

SIT / SRN PROJEKTPRÄSENTATION

Vortragende:

David Seemann

Jochen Schwander

Marcel Math

Phil-Patrick Kwiotek

GLIEDERUNG

- Herangehensweise
- Registrierung
- Login

Registrierungsvorgang

Registrierung

Desktop
Client

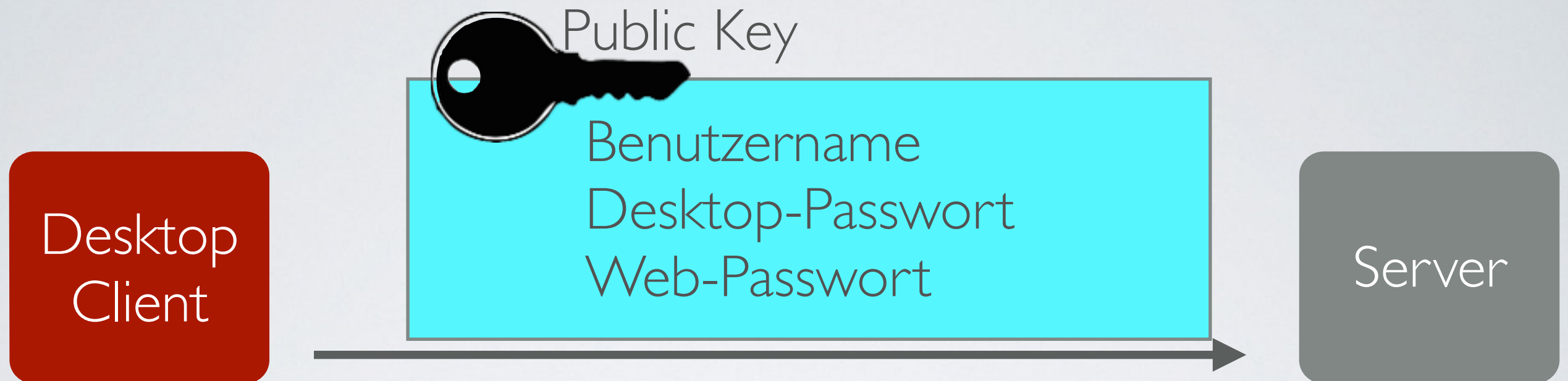
Benutzername

Desktop-Passwort

Web-Passwort

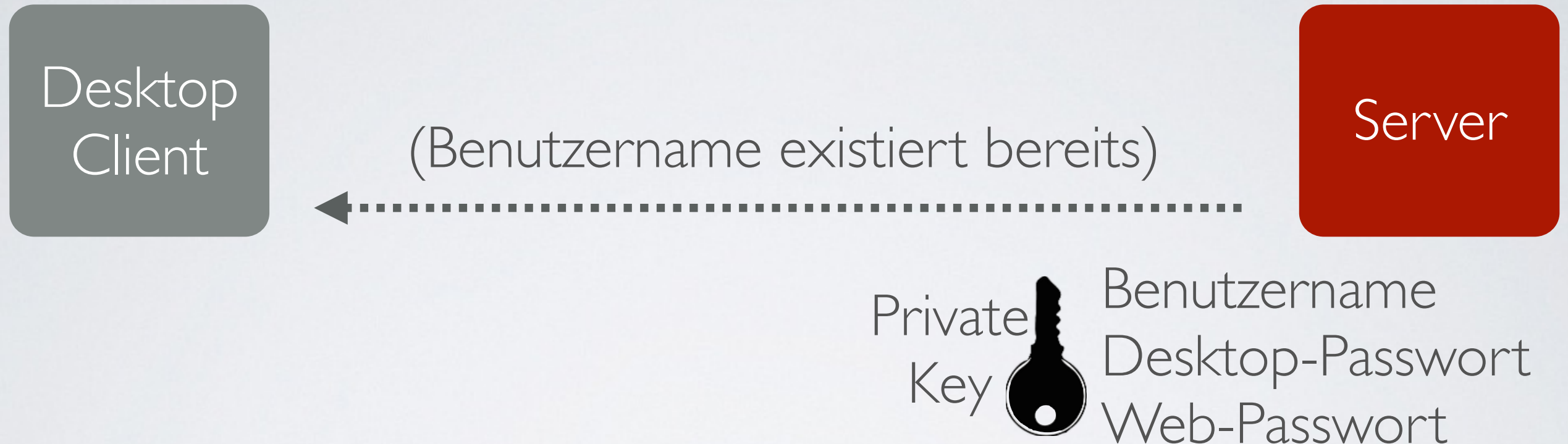
- Client wählt Username und Passwörter

Registrierung



- Desktop Client sendet Passwörter & Benutzername mit Public-Key verschlüsselt an Server

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

Login

Public Key



D-H: g, p, A

Desktop-Passwort

Benutzername

Desktop
Client

Server

a, g, p

$A = g^a \bmod p$


Desktop-Passwort

Benutzername

- Desktop Client beginnt Diffie-Hellman-Schlüsselaustausch
- Desktop Client sendet D-H-Parameter, Desktop-Passwort & Benutzername mit Public-Key verschlüsselt an Server

Registrierung

Server

Private
Key  D-H: g, p, A
Desktop-Password
Benutzername

- Server entschlüsselt D-H-Parameter, Desktop-Password & Benutzername

Registrierung

überprüfe:

$$x \stackrel{?}{=} h(\text{Desktop-Passwort} + \text{Salt})$$

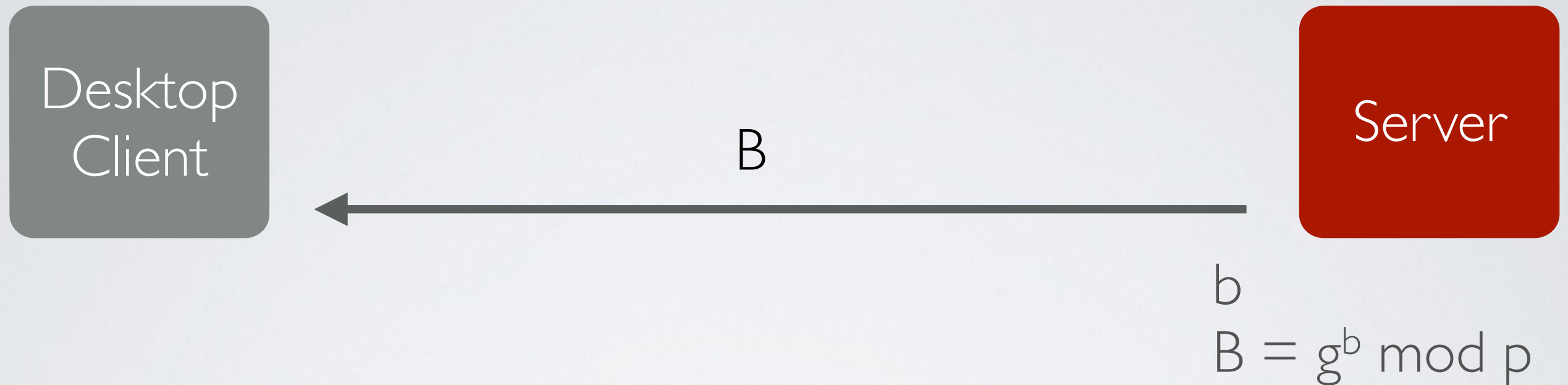
Server

DB

$$\begin{aligned} h(\text{Web-Passwort} + \text{Salt}) &= x \\ \underline{h(\text{Desktop-Passwort} + \text{Salt})} &\quad \text{Salt} \end{aligned}$$

- Server holt sich Benutzerdaten aus der Datenbank und hinterlegt diese für später.
- Server überprüft ob Hash von Desktop-Passwort dem Datenbankeintrag für diesen User übereinstimmt

Login



- Server setzt Diffie-Hellman-Schlüsselaustausch fort und sendet Desktop Client sein B

Login



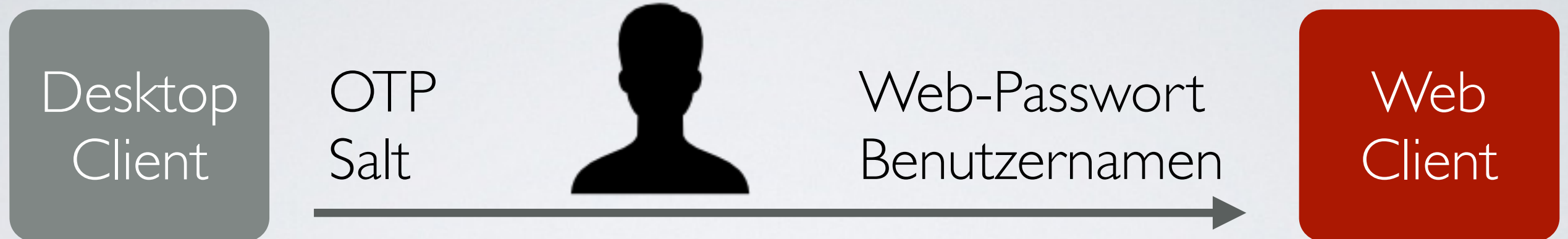
- Server & Desktop Client berechnen K , der geheime Schlüssel
- Server & Desktop Client starten AES-verschlüsselten Stream.
 K dient dabei als geheimer Schlüssel.

Login



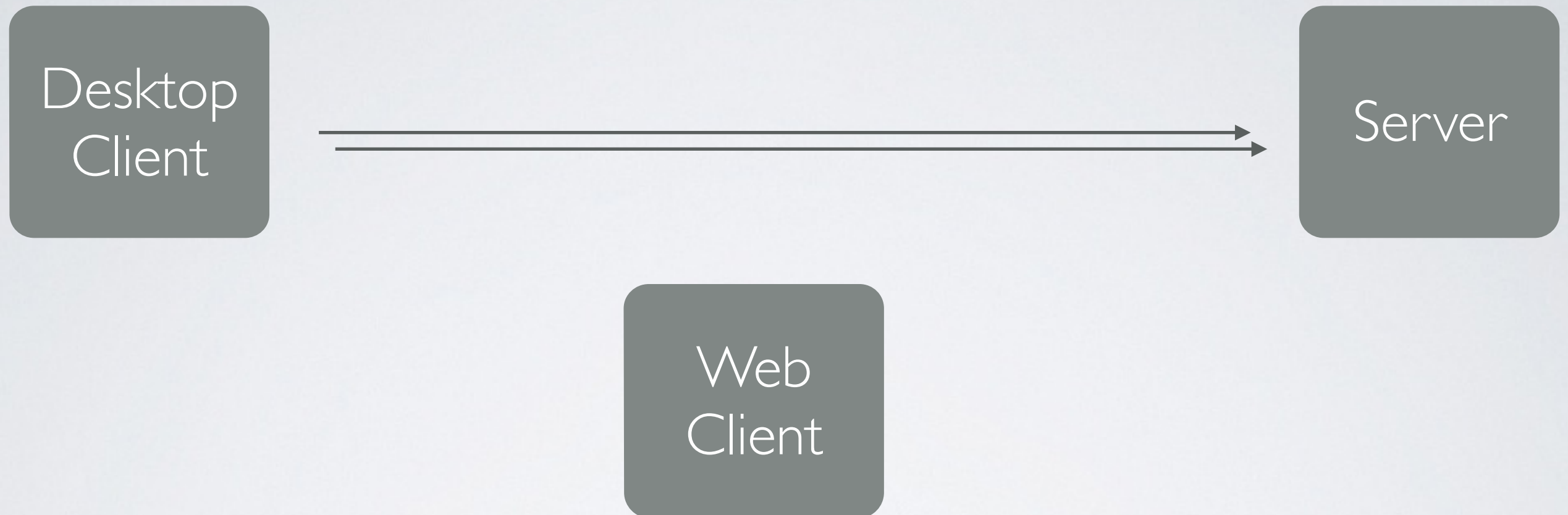
- Server berechnet One Time Password (OTP) und schickt es zusammen mit dem Salt aus der Datenbank an den Desktop Client

Login



- Desktop Client zeigt Benutzer OTP & Salt
- Der Benutzer kopiert OTP & Salt, fügt sie im Web Client ein
- Der Benutzer gibt zusätzlich sein Web-Passwort und seinen Benutzernamen ein

Login



- Server generiert Salt für Passwörter
- Server legt Benutzer in Datenbank an und sendet Salt an Client

Registrierung

