

T.I.S.P. Community Meeting

Frankfurt a.M., 10. - 11.11.2016

Sicherer Zugang zu Intranet- Applikationen für Geschäftspartner

Reinhold Leitner

Primetals Technologies Austria GmbH

Lösungen entlang der gesamten Wertschöpfungskette – inklusive Lifecycle Services und hochklassiger Ausrüstung



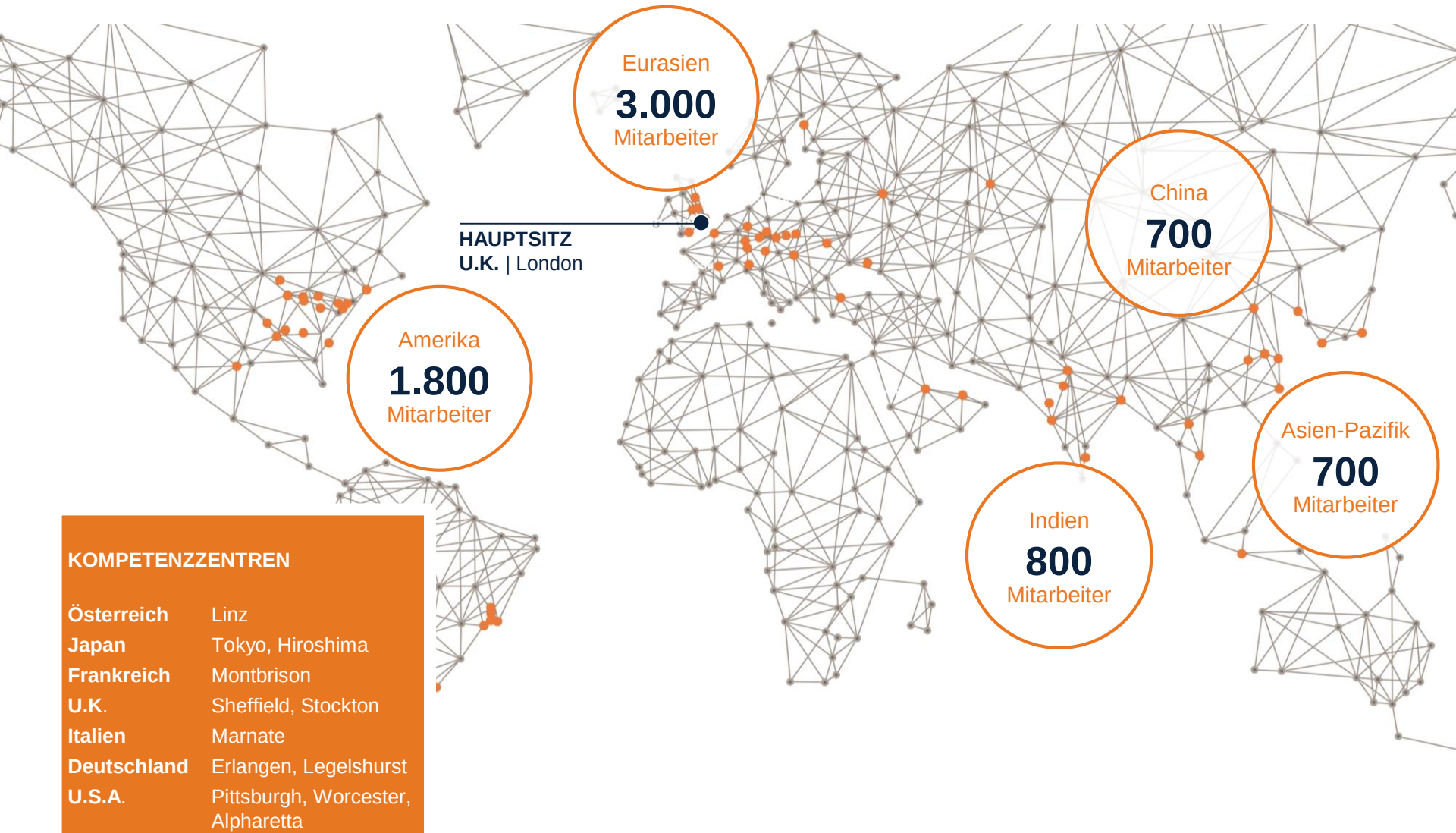
BERATUNGS- UND FINANZDIENSTLEISTUNGEN

ENERGIEEFFIZIENZ UND UMWELTSCHUTZ

ELEKTRIK UND AUTOMATISIERUNG

METALLURGISCHE SERVICES

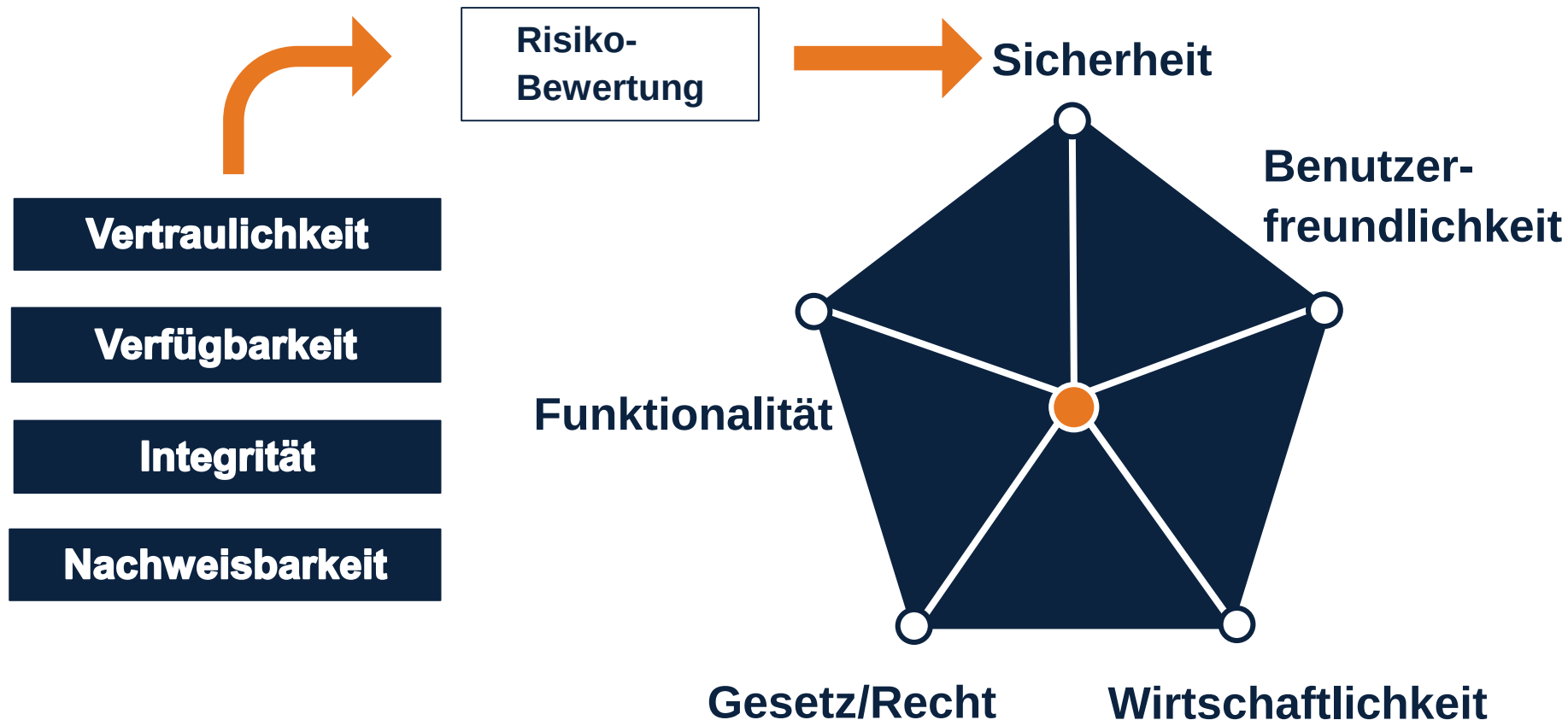
Globales Netzwerk von Niederlassungen, Engineering-, Fertigungs- und Servicecentern



Ziel

Zusammenarbeit mit Geschäftspartnern

- **Austausch von Daten (Dokumenten etc.) mit Kunden und Zulieferern**
- **Zugang zu Kunden-Anlagen durch Primetals während der Inbetriebnahme und der Produktion**



Zusammenarbeit mit Geschäftspartnern

Datei & Dokumenten Transfer

- E-Mail
- (S)FTP
- Secure File Exchange via Web
- ...



Datei & Dokumenten Sharing

- Netzlaufwerke
- SharePoint
- Cloud Services (Dropbox, ...)
- ...



Interaktive Anwendungen

- Fat Clients (e.g. SAP)
- Web Services, Social Media ...
- Datenbank Replikation
- Desktop Sharing
-



Design Kriterien

- **Stärke der Authentifizierung (personalisiert ...)**
- **Stärke der Verschlüsselung (Daten in Bewegung, Daten in Ruhe)**
- **Notwendige Autorisierung (Need-to-Know Prinzip)**
- **Implementierungsaufwand beim Geschäftspartner und im eigenen Bereich**
- **Kompatible Netzwerk Topologie und IT Infrastruktur**
- **IT Strategie des Geschäftspartners und eigene IT Strategie**
- **Netzwerk-Voraussetzungen: Latenz, Bandbreite**
- **Anzahl der Benutzer**
- **IT Unterstützung des Geschäftspartners**
- **Einmal-Kosten und laufende Kosten**
- **Service Level Agreements (SLA): Verfügbarkeit ...**
- **Verträge mit den Geschäftspartnern**
- **Prozess bei Beendigung der Zusammenarbeit**
- **...**



Authentifizierung

Motivation

- Schwache Authentifizierungsmethoden wie Benutzername/Passwort sind nicht ausreichend.
- Abhängig von der Risikobewertung sind zusätzliche Authentifizierungsverfahren zu implementieren (Zwei-Faktor-Authentifizierung ...).

Zwei-Faktor-Authentifizierung (Beispiele)

- Zertifikate:
Software Zertifikate, Smartcards (Karten, USB sticks)
- Einmal-Passwort:
Versand via E-Mail oder SMS
-
- Prüfung der IP Adresse der Quelle,
- Einrichtung eines Site-to-Site Tunnels



Zertifikat-Generierung

- Certification Authority (CA)
z.B. von Windows (Enterprise) Server
- MakeCert (Teil von Microsoft Windows SDK, obsolet!) oder Powershell Cmdlet New-SelfSignedCertificate (Windows 8 und Windows Server 2012 oder höher).
-



Selbstsignierte Zertifikate

Windows Powershell Beispiel

New-SelfSignedCertificate

```
-Type Custom
-Subject "E=TestUser@primetals.com,CN=TestCert,O=Primetals"
-TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2",
"2.5.29.17={text}Email=TestUser@primetals.com)"
-KeyUsage DigitalSignature -KeyAlgorithm RSA -KeyLength 2048
-CertStoreLocation "Cert:\CurrentUser\My"
```

Ergebnis:

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	TestUser@primetals.com, TestCer...
Valid from	Wednesday, August 24, 2016 6:1...
Valid to	Thursday, August 24, 2017 6:33:...
Subject	TestUser@primetals.com, TestCer...
Public key	RSA (2048 Bits)
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5...
Subject Alternative Name	RFC822 Name=TestUser@primet...
Subject Key Identifier	3b 17 f1 79 ac 32 b1 f6 c0 de af 7...
Key Usage	Digital Signature (80)
Thumbprint algorithm	sha1
Thumbprint	3e 42 5a e5 bc c2 8f 01 55 90 96 ...

Client Authentication (1.3.6.1.5.5.7.3.2)

Siehe auch : <https://technet.microsoft.com/library/hh848633>

Selbstsignierte Zertifikate mit "Certification Authority (CA)"

Erstelle „CA“ Zertifikat

```
$d=Get-Date 2026-12-31
```

```
New-SelfSignedCertificate -Type Custom -NotAfter $d  
-FriendlyName "Test CA" -Subject "CN=Test CA,O=Test GmbH"  
-KeyUsage DigitalSignature, CertSign -KeyAlgorithm RSA  
-KeyLength 4096 -CertStoreLocation "Cert:\CurrentUser\My"
```



Referenz zum „CA“ Zertifikat

```
Set-Location -Path "Cert:\CurrentUser\My"
```

```
$SignCert = (Get-ChildItem ThumbprintOfCACertificate)
```

Erstelle Zertifikat, durch „CA“ signiert

```
New-SelfSignedCertificate
```

```
-Signer $SignCert -Type Custom  
-Subject "E=TestUser@primetals.com,CN=TestCert,O=Primetals"  
-TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2",  
"2.5.29.17={text}Email=TestUser@primetals.com")  
-KeyUsage DigitalSignature -KeyAlgorithm RSA -KeyLength 2048  
-CertStoreLocation "Cert:\CurrentUser\My"
```



Windows Server Certification Authority

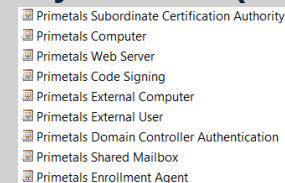
Referenz

- Certification Authority Guidance
[https://technet.microsoft.com/en-us/library/hh831574\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831574(v=ws.11).aspx)



Features

- Unterstützung von Hardware Security Modules (HSM)
- Untergeordnete CAs
- Vorlagen
- Zugriffskontrolle
- Active Directory (AD) Integration
- Zertifikatsperrliste (Certificate Revocation List, CRL)
- Integration von fremden PKIs in das AD (via User Principal Name)



Smartcards

- Karten
- USB Sticks
(z.B. eToken von SafeNet)



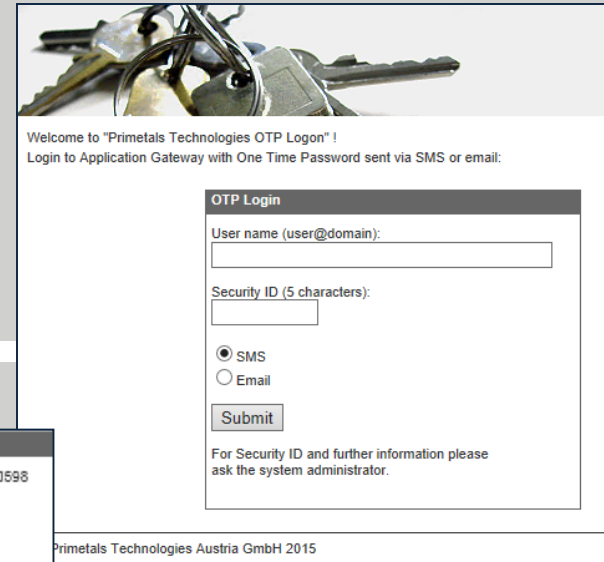
Der private Schlüssel verlässt die Smartcard nicht!

Bemerkung: Installation von Treiber Software ist notwendig.

Einmal-Passwort

Eingabe

- E-Mail Adresse
- Security ID



Welcome to "Primetals Technologies OTP Login" !
Login to Application Gateway with One Time Password sent via SMS or email:

OTP Login

User name (user@domain):

Security ID (5 characters):

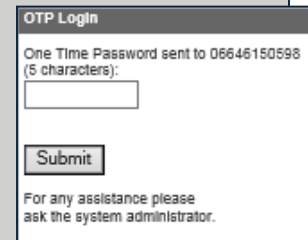
☒ SMS
☐ Email

For Security ID and further information please ask the system administrator.

Primetals Technologies Austria GmbH 2015

Einmal-Passwort wird via SMS oder E-Mail versandt

- Eingabe des Einmal-Passworts



OTP Login

One Time Password sent to 06646150598 (5 characters):

For any assistance please ask the system administrator.

Primetals Technologies Austria GmbH 2015

Implementierung

- Portal, das den Datenverkehr überwacht
- Kann mit jeder Web-Applikation verwendet werden
- Zusätzliches Cookie um die Web-Session zu identifizieren

Netzwerk Zugriff via Internet

Web Anwendungen

- https (“Firewall Bypass Protocol”)
- Server verlangt Zertifikate vom Client via TLS oder
- Einmal-Passwort



Remote Desktop Gateway (RDG)

- Remote Desktop Protocol (RDP) via https, Smartcard Unterstützung
- Web Proxies werden unterstützt (IE Einstellungen)
- Bestandteil des Windows Betriebssystems



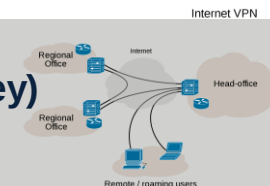
Remote Access Service (RAS) (Client zu Site)

- Secure Socket Tunneling Protocol (SSTP), basierend auf https
- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)
-
- Implementierungen von verschiedenen Herstellern verfügbar

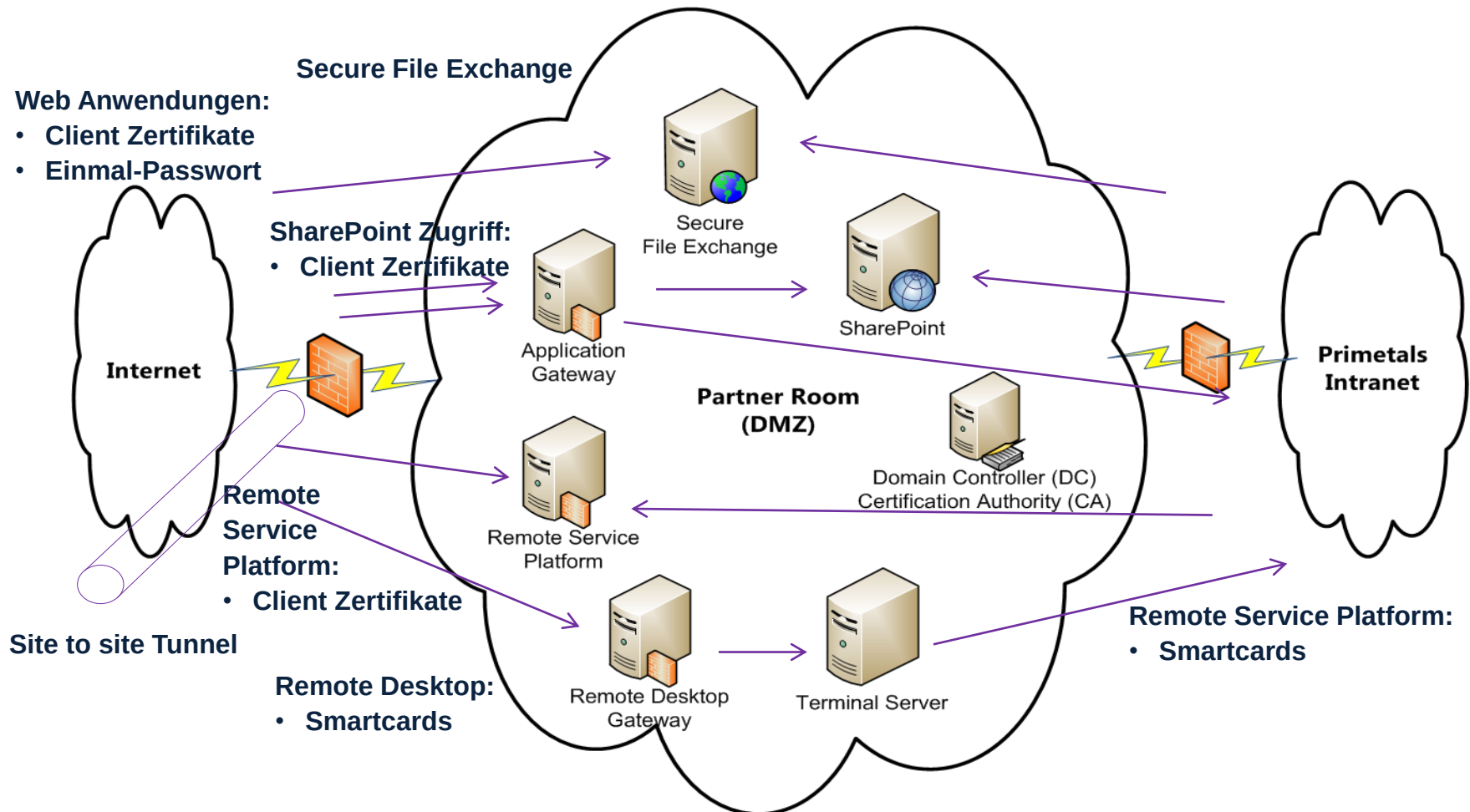


Site-to-Site Tunnel

- IPSEC mit Zertifikat oder Passwort (preshared key)
-



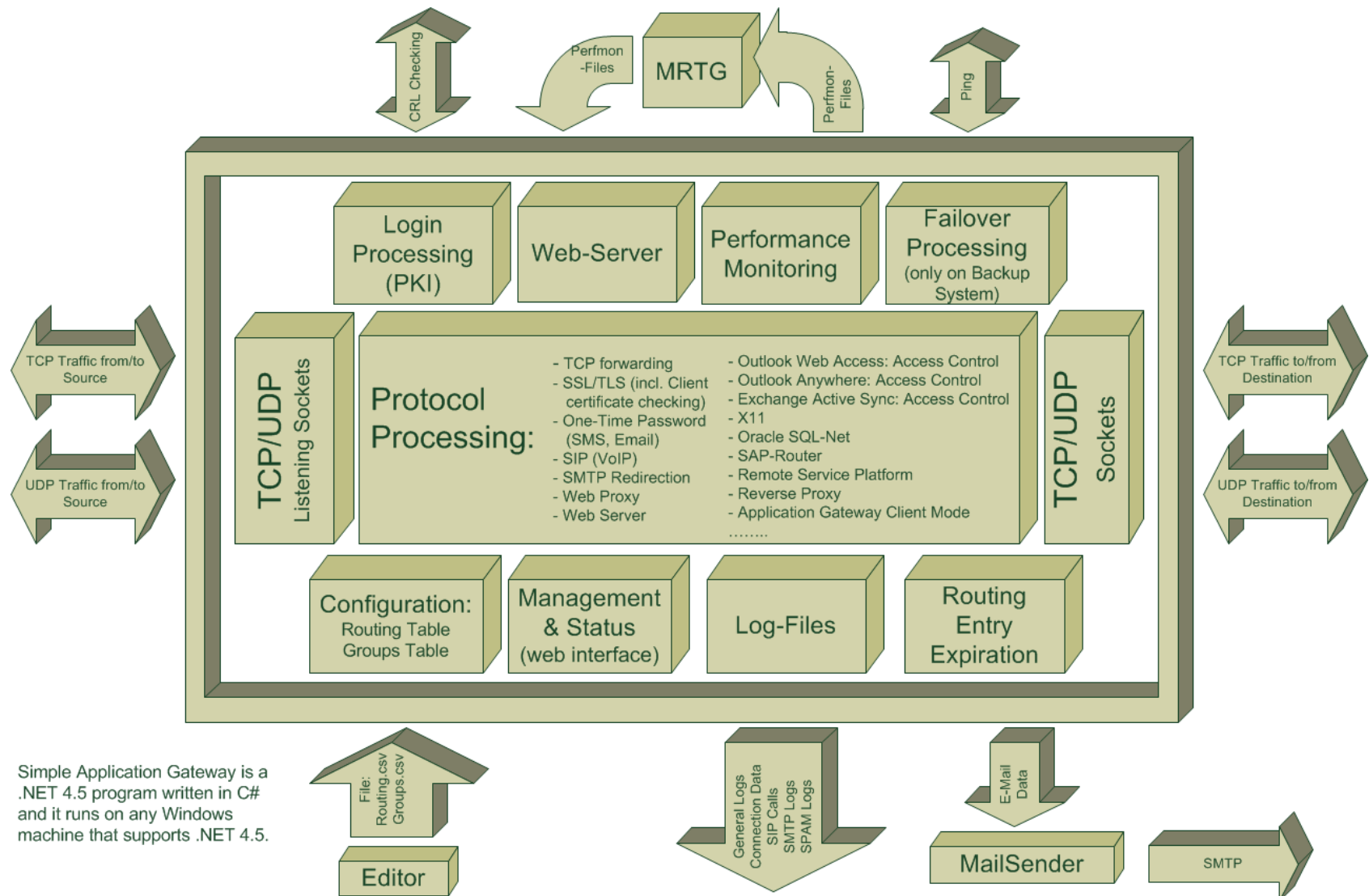
Partner Raum in Demilitarized Zone (DMZ)



Keine direkten TCP Verbindungen zwischen Internet und Intranet.

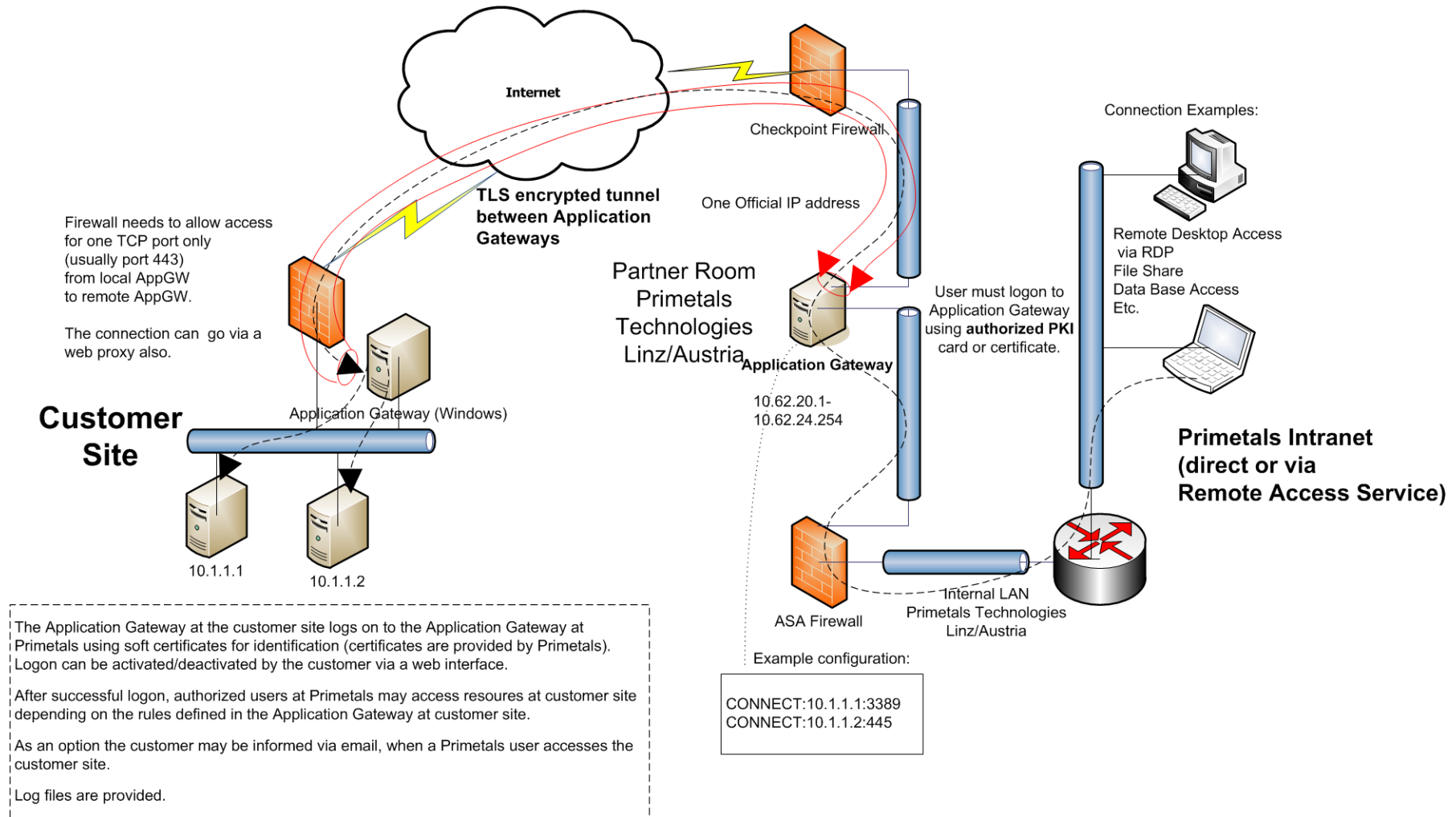
Alle Verbindungen werden über Proxies geroutet: Kein IP Routing durch die DMZ !

Simple Application Gateway



Simple Application Gateway is a .NET 4.5 program written in C# and it runs on any Windows machine that supports .NET 4.5.

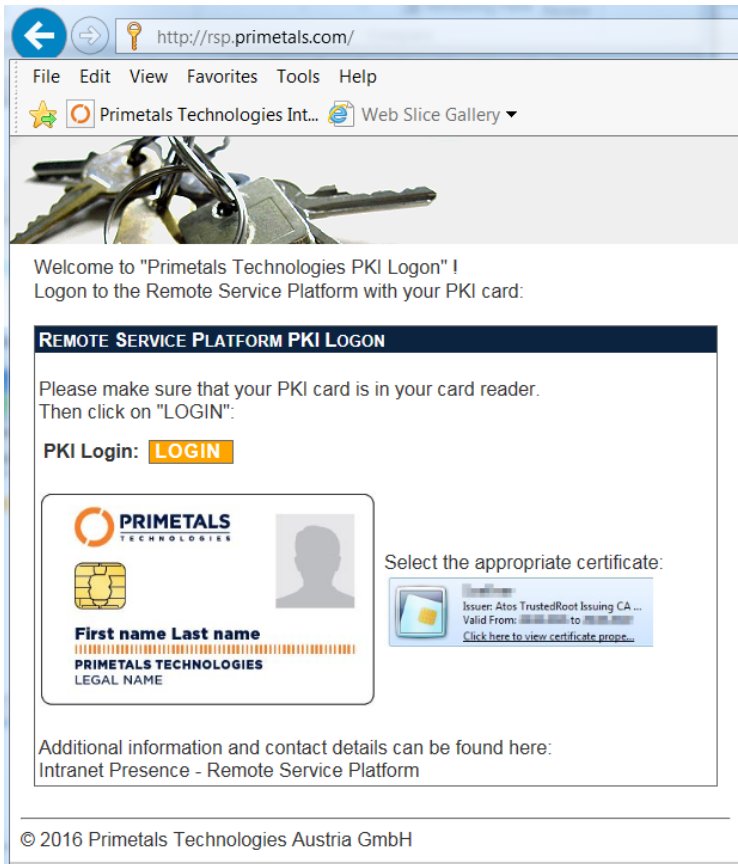
Remote Service Platform



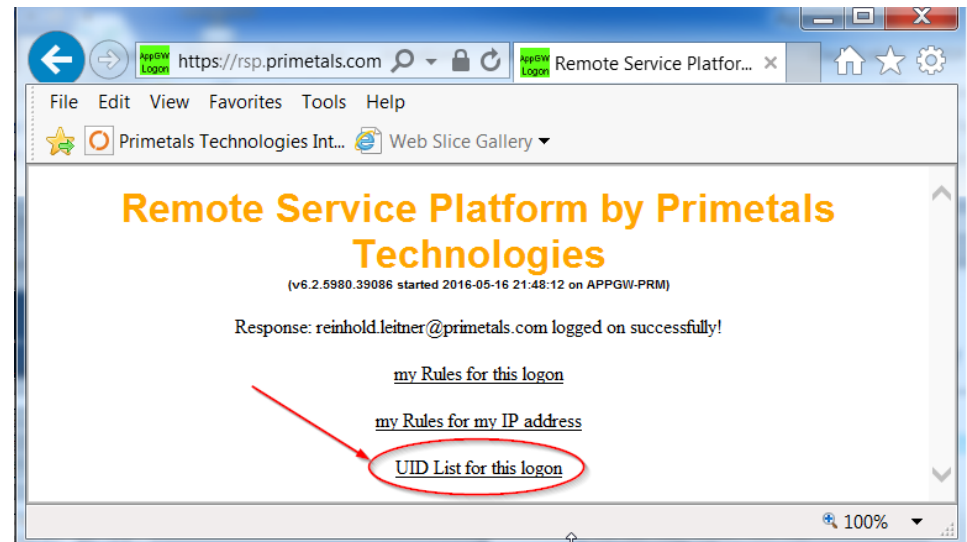
Zugang zu Kundenanlagen

Anmeldung am Application Gateway

1) Anmeldung am Application Gateway via Smartcard <http://rsp.primetals.com>



2) Anwählen der Liste der Kundenanlagen:



Zugang zu Kundenanlagen

3) Liste der Kunden: **UID List (my logon: reinhold.leitner@primetals.com)**

UID	UIDname	Users	Responsible
S101	IT ISEC VLAN5	RSPtest	reinhold.leitner@primetals.com, robert.soellner@primetals.com
S	All links are active!	RSPtest	reinhold.leitner@primetals.com
S103	VSP BF1	VSP BF1, RSPmgmt	praveen.mishra@primetals.com

4) Liste der verfügbaren Verbindungen zu Kundenanlagen: **Routing Table (UID: S101, UIDname: IT ISEC VLAN5)**

last loaded 2016-05-17 10:58:29, last written 2016-05-17 10:58:15

ID	Source IP	Gateway IP	Gateway Port	Destination IP	Type	UID	Shortcut	Comment
28	RSPtest	10.62.22.11	88	rl.itisec.rsp@primetals.com:F1	more...	S101.1	http://*	AppGw Status
29	RSPtest	10.62.22.11	445	rl.itisec.rsp@primetals.com:F2	more...	S101.2	Share-LEITNEREpc.bat	Network Share
30	RSPtest	10.62.22.11	5900	rl.itisec.rsp@primetals.com:F4	more...	S101.3	Leitner-PC.vnc	VNC
31	RSPtest	10.62.22.11	3389	rl.itisec.rsp@primetals.com:F3	more...	S101.4	Leitner-PC.rdp	RDP
32	RSPtest	10.62.22.11	80	rl.itisec.rsp@primetals.com:F3	more...	S101.5	Leitner-PC-WebDAV.bar	WebDAV

Shortcuts zu

- Management des Application Gateway beim Kunden
- Netzlaufwerk
- VNC Verbindung
- RDP Verbindung
- ...

Shortcuts

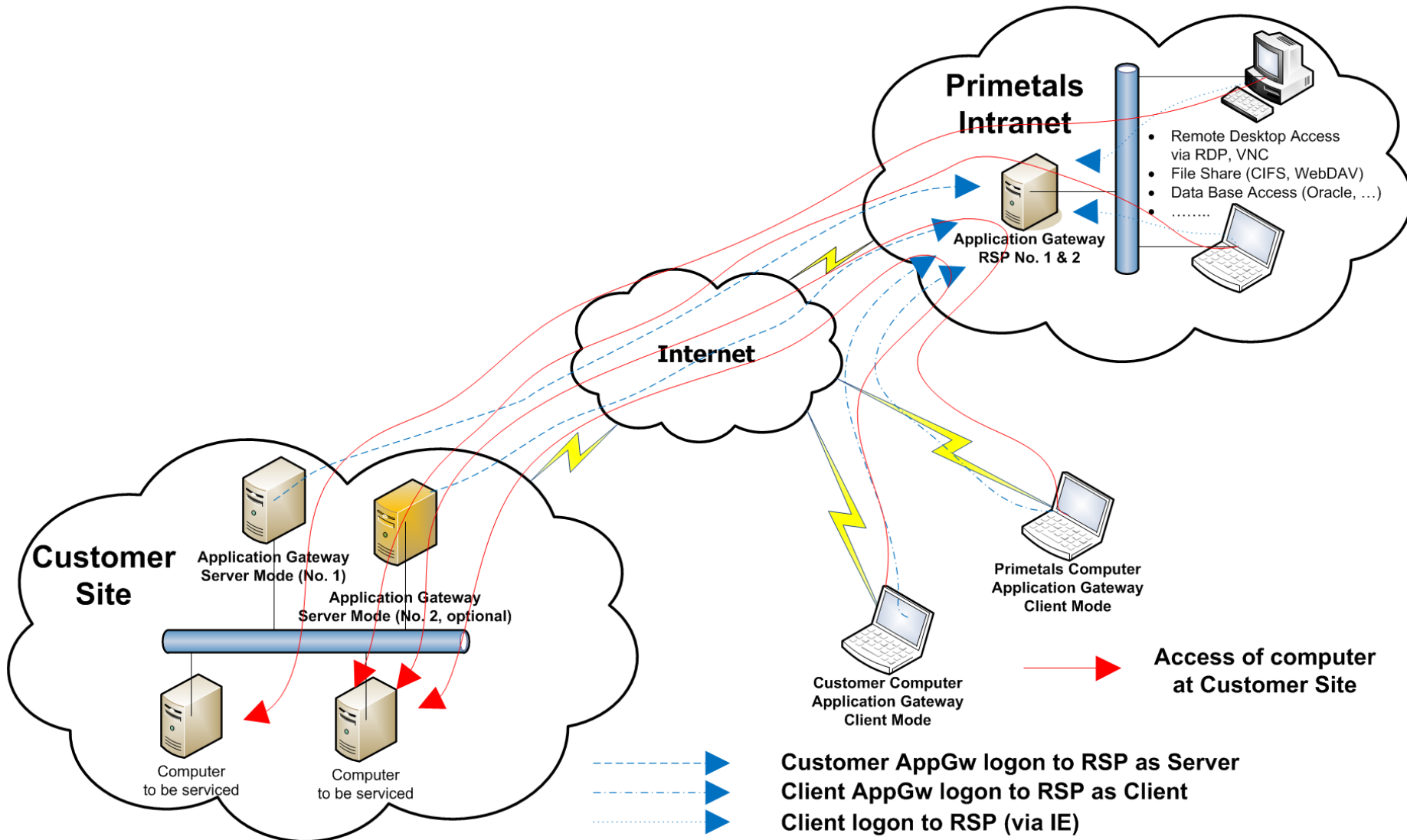
- sind auf Webseiten oder Netzlaufwerken abgespeichert
- werden von Primetals Usern verwaltet (Function, Zugriffskontrolle, Passwort Speicher)

5) Klick Shortcut:

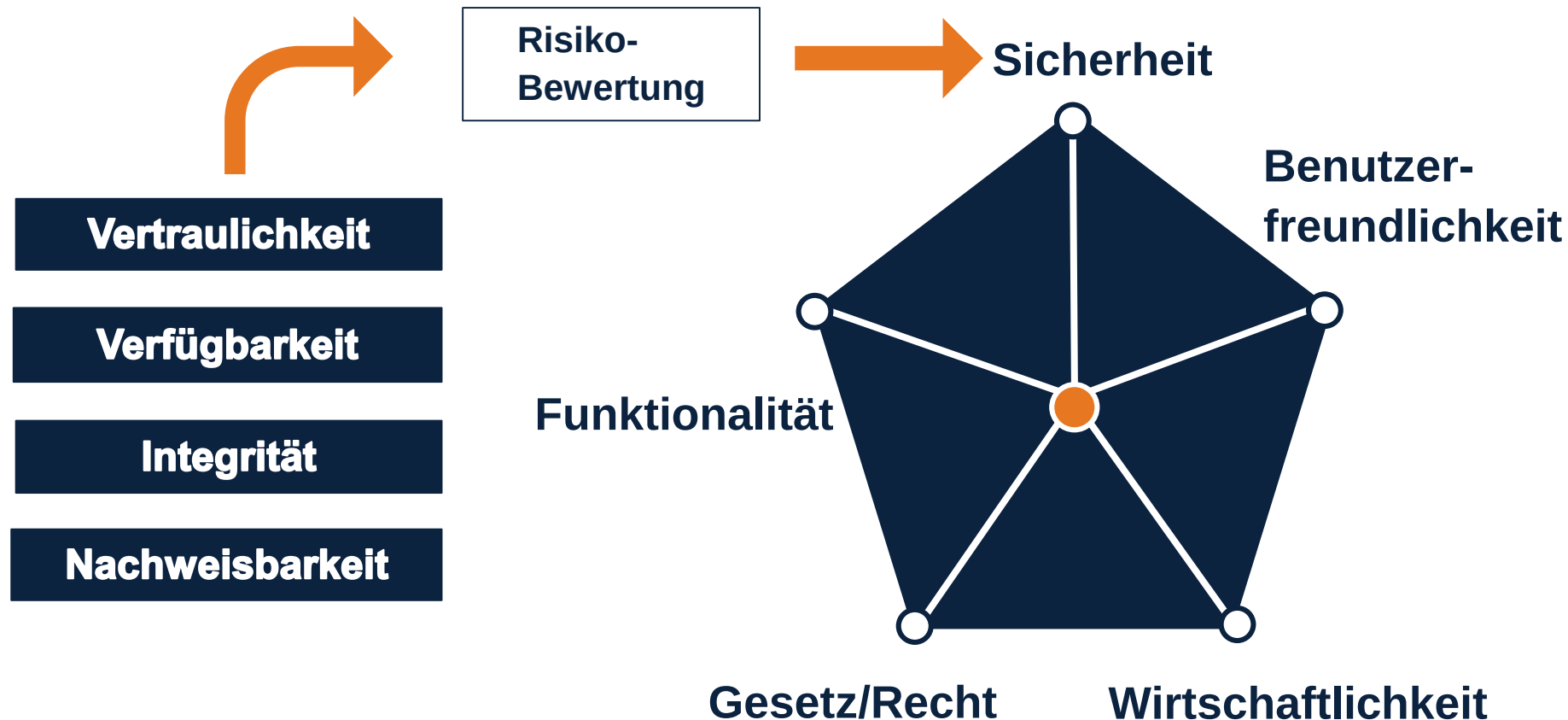
Der Shortcut verbindet zu einer internen Adresse aus 10.62.22.0/23 oder 10.62.30.0/23 und aktiviert die Verbindung zum Kunden-System.

Remote Service Platform by Primetals

- Access from Internet
- Access out of PT Intranet



Wähle die passende Lösung ...



Kontakt

Reinhold Leitner
IQ IT ISEC

Primetals Technologies Austria GmbH
Turmstrasse 44
4031 Linz
Austria

M +43 (664) 6150598
E reinhold.leitner@primetals.com

primetals.com

The information (including, e.g., figures and numbers) provided in this document contains merely general descriptions or characteristics of performance based on estimates and assumptions which have not been verified.

It is no representation, does not constitute and/or evidence a contract or an offer to enter into a contract to any extent and is not binding upon the parties. Any obligation to provide and/or demonstrate respective characteristics shall only exist if expressly agreed in the terms of the contract.

These estimates and assumptions have to be analyzed on a case-to-case basis and might change as a result of further product development.

Primetals Technologies excludes any liability whatsoever under or in connection with any provided information, estimates and assumptions. The provided information, estimates and assumptions shall be without prejudice to any possible future offer and/or contract.

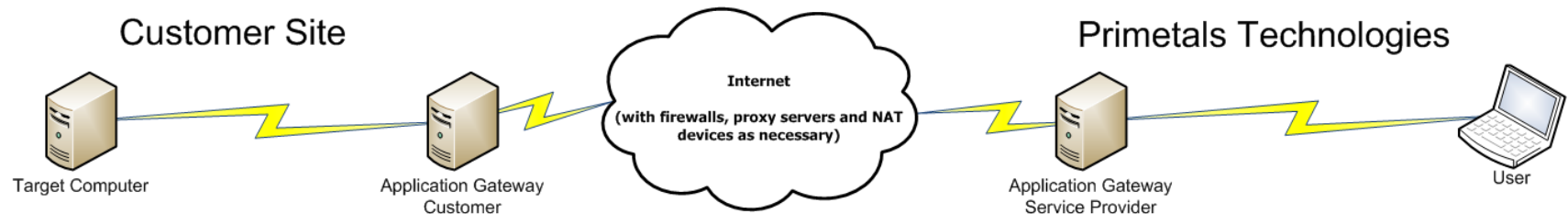
Any use of information provided by Primetals Technologies to the recipient shall be subject to applicable confidentiality obligations and for the own convenience of and of the sole risk of the recipient.



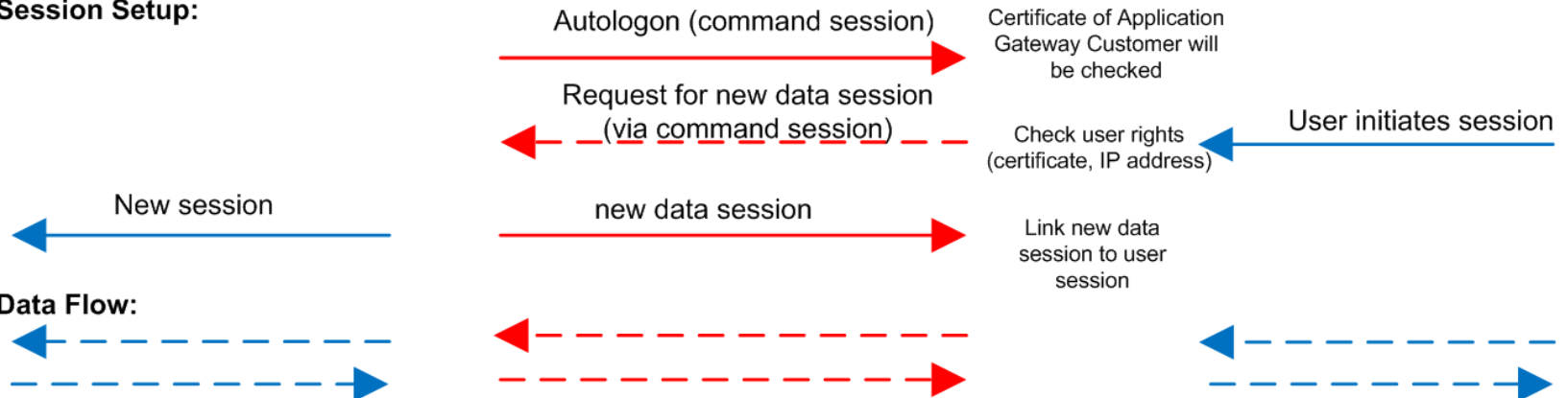
**Vielen Dank für Ihre
Aufmerksamkeit!**

Message Flow with Application Gateway at Customer Site

User at Primetals Technologies accesses a computer at customer site



Session Setup:



Remarks:

- Autologon sessions (command sessions) can be activated and/or terminated by the customer at Application Gateway Customer at any time.
- Autologon (command session, usually https via port 443) can be routed via various proxy servers and NAT devices.
- Firewall at customer site must allow only one outgoing session (usually https via port 443) to one specific address in the Internet.
- Customer sender address (as visible in the Internet) need may be dynamic and can be changed at any time.
- There is no incoming session establishment via the Internet to the Application Gateway Customer.
- Data sessions can be terminated by the customer at any time.
- Access to computers at customer site can be restricted/disallowed by the customer.
- Customer can be notified by email at user session activation and/or termination.

Session Setup:



Data:

