

Nachrichten & Kanäle

MeshCore Hessen – Nachrichten & Kanäle

- [Kommunikation](#)
 - [QR-Codes für Kontakte und Kanäle](#)
 - [Verschlüsselung, Schlüssel und Vertrauen](#)
 - [Kanäle und Gruppenkommunikation](#)
 - [Adverts – Knoten im Netz bekannt machen](#)
 - [Kontakte und Direktnachrichten](#)

Kommunikation

QR-Codes für Kontakte und Kanäle

Die offizielle MeshCore-Dokumentation definiert QR-Code- beziehungsweise URI-Formate zum Übertragen von Kontakten und Kanälen. Sie vermeiden das manuelle Abtippen langer Schlüssel und sind deshalb besonders praktisch beim Einrichten von Gruppen oder beim sicheren Austausch eines bekannten Kontakts.

Kontakt hinzufügen

Ein Kontakt-QR-Code kann Name, vollständigen Public Key und Knotentyp enthalten. Die aktuelle Spezifikation unterscheidet dabei Companion, Repeater, Room Server und Sensor.

Der Public Key ist der entscheidende technische Identifikator. Der Name ist die menschenlesbare Bezeichnung.

Kanal hinzufügen

Ein Kanal-QR-Code enthält mindestens Kanalname und Secret. Optional kann ein Region Scope mitgegeben werden, sofern die verwendete App-Version diese Funktion unterstützt.

Privater Kanal

Bei einem privaten Kanal ist das Secret tatsächlich geheim. Ein QR-Code mit diesem Secret entspricht daher einer Weitergabe des Kanalzugangs.

Er sollte nur an Personen verteilt werden, die den Kanal nutzen dürfen. Ein Screenshot in einer öffentlichen Gruppe oder auf einer Webseite würde den privaten Charakter zunichtemachen.

Hashtag-Kanal

Bei Hashtag-Kanälen ist der Schlüssel aus dem Namen ableitbar. Ein QR-Code erleichtert hier hauptsächlich die fehlerfreie Einrichtung. Er verwandelt einen Hashtag-Kanal nicht in einen privaten Kanal.

QR-Code prüfen

Vor der Verteilung sollte geprüft werden, ob der QR-Code tatsächlich den vorgesehenen Kontakt oder Kanal enthält. Besonders bei privaten Kanälen ist eine falsche oder alte Schlüsselversion problematisch.

MeshCore Hessen

Für öffentliche Communitykanäle können QR-Codes auf Informationsseiten sinnvoll sein. Private Organisationskanäle sollten dagegen nicht öffentlich im Wiki hinterlegt werden.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [meshcore-cli – offizielles Projekt](#)
- [MeshCore Wiki DE – ergänzende Communityquelle](#)

Redaktioneller Hinweis: Diese Seite ist eine eigenständige Darstellung für MeshCore Hessen. Sachinformationen wurden anhand der oben genannten Quellen geprüft. Texte, Bilder und die Gliederung des MeshCore Wiki DE wurden nicht übernommen; die Seite wird nur als ergänzende Communityquelle zur Faktenkontrolle genannt. Für technische Details hat die aktuelle offizielle MeshCore-Dokumentation Vorrang. Deutschlandbezogene Funkrechtsangaben werden an den Veröffentlichungen der Bundesnetzagentur geprüft.

Urheberrecht: Technische Begriffe, Protokollnamen, Befehlsnamen, Zahlenwerte und andere notwendige Sachangaben werden unverändert verwendet, soweit dies für fachliche Richtigkeit erforderlich ist. Es werden keine längeren fremden Textpassagen oder Bilder reproduziert.

Prüfstand: 18. August 2026

Verschlüsselung, Schlüssel und Vertrauen

MeshCore verwendet Kryptografie an mehreren Stellen. Trotzdem bedeutet das Wort „verschlüsselt“ nicht automatisch, dass jede Kommunikationsart dieselben Sicherheits- und Identitätseigenschaften besitzt.

Knotenidentität

Node Adverts enthalten einen Ed25519-Public-Key und eine Signatur. Damit besitzt ein Knoten eine kryptografische Identität, die über seinen frei wählbaren Anzeigenamen hinausgeht.

Ein Anzeigename sollte deshalb als Beschriftung betrachtet werden, nicht als alleiniger Identitätsnachweis.

Direktkommunikation

Direktkommunikation richtet sich an eine konkrete Gegenstelle und nutzt die kryptografischen Identitäten der Knoten. Für sensible Kommunikation sollte ein Kontakt über einen vertrauenswürdigen Weg verifiziert werden, beispielsweise durch direkten Austausch beziehungsweise einen kontrolliert übermittelten Kontakt-QR-Code.

Gruppenkanäle

Gruppenkanäle verwenden einen gemeinsamen Schlüssel. Wer diesen Schlüssel besitzt, kann den Kanalinhalt entschlüsseln.

Bei privaten Kanälen ist dieser Schlüssel zufällig und geheim. Bei Hashtag-Kanälen wird er dagegen aus dem Namen abgeleitet und ist damit für jeden rekonstruierbar, der den Namen kennt oder errät.

Gruppenabsender sind nicht verifiziert

Die aktuelle offizielle Payload-Spezifikation weist ausdrücklich darauf hin, dass Group Text Messages keinen signierten Absender besitzen. Der sichtbare Name ist Teil des Nachrichtentextes.

Das ist für Communitykanäle wichtig: Eine Nachricht mit dem Namen eines bekannten Administrators beweist allein noch nicht, dass sie tatsächlich von dessen Knoten stammt.

QR-Codes und Geheimnisse

Ein Kontakt-QR-Code enthält öffentliche Kontaktinformationen. Ein Kanal-QR-Code kann dagegen den geheimen Kanalschlüssel enthalten.

Ein QR-Code für einen privaten Kanal darf daher nicht wie ein harmloser öffentlicher Einladungslink behandelt werden. Wer ihn fotografiert oder kopiert, kann den Schlüssel erhalten.

Was Verschlüsselung nicht löst

Verschlüsselung verhindert nicht automatisch Metadatenbeobachtung, Funkstörungen, absichtliches Jamming, kompromittierte Endgeräte oder die Weitergabe eines geheimen Kanalschlüssels durch einen berechtigten Teilnehmer.

MeshCore sollte deshalb mit einem realistischen Sicherheitsmodell betrieben werden: Kryptografie schützt bestimmte Inhalte und Identitäten, ersetzt aber keine verantwortungsvolle Schlüsselverwaltung.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [meshcore-cli – offizielles Projekt](#)
- [MeshCore Wiki DE – ergänzende Communityquelle](#)

Redaktioneller Hinweis: Diese Seite ist eine eigenständige Darstellung für MeshCore Hessen. Sachinformationen wurden anhand der oben genannten Quellen geprüft. Texte, Bilder und die Gliederung des MeshCore Wiki DE wurden nicht übernommen; die Seite wird nur als ergänzende Communityquelle zur Faktenkontrolle genannt. Für technische Details hat die aktuelle offizielle MeshCore-Dokumentation Vorrang. Deutschlandbezogene Funkrechtsangaben werden an den Veröffentlichungen der Bundesnetzagentur geprüft.

Urheberrecht: Technische Begriffe, Protokollnamen, Befehlsnamen, Zahlenwerte und andere notwendige Sachangaben werden unverändert verwendet, soweit dies für fachliche Richtigkeit erforderlich ist. Es werden keine längeren fremden Textpassagen oder Bilder reproduziert.

Prüfstand: 18. August 2026

Kanäle und Gruppenkommunikation

Kanäle ermöglichen Gruppenkommunikation. Mehrere Teilnehmer verwenden denselben Kanal und können darüber Nachrichten austauschen. Dabei unterscheidet die aktuelle offizielle Companion-Protokoll-Dokumentation drei wichtige Kanalarten: den öffentlichen Standardkanal, Hashtag-Kanäle und private Kanäle.

Öffentlicher Kanal

Der öffentliche Standardkanal verwendet einen öffentlich bekannten Schlüssel. Nachrichten dort müssen als öffentlich betrachtet werden. Er eignet sich für allgemeine Kommunikation, bei der Vertraulichkeit nicht erwartet wird.

Hashtag-Kanäle

Bei Hashtag-Kanälen wird der Schlüssel deterministisch aus dem Kanalnamen abgeleitet. Wer den Namen kennt oder errät, kann denselben Schlüssel berechnen.

Das bedeutet: Ein Hashtag-Kanal kann den Funkinhalt zwar verschlüsselt übertragen, ist aber **kein privater Kanal**. Ein leicht erratbarer Name wie `#test` oder `#hessen` ist kein Geheimnis.

Hashtag-Kanäle eignen sich daher zur thematischen Trennung öffentlicher Kommunikation, nicht zur Absicherung vertraulicher Inhalte.

Private Kanäle

Private Kanäle verwenden einen zufällig erzeugten geheimen 16-Byte-Schlüssel. Nur Teilnehmer, die diesen Schlüssel besitzen, sollen den Kanal lesen können.

Der Schlüssel muss deshalb wie ein Zugangsschlüssel behandelt werden. Wird er öffentlich gepostet, in einem öffentlichen QR-Code veröffentlicht oder unkontrolliert weitergegeben, ist die

Vertraulichkeit des Kanals verloren.

Absender in Gruppenkanälen

Ein wichtiger technischer Unterschied zu Direktkontakten: Die offizielle Payload-Dokumentation bezeichnet Group Text Messages als **unverified**. Der im entschlüsselten Nachrichtentext enthaltene Absendername ist nicht kryptografisch signiert. Jeder Teilnehmer mit dem Kanalschlüssel kann grundsätzlich einen beliebigen Namen in eine Gruppenmeldung schreiben.

Daher sollte ein sichtbarer Name in einem Kanal nicht als starker Identitätsnachweis verwendet werden.

Kanalindex und Anzahl

Die konkrete Anzahl verwaltbarer Kanäle und Clientdarstellung ist implementierungs- und versionsabhängig. Das Companion-Protokoll führt Kanalverwaltung über indizierte Slots. Dieses Wiki vermeidet pauschale Aussagen aus älteren App-Versionen und verweist bei technischen Grenzen auf die aktuelle Client-/Firmwaredokumentation.

Kanäle und Scopes

Ein Kanal beantwortet die Frage „Wer besitzt den passenden Kanalschlüssel?“. Ein Scope beantwortet dagegen, in welchem Regionsbereich ein dafür vorgesehenes Flood-Paket weitergetragen werden soll.

Diese beiden Konzepte dürfen nicht verwechselt werden. Ein privater Kanal kann trotzdem unnötig weit geflutet werden, wenn sein Scope zu groß gewählt ist. Umgekehrt macht ein lokaler Scope einen öffentlichen Kanal nicht vertraulich.

Community-Einsatz

Für MeshCore Hessen sind thematische Hashtag-Kanäle für offene lokale Kommunikation denkbar. Vertrauliche Gruppen benötigen dagegen echte private Kanäle mit zufälligem Schlüssel. Welche öffentlichen Communitykanäle tatsächlich genutzt werden, sollte zentral dokumentiert werden, damit nicht mehrere fast gleich benannte Kanäle entstehen.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [meshcore-cli – offizielles Projekt](#)
- [MeshCore Wiki DE – ergänzende Communityquelle](#)

Redaktioneller Hinweis: Diese Seite ist eine eigenständige Darstellung für MeshCore Hessen. Sachinformationen wurden anhand der oben genannten Quellen geprüft. Texte, Bilder und die Gliederung des MeshCore Wiki DE wurden nicht übernommen; die Seite wird nur als ergänzende Communityquelle zur Faktenkontrolle genannt. Für technische Details hat die aktuelle offizielle MeshCore-Dokumentation Vorrang. Deutschlandbezogene Funkrechtsangaben werden an den Veröffentlichungen der Bundesnetzagentur geprüft.

Urheberrecht: Technische Begriffe, Protokollnamen, Befehlsnamen, Zahlenwerte und andere notwendige Sachangaben werden unverändert verwendet, soweit dies für fachliche Richtigkeit erforderlich ist. Es werden keine längeren fremden Textpassagen oder Bilder reproduziert.

Prüfstand: 18. August 2026

Adverts - Knoten im Netz bekannt machen

Ein Advert ist die Bekanntmachung eines MeshCore-Knotens. Damit teilt ein Gerät anderen Empfängern mit, dass es existiert und unter welcher kryptografischen Identität es angesprochen werden kann. Adverts sind deshalb ein grundlegender Teil der Kontaktfindung, aber keine normale Chatnachricht.

Welche Informationen ein Advert enthält

Die aktuelle offizielle Payload-Spezifikation definiert für einen Node Advert einen 32 Byte langen Ed25519-Public-Key, einen Zeitstempel, eine Ed25519-Signatur und optionale Anwendungsdaten. Die optionalen Daten können unter anderem Knotentyp, Position und Namen enthalten.

Die Signatur bezieht sich auf die Identitätsdaten des Adverts. Dadurch ist ein Knoten nicht lediglich durch einen frei gewählten Anzeigenamen definiert. Zwei Geräte können denselben sichtbaren Namen verwenden, besitzen aber nicht automatisch dieselbe kryptografische Identität.

Zero-Hop-Advert

Ein Zero-Hop-Advert wird lokal ausgesendet. Es wird nicht als Flood durch Repeater weitergetragen. Diese Variante eignet sich beispielsweise zum Kennenlernen direkt erreichbarer Teilnehmer und für lokale Funktionstests.

„Zero Hop“ bedeutet dabei nicht „null Funkstrecken“. Das sendende Gerät strahlt das Paket natürlich aus. Gemeint ist, dass keine zusätzlichen Repeater-Hops angehängt werden.

Flood-Advert

Ein Flood-Advert darf durch geeignete Repeater weitergetragen werden. Dadurch kann die Bekanntmachung eines Knotens Teilnehmer erreichen, die ihn nicht direkt empfangen können.

Das ist praktisch, verursacht aber zusätzliche Funklast: Jeder Repeater, der das Paket tatsächlich weiterträgt, benötigt eine weitere Aussendung. In größeren Netzen sollten Flood-Adverts deshalb bewusst eingesetzt werden.

Adverts und Privatsphäre

Wer Positionsdaten in einem Advert veröffentlicht, macht diese Information für die Empfänger des Adverts sichtbar. Für private Companion-Geräte sollte daher bewusst entschieden werden, ob eine Position übertragen werden soll.

Bei öffentlich dokumentierter Community-Infrastruktur kann eine Standortinformation sinnvoll sein. Auch dort muss nicht zwangsläufig jede Detailinformation veröffentlicht werden.

Automatische Adverts bei Infrastruktur

Repeater und andere Infrastrukturrollen können Adverts nach konfigurierten Intervallen aussenden. Die konkreten Standardintervalle können sich mit Firmwareständen ändern. Dieses Wiki schreibt deshalb keinen historischen Standardwert als zeitlos gültig fest; maßgeblich ist die aktuelle CLI beziehungsweise Firmware.

Bedeutung für MeshCore Hessen

Für ein regionales Netz sollten Adverts nicht als „Präsenzspam“ verstanden werden. Ihr Zweck ist Auffindbarkeit und Identität. Bei Infrastruktur ist eine nachvollziehbare Benennung hilfreich, beispielsweise mit Region und Funktion. Persönliche Geräte sollten dagegen keine unnötigen personenbezogenen Daten im Namen oder in Positionsinformationen preisgeben.

Verwandte Seiten

Direktnachrichten bauen auf bekannten Kontakten und deren Identität auf. Flood-Adverts berühren außerdem die Themen Flood Routing, Hop-Grenzen sowie Regions und Scopes, die im Bereich Netzwerk & Routing vertieft werden.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [meshcore-cli – offizielles Projekt](#)
- [MeshCore Wiki DE – ergänzende Communityquelle](#)

Redaktioneller Hinweis: Diese Seite ist eine eigenständige Darstellung für MeshCore Hessen. Sachinformationen wurden anhand der oben genannten Quellen geprüft. Texte, Bilder und die Gliederung des MeshCore Wiki DE wurden nicht übernommen; die Seite wird nur als ergänzende Communityquelle zur Faktenkontrolle genannt. Für technische Details hat die aktuelle offizielle MeshCore-Dokumentation Vorrang. Deutschlandbezogene Funkrechtsangaben werden an den Veröffentlichungen der Bundesnetzagentur geprüft.

Urheberrecht: Technische Begriffe, Protokollnamen, Befehlsnamen, Zahlenwerte und andere notwendige Sachangaben werden unverändert verwendet, soweit dies für fachliche Richtigkeit erforderlich ist. Es werden keine längeren fremden Textpassagen oder Bilder reproduziert.

Prüfstand: 18. August 2026

Kontakte und Direktnachrichten

Direktnachrichten richten sich an einen konkreten MeshCore-Kontakt. Anders als bei einem Gruppenkanal ist das Ziel damit nicht „jeder mit demselben Kanal“, sondern eine bestimmte kryptografische Gegenstelle.

Kontaktidentität

Ein MeshCore-Kontakt besteht nicht nur aus einem Namen. Die technische Identität basiert auf dem Public Key des Knotens. Ein Name ist eine menschenlesbare Ergänzung.

Das ist wichtig, weil Anzeigenamen nicht eindeutig sein müssen. Wer einen sicher bekannten Kontakt importiert oder per QR-Code übernimmt, sollte daher nicht allein den sichtbaren Namen als Identitätsnachweis betrachten.

Wie Kontakte bekannt werden

Kontakte können durch empfangene Adverts bekannt werden. Zusätzlich definiert die offizielle QR-Code-Dokumentation ein Format zum Hinzufügen eines Kontakts. Dabei werden Name, vollständiger öffentlicher Schlüssel und Kontaktyp übertragen.

Ein QR-Code ist besonders hilfreich, wenn ein bestimmter Kontakt unabhängig von zufällig empfangenen Adverts sicher in einen Client übernommen werden soll.

Direktnachrichten und Routing

Eine Direktnachricht kann das Ziel direkt oder über einen Routingpfad erreichen. MeshCore unterscheidet auf Paketebene Flood- und Direct-Routing. Bei Direct-Routing enthält das Paket einen Pfad, der die vorgesehenen Zwischenstationen beschreibt.

Wenn ein passender Weg noch nicht bekannt ist, können Discovery- und Flood-Mechanismen bei der Pfadfindung helfen. Ein ermittelter Rückweg kann anschließend für weitere Kommunikation genutzt werden.

Bestätigungen

Die Payload-Spezifikation kennt Acknowledgment-Pakete. Eine Bestätigung auf Protokollebene ist hilfreicher als die bloße Annahme, dass eine ausgesendete Nachricht angekommen sein müsse.

Trotzdem sollte MeshCore nicht wie ein garantiert zustellendes Mobilfunknetz behandelt werden. Funkwege können sich ändern, Knoten können offline sein und Pakete können kollidieren oder verloren gehen.

Verschlüsselung

Direkte Nachrichten verwenden kryptografische Mechanismen, die an die Identitäten der beteiligten Knoten gebunden sind. Für Anwender ist wichtig, private Direktkommunikation von Gruppenkanälen zu unterscheiden: Bei Gruppenkanälen teilen alle Teilnehmer einen Kanalschlüssel; bei Direktkontakten liegt ein anderes Vertrauensmodell zugrunde.

Mobile Teilnehmer

Routingpfade können veralten, wenn sich ein Teilnehmer oder ein wichtiger Zwischenknoten bewegt. Das betrifft insbesondere die Erwartung, dass ein einmal erfolgreicher Weg dauerhaft gültig bleibt.

Praxis

Für wichtige Tests sollte zunächst ein bekannter Kontakt in kurzer Entfernung verwendet werden. Erst danach lässt sich sinnvoll untersuchen, ob ein Fehler an Kontaktidentität, Routing oder Funkreichweite liegt.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [meshcore-cli – offizielles Projekt](#)
- [MeshCore Wiki DE – ergänzende Communityquelle](#)

Redaktioneller Hinweis: Diese Seite ist eine eigenständige Darstellung für MeshCore Hessen. Sachinformationen wurden anhand der oben genannten Quellen geprüft. Texte, Bilder und die

Gliederung des MeshCore Wiki DE wurden nicht übernommen; die Seite wird nur als ergänzende Communityquelle zur Faktenkontrolle genannt. Für technische Details hat die aktuelle offizielle MeshCore-Dokumentation Vorrang. Deutschlandbezogene Funkrechtsangaben werden an den Veröffentlichungen der Bundesnetzagentur geprüft.

Urheberrecht: Technische Begriffe, Protokollnamen, Befehlsnamen, Zahlenwerte und andere notwendige Sachangaben werden unverändert verwendet, soweit dies für fachliche Richtigkeit erforderlich ist. Es werden keine längeren fremden Textpassagen oder Bilder reproduziert.

Prüfstand: 18. August 2026