暗号技術を用いたセキュアグループコミュニケーションの提案

棚田　慎也 †*，鈴木　秀和 †，内藤　克浩 ‡，渡邊　晃 †
名城大学 †，愛知工業大学 ‡

1　はじめに

ネットワーク技術の発展により, インターネットを介したセキュアな情報共有に関心が高まっている. セキュアな情報共有を実現するために, グループメンバ間でグループ鍵と呼ばれる共通鍵を用いて暗号化を行う方式が一般的に用いられている. しかし, 現存する方式ではサーバ管理者が暗号鍵を所有していたり, グループ退会者がグループ鍵を所有していたりすることにより, 悪意のあるサーバ管理者やグループ退会者からの情報漏えいが懸念されている. そこで本稿では, 代表的アプリケーションであるチャットを例にとり, 生成元が異なる 2 つの乱数を異なる配送経路でグループメンバへ配送し,2 つの乱数からグループ鍵を生成する. これによりグループメンバのみによるセキュアグループコミュニケーションを提案する.

2　現状のチャットシステムの概要

代表的なチャットアプリケーションである LINE を用いて既存の通信方式を説明する.Fig. 1 に LINE におけるグループチャットの通信方式を示す. ユーザがアカウント登録を行う際にエンド端末とチャットサーバ間の暗号鍵が設定される.LINE はエンド端末とチャットサーバによって構成されている. ユーザはグループに招待したいユーザを自由に勧誘しグループを生成する. グループメンバへメッセージを送信する際には, エンド端末とチャットサーバ間の暗号鍵を用いて, 通信経路において暗号化を行う. そのメッセージをチャットサーバで一度平文の状態に復号し, 宛先の端末との間の暗号鍵を用いて再度暗号化を行い, 宛先の端末へ送信する.LINE はこのように, チャットサーバに平文で情報が蓄積されるためセキュリティが脆弱である.

このような課題を解決するため, 鍵サーバからあらかじめグループメンバにグループ鍵を配布し, チャットメッセージ自体を暗号化する方法 [1] が考えられる. しかし, グループメンバが使用するグループ鍵を鍵サーバも所有していることや, グループ退会者が所有していることにより, 悪意のある鍵サーバ管理者やグループ退会者による盗聴が可能になるという課題がある.

3　提案方式

3.1　概要

本提案は悪意のあるサーバ管理者やグループ退会者による情報漏えいを防ぎ, セキュアなグループコミュニケーションを実現することを目的とする. この目的を達成するために, 生成元が異なる 2 つの乱数 (以下 RN1,RN2) を異なる配送経路でグループメンバに配布し, その 2 つの乱数から新たなグループ鍵 (以下 GK) を生成する. そのため, 鍵管理サーバ (Key Management Server:以下 KMS) の管理者には GK を生成できない. この GK を用いて, 同一の GK を所有しているユーザのみが正式メンバとなり相互通信を行う.

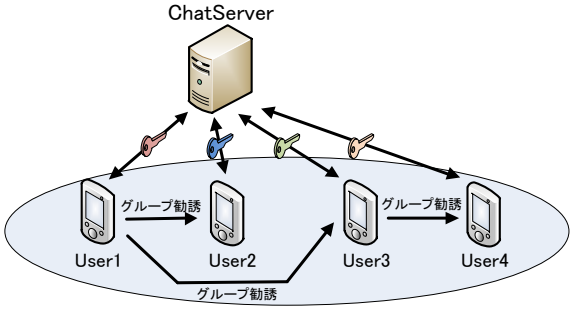


Fig. 1　Communication method of LINE.

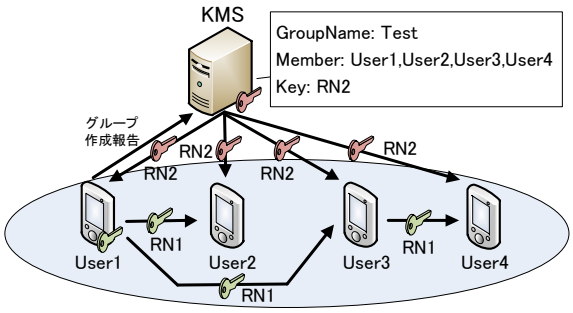


Fig. 2　Proposal of group key sharing method.

3.2　構成要素

Fig. 2 に提案方式におけるグループ鍵共有方式を示す. 提案方式のシステム構成は KMS とエンド端末からなる. これらの装置はいずれも公開鍵証明書を持つものとする.Fig. 2 ではチャットサーバは省略している. これにより装置間の双方向認証を確実に実行する.KMS はグループ名やメンバの管理,RN2 の生成と配布および管理を行う. エンド端末では,KMS へのグループ作成報告やメンバ変更の報告,RN1 の生成や共有および GK の生成, 管理を行う. なお, 公開鍵は RSA(鍵長 1024 ビット以上), 共通鍵は AES(鍵長 128 ビット以上) を使用し暗号化アルゴリズム上はセキュリティの課題がないことを前提とする.

3.3　グループ鍵共有方式

ユーザがグループを作成する際に最初のエンド端末において RN1 を生成する. グループメンバとして招待されたユーザ

Proposal of Secure Group Communication using Encryption Technology

†Shinya Tanada, †Hidekazu Suzuki, ‡Katsuhiro Naito, †Akira Watanabe
†Meijo University, ‡Aichi Insutitute of Technology

はさらに新たにメンバを招待することができる. メンバの招待時に公開鍵証明書を用いてエンド端末間で直接認証を行い, 認証が成功した場合招待された側の公開鍵を用いて RN1 を共有していく.

Fig. 2 は, ユーザ 1 がユーザを招待したため, ユーザ 1 から KMS へグループ作成報告を送信し, その通知を受け取った KMS は当該グループの RN2 を生成し, グループメンバへ配布を行っている様子を示している.RN2 の配布も RN1 と同様に公開鍵証明書を用いてエンド端末と KMS 間で相互認証を行い, 認証が成功した場合エンド端末側の公開鍵を用いて RN2 を配布する.RN2 は一定の更新期間を設け KMS が定期的に生成しメンバに配布する. また参加していたユーザが退会する場合や新たにユーザを追加した場合にも RN2 を更新する. これによりユーザが退会した後の通信内容を閲覧できないようにするための前方安全性や, 新たに参加したユーザが参加する前の通信内容を閲覧できないようにするための後方安全性を確保することができる.

RN1 と RN2 を取得したエンド端末は [RN1|RN2|Group Name] のハッシュ値をグループの暗号鍵 GK として生成する. 同一の GK を所有しているメンバのみが正式メンバとなり相互通信を行うことができる.

3.4 鍵の更新処理

メンバが退会した場合と新たにメンバを追加した場合には以下のようにして鍵を更新する.

3.4.1 メンバが退会した場合

メンバが退会した場合の更新処理の例としてユーザ 3 がユーザ 4 を退会させるケースを Fig. 3 に示す. まずユーザ 3 からユーザ 4 へ退会指示を送る. 退会指示を受け取ったユーザ 4 は強制的に退会させられ, そのタイミングでユーザ 3 から KMS へユーザ 4 の退会通知を送る. 退会通知を受け取った KMS は新しい RN2' を生成し, 自身のデータベースにあるメンバと RN2 の情報を更新する. 新しい RN2' を更新されたメンバへ配布する. 各ユーザは新しい RN2' を用いて GK を生成することにより前方安全性を確保することができる.

3.4.2 新たにメンバを追加した場合

グループにいるメンバが新たにユーザを招待することができる. このとき,RN1 を招待したユーザから招待されたユーザに配布する. そのタイミングで KMS に新たなユーザ招待の通知を送る.KMS は新しい RN2' を更新されたグループメンバへ配布を行う. 各ユーザは新しい RN2' を用いてエンド端末において GK を生成することにより後方安全性を確保することができる.

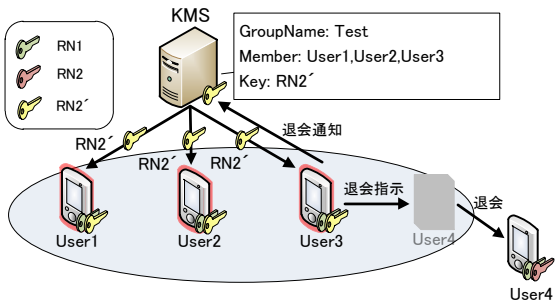


Fig. 3 Update process of group key.

Table 1 Comparison of chat applications.

	項目 (1)	項目 (2)	項目 (3)	項目 (4)
LINE	○	×	×	○
Skype	○	×	×	○
ChatSecure	○	○	○	-
提案方式	○	○	○	○

4 評価

Table 1 にチャットアプリケーションの比較表を示す. 項目 (1)~(3) は電子フロンティア財団 (Electronic Frontier Foundation:以下 EFF)[1] により提示されたチャットアプリケーションのセキュリティ評価項目の一部であり, 項目 (4) は独自に追加した評価項目である. 評価項目の内容は以下のとおりである.

(1) 通信経路が暗号化されている.
(2) 管理者が読めないように暗号化されている.
(3) 暗号鍵が盗まれても過去の通信内容が安全である.
(4) 退会したメンバが通信内容を盗聴できない.

比較対象は, 主流なチャットアプリケーションである LINE と Skype および EFF によるセキュリティ評価項目を全て満たしている ChatSecure の 3 つである.LINE,Skype は通信経路では暗号化されているが, サーバに情報が蓄積してしまうことやサーバとエンド端末間の鍵をサーバが所持しているためセキュリティが脆弱であることがわかる. 一方,ChatSecure は,1 対 1 のチャットアプリケーションであるためグループチャットを行うことはできない.

提案方式について考察を行うと, 項目 (1) は,GK を用いて暗号通信を行うため満たしている. 項目 (2) において RN1 を用いて GK を生成するため RN1 を所有していない KMS は通信内容を読み取ることはできない. 項目 (3) において RN2 を一定期間またはメンバ参加退会時に更新を行うため暗号鍵が盗まれたとしても一定期間内の通信内容が読み取られてしまうだけでその GK を使用する前の通信内容は安全である. 項目 (4) ではメンバ退会時に KMS に通知することで RN2 の更新を行いメンバ退会後のグループメンバへ配布するため退会したメンバが通信内容を読み取ることはできない. ただし, 退会したメンバでもそのメンバがグループに在籍していた期間の通信内容を閲覧することはできる.

5 まとめ

本稿では, 通信端末に公開鍵証明書を付与し, 生成元が異なる 2 つの乱数を共有し, その 2 つの乱数を用いてグループ鍵を生成することでセキュアなグループコミュニケーションが可能であることを示した. またグループ鍵を適宜更新することによりセキュリティの向上を図った. 今後は実装と評価を行っていく予定である.

参考文献

[1] GSAKMP: Group Secure Association Key Management Protocol, RFC4535, IETF (2006).
[2] Electronic Frontier Foundation : Secure Messaging Scorecard. https://www.eff.org/secure-messaging-scorecard .

暗号技術を用いた
セキュアグループコミュニケーションの提案

棚田 慎也† 鈴木 秀和† 内藤 克浩‡ 渡邊 晃†

†名城大学 理工学部
‡愛知工業大学 情報科学部

Watanabe Lab.

研究背景

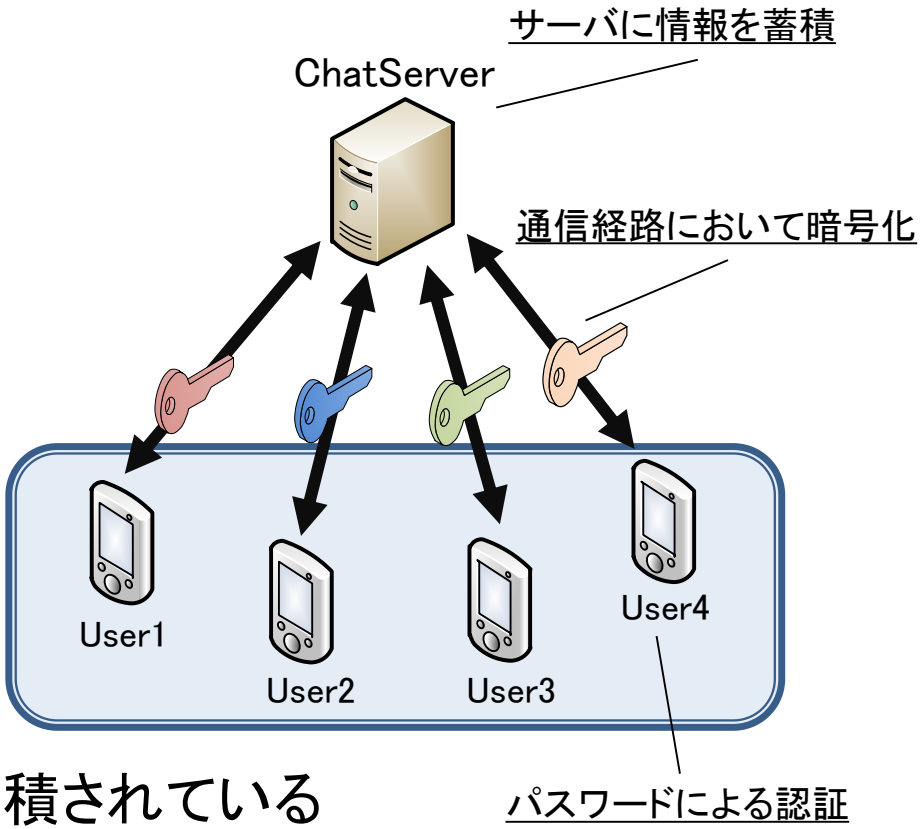
- ネットワーク技術の発展
  - インターネットを介した情報共有
- グループコミュニケーションの有用性
  - セキュリティが重要
- EFF(Electronic Frontier Foundation) のセキュリティ評価※1
  - 管理者が読めないように暗号化されているか
    - 米国NSA 大手IT企業のサーバから直接情報を取得

暗号技術を用いたセキュアグループコミュニケーションの提案

※1 Secure Messaging Scorecard <https://www.eff.org/secure-messaging-scorecard>

既存技術 –LINE–

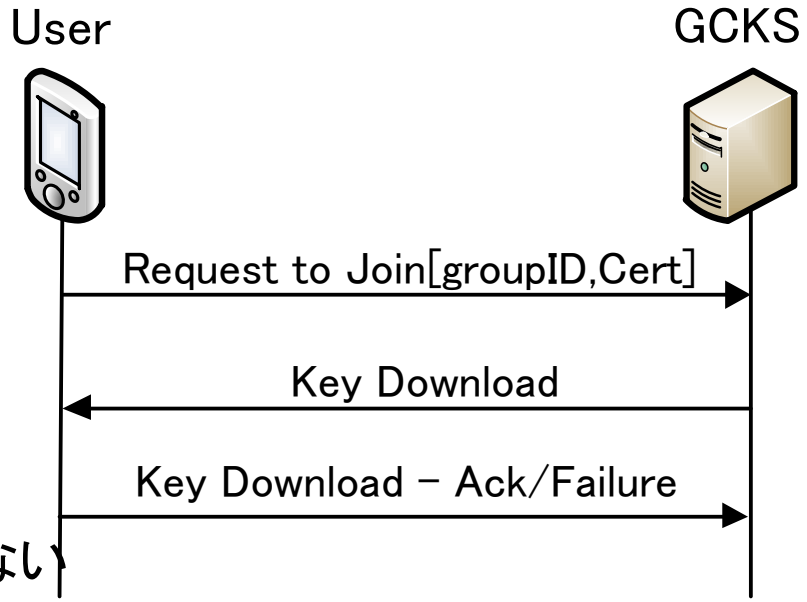
- チャットサーバ
  - 共通鍵を用いて通信
  - 通信内容を蓄積
- エンド端末
  - ログイン時に共通鍵設定
  - グループ生成
  - グループ勧誘
- 課題
  - 平文の状態でサーバに情報が蓄積されている
  - 参加・退会時のセキュリティが考慮されていない



既存技術 –GSAKMP–

(Group Secure Association Key Management Protocol)

- 暗号化グループを生成・管理するフレームワーク(RFC4345)
  - グループオーナー
    - セキュリティポリシー作成
  - 鍵サーバGCKS
    (Group Controller Key Server)
    - グループ鍵生成・配布・更新
    - グループメンバ管理
    - 公開鍵証明書を所有
  - グループメンバ
    - 公開鍵証明書を所有



- 前方安全性/後方安全性の確保
  - 退会後/参加前の通信内容を閲覧できない

- 課題
  - GCKSからグループ鍵を配布
    - 悪意のある鍵サーバ管理者による閲覧

研究の目的

- グループメンバのみによるセキュアなグループコミュニケーション
  - サーバ管理者が通信内容を閲覧できない
  - 前方安全性/後方安全性の確保を行う

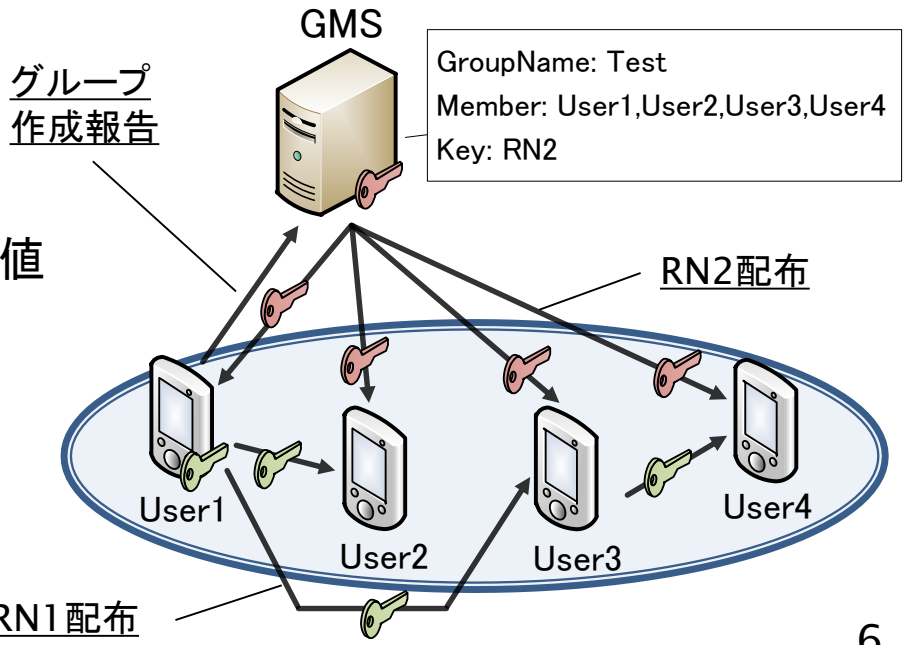
提案方式の概要

- 生成元が異なる2つの乱数を異なる配送経路でメンバに配布
- 2つの乱数を用いてグループ鍵GKを生成
  - GKを所有しているメンバのみによる相互通信
- 適切なタイミングでグループ鍵の更新を行う
  - 前方安全性,後方安全性の確保

提案方式の構成

- GMS(Group Management Server)
  - グループ作成・管理
  - 乱数RN2生成・配布・更新
  - 公開鍵証明書を所有

- エンド端末
  - RN1生成・共有
  - GK生成
    - [RN1|RN2|GroupName]のハッシュ値



提案方式 –乱数RN1共有方式–

1．エンド端末が公開鍵証明書所有

○確実な認証を行うことができる

×公開鍵証明書の取得費用や管理コストがかかる

2．エンドツーエンド通信

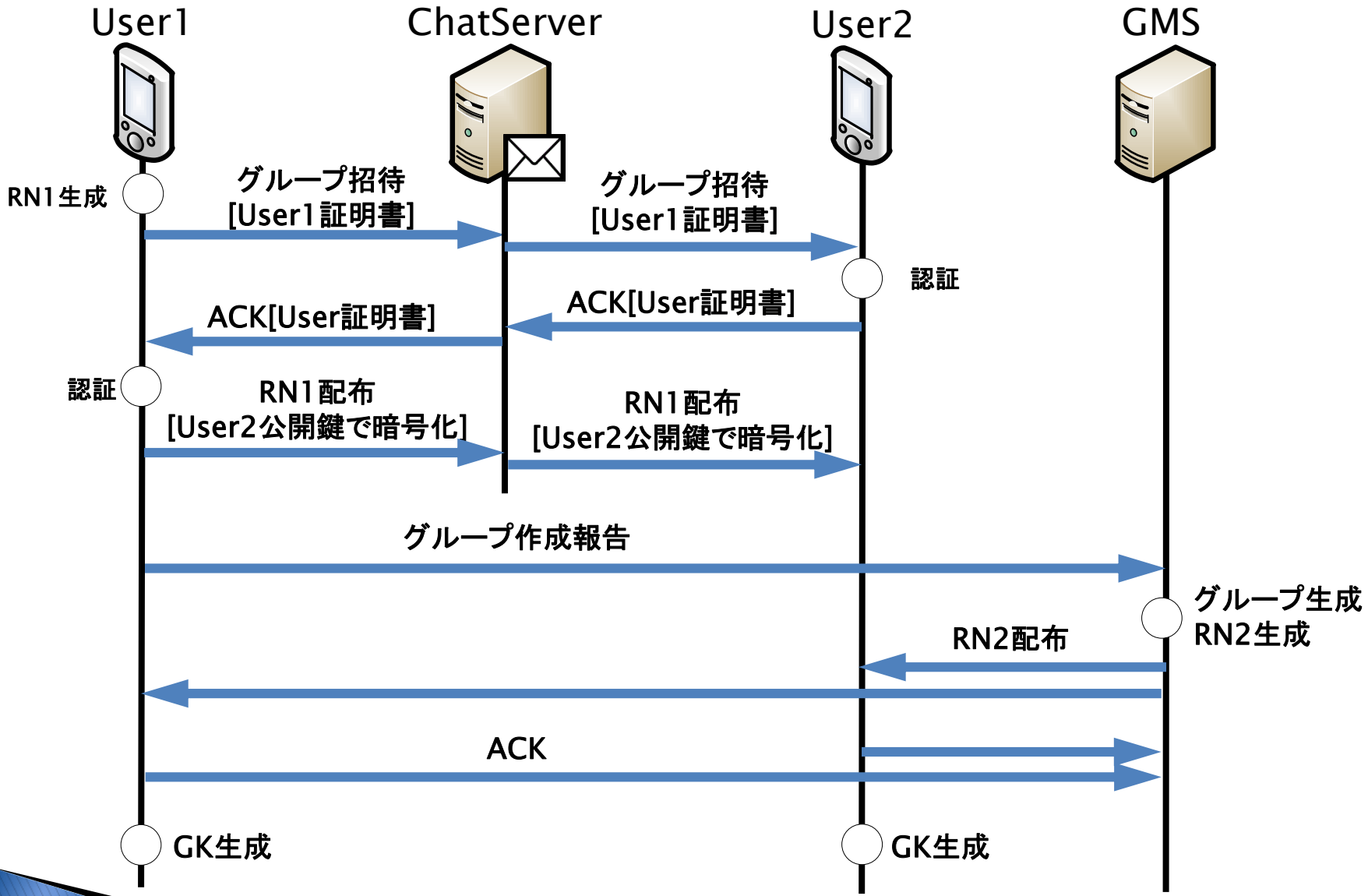
➢NTMobile[1]を用いたエンドツーエンド通信

○公開鍵証明書の取得費用や管理コストがかからない

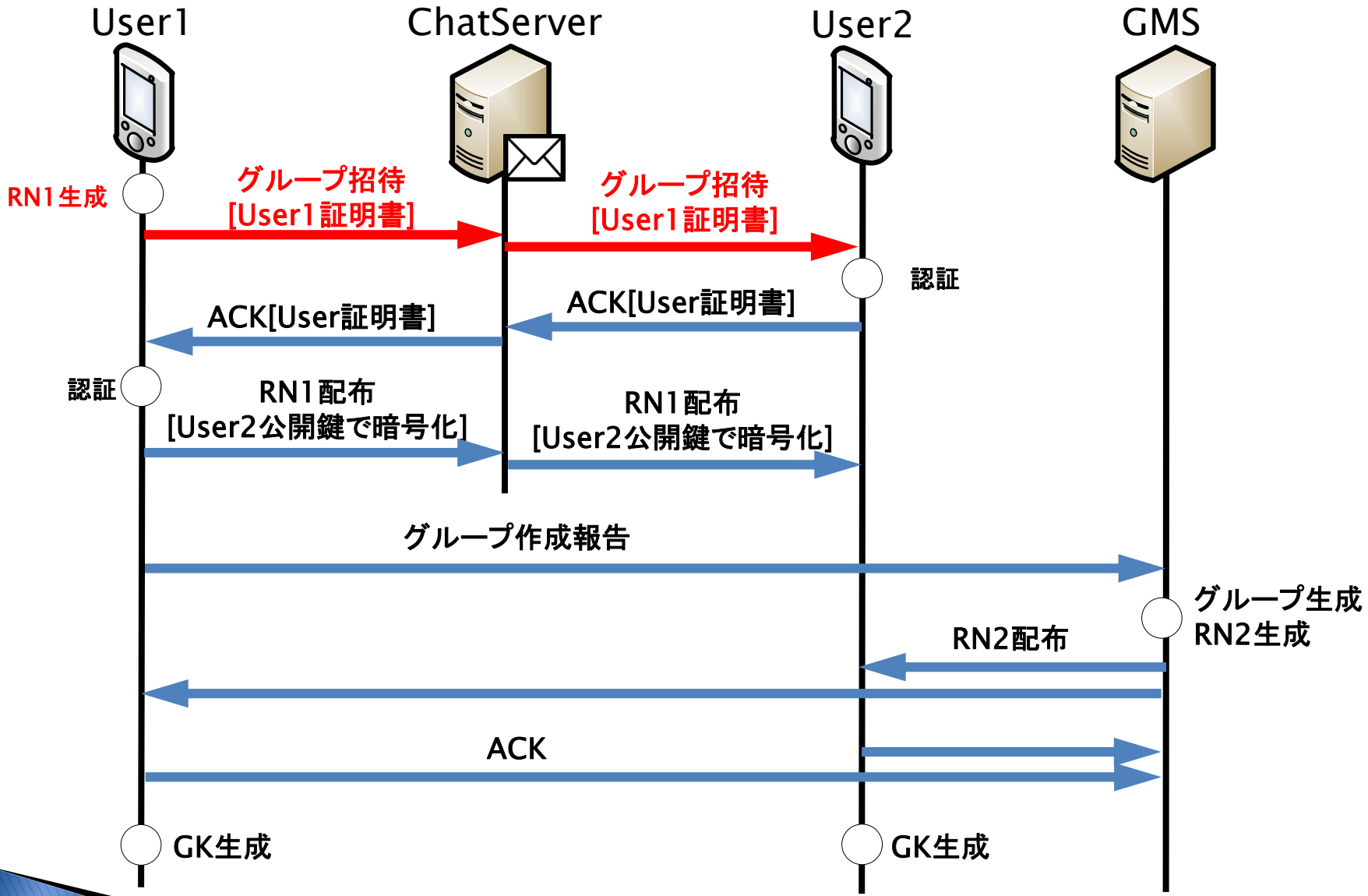
△NTMobileを実装する必要がある

[1] 納堂博史，杉原史人，鈴木秀和，内藤克浩，渡邊晃：
NTMobileの実用化に向けた統合的枠組の検討，
情報処理学会研究報告MBL研究会，Vol.2015-MBL-77，No.20，pp.1－8，2015年12月．

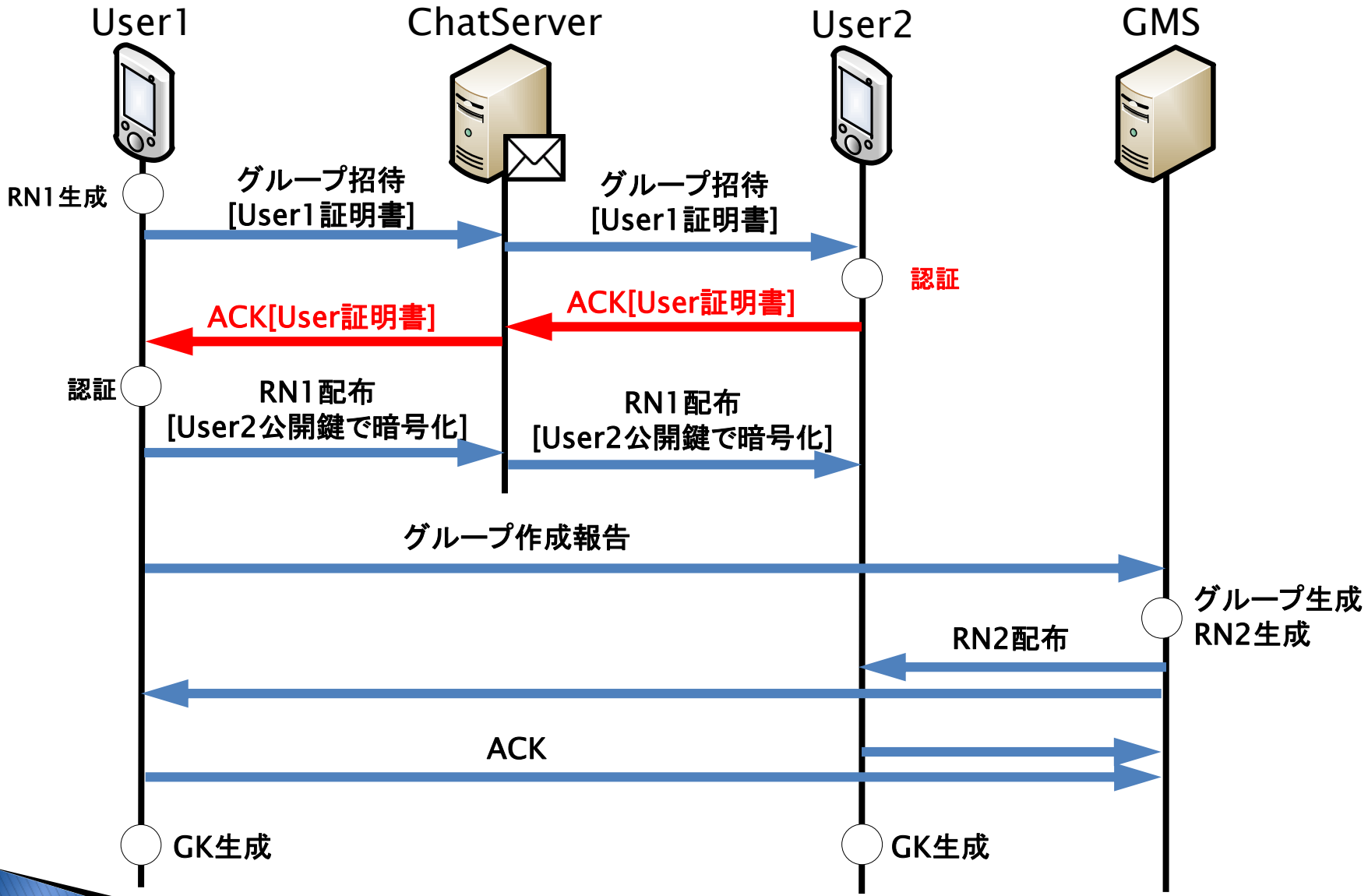
提案方式 –グループ鍵共有方式–



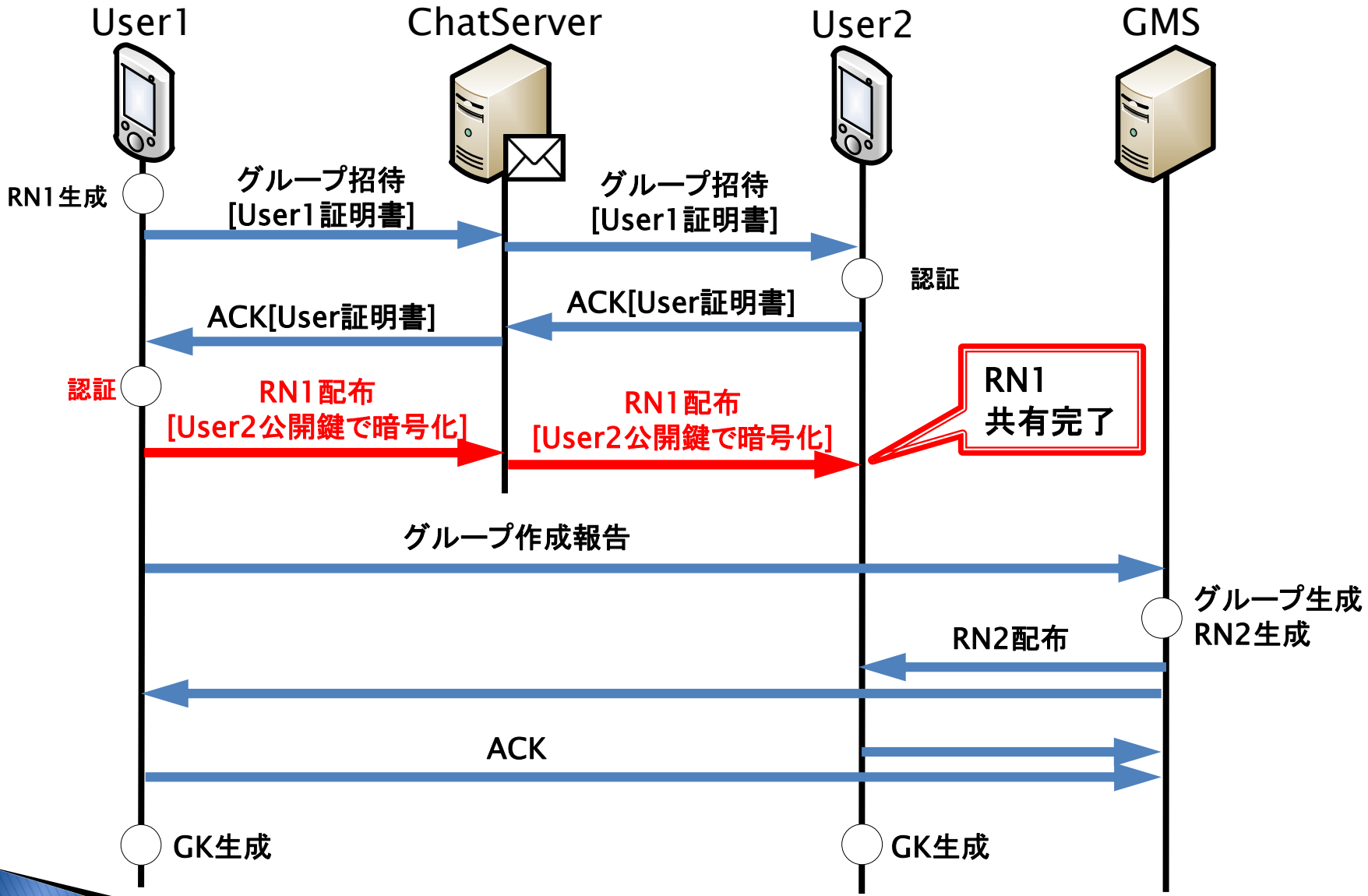
提案方式 –グループ鍵共有方式–



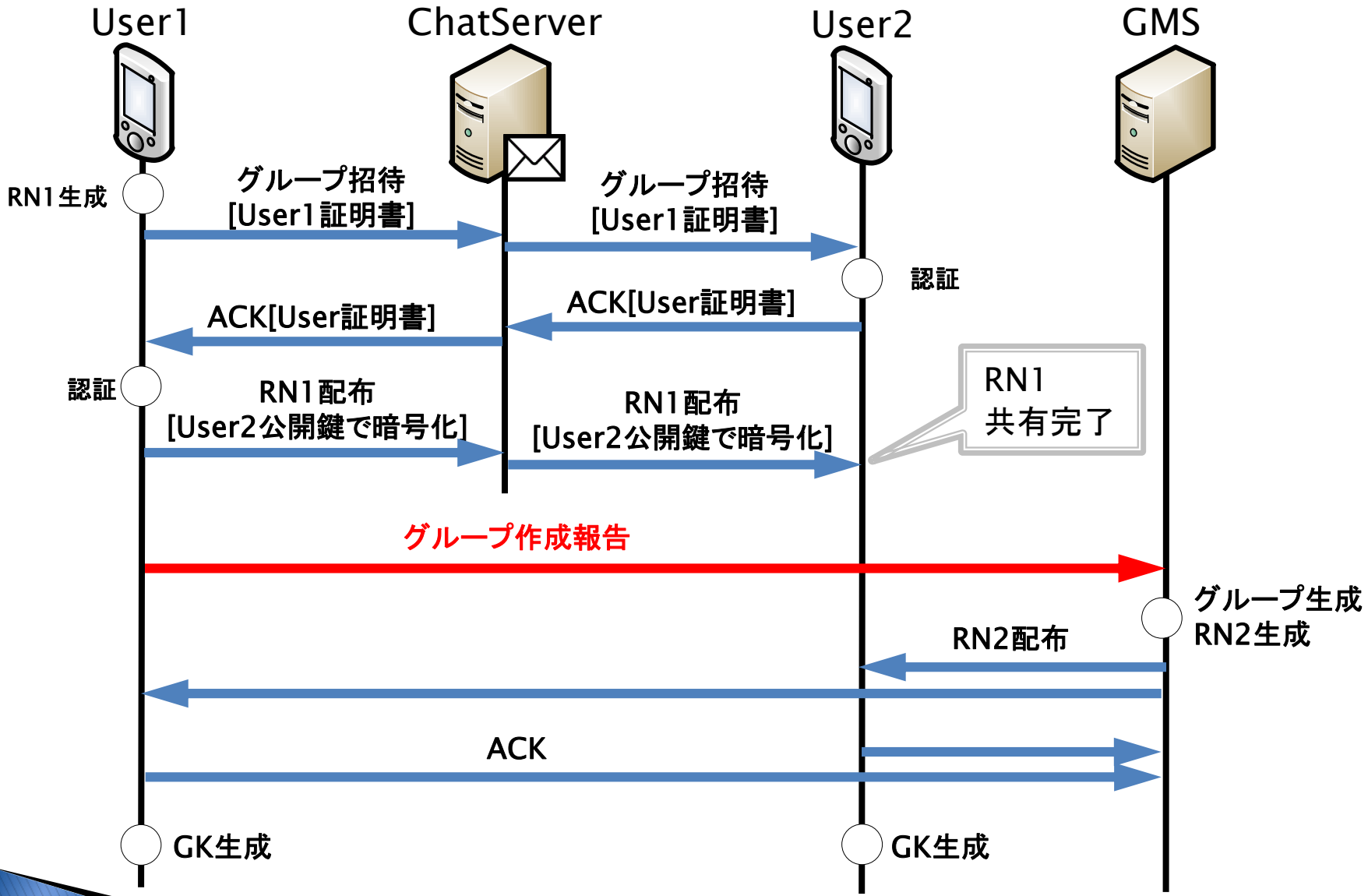
提案方式 –グループ鍵共有方式–



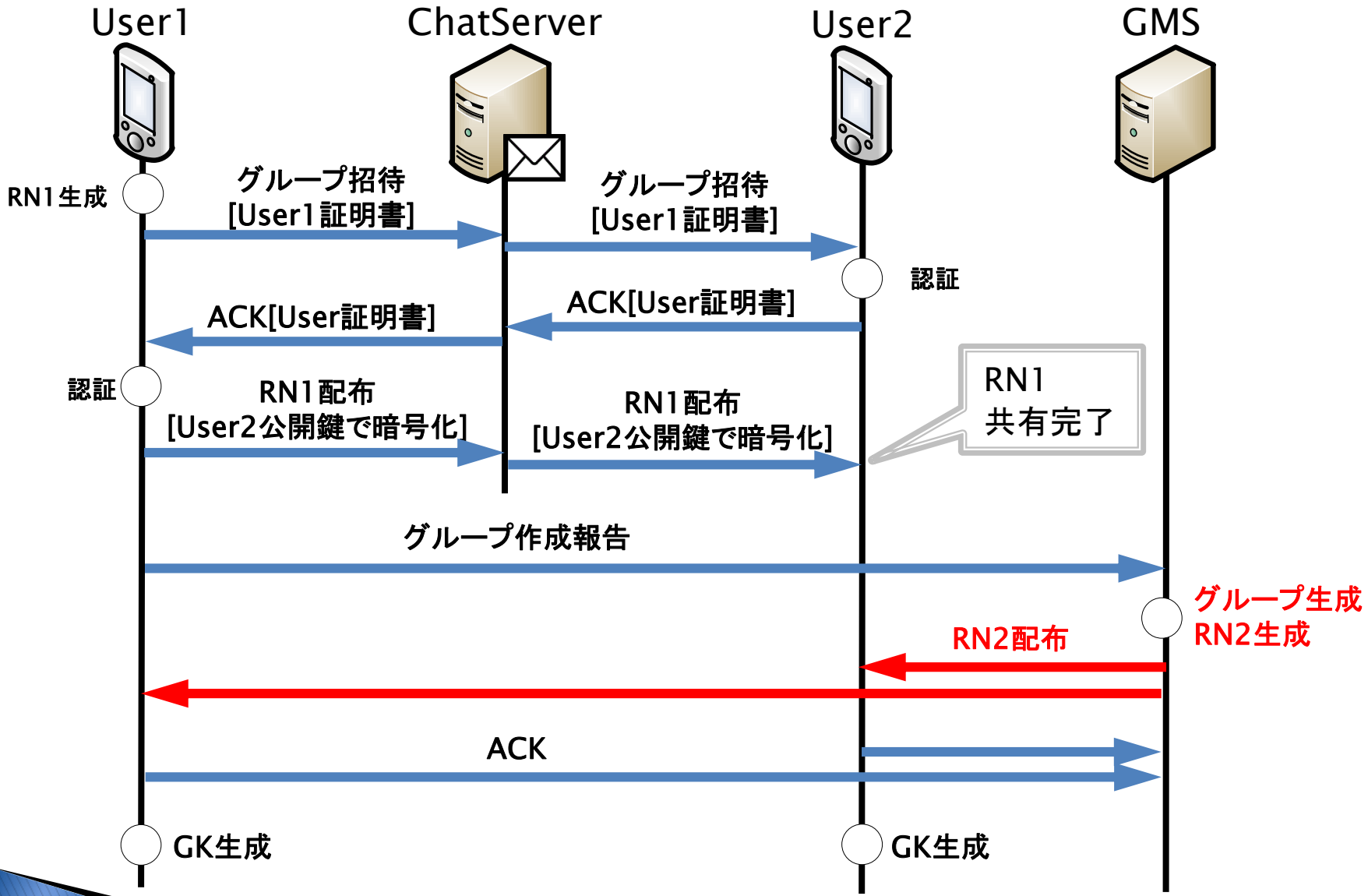
提案方式 –グループ鍵共有方式–



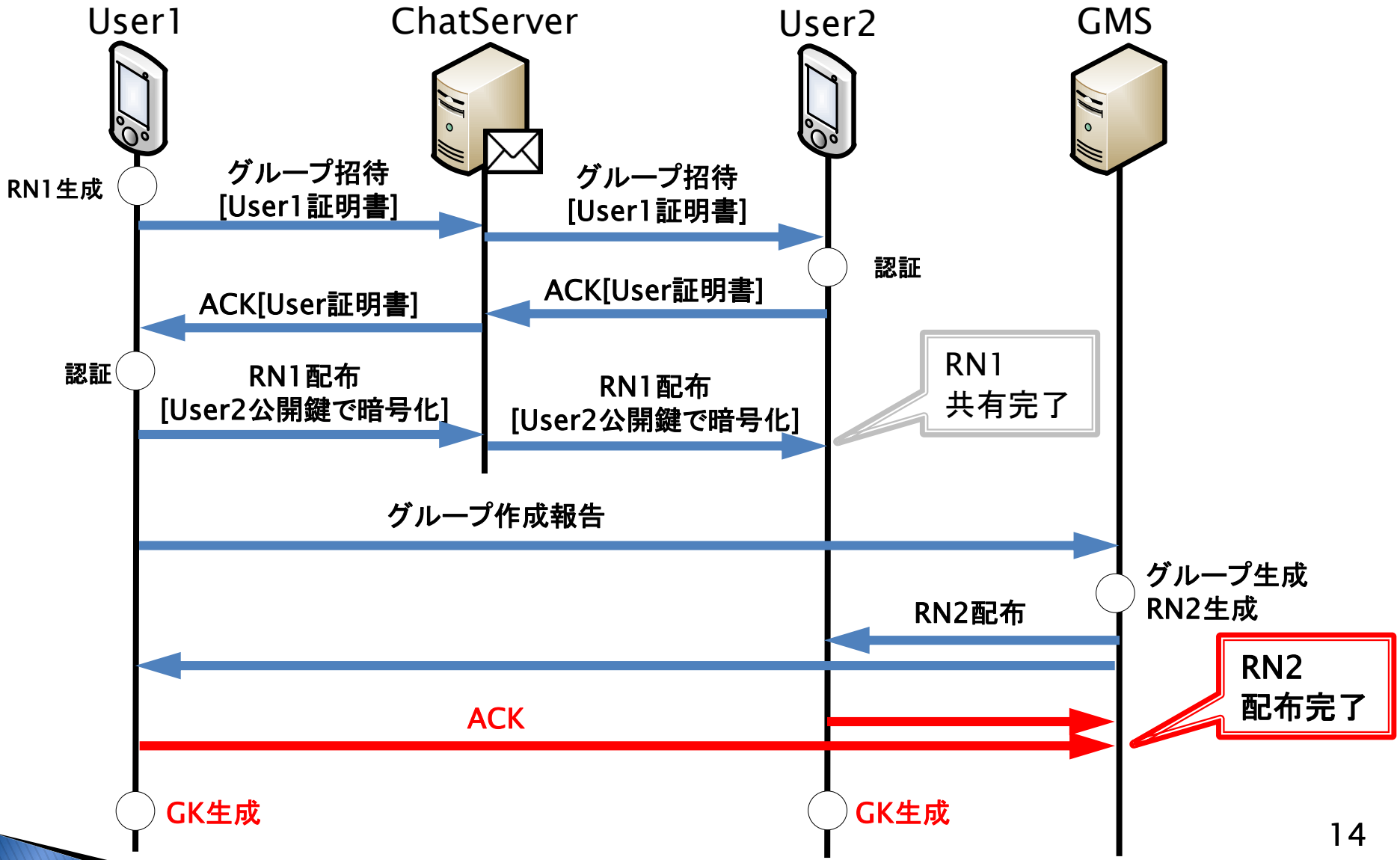
提案方式 –グループ鍵共有方式–



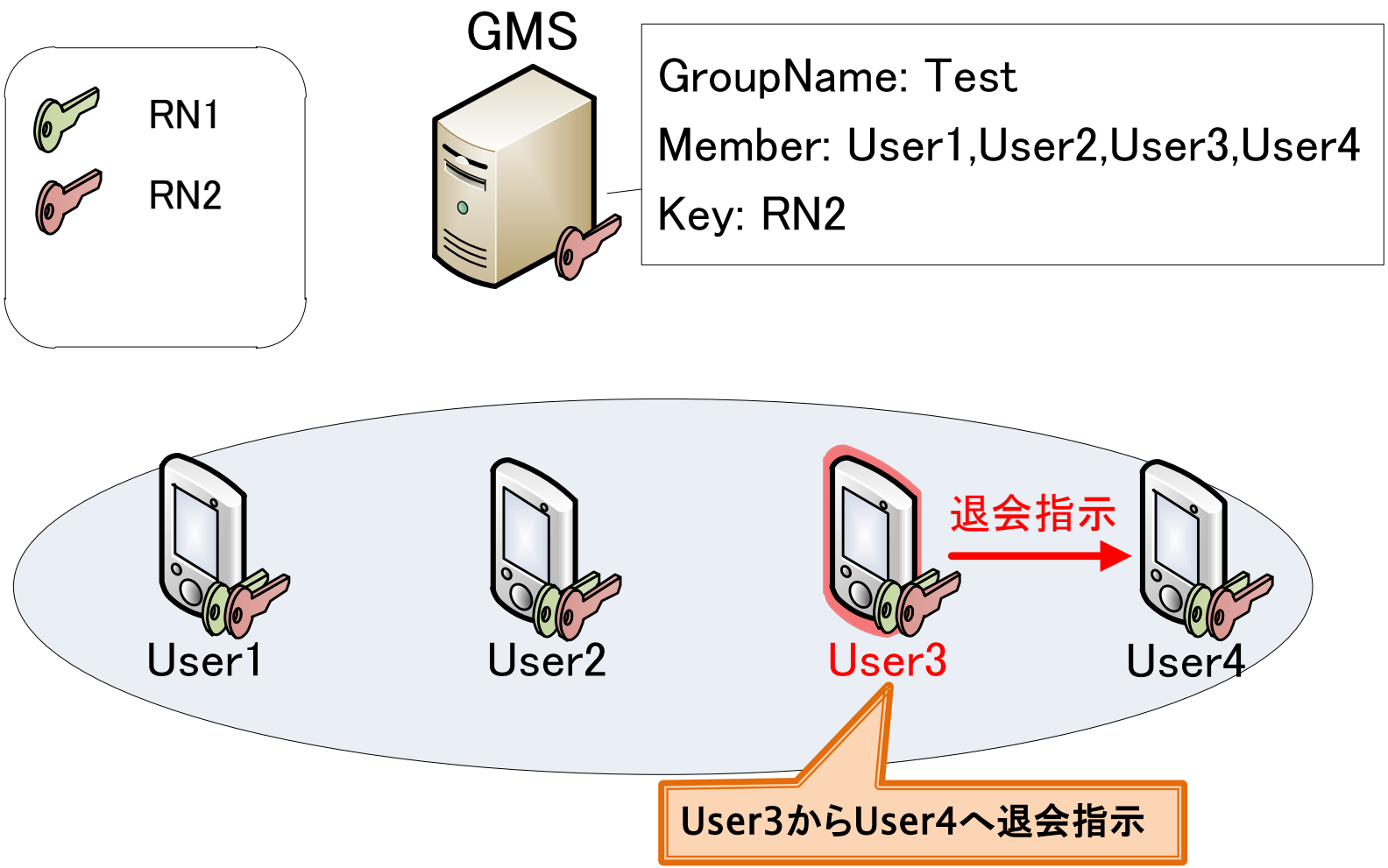
提案方式 –グループ鍵共有方式–



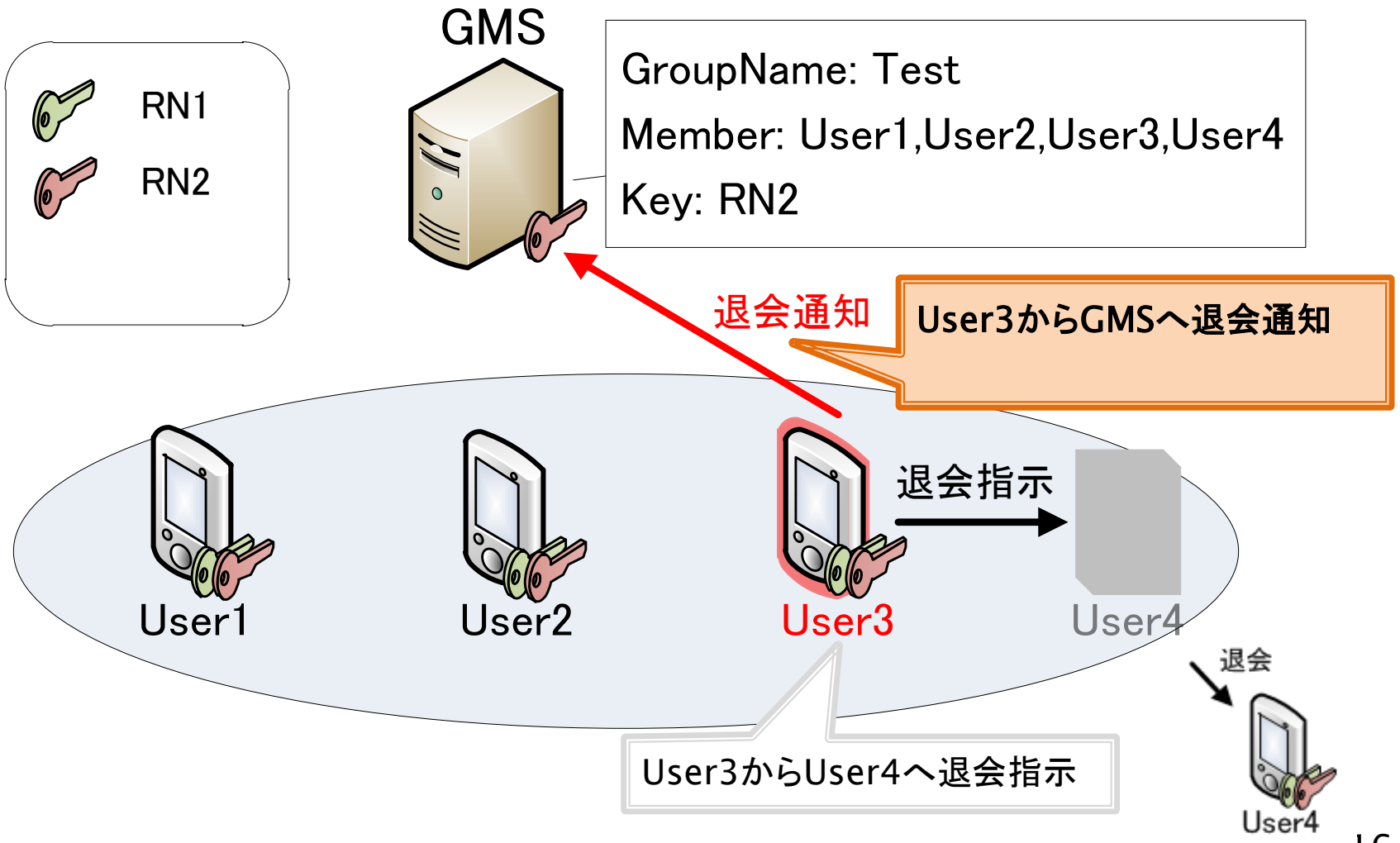
提案方式 –グループ鍵共有方式–



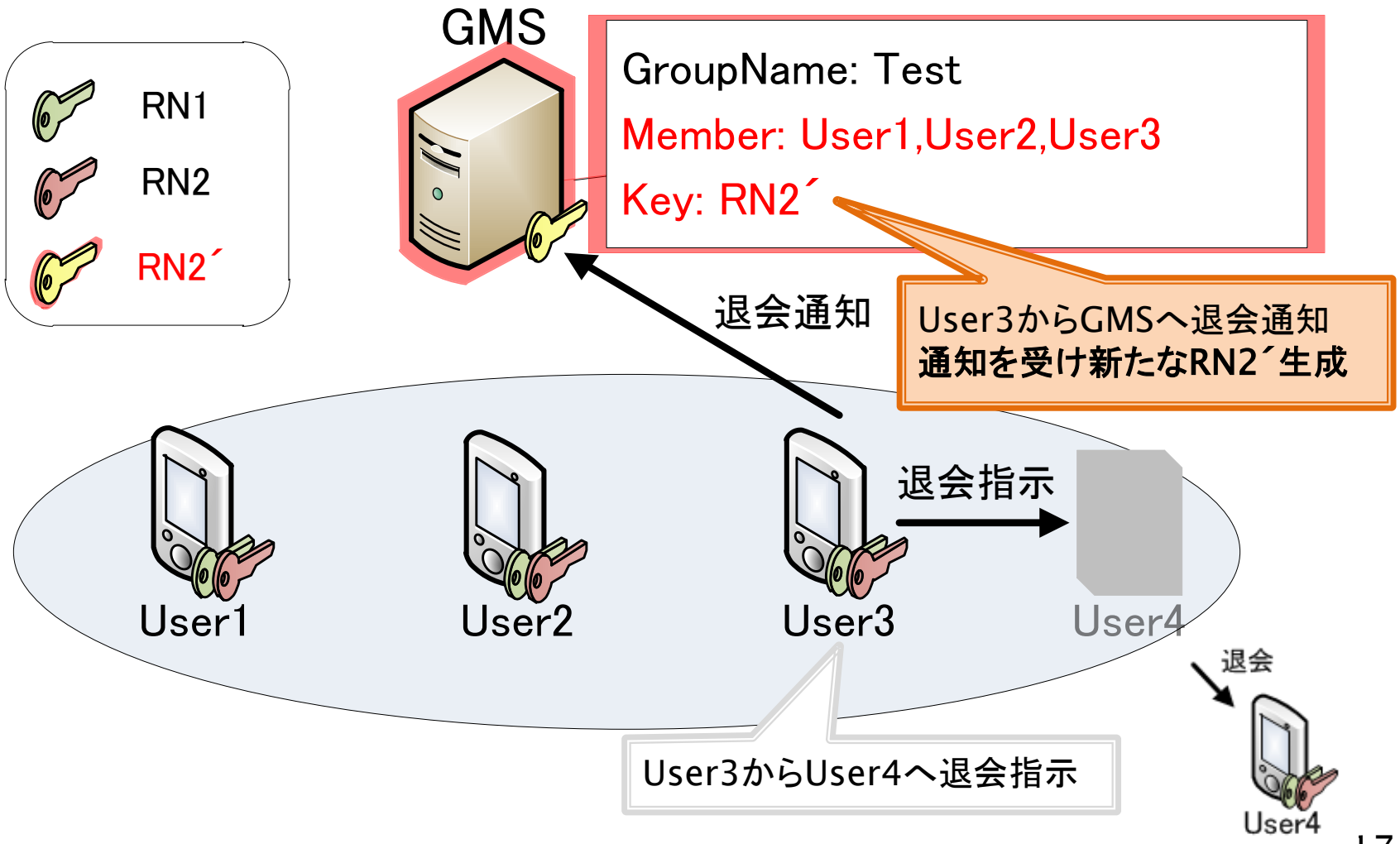
提案方式 –グループ鍵更新処理–



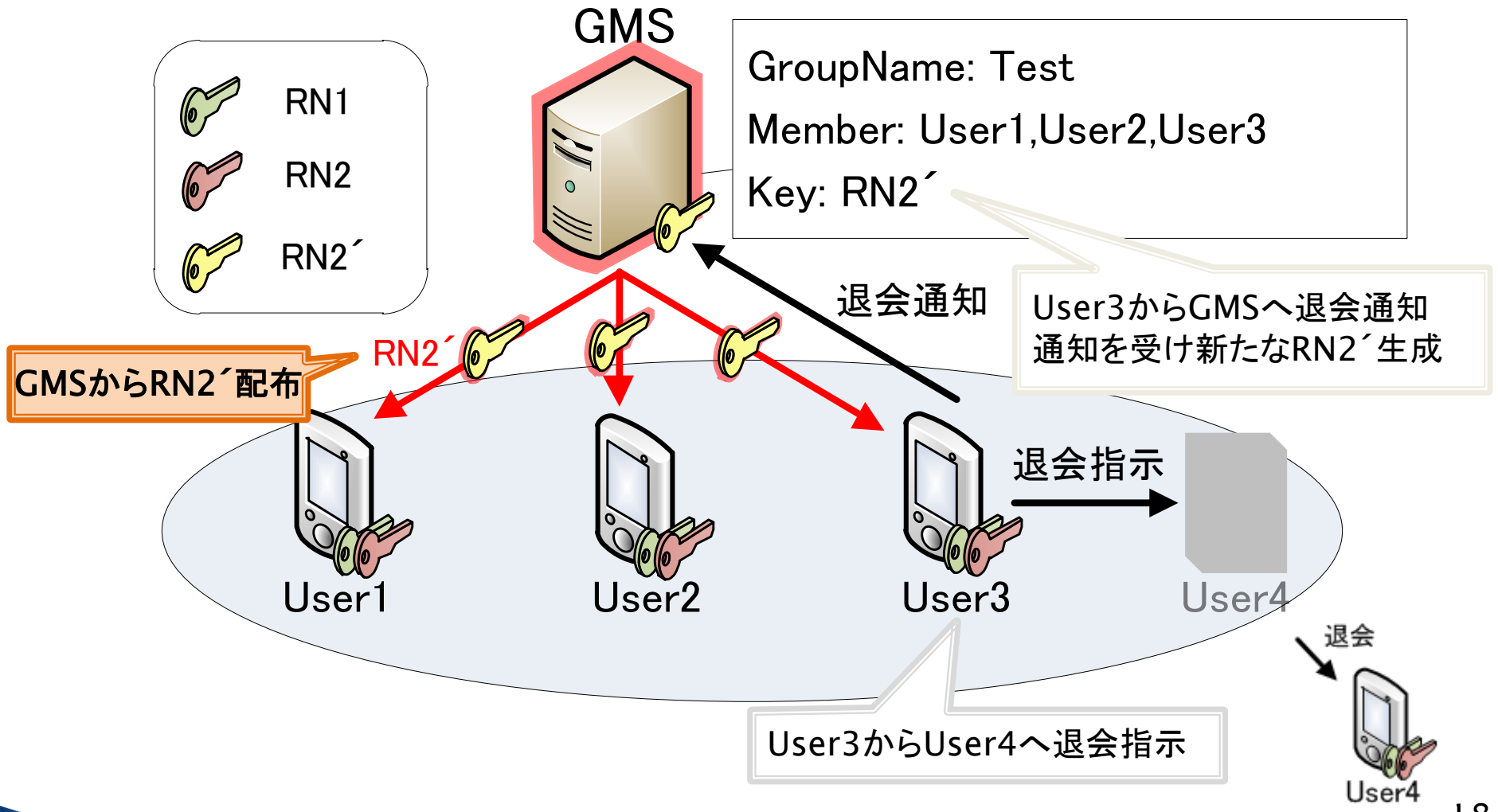
提案方式 –グループ鍵更新処理–



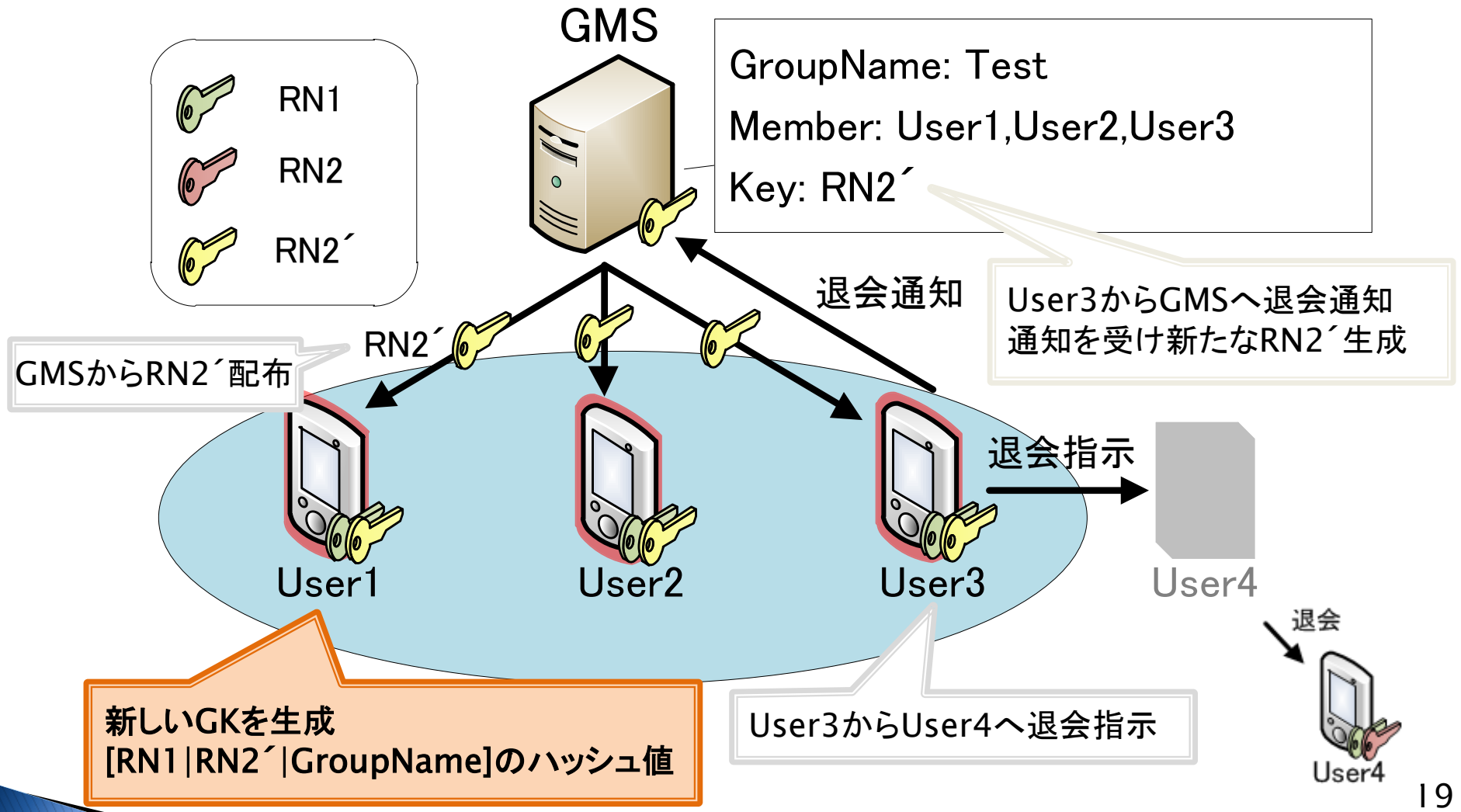
提案方式 –グループ鍵更新処理–



提案方式 –グループ鍵更新処理–



提案方式 –グループ鍵更新処理–



評価

- (1)通信経路が暗号化されている
- (2)管理者が読めないように暗号化されている
- (3)前方安全性と後方安全性を満たしている

(1),(2)・・・EFFによるメッセージアプリケーションのセキュリティ評価項目
(3)・・・独自に追加した評価項目

	項目(1)	項目(2)	項目(3)
LINE	○	×	×
GSAKMP	○	×	○
提案方式	○	○	○

まとめ

- セキュアグループコミュニケーションの提案
  - 2つの乱数を異なる配送経路で配布
  - 2つの乱数からグループ鍵を生成
    - サーバ管理者による通信内容閲覧を防止
  - グループ鍵更新処理を定義
    - 前方安全性/後方安全性を確保

- 今後の予定
  - 鍵更新期間の検討
  - 実装及び性能評価

補足資料

EFFによる Secure Messaging Scorecard

- 1. トランジットで暗号化がされているか?
- 2. プロバイダーが読めないように暗号化されているか?
- 3. 連絡先の確認が可能か?
- 4. 鍵が盗まれても過去の通信内容が安全か?
- 5. コードが公開されていて, 個別の評価が可能か?
- 6. セキュリティの方針は適切に文書化されているか?
- 7. コードは監査を受けているか?

	項目1	項目2	項目3	項目4	項目5	項目6	項目7
LINE	○	×	×	×	×	×	×
Skype	○	×	×	×	×	×	×

GK作成における検討

- RN1のみの場合
  - エンド端末において鍵の更新,配布が必要
  - RN1が漏えいしてしまうと盗聴可能
    - RN2もあればRN1のみではGKを作ることが出来ない
- RN2のみの場合
  - 管理者が盗聴可能
- RN1・RN2によるGK作成
  - 二重化によるセキュリティ向上
  - RN1では更新などの処理が不要になる

GMSにおける検討

- チャットサーバとは別にGMSを設置
  - 負荷分散
  - GMSはグループ管理,乱数の配布・更新のみ
  - 既存技術への導入が可能

- 課題
  - GMSがRN2の更新・配布を行う
    - ⇒利用グループの増加によりGMSへの負荷が大きくなる
    - ⇒RN2の更新頻度の検討を行う必要がある

RN2バージョン機能

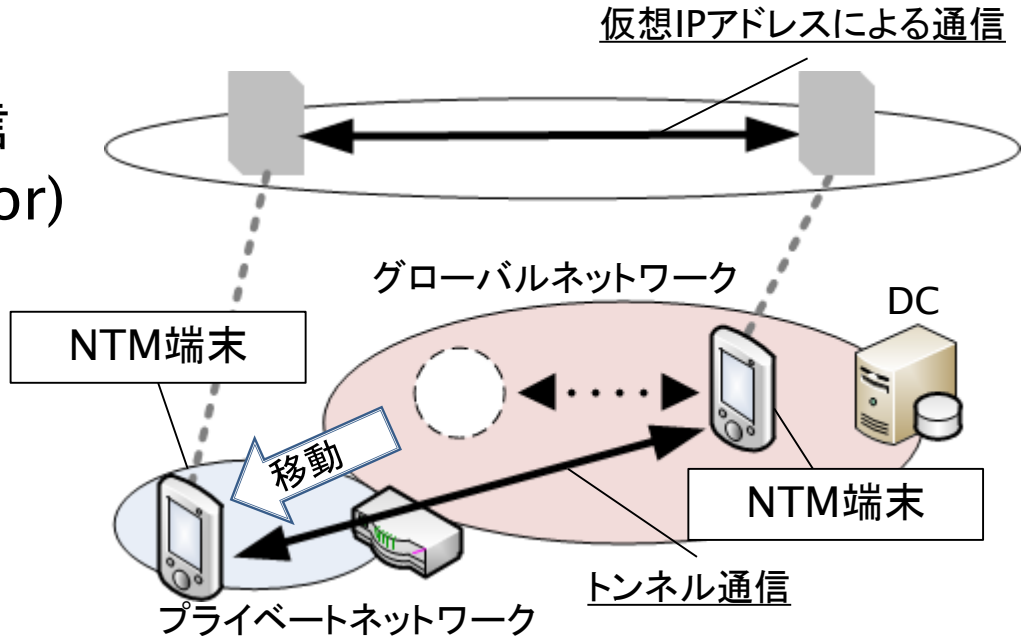
- RN2更新処理における課題
  - 電源がオフである
  - ネットワークが輻輳している
  - 電波が届かない状態である

} 新しいRN2を配布できない

- RN2にバージョン機能を付与
  - 電源をオンにしたタイミングで必ずGMSに問い合わせ
  - メッセージフォーマット内にRN2バージョンを付与
  - メッセージ受信側が自身のRN2バージョンと比較
    - 受信側のバージョンが古い → GMSへ配布要求
    - 送信側のバージョンが古い → 送信側へ通知 → GMSへ配布要求

NTMobile (Network Traversal with Mobility)

- 移動透過性と通信接続性を実現する技術[1]
  - NTM端末
    - 仮想IPアドレスを用いた通信
  - DC(Direction Coordinator)
    - 経路指示を行う
  - 仮想IPアドレス
    - 実IPアドレスに依存しない

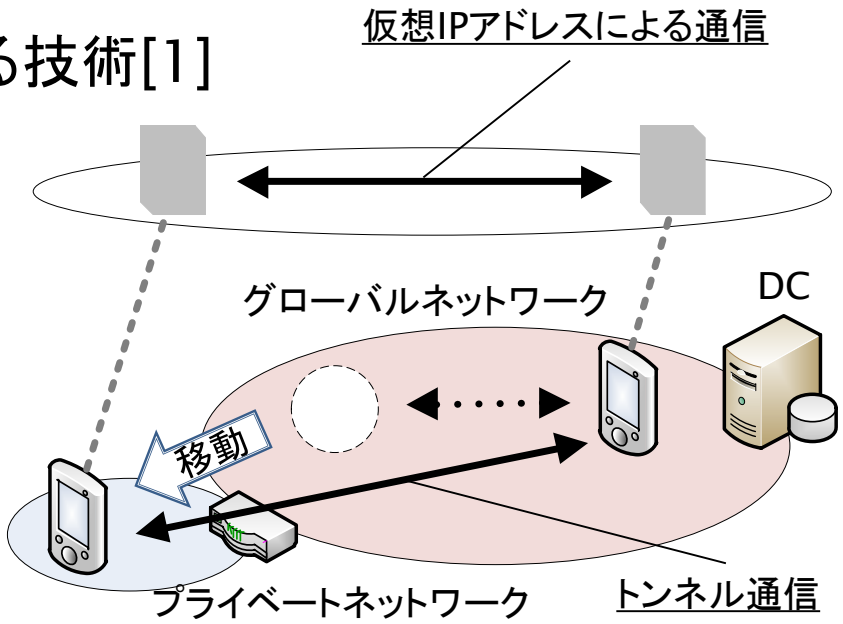


- トンネルによるエンドツーエンド通信

実装方針

- 仮想マシン上にGMS(Group Management Server)を構築
- NTMobile(Network Traversal with Mobility)[1]を使用
  - エンド端末間通信をサポート

- NTMobile
  - 移動透過性と通信接続性を実現する技術[1]
    - NTM端末
      - 仮想IPアドレスを用いた通信
    - DC(Direction Coordinator)
      - 経路指示



[1] 納堂博史，杉原史人，鈴木秀和，内藤克浩，渡邊晃：
NTMobileの実用化に向けた統合的枠組の検討，
情報処理学会研究報告MBL研究会，Vol.2015-MBL-77，No.20，pp.1－8，2015年12月．