

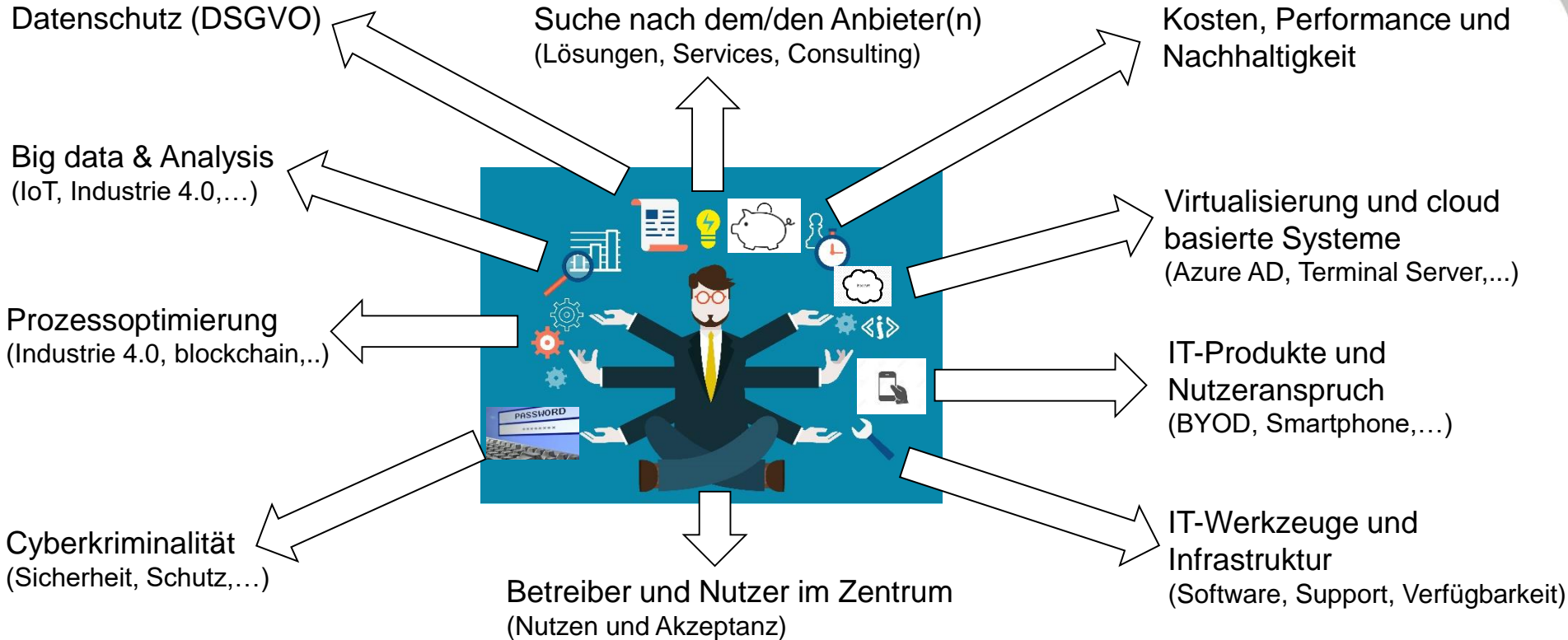


PalmSecure™

Ihre Hand ist Ihre Lösung

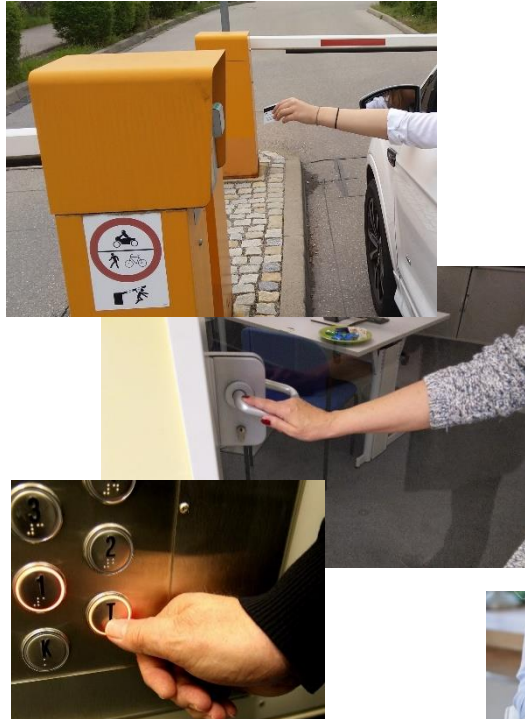
Nicole Krebs,  
Business Development

# Digitalisierung – Quo vadis?



# ...und täglich grüßt das Murmeltier...

## Zutritt



## Zugriff/Zugang



## Zeiterfassung



## Zahlungsmittel



## Zusätzliche Lösungen



Digitale  
Signatur,  
Mail  
Verschlüsselung,...

Frage:



Was haben alle diese  
Tätigkeiten gemeinsam?

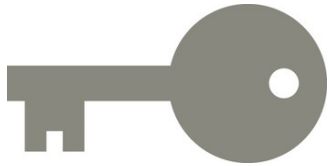


Jeder von uns führt diese Tätigkeiten  
zigfach pro Tag durch

Einige davon sind bekanntermaßen  
große Sicherheitsrisiken in der heutigen  
IT bzw. dem Unternehmensumfeld

Alle werden „manuell“ mit der Hand  
durchgeführt

Für fast sämtliche dieser Tätigkeiten etablieren Unternehmen zur Absicherung Kombinationen verschiedenster Mechanismen



RFID Karten, Token, Badges, Zugangscodes / Passworte,...

Sind diese Methoden wirklich "sicher"? NEIN, denn...



sie sind mehr oder weniger leicht korrumpierbar



sie sind untereinander nicht oder nur mit enormem Aufwand kompatibel



sie werden vergessen/verloren oder bewusst unterwandert



im Falle eines Mißbrauchs kann keine zweifelsfreie Identifikation der Person vorgenommen werden, welche die Aktion tatsächlich ausgeführt hat

# Was bietet Ihnen Fujitsu PalmSecure™?



- Hochsichere Authentifizierung über die innere biometrische Modalität der individuell spezifischen Handvenenmuster



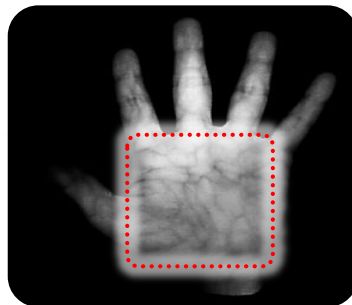
## 1 Maximale Sicherheit

- Versteckt unter der Haut
- Einzigartig (auch bei Zwillingen)
- Unveränderliches Merkmal



## 2 Maximale Präzision

- Komplexität der Handvenenmuster
- Handvenen sind unempfindlich gegenüber externen Einflüssen



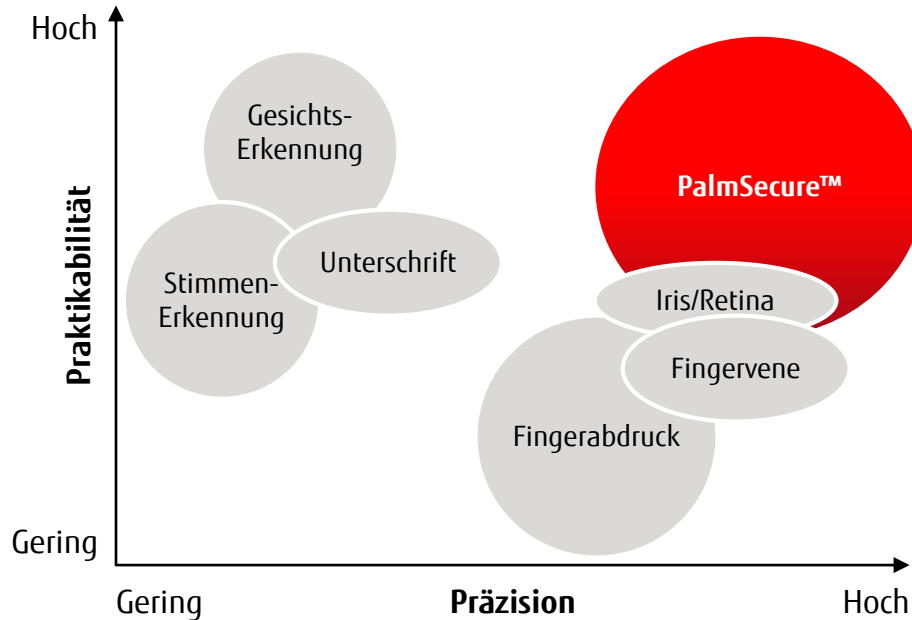
## 3 Maximale Benutzerakzeptanz

- Hygienische, kontaktfreie Nutzung
- Einfache, intuitive Handhabung





# Vergleich der Präzision von Authentifizierungen



## Vergleich von False Acceptance Rate (FAR) & False Rejection Rate (FRR)

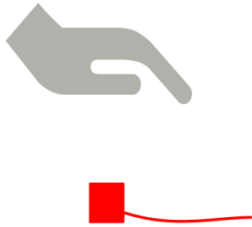
Art der Authentifizierung	FAR (%) =	FRR (%) =
Gesichtserkennung	~ 1.3	~ 2.6
Stimmenerkennung	~ 0.01	~ 0.3
Fingerabdruck	~ 0.001	~ 0.1
Fingervene	~ 0.0001	~ 0.01
Iris/Retina	~ 0.0001	~ 0.01
<b>PalmSecure™</b>	<b>&lt; 0.00001</b>	~ 0.01



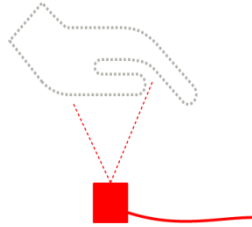
**PalmSecure™ ist die Technologie mit der höchsten Präzision und Praktikabilität.**

# Wie funktioniert PalmSecure™

Hand über dem Sensor positionieren



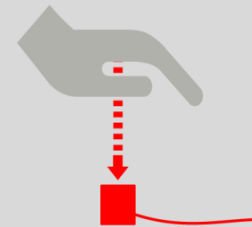
Fokussierung und Lebenderkennung



Hand wird mittels Nahinfrarotlicht gescannt



Handvenenmuster wird aufgezeichnet



Sichere Speicherung des Hashwerts



h3 9d j1 9f 0q a2 09 s0

Konvertierung des biometrischen Musters, zweite AES Verschlüsselung



1011010010101000

Übertragung an PC oder Controller



101011010010101000

Übertragung an PC oder Controller

Erste Verschlüsselung mittels AES



1010100  
1010100010101  
01101001010100  
000101010010101  
110101000101010  
10101000101010  
01101000101010  
0110100101010  
101101



## Fujitsu hat als einziges biometrisch basiertes Authentifizierungsverfahren eine Zertifizierung des BSI

- End-to-end security nach common criteria EAL 2 BSI-DSZ-CC-0511
- <https://www.commoncriteriaportal.org/files/epfiles/0511b.pdf>

## Einordnung der Technologie außerhalb Deutschlands

- Reference recommendation of CNIL (Frankreich) and CESG (Ver. Königreich)
- Empfohlene biometrische Technologie für Banken durch Bankenverbände (SRC, BDB, DSGVO)
- HIPAA konform – Empfohlene Lösung zur Patientenidentifikation in den USA und der Türkei

## Konformität mit GDPR/DSGVO

- Fujitsu ordnet biometrisches Informationsmaterial vor allem auch unter Berücksichtigung des Datenschutz korrekt ein und unterstützt Kunden und Partner bei der Einhaltung rechtlicher Vorgaben

## PalmSecure™ USB Hand Guide Kit und USB Maus

- 1:1 Verifikation und 1:n Identifikation
- Externe Hardware zur Funktion mit Geräten ohne verbauten Sensor
- Verfügbar als F-Pro (seit 2017) oder M1E
- Für Fujitsu Geräte oder 3<sup>rd</sup> Party Hardware



## PalmSecure™ U-Guide

- Zur Verwendung in Verbindung mit dem OEM Sensor
- Hauptnutzen ist zur Registrierung von Benutzern (Enrollment Station)



## PalmSecure™ embedded sensor

- Nur 1:1 Verifikation
- Integration NUR in Fujitsu Hardware
- Integration in Fujitsu Tastatur
- Nutzung für Applikationen bzw. Endgeräte Sicherung



# PalmSecure™

PalmSecure und das Murmeltier

# Einsatzgebiete zur Nutzung

Zutrittsystem

Integration an IoT  
Umfelder

Bargeldloses  
Zahlungssystem

Login an Windows  
session „fat client“

Zeiterfassung

Sicheres Drucken  
(„follow me print“)

Login an terminal server  
sessions „thin client“

Integration in  
blockchain

„single sign on“



# Umfassende und kombinierbare Lösungsszenarien

## Eigenschaften



Einmaliges Enrollment für alle Szenarien



Integration in eigene und 3rd party Umgebung

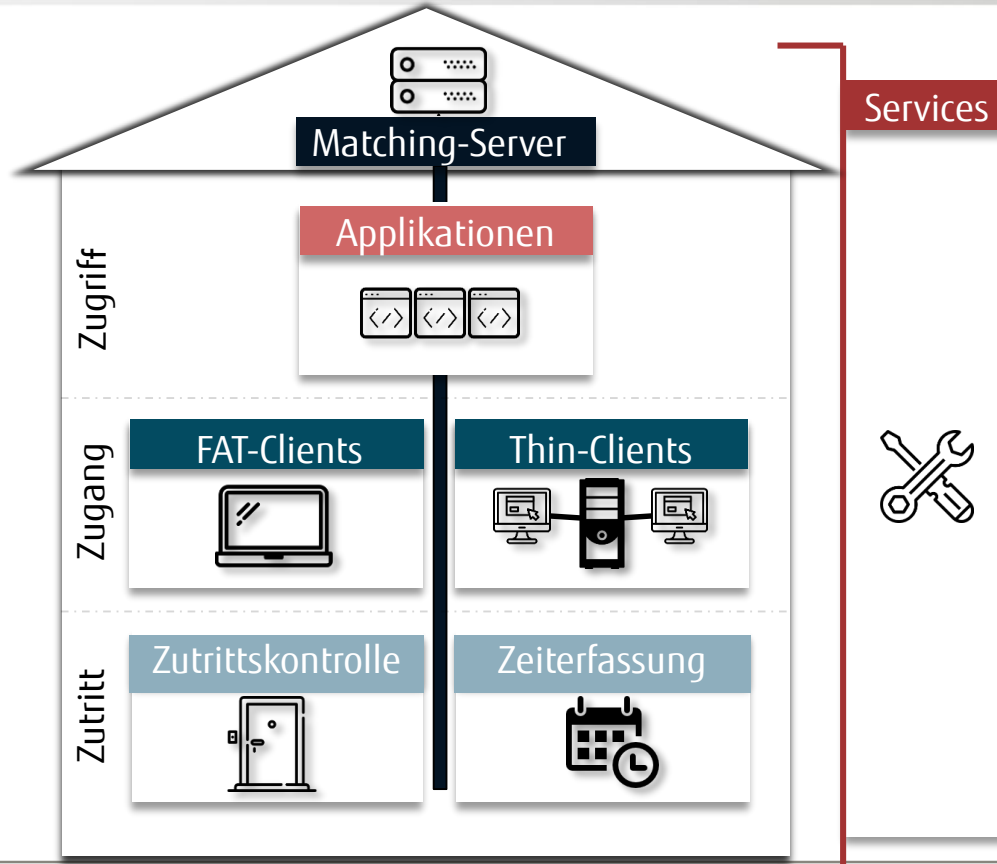


Lauffähig auf:

- Windows
- Ubuntu 16
- IGEL
- eLux



Einfache Integration in bestehende Systeme

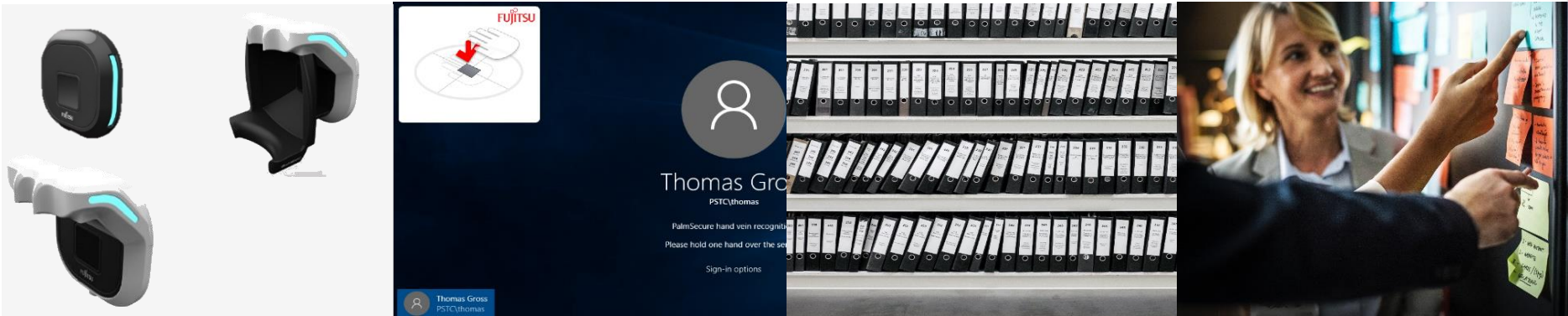


## Dienstleistungen



- Use-Case Untersuchung
- Solution Design
- Consulting auf technischer, fachlicher und organisatorischer Ebene
- Prozessberatung
- Organisationsberatung
- Projektmanagement
- Implementierung
- Konfiguration





## ID Gatekeeper

- Standardisiertes biometrisches Zutrittssystem für Unternehmen jeder Größe.
- Die Integration in existierende Systeme ist konzeptionell vorgesehen und möglich.
- 1:1 Verifikation oder 1:n Identifikation zur Authentifizierung sind möglich.

## ID LoginV2

- Komponente für die logische Zugangskontrolle zu IT-Systemen mit zentralem Nutzermanagement.
- Hierzu zählen FAT- und Thin-Clients.
- 1:1 Verifikation oder 1:n Identifikation zur Authentifizierung sind möglich.

## ID LifePass

- Komponente für die Integration der PalmSecure-Technologie in Systeme mit mangelnder Identitätskontrolle.
- 1:1 Verifikation oder 1:n Identifikation zur Authentifizierung sind möglich.

## Services

Ein Service-Katalog mit Themen zum Solution design und Beratungsleistungen über verschiedene Prozessebenen runden das Portfolio ab.

# ID GateKeeper – Verfügbare terminals

- ID GateKeeper -  
modulares Terminal  
(Triple1)



▪ Ohne Handführung

▪ Nur mit Fingerstütze

▪ Volle Handführung

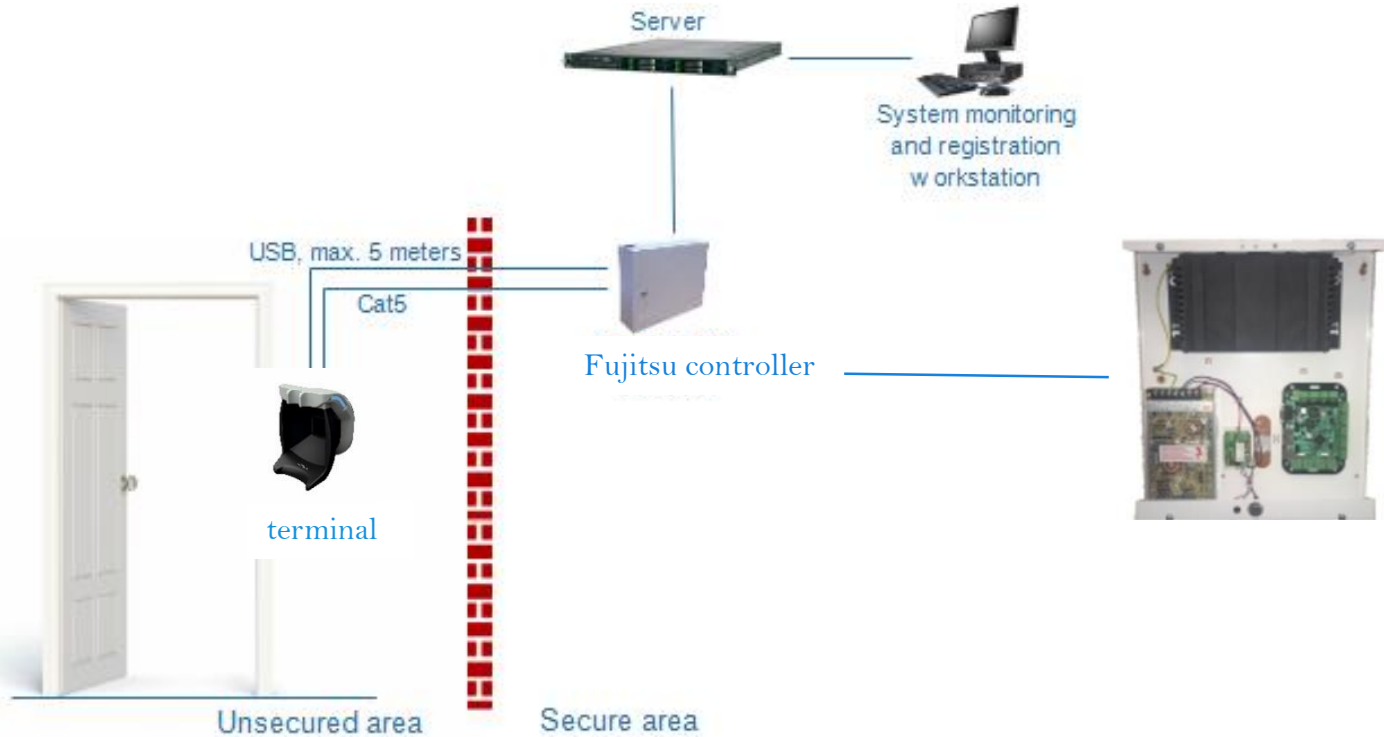
- ID GateKeeper –  
Terminal mit RFID  
(Triple1+)



ID GateKeeper –  
Zeiterfassungs Terminal  
(TripleTime)



# ID GateKeeper System Architektur



# Was kann ID LoginV2 leisten?



FAT-Client



Thin-Client

<i>Betriebssystem</i>	Windows 7, 8, 8.1, 10 (x86 / x64)	Windows 10 IoT, IGEL, eLuX, Ubuntu 16
<i>Virtualisierung</i>	Unabhängig	Vmware, Citrix, Microsoft RDP
<i>Authentifizierung</i>	Verifikation (Nutzername+Template)	Identifikation (nur Template)
<i>Features</i>	Multifaktor, OTP, Offline Modus	Sessionmitnahme

## Zugriff/Zugang

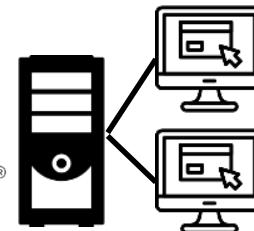
**Microsoft**



**Microsoft**

**CITRIX**

**vmware**

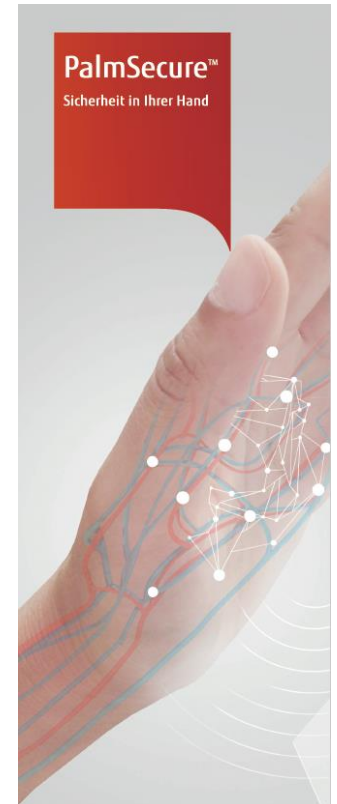


## ■ Sicherheit für weitere Applikationen

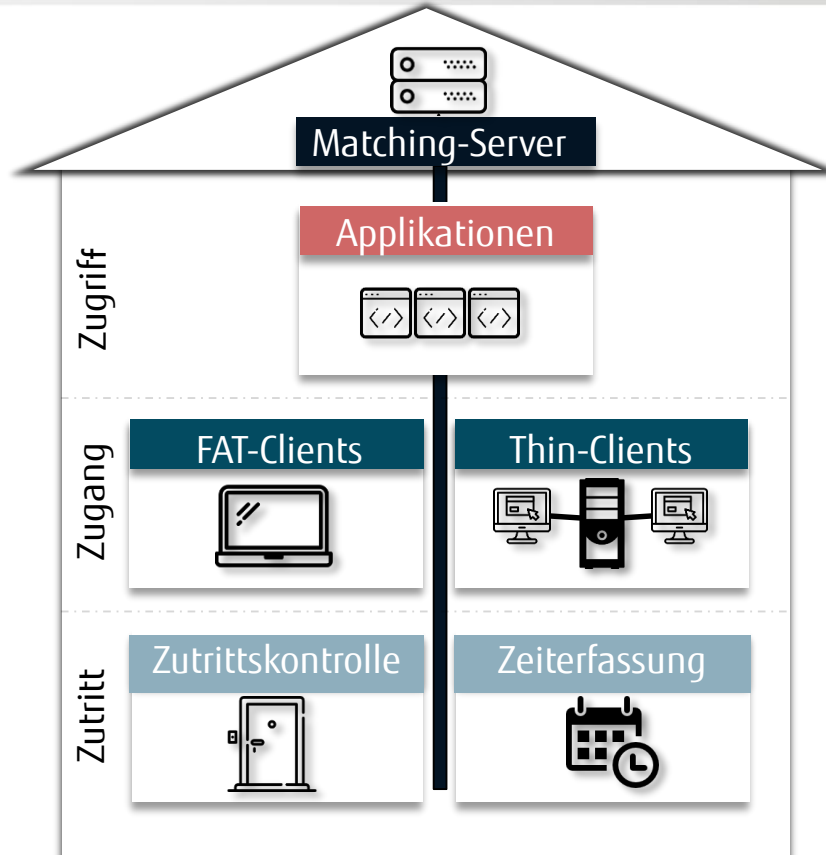
- Kunden nutzen heute bereits zentrale Tools, Applikationen, Prozesse und Systeme zur Arbeit
- Sicheres Log-in für Software Applikationen & Devices
- Projektspezifische Entwicklung und Implementierung

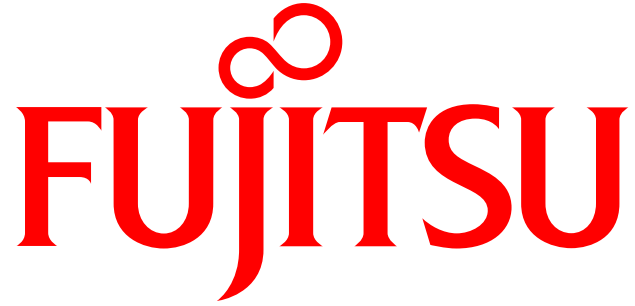
## ■ Mögliche Szenarien zur Benutzung aus Projekten

- Drei Casinos in Süddeutschland etablieren fast Lanes für Dauerbenutzer mit ca. 20k Benutzern
- Großbäckerei plant eine Implementierung an 11 Industrie Maschinen



# Wir freuen uns auf Ihre Projektideen





shaping tomorrow with you