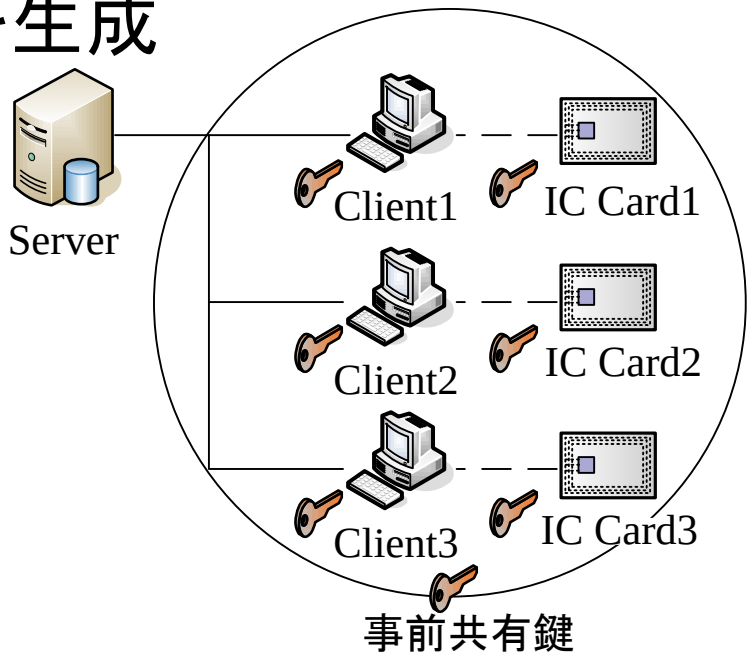
既存技術と課題

- 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
- 共有鍵を用いて暗号化キーを生成

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

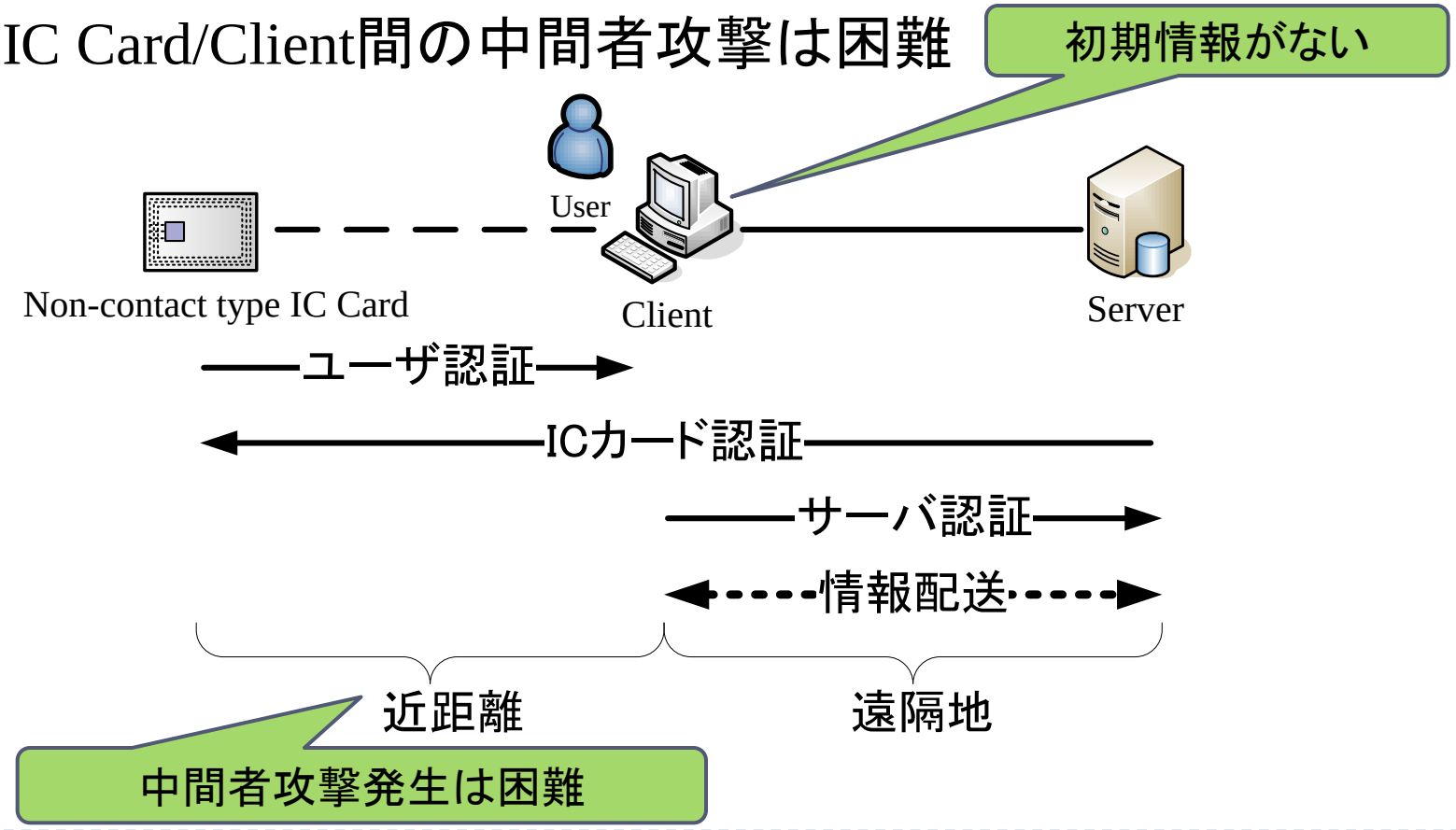
関連技術

- 公開鍵暗号
  - 暗号化と復号に異なる鍵を使用する暗号方式
  - 一方の鍵で暗号化したものは、もう一方の鍵でしか復号化できない
  - デジタル署名による認証も可能
  - 演算に時間がかかる→共通鍵暗号との併用

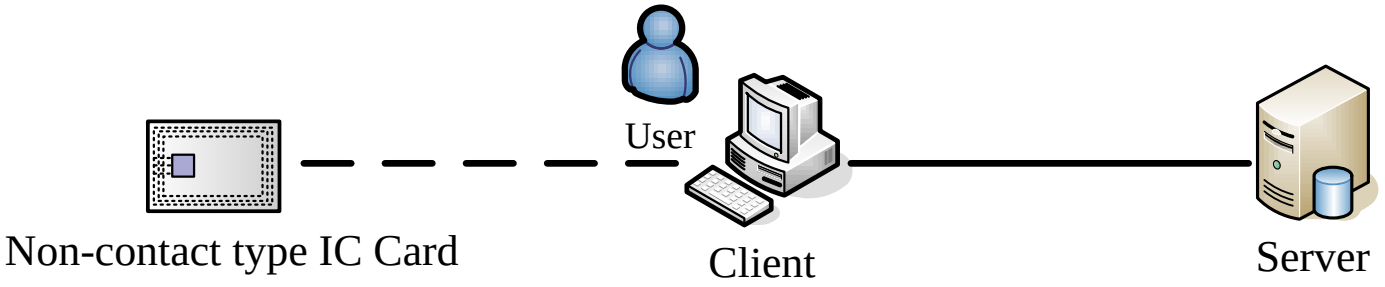
- Diffie-Hellman鍵交換
  - 乱数を通信路上で交換して、共通鍵を生成
  - 第三者が乱数を盗聴しても、鍵の取得が不可能

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間の中間者攻撃は困難



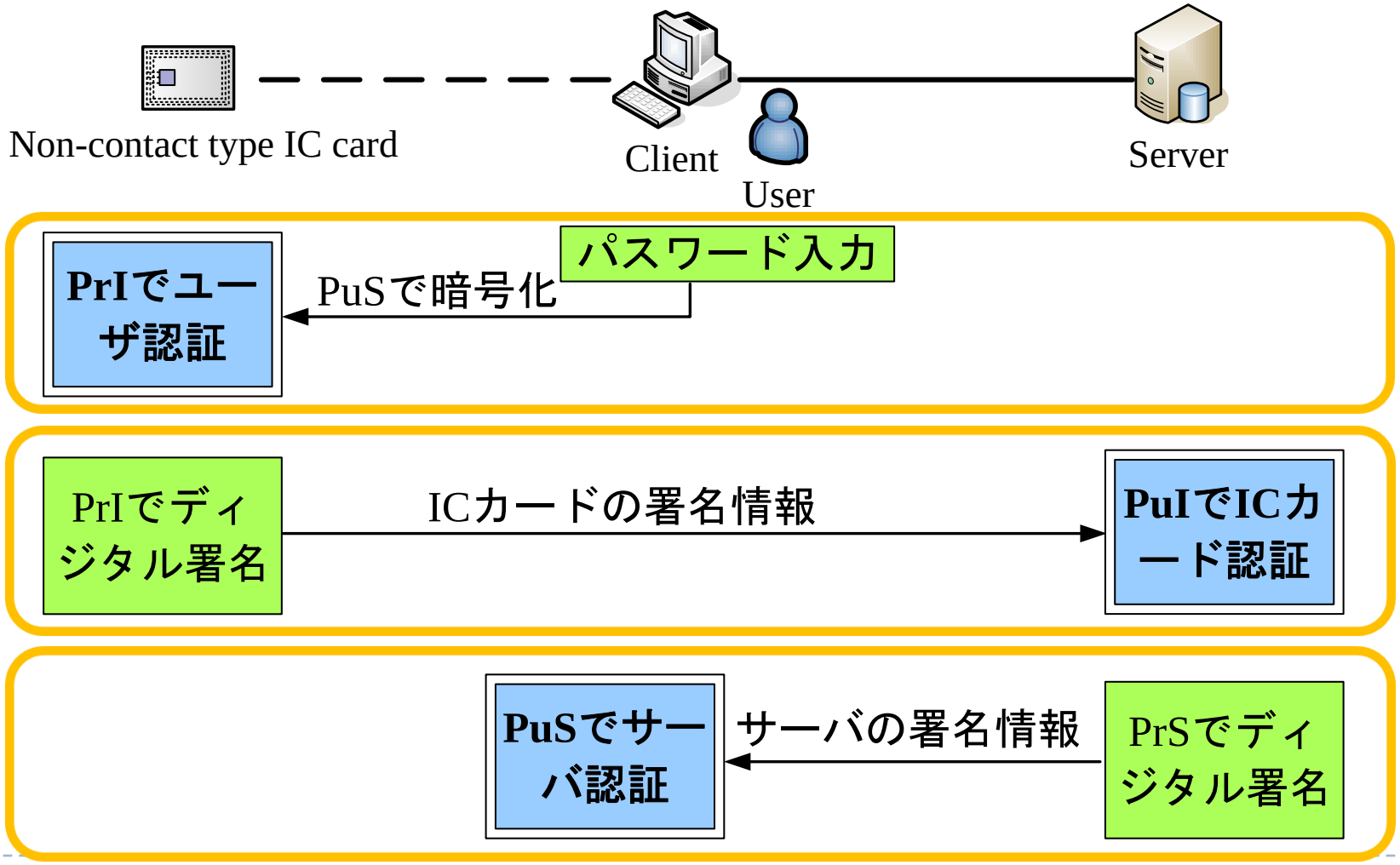
SPAICの初期情報



	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）

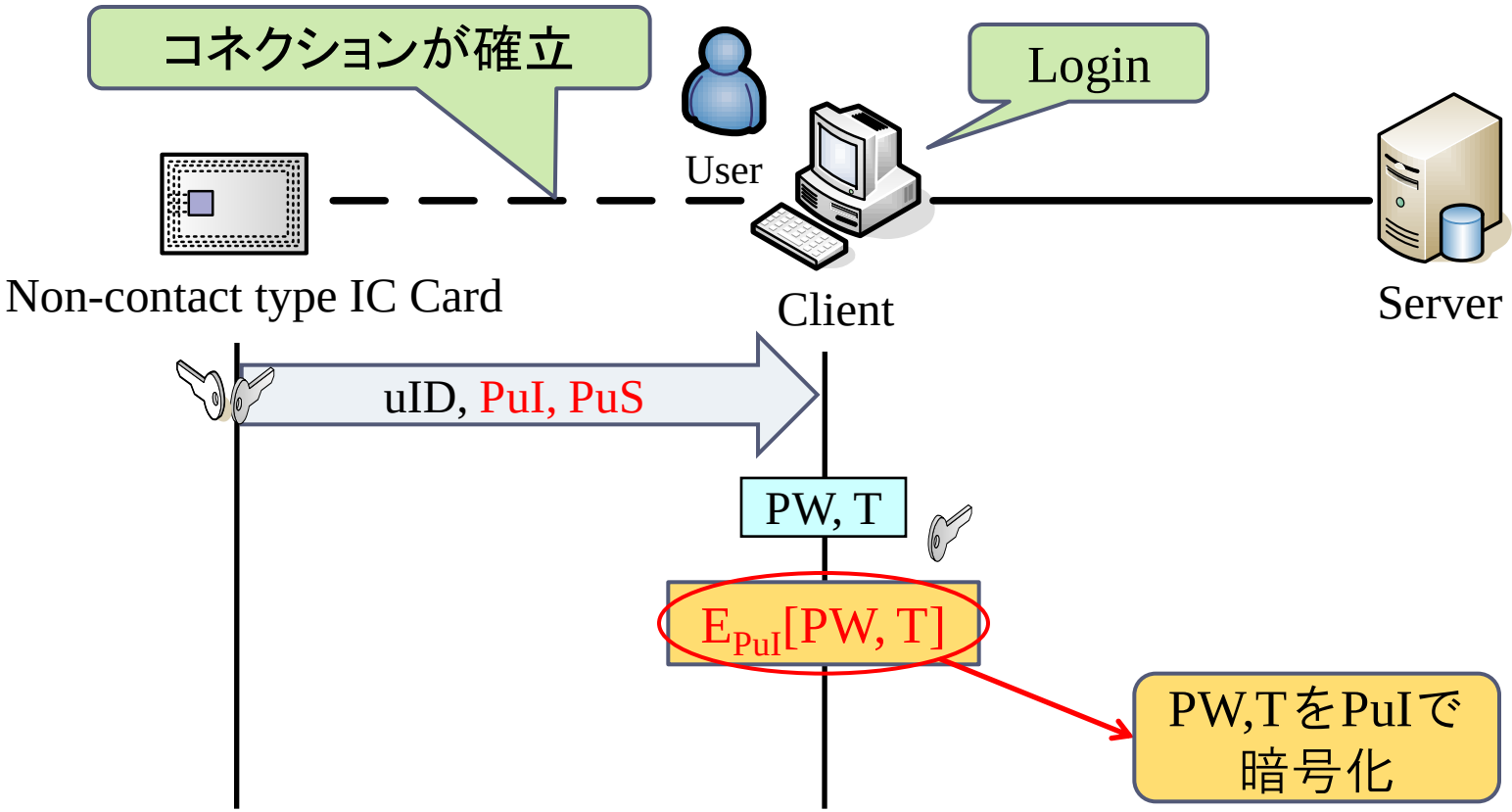
SPAICの動作概要

- SPAICの認証動作は三段階



SPAICの動作：ユーザ認証

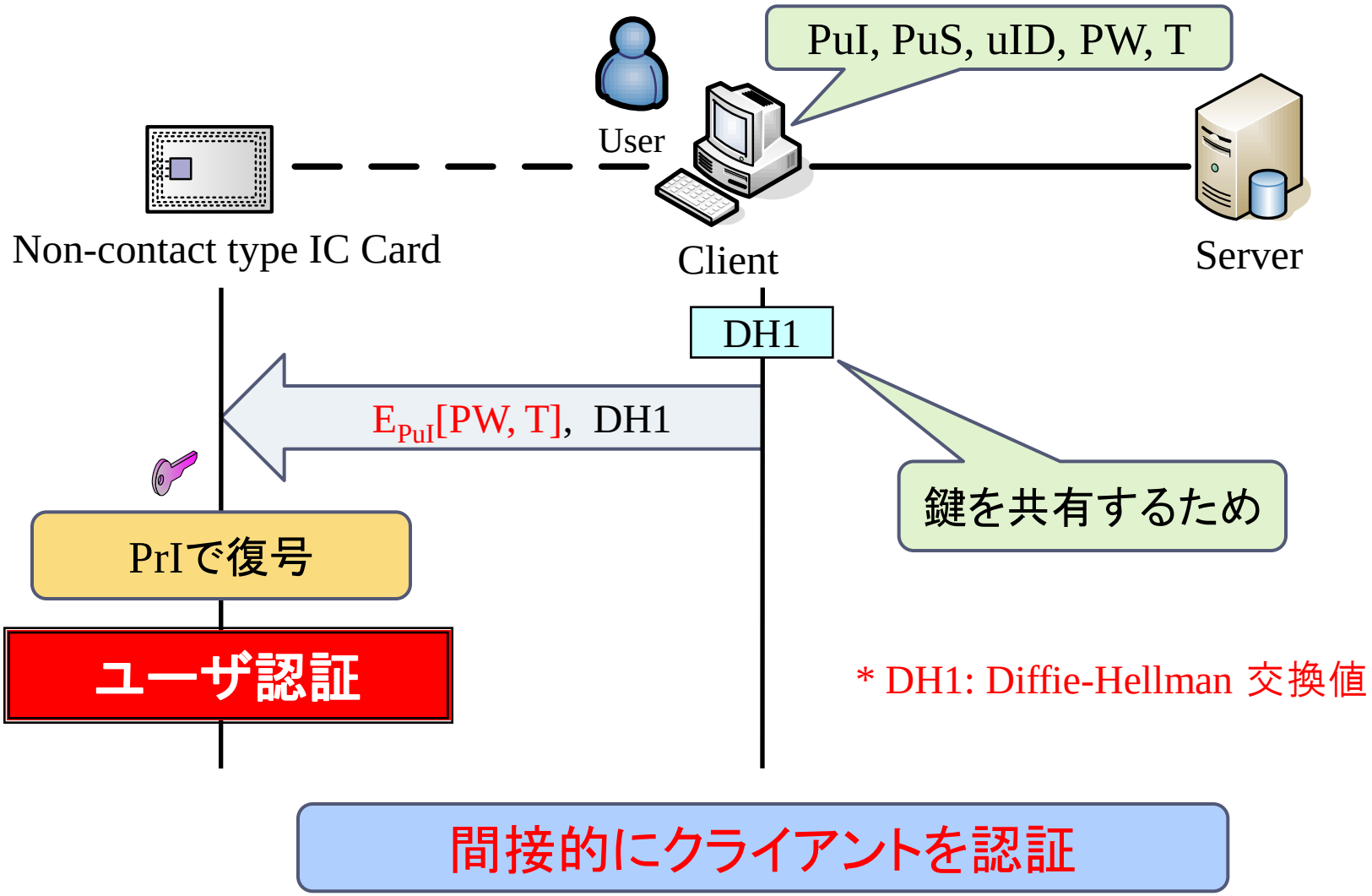
- ICカードはパスワードや生体情報によりユーザ認証



*PW：パスワード
*T：生体情報テンプレート

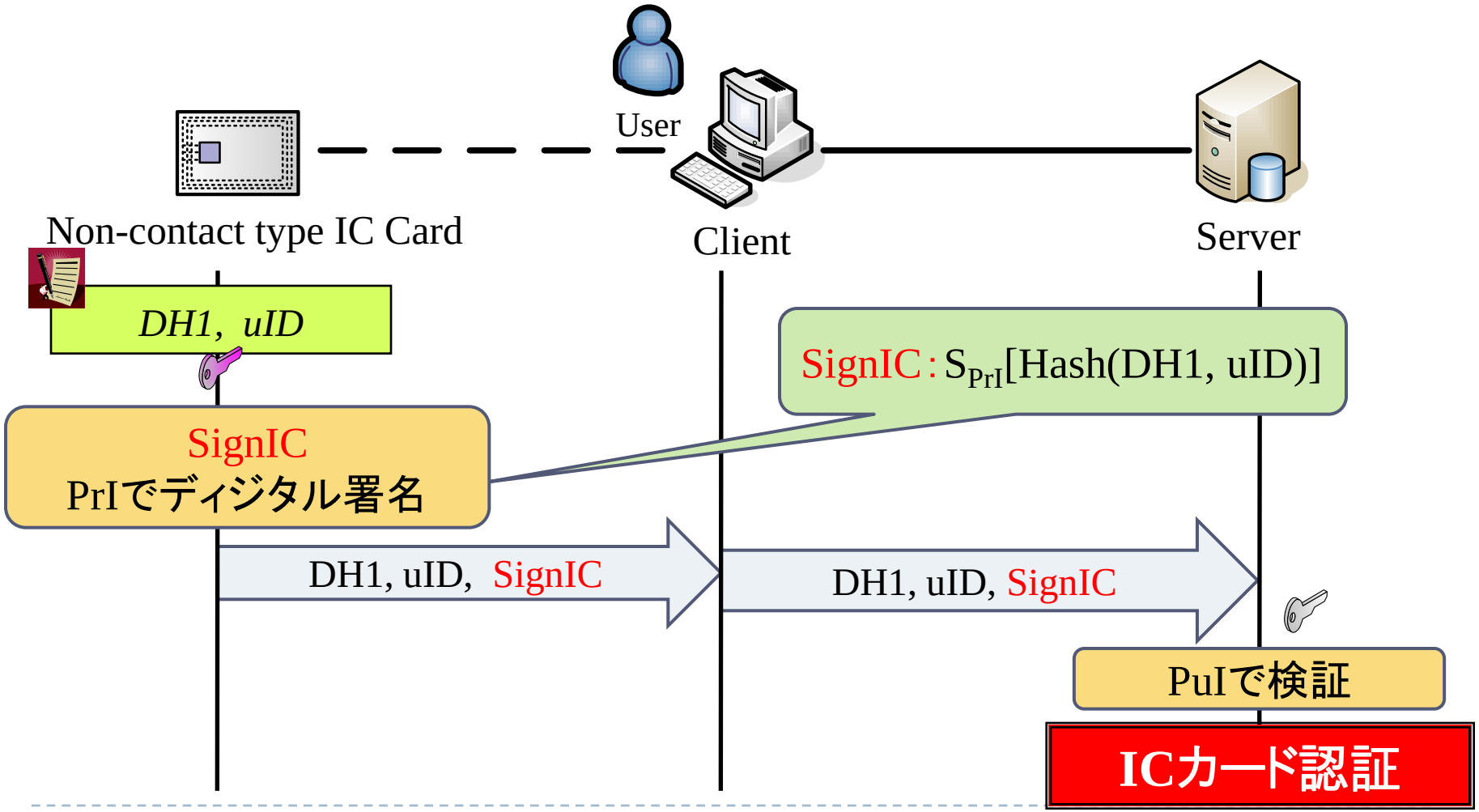
*DoS攻撃，リプレイ攻撃への対応を除く

SPAICの動作：ユーザ認証



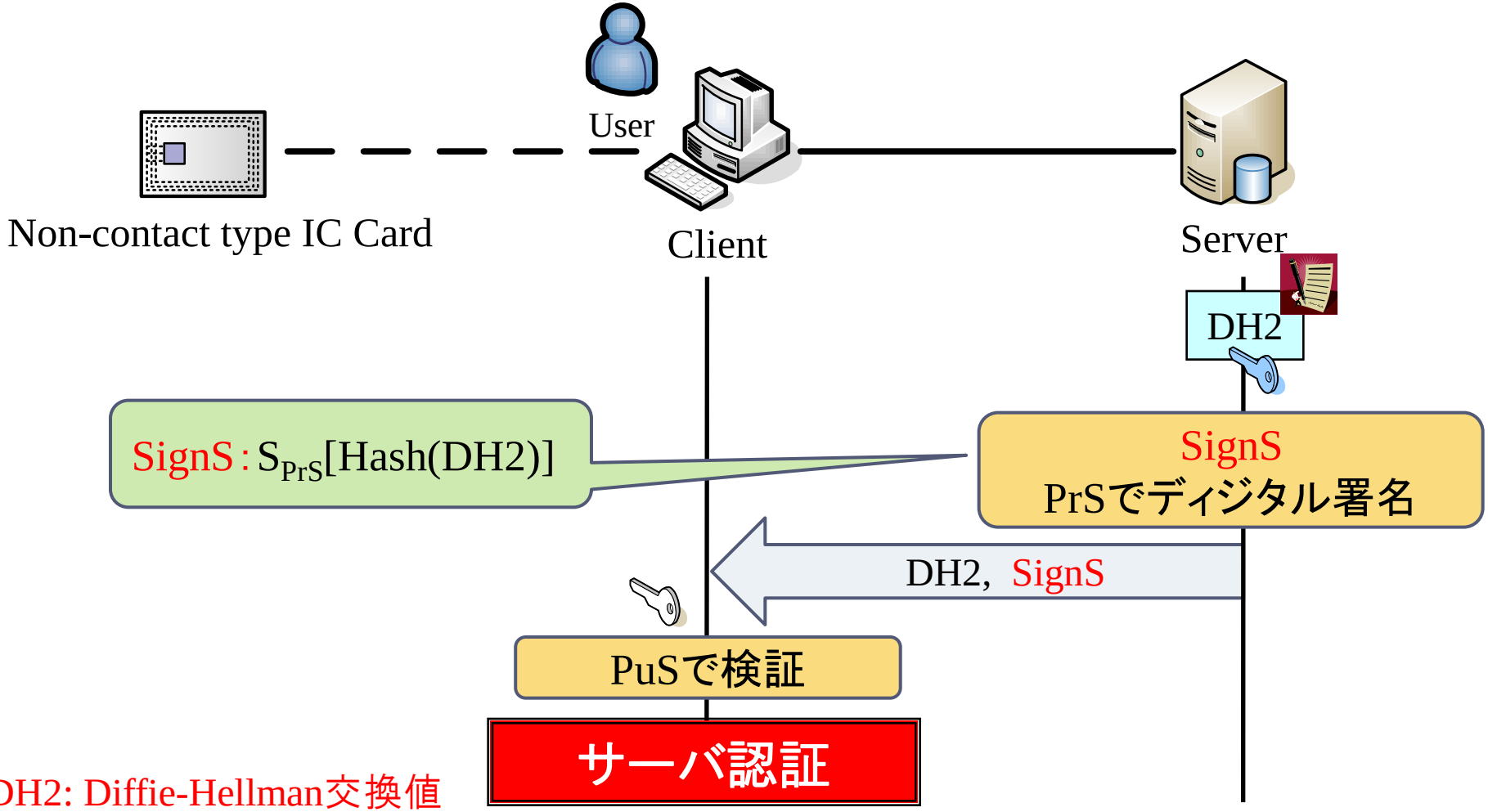
SPAICの動作：ICカード認証

- サーバはディジタル署名を検証することよりICカード認証



SPAICの動作：サーバ認証

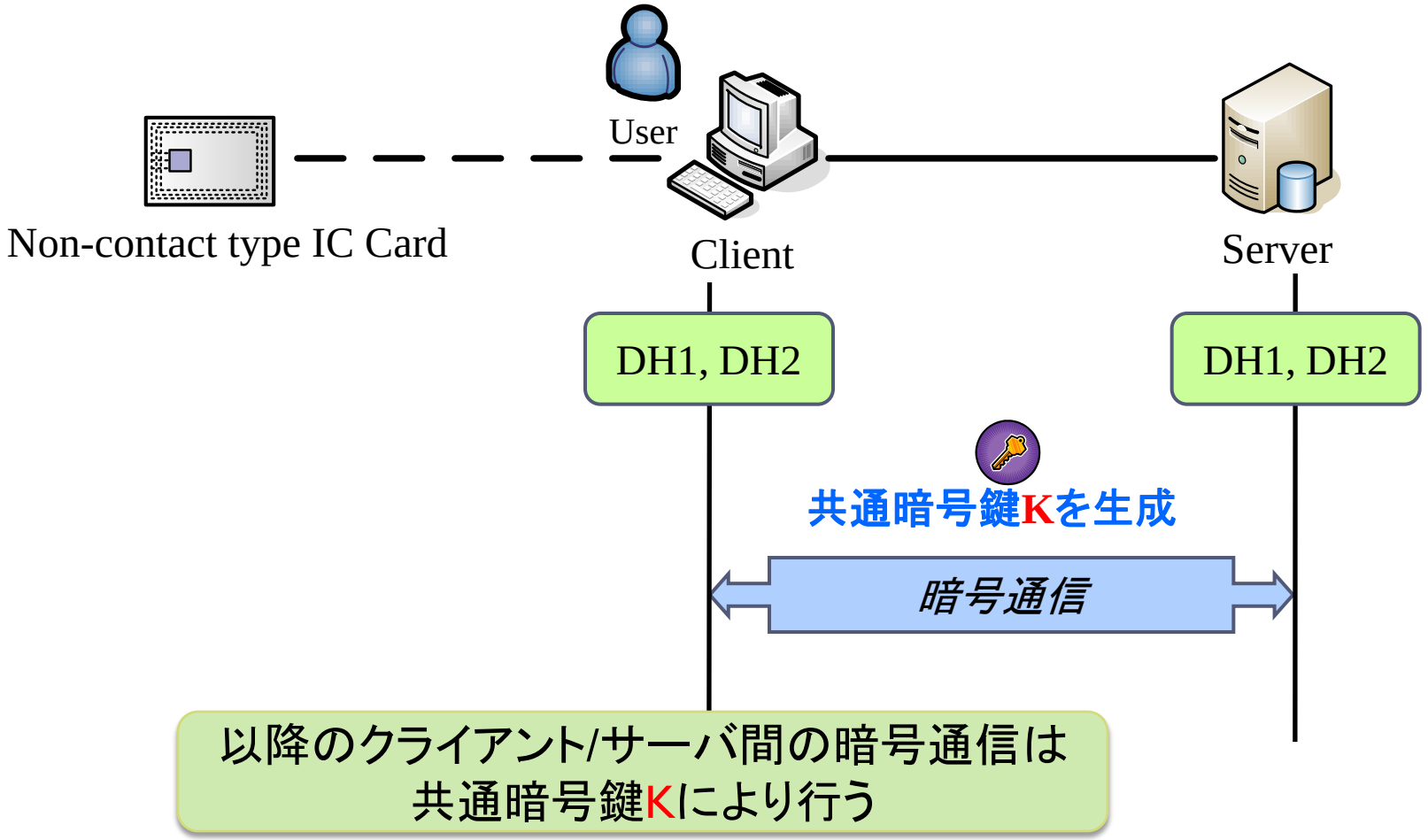
- クライアントはディジタル署名を検証することよりサーバ認証



* DH2: Diffie-Hellman交換値

SPAICの動作：暗号鍵生成

- DH1，DH2より暗号鍵を生成

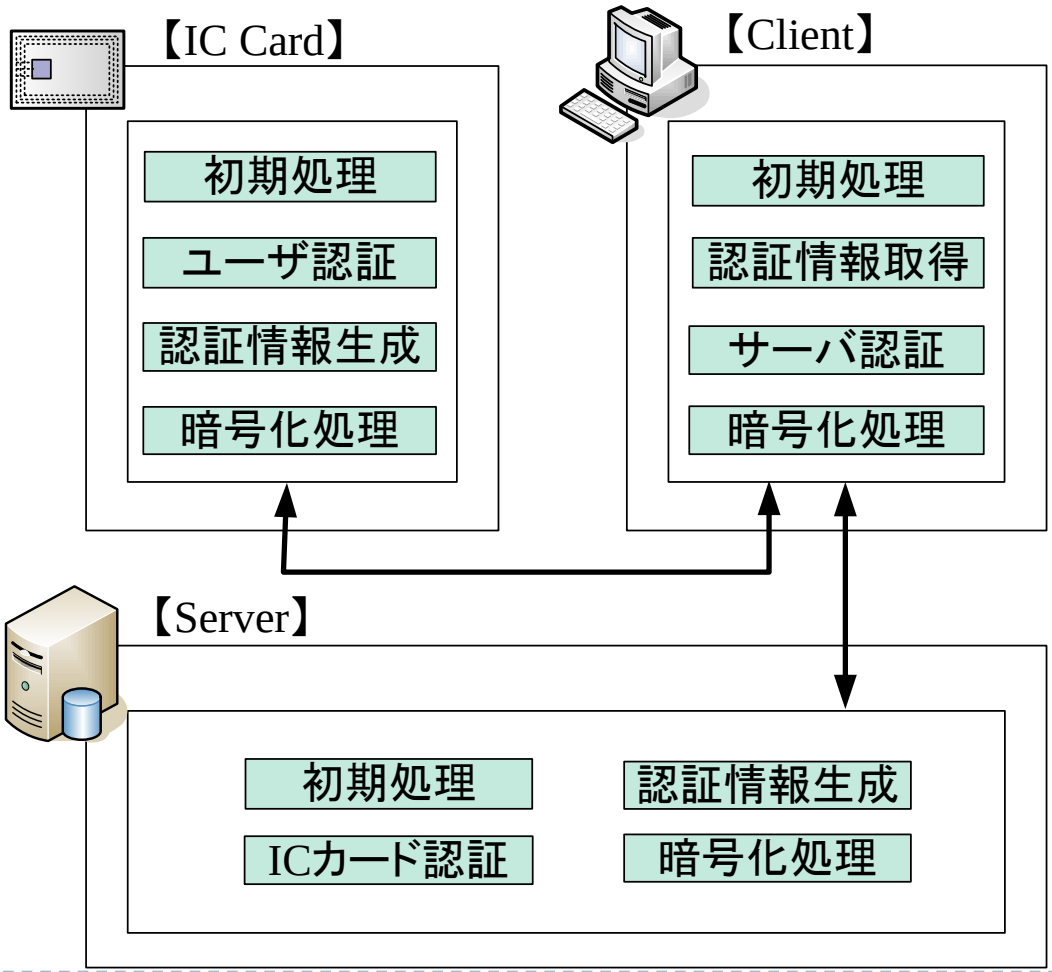


評価

	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への負荷	○ 中程度	△ 高い

実装モジュール

- クライアントおよびサーバにおける実装モジュール



USBトークンによる試作

- SPAICは非接触ICカードの利用が前提
- ICカードの開発環境を準備するのは困難

- 試作システムには，USBトークンを利用
  - ICカード同様CPUとメモリを内蔵
  - 内部で演算機能を持つ、暗号・認証処理が可能
  - ただし、プログラミングができない

- ICカード対応プログラムはPC上で開発
- 将来、ICカードへ移植

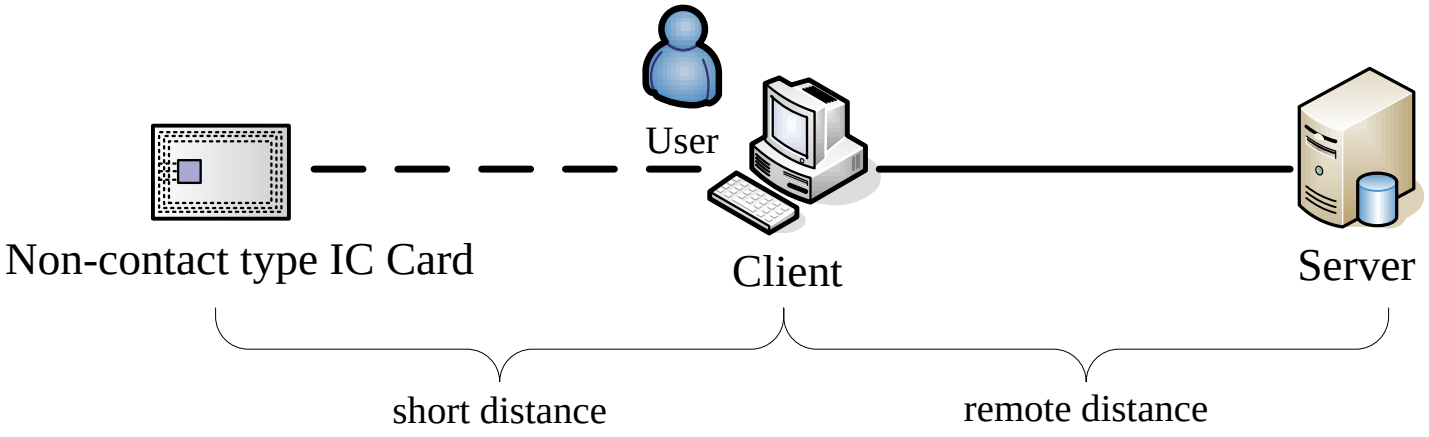
むすび

- まとめ
  - 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
  - 実装を完成
  - 詳細な性能評価

中間者攻撃への対応

- 中間者攻撃（Man-in-the-middle Attack）
  - データの送信者と受信者の間に第三者が介入し、送信者と受信者の双方になりすますことによってデータの盗聴や改変を行う攻撃
- 中間者攻撃の防止
  - ディジタル署名を利用



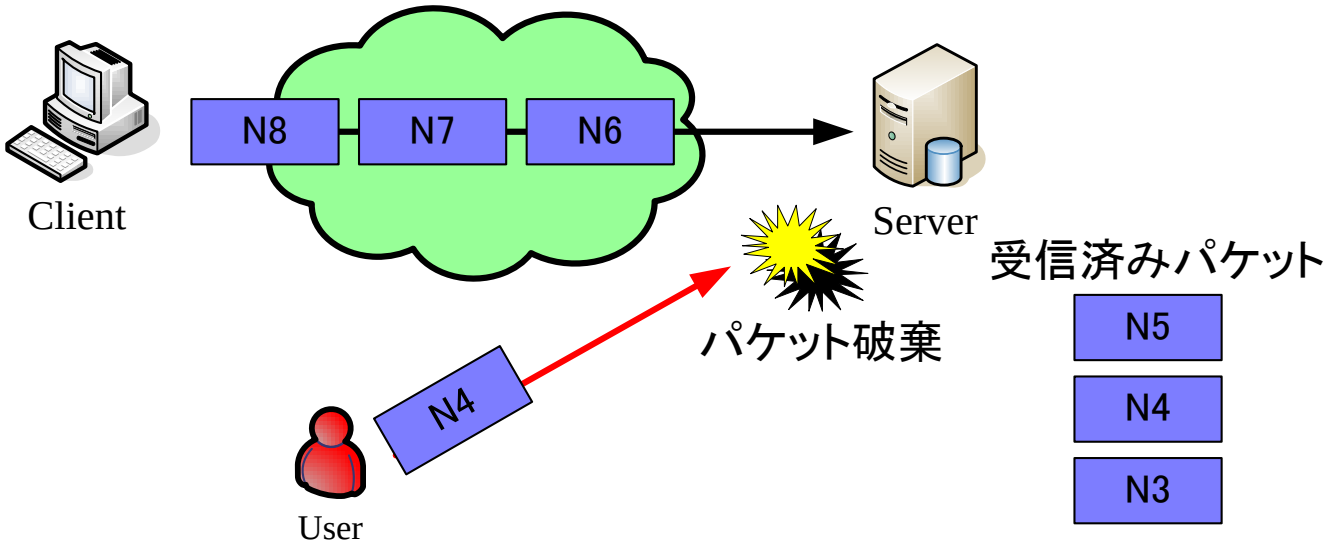
DoS攻撃への対応

- DoS攻撃（Denial of Service Attack ）
  - 大量のパケットを送信してサーバをダウンさせるサービス拒否攻撃

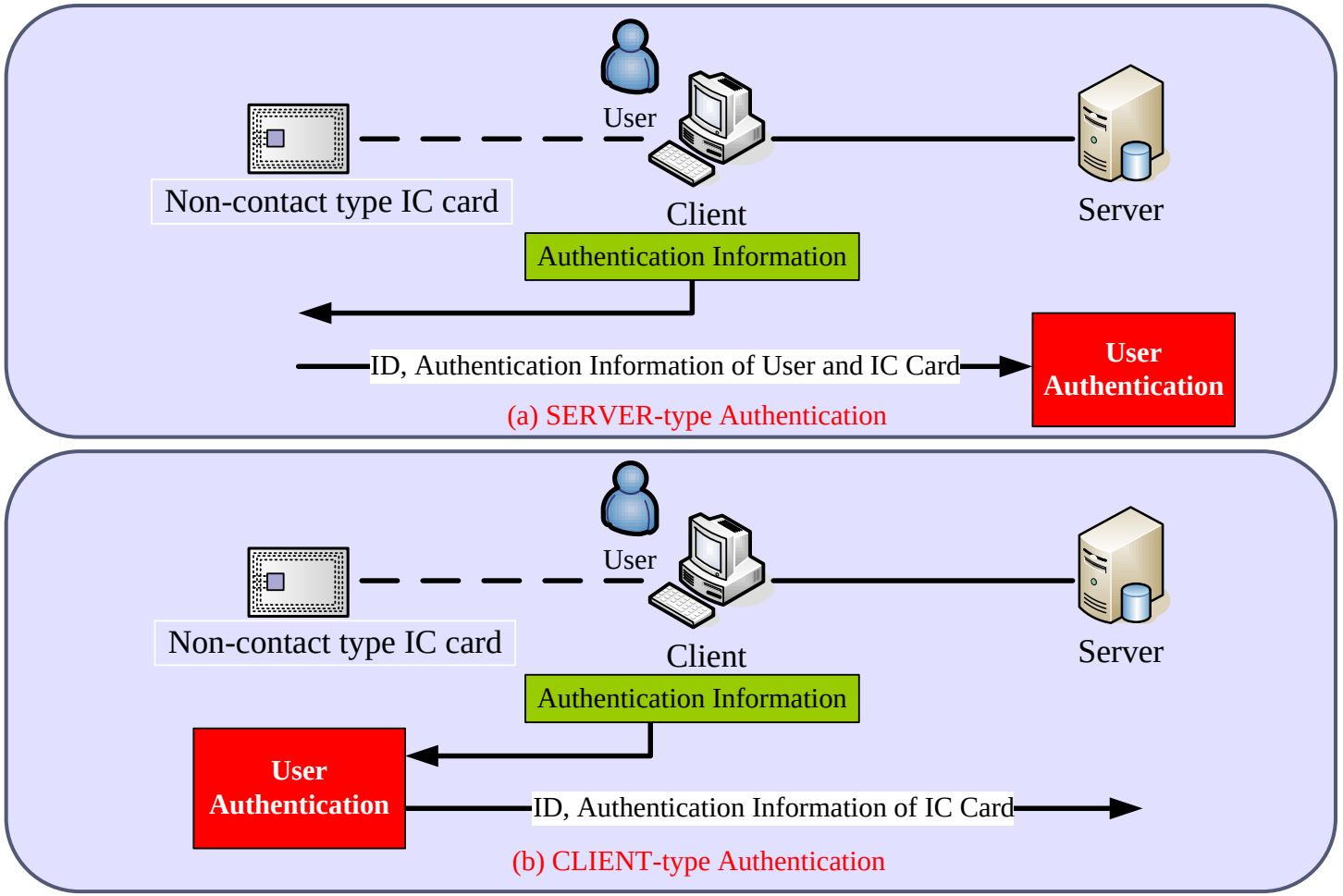
- DoS攻撃の防止
  - Client/Server間でCookieの交換で対応する
  - 通信相手はActiveな相手かどうかをチェック
  - 単純なDoS攻撃に効果がある
  - Cookieまで計算して攻撃を行ってきた場合

リプレイ攻撃への対応

- リプレイ攻撃（Replay Attack）
  - 以前の通信内容を入手して、同じ内容を送信する攻撃
- リプレイ攻撃の防止
  - 乱数を利用
  - 重複している場合は、そのパケットを破棄

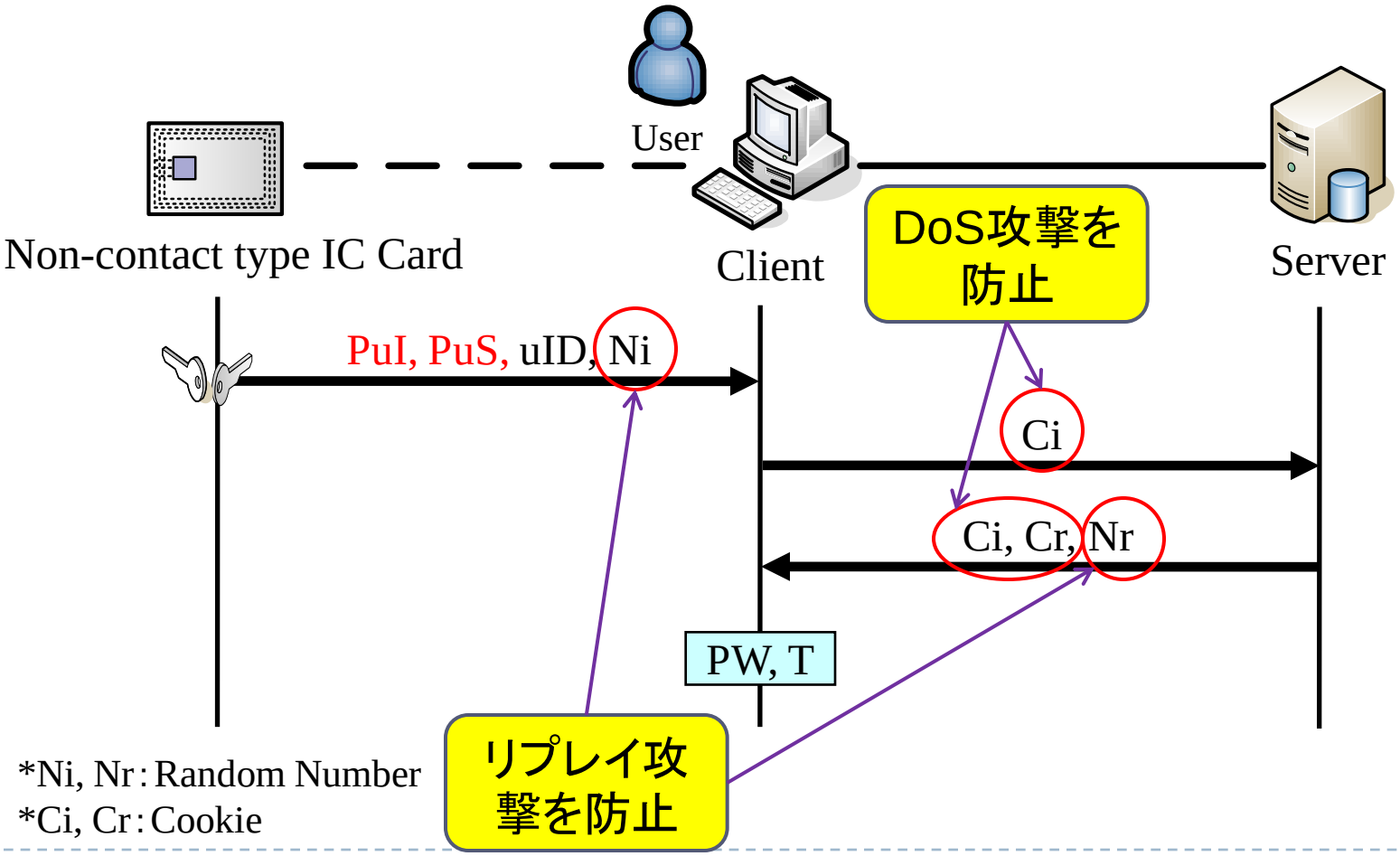


ユーザ認証方式

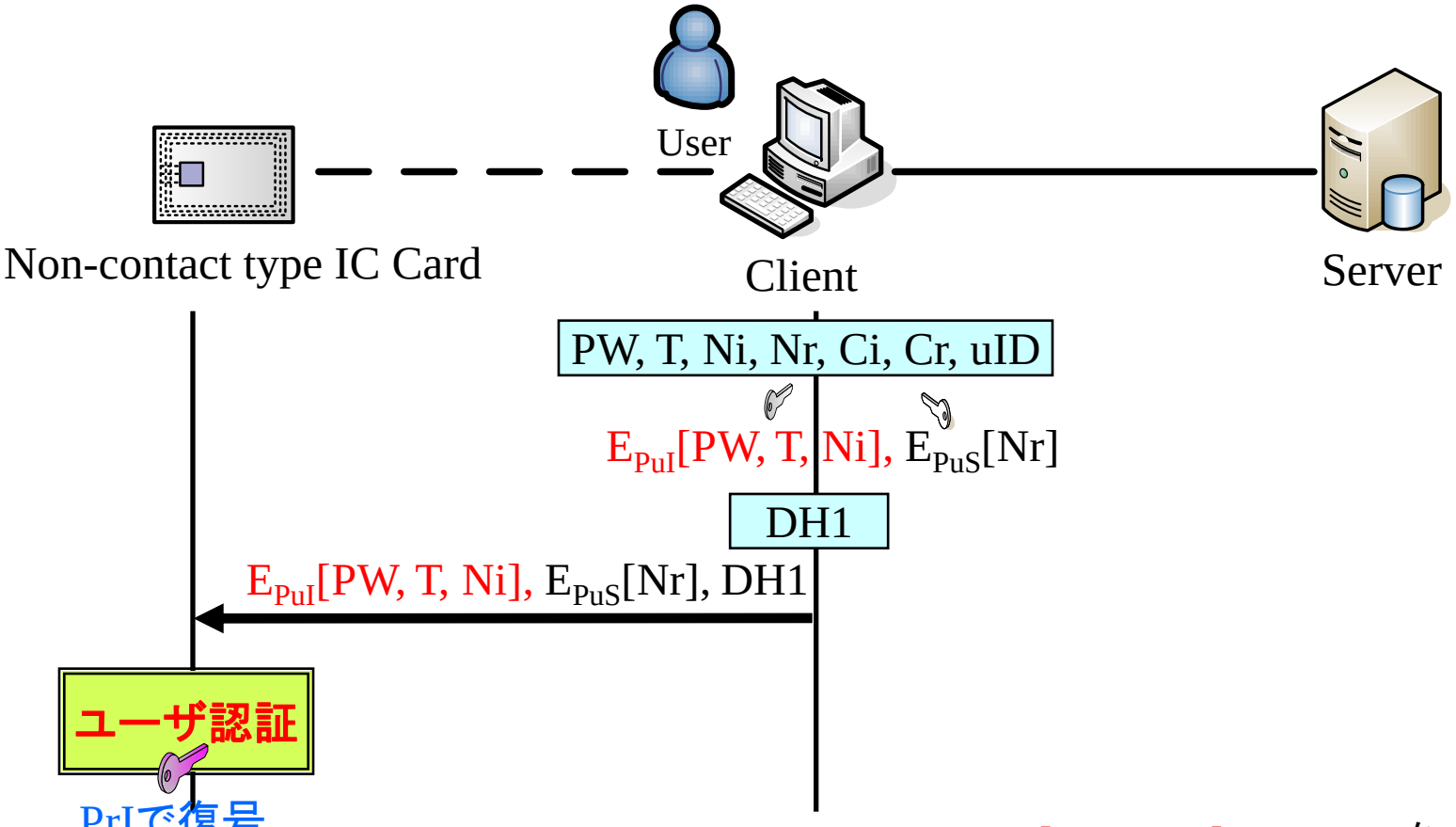

User
Non-contact type IC card
Client
Server
Authentication Information
ID, Authentication Information of User and IC Card
User Authentication
(a) SERVER-type Authentication
User
Non-contact type IC card
Client
Server
Authentication Information
User Authentication
ID, Authentication Information of IC Card
(b) CLIENT-type Authentication

SPAICの動作：ユーザ認証(1)

- ICカードはパスワードや生体情報によりユーザ認証

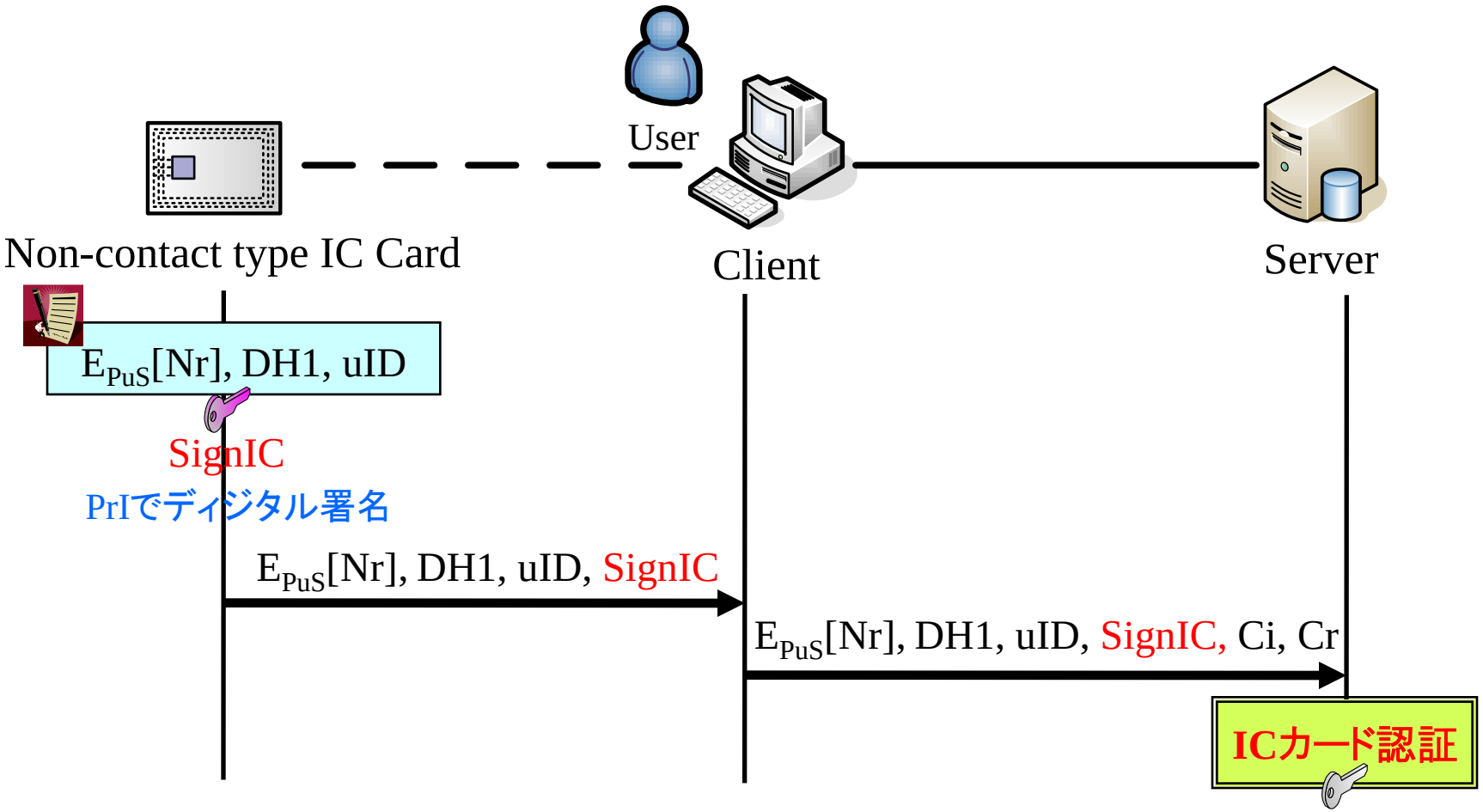


SPAICの動作：ユーザ認証(2)



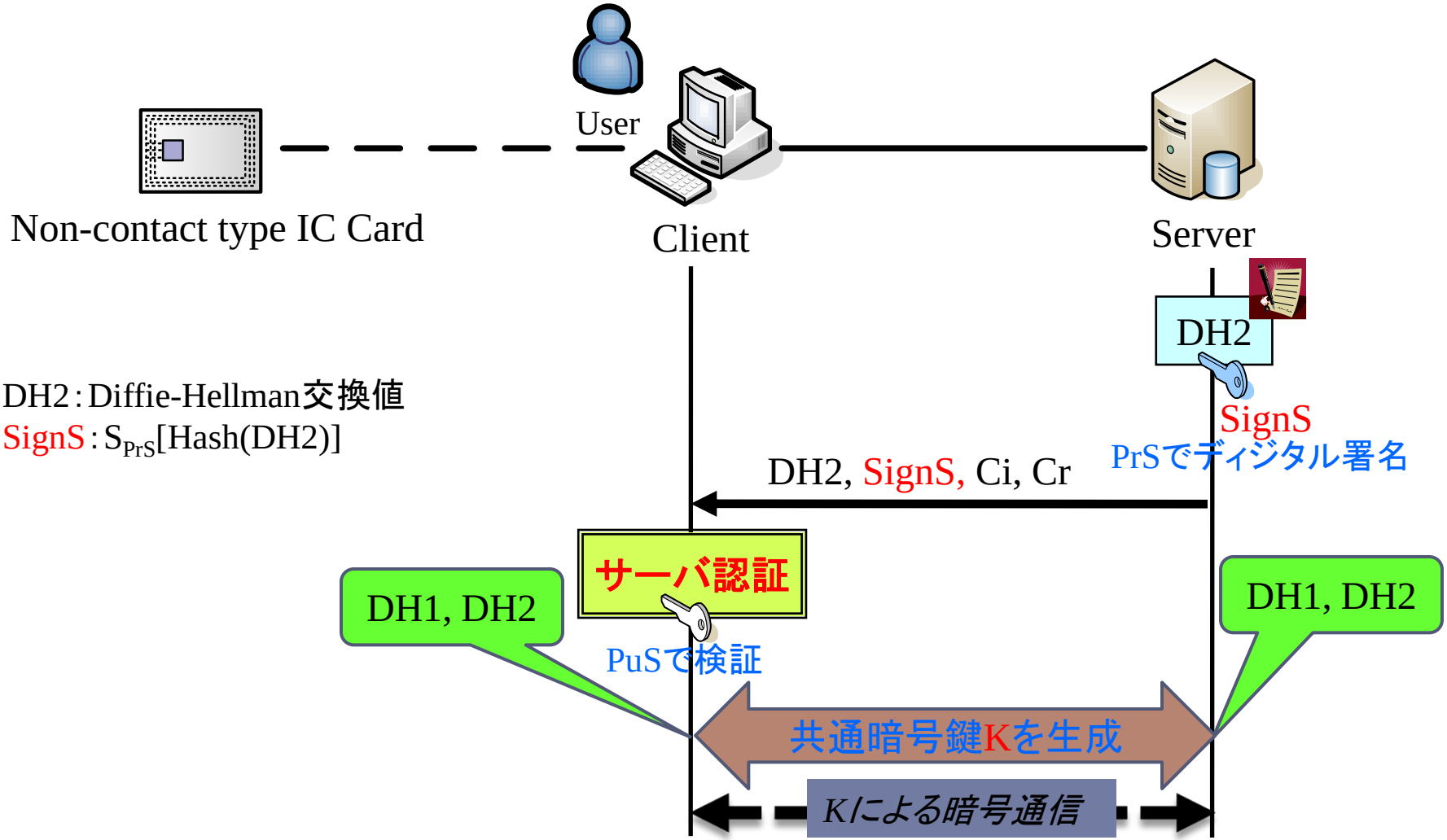
* E_{PuI}[PW, T, Ni]：PW, T, NiをPuIで暗号化
* E_{PuS}[Nr]：NrをPuSで暗号化
* DH1：Diffie-Hellman交換値

SPAICの動作：ICカード認証



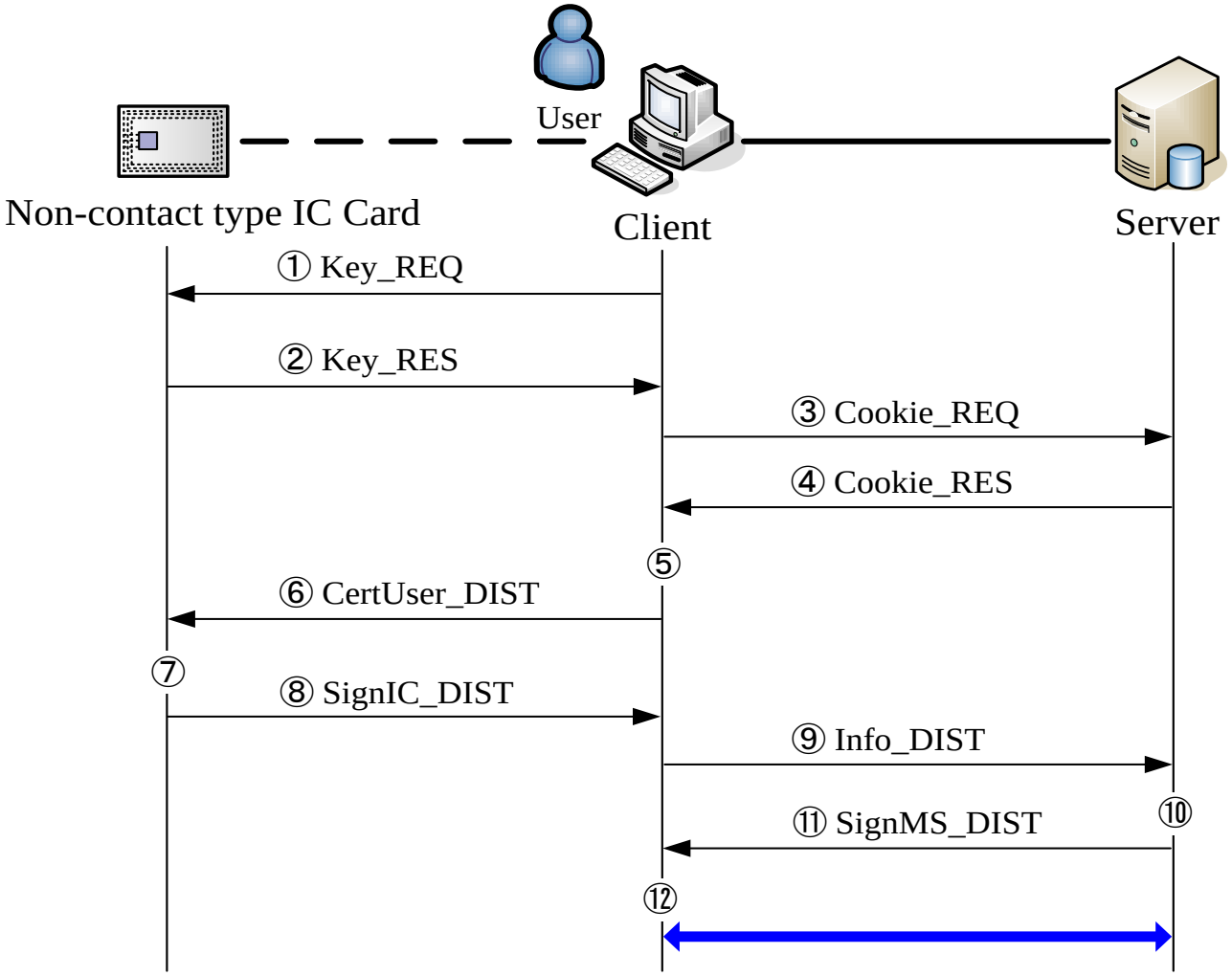
* SignIC : S_{PrI}[Hash(E_{PuS}[Nr], DH1, uID)]

SPAICの動作：サーバ認証

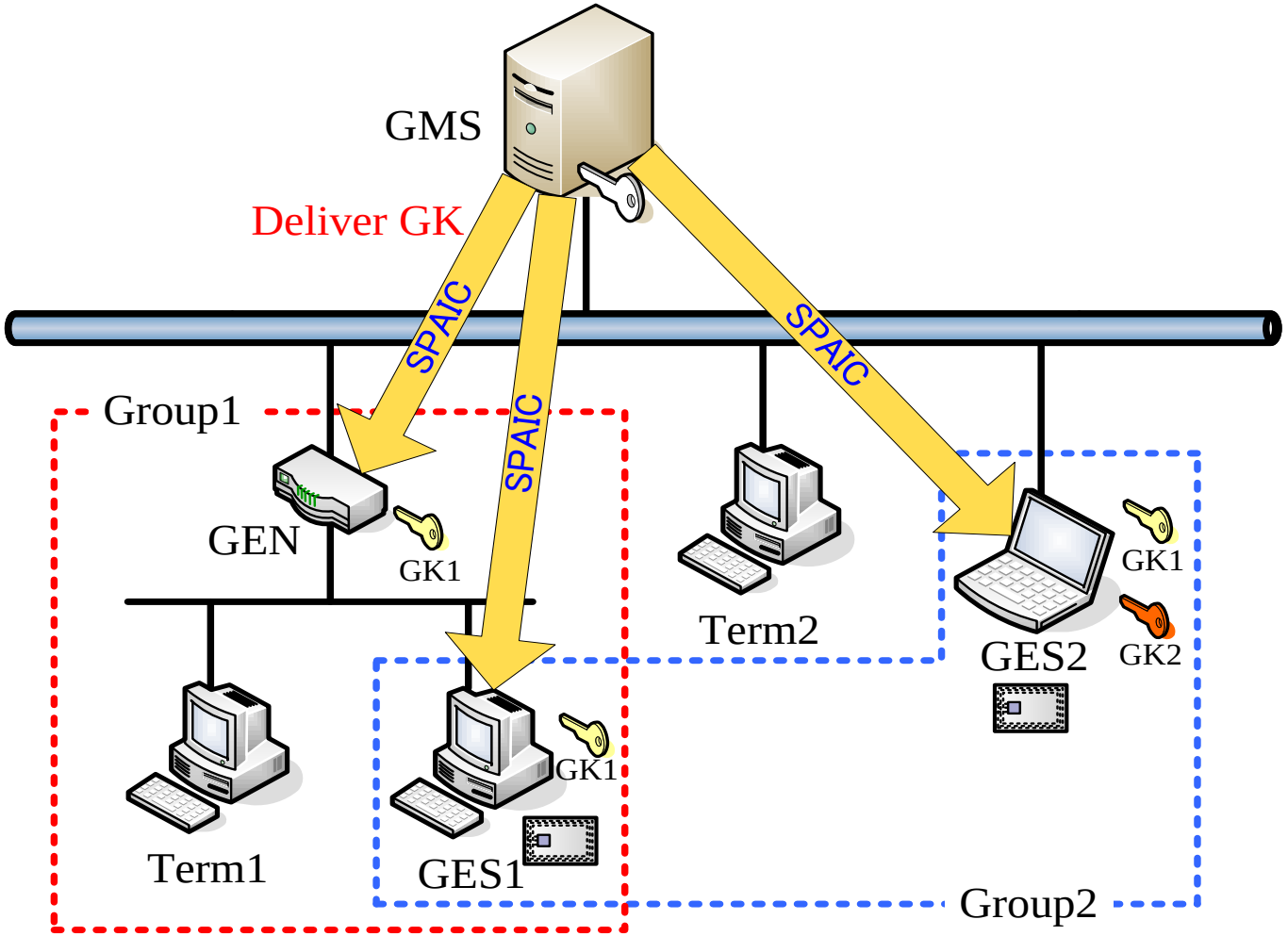


* DH2：Diffie-Hellman交換値
* SignS：S_{PrS}[Hash(DH2)]

詳細シーケンス


User
Non-contact type IC Card
Client
Server
① Key_REQ
② Key_RES
③ Cookie_REQ
④ Cookie_RES
⑤
⑥ CertUser_DIST
⑦
⑧ SignIC_DIST
⑨ Info_DIST
⑩
⑪ SignMS_DIST
⑫

システム構成


GMS
Deliver GK
SPAIC
SPAIC
SPAIC
Group1
GEN
GK1
Term2
GK1
GES2
GK2
GK1
Term1
GES1
Group2