

KonsortSWD 

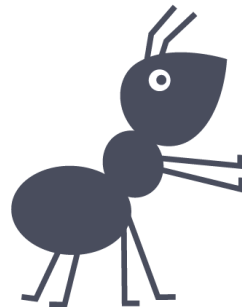
Consortium for the  
Social, Behavioural, Educational  
and Economic Sciences



**RDCnet**

In cooperation with

**nfdi**



3. Workshop RDCnet

# Pilotnetzwerk

14. April 2023

Jan Goebel, Kenny Pedrique, Neil Murray

Kontakt: [nmurray@diw.de](mailto:nmurray@diw.de)

# Agenda Workshop



Status quo und Ziel des Pilotnetzwerk



Vorgehen Verbindungsaufbau (Beispiel IZA-SOEP)



Diskussion: Multi-Faktor Authentifizierung



Diskussion: Zugangsrestriktion Netzwerk



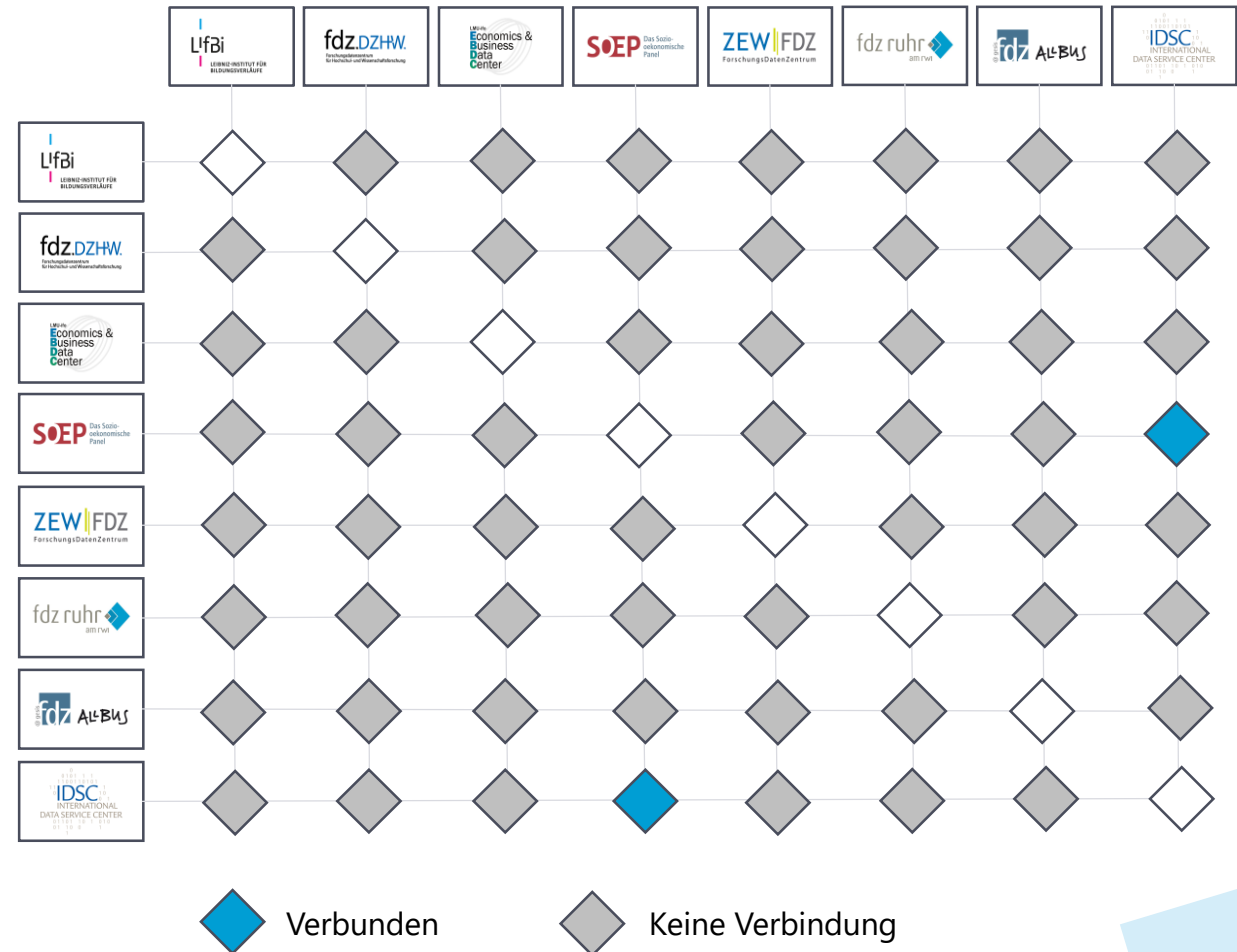
Buchungsplattform: Live Demo

# Pilotnetzwerk: Ziel und Status quo

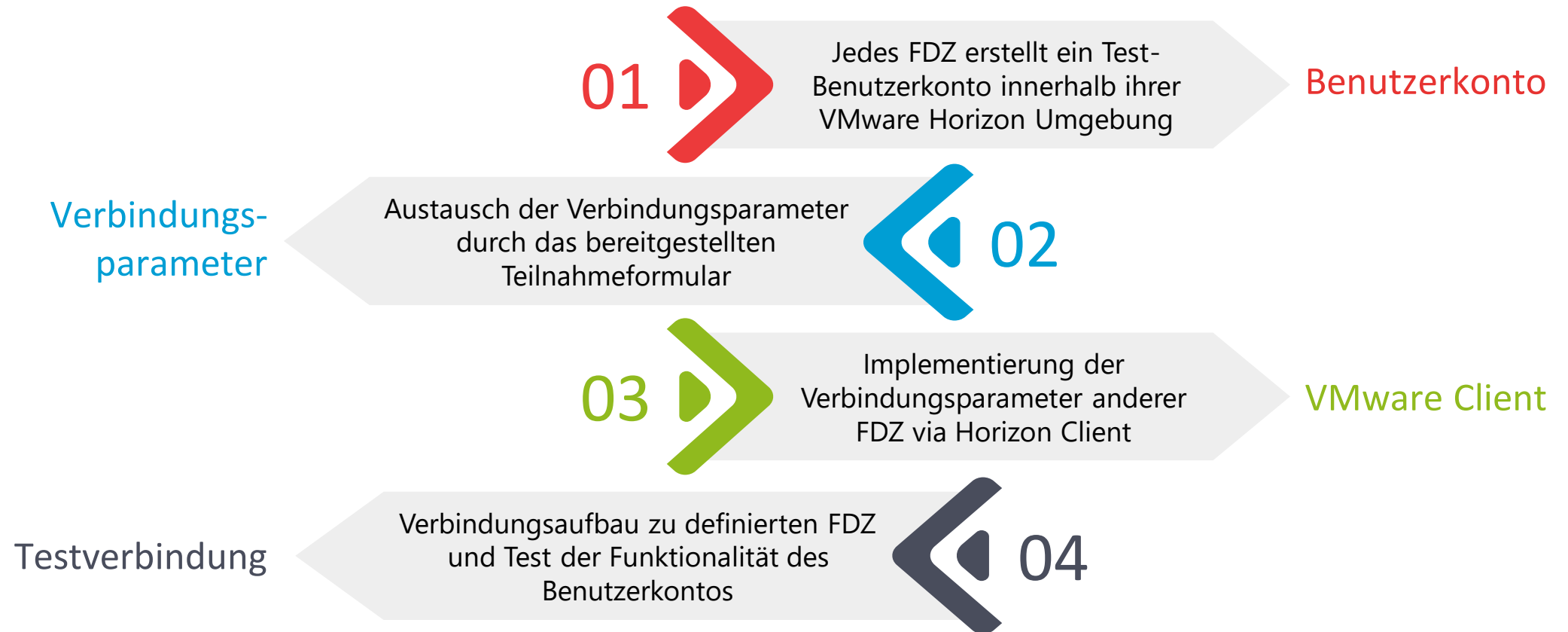
## Ziel

Multilateraler Verbindungsaufbau zwischen allen FDZ via VMware

- I. **Verbindung von:** Thin Client/Endgerät via VMware Client
- II. **Verbindung zu:** Test-Benutzerkonto via FDZ Horizon Connection Server



# Vorgehen Verbindungsaufbau:



# Vorgehen Verbindungsaufbau:

01



Jedes FDZ erstellt ein Test-Benutzerkonto innerhalb ihrer VMware Horizon Umgebung



„Ausstattung“ nach eigenem Ermessen



Restriktion: keine sensiblen Daten, kein Zugang auf interne Ressourcen





Priorität: gleichbleibender Connection Server



Keine 2FA notwendig

# Vorgehen Verbindungsaufbau:

KonsortSWD   
 Konsortium für die  
 Sozial-, Verhaltens-, Bildungs- und  
 Wirtschaftswissenschaften



**RDCnet**

Pilotnetzwerk

## Teilnahmeformular für Forschungsdatenzentren

### 1. Angaben zum FDZ

**Forschungsdatenzentrum:**

**Anschrift:**

PLZ:  Ort:

**Öffnungszeiten:** Wochentage:  Uhrzeit:  bis

Buchbare Zeitslots<sup>1</sup>:

**Ansprechpartner**

Organisation & Leitung:

Technik & IT:

Buchung & Terminanfragen<sup>2</sup>:

### 2. Verbindungsparameter VMware Horizon

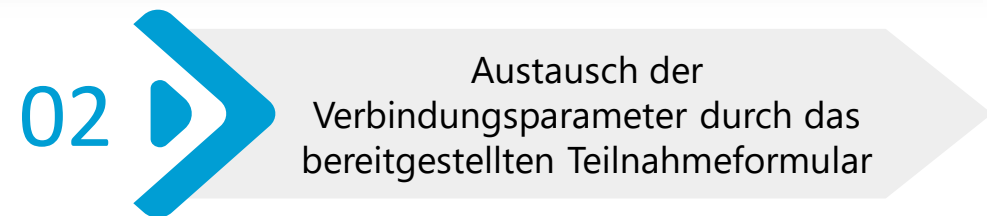
Host-Name oder IP

Horizon Connection Server:

Domäne (Active Directory)<sup>3</sup>:

Freizugebende Ports<sup>4</sup>:

Port	Beschreibung
<input type="text" value="TCP/443"/>	<input type="text" value="HTTPS"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>



# Vorgehen Verbindungsaufbau:

### 3. Testbenutzerkonto

**Wichtig: Auf dem Testbenutzerkonto keine sensiblen Daten bereitstellen sowie den Zugang zu internen Ressourcen verbieten.**

Benutzername:

Passwort:

Desktop-Pool:

Ist eine 2-Faktor-Authentifizierung für das Testbenutzerkonto implementiert?<sup>5</sup>

Ja  Nein

Wenn ja, welche Art?

TAN-Liste

OTP

Andere  und zwar:

Ist ein Skript zum Test der Performanz/Funktionalität hinterlegt?

Ja  Nein

Wenn ja, bitte Anleitung zur Ausführung des Skripts angeben:

Beispiel: Das Skript "test.do" ist in C:\Users\mmustermann abgelegt. Das Skript muss lediglich mit Stata17 gestartet und als Ganzes ausgeführt werden. Falls das Skript länger als 1 Minute zur Ausführung benötigt, bitten wir um Meldung.

### Sonstige Informationen

Bitte geben Sie hier ggf. notwendige Ergänzungen an. Dies kann z.B. die Nutzung der Multifaktor-Authentifizierung im späteren Produktivbetrieb betreffen, die nicht durch den Nutzenden, sondern durch das FDZ-Personal des GWAP-stellenden FDZ durchgeführt werden muss.

02



Austausch der  
Verbindungsparameter durch das  
bereitgestellte Teilnahmeformular

# Vorgehen Verbindungsaufbau:

## 03



Implementierung der  
Verbindungsparameter anderer  
FDZ via Horizon Client



Optimal: Implementierung am Endgerät das für das RDCnet vorgesehen ist

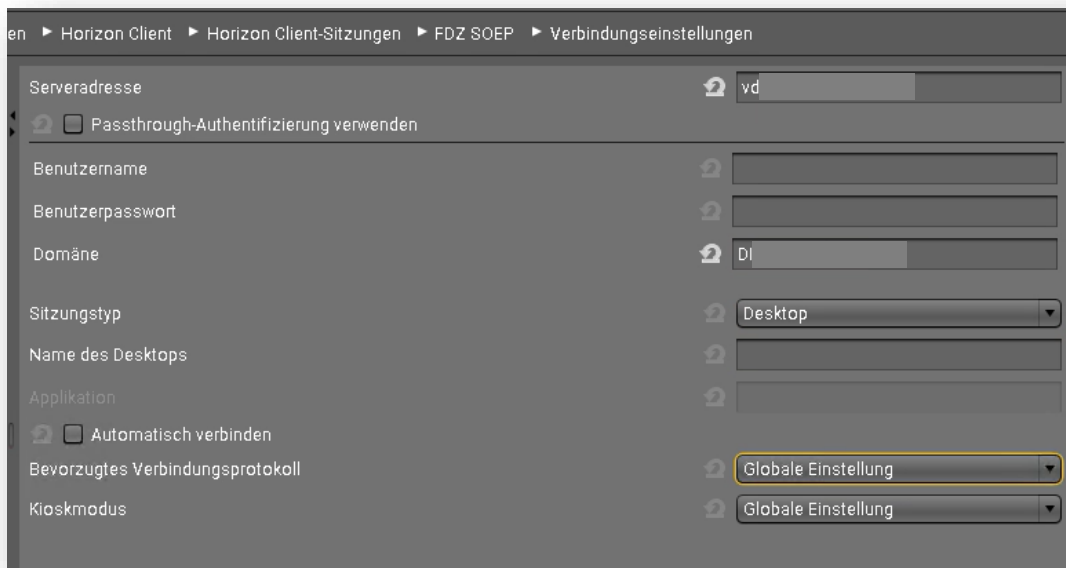


Abb.: Konfiguration Horizon Sitzung an IGEL Thin-Client

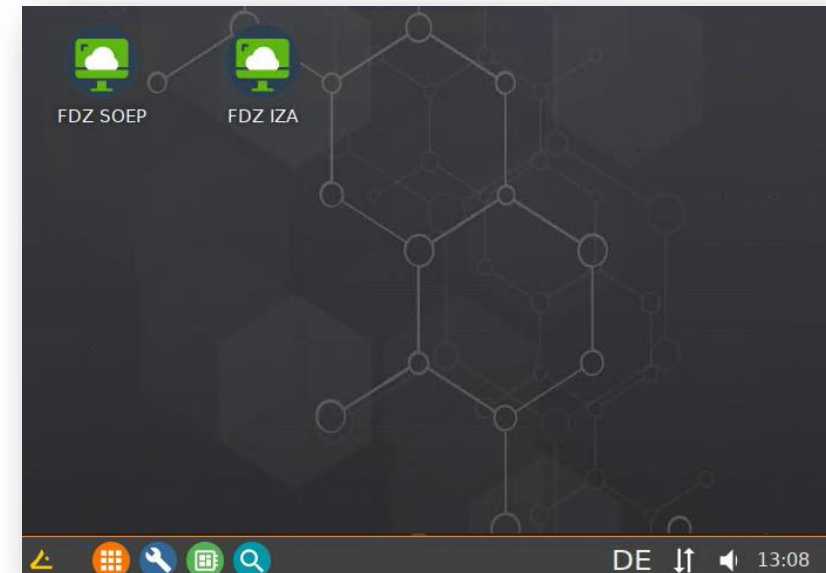



Abb.: Desktop IGEL Thin-Client



# Vorgehen Verbindungsaufbau:

04  Verbindungsaufbau zu definierten FDZ und Test der Funktionalität des Benutzerkontos

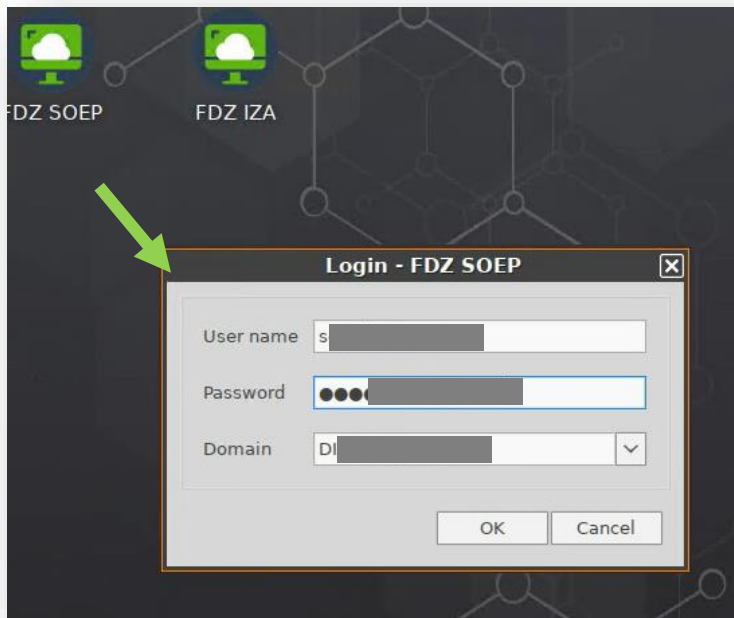


Abb.: Verbinden mit Test-Benutzer Daten

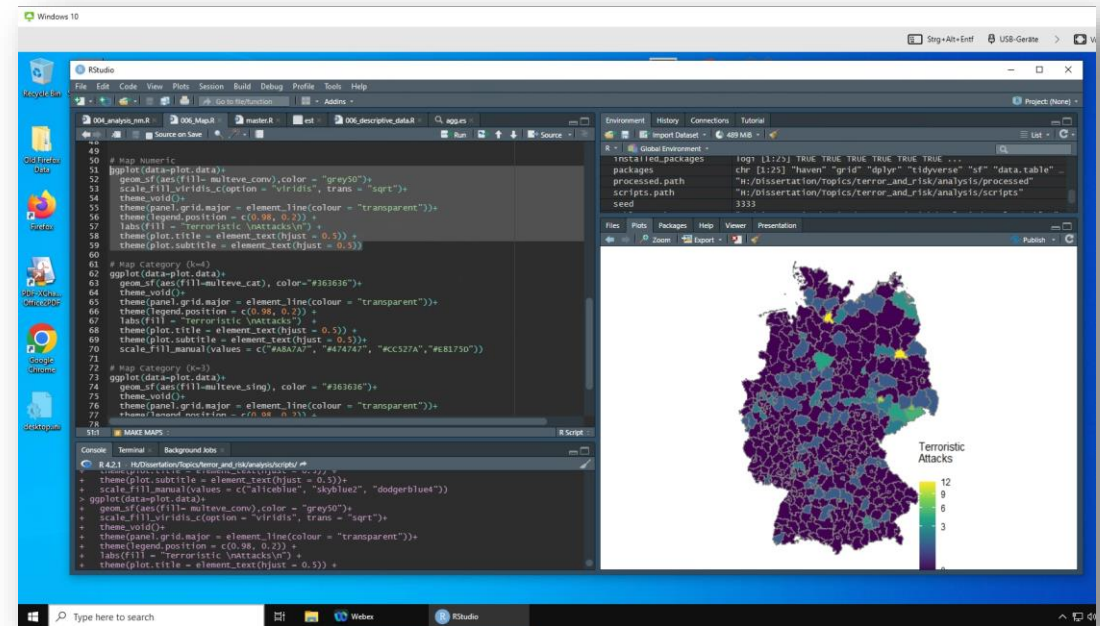
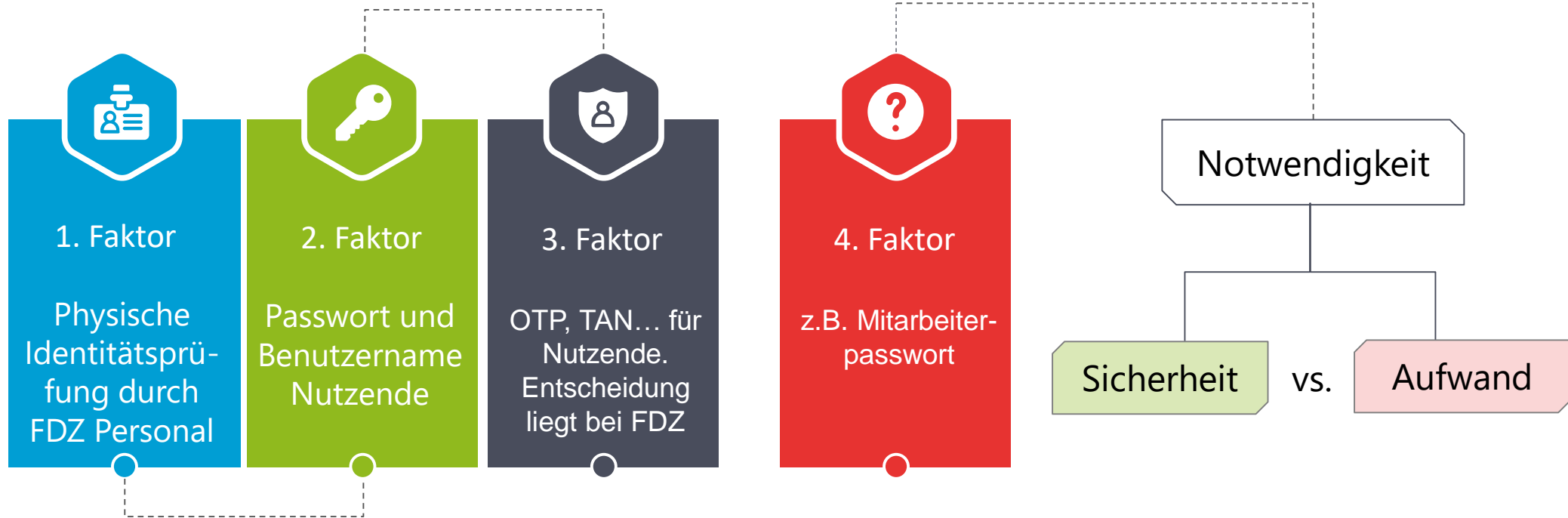
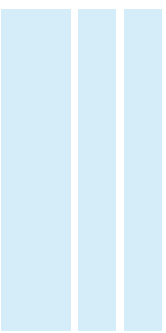
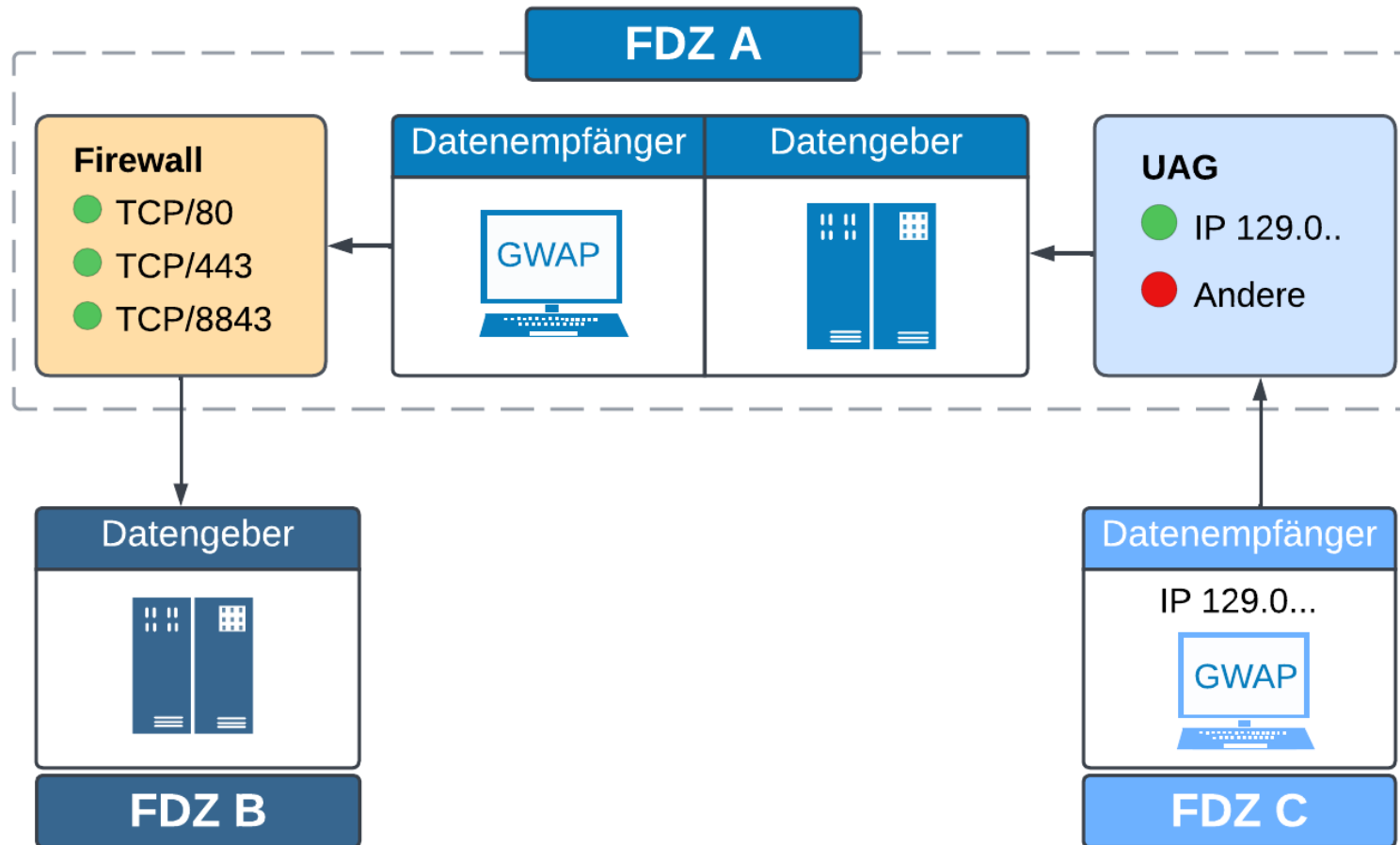


Abb.: Virtual Desktop für Nutzende

# Diskussion: Multi-Faktor-Authentifizierung



# Diskussion: Netzwerkrestriktion



# Diskussion: Netzwerkrestriktion

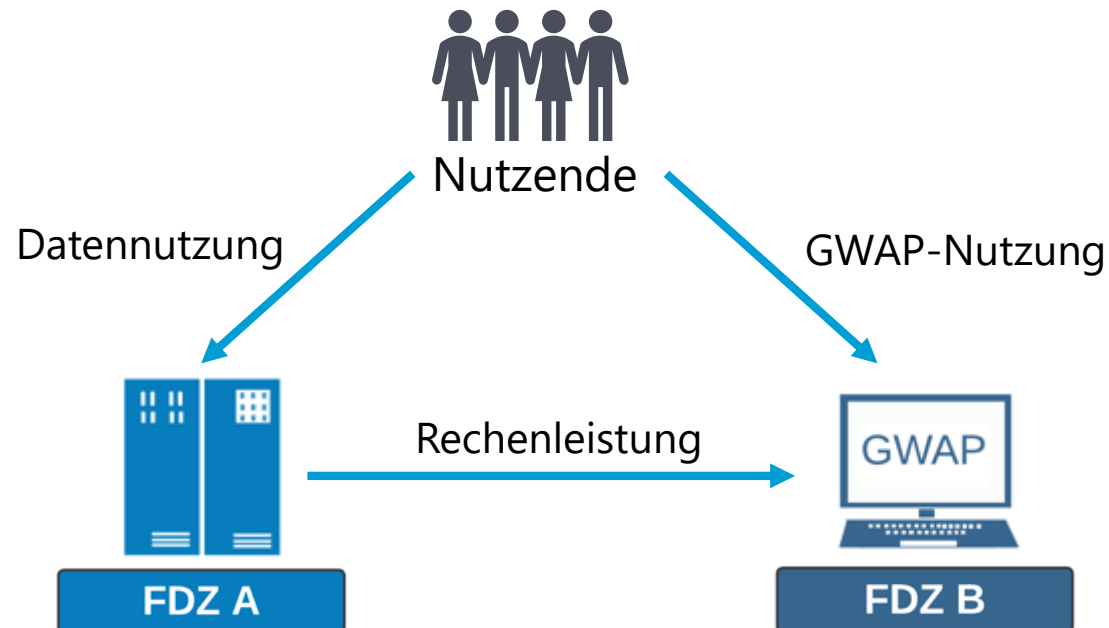
- 1. Ausgehende Verbindungen:** Notwendige Ports der Connection Server/UAG der Partner-FDZ müssen innerhalb der eigenen Firewall freigegeben werden.
- 2. Eingehende Verbindung:** Statische IP-Adressen von VMware Clients (z.B. Thin Clients) der Partner-FDZ müssen in einer IP-Whitelist der UAG aufgenommen werden.
- 3. Alternative: Client-Zertifikate**
  - Zusätzliche Sicherheit
  - Größerer Aufwand durch Erstellung, Austausch und Einbindung der Zertifikate.



# Gemeinsames Buchungssystem

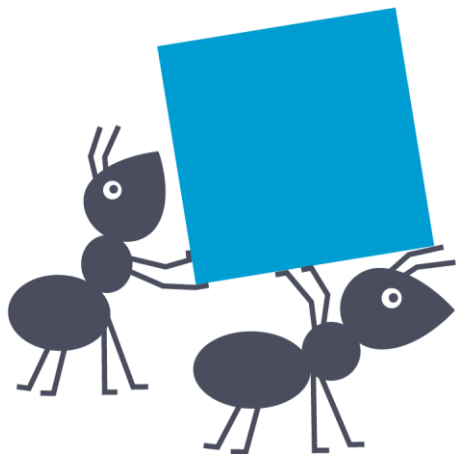
Buchungssystem mit **zwei Kriterien**:

1. Verfügbarkeit des GWAP
2. Verfügbarkeit virtueller Maschinen/Rechenleistung



RDCnet Buchungssystem

# Danke für eure Aufmerksamkeit



Gute  
Zusammenarbeit  
startet im  
Kleinen

In cooperation with



KonsortSWD wird Rahmen der NFDI durch die Deutsche  
Forschungsgemeinschaft (DFG) gefördert - Projektnummer: **442494171**