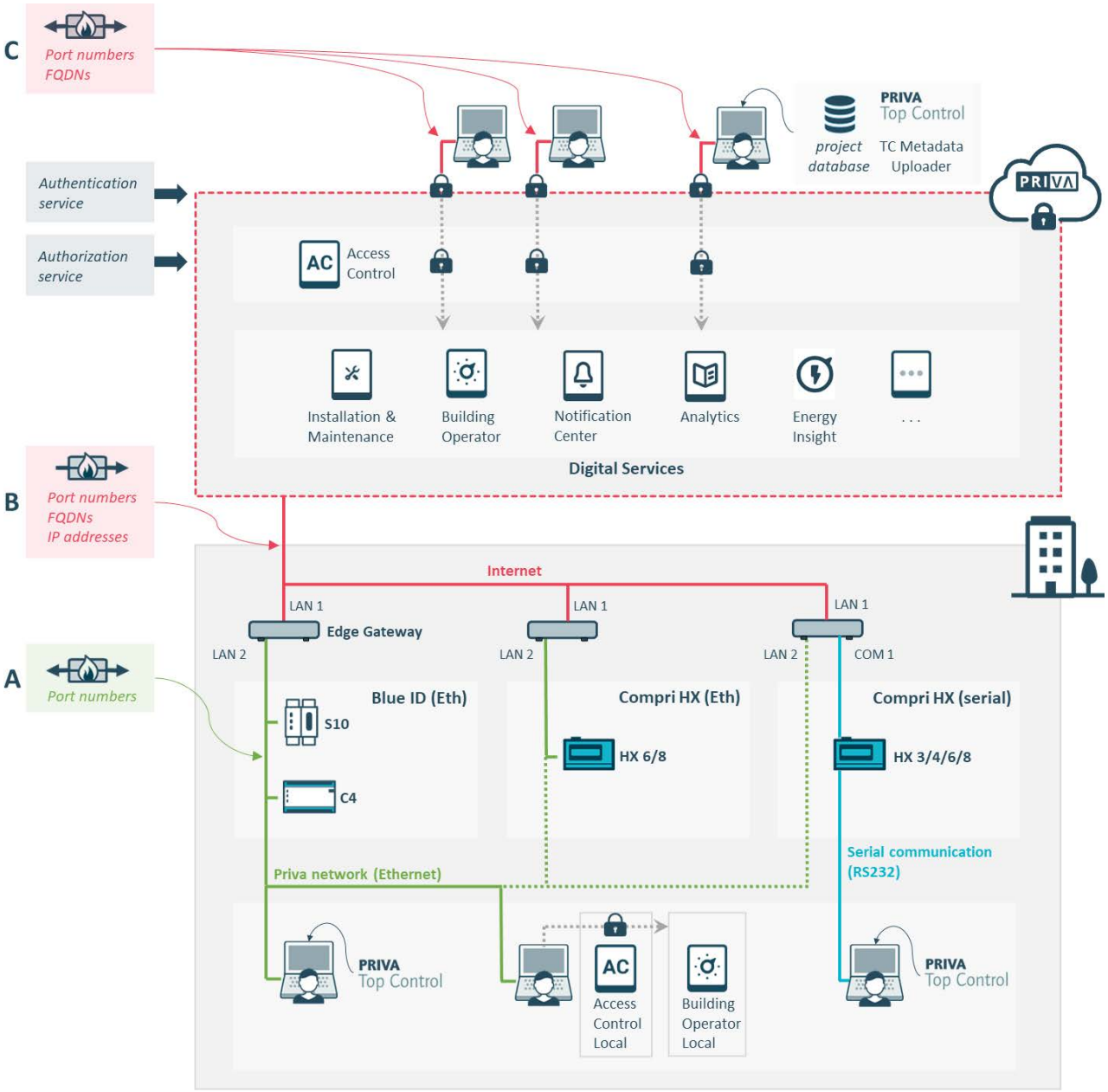
> ICT-INFORMATIE

Priva Blue ID, Top Control, Digital Services

Hoe beschermt Priva de data van uw gebouw? En wat moet u doen om communicatie tussen de Priva hardware en software op een veilige manier mogelijk te maken?

Netwerkoverzicht

De afbeelding toont de aangeraden netwerkconfiguratie waarbij het Priva-netwerk gescheiden is van het internet. Houd er rekening mee dat het veiligheidsrisico's met zich meebrengt als het Priva-netwerk niet van het internet gescheiden is.



A Zie: A) Communicatie binnen het lokale netwerk (pag. 3)

B Zie: B) Communicatie tussen gateway en Priva Cloud (pag. 5)

C Zie: C) Communicatie tussen browsers en Priva Cloud (pag. 8)

Functie Edge Gateway / Cloud Connector

Gebouwbeheersystemen mogen nooit op een netwerk met internettoegang draaien. Om cloud services te kunnen gebruiken, is natuurlijk wel communicatie tussen het beheersysteem en de Priva Cloud nodig. De Edge Gateway en de Cloud Connector zijn gateways die dit op een veilige manier mogelijk maken. De Edge Gateway is de opvolger van de Cloud Connector.

De gateway staat alleen uitgaande verbindingen toe. Zo beschermt het het gebouwbeheersysteem tegen toegang door onbevoegden via het internet. Inkomende verbindingen staat de gateway niet toe. Als de gateway de verbinding naar buiten toe opzet, zal inkomend verkeer binnen die actieve sessie wel worden toegestaan. Dit maakt het mogelijk om met een applicatie/dienst van buitenaf waarden aan te passen.

De data die wordt overgedragen tussen de gateway en de cloud is beveiligd aan de hand van versleuteling. In tegenstelling tot andere methoden voor toegang tot gebouwautomatiseringssystemen, zoals een VPN, maakt deze architectuur gebruik van een systeem op basis van berichten, dus is er geen volledige datalink tussen het gebouw en de buitenwereld. Er wordt slechts in heel beperkte mate data uitgewisseld.

Updates van Windows 10 IoT op de Cloud Connector worden automatisch gedownload en geïnstalleerd volgens het standaard Windows Update machanisme. Er wordt geen herstart geforceerd binnen de standaard actieve uren van de Cloud Connector (8.00-17.00 uur).

Updates van Linux op de Edge Gateway worden uitgevoerd in Installation & Maintenance (module FirmwareUpdater).

Support van Priva

Priva kan eenvoudig support op afstand leveren via TeamViewer op de Cloud Connector. Hiervoor moet poort 5938 open staan.

Bij de Edge Gateway is support via TeamViewer niet van toepassing omdat deze gateway extern niet direct benaderbaar is.

Beveiligingsmaatregelen van Microsoft

Alle Digital Services zijn vormgegeven op basis van het cloudplatform van Microsoft Azure. De services van Priva maken gebruik van de standaardcomponenten IoT-hub en Service Bus van Microsoft Azure voor de communicatie tussen het Priva-netwerk en de cloud. Gedetailleerde informatie over de beveiliging van Microsoft vindt u in het Microsoft Trust Center.

A) Communicatie binnen het lokale netwerk

Om de communicatie binnen het lokale netwerk mogelijk te maken, moeten specifieke poorten open staan in de firewall (indien een firewall aanwezig is).

Zie **A** in de afbeelding in Netwerkoverzicht (pag. 1).

Poortnummers (communicatie binnen lokale netwerk)

In de tabel hieronder staan de poortnummers die nodig zijn voor de communicatie tussen de Priva Blue ID/Compri HX-hardware en Top Control-applicaties en de Cloud Connector of Edge Gateway. Ook staat hierin aangegeven of de poorten gebruik maken van ingaande of uitgaande communicatie. De configuratie van de poorten in de firewall is afhankelijk van de gebruikte Top Control-applicaties en de gemaakte netwerkconfiguratie in het project.

Poort	Details	Transport-protocol	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
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	
7661	DDS	UDP									→ 10	

Poort	Details	Transport-protocol	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
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 t/m 47817[16]	BACnet [6]	UDP	←									

← = ingaand
→ = uitgaand
↔ = in- en uitgaand

[1] Alleen online help

[2] Standaard poortnummer, kan gewijzigd worden

[3] Bij lokaal communiceren

[4] TC LAN Manager zoekt een vrij te gebruiken poortnummer

[5] Priva-eigen protocol

[6] Gereserveerde poorten, instelbaar in TC Engineer

[7] Bij gebruik van een Compri HX connectie

[8] Alleen SNMP Trap wordt ondersteund in Top Control 8

[9] LAN-poort aangesloten op internet
(Edge Gateway: LAN 1, Cloud Connector: LAN 3)

[10] LAN-poort aangesloten op Priva-netwerk
(Edge Gateway: LAN 2, Cloud Connector: LAN 1)

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

[12] Local Operator Authorization Service

[13] Local Operator User Management UI

[14] Local Operator UI

[15] Local Operator API

[16] Kies één van de genoemde poortnummers

[17] Kies één van de genoemde poortnummers. De gekozen poortnummers uit de twee rijen met opmerking 17 moeten elkaar opvolgen (bijv. 23456 en 23457).

B) Communicatie tussen gateway en Priva Cloud

Om de communicatie tussen de gateway en de Priva Cloud mogelijk te maken, moeten specifieke poorten open staan in de firewall. Daarnaast moet de communicatie met de Priva Cloud toegestaan worden op basis van FQDN's of op basis van IP-adressen.

Zie **B** in de afbeelding in Netwerkoverzicht (pag. 1).

Poortnummers (gateway - Priva Cloud)

In de tabel hieronder staan de poortnummers die nodig zijn voor communicatie tussen de gateway en de Priva Cloud. Alle poorten maken alleen gebruik van uitgaande communicatie. Poort 5938 is nodig voor support van Priva met TeamViewer (alleen op de Cloud Connector).

Poort	Details	Transport-protocol	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]

→ = uitgaand

[1] LAN-poort aangesloten op internet
(Edge Gateway: LAN 1, Cloud Connector: LAN 3)

FQDN's (gateway - Priva Cloud)

In de tabellen hieronder staan de Fully Qualified Domain Names (FQDN) weergegeven die nodig zijn voor communicatie tussen de gateway en de Priva Cloud. U heeft de keus om wildcards (adressen startende met *) te gebruiken of de volledige FQDN's vrij te geven. De lijst van volledige FQDN's is echter wel dynamisch; er kunnen in de toekomst FQDN's toegevoegd worden en ze kunnen gewijzigd worden. Het gebruik van wildcards is meer onderhoudsvriendelijk omdat de lijst van wildcards minder vaak zal wijzigen dan de lijst van volledige FQDN's.

We raden aan om ten minste de wildcard *.priva.com te whitelisten omwille van toekomstige ontwikkelingen.

FQDN's: van Edge Gateway naar cloud

FQDN	Service
***.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
***.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)	
Landsafhankelijk, bijv.: 0.nl.pool.ntp.org	NTP-server
Overige	
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] Services van de gateway (configuratie van de gateway, gateway updates, authorisatie, metadata, ...)

[2] Bij het uitvoeren van de connectivity check (in de lokale configuratieapplicatie) zal aka.ms omleiden naar andere endpoints: raw.githubusercontent.com/* (aan verandering onderhevig).

FQDN's: van Cloud Connector naar cloud

FQDN	Service
***.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 *(verouderd)*	Gateway services[1]
connect.priva.com *(verouderd)*	Gateway services[1]
gps.priva.com	Gateway services[1]
state.priva.com	Gateway services[1]
tenantapi.priva.com	Gateway services[1]
Overige	
prdinstallupdatesa.blob.core.windows.net (HTTPS)	Gateway services[1]

[1] Services van de gateway (configuratie van de gateway, gateway updates, authorisatie, metadata, ...)

IP-adressen (gateway - Priva Cloud)

Priva gebruikt de "EuropeWest" en "EuropeNorth" IP-adresreeksen van Microsoft die nodig zijn voor Priva Digital Services. Deze reeksen worden dynamisch gebruikt door Microsoft en kunnen daarom niet specifiek genoemd worden. De reeksen die Microsoft gebruikt, zijn te vinden op hun website: ga naar https://www.microsoft.com/en-us/download/details.aspx?id=56519 en download het json-bestand.

Dit bestand wordt wekelijks bijgewerkt. Nieuwe reeksen die in het bestand worden toegevoegd, worden gedurende ten minste één week niet gebruikt in Azure. Indien u gebruik maakt van de IP-adres beperkingslijst, download dan elke week het nieuwe json-bestand en voer de nodige wijzigingen uit op uw locatie om diensten die in Azure worden uitgevoerd correct te identificeren.

Maak geen gebruik van IP-adresreeks 172.23.105.0/24. Deze reeks wordt namelijk al intern in de Edge Gateway gebruikt.

Internetverbinding

Alle Priva Digital Services vereisen een breedband-internetverbinding met een minimale upload- en downloadsnelheid van 1 Mbps.

C) Communicatie tussen browsers en Priva Cloud

Om de communicatie tussen de browsers van de Priva Digital Services-gebruikers en de Priva Cloud mogelijk te maken, moet poort 443 open staan in de firewall en moet de communicatie met de Priva Cloud toegestaan worden op basis van FQDN's.

Zie **C** in de afbeelding in Netwerkoverzicht (pag. 1).

Poortnummers (browser - Priva Cloud)

In de tabel hieronder staat het poortnummer dat nodig is voor communicatie tussen de browsers van de Priva Digital Services-gebruikers en de Priva Cloud.

Poort	Details	Transport-protocol	
443	HTTPS, WSS[1]	TCP	

[1] WSS staat voor WebSocket Secure. In tegenstelling tot HTTP maakt het WebSocket-protocol full-duplex communicatie mogelijk tussen browsers en de Priva Cloud (die wordt gebruikt om real-time waarden te verkrijgen zonder HTTP-polling).

 = in- en uitgaand

FQDN's (browser - Priva Cloud)

In de tabel hieronder staan de Fully Qualified Domain Names (FQDN) weergegeven die nodig zijn voor communicatie tussen de browsers van de Priva Digital Services-gebruikers en de Priva Cloud. De tabel toont alleen de wildcards (adressen startende met *).

FQDN's: van browser naar cloud

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

[1] WSS staat voor WebSocket Secure. In tegenstelling tot HTTP maakt het WebSocket-protocol full-duplex communicatie mogelijk tussen browsers en de Priva Cloud (die wordt gebruikt om real-time waarden te verkrijgen zonder HTTP-polling).

Internetverbinding

Alle Priva Digital Services vereisen een breedband-internetverbinding met een minimale upload- en downloadsnelheid van 1 Mbps.

Specificaties communicatie Priva Blue ID

Ethernet	
Toegepaste netwerkstandaard	IEEE 802.3 (37 ... 57 Vdc) 10BASE-T (10 Mbps) 100BASE-TX (100 Mbps) auto negotiation auto-MDIX IPv4
DHCP	niet ondersteund
Transmissiesnelheid	10 Mbps en 100 Mbps
Aansluiten apparatuur van derden toegestaan	ja
Vereist kabeltype	UTP of STP, minimaal categorie 5E
Maximale kabellengte	100 m
Connectortype	RJ45

Power over Ethernet is alleen van toepassing op Priva Blue ID S-Lijn.

Power over Ethernet	
Toegepaste netwerkstandaard	IEEE 802.3af (37 ... 57 Vdc) Powered Device (PD) Class 0

Kabels (Priva Blue ID S-Lijn)

Module	Specificaties toe te passen kabel
Priva Blue ID S-Lijn SN1 Netwerkmodule, Priva Blue ID S-Lijn SN2 Netwerkmodule en Priva Blue ID S-Lijn SN3 Netwerkmodule	• type: UTP of STP, minimaal categorie 5E • maximale lengte: 100 m • connectortype: RJ45
Priva Blue ID S-Lijn SN3t Netwerkmodule *De SN3t-module wordt niet meer geleverd. U kunt de ORing Netwerkmodule gebruiken voor 2-wire.*	Naast de hierboven genoemde kabel kan de volgende kabel toegepast worden: • type: twisted pair (telefoon- of datakabel) • aderdoorsnede: 0,2 ... 2,5 mm² zonder adereindhuls 0,25 ... 2,5 mm² met adereindhuls • maximale lengte tussen twee controllers: 500 m nominaal[1] • maximale totale lengte: 1000 m nominaal[1] • connectortype: tweepolige schroefconnector (aansluiting polariteitsongevoelig)
ORing Netwerkmodule	• 2-draads (telefoon- of datakabel) CAT5/6 is ook toegestaan • maximale kabellengte tussen twee ORing-modules: 500 m • connectortype: 2-pins veerdrukklem (aansluiting polariteitsongevoelig)
Priva Blue ID TouchPoint	• type: UTP of STP, minimaal categorie 5E • maximale lengte: 100 m • connectortype: RJ45

[1] De maximale kabellengte is gebaseerd op testresultaten met twisted-pairkabel categorie 5E en Alpha Wire 5261C; bij andere kabeltypen is de maximale lengte mogelijk kleiner.

Kabels (Priva Blue ID C-Lijn)

Module	Specificaties toe te passen kabel
Priva Blue ID C4 C-MX34(m) - ethernet	• type: UTP of STP, minimaal categorie 5E • maximale lengte: 100 m • connectortype: RJ45
ORing Netwerkmodule	• 2-draads (telefoon- of datakabel) CAT5/6 is ook toegestaan • maximale kabellengte tussen twee ORing-modules: 500 m • connectortype: 2-pins veerdrukklem (aansluiting polariteitsongevoelig)
Priva Blue ID TouchPoint	• type: UTP of STP, minimaal categorie 5E • maximale lengte: 100 m • connectortype: RJ45

Specificaties communicatie Compri HX

Aansluiting Ethernet (alleen Compri HX 6E/8E)	
Ondersteunde netwerkklassen	A, B en C
Transmissiesnelheid	10 Mbit/sec
Netwerktype	10BASE-T volgens norm IEEE 802.3
NE2000 Compatibel	Ja
Connectortype	RJ45
Kabeltype	UTP of STP, minimaal categorie 5E
Maximale kabellengte	100 m
Aansluiten met ingeschakelde Compri HX	Toegestaan

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

Aansluiting RS232	
Maximale transmissiesnelheid	38k4 bps
Connectortype	RJ45 volgens EIA-561
Aansluiten met ingeschakelde Compri HX	Toegestaan

Priva (hoofdkantoor)
Zijlweg 3
2678 LC De Lier
Nederland

Zie www.priva.com voor contactgegevens van een Priva kantoor of partner voor uw regio.