

Sicherheit & Datenschutz

MeshCore Hessen – Sicherheit & Datenschutz

- [Sicherheit](#)
 - [Metadaten und Privatsphäre](#)
 - [Repeater und Room Server administrativ absichern](#)
 - [Gruppenkanäle und gemeinsame Schlüssel](#)
 - [Direktnachrichten und Verschlüsselung](#)
 - [Das Sicherheitsmodell von MeshCore verstehen](#)
 - [Datenschutz bei MeshCore-Hessen-Diensten](#)
 - [Backups und geheime Daten schützen](#)
 - [Identitäten und Public Keys](#)

Sicherheit

Metadaten und Privatsphäre

Auch verschlüsselte Kommunikation erzeugt Metadaten. Für eine realistische Datenschutzbetrachtung dürfen diese nicht mit dem Nachrichteninhalt verwechselt werden.

Funkaktivität

Ein Empfänger in Reichweite kann feststellen, dass Funkverkehr stattfindet. Verschlüsselung macht einen Sender nicht physikalisch unsichtbar.

Adverts

Adverts dienen der Bekanntmachung eines Knotens und können Informationen über Identität beziehungsweise Knoteneigenschaften transportieren. Welche Felder aktuell enthalten sind, richtet sich nach Protokoll und Firmware.

Position

Wenn ein Nutzer oder Infrastrukturknoten Positionen veröffentlicht, können daraus Bewegungs- oder Standortinformationen entstehen.

Internet-Bridge

Werden Funkmetadaten an MQTT, Karten oder Datenbanken übertragen, erweitert sich der Kreis möglicher Empfänger erheblich.

Logs

Debuglogs können Knotenkennungen, Zeitstempel und andere technische Metadaten enthalten. Vor einer öffentlichen Supportanfrage werden sie geprüft.

Datenminimierung

MeshCore Hessen speichert bei eigenen Zusatzdiensten nur die Daten, die für den dokumentierten Zweck erforderlich sind.

Erwartungsmanagement

Das Wiki unterscheidet deshalb klar zwischen verschlüsseltem Nachrichteninhalte, pseudonymen technischen Identitäten und tatsächlicher Anonymität. Diese Begriffe sind nicht gleichbedeutend.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [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

Repeater und Room Server administrativ absichern

Ein Repeater kann öffentlichen Funkverkehr weiterleiten und trotzdem einen geschützten Administrationszugang besitzen. Diese beiden Funktionen sind getrennt zu behandeln.

Admin-Passwort

Produktive Infrastruktur erhält ein starkes, einzigartiges Administrationspasswort.

Wiederverwendung desselben Passworts auf allen Standorten vergrößert die Auswirkung eines Leaks.

Berechtigungen

Aktuelle MeshCore-Infrastruktur unterstützt abgestufte Zugriffsmöglichkeiten beziehungsweise ACL-Funktionen. Rechte werden nur so weit vergeben, wie sie für die jeweilige Aufgabe benötigt werden.

Gastzugänge

Room-Server-Gastfunktionen sind keine Administratorrechte. Gast- und Adminzugang erhalten getrennte Zugangsdaten und Zwecke.

Remote und lokal

Nicht alle lokalen seriellen Befehle sind remote verfügbar. Das ist bei Wartungsplanung und Sicherheitsbewertung zu berücksichtigen.

Zugangsdaten speichern

Passwörter gehören in einen geeigneten Passwortmanager oder eine geschützte Betreiberverwaltung, nicht in öffentliche Standorttabellen.

Personalwechsel

Verlässt ein Administrator das Betreiberteam oder geht ein Gerät verloren, werden betroffene Zugangsdaten überprüft und bei Bedarf geändert.

Protokollierung

Wichtige administrative Änderungen werden mit Datum dokumentiert. Das erleichtert die Unterscheidung zwischen Fehlkonfiguration und technischem Defekt.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [meshcore-cli – offizielles Projekt](#)
- [Bundesnetzagentur – Allgemeinzuteilungen](#)
- [Bundesnetzagentur – Vfg. 91/2025](#)
- [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

Gruppenkanäle und gemeinsame Schlüssel

Gruppenkanäle verwenden ein anderes Vertrauensmodell als direkte Kontakte. Teilnehmer eines privaten Kanals benötigen die passende gemeinsame Kanalkonfiguration beziehungsweise den zugehörigen Schlüssel.

Gemeinsames Geheimnis

Wer den gültigen Kanalschlüssel besitzt, kann grundsätzlich an der durch diesen Schlüssel geschützten Kommunikation teilnehmen.

Kanalname reicht nicht

Ein gleicher sichtbarer Kanalname beweist nicht, dass zwei Teilnehmer denselben privaten Kanal verwenden. Entscheidend ist die kryptografische Konfiguration.

Schlüsselweitergabe

Ein privater Kanalschlüssel sollte nur an Personen weitergegeben werden, die tatsächlich Zugriff erhalten sollen. Er gehört nicht in öffentliche Screenshots, Forenposts oder Wiki-Beispiele.

Ausscheiden eines Mitglieds

Bei gemeinsam genutzten Schlüsseln kann ein ehemaliges Mitglied einen einmal erhaltenen Schlüssel weiterhin kennen. Soll dieser Zugriff entzogen werden, ist eine Schlüsselrotation erforderlich.

Öffentliche Kanäle

Ein bewusst öffentlich konfigurierter Kanal besitzt ein anderes Schutzziel als eine private Gruppe. Nutzer sollten nicht allein aus dem Wort „Kanal“ auf Vertraulichkeit schließen.

MeshCore Hessen

Für Communitykanäle wird klar dokumentiert, ob sie öffentlich oder zugangsbeschränkt gedacht sind. Echte produktive Schlüssel werden niemals im öffentlichen Wiki veröffentlicht.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [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

Direktnachrichten und Verschlüsselung

Direktnachrichten sind für Kommunikation zwischen konkreten MeshCore-Kontakten vorgesehen. Die offizielle Protokolldokumentation beschreibt dafür verschlüsselte Payloadtypen und kryptografische Verarbeitung.

Ende-zu-Ende-Prinzip

Der Nachrichteninhalt wird für die Kommunikationspartner geschützt. Repeater transportieren Pakete, ohne dafür den eigentlichen Klartext der Direktnachricht kennen zu müssen.

Routing ist getrennt vom Inhalt

Ein Repeater benötigt Informationen, um ein Paket weiterzuleiten. Daraus folgt nicht, dass er den verschlüsselten Nachrichteninhalt lesen kann.

Identität des Kontakts

Verschlüsselung schützt nur dann vor Kommunikation mit der falschen Person, wenn der richtige kryptografische Kontakt verwendet wird. Ein ähnlicher Anzeigename genügt nicht.

Zustellung

Verschlüsselung garantiert keine Zustellung. Funkstörung, ungültige Pfade oder ein nicht erreichbares Ziel können weiterhin dazu führen, dass eine Nachricht nicht ankommt.

Endgerät

Nach erfolgreicher Entschlüsselung liegt der Inhalt beim Empfänger im Klartext vor. Displaysperre, Betriebssystemschutz und App-Zugriff bleiben daher relevant.

Keine überzogenen Versprechen

Im MeshCore-Hessen-Wiki wird nicht behauptet, Direktnachrichten seien unabhängig von Gerätekompromittierung oder Implementierungsfehlern „absolut sicher“. Beschrieben wird, welchen Schutz das Protokoll vorsieht.

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

Das Sicherheitsmodell von MeshCore verstehen

MeshCore ist ein dezentrales Funknetz. Sicherheit muss deshalb auf mehreren Ebenen betrachtet werden: Identität, Nachrichteninhalte, Administrationszugriff, Funkmetadaten und die Sicherheit der eingesetzten Geräte.

Kein zentraler Betreiber

Im normalen Mesh gibt es keinen zentralen Server, der sämtliche Teilnehmer authentifiziert oder Nachrichten verteilt. Knoten besitzen eigene kryptografische Identitäten und kommunizieren über Funk miteinander.

Verschlüsselung ist nicht Unsichtbarkeit

Verschlüsselung kann Nachrichteninhalte schützen. Funkaktivität selbst bleibt jedoch beobachtbar. Ein Empfänger kann je nach Pakettyp und Situation weiterhin technische Metadaten erkennen.

Direkte Nachrichten und Kanäle

MeshCore verwendet unterschiedliche Mechanismen für direkte Kommunikation und Gruppenkanäle. Diese dürfen im Wiki nicht unter dem vereinfachenden Satz „alles ist gleich verschlüsselt“ zusammengefasst werden.

Infrastruktur

Repeater benötigen für ihre Weiterleitungsfunktion nicht den Klartext einer privaten Nachricht. Administration ist davon getrennt und wird mit eigenen Zugriffsrechten abgesichert.

Endgeräte

Ein entsperartes Smartphone oder ein ungeschützter Computer kann Nachrichten offenlegen, obwohl die Funkübertragung korrekt verschlüsselt war. Gerätesicherheit gehört daher zum Gesamtsystem.

Projektregel

MeshCore Hessen beschreibt Sicherheitsfunktionen exakt nach dem aktuellen Protokollstand und vermeidet absolute Aussagen wie „nicht hackbar“, „vollständig anonym“ oder „100 % sicher“.

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

Datenschutz bei MeshCore-Hessen-Diensten

Die dezentrale MeshCore-Funkkommunikation und von MeshCore Hessen betriebene Onlinedienste sind datenschutzrechtlich nicht dasselbe.

Eigene Dienste

Sobald MeshCore Hessen beispielsweise eine Webseite, Karte, MQTT-Bridge, Botdatenbank oder ein Monitoring betreibt, muss für die dortige Datenverarbeitung ein eigener Zweck definiert werden.

Öffentliche Infrastruktur

Bei Repeatern kann eine öffentliche Darstellung von Name und ungefährender Position sinnvoll sein. Exakte Zugangsdaten zu Gebäuden oder private Kontaktdaten der Standortgeber gehören nicht auf die öffentliche Karte.

Persönliche Nodes

Positions- oder Aktivitätsdaten persönlicher Teilnehmer werden nicht automatisch veröffentlicht, nur weil sie technisch empfangen werden können.

Bot

Ein Testbot benötigt für eine einfache Pingantwort keine dauerhafte Speicherung kompletter Nachrichtenverläufe.

Logs

Technische Logs erhalten eine definierte Aufbewahrung und Zugriffsbeschränkung.

Datenschutzerklärung

Sobald produktive MeshCore-Hessen-Dienste Daten verarbeiten, wird die Datenschutzerklärung der Website um die tatsächlich eingesetzten Dienste ergänzt. Keine Vorlage sollte Funktionen behaupten, die noch gar nicht betrieben werden.

Trennung

Das öffentliche Wiki erklärt die Technik. Interne Betreiberunterlagen enthalten dagegen nur die zusätzlichen Daten, die für Administration und Wartung erforderlich sind.

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

Backups und geheime Daten schützen

Konfigurationssicherungen können sensible Informationen enthalten. Ein Backup ist deshalb nicht automatisch eine harmlose Textdatei.

Vor dem Speichern prüfen

Exportierte JSON-Dateien, App-Backups und CLI-Ausgaben werden darauf geprüft, ob Schlüssel, Passwörter, Tokens oder Identitätsdaten enthalten sind.

Speicherort

Sensible Backups werden verschlüsselt beziehungsweise in einem angemessen geschützten Speicher abgelegt.

Git

Geheime Werte werden nicht in öffentliche Git-Repositories eingecheckt. Ein späteres Löschen aus der aktuellen Datei entfernt sie nicht automatisch aus der gesamten Versionshistorie.

Screenshots

Auch Screenshots von Konfigurationsseiten können QR-Codes, Schlüssel oder Passwörter enthalten.

Testdaten

Dokumentationen verwenden ausdrücklich erzeugte Beispielwerte. Echte produktive Schlüssel werden nicht „kurz zum Erklären“ verwendet.

Wiederherstellung

Backups erhalten Datum und zugehörige Firmwareversion. Vor einer kritischen Wiederherstellung wird geprüft, ob Format und Softwarestand kompatibel sind.

Löschung

Nicht mehr benötigte Sicherungen werden kontrolliert entfernt. Mehr Kopien erhöhen nicht automatisch die Ausfallsicherheit, wenn niemand weiß, wo sensible Kopien liegen.

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

Identitäten und Public Keys

MeshCore-Knoten besitzen kryptografische Identitäten. Diese ermöglichen es, Kontakte eindeutig zuzuordnen, ohne dass ein zentraler Benutzerkontoserver erforderlich ist.

Schlüssel statt Benutzerkonto

Die technische Identität eines Knotens ist nicht einfach sein Anzeigename. Namen können geändert oder mehrfach verwendet werden.

Für sicherheitsrelevante Zuordnung ist deshalb die kryptografische Identität entscheidend.

Public Key

Ein öffentlicher Schlüssel darf – seinem Zweck entsprechend – anderen Teilnehmern bekannt sein. Der dazugehörige private Schlüssel beziehungsweise geheime Identitätsanteil muss dagegen geschützt bleiben.

Kontaktaufnahme

Adverts helfen dabei, Knoten im Mesh bekannt zu machen. Ein sichtbarer Name allein ist kein ausreichender Identitätsnachweis für sensible Kommunikation.

Gerätewechsel

Bei einem vollständigen Identitätswechsel kann ein Gerät für andere Teilnehmer wie ein neuer Kontakt erscheinen. Vor dem Löschen oder Zurücksetzen wichtiger Infrastruktur muss deshalb geklärt werden, welche Identitätsdaten betroffen sind.

Backup

Wenn eine verwendete Anwendung oder Firmware Identitätssicherung unterstützt, wird diese getrennt von normalen Konfigurationswerten betrachtet. Ein Radio-Preset ist kein kryptografischer Identitätsbackup.

Veröffentlichung

Öffentliche Infrastruktur kann ihre Identität bewusst bekannt machen. Private Nutzer sollten trotzdem verstehen, welche Daten ein Advert veröffentlicht und welche nicht.

Quellen, Rechte und redaktionelle Prüfung

- [MeshCore – offizielle Dokumentation](#)
- [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