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

120430063 棚田 慎也
渡邊研究室

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. これを実現するためにグループでの情報共有の際にグループ鍵と呼ばれる共通鍵を用いて暗号化する方法が一般的に用いられる. しかし, 既存の方式ではサーバ管理者やグループ退会者がグループ鍵を所有していることから情報が漏えいしてしまう恐れがある. そこで本稿では, 生成元が異なる 2 つの乱数を異なる配送経路で配送し, その 2 つの乱数を用いてグループ鍵を生成することによるセキュリティを向上したセキュアグループコミュニケーションシステムを提案する.

2. 既存技術

グループ鍵を用いた既存技術で GSAKMP(RFC4535)[1] がある.GSAKMP はグループオーナー (GO), グループ鍵管理サーバ (GCKS), グループメンバ (GM) で構成されている.GO により作成されたセキュアポリシーを基にメンバのアクセス制御を実行する. そのセキュアポリシーに基づき GCKS はメンバの管理や鍵の生成を行う.GM は自身の公開鍵証明書を用いて GCKS の認証を受け, 成功した場合,GCKS からグループ鍵を受け取る. また,GCKS から鍵更新用の鍵も配布され, 一定期間で鍵を更新するようにセキュアポリシーにより設定されている. しかし,GCKS がグループ鍵を所有しているため, 悪意のあるサーバ管理者に通信内容を読み取られてしまう恐れがある.

3. 提案方式

3.1 概要

本提案はサーバ管理者が通信内容を読み取ることができないセキュアなグループコミュニケーションシステムを実現する. システム構成は鍵管理サーバ (Key Management Server:以下 KMS) とエンド端末からなり, グループの定義は管理者が行ってもよいが, ユーザが主体となることもできる.KMS はグループ名とメンバの管理, 乱数 RN2 の生成を行う. エンド端末はグループメンバの勧誘と乱数 RN1 の生成および共有を行う. エンド端末と KMS に公開鍵証明書を持たせ相互認証を確実に行い, 認証成功時にその公開鍵を用いて RN1,RN2 の共有を行う.2 つの乱数 RN1,RN2 を用いて GK を生成する. 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) を利用し, 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.

3.2 グループ鍵共有方式

図 1 に提案方式におけるグループ鍵共有方式を示す. 最初のユーザがグループを作成する際に RN1 の生成を行う. メンバをグループへ招待するとき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, その公開鍵を用いて RN1 を共有する. グループ作成時に招待側のユーザから KMS にグループ作成報告を送る. 報告を受け取った KMS は RN2 の生成を行い, グループ内の全てのメンバへ配布する.RN2 は一定の更新期間を設け定期的に生成し更新する. またメンバが新たに参加したタイミングやメンバが退会したタイミングでは必ず RN2 を更新することで, 前方安全性と後方安全性を確保する.RN1 と RN2 を取得したエンド端末は [RN1|RN2|GroupName] のハッシュ値を GK として生成する. 各エンド端末において生成した GK を用いて暗号化通信を行うため, 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.

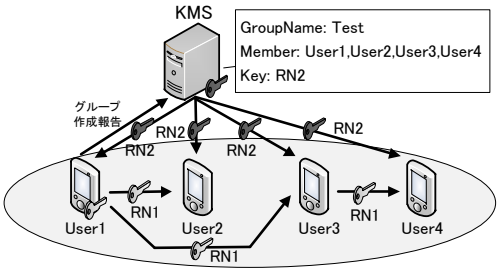


図 1: 提案方式におけるグループ鍵共有方式

表 1: 類似技術における比較

	項目 1	項目 2	項目 3	項目 4
GSAKMP	○	×	○	○
ChatSecure	○	○	○	-
提案方式	○	○	○	○

4. 評価

表 1 に類似技術の比較を示す. 項目 1~3 は電子フロンティア財団 (Electronic Frontier Foundation:以下 EFF)[2] により提示された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. その時点のグループメンバのみが通信を行える.

比較対象は GSAKMP と ChatSecure である.GSAKMP はサーバ管理者が通信内容を読み取れる恐れがある. 一方 ChatSecure は EFF による評価項目を全て満たしているが 1 対 1 のチャットであり, グループを形成できない. 提案方式では,2 つの乱数を異なる配送経路で共有し,RN2 を更新することで項目を全て満たすことができる.

5. まとめ

本稿では, 生成元が異なる 2 つの乱数を共有し, 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を提案した. 今後は実装や再評価を行う予定である.

参考文献

[1] GSAKMP: Group Secure Association Key Management Protocol, RFC4535, IETF (2006)

[2] Electronic Frontier Foundation : Secure Messaging Scorecard,available from "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

理工学部 情報工学科
120430063
渡邊研究室 棚田 慎也

Watanabe Lab.

研究背景

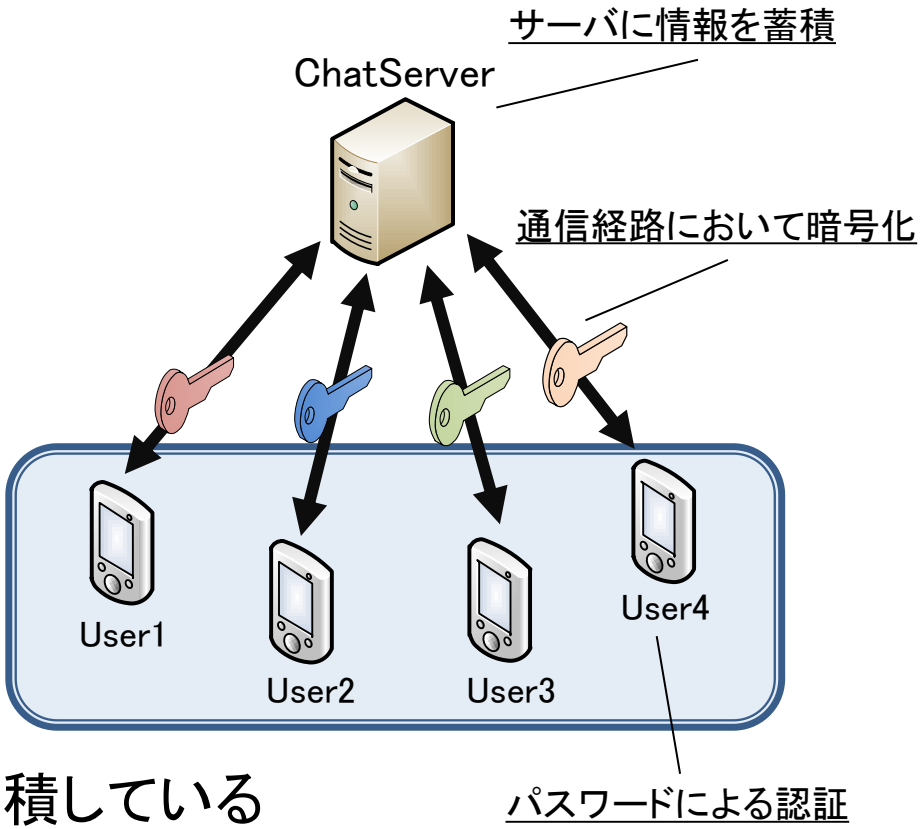
- ネットワーク技術の発展
  - インターネットを介した情報共有
- チャットアプリケーションの普及
  - 強力なコミュニケーションツール
- 米国NSA 大手IT企業のサーバから直接情報を取得
  - EFF(Electronic Frontier Foundation)によるメッセージアプリケーション評価※1
    - セキュリティがぜい弱である

暗号技術を用いたセキュアな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
  - 新規登録時に共通鍵設定
  - 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している



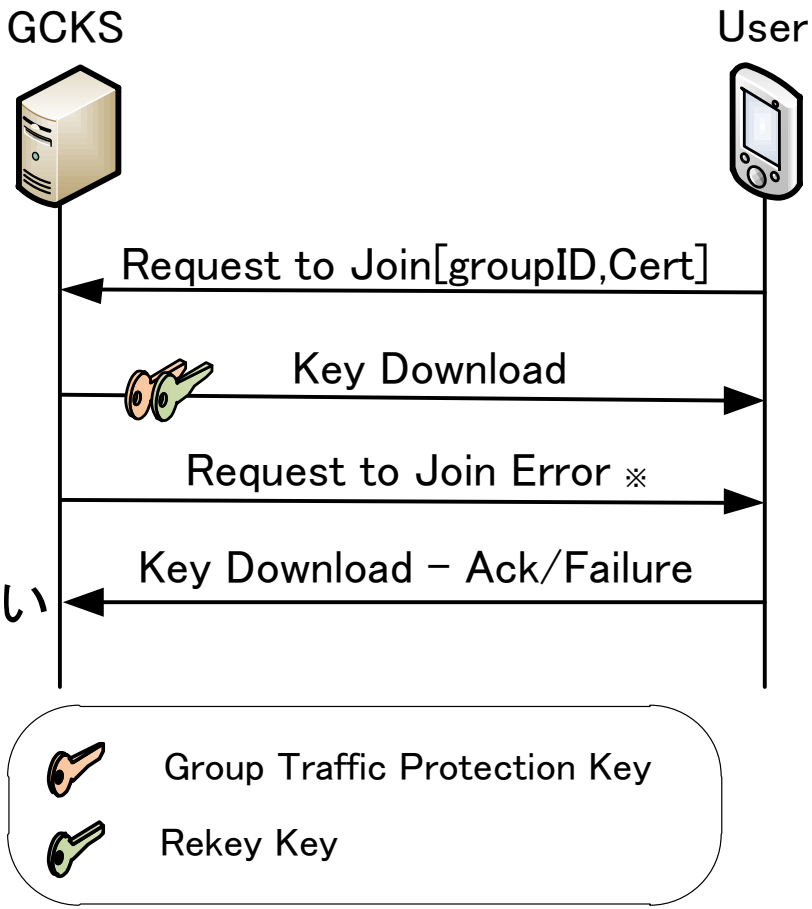
既存技術 -GSAKMP-

(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
    - 悪意のある管理者による閲覧



※ Option

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
    - 退会した後の通信内容を閲覧できない
    - 参加する前の通信内容を閲覧できない

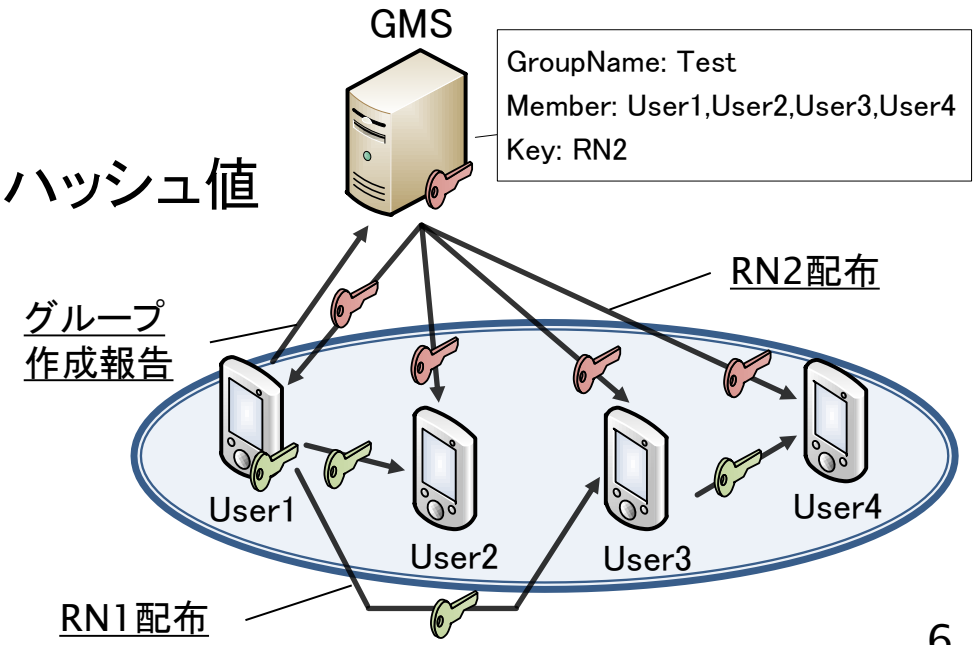
提案方式の概要

- 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
  - サーバではグループ鍵を生成できない
  - GKを所有しているメンバのみによる相互通信
- グループ鍵の更新を行う
  - 前方安全性,後方安全性の確保

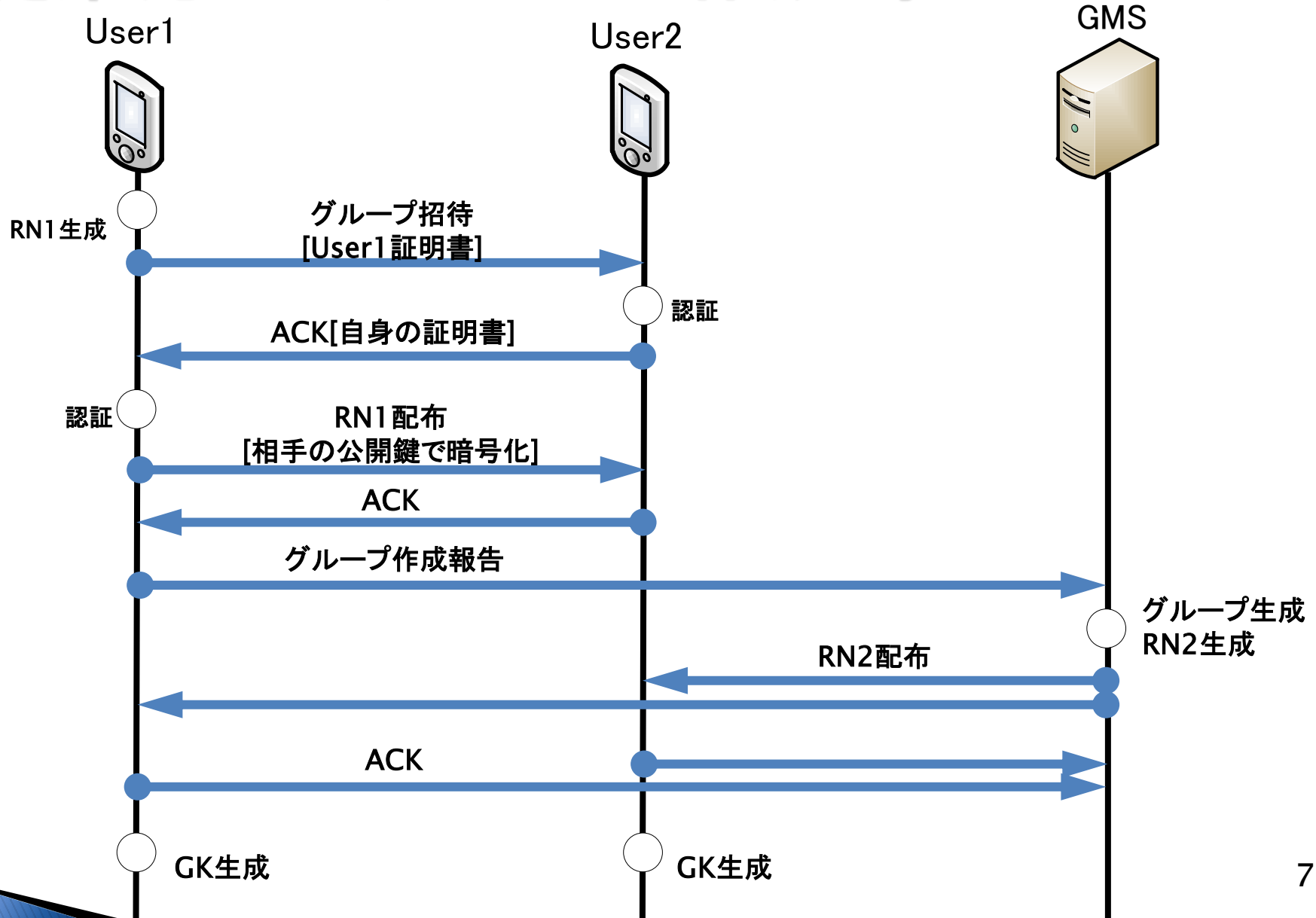
提案方式の構成

- 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

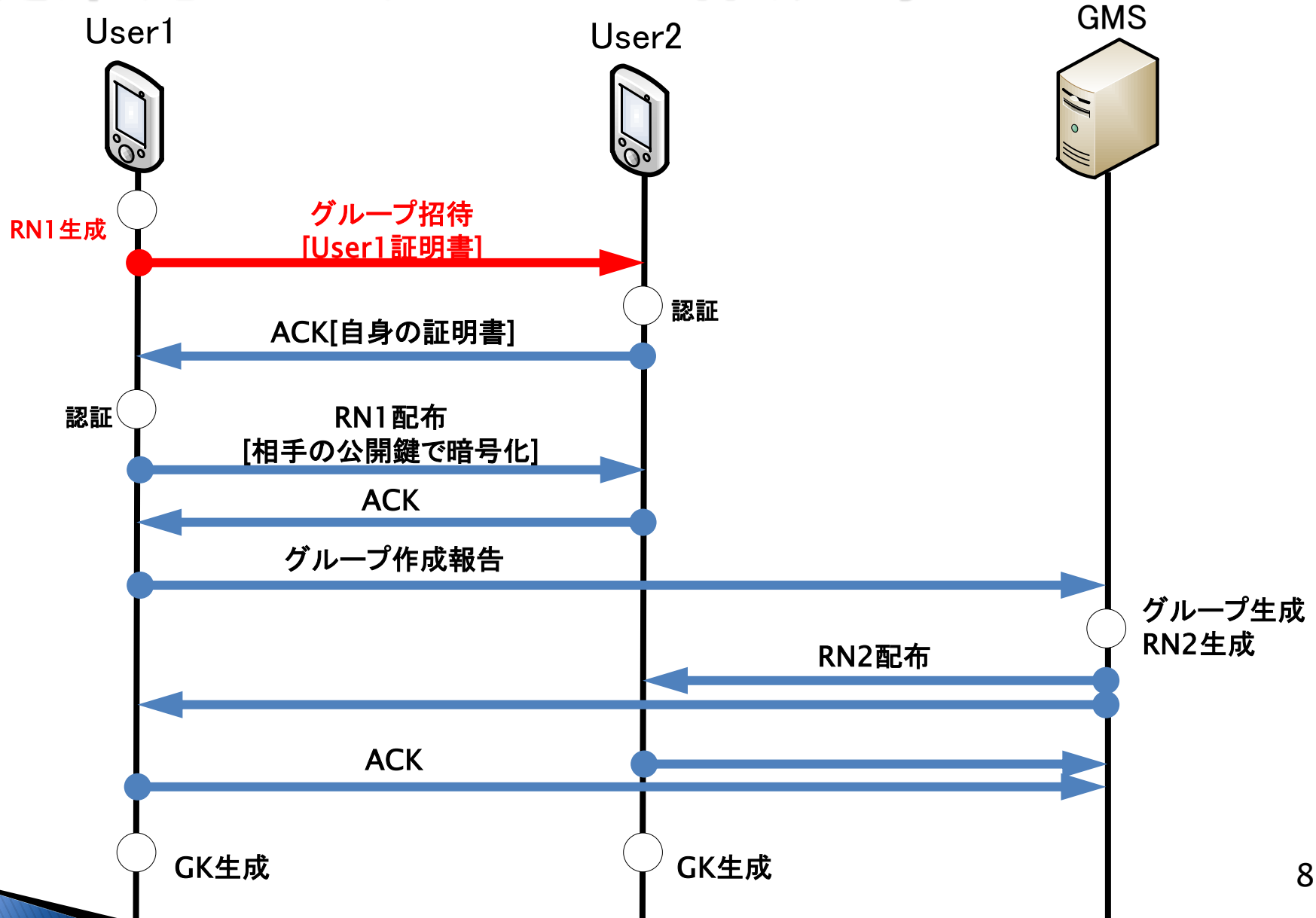
- エンド端末
  - RN1生成・共有
  - GK生成[RN1|RN2|GroupName]のハッシュ値
  - 公開鍵証明書を所有



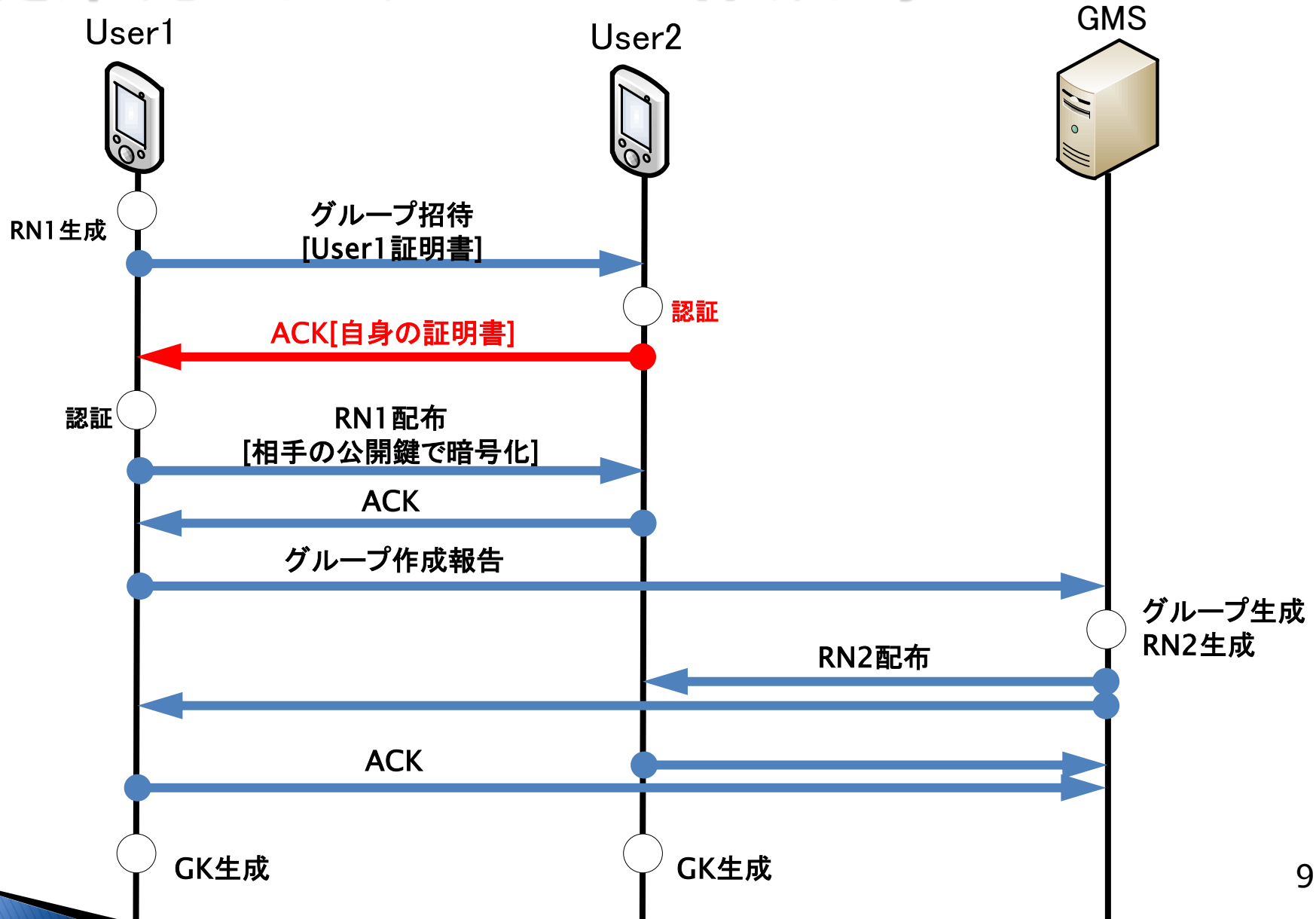
提案方式 –グループ作成時–



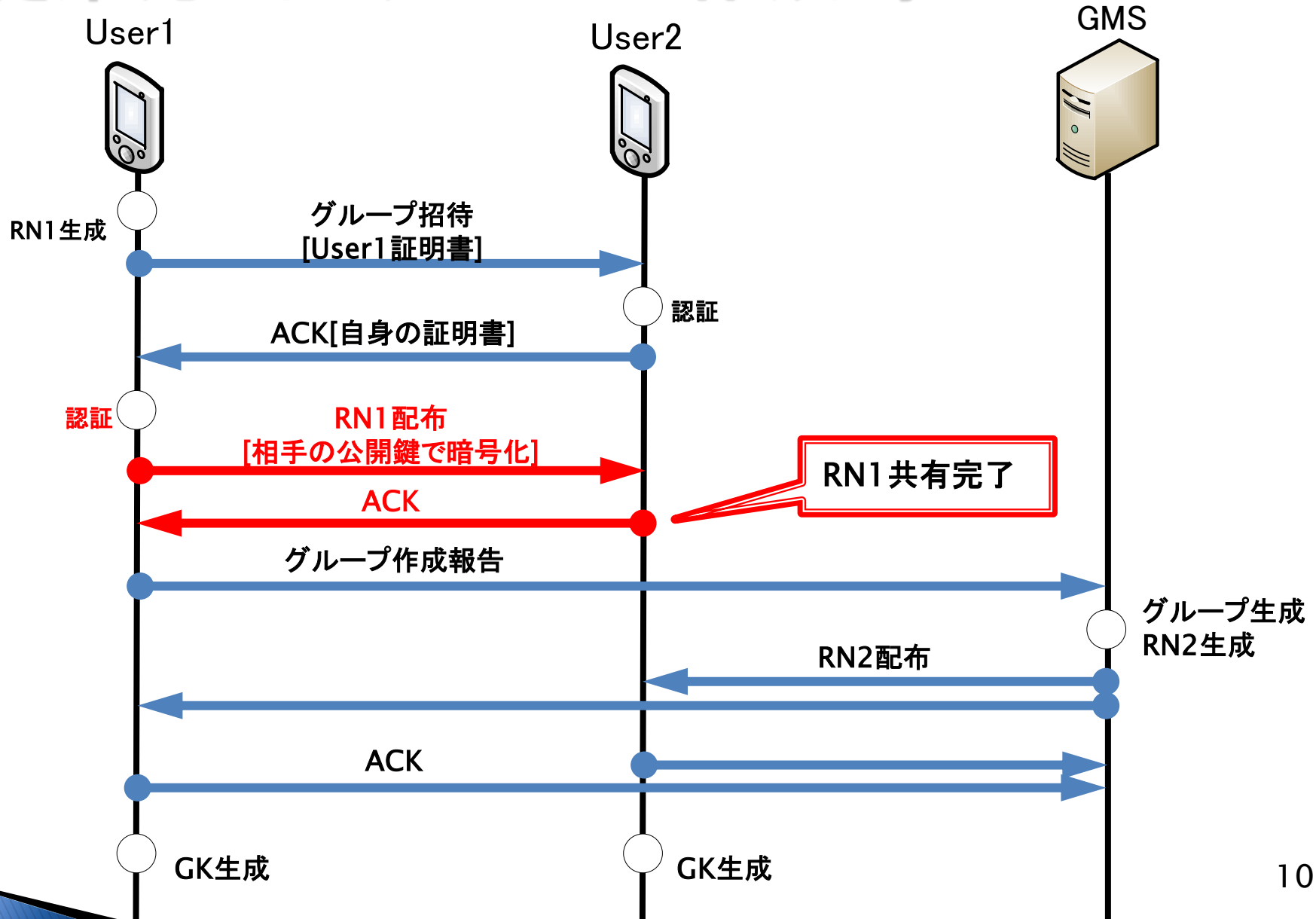
提案方式 –グループ作成時–



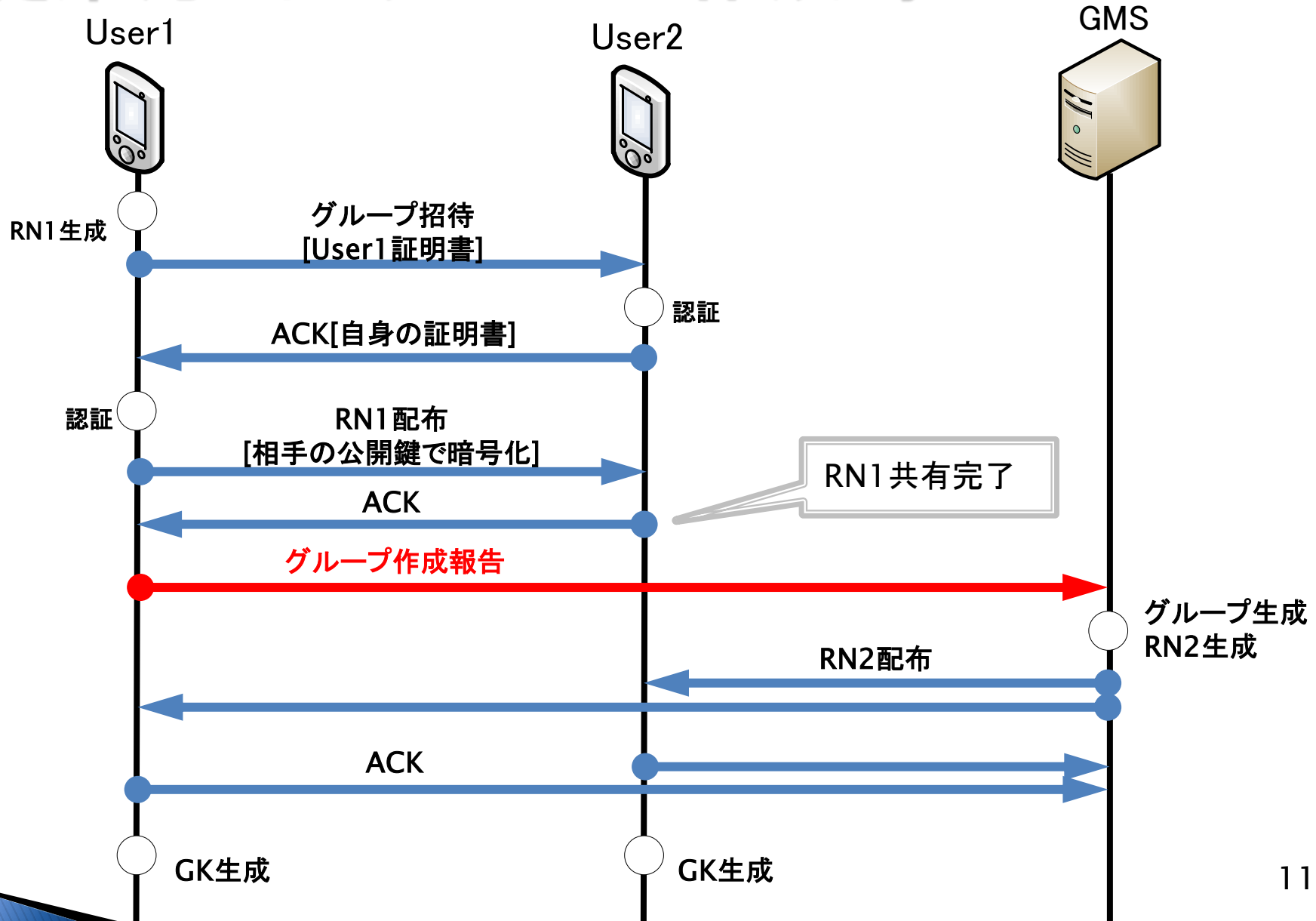
提案方式 –グループ作成時–



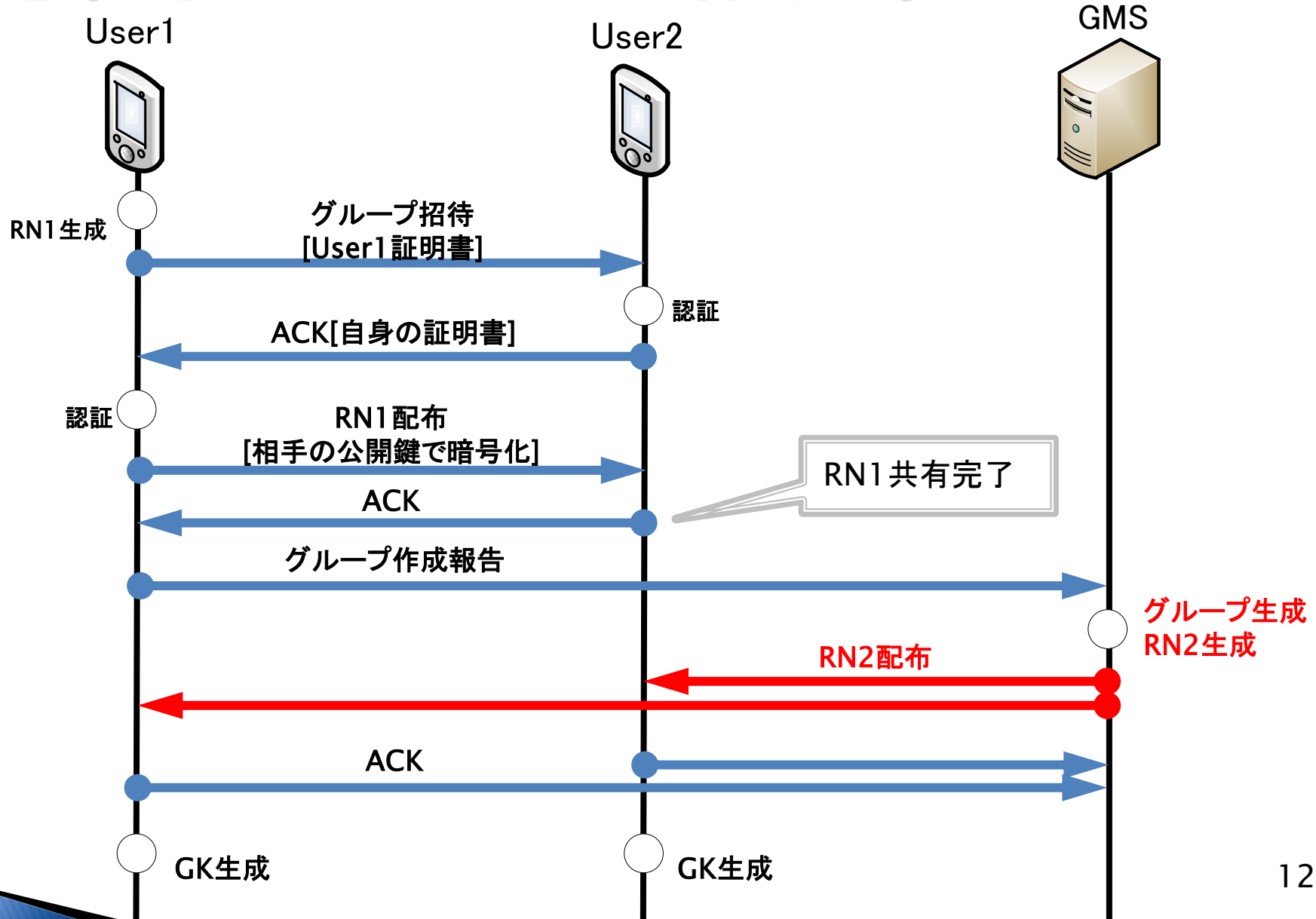
提案方式 –グループ作成時–



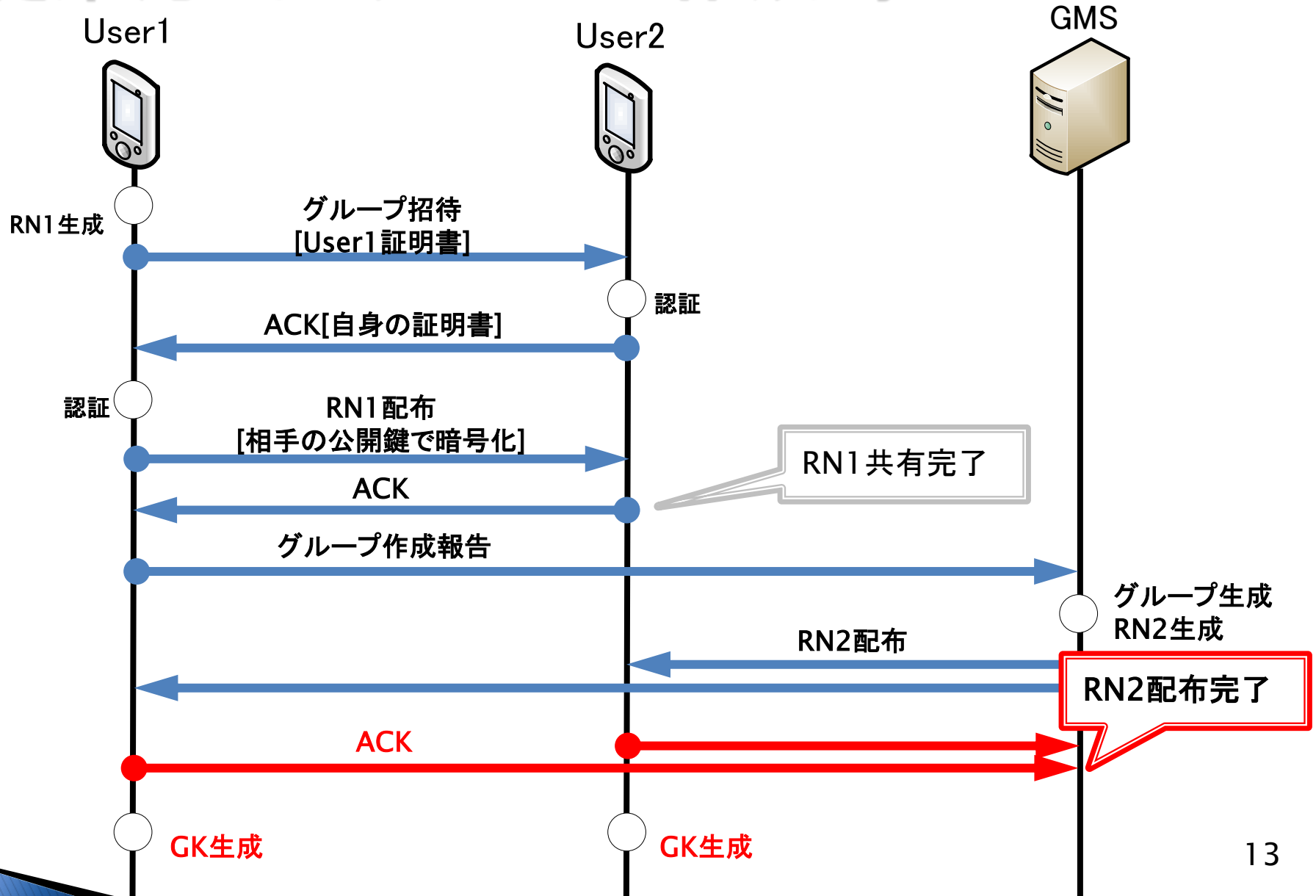
提案方式 –グループ作成時–



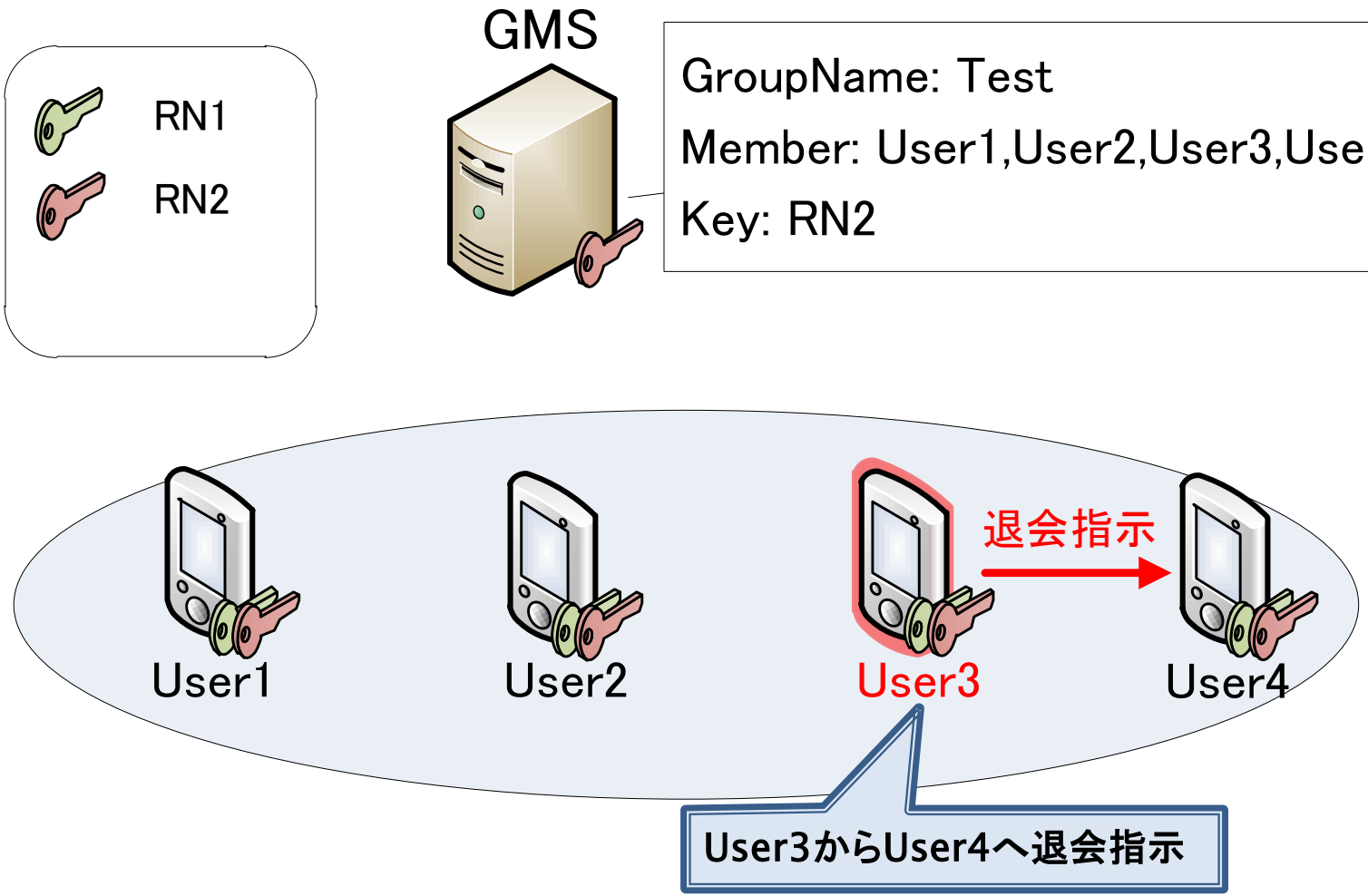
提案方式 –グループ作成時–



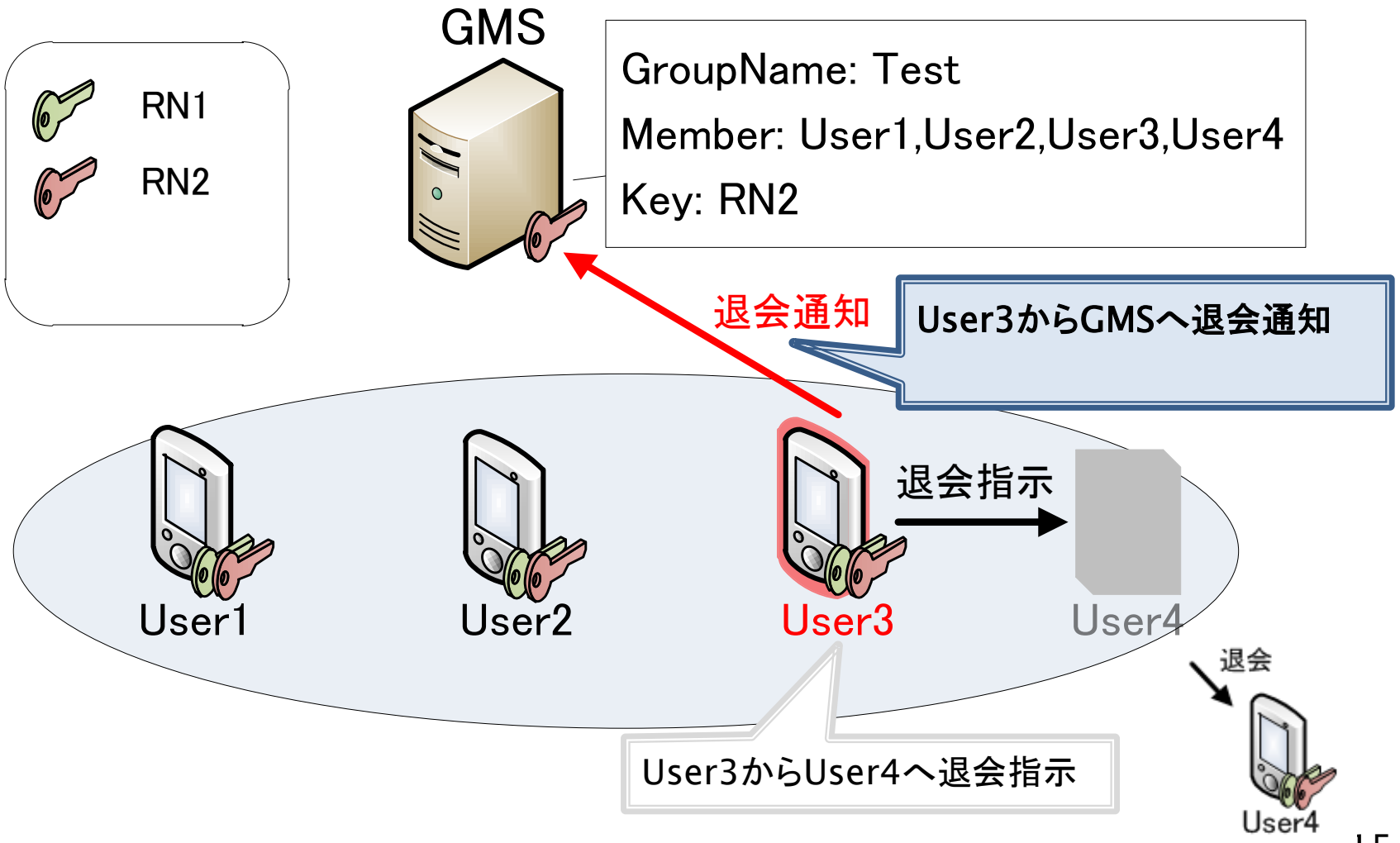
提案方式 –グループ作成時–



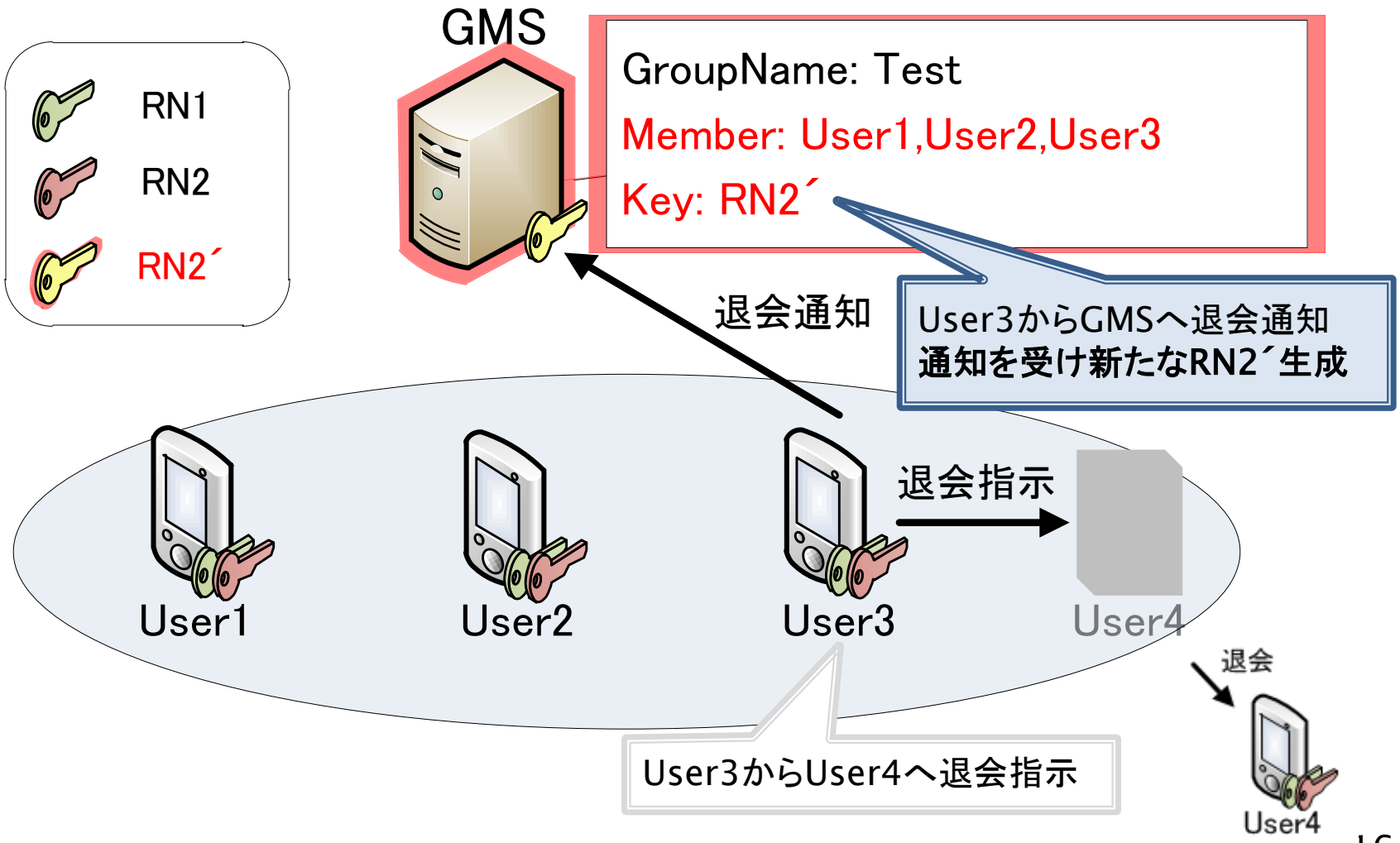
提案方式 –グループ鍵更新処理–



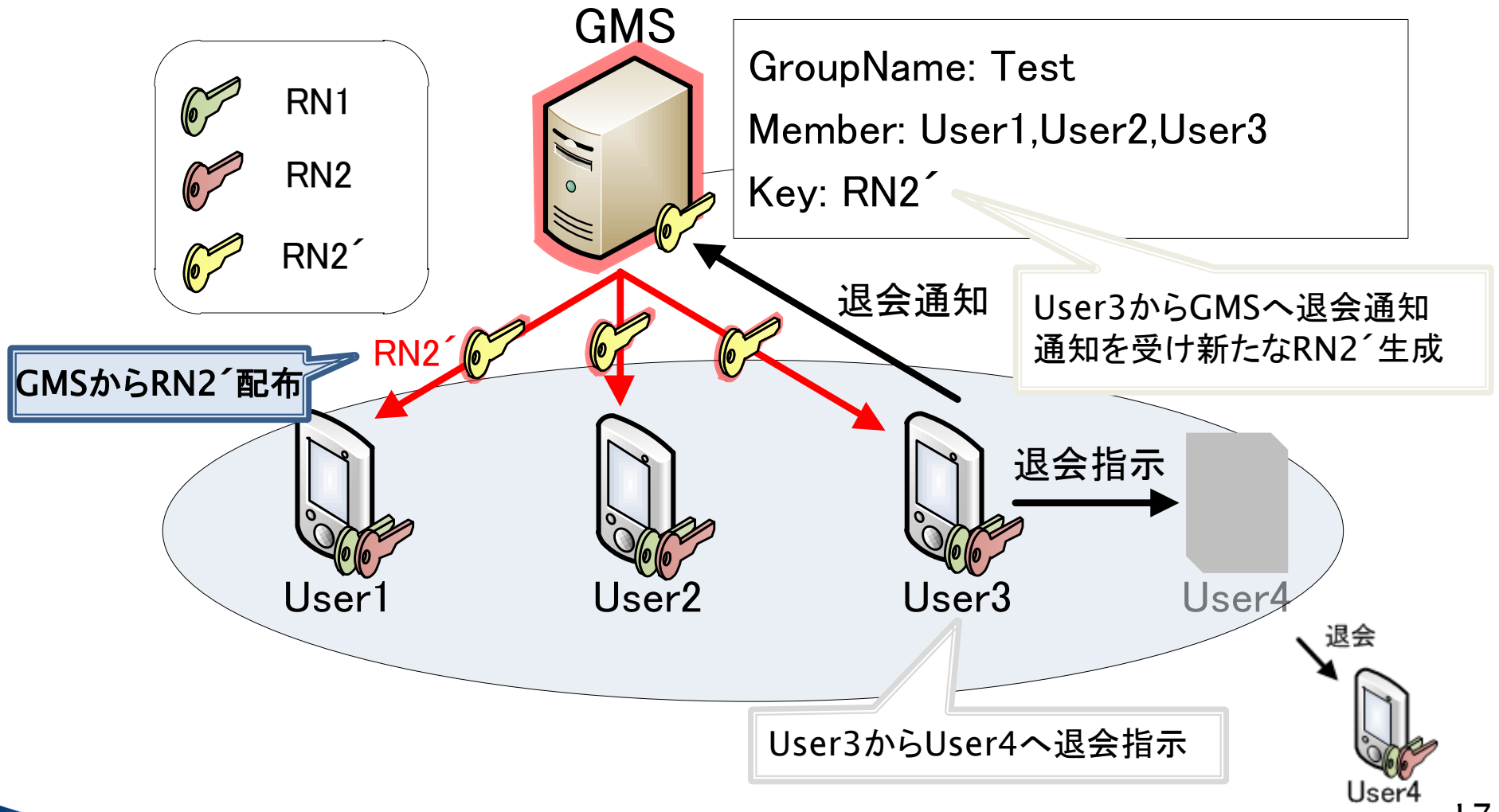
提案方式 –グループ鍵更新処理–



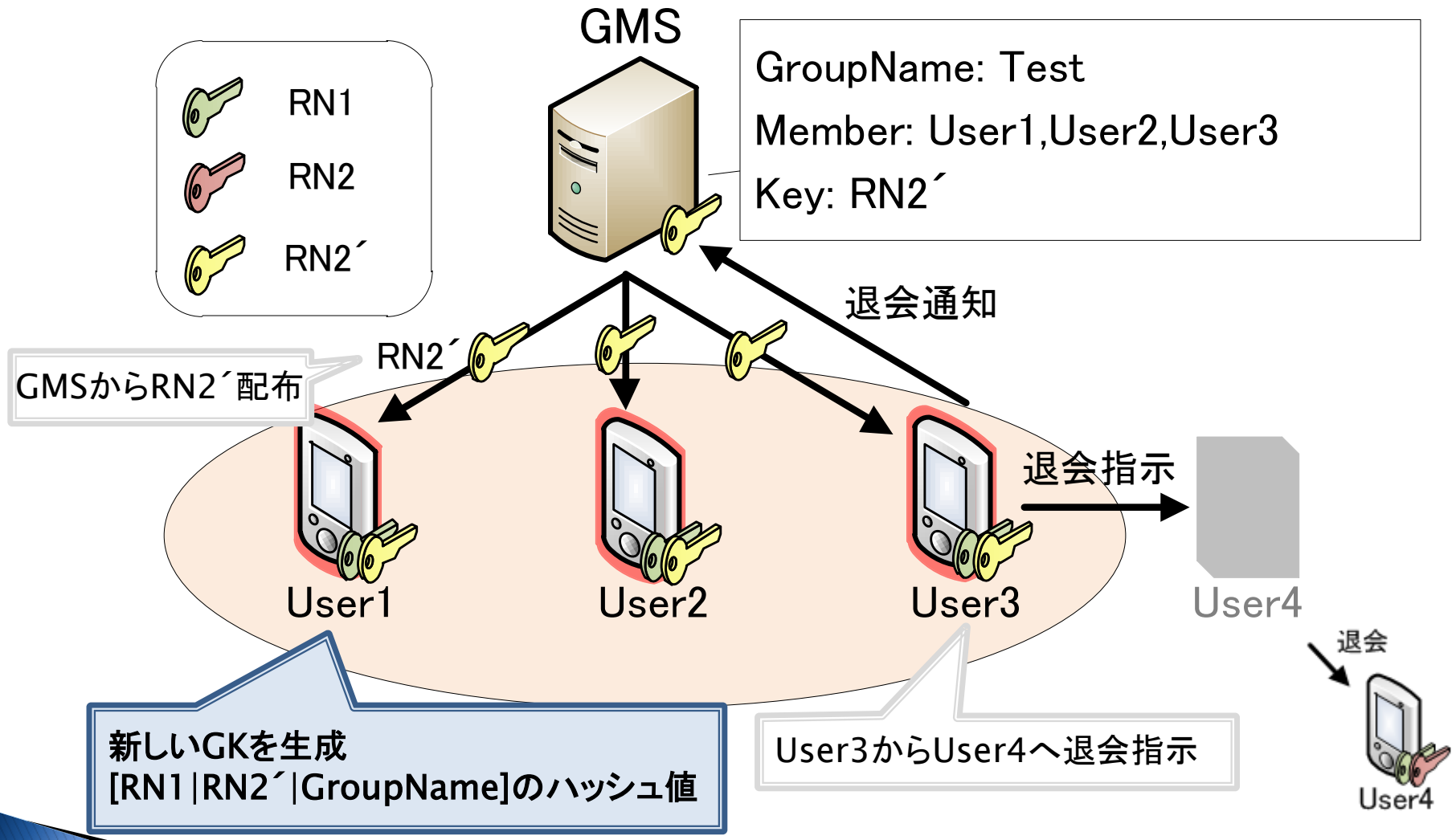
提案方式 –グループ鍵更新処理–



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
- (4)グループ通信を行える

(1),(2)・・・EFFによるチャットアプリケーションのセキュリティ評価項目

(3),(4)・・・独自に追加した評価項目

	項目(1)	項目(2)	項目(3)	項目(4)
LINE	○	×	×	○
GSAKMP	○	×	○	○
ChatSecure※1	○	○	–	×
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
    - 公開鍵証明書を用いてなりすましを防止
  - グループ鍵更新処理を定義

- 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

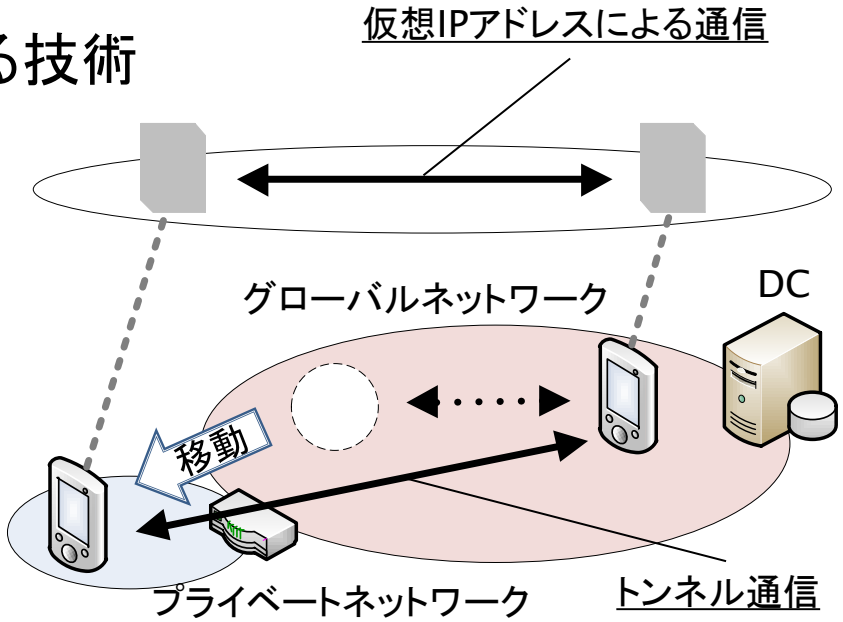
} 新しいRN2を配布できない

- 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

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
    - 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．