社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2003－UBI－2 (30)
2003／11／19

Key-insulated 公開鍵を用いた セキュアなサービスモビリティの実現

金子 晋丈 * 林 素娟 ** 森川 博之 * 青山 友紀 **

あらまし コンピューティングデバイスやネットワークリソースが遍在する環境では，積極的に通信のエンドポイントを切り替えていくサービスモビリティが望まれる．サービスモビリティを実現するためには，通信を安全に切りることが必須となる．筆者らは，サービス移動をセキュアに行うための機構として，端末固有情報に依存しない通信インタフェースを提供するセッションレイヤモビリティサポートを用い，これに key-insulated 公開鍵暗号方式を適用することによって端末に依存しない通信の移動を実現しようと考えた．Key-insulated 公開鍵暗号方式は，秘密鍵を安全でないデバイス上で利用することを考え，ステージに分けて秘密鍵が管理されているため，端末に依存しない認証処理を可能とする．本方式では，1 つのセッションに 1 つの key-insulated 公開鍵を割り当て，ユーザの移動にステージを対応づけることにより，key-insulated 公開鍵のセッションレイヤモビリティサポートへの適用を実現している．
キーワード 多様化，セッションレイヤ モビリティサポート，セキュリティ，key-insulated 公開鍵暗号方式

Secure Service Mobility Using Key-insulated Publickey Cryptosystem

Kunitake KANEKO*, SoYeon Lim**, Hiroyuki MORIKAWA**, and Tomonori AOYAMA*

Abstract: In the environment where the computing devices and access links are ubiquity, it is desired to switch the resources according to our context (service mobility). In order to realize service mobility, security consideration is indispensable. First, we use sesseion layer mobility support which provides an interface independent of the lower layer details and enhance it to realize secure service migration using key-insulated public-key cryptosystems. Key-insulated cryptosystems have developed for using the private key on insecure device. Therefore, they use the private key refleshed at discrete time periods and realize terminal independent public-key cryptosystems. We enable the secure service migration using the key-insulated private key corredpondent to every migration.
Keywords: heterogeneous, session layer mobility support, security, key-insulated public-key cryptosystems

1. はじめに

インターネットは，接続されるコンピューティングデバイスやそれらをインターネットに接続するアクセスリンクにおいて多様化の時代を迎えている．リソースが多様化したインターネット環境では，現在の携帯電話端末のように単一のデバイスを常時持ち歩き使い続けるだけではなく，その場その時の利用要求に応じてリソースを周辺環境の中から選択し切り替えて利用することが望まれる．筆者らは，ユーザの周辺環境やリソースに関する要求事項は時々刻々と変化するものであると考え，ユーザに常に最適な通信環境を提供することを目的として，たとえ通信中であっても積極的にリソースの選択・切り替えを可能にする技術（サービスモビリティ）に関して検討を行っている．以下に簡単なサービスシナリオを述べる．

ここはアリスのオフィスである．商品の買い付けに出かけている部下のボブからアリスに電話がかかってきた．ボブは，買い付けの是非についてテレビ電話で商品を見せながら，アリスの意見を参考にしたいと考えたのである．しかし，彼女は手近にあった携帯電話でボブの電話にでてしまった．ボブはアリスに電話の意図を伝え，アリスは携帯電話からデスクトップコンピュータに通信を切り替えた．アリスは，大画面のディスプレイが接続されたデスクトップコンピュータで，その商品を細部まで確認し，ボブに購入を勧めた．

サービスモビリティは，ユーザが利用したいと思うデバイスを周辺環境から発見し選択するサービス選択技術，サービス選択によって決定したデバイスに通信を移動させるサービス移動技術，新しく利用するデバイスや通信リンクの性能に応じてサービス品質を柔軟に変化させるサービス適合技術によって構成されている [1]．上記のシナリオを例にとると，アリスが商品を確認する際にオフィスの中から大画面のディスプレイが接続されたデスクトップコンピュータを選択可能

* 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo
** 東京大学大学院新領域創成科学研究科
Graduate School of Frontier Sciences, The University of Tokyo

にする技術がサービス選択であり，その後，アリスがボブとの通信を携帯電話からデスクトップコンピュータへの切り替えられるようにする技術がサービス移動技術，そして，音声通信に映像通信を加えるとともに，商品の細部を確認するために高解像度の映像に通信を変更させる技術がサービス適合技術となる．本稿では，特に，通信サービスを継続しながら，通信のエンドポイントをユーザの要求に応じてネットワークや端末を跨いで切り替えるサービス移動技術について述べる．

これまでインターネットにおける通信の移動透過性は，移動に無関係な識別子を設け，その識別子に対して移動によって変化する識別子を対応づけることによって実現されてきた．さらに，この対応付けの変更を行う際に認証処理を行うことで，モビリティサポートが持つ潜在的なセキュリティ上の脆弱性である通信ハイジャックを防いでいる．IETF [2] を中心に検討されてきた Mobile IP [3] は，アドレス空間の異なるネットワークを渡り歩く単一の端末に対して，パケット到達性を与える技術であり，ターミナルモビリティサポートと呼ばれている．ターミナルモビリティでは，端末に付与される IP アドレスは移動によって変化するものの，端末自体は変化しないため，端末ごとに固有の識別子を与えることで移動に無関係な識別子を導入することが可能となる．また，対応付けの変更に必要な認証情報はユーザが利用する端末に保存されており，その端末の安全性が確保されていれば安全に識別子の対応付けを変更できる．

例えば，Mobile IP や LIN6 [4] では端末ごとの固有識別子としてネットワークアドレスと同じ空間に端末のネットワーク位置に依存しないアドレス(順に，ホームアドレス・LIN6 アドレス）を定義している．また，TCP Migrate [5] は問題点を TCP に絞り，端末が不変であれば IP アドレスの変化のみでポート番号やシーケンス番号など TCP 固有の情報に依存しないことから，TCP を拡張し TCP 内部に TCP コネクション固有の識別子を設けることで移動による IP の変化に対応している．すなわち，ターミナルモビリティでは端末が不変であるという制約条件を生かし，移動に無関係な識別子を導入しているといえよう．また，認証に関しても同様に，認証情報の安全性を端末の単一性が保証している．

一方で，サービスモビリティは端末を跨いだ移動を実現するため，端末の固有情報や TCP コネクションの固有情報を移動に無関係な識別子として用いることはできない．さらに端末が変わるため，通信を識別するための情報，および対応付けを変更する際に必要な認証情報を端末から端末に移動させる必要がある．前者に関して，筆者らは端末や TCP コネクションなどの固有情報に依存しない自由度の高い通信の実現に向けてセッションレイヤモビリティサポートを検討してきた．そこで本稿では，特にサービスモビリティにおける移動認証技術に着目する．サービスモビリティでは，これまでのネットワーク移動のみを対象にしたターミナルモビリティと異なり，端末を跨いだ移動となるため，認証情報の安全性を端末の単一性に求めることができない．すなわち，サービスモビリティを実現するためには，複数の端末を切り替えながら利用する場合においても認証情報を安全に管理するとともに，セキュアなサービスモビリティを実現する手法について新たに検討する必要がある．以下では，基盤となる移動透過技術としてセッションレイヤモビリティサポートを採用し，公開鍵を変更することなく秘密鍵を更新可能な key-insulated 公開鍵暗号方式 [6] を用いたセキュアなサービス移動技術の実現について述べる．

本稿の構成は以下の通りである．まず 2. でセッションレイヤモビリティサポートの特徴を述べ，3. で key-insulated 公開鍵暗号方式について述べる．次に 4. でサービスモビリティに必要な認証技術，およびその具体的な手法として，セッションレイヤモビリティサポートへの key-insulated 公開鍵の適用について述べる．最後に，5. で本稿をまとめる．

2. セッションレイヤモビリティサポート

セッションレイヤモビリティサポートはトランスポートレイヤとアプリケーションレイヤの中間に設けられたセッションレイヤによってモビリティをサポートする機構である．本セッションレイヤモビリティサポートの特徴は，端末や IP アドレス等の端末固有情報に依存しない通信インタフェースをアプリケーションに提供するところにある（図 1)．

現在最もよく利用されている通信インタフェースである socket API [7] は，デバイス I/O と通信 I/O を統一的に扱うことができる優れた I/O フレームワークであり，アプリケーションはこの socket インタフェースを直接呼び出して使っている．しかしながら，socket API は，扱う I/O が静的であることを前提としており，I/O が動的に変化することを想定していない．そのため，例えば IP アドレスの変更といった I/O に動的な変化が生じた場合，アプリケーションは，その通信インタフェースを利用することができなくなり，通信は途絶してしまう．これは，通信インタフェースに IP アドレスなどの端末固有情報が強固に関連づけられ，通信インタフェースが開かれている限り関連づけられた情報を変更できないことが原因となっている．

アプリケーションが通信を維持したまま，コンピューティングデバイスや通信リンクなど通信のエンドポイントを柔軟かつ積極的に切り替えられるようにするには，このような静的な I/O を前提とし，それを

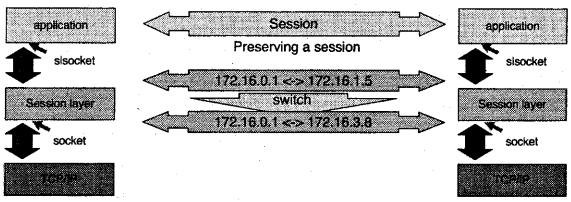

図 1 セッションレイヤモビリティサポート

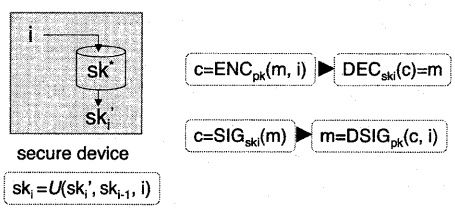

図 2 Key-insulated 公開鍵暗号方式

アプリケーションが直接利用する通信 API では不十分である．筆者らは，アプリケーションが扱う通信インタフェースから端末固有情報を排することで，I/O の動的な変更に対応できる通信インタフェースを開発し，このインタフェースに socket 等の静的なインタフェースを動的に接続することで，ネットワークを跨ぐモビリティだけではなく，端末を跨ぐモビリティを実現している．筆者らは，この新しい通信インタフェースを slsocket (session layer socket) と呼び，slsocket には session ID と呼ぶ端末固有情報に依存しない識別情報を与えている．

また，セッションレイヤモビリティサポートは，通信のエンドポイントとなる端末のセッション層がもう一方のエンドポイントのセッション層とネゴシエーションを行うことによってモビリティを実現している．すなわち，セッションレイヤではエンドポイント間で移動要求メッセージを送信し，この要求によりセッション層内部で静的な I/O である socket を新たに作成し通信相手に接続した後，これを動的に slsocket に接続している．エンドポイントのセッションレイヤ間のネゴシエーションは，TCP においてエンドホストが再送制御を行うのと同様にインターネットのエンドツーエンドの考え方 [8] に則っており，通信の移動をエンドポイント自体が管理できるとともにスケーラビリティを確保することができる．

3. Key-insulated 公開鍵暗号方式

Key-insulated 公開鍵暗号方式 [7] は，2002 年に Y. Dodis らによって提案された公開鍵暗号方式である．この暗号方式は，秘密鍵の漏洩が現在のセキュリティシステムの脆弱性に繋がっていることを問題点とし，これまで，安全性が確保された単一のデバイスで管理することを前提としてきた秘密鍵にステージと呼ばれる期間を与えることで，安全性が確保されない端末においても秘密鍵を利用可能とするものである．(図 2) 仮に特定のステージの秘密鍵が漏洩したとしても，ステージを変化させれば安全性を確保することが可能になる．また，この暗号方式において公開鍵はステージに依らず不変である．以下に，この暗号方式の概要を簡単に示す．なお，本暗号方式は，暗号化・復号化，電子署名のいずれにも用いることができる．

ユーザは，ひとつの公開鍵 PK を決定する．この PK に対応する親秘密鍵 SK* を物理的に安全なデバイスに保管する．全ての復号処理は，秘密鍵の漏洩が心配される安全性が保証されないデバイスにおいて行うものとする．この暗号方式は，ステージ 1, 2, . . . , N(単純にこれをある単位時間と考えてもよい；例，一日) に分けて処理する．それぞれのステージの最初に，ユーザは，安全なデバイスから復号に使う一時的な秘密鍵を受け取る．ここで，ステージ i における一時的な秘密鍵を SK_i とする．一方，公開鍵 PK は，メッセージを暗号化するのに使われ，ステージに依らず不変である．その代わり，暗号文には，ステージを示すラベルが付与される．また，復号処置を行う非安全デバイスは，繰り返しによる鍵の漏洩の脆弱性を持っているため，最大利用ステージ t ($t < N$) を設け，で用いることを前提とする．

具体的な SK_i の生成方法は以下の通りである．まず，(PK, SK) を生成し，PK を公開し，さらに SK から SK* と SK_0 を生成する．SK_0 は，ユーザがステージ 0 における秘密鍵として利用し，SK* は安全なデバイスに保管する．次にユーザがステージ i における秘密鍵を要求すると，SK* が保存されているデバイスは，部分鍵 SK_i' をユーザに渡す．ユーザは，SK_{i-1} と SK_i' を

用いて完全鍵 SK_i を生成する．この方法を用いると全てのステージにおいて，SK* だけ，もしくは SK_{i-1} だけではステージ i の完全鍵を生成できないため，特定の端末に依存しない鍵の保管が可能になり，セキュリティが高まる．

4. セキュアなサービス移動技術

4.1 サービスモビリティに必要な認証技術

2. で述べたように，セッションレイヤモビリティサポートは端末の固有情報に依存しない通信インタフェースをアプリケーションに提供し，エンドツーエンドのネゴシエーションによって宛先を切り替えることでネットワークや端末を跨ぐモビリティを実現する機構である．サービスモビリティを安全に利用できるようにするためには単純な切替処理だけでは十分ではない．なぜなら，モビリティサポートは宛先の動的な切り替えを可能にする技術であるため，悪意のあるユーザによって意図せず通信を切断されるだけでなくハイジャックされる可能性を潜在的に持っているからである．筆者らは，セッションレイヤモビリティサポートのエンドツーエンドのネゴシエーション機構に着目し，通信のエンドポイント間で認証情報を伴ったアソシエーションを構築することで，モビリティサポートの安全性を確保しようと考えた．

まず，サービスモビリティにおけるセキュリティ上の脆弱性について述べる．セッションレイヤモビリティサポートでは，セッション情報を通信のエンドポイントとなる端末から端末へと受け渡していくことで，モビリティを実現している．そのため，認証情報を含んだセッション情報が移動後も端末に残り，その情報を悪意のあるユーザに盗まれると，ユーザの意図しない移動要求を送られ，セッションが乗っ取られる可能性がある．特にコンピューティングデバイスが遍在する環境では，ユーザは，持ち歩いているデバイスだけでなく周囲のデバイスも自由かつ積極的に利用すると考えられるため，常に安全性が保証された端末を利用できるとは限らない．このような環境におけるモビリティサポートでは，ユーザの利用端末は安全ではないという前提に立って認証処理を設計する必要がある．

一方で，セッションレイヤモビリティサポートのエンドツーエンドの考え方から，認証処理は当該通信のもう片方のエンドポイントである通信相手も自由にデバイスやネットワークを選択できると考えると，セッションレイヤがネゴシエーションを行う相手端末は，通信によって毎回変化すると考えられる．このような環境では，秘密情報の共有（共有鍵暗号方式）を前提にすることはできず，公開鍵暗号方式を用いることが妥当であろう．また，ユーザのどちらかが端末を変更するごとに鍵を再生成するという手法も考えられるが，鍵生成に要する計算能力や公開鍵の交換手段をモバイル環境における貧弱な計算機環境から考えると非現実的であり，仮にこのような手法を採用したとしてもその高い認証コストから移動を自由に行えなくなる．

以上に加えて，モビリティサポートそのものが持つ脆弱性を回避する機構を検討しなくてはならない．すなわち，移動の切り替えは通信相手のセッションレイヤが通知するメッセージによって行われるため，送られてきた移動要求メッセージがユーザの意図したものであるか，移動要求メッセージを送信したとしてその内容は改竄されていないかを，移動要求メッセージの受信時に確認しなければならない．このような確認には，メッセージの送信者を特定し，内容改竄の有無を検出できる電子署名が必要である．また，悪意のあるユーザが過去の移動要求メッセージをコピーして保存し，その後再送信するリプレイアタックを防ぐことも必要となる．この場合，メッセージそのものは送信者が電子署名を付与しているため，何らかのシーケンス番号によって管理する必要がある．

以上から，セッションレイヤモビリティサポートに要求される認証処理は，下記の要求条件を満たす必要がある．

(1) 複数の端末を切り替えて利用すること（ただし，同時利用は 1 端末のみ）
(2) 利用端末は，安全ではないという前提をもつセキュリティモデルであること
(3) 認証情報を端末間移動させる際に，高い計算能力，複雑な鍵交換のシステムを必要としないこと
(4) 移動要求メッセージの内容および送信者を保証する電子署名を利用可能であること
(5) リプレイアタックを防止するシーケンス番号が与えられていること

上記条件を満たす暗号方式として，3. で述べた key-insulated 公開鍵暗号方式が存在する．次節では，key-insulated 公開鍵暗号方式をセッションレイヤモビリティサポートに適用したセキュアなサービスモビリティの実現手法について述べる．

4.2 セッションレイヤモビリティサポートへの key-insulated 公開鍵暗号方式の適用

ここでは，一つのセッションに対して一つの key-insulated 公開鍵を用いるものとする．これは，一人のユーザが同時に複数のセッションを別々の端末で動作させることが考えられるためである．

まず，key-insulated 公開鍵暗号方式が前節で述べた要求条件を満たしていることを示す．要求条件 1，2 および 4 に関しては，3. に述べたとおりであるため省略する．要求条件 3 に関して，一般的な公開

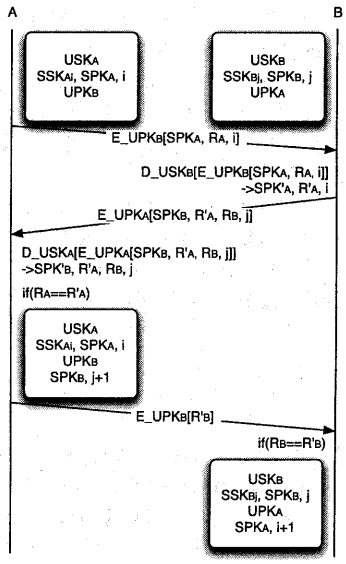

図 3 通信開始時の鍵交換手順

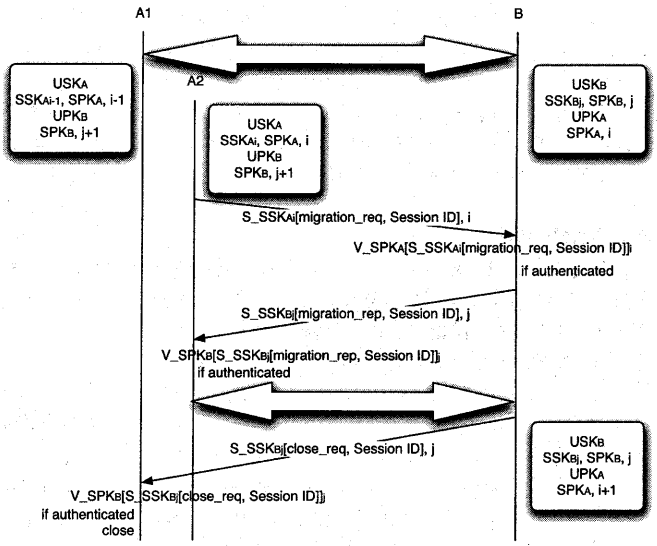

図 4 移動要求時の処理手順

鍵暗号方式の鍵生成にかかる計算量は O(logN) であるのに対し，key-insulated 公開鍵暗号方式の SK_i 生成にかかる計算量は O(1) であり，計算量は少ないため条件を満たしている．また，要求条件 5 については，key-insulated 公開鍵暗号方式におけるステージ i を移動要求の回数に対応させることで，リプレイアタックを防止することができる．これは，key-insulated 秘密鍵 SK_i がステージ i においてのみ有効であることを用いている．移動要求が受理されたときに，ステージを更新し，新たな秘密鍵 SK_{i+1} を作成することにより SK_i を移動要求メッセージの秘密鍵として利用することを無効化することができる．

以下では，セッションレイヤモビリティサポートへの key-insulated 公開鍵暗号方式の適用に関して具体的な手法を述べる．まず，通信開始時における鍵交換の仕組みについて述べ，次に，移動要求時の処理について述べる．

通信開始時の鍵交換

Key-insulated 公開鍵は，前に述べたように一セッションに対して一つの公開鍵を割り当てる．すなわち，通信開始時に当該セッションで利用する key-insulated セッション公開鍵を交換しなければならない．公開鍵暗号方式では，公開鍵を安全に交換することができなければ，中間者攻撃によって通信の安全性を確保することができない．ここでは，PKI（Public Key Infrastructure）を用いることで，セッション公開鍵の安全な交換を実現する．前提として，全てのユーザは PKI に公開鍵を預けており，PKI を通して，任意のユーザの公開鍵を安全に入手できるものとする．ユーザ A は，ユーザ B と通信を行おうとしているものとする．なお，安全なデバイスにセッション親秘密鍵 SSK* が保存されており，利用端末には，ステージ 0 におけるセッション秘密鍵が保存されているものとする（図 3）．図中の "E_" は暗号処理を，"D_" は復号処理を示す．

A は B の公開鍵を PKI を通して入手し，そのユーザ公開鍵 UPK_B を用いて，セッション用の公開鍵 SPK_A および乱数 A を暗号化して B に送信する．B は，A からのメッセージを復号し，SPK_A と乱数 A' を得る．B は続いて A のユーザ公開鍵 UPK_A を PKI を通じて入手し，B のセッション用公開鍵 SPK_B と，乱数 B，乱数 A' を UPK_A を用いて暗号化し A に返信する．A は，B からのメッセージを復号し，SPK_B，乱数 B'，乱数 A' を得る．ここで，最初に生成した乱数 A と乱数 A' の一致を確認し，SPK_B を保存する．最後に，UPK_B で乱数 B' を暗号化して送信し，B においても乱数 B と B' の一致を確認し，SPK_A を保存する．鍵交換終了後，A，B の利用端末では，移動要求メッセージの処理に備える．移動の度にステージを変えることで，本システムは安全性を確保しているため，移動要求メッセージの待ち受けは，ステージ 1 で待つことになる．ただし，鍵交換終了後で移動を行うまでの通信には，ステージ 0 における SSK_0 が用いられることに注意されたい．

ここでは，key-insulated 公開鍵における最初のステージを 0 としているが，任意のステージ i，j か

ら始めることが可能である．この場合，利用端末に SSK_i，SSK_j が保存されており，セッション公開鍵の交換においてステージ i，j をそれぞれ通知することになる．なお，i と j はそれぞれ独自のパラメータであり，A の移動回数に応じて i が増加し，B の移動回数に応じて j が増加する．詳細は，次に述べる．

移動要求時の処理

移動要求時には，新しいステージのセッション用秘密鍵を用いて移動を相手に通知する．ここでは，A が端末 A1 から A2 に移動するときを例に述べる．本手法では，移動先端末 A2 から移動要求メッセージを送信する．これは，特にモバイル環境において，不意にネットワークから切断される等のディスコネクション状態が発生しても，新しい端末で通信を継続できるようにするためである．まず，A は，移動先端末 A2 に新しいステージ i のセッション用秘密鍵を保存する．（注：A1 には，ステージ i-1 のセッション用秘密鍵が存在している．）（図 4）図中の "S_" は電子署名の処理を，"V_" は電子署名の認証処理を示している．

A2 は，SSK_{Ai} を用いて移動要求に関する電子署名を作成し，これとステージを示す i をメッセージに付与して，B に送信する．B は，ステージ i-1 の移動要求メッセージ受理後，ステージ i の移動要求メッセージを待っており，A2 からのメッセージを認証する．認証処理後，B は，A2 に移動要求に対する ACK を SSK_A を用いて署名を付けて返す．その後，B は，A1 に対し，接続終了要求を SSK_A を用いて署名を付けて送信する．これらふたつの B からのメッセージは，ステージ j のセッション秘密鍵 SSK_{Bj} を用いて電子署名が付与されている．A1 および A2 で移動要求待ち受け用のステージは，j+1 であるが，この処理は移動要求ではないため，待ち受け用ステージ j+1 よりステージ数が一つ少ない，ステージ j の鍵を用いて処理されている．なお，ステージ j の電子署名を送信しても，key-insulated 公開鍵では公開鍵が不変なため，認証することは可能である．最後に，B は移動要求を受け付けるステージを i+1 にする．なお，図中の session ID は，セッション認証情報の検索を高速に行うためのものである．

5. おわりに

本稿では，サービスモビリティを実現するためのサービス移動をセキュアに行うための機構として，セッションレイヤモビリティサポートに key-insulated 公開鍵暗号方式を用いる手法について述べた．Key-insulated 公開鍵暗号方式は，秘密鍵を安全でないデバイス上で利用することを考え，秘密鍵がステージに分けて管理されている．本方式では，ひとつのセッションに一つの key-insulated 公開鍵を割り当て，ユーザの移動にステージを対応づけることにより，デバイスに依存しないモビリティサポートの認証処理を実現することができる．

本稿では，サービスモビリティを実現するためのサービス移動技術としてセッションレイヤモビリティサポートを述べ，Key-insulated 公開鍵暗号方式について説明し，最後に，認証処理に関する手続きを示した．

参考文献

[1] K. Kaneko, H. Morikawa, and T. Aoyama, "Session Layer Mobility Support for 3C Everywhere Environments," In Proc. of the 6th International Symposium on Wireless Personal Multimedia Communications (WPMC 2003), pp. V2-347-351, Yokosuka, Japan, Oct. 2003.

[2] IETF, Internet Engineering Task Force, http://www.ietf.org/

[3] C. E. Perkins, "IP mobility support for IPv4," RFC 3220, Internet Engineering TaskForce, Jan. 2002.

[4] F. Teraoka, Y. Yokore, and M. Tokoro, "A network architecture providing host migration transparency," In Proc. ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM), pp. 209-220, Zurich, Switzerland, Sep. 1991.

[5] A. C. Snoeren and H. Balakrishnan, "An end-to-end approach to host mobility," In Proc. of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 155-166, Boston, Massachusetts, Aug. 2000.

[6] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated Public-key Cryptosystems," Advances in Cryptology -EUROCRYPT 2002, Lecture Notes in Computer Science vol. 2332, L. Knudsen ed., Springer-Verlag, 2002.

[7] M. K. McKusick, K. Bostic, M. J. Karels, and J. S. Quarterman, "The Design and Implementation of the 4.4BSD Operating System," Addison Wesley, Reading, Massachusetts, Apr. 1996.

[8] J. H. Saltzer, D. P. Reed, and D. D. Clark, "End-to-End Arguments in System Design," ACM Transactions on Computer Systems, 2(4), pp. 277-88, Nov. 1984.