

SASL RememberMe 🤪😓

The problem: Re-login and logout

- IMAP re-connect
- Why again? 2FA
- Mail check: Why did it not tell me about my new mail?
I didn't know that I had new mail.
- „It worked yesterday, and now it doesn't work anymore“

You're still you

- Strong authentication during setup: Passkey
- Stay logged in: You're still you
- Explicitly kick out lost devices

Solution: Token

- Proves that you're still the same
- More secure than passwords (status quo): Can be revoked etc.
- Device-specific: Can be tracked
- Generic: Independent from original authentication method
- → Can upgrade from passwords, OAuth2, Passkey

Opaque token

- OAuth2 refresh token with very long expiry
- OAuth2: App-specific password, auto-generated via API
- Secret token, stored in mail server auth DB
- JWT, signed → Check signature
- Any other signed token → Check signature

→ Allows many different mechanisms

Wire protocol

- SASL PASSKEY succeeded. Response:
OK You're in
{ sasl: „REMEMBERME“, token: „abdea6565abdea6565“ }
- or:
- IMAP command, after successful login:
IMAP Client: „REMEMBERME“
IMAP Server: „abdea6565abdea6565“
- Login: SASL REMEMBERME
SASL Client: REMEMBERME abdea6565abdea6565
SASL Server: OK You're in

Difference to HT

- NOT hashed password
 - That's what allows the different mechanisms
 - With hashing, tied to that one specific mechanism and hashing function
 - HT also useful, for other use cases
- Both specs are valuable