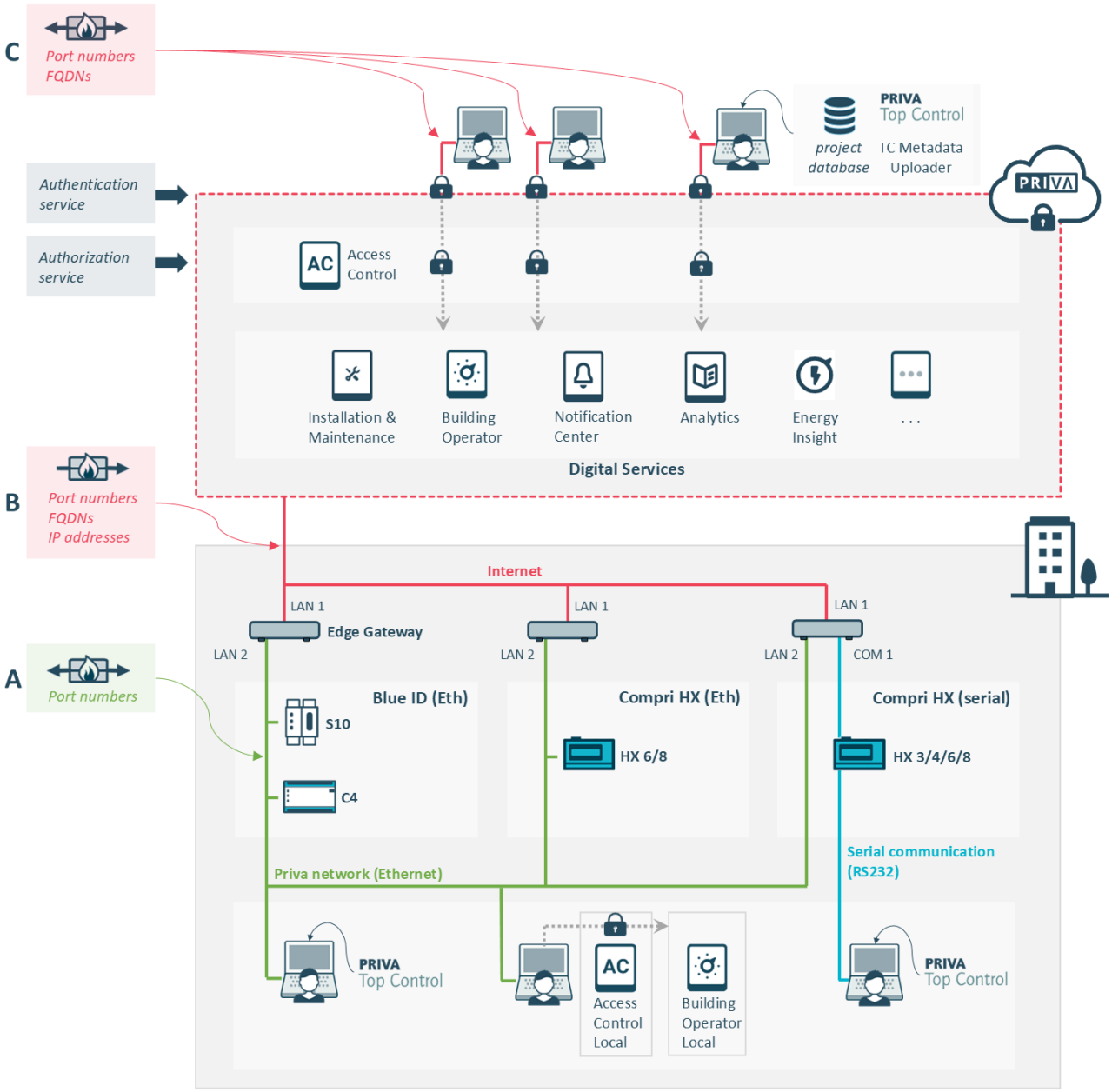
> INFORMATION DE TIC

Priva Blue ID, Top Control, Digital Services

Comment Priva protège-t-il les données de votre bâtiment ? Et que devez-vous faire pour permettre la communication entre le matériel et le logiciel Priva de manière sécurisée ?

Aperçu du réseau

L'illustration montre la configuration de réseau recommandée, où le réseau Priva est séparé de l'Internet. Tenez compte du fait que si le réseau Priva n'est pas séparé de l'Internet, l'installation court des risques de sécurité.



A Voir : A) Communication à l'intérieur du réseau local (page 3)

B Voir : B) Communication entre la passerelle et le Priva Cloud (page 5)

C Voir : C) Communication entre navigateurs et Priva Cloud (page 8)

Fonction Edge Gateway / Cloud Connector

Les systèmes de gestion de bâtiment ne doivent jamais fonctionner sur un réseau avec accès à Internet. Mais pour pouvoir utiliser des services cloud, il faut naturellement qu'une communication soit établie entre le système de gestion et le Priva Cloud. Le Edge Gateway et le Cloud Connector sont des passerelles qui le permettent de manière sécurisée. Edge Gateway est le successeur de Cloud Connector.

La passerelle autorise uniquement les connexions sortantes. Elle protège ainsi le système de gestion de bâtiment contre tout accès non autorisé via Internet. La passerelle n'autorise pas les connexions entrantes. Lorsque la passerelle établit la connexion vers l'extérieur, un trafic entrant sera toutefois autorisé dans le cadre de cette session active. Ceci permet de modifier des valeurs de l'extérieur à l'aide d'une application ou d'un service.

Les données transférées entre la passerelle et le cloud sont sécurisées par cryptage. Contrairement à d'autres méthodes d'accès aux systèmes d'automatisation du bâtiment, tels qu'un VPN, cette architecture utilise un système basé sur des messages, il n'y a donc pas de lien de données complet entre le bâtiment et le monde extérieur. Seule une quantité très limitée de données est échangée.

Les mises à jour de Windows 10 IoT sur le Cloud Connector sont automatiquement téléchargées et installées selon le mécanisme standard de Windows Update. Aucun redémarrage n'est forcé pendant les heures d'activité standard du Cloud Connector (8h00-17h00).

Les mises à jour de Linux sur le Edge Gateway sont effectuées dans Installation & Maintenance (module FirmwareUpdater).

Support de Priva

En cas d'utilisation du Cloud Connector, Priva peut fournir du support à distance simplement via TeamViewer. Le port 5938 doit être ouvert à cet effet.

En cas d'utilisation du Edge Gateway, Priva peut fournir du support à distance via Remote Monitor. Remote Monitor est disponible à partir de la version de firmware 2.13.1. Pour Remote Monitor, aucun port supplémentaire ne doit être ouvert, la communication se fait via HTTPS et WebSocket Secure (WSS) (port 443). Cependant, le FQDN edge-status.priva.com est nécessaire.

Qu'est-ce que Remote Monitor ?

Remote Monitor est un service de Priva qui est constitué de deux composants :

- service qui tourne sur le Edge Gateway,
- serveur dans Microsoft Azure.

Remote Monitor a deux fonctions :

- Priva peut voir quelles passerelles sont en ligne. La passerelle envoie périodiquement un message au serveur via une API. Cette API renvoie une liste de toutes les passerelles en ligne et des passerelles qui étaient auparavant en ligne mais qui sont actuellement hors ligne.
- Priva peut fournir du support pour votre passerelle via une connexion SSH cryptée.

La communication avec la passerelle est entièrement sécurisée et protégée :

- La communication entre la passerelle et le cloud est initiée par la passerelle.
- Toutes les communications sont sécurisées via TLS.
- Les passerelles ont besoin d'un certificat client qui est émis par Priva pour s'authentifier avec le serveur cloud. De cette manière, seules de vraies Edge Gateways Priva peuvent se connecter avec le serveur.
- Toutes les communications sont protégées par des mots de passe et des jetons spécifiques à chaque passerelle, qui sont uniquement accessibles à des collaborateurs spécifiques de Priva.
- Les mots de passe et les jetons sont générés par Azure KeyVault.

Remote Monitor tourne comme un service distinct, indépendant d'IoT Edge, et continue donc de fonctionner en cas de problèmes avec IoT Edge.

Mesures de protection de Microsoft

Tous les Digital Services s'appuient sur la plateforme de cloud de Microsoft Azure. Les services de Priva utilisent les composants standard IoT-hub et Service Bus de Microsoft Azure pour la communication entre le réseau Priva et le cloud. Les informations détaillées de protection de Microsoft sont disponibles dans le Microsoft Trust Center.

A) Communication à l'intérieur du réseau local

Pour permettre la communication au sein du réseau local, des ports spécifiques doivent être ouverts dans le pare-feu (si un pare-feu est présent).

Voir **A** dans l'illustration de Aperçu du réseau (page 1).

Numéros de port (communication au sein du réseau local)

Le tableau ci-dessous indique les numéros de port requis pour la communication entre le matériel Priva Blue ID/Compri HX et les applications Top Control et le Cloud Connector ou Edge Gateway. Celui-ci précise également si les ports utilisent une communication entrante ou sortante. La configuration des ports dans le pare-feu dépend des applications Top Control utilisées et de la configuration du réseau créée dans le projet.

Port	Détails	Protocole transport	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	

Port	Détails	Protocole transport	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	←									

↔ = entrant
↔ = sortant
↔ = entrant et sortant

[1] Aide en ligne uniquement

[2] Numéro de port standard, peut être modifié

[3] Lors de la communication locale

[4] TC LAN Manager recherche un numéro de port libre

[5] Protocole propre à Priva

[6] Ports réservés, réglables en TC Engineer

[7] En cas d'utilisation d'une connexion Compri HX

[8] Seul SNMP Trap est supporté dans Top Control 8

[9] Port LAN connecté à internet
(Edge Gateway : LAN 1, Cloud Connector : LAN 3)

[10] Port LAN connecté au réseau Priva
(Edge Gateway : LAN 2, Cloud Connector : LAN 1)

[11] Port de service
(Edge Gateway : LAN 3, Cloud Connector : LAN 2)

[12] Service d'autorisation d'opérateurs locaux

[13] IU de gestion des opérateurs locaux

[14] IU des opérateurs locaux

[15] API des opérateurs locaux

[16] Composez l'un des numéros de port répertoriés

[17] Composez l'un des numéros de port répertoriés. Les numéros de port sélectionnés dans les deux lignes de la remarque 17 doivent se suivre (p. ex. 23456 et 23457).

B) Communication entre la passerelle et le Priva Cloud

Pour permettre la communication entre la passerelle et le Priva Cloud, il faut que certains ports spécifiques soient ouverts dans le pare-feu. Il convient en outre d'autoriser la communication avec le Priva Cloud sur la base des noms de domaine FQDN ou sur la base des adresses IP.

Voir **B** dans l'illustration de Aperçu du réseau (page 1).

Numéros de ports (passerelle - Priva Cloud)

Le tableau ci-dessous reprend les numéros de port nécessaires dans le cadre de la communication entre la passerelle et le Priva Cloud. Tous les ports utilisent uniquement la communication sortante. Le port 5938 est nécessaire pour l'assistance Priva avec TeamViewer (uniquement sur le Cloud Connector).

Port	Détails	Protocole transport	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]

 = sortant

[1] Port LAN connecté à internet
(Edge Gateway : LAN 1, Cloud Connector : LAN 3)

FQDN (passerelle - Priva Cloud)

Les tableaux suivants reprennent les noms de domaines complets (Fully Qualified Domain Names ou FQDN) nécessaires dans le cadre de la communication entre la passerelle et le Priva Cloud. Vous avez la possibilité d'utiliser des adresses génériques (adresses commençant par *) ou d'indiquer le FQDN complet. La liste des noms de domaines complets est dynamique ; il est possible d'y ajouter des FQDN ultérieurement et de les modifier. L'utilisation d'adresses génériques facilite la maintenance du fait qu'une liste comportant des adresses génériques changera moins souvent qu'une liste de FQDN complets.

Nous recommandons de mettre sur liste blanche au moins le adresse générique *.priva.com pour des raisons de développement futur.

FQDN : depuis Edge Gateway vers le 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]
prdfileuploadersa.blob.core.windows.net	Gateway services[1]

FQDN	Service
prdhdptsgwtelemetrysa.blob.core.windows.net	Cloud History
prdprivaauditlogs.blob.core.windows.net	Gateway services[1]
***.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]
edge-status.priva.com (HTTPS, WSS)	Gateway service Remote Monitor
local-auth-provisioning.priva.com	Gateway services[1]
***.pool.ntp.org** (NTP)	
Dépend du pays, par exemple : 0.fr.pool.ntp.org	Serveur NTP
***.oms.opinsights.azure.com** (HTTPS)	Gateway services[1]
Autres	
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]
westeurope.data.mcr.microsoft.com (HTTPS)	Gateway services[1]

[1] Services de la passerelle (configuration de la passerelle, mises à jour de la passerelle, autorisation, métadonnées,...)

[2] Lors de l'exécution de la vérification de la connectivité (dans l'application de configuration locale), aka.ms redirigera vers d'autres endpoints : raw.githubusercontent.com/* (sous réserve de modification).

FQDN : depuis Cloud Connector vers le 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 *(obsolète)*	Gateway services[1]
connect.priva.com *(obsolète)*	Gateway services[1]
gps.priva.com	Gateway services[1]
state.priva.com	Gateway services[1]
tenantapi.priva.com	Gateway services[1]
Autres	
prdinstallupdatesa.blob.core.windows.net (HTTPS)	Gateway services[1]

[1] Services de la passerelle (configuration de la passerelle, mises à jour de la passerelle, autorisation, métadonnées,...)

Adresses IP (passerelle - Priva Cloud)

Priva utilise les séries d'adresses IP "EuropeWest" et "EuropeNorth" de Microsoft requises pour les Priva Digital Services. Ces séries sont utilisées de manière dynamique par Microsoft et ne peuvent donc pas être mentionnées spécifiquement. Les séries utilisées par Microsoft sont disponibles sur leur site Web : rendez-vous sur https://www.microsoft.com/en-us/download/details.aspx?id=56519 et téléchargez le fichier json.

Ce fichier est actualisé chaque semaine. Les nouvelles séries ajoutées au fichier ne sont pas utilisées dans Azure pendant au moins une semaine. Si vous utilisez la liste de limitations d'adresses IP, téléchargez chaque semaine le nouveau fichier json et effectuez les modifications nécessaires sur votre site pour identifier correctement les services exécutés dans Azure.

N'utilisez pas la plage d'adresses 172.23.105.0/24. Cette plage est déjà utilisée en interne dans la Edge Gateway.

Connexion Internet

Tous les Priva Digital Services nécessitent une connexion Internet à haut débit avec une vitesse d'au moins 1 Mbps en liaison montante et en liaison descendante.

C) Communication entre navigateurs et Priva Cloud

Pour permettre la communication entre les navigateurs des utilisateurs de Priva Digital Services et le Priva Cloud, il faut que le port 443 soit ouvert dans le pare-feu et que la communication avec le Priva Cloud soit autorisée sur la base des FQDN.

Voir **C** sur l'illustration dans Aperçu du réseau (page 1).

Numéros de ports (navigateur - Priva Cloud)

Le tableau suivant reprend le numéro de port qui est nécessaire dans le cadre de la communication entre les navigateurs des utilisateurs de Priva Digital Services et le Priva Cloud.

Port	Détails	Protocole de transport	
443	HTTPS, WSS[1]	TCP	

[1] WSS signifie WebSocket Secure. Contrairement au protocole HTTP, le protocole WebSocket permet une communication en duplex intégral entre les navigateurs et le Priva Cloud (qui est utilisé pour obtenir des valeurs en temps réel sans polling HTTP).

 = entrant et sortant

FQDN (navigateur - Priva Cloud)

Le tableau suivant reprend les noms de domaines complets (Fully Qualified Domain Names ou FQDN) nécessaires dans le cadre de la communication entre les navigateurs des utilisateurs de Priva Digital Services et le Priva Cloud. Le tableau montre uniquement les parties génériques (adresses commençant par *).

FQDN : du navigateur vers le cloud

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

[1] WSS signifie WebSocket Secure. Contrairement au protocole HTTP, le protocole WebSocket permet une communication en duplex intégral entre les navigateurs et le Priva Cloud (qui est utilisé pour obtenir des valeurs en temps réel sans polling HTTP).

Connexion Internet

Tous les Priva Digital Services nécessitent une connexion Internet à haut débit avec une vitesse d'au moins 1 Mbps en liaison montante et en liaison descendante.

Spécifications de la communication Priva Blue ID

Ethernet	
Norme réseau appliquée	IEEE 802.3 (37 ... 57 Vcc) 10BASE-T (10 Mbps) 100BASE-TX (100 Mbps) auto-négociation auto-MDIX IPv4
DHCP	non pris en charge
Vitesse de transmission	10 Mbps et 100 Mbps
Le raccordement d'appareils tiers est autorisé	oui
Type de câble requis	UTP ou STP, catégorie minimum 5E
Longueur de câble maximum	100 m
Type de connecteur	RJ45

Power over Ethernet s'applique uniquement sur Priva Blue ID S-Line.

Power over Ethernet	
Norme réseau appliquée	IEEE 802.3af (37 ... 57 Vcc) Powered Device (PD) Classe 0

Câbles (Priva Blue ID S-Line)

Module	Spécifications du câble à utiliser
Module de réseau Priva Blue ID S-Line SN1 , Module de réseau Priva Blue ID S-Line SN2 et Module de réseau Priva Blue ID S-Line SN3	• type : UTP ou STP, catégorie 5E minimum • longueur maximale : 100 m • type de connecteur : RJ45
Module de réseau Priva Blue ID S-Line SN3t *Le module SN3t n'est plus disponible. Vous pouvez utiliser le Module de réseau ORing pour un raccordement bifilaire.*	Outre le câble susmentionné, le câble suivant peut également être utilisé : • type : paire torsadée (câble de téléphone ou de données) • section du fil : 0,2 ... 2,5 mm² sans embout de câblage 0,25 ... 2,5 mm² avec embout de câblage • longueur maximale entre deux régulateurs : 500 m nominale[1] • longueur totale maximale : 1000 m nominale[1] • type de connecteur : connecteur à vis et à 2 broches (raccordement indépendant de la polarité)
Module de réseau ORing	• bifilaire (câble téléphonique ou de données) CAT5/6 également autorisé • longueur maximale du câble entre deux module ORings : 500 m • type de connecteur : Borne à ressort de rappel à 2 broches (raccordement indépendant de la polarité)
TouchPoint Priva Blue ID	• type : UTP ou STP, catégorie 5E minimum • longueur maximale : 100 m • type de connecteur : RJ45

[1] La longueur maximale du câble est basée sur les résultats d'essais avec un câble à paire torsadée de catégorie 5E et un Alpha Wire 5261C ; la longueur maximale pour d'autres types de câble est probablement inférieure.

Câbles (Priva Blue ID C-Line)

Module	Spécifications du câble à utiliser
Priva Blue ID C4 C-MX34(m) - Ethernet	• type : UTP ou STP, catégorie 5E minimum • longueur maximale : 100 m • type de connecteur : RJ45
Module de réseau ORing	• bifilaire (câble téléphonique ou de données) CAT5/6 également autorisé • longueur maximale du câble entre deux module ORings : 500 m • type de connecteur : Borne à ressort de rappel à 2 broches (raccordement indépendant de la polarité)
TouchPoint Priva Blue ID	• type : UTP ou STP, catégorie 5E minimum • longueur maximale : 100 m • type de connecteur : RJ45

Spécifications de la communication Compri HX

Connexion Ethernet (uniquement Compri HX 6E/8E)	
Classes de réseau supportées	A, B et C
Vitesse de transmission	10 Mbit/s
Type de réseau	10BASE-T selon la norme IEEE 802.3
Compatible NE2000	Oui
Type de connecteur	RJ45
Type de câble	UTP ou STP, catégorie minimum 5E
Longueur de câble maximum	100 m
Raccordement avec Compri HX activé	Autorisé

Câbles (Compri HX 3/4/6E/8E)

Raccordement du RS232	
Vitesse maximale de transmission	38k4 bps
Type de connecteur	RJ45 d'après EIA-561
Raccordement avec Compri HX activé	Autorisé

Priva (siège social)
Zijlweg 3
2678 LC De Lier
Pays-Bas

Pour contacter l'équipe Priva ou l'un de nos partenaires dans votre secteur, vous pouvez vous rendre sur le site web www.priva.com