Từ hội thoại Kerberos 4 sau:

Đoạn hội thoại sau giúp xác thực người dùng phân tán nhưng chưa giúp cho C xác thực TGS và V

* **Một lần mỗi phiên người dùng đăng nhập**
  1. C → AS: *IDc* ║ *IDtgs*
  2. AS → C: E(*Kc*, *Thẻtgs*)
* **Một lần với mỗi kiểu dịch vụ**

1. C → TGS: *IDc* ║ *IDv* ║ *Thẻtgs*
2. TGS → C: *Thẻv*

* **Một lần với mỗi phiên dịch vụ**

1. C → V: *IDc* ║ *Thẻv*

*Thẻtgs* = E(*Ktgs*, [*IDc* ║ *ADc* ║ *IDtgs* ║ *TS*1 ║ *Hạn*1])

*Thẻv* = E(*Kv*, [*IDc* ║ *ADc* ║ *IDv* ║ *TS*2 ║ *Hạn*2])

Xây dựng đoạn hội thoại mới giúp C, TGS xác thực được lẫn nhau; C, V xác thực được lẫn nhau

Tuy nhiên, phiên bản mới thỏa mãn các điều kiện sau:

* Server xác thực AS, server cấp thẻ TGS, mỗi người dùng *IDc* và mỗi server dịch vụ V đều có một khóa công khai RSA vừa có chức năng ký vừa có chức năng mã hóa được chứng thực từ trước bởi một cơ quan chứng thực chung CA
* Ngay từ đầu AS đã có chứng thực khóa công khai CA<<*IDc*>> của mỗi người dùng *IDc*, AS đã có chứng thực khóa công khai CA<<TGS>> của TGS, TGS đã có các chứng thực khóa công khai CA<<AS>> của AS và CA<<V>> của mỗi server dịch vụ V, mỗi server dịch vụ V đều có chứng thực khóa công khai CA<<TGS>> của TGS
* Người dùng *IDC* không có mật khẩu *PC* được lưu giữ dưới dạng giá trị băm *Kc* trên server xác thực AS như trong hội thoại trên
* Server xác thực AS không có khóa bí mật chung *Ktgs* với server cấp thẻ TGS như trong hội thoại trên
* Server cấp thẻ TGS không có khóa bí mật chung *Kv* với mỗi server dịch vụ *V* như trong hội thoại trên