

Realm Crossover with SIP-SASL

Rick van Rein
rick+ietf@openfortress.nl

Context: Realm Crossover

- Domains validate their User Identities
- Trust in a domain based on DNSSEC/DANE
- Trust in a user based on a domain's IdP
- End-user controls users, aliases, groups, ...
- Same `user@domain.name` in all protocols

Context: SASL for Realm Crossover

- Works for most protocols – not all: HTTP, SIP
- Flexibility for authentication mechanisms
 - Support for channel binding
 - Support for mutual auth (Kerberos, OPAQUE)
 - Shared credentials – may derive symkeys

Context: Other options

- Digest – password must be shared
- TLS – hop-by-hop rather than end-to-end
- STIR – limited to phone numbers
- Certificates – flexible data, static protocols
- *Possibly fragmenting identity management*

Use case: SIP for Wireguard

- Dynamic VPNs between fresh contacts
 - Mutual Authentication with Realm Crossover
 - Quantum Relief with PSK derivation

```
m=application 1919 udp vnd.wireguard  
a=fmtp:vnd.wireguard pubkey=... pskmth=...
```

Foundation: HTTP-SASL

draft-vanrein-httpauth-sasl

```
WWW-Authenticate: SASL
  realm="members only"
  mech="GS2-KRB5-PLUS SCRAM-SHA-256-PLUS OPAQUE",
  s2s="[xxxxx]"
```

```
Authorization: SASL
  realm="members only"
  mech="SCRAM-SHA-256-PLUS",
  c2s="[n, ,n=user,r=r0pr...q0] ",
  s2s="[xxxxx]"
```

[base64]

Variations: SIP-SASL

draft-vanrein-sipauth-sasl

- Mutually authenticate From: and To:
- End-to-end key derivation where possible
- Channel Binding to SIP transaction + SDP
- Only plaintext-safe SASL mechanisms