



Simons  Voss



SmartBridge

Handbuch

08.08.2022

Simons  Voss
technologies

Inhaltsverzeichnis

1	Allgemein	3
2	Allgemeine Sicherheitshinweise.....	4
3	Produktspezifische Sicherheitshinweise	7
4	Bedeutung der Textformatierung.....	8
5	Lieferumfang.....	9
5.1	Zubehör	9
6	Anschlüsse.....	10
7	Montage.....	11
7.1	SmartBridges aufstellen.....	14
7.1.1	Eine SmartBridge	14
7.1.2	Zwei oder mehrere SmartBridges.....	14
7.2	Antenne.....	15
8	Inbetriebnahme.....	17
8.1	SmartBridge in MobileKey.....	17
8.1.1	SmartBridges einrichten	17
8.1.2	SmartBridges löschen	19
9	Browserschnittstelle	20
10	Wartung.....	25
11	Signalisierung.....	26
12	Fehlerbehebung	27
12.1	Zurücksetzen	27
13	Technische Daten.....	29
13.1	Optionale externe Antenne	31
13.1.1	Elektrische Spezifikationen	31
13.1.2	Anschluss-Spezifikationen.....	31
13.1.3	Mechanische Spezifikationen und Abmessungen.....	31
14	Konformitätserklärung	33
15	Hilfe und weitere Informationen.....	34

1 Allgemein

Mit der SmartBridge können Sie die netzwerkfähigen Komponenten des MobileKey-Systems drahtlos verwalten und programmieren:

- Programmieren Sie aus der Ferne. Sie müssen nicht mehr lokal zur Schließung gehen, sondern können die Änderungen an den Komponenten über das WaveNet direkt programmieren.
- Lesen Sie aus der Ferne die Zutrittslisten aus. Wenn Sie viele Schließungen mit Zutrittsprotokoll haben, dann sparen Sie viel Zeit, indem Sie zentral alle Schließungen auslesen können.
- Führen Sie Notöffnungen durch. Gestatten Sie Benutzern den Zutritt, ohne die jeweilige Schließung aufsuchen zu müssen.



HINWEIS

Kompatibilität zu MobileKey

Das Gerät wird mit anderer Firmware auch in anderen Produktfamilien verwendet. Sie können das Gerät mit dieser Firmware (=SmartBridge) nur für MobileKey verwenden.

- Prüfen Sie die Artikelnummer.
- ↳ Wenn die Artikelnummer MK.SMARTBRIDGE lautet, dann handelt es sich um eine SmartBridge.

2 Allgemeine Sicherheitshinweise

Signalwort (ANSI Z535.6)	Mögliche unmittelbare Auswirkungen bei Nichtbeachtung
Gefahr	Tod oder schwere Verletzung (wahrscheinlich)
Warnung	Tod oder schwere Verletzung (möglich, aber unwahrscheinlich)
Vorsicht	Leichte Verletzung
Achtung	Sachschäden oder Fehlfunktionen
Hinweis	Geringe oder keine



WARNUNG

Versperrter Zugang

Durch fehlerhaft montierte und/oder programmierte Komponenten kann der Zutritt durch eine Tür versperrt bleiben. Für Folgen eines versperrten Zutritts wie Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss Technologies GmbH nicht!

Versperrter Zugang durch Manipulation des Produkts

Wenn Sie das Produkt eigenmächtig verändern, dann können Fehlfunktionen auftreten und der Zugang durch eine Tür versperrt werden.

- Verändern Sie das Produkt nur bei Bedarf und nur in der Dokumentation beschriebenen Art und Weise.

ACHTUNG

Beschädigung durch elektrostatische Entladung (ESD)

Dieses Produkt enthält elektronische Bauteile, die durch elektrostatische Entladungen beschädigt werden können.

1. Verwenden Sie ESD-gerechte Arbeitsmaterialien (z.B. Erdungsarmband).
2. Erden Sie sich vor Arbeiten, bei denen Sie mit der Elektronik in Kontakt kommen könnten. Fassen Sie dazu geerdete metallische Oberflächen an (z.B. Türzargen, Wasserrohre oder Heizungsventile).

Beschädigung durch Öle, Fette, Farben und Säuren

Dieses Produkt enthält elektronische und/oder mechanische Bauteile, die durch Flüssigkeiten aller Art beschädigt werden können.

- Halten Sie Öle, Fette, Farben und Säuren vom Produkt fern.

Beschädigung durch aggressive Reinigungsmittel

Die Oberfläche dieses Produkts kann durch ungeeignete Reinigungsmittel beschädigt werden.

- Verwenden Sie ausschließlich Reinigungsmittel, die für Kunststoff- bzw. Metalloberflächen geeignet sind.

Beschädigung durch mechanische Einwirkung

Dieses Produkt enthält elektronische Bauteile, die durch mechanische Einwirkung aller Art beschädigt werden können.

1. Vermeiden Sie das Anfassen der Elektronik.
2. Vermeiden Sie sonstige mechanische Einwirkungen auf die Elektronik.

Beschädigung durch Überstrom oder Überspannung

Dieses Produkt enthält elektronische Bauteile, die durch zu hohen Strom oder zu hohe Spannung beschädigt werden können.

- Überschreiten Sie die maximal zulässigen Spannungen und/oder Ströme nicht.

Beschädigung durch Verpolung

Dieses Produkt enthält elektronische Bauteile, die durch die Verpolung der Spannungsquelle beschädigt werden können.

- Verpolen Sie die Spannungsquelle nicht (Batterien bzw. Netzteile).

Störung des Betriebs durch Funkstörung

Dieses Produkt kann unter Umständen durch elektromagnetische oder magnetische Störungen beeinflusst werden.

- Montieren bzw. platzieren Sie das Produkt nicht unmittelbar neben Geräten, die elektromagnetische oder magnetische Störungen verursachen können (Schaltnetzteile!).

Störung der Kommunikation durch metallische Oberflächen

Dieses Produkt kommuniziert drahtlos. Metallische Oberflächen können die Reichweite des Produkts erheblich reduzieren.

- Montieren bzw. platzieren Sie das Produkt nicht auf oder in der Nähe von metallischen Oberflächen.



HINWEIS

Bestimmungsgemäßer Gebrauch

MobileKey-Produkte sind ausschließlich für das Öffnen und Schließen von Türen und vergleichbaren Gegenständen bestimmt.

- Verwenden Sie MobileKey-Produkte nicht für andere Zwecke.

Qualifikationen erforderlich

Die Installation und Inbetriebnahme setzt Fachkenntnisse voraus.

- Nur geschultes Fachpersonal darf das Produkt installieren und in Betrieb nehmen.

Fehlerhafte Montage

Für Beschädigungen der Türen oder der Komponenten durch fehlerhafte Montage haftet die SimonsVoss Technologies GmbH nicht.

Änderungen bzw. technische Weiterentwicklungen können nicht ausgeschlossen und ohne Ankündigung umgesetzt werden.

Die deutsche Sprachfassung ist die Originalbetriebsanleitung. Andere Sprachen (Abfassung in der Vertragssprache) sind Übersetzungen der Originalbetriebsanleitung.

Lesen Sie alle Anweisungen zur Installation, zum Einbau und zur Inbetriebnahme und befolgen Sie diese. Geben Sie diese Anweisungen und jegliche Anweisungen zur Wartung an den Benutzer weiter.

3 Produktspezifische Sicherheitshinweise



VORSICHT

Verbrennungsgefahr durch heiße Platine

Wenn Sie das Gerät mit Power-over-Ethernet (PoE) versorgen, dann kann die Platine sehr heiß sein.

- Lassen Sie das Gerät abkühlen, bevor Sie das Gehäuse öffnen.

Stromschlaggefahr durch angeschlossene Stromversorgung

Das Gerät ist im Betriebszustand mit Spannung versorgt. Wenn Sie das Gehäuse öffnen und stromführende Teile berühren, können Sie einen Stromschlag bekommen.

1. Wenn die Stromversorgung angeschlossen ist, dann öffnen Sie das Gehäuse nicht.
2. Trennen Sie die Stromversorgung (bzw. ziehen Sie das Netzkabel), bevor Sie das Gehäuse öffnen.



HINWEIS

Unbefugter Zugriff mit Standard-Zugangsdaten

1. Ändern Sie das frei einsehbare Webserver-Standardpasswort. Unbefugte können zwar keinen Zutritt erlangen, aber die Konfiguration ändern. In diesem Fall erreichen Sie das Gerät nicht mehr und müssen es zurücksetzen.
2. Verwenden Sie keine Leerzeichen am Anfang oder am Ende (werden von manchen Browsern nicht übertragen).

Weitere Dokumentation

Sie finden weitere Dokumentation zu MobileKey-Produkten auf der SimonsVoss-Seite (<https://www.simons-voss.com/de/downloads/dokumente.html>).

4 Bedeutung der Textformatierung

Diese Dokumentation verwendet Textformatierung und Gestaltungselemente, um das Verständnis zu erleichtern. Die Tabelle erklärt die Bedeutung möglicher Textformatierungen:

Beispiel	Schaltfläche
<input checked="" type="checkbox"/> Beispiel	Checkbox
<input type="checkbox"/> Beispiel	
<input checked="" type="radio"/> Beispiel	Option
[Beispiel]	Registerkarte/Tab
"Beispiel"	Name eines angezeigten Fensters
Beispiel	Obere Programmleiste
Beispiel	Eintrag in der ausgeklappten oberen Programmleiste
Beispiel	Kontextmenü-Eintrag
▼ Beispiel	Name eines Dropdown-Menüs
"Beispiel"	Auswahlmöglichkeit in einem Dropdown-Menü
"Beispiel"	Bereich
Beispiel	Feld
<i>Beispiel</i>	Name eines (Windows-)Dienstes
<i>Beispiel</i>	Befehle (z.B. Windows-CMD-Befehle)
Beispiel	Datenbank-Eintrag
[Beispiel]	MobileKey-Typauswahl

5 Lieferumfang

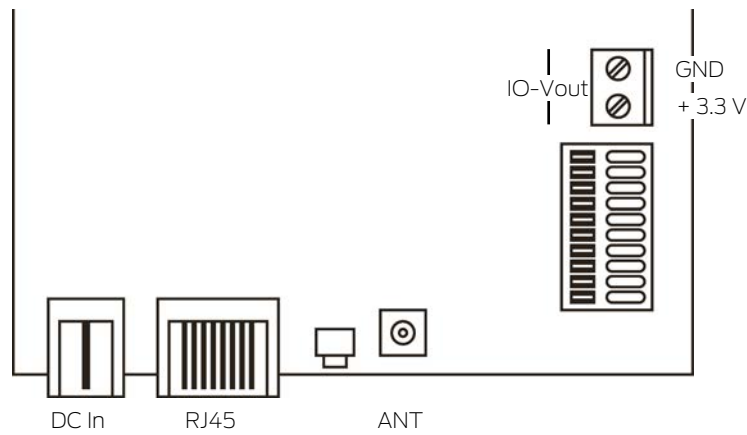
- SmartBridge: Deckel, Bodenplatte mit Platine und drei vormontierten Zugentlastungen
- Abziehbarer Aufkleber mit MobileKey-ID
- Kurzanleitung

5.1 Zubehör

Mit optional erhältlichem Zubehör können Sie Ihr Gerät an unterschiedliche Einsatzzwecke anpassen.

Bestellnummer	Name	Zweck
ANTENNA.EXT.868	Externe Antenne	Sie können die externe Antenne mit dem MCX-Anschluss der Platine verbinden und den Empfang verbessern (siehe <i>Antenne</i> [▶ 15]).
POWER.SUPPLY.2	Netzteil (12 V _{DC} , 500 mA)	Sie können mit diesem Netzteil Ihr Gerät versorgen.

6 Anschlüsse



HINWEIS

IO-Connector nur für RouterNode 2

Sie können die Anschlüsse des IO-Connectors nur am RouterNode 2 nutzen.

Anschluss		Bedeutung
DC In	Rundstecker	Stromversorgung mit Rundsteckverbinder
IO-V _{out}	Klemmblock: GND	Hilfsspannungsausgang - Masseverbindung
	Klemmblock: +3,3 V	Hilfsspannungsausgang - Pluspol
RJ45		Netzwerkverbindung
ANT		Anschluss für externe Antenne (siehe <i>Antenne</i> [▶ 15])

7 Montage

Das Gerät kann horizontal und vertikal montiert werden. Sie können die horizontale Montage einfach und sicher mit den integrierten Befestigungslöchern durchführen. Beachten Sie die Abstrahlcharakteristik der internen Antenne (siehe *Antenne* [▶ 15]) und richten Sie das Gerät passend aus.

ACHTUNG

Beeinträchtigung des Empfangs durch Störquellen

Dieses Gerät kommuniziert kabellos. Kabellose Kommunikation kann durch Metalloberflächen und Störquellen beeinträchtigt werden oder ausfallen.

1. Montieren Sie das Gerät nicht auf Metalloberflächen.
2. Halten Sie das Gerät von elektrischen und magnetischen Störquellen fern.

Unbefugter Zugriff

Wenn die elektrischen Kontakte im Gerät durch Unbefugte kurzgeschlossen werden, dann kann es zu unerwünschten Reaktionen kommen.

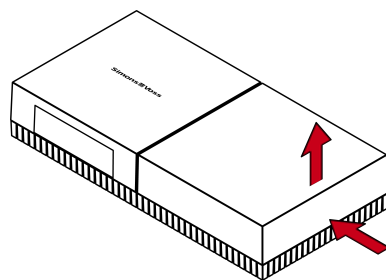
- Montieren Sie das Gerät in einer Umgebung, die vor unbefugtem Zugriff geschützt ist.

Funktionsstörungen durch Witterung

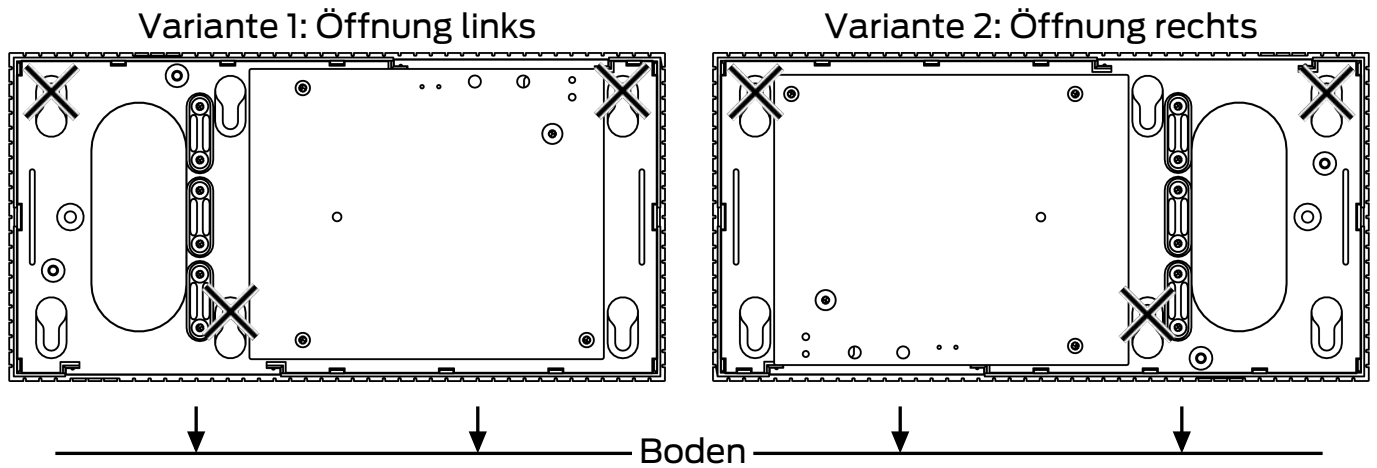
Dieses Gerät ist nicht gegen Spritzwasser und andere Witterungseinflüsse geschützt.

- Montieren Sie das Gerät in einer Umgebung, die vor Witterungseinflüssen geschützt ist.

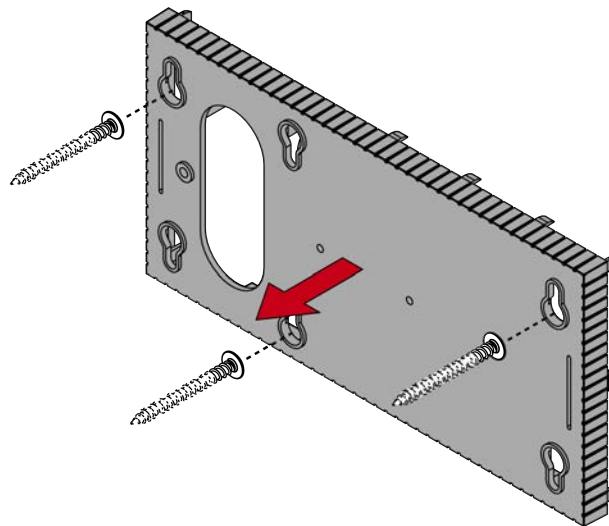
1. Drücken Sie den Gehäusedeckel wie gezeigt ein und nehmen Sie den Deckel ab.



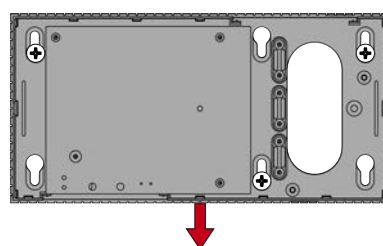
- Halten Sie die Bodenplatte an die gewünschte Stelle und zeichnen Sie die Bohrlöcher an.



- Bohren Sie mit einem geeigneten Bohrer die benötigten Löcher.
- Verwenden Sie geeignete Dübel und schrauben Sie die Schrauben für die Bodenplatte hinein.
- Setzen Sie die Bodenplatte so auf, dass die Schraubenköpfe durch die Aussparungen geführt werden.



- Verschieben Sie die Bodenplatte so, dass die Schraubenköpfe über die Nuten geschoben werden.



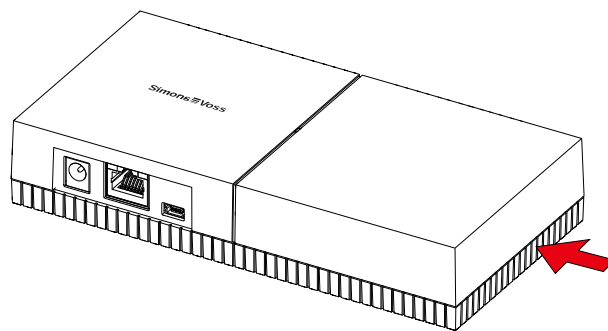
7. Stecken Sie den Deckel wieder auf die Bodenplatte.

↳ Montage abgeschlossen.

Leitungszuführung

Sie können die Leitungen sowohl auf (Aufputz) als auch unter dem Putz (Unterputz) verlegen.

- Wenn Sie die Leitungen unter dem Putz verlegen, dann nutzen Sie die in der Bodenplatte integrierte Öffnung.
 - Wenn Sie die Leitungen auf dem Putz verlegen, dann müssen Sie das Gehäuse modifizieren.
 - ✓ Stromversorgung getrennt.
1. Drücken Sie den gerippten Bereich seitlich nach innen und nehmen Sie den Gehäusedeckel ab.



2. Prüfen Sie die benötigte Breite der Gehäuseöffnung. Die Höhe der Öffnung beträgt ca. 7 mm. Jeder entfernte Steg verbreitert die Öffnung um 4 mm.
3. Wählen Sie eine Stelle, an der Sie die Stege entfernen.

ACHTUNG

Mangelnde Passgenauigkeit durch entfernte Clips

Der Gehäusedeckel wird durch Clips auf den Stegen positioniert und gehalten. Wenn Sie diese Clips absägen oder abbrechen, wird der Gehäusedeckel an dieser Stelle nicht mehr gehalten.

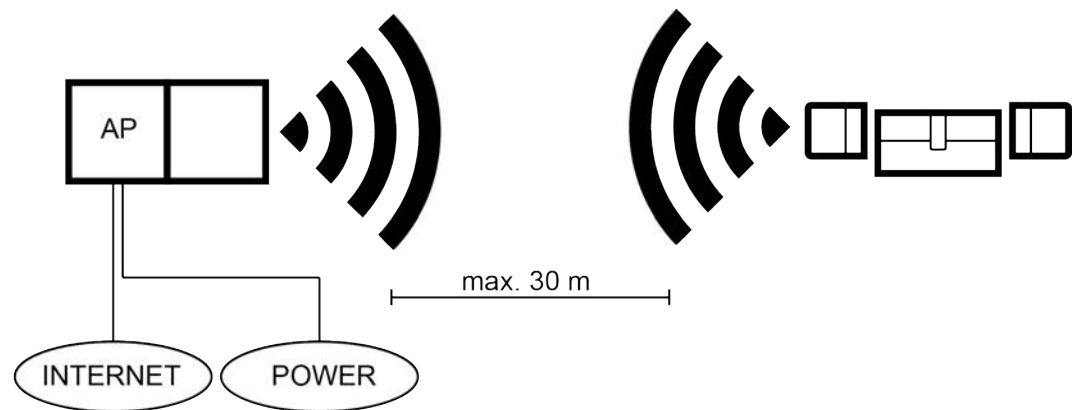
1. Entfernen Sie keine Stege, über denen sich ein Clip befindet.
 2. Beschädigen Sie während des Sägens keine Clips.
 4. Sägen Sie die Stege mit einer geeigneten Säge an beiden Enden der gewünschten Öffnung bis zur Bodenplatte durch.
 5. Biegen Sie die Stege im Bereich der gewünschten Öffnung hin und her, bis die Stege abbrechen.
- ↳ Gehäuse ist für Aufputzmontage vorbereitet.

7.1 SmartBridges aufstellen

SmartBridges können je nach Einsatz und Konfiguration auf unterschiedliche Weise betrieben werden. Im Folgenden werden die wichtigsten Szenarien gezeigt.

7.1.1 Eine SmartBridge

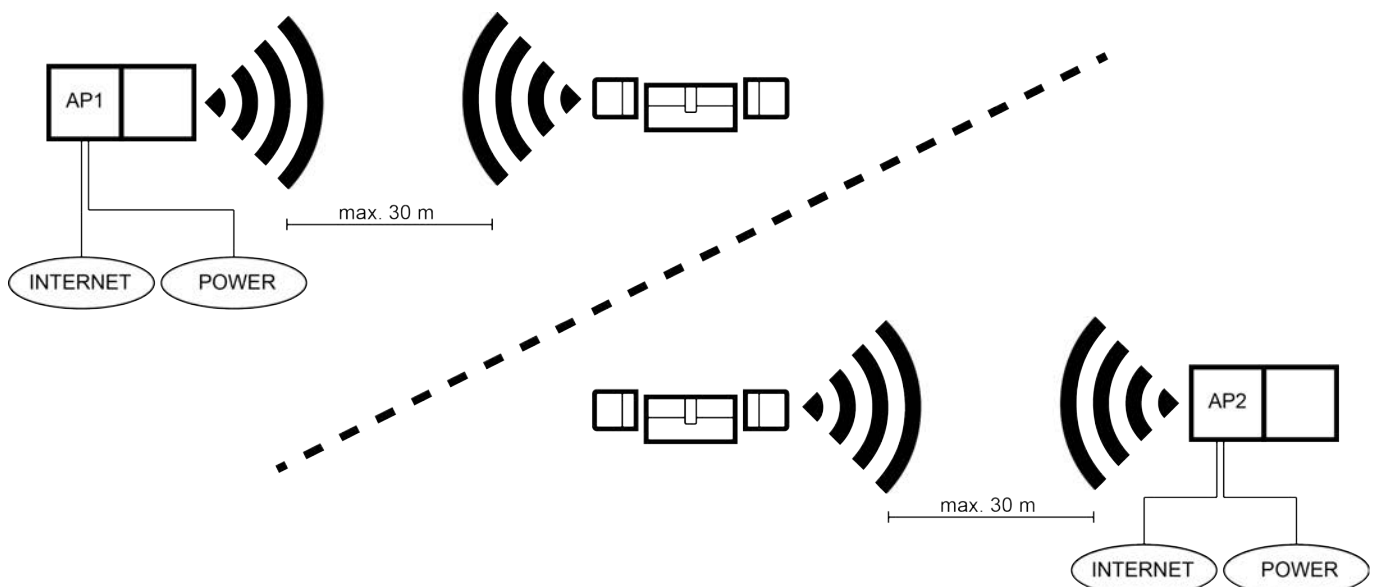
Der Einsatz einer als Accesspoint konfigurierten SmartBridge ist der einfachste Anwendungsfall für MobileKey ONLINE.



7.1.2 Zwei oder mehrere SmartBridges

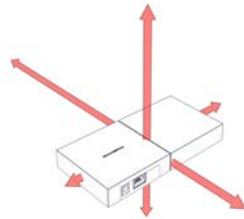
MobileKey ONLINE kann mehrere Accesspoints verwalten. Auf diese Weise können mehrere Standorte oder sehr weit entfernte Schlösser mit dem MobileKey ONLINE Netzwerk abgedeckt werden.

Welches Schloss von welchem Accesspoint angesprochen wird, wird von MobileKey ONLINE automatisch durch Berücksichtigung der Signalstärke bestimmt. Den Weg der Kommunikation können Sie im Menü "NETZWERK" nachverfolgen, indem Sie die Option "Zeige zugewiesene SmartBridge" aktivieren.



7.2 Antenne

Die interne Antenne strahlt wie abgebildet ab. Die Sende- und Empfangsleistung ist also je nach Richtung unterschiedlich und wird möglicherweise durch die Umgebung beeinflusst (Störquellen und/oder metallische Oberflächen).



Externe Antenne



Setzen Sie die externe Antenne ein, wenn eines der folgenden Probleme auftritt.

- Sende- und Empfangsverhalten nicht stabil
- Reichweite zu gering
- Senden und Empfangen im Außenbereich (LockNodes im Außenbereich vorhanden)

Die externe Antenne ist für den Außeneinsatz geeignet. Damit können Sie das Gerät im geschützten Bereich platzieren, während die Antenne sich im Außenbereich befindet.

Im Lieferumfang der externen Antenne befindet sich:

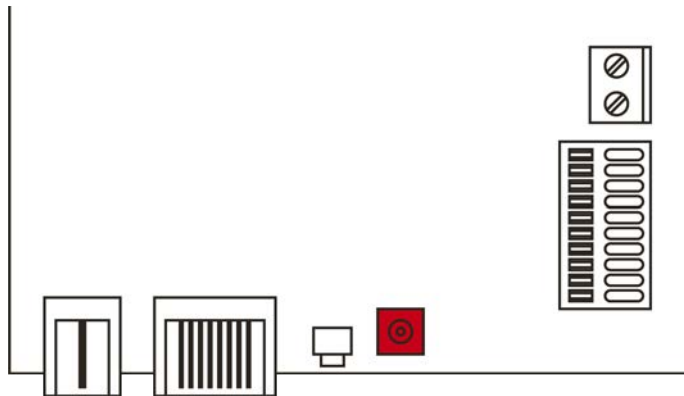
- integrierter Magnetfuß
- Wandbefestigungsmaterial

■ Dübel und Schrauben

Sie müssen nach dem Anschluss der externen Antenne keine Einstellungen verändern. Wenn die externe Antenne angeschlossen ist, dann sendet das Gerät über die interne und die externe Antenne (die interne Antenne wird durch den Anschluss der externen Antenne nicht deaktiviert).

✓ Stromversorgung getrennt.

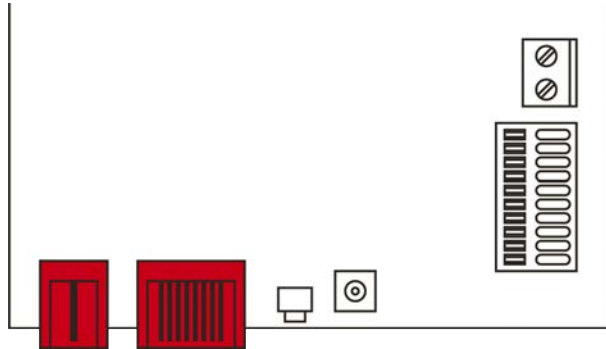
1. Öffnen Sie das Gehäuse.
2. Suchen Sie die Anschlussbuchse auf der Platine.



3. Schließen Sie die externe Antenne an der Anschlussbuchse an.
↳ Externe Antenne ist angeschlossen.
4. Schließen Sie das Gehäuse wieder.
↳ Gerät sendet über interne und externe Antenne.

8 Inbetriebnahme

1. Montieren Sie das Gerät (siehe *Montage* [▶ 11]).
2. Versorgen Sie das Gerät mit Spannung.




3. Verbinden Sie das Gerät mit Ihrem Netzwerk.
 4. Verknüpfen Sie das Gerät mit Ihrem System (siehe *SmartBridge in MobileKey* [▶ 17] sowie das MobileKey-Handbuch).
- ↳ Gerät ist in Betrieb genommen und blinkt langsam grün (siehe *Signalisierung* [▶ 26]).

8.1 SmartBridge in MobileKey

8.1.1 SmartBridges einrichten

So fügen Sie in der Web-App eine neue SmartBridge hinzu:

1. Klicken Sie auf die Menü-Schaltfläche .
↳ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche NETZWERK.
↳ Netzwerkansicht öffnet sich.

3. Fügen Sie eine neue SmartBridge über die -Schaltfläche bei SmartBridges hinzu.
 - ↳ Dialog zum Hinzufügen einer neuen SmartBridge startet.
4. Vergeben Sie einen eindeutigen Namen (z.B. "SmartBridge Büro 2").
5. Geben Sie die MobileKey-ID ein (Siehe Verpackung oder Rückseite der SmartBridge, Format XXXX-XXXX-XXXX-XXXX).
6. Wenn Sie eine weitere SmartBridge anlegen wollen, dann markieren Sie die Checkbox weitere anlegen.
 - ↳ Mit dieser Checkbox bleiben Sie nach dem Speichern in dieser Ansicht und können sofort eine weitere SmartBridge anlegen.
7. Klicken Sie auf die Schaltfläche **Speichern**.
 - ↳ SmartBridge ist angelegt.



HINWEIS

SmartBridge-Verbindung zum Server

Ihre SmartBridge baut etwa alle 15 Sekunden eine Verbindung zum Server auf. Wenn Sie unmittelbar nach dem Einrichten der SmartBridge die Netzwerkkonfiguration starten, dann kann der Server die SmartBridge noch nicht identifizieren und die Netzwerkkonfiguration schlägt fehl.

- Warten Sie nach dem Einrichten der SmartBridge etwa zwanzig Sekunden, bevor Sie die Netzwerkkonfiguration starten.

Standardpasswort ändern

Unbefugter Zugriff mit Standard-Zugangsdaten

1. Ändern Sie das frei einsehbare Webserver-Standardpasswort. Unbefugte können zwar keinen Zutritt erlangen, aber die Konfiguration ändern. In diesem Fall erreichen Sie das Gerät nicht mehr und müssen es zurücksetzen.
2. Verwenden Sie keine Leerzeichen am Anfang oder am Ende (werden von manchen Browsern nicht übertragen).

Ändern Sie das Standardpasswort Ihrer SmartBridge:

1. Ermitteln Sie mit dem OAM-Tool die IP-Adresse Ihrer SmartBridge.
2. Rufen Sie mit einem Browser die Weboberfläche Ihrer SmartBridge auf (Benutzername: SimonsVoss, Passwort: SimonsVoss).
3. Vergeben Sie ein neues Passwort.

Detaillierte Informationen zum OAM-Tool und zu Ihrer SmartBridge finden Sie im OAM-Tool-Handbuch, in der Kurzanleitung Ihrer SmartBridge und dem SmartBridge-Handbuch.





8.1.2 SmartBridges löschen



HINWEIS

Die LockNodes der Schlösser können nur über die verbundene SmartBridge zurückgesetzt werden. Sofern die Schlösser nicht zum Löschen vorgemerkt sind, behalten diese die jeweilige Konfiguration. Allerdings sind die Schlösser danach nur über eine neue SmartBridge oder über das Programmiergerät erreichbar.

So löschen Sie Ihre SmartBridge in der Web-App:

- ✓ Verbundene Schlösser weisen Status "ONLINE" auf.
- 1. Klicken Sie auf die Menü-Schaltfläche .
 - ↳ Menü öffnet sich.
- 2. Klicken Sie auf die Schaltfläche  NETZWERK.
- 3. Klicken Sie auf die zu löschende SmartBridge.
- 4. Klicken Sie auf die Schaltfläche  LÖSCHEN.
 - ↳ Die SmartBridge wird zum Löschen vorgemerkt.
- 5. Starten Sie die Netzwerkkonfiguration über die Schaltfläche  Konfiguration starten.
- 6. Der Programmiervorgang (in diesem Fall das Zurücksetzen der SmartBridge) wird ausgeführt. Die SmartBridge kann anschließend in jeder MobileKey-Schließanlage neu eingebunden werden.

9 Browserschnittstelle

Sie können für RouterNodes, GatewayNodes und SmartBridges mit Ethernet-Schnittstelle über den Browser unter anderem einstellen:

- Änderungen über das OAM-Tool erlauben
- Passwort für die Weboberfläche
- IP-Adresse/DHCP-Betrieb
- SNMP-Port öffnen und schließen

Aufruf

Sie erhalten das Gerät mit folgender werkseitiger Konfiguration:

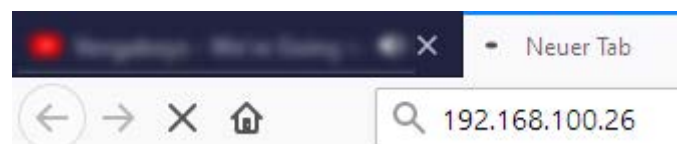
IP-Adresse	192.168.100.100 (falls kein DHCP-Server gefunden wird)
Subnetz-Maske	255.255.0.0
Benutzername	SimonsVoss
Passwort	SimonsVoss

Der Ablauf ist für RouterNodes beschrieben. Verfahren Sie für SmartIntego-GatewayNodes und MobileKey-SmartBridges ebenso.

Ändern Sie nach dem ersten Aufruf das Standardpasswort.

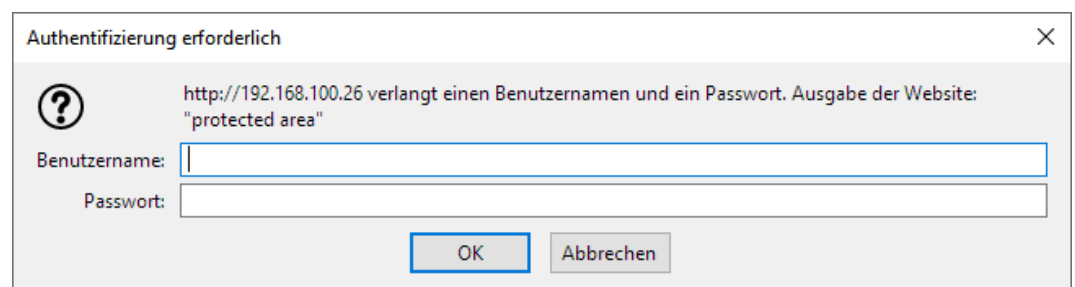
- ✓ Browser geöffnet.
- ✓ Zugangsdaten zur Browserschnittstelle (Name und Passwort) bekannt.

1. Geben Sie in das Adressfeld Ihres Browsers die IP-Adresse ein.



2. Bestätigen Sie die Eingabe mit der Enter-Taste.

- ↳ Fenster "Authentifizierung erforderlich" öffnet sich.



3. Geben Sie die Zugangsdaten ein.

4. Klicken Sie auf die Schaltfläche **OK**.
↳ Systemübersicht der Browserschnittstelle ist sichtbar.

ÜBERSICHT
WAVENET
VERBINDUNG

System Information: Übersicht

Version:

Firmware Version: 40.11.00

Netzwerkconfiguration:

MAC Adresse:	94:50:89:00:36:44
Host Name:	SV_003644
DHCP:	Ein
IP-Adresse:	192.168.100.26
Subnetzmaske:	255.255.255.0
Gateway:	192.168.100.1
DNS-Server1:	192.168.100.1
DNS-Server2:	0.0.0.0
SV Port:	2101
SV SecPort:	2153



HINWEIS

Weboberfläche ab Firmware 40.12 nicht mehr mit Standardpasswort nutzbar

Ab Firmwareversion 40.12 bleibt die Browserschnittstelle solange gesperrt, bis das Standardpasswort geändert wurde.

- Ändern Sie das Standardpasswort.
- ↳ Browserschnittstelle wird entsperrt und Einstellungen können geändert werden.



HINWEIS

Unbefugter Zugriff mit Standard-Zugangsdaten

1. Ändern Sie das frei einsehbare Webserver-Standardpasswort. Unbefugte können zwar keinen Zutritt erlangen, aber die Konfiguration ändern. In diesem Fall erreichen Sie das Gerät nicht mehr und müssen es zurücksetzen.
2. Verwenden Sie keine Leerzeichen am Anfang oder am Ende (werden von manchen Browsern nicht übertragen).

Änderung der IP-Adresse über das OAM-Tool sperren/erlauben

Solange Sie die ▼ **OAM-Tool erlauben** nicht erlauben, können Sie auch keine Updates über das OAM-Tool einspielen.

- ✓ Browserschnittstelle geöffnet.
- 1. Öffnen Sie über | KONFIGURATION | die Registerkarte [PORT].
 - ↳ Sie sehen die Übersicht der TCP-Port-Einstellungen des RouterNode
- 2.

NETZWERK
PORT
ETHERNET SCHNITTSTELLE
WAVENET

Konfiguration: Port-Einstellungen ändern

TCP-Port Einstellungen:

SV Port:	<input type="text" value="2101"/>
SV SecPort:	<input type="text" value="2153"/>
SV Zeitabschaltung [s]:	<input type="text" value="30"/>
HTTP:	<input type="text" value="Ein"/>
Telnet:	<input type="text" value="Aus"/>
OAM-Tool erlauben:	<input type="text" value="Ja"/>

- 2. Wählen Sie im Dropdown-Menü ▼ **OAM-Tool erlauben** den Eintrag "Ja" (Änderung der IP durch OAM-Tool erlauben) bzw. "Nein" (Änderung der IP durch OAM-Tool sperren) aus.
- 3. Klicken Sie auf die Schaltfläche **Save**.
- ↳ Änderung der IP-Adresse über das OAM-Tool ist gesperrt/erlaubt.

Passwort ändern

Einige Browser übertragen keine Leerzeichen, die am Anfang des Passworts stehen. Beginnen Sie das Passwort deshalb nicht mit Leerzeichen.

✓ Browserschnittstelle geöffnet.

1. Öffnen Sie über | ADMINISTRATION | die Registerkarte [PASSWORT].

PASSWORT
ZERTIFIKATE
WERKSEINSTELLUNG
NEUSTART

Administration: Passwort ändern

Neues Passwort:

Neues Passwort:	<input type="text"/>
Passwort bestätigen:	<input type="text"/>
<input type="button" value="Passwort speichern"/>	

2. Geben Sie Ihr neues Passwort ein.

3. Wiederholen Sie Ihr neues Passwort.

4. Klicken Sie auf die Schaltfläche **Passwort speichern**.

↳ Passwort ist geändert.

SNMP-Port schließen und öffnen

Der SNMP-Port ist ab Werk und nach jedem Zurücksetzen geöffnet. Nicht benötigte Ports sollten generell geschlossen werden. Wenn Sie den SNMP-Port schließen, dann findet das OAM-Tool den RouterNode 2 nicht mehr.

✓ Browserschnittstelle geöffnet.

1. Öffnen Sie über | KONFIGURATION | die Registerkarte [PORT].

↳ Sie sehen die Übersicht der TCP-Port-Einstellungen des RouterNode 2.

NETZWERK
PORT
ETHERNET SCHNITTSTELLE
WAVENET

Konfiguration: Port-Einstellungen ändern

TCP-Port Einstellungen:

SV Port:	<input type="text" value="2101"/>
SV SecPort:	<input type="text" value="2153"/>
SV Zeitabschaltung [s]:	<input type="text" value="30"/>
HTTP:	<input type="text" value="Ein"/>
Telnet:	<input type="text" value="Aus"/>
OAM-Tool erlauben:	<input type="text" value="Ja"/>
<input type="button" value="Speichern"/>	

2. Wählen Sie im Dropdown-Menü ▼ **SNMP-Port** den Eintrag "Ja" (SNMP-Port öffnen) bzw. "Nein" (SNMP-Port schließen) aus.

3. Klicken Sie auf die Schaltfläche **Save**.
- ↳ SNMP-Port ist geöffnet bzw. geschlossen.

10 Wartung

Das Gerät selbst ist wartungsfrei. Allerdings ist die Performance von Funknetzwerken immer abhängig von Umgebungseinflüssen. Diese Einflüsse können sich ändern und die Performance Ihres Funknetzwerks beeinflussen. Überprüfen Sie deshalb in regelmäßigen Abständen die Netzwerkkonfiguration und die Performance Ihres Funknetzwerks.

11 Signalisierung

Signal	Bedeutung
Grünes Blinken (~1,5 Hz)	Konfiguriert und betriebsbereit.
Grünes Blinken (~0,3 Hz)	Nicht konfiguriert, aber betriebsbereit
Rotes Blinken (kurzzeitig)	Neustart
Grünes Flackern	Datenübertragung

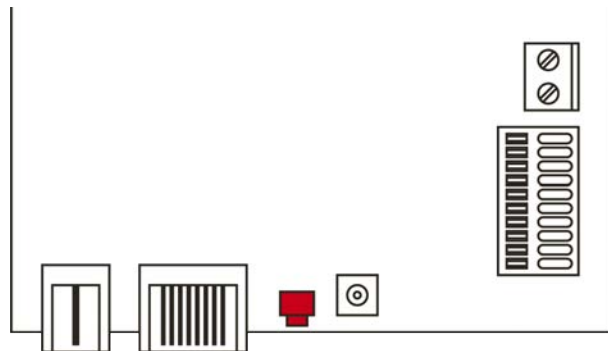
12 Fehlerbehebung

Wenn im Betrieb Probleme auftreten, dann können Sie diese möglicherweise selbst beheben:

1. Prüfen Sie die Stromversorgung der betroffenen Geräte.
2. Prüfen Sie die Netzwerkverbindung.
3. Prüfen Sie die vergebenen Berechtigungen.

12.1 Zurücksetzen

Wenn Probleme auftreten sollten oder Sie das Gerät in den Ausgangszustand zurücksetzen wollen, dann können Sie das Gerät mit dem Resettaster zurücksetzen.



Unterscheiden Sie dabei zwischen:

- MobileKey-Konfiguration zurücksetzen: Sie setzen alle MobileKey-Einstellungen zurück.
- Netzwerkkonfiguration zurücksetzen: Sie setzen alle Netzwerkeinstellungen zurück (IP-Adresse, DHCP-Einstellungen, Hostname).



HINWEIS

Wiederherstellung der IP-Adresse

Wenn die IP-Adresse durch einen DHCP-Server vergeben wird (Standard-einstellung), dann weist der DHCP-Server je nach Einstellung sofort nach dem Zurücksetzen die IP-Adresse wieder zu.

MobileKey-Konfiguration zurücksetzen

1. Trennen Sie die Stromversorgung (Rundstecker bzw. Netzwerkkabel bei PoE).
2. Warten Sie 20 Sekunden.
3. Drücken und halten Sie den Resettaster.
4. Schließen Sie die Stromversorgung wieder an (Rundstecker bzw. Netzwerkkabel bei PoE).

5. Lassen Sie den Resetknopf nach einer Sekunde los.
 - ↳ Gerät blinkt wieder grün (siehe *Signalisierung* [▶ 26]).
 - ↳ MobileKey-Konfiguration zurückgesetzt.

Netzwerkconfiguration zurücksetzen

1. Trennen Sie die Stromversorgung (Rundstecker bzw. Netzwerkkabel bei PoE).
2. Warten Sie 20 Sekunden.
3. Drücken und halten Sie den Resettaster.
4. Schließen Sie die Stromversorgung wieder an (Rundstecker bzw. Netzwerkkabel bei PoE).
5. Lassen Sie den Resetknopf nach fünf Sekunden los.
 - ↳ Gerät blinkt wieder grün (siehe *Signalisierung* [▶ 26]).
 - ↳ Netzwerkconfiguration zurückgesetzt.



HINWEIS

Unbefugter Zugriff mit Standard-Zugangsdaten

1. Ändern Sie das frei einsehbare Webserver-Standardpasswort. Unbefugte können zwar keinen Zutritt erlangen, aber die Konfiguration ändern. In diesem Fall erreichen Sie das Gerät nicht mehr und müssen es zurücksetzen.
2. Verwenden Sie keine Leerzeichen am Anfang oder am Ende (werden von manchen Browsern nicht übertragen).

Sie erhalten das Gerät mit folgender werkseitiger Konfiguration:

IP-Adresse	192.168.100.100
Benutzername	SimonsVoss
Passwort	SimonsVoss

Die IP-Adresse Ihres Geräts in Ihrem Netzwerk lässt sich mit dem kostenlosen OAM-Tool (<https://www.simons-voss.com/de/downloads/software-downloads.html>) bestimmen. Nähere Informationen finden Sie im Handbuch.

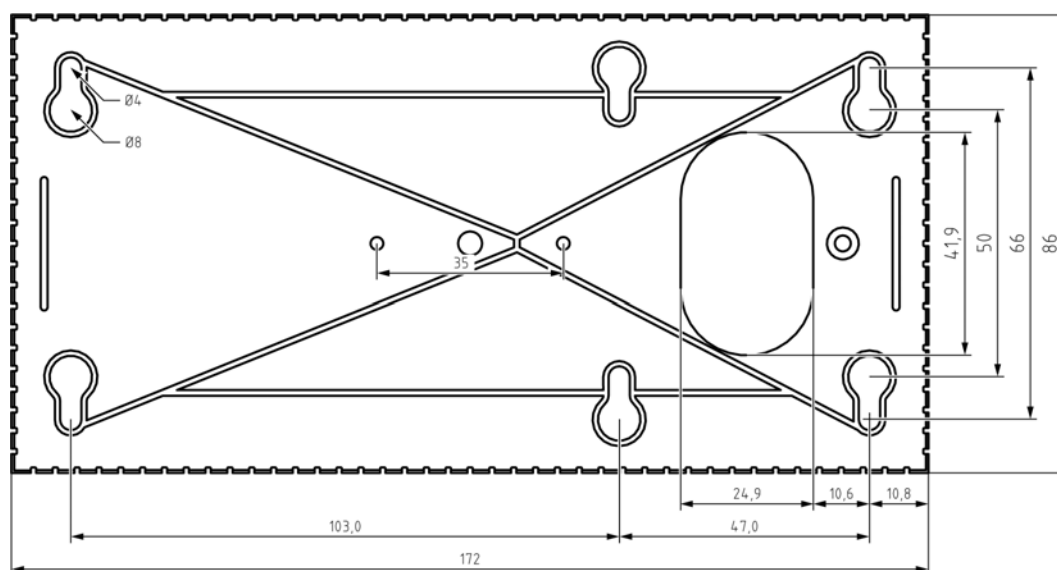
13 Technische Daten

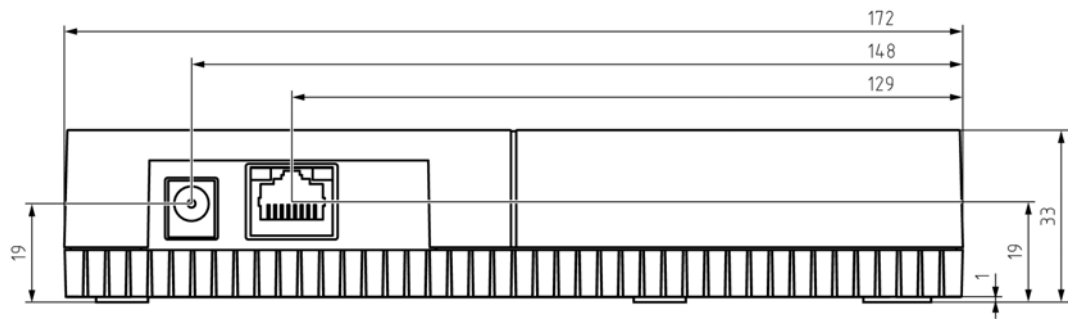
Allgemein	
Maße	172 mm × 86 mm × 33 mm
Gewicht	ca. 100 g
Material	ABS-Kunststoff, UV-stabil
Farbe	Weiß (wie RAL 9016 "Verkehrsweiß")
Montage	<ul style="list-style-type: none"> ■ horizontal ■ vertikal ■ Wandmontage möglich ■ integrierte Zugentlastung (3x)
Anschlüsse	<ul style="list-style-type: none"> ■ RJ45 (Netzwerk/PoE) ■ Rundstecker Ø 5,5 mm, Ø Stift 2,0 mm (Stromversorgung) ■ Schraubklemmblock 2-pol, Aderdurchmesser 0,14 mm² bis 1,5 mm² (Stromversorgung für externe Anwendungen) ■ MCX-Buchse (Optionale externe Antenne)
Umgebung	
Temperatur	<ul style="list-style-type: none"> ■ Betrieb: -10 °C bis +55 °C ■ Lagerung: -20 °C bis +60 °C
Luftfeuchtigkeit	Max. 90% ohne Kondensation
Schutzklasse	IP20
Elektrik	
Betriebsspannung	<p>9 V_{DC} bis 32 V_{DC} (verpolungssicher) oder PoE nach IEEE 802.3af</p> <p>Stromversorgung über PoE und Rundstecker gleichzeitig möglich: Rundstecker > 12 V_{DC} → Rundstecker verwendet, Rundstecker < 12 V_{DC} → PoE verwendet</p>
Leistung	max. 3 W
Ausgang VOUT	3,0 V _{DC} bis 3,3 V _{DC} , max. 200 mA
Schnittstellen	

RJ45	<ul style="list-style-type: none"> ■ Netzwerkschnittstelle ■ 10T/100T ■ HP Auto_MDX ■ DHCP-Client (DHCP: on) ■ IPv4 ■ Services: <ul style="list-style-type: none"> ■ TCP: 1x am Port 2101 ■ UDP: 1x für Digi-Scan (OAM-Tool) ■ Webserver: Enable
868-MHz-Funk	WaveNet-Schnittstelle, Reichweite bis zu 30 m
Signalisierung	
LED	RGB-LED (Gehäusemitte)
Software	
Programmierung	via TCP/IP-Schnittstelle

Funkemissionen		
SRD (WaveNet)	868,000 MHz - 868,600 MHz	<25 mW ERP

Es liegen keine geografischen Beschränkungen innerhalb der EU vor.





13.1 Optionale externe Antenne

13.1.1 Elektrische Spezifikationen

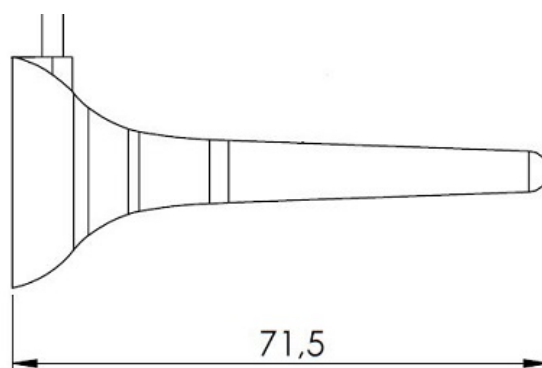
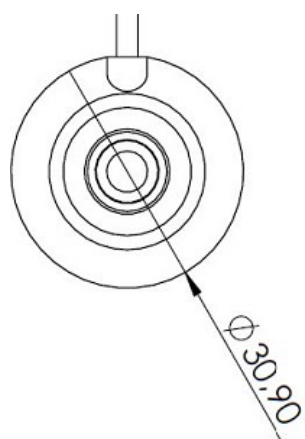
Typ	Multiband-Antenne
Frequenzen	<ul style="list-style-type: none"> ■ AMPS (824 - 894 MHz) ■ GSM (900 MHz) ■ DCS (1800 MHz) ■ PCS (1900 MHz) 3G (UMTS 2,1 GHz)
Impedanz	50 Ω
Polarisation	Linear
Verstärkung	2,2 dBi max.
VSWR	< 3:1
Betriebstemperatur	-40 °C to +85 °C

13.1.2 Anschluss-Spezifikationen

Anschluss	MCX männlich
Kabel	RG174U
Kabellänge	250 cm

13.1.3 Mechanische Spezifikationen und Abmessungen

Befestigung	Magnetische Befestigung
Material	ABS
Max. Abmessungen	30,9 mm x 71,5 mm (\varnothing x H)
Gewicht	50 g 'Anschluss mit Kabel von oben montiert'
Farbe	Schwarz



14 Konformitätserklärung

Hiermit erklärt die SimonsVoss Technologies GmbH, dass der Artikel (MK.SMARTBRIDGE.ER) folgenden Richtlinien entspricht:

- 2014/53/EU "Funkanlagen"
- 2014/30/EU "EMV"
- 2012/19/EU "WEEE"
- 2011/65/EU "RoHS"
- sowie der Verordnung (EG) 1907/2006 "REACH"

Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar:

<https://www.simons-voss.com/de/zertifikate.html>



15 Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der Homepage:

<https://www.simons-voss.com/de/dokumente.html>

Software und Treiber

Software und Treiber finden Sie auf der Website:

<https://www.simons-voss.com/de/service/software-downloads.html>

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate finden Sie auf der Homepage:

<https://www.simons-voss.com/de/zertifikate.html>

Informationen zur Entsorgung

- Entsorgen Sie das Gerät (MK.SMARTBRIDGE.ER/WNM.RN2.ER.IO/WN.RN2.ER/SI.GN2.ER(.M)) nicht mit dem Hausmüll, sondern gemäß der europäischen Richtlinie 2012/19/EU bei einer kommunalen Sammelstelle für Elektro-Sonderabfälle.
- Führen Sie die Verpackung einer umweltgerechten Wiederverwertung zu.



Technischer Support

Unser technischer Support hilft Ihnen gerne weiter (Festnetz, Kosten abhängig vom Anbieter):

+49 (0) 89 / 99 228 333

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

support-simonsvoss@allegion.com

FAQ

Informationen und Hilfestellungen finden Sie im FAQ-Bereich:

<https://faq.simons-voss.com/otrs/public.pl>

Adresse

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Deutschland



Das ist SimonsVoss

SimonsVoss, der Pionier funkgesteuerter, kabelloser Schließtechnik, bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, kleine und große Unternehmen sowie öffentliche Einrichtungen.

SimonsVoss-Schließsysteme verbinden intelligente Funktionalität, hohe Qualität und preisgekröntes Design Made in Germany.

Als innovativer Systemanbieter legt SimonsVoss Wert auf skalierbare Systeme, hohe Sicherheit, zuverlässige Komponenten, leistungsstarke Software und einfache Bedienung. Damit wird SimonsVoss als ein

Technologieführer bei digitalen Schließsystemen angesehen.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs.

SimonsVoss ist ein Unternehmen der ALLEGION Group – ein global agierendes Netzwerk im Bereich Sicherheit. Allegion ist in rund 130 Ländern weltweit vertreten (www.allegion.com).

Made in Germany

Für SimonsVoss ist „Made in Germany“ ein ernsthaftes Bekenntnis: Alle Produkte werden ausschließlich in Deutschland entwickelt und produziert.

© 2022, SimonsVoss Technologies GmbH, Unterföhring

Alle Rechte vorbehalten. Texte, Bilder und Grafiken unterliegen dem Schutz des Urheberrechts.

Der Inhalt dieses Dokuments darf nicht kopiert, verbreitet oder verändert werden. Technische Änderungen vorbehalten.

SimonsVoss und MobileKey sind eingetragene Marken der SimonsVoss Technologies GmbH.

SimonsVoss
technologies

Made in Germany

A BRAND OF

