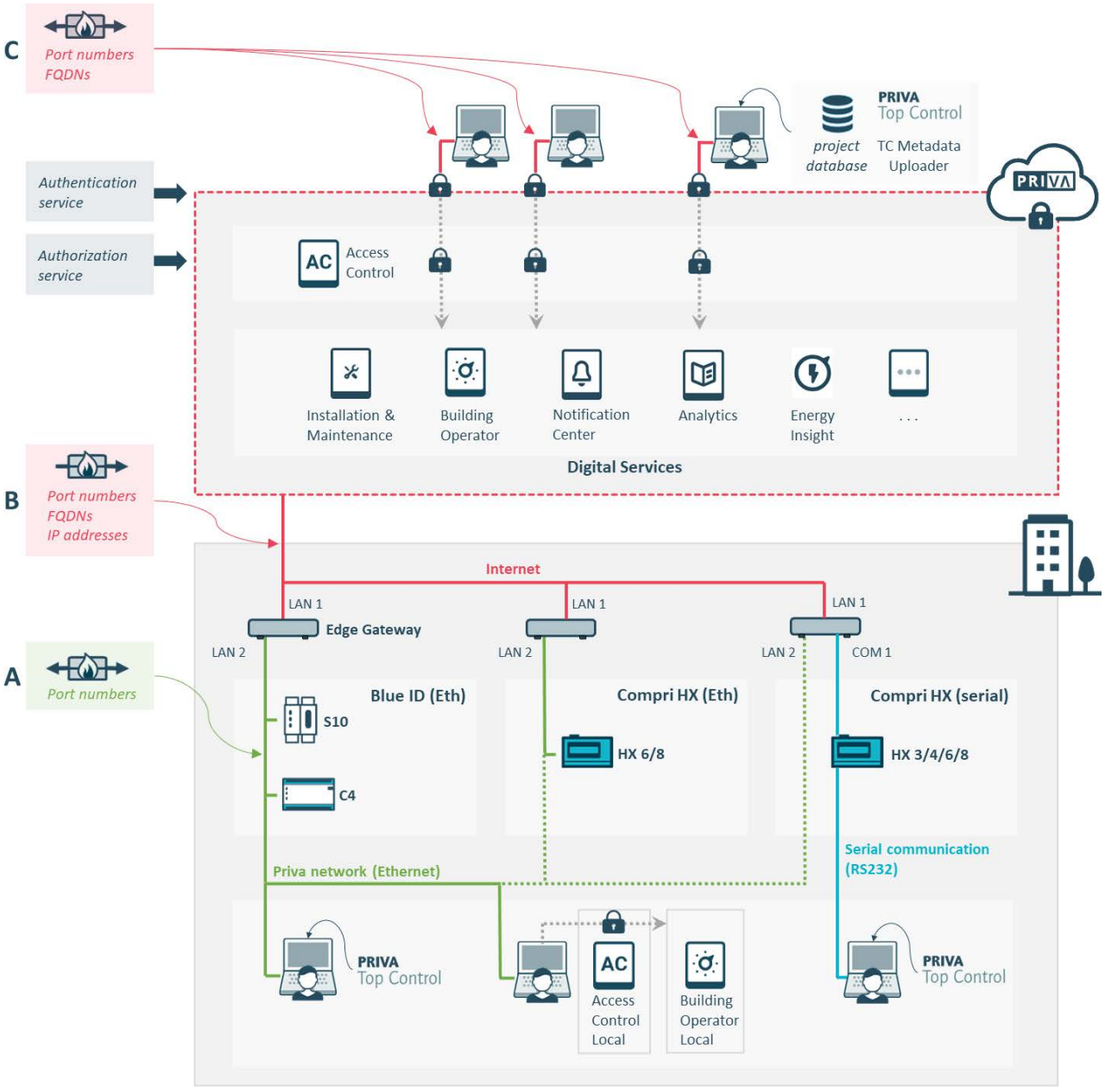
> ICT-INFORMATION

Priva Blue ID, Top Control, Digital Services

Wie schützt Priva die Daten Ihres Gebäudes? Und was müssen Sie tun, um eine sichere Kommunikation zwischen der Hardware und Software von Priva zu ermöglichen?

Netzwerkübersicht

Die Abbildung zeigt die empfohlene Netzwerkkonfiguration, wobei das Priva-Netzwerk vom Internet getrennt ist. Berücksichtigen Sie, dass Sicherheitsrisiken entstehen, wenn das Priva-Netzwerk nicht vom Internet getrennt ist.



A Siehe: A) Kommunikation im lokalen Netzwerk (Seite 3)

B Siehe: B) Kommunikation zwischen Gateway und Priva Cloud (Seite 5)

C Siehe: C) Kommunikation zwischen Browsern und Priva Cloud (Seite 8)

Funktion Edge Gateway/Cloud Connector

Gebäudeverwaltungssysteme dürfen in keinem Fall innerhalb eines Netzwerks mit Internetzugang ausgeführt werden. Zur Verwendung von Cloud-Diensten ist natürlich Kommunikation zwischen dem Verwaltungssystem und der Priva Cloud erforderlich. Das Edge Gateway und das Cloud Connector sind Gateways, die das auf geschützte Weise ermöglichen. Das Edge Gateway ist der Nachfolger des Cloud Connector.

Das Gateway lässt ausschließlich abgehende Verbindungen zu. Dadurch schützt es das Gebäudeverwaltungssystem vor Zugriff durch Unbefugte über das Internet. Eingehende Verbindungen lässt es nicht zu. Wenn das Gateway die abgehende Verbindung einrichtet, werden eingehende Daten innerhalb der aktiven Session jedoch zugelassen. Dies ermöglicht den Abgleich der Werte von außen mittels einer Anwendung/eines Dienstes.

Die zwischen Gateway und Cloud übertragenen Daten werden durch Verschlüsselung geschützt. Im Gegensatz zu anderen Zugriffsmethoden auf Gebäudeautomatisierungssysteme, beispielsweise VPN, verwendet diese Architektur ein nachrichtenbasiertes System, sodass keine vollständige Datenverbindung zwischen dem Gebäude und der Außenwelt besteht. Daten werden nur in sehr eingeschränktem Umfang ausgetauscht.

Windows 10 IoT-Updates auf das Cloud Connector werden im Rahmen des standardmäßigen Windows-Aktualisierungsverfahrens automatisch heruntergeladen und installiert. Innerhalb der Zeiten, in denen das Cloud Connector standardmäßig aktiv ist (8.00-17.00 Uhr), wird kein Neustart erzwungen.

Linux-Updates auf das Edge Gateway werden in Installation & Maintenance (Modul FirmwareUpdater) ausgeführt.

Support durch Priva

Priva kann über TeamViewer auf dem Cloud Connector einfach aus der Ferne Support bieten. Dafür muss Port 5938 offen sein.

Für das Edge Gateway gibt es keinen Support per TeamViewer, weil auf dieses Gateway nicht direkt von außen zugegriffen werden kann.

Sicherheitsmaßnahmen von Microsoft

Alle Digital Services wurden auf Basis der Cloud-Plattform von Microsoft Azure entworfen. Die Services von Priva nutzen für die Kommunikation zwischen Priva-Netzwerk und Cloud die Standardkomponenten IoT-Hub und Service Bus von Microsoft Azure. Detaillierte Angaben zum Schutz durch Microsoft finden Sie im Microsoft Trust Center.

A) Kommunikation im lokalen Netzwerk

Um die Kommunikation innerhalb des lokalen Netzwerks zu ermöglichen, müssen bestimmte Ports in der Firewall offen sein (sofern eine Firewall vorhanden ist).

Siehe **A** in der Abbildung in Netzwerkübersicht (Seite 1).

Portnummern (Kommunikation im lokalen Netzwerk)

Die nachstehende Liste enthält die Portnummern, die für die Kommunikation zwischen der Priva Blue ID/Compri HX-Hardware und den Top Control-Anwendungen und dem Cloud Connector oder dem Edge Gateway erforderlich sind. Dort finden Sie auch Angaben dazu, ob der Port eingehende oder abgehende Kommunikation nutzt. Die Konfiguration der Ports in der Firewall hängt von den verwendeten Top Control-Anwendungen und der im Projekt angelegten Netzwerkkonfiguration ab.

Port	Details	Transport-protokoll	Priva Blue ID, Compri HX	TC Engineer	TC Operator	TC Manager	TC ServeCenter	TC History Proxy	TC History	TC LANManager	Edge Gateway	Cloud Connector
25 465 587 [16]	SMTP(S)[16]	TCP	→				→					
53	DNS	TCP/UDP	→	→	→	→	→	→	→	→	→ 9,10,11	→ 10
67	DHCP	TCP									→	
80	HTTP	TCP	←	→ 1	→ 1	→	→ 1	→ 1	→ 1	→ 1	← 10,11	
123	NTP	UDP	←								→ 9,10	→ 10
161	SNMP [8]	TCP/UDP	→									
502 [2]	Modbus	TCP	←									
514	Rsyslog	UDP									→ 10	
1883	MQTT	TCP									→ 10	
1900	SSDP	UDP									→ 10	
5000	LOAS [12]	TCP									→ 10	
5001	LOUM [13]	TCP									→ 10	
5002	LOU [14]	TCP									→ 10	
5003	LOAS [15]	TCP									→ 10	
5353	mDNS	TCP/UDP	←	←	←	←					→ 10	→ 10
7650	DDS	UDP									→ 10	
7651	DDS	UDP									→ 10	
7660	DDS	UDP									→ 10	

Port	Details	Transport-protokoll	Priva Blue ID, Compri HX	TC Engineer	TC Operator	TC Manager	TC ServeCenter	TC History Proxy	TC History	TC LAN Manager	Edge Gateway	Cloud Connector
7661	DDS	UDP									← 10	
8080 [2]	HTTP	TCP				←		←				
9093	XML	TCP	←									
9354	SBMP	TCP (TLS 1.2)										←
9508	PTP	UDP									← 10	
15000	Priva [5,7]	UDP	↔								↔ 10	↔ 10
15001	Priva [5]	UDP	↔	↔ 3	↔ 3		↔ 3		↔ 3	↔	↔ 10	↔ 10
23456 24690 25924 27158[17]	Priva [4]	TCP		↔	↔		↔	↔	↔	↔		
23457 24691 25925 27159[17]	Priva [4]	UDP		↔	↔		↔	↔	↔	↔		
47808 bis 47817[16]	BACnet [6]	UDP	↔									

← = eingehend
→ = ausgehend
↔ = ein- und ausgehend

[1] Nur Online-Hilfe

[2] Standardportnummer, kann geändert werden

[3] Für „Lokal kommunizieren“

[4] TC LAN Manager sucht eine freie, verwendbare Portnummer

[5] Priva-eigenes Protokoll

[6] Reservierte Ports, einstellbar in TC Engineer

[7] Bei Verwendung einer Compri HX-Verbindung

[8] Nur SNMP Trap wird in Top Control 8 unterstützt

[9] LAN-Port für den Internetanschluss
(Edge Gateway: LAN 1, Cloud Connector: LAN 3)

[10] LAN-Port- den Anschluss an das Priva-Netzwerk
(Edge Gateway: LAN 2, Cloud Connector: LAN 1)

[11] Serviceport
(Edge Gateway: LAN 3, Cloud Connector: LAN 2)

[12] Lokaler Autorisierungsservice für Bediener

[13] Lokale Benuzterverwaltungs-UI für Bediener

[14] Lokale Bediener-UI

[15] Lokale Bediener-API

[16] Wählen Sie eine der angegebenen Portnummern aus

[17] Wählen Sie eine der angegebenen Portnummern aus. Die ausgewählten Portnummern aus den beiden Zeilen mit Anmerkung 17 müssen aufeinander folgen (z. B. 23456 und 23457).

B) Kommunikation zwischen Gateway und Priva Cloud

Um die Kommunikation zwischen dem Gateway und der Priva Cloud zu ermöglichen, müssen bestimmte Ports in der Firewall geöffnet sein. Auch muss die Kommunikation mit der Priva Cloud auf Grundlage von FQDNs oder der IP-Adressen zugelassen werden.

Siehe **B** in der Abbildung in Netzwerkübersicht (Seite 1).

Portnummern (Gateway – Priva Cloud)

Die nachstehende Tabelle beinhaltet die für Kommunikation zwischen der Priva Cloud und dem Gateway erforderlichen Portnummern. Alle Ports nutzen nur ausgehende Kommunikationsverbindungen. Port 5938 ist für den Support von Priva mit TeamViewer erforderlich (nur auf dem Cloud Connector).

Port	Details	Transport-protokoll	Edge Gateway	Cloud Connector
123	NTP	UDP	[1]	
443	HTTPS	TCP	[1]	[1]
5671	AMQP	TCP	[1]	[1]
5672	AMQP	TCP	[1]	[1]
5938	Team-Viewer	TCP		[1]
8883	MQTT	TCP	[1]	[1]
9354	SBMP	TCP (TLS 1.2)		[1]

= ausgehend

[1] LAN-Port für den Internetanschluss (Edge Gateway: LAN 1, Cloud Connector: LAN 3)

FQDNs (Gateway – Priva Cloud)

Die nachstehenden Tabellen beinhalten die Fully Qualified Domain Names (FQDN), die für die Kommunikation zwischen dem Gateway und der Priva Cloud erforderlich sind. Sie haben die Wahl, Wildcards (mit * beginnende Adressen) zu verwenden oder die kompletten FQDNs freizugeben. Die Liste der kompletten FQDNs ist jedoch dynamisch; FQDNs können später hinzugefügt und geändert werden. Der Pflegeaufwand ist bei der Verwendung von Wildcards geringer, da sich die Wildcard-Liste seltener ändert als die Liste der vollständigen FQDNs.

Wir empfehlen, zumindest den Wildcard *.priva.com für zukünftige Entwicklungen auf die Whitelist zu setzen.

FQDNs: vom Edge Gateway zur Cloud

FQDN	Service/Dienst
***.servicebus.windows.net** (HTTPS)	
priva-lwe-prod-gateway-master-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition2-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition3-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition4-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition5-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition6-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition7-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition8-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition9-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition10-weu.servicebus.windows.net	Remote Management, Cloud History
***.blob.core.windows.net** (HTTPS)	
coprdfrontend2sawe.blob.core.windows.net	Gateway-Services[1]
edgegatewayfirmware.blob.core.windows.net	Gateway-Services[1]
prddevicemetadatasa.blob.core.windows.net	Gateway-Services[1]
prdhdptsgwtelemetrysa.blob.core.windows.net	Cloud History
prdprivaauditlogs.blob.core.windows.net	Gateway-Services[1]

FQDN	Service/Dienst
***.priva.com** (HTTPS)	
cr.priva.com	Gateway-Services[1]
cr-data-westeurope.priva.com	Gateway-Services[1]
data-gateway-fileuploader.priva.com	Gateway-Services[1]
edge-remote.priva.com	Gateway services[1]
local-auth-provisioning.priva.com	Gateway-Services[1]
***.pool.ntp.org** (NTP)	
Länderabhängig, z.B.: 0.de.pool.ntp.org	NTP-Server
Andere	
aka.ms [2] (HTTPS)	Gateway-Services[1]
global.azure-devices-provisioning.net (HTTPS)	Gateway-Services[1]
mcr.microsoft.com (HTTPS)	Gateway-Services[1]
prd-priva-generic-ih.azure-devices.net (HTTPS, MQTT, AMQP)	Gateway-Services[1]
priva.azurecr.io (HTTPS)	Gateway-Services[1]
priva.westeurope.data.azurecr.io (HTTPS)	Gateway-Services[1]

[1] Gatewaybezogene Services/Dienste (Konfiguration des Gateways, Gateway-Updates, Autorisierung, Metadaten...)[1]

[2] Beim Ausführen der Konnektivitätsprüfung (in der lokalen Konfigurationsanwendung) leitet aka.ms zu anderen Endpunkten weiter: raw.githubusercontent.com/* (Änderungen vorbehalten).

FQDNs: vom Cloud Connector zur Cloud

FQDN	Service/Dienst
***.servicebus.windows.net** (HTTPS, SBMP)	
priva-lwe-prod-gateway-master-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition2-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition3-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition4-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition5-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition6-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition7-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition8-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition9-weu.servicebus.windows.net	Remote Management, Cloud History
priva-lwe-prod-gateway-partition10-weu.servicebus.windows.net	Remote Management, Cloud History
***.priva.com** (HTTPS)	
accesscontrolapi.priva.com	Gateway-Services[1]
assetapi.priva.com	Gateway-Services[1]
auth.priva.com	Gateway-Services[1]
authorization.priva.com *(obsolet)*	Gateway-Services[1]
connect.priva.com *(obsolet)*	Gateway-Services[1]
gps.priva.com	Gateway-Services[1]
state.priva.com	Gateway-Services[1]
tenantapi.priva.com	Gateway-Services[1]
Andere	
prdinstallupdatesa.blob.core.windows.net (HTTPS)	Gateway-Services[1]

[1] Gatewaybezogene Services/Dienste (Konfiguration des Gateways, Gateway-Updates, Autorisierung, Metadaten...)[1]

IP-Adressen (Gateway – Priva Cloud)

Priva verwendet die IP-Adressbereiche „EuropeWest“ und „EuropeNorth“ von Microsoft, die für Priva Digital Services erforderlich sind. Diese Bereiche werden von Microsoft dynamisch genutzt und können daher nicht näher bezeichnet werden. Angaben zu den von Microsoft genutzten Bereichen sind auf der Website https://www.microsoft.com/en-us/download/details.aspx?id=56519 zu finden. Laden Sie die json-Datei herunter.

Die Datei wird wöchentlich aktualisiert. Neu in die Datei aufgenommene Bereiche dürfen mindestens eine Woche lang nicht in Azure verwendet werden. Falls Sie die IP-Adressen-Beschränkungsliste verwenden, laden Sie wöchentlich die neue json-Datei herunter und implementieren Sie die erforderlichen Änderungen an Ihrem Standort, um die in Azure ausgeführten Dienste korrekt zu identifizieren.

Verwenden Sie nicht den IP-Adressbereich 172.23.105.0/24. Dieser Bereich wird bereits intern im Edge Gateway verwendet.

Internetverbindung

Alle Priva Digital Services erfordern eine Breitband-Internetverbindung mit einer Upload- und Download-Geschwindigkeit von mindestens 1 Mbit/s.

C) Kommunikation zwischen Browsern und Priva Cloud

Um die Kommunikation zwischen den Browsern der Priva Digital Services-Benutzer und der Priva Cloud zu ermöglichen, muss Port 443 in der Firewall geöffnet sein und die Kommunikation mit der Priva Cloud muss auf Basis von FQDNs zugelassen sein.

Siehe **C** in der Abbildung in Netzwerkübersicht (Seite 1).

Portnummern (Browser – Priva Cloud)

Die nachstehende Tabelle beinhaltet die Portnummer, die für die Kommunikation zwischen dem Browser der Priva Digital Services-Benutzer und der Priva Cloud erforderlich sind.

Port	Details	Transport-protokoll	
443	HTTPS, WSS[1]	TCP	

[1] WSS steht für WebSocket Secure. Im Gegensatz zu HTTP ermöglicht das WebSocket-Protokoll eine Vollduplex-Kommunikation zwischen Browsern und der Priva Cloud (die zum Erhalten von Echtzeitwerten ohne HTTP-Abfrage verwendet wird).

 = ein- und abgehend

FQDNs (Browser – Priva Cloud)

Die nachstehende Tabelle beinhaltet die Fully Qualified Domain Names (FQDN), die für die Kommunikation zwischen dem Browser der Priva Digital Services-Benutzer und der Priva Cloud erforderlich sind. Die Tabelle zeigt nur die Wildcards (mit * beginnende Adressen).

FQDNs: vom Browser zur Cloud

FQDN Wildcard	Service/Dienst
***.priva.com** (HTTPS, WSS[1])	Priva Digital Services
***.erbis.one** (HTTPS, WSS[1])	Energy Insight by ErbisOne

[1] WSS steht für WebSocket Secure. Im Gegensatz zu HTTP ermöglicht das WebSocket-Protokoll eine Vollduplex-Kommunikation zwischen Browsern und der Priva Cloud (die zum Erhalten von Echtzeitwerten ohne HTTP-Abfrage verwendet wird).

Internetverbindung

Alle Priva Digital Services erfordern eine Breitband-Internetverbindung mit einer Upload- und Download-Geschwindigkeit von mindestens 1 Mbit/s.

Spezifikationen Kommunikation Priva Blue ID

Ethernet	
Verwendeter Netzwerkstandard	IEEE 802.3 (37 ... 57 V DC) 10BASE-T (10 Mbit/s) 100BASE-TX (100 Mbit/s) Autonegotiation Auto-MDIX IPv4
DHCP	nicht unterstützt
Übertragungsrate	10 Mbit/s und 100 Mbit/s
Anschluss von Geräten von Drittanbietern zulässig	Ja
Vorgeschriebener Kabeltyp	UTP oder STP, mindestens Kategorie 5e
Maximale Kabellänge	100 m
Anschlusstyp	RJ45

Power over Ethernet ist nur bei der Priva Blue ID S-Line anwendbar.

Power over Ethernet (Stromversorgung über Ethernet)	
Verwendeter Netzwerkstandard	IEEE 802.3af (37 ... 57 V DC) Powered Device (PD) Klasse 0

Kabel (Priva Blue ID S-Line)

Modul	Technische Daten des zu verwendenden Kabels
Priva Blue ID S-Line SN1 Netzwerkmodul, Priva Blue ID S-Line SN2 Netzwerkmodul und Priva Blue ID S-Line SN3 Netzwerkmodul	• Typ: UTP oder STP, mindestens Kategorie 5e • maximale Länge: 100 m • Verbindertyp: RJ45
Priva Blue ID S-Line SN3t Netzwerkmodul mit 2-Draht *Das SN3t Modul ist nicht mehr lieferbar. Für 2-Draht können Sie das ORing Netzwerkmodul verwenden.*	Neben dem oben aufgeführten Kabel kann folgendes Kabel verwendet werden: • Typ: Twisted-Pair-Kabel (Telefon- oder Datenkabel) • Aderquerschnitt: 0,2 ... 2,5 mm² (ohne Aderendhülse) 0,25 ... 2,5 mm² (mit Aderendhülse) • maximale Kabellänge zwischen zwei Controllern: 500 m (Nennwert)[1] • maximale Gesamtlänge: 1000 m (Nennwert)[1] • Verbindertyp: zweipoliger Schraubverbinder (polaritätsneutraler Anschluss)
ORing Netzwerkmodul	• 2-Draht (Telefon- oder Datenkabel) CAT5/6 ist ebenfalls zulässig • maximale Kabellänge zwischen zwei ORing Modulen: 500 m • Verbindertyp: 2-polige Federkraftklemme (polaritätsneutraler Anschluss)
Priva Blue ID TouchPoint	• Typ: UTP oder STP, mindestens Kategorie 5e • maximale Länge: 100 m • Verbindertyp: RJ45

[1] Die maximale Kabellänge beruht auf Testergebnissen mit Twisted-Pair-Kabeln der Kategorie 5e und Alpha Wire 5261C. Bei anderen Kabelarten ist die maximale Länge möglicherweise kürzer.

Kabel (Priva Blue ID C-Line)

Modul	Technische Daten des zu verwendenden Kabels
Priva Blue ID C4 C-MX34(m) – Ethernet	• Typ: UTP oder STP, mindestens Kategorie 5e • maximale Länge: 100 m • Verbindertyp: RJ45
ORing Netzwerkmodul	• 2-Draht (Telefon- oder Datenkabel) CAT5/6 ist ebenfalls zulässig • maximale Kabellänge zwischen zwei ORing Modulen: 500 m • Verbindertyp: 2-polige Federkraftklemme (polaritätsneutraler Anschluss)
Priva Blue ID TouchPoint	• Typ: UTP oder STP, mindestens Kategorie 5e • maximale Länge: 100 m • Verbindertyp: RJ45

Spezifikationen Kommunikation Compri HX

Ethernet-Anschluss (nur Compri HX 6E/8E)	
Unterstützte Netzwerkklassen	A, B und C
Übertragungsrate	10 Mbit/s
Netzwerktyp	10BASE-T gemäß IEEE 802.3
NE2000-kompatibel	Ja
Steckverbindertyp	RJ45
Kabeltyp	UTP oder STP, mindestens Kategorie 5e
Maximale Kabellänge	100 m
Anschließen bei eingeschaltetem Compri HX	Zulässig

Kabel (Compri HX 3/4/6E/8E)

RS232-Anschluss	
Maximale Übertragungsrate	38,4 kBit/s
Steckverbindertyp	RJ45 gemäß EIA-561
Anschließen bei eingeschaltetem Compri HX	Zulässig

Priva (Hauptsitz)
Zijlweg 3
2678 LC De Lier
Die Niederlande

Unter www.priva.com finden Sie die Kontaktinformationen eines Priva Büros oder Partners für Ihre Region.