

Registrierung

Desktop
Client

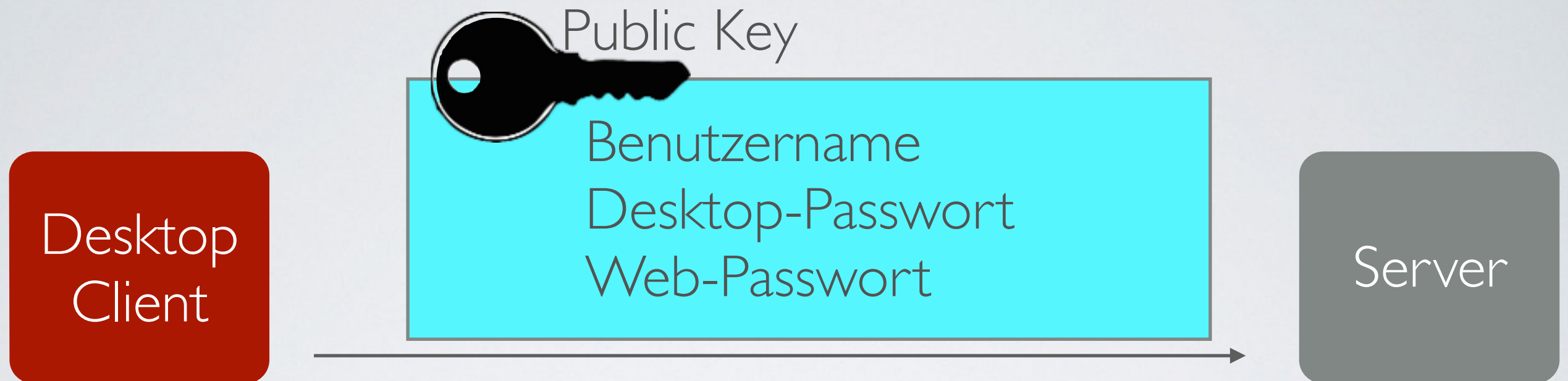
Benutzername

Desktop-Passwort

Web-Passwort

- Client wählt Username und Passwörter

Registrierung



- Benutzername und Passwörter werden mit Public-Key von Server verschlüsselt und an Server gesendet.

Registrierung



- Server entschlüsselt Benutzername und Passwörter
- Server prüft ob Benutzername noch verfügbar ist

Registrierung



Server

Salt

$h(\text{Web-Passwort} + \text{Salt})$

$h(\text{Desktop-Passwort} + \text{Salt})$

- Server generiert Salt
- Server erstellt Salted-Hash von Passwörtern

Registrierung



- Server legt Benutzer in Datenbank an und sendet Salt an Client