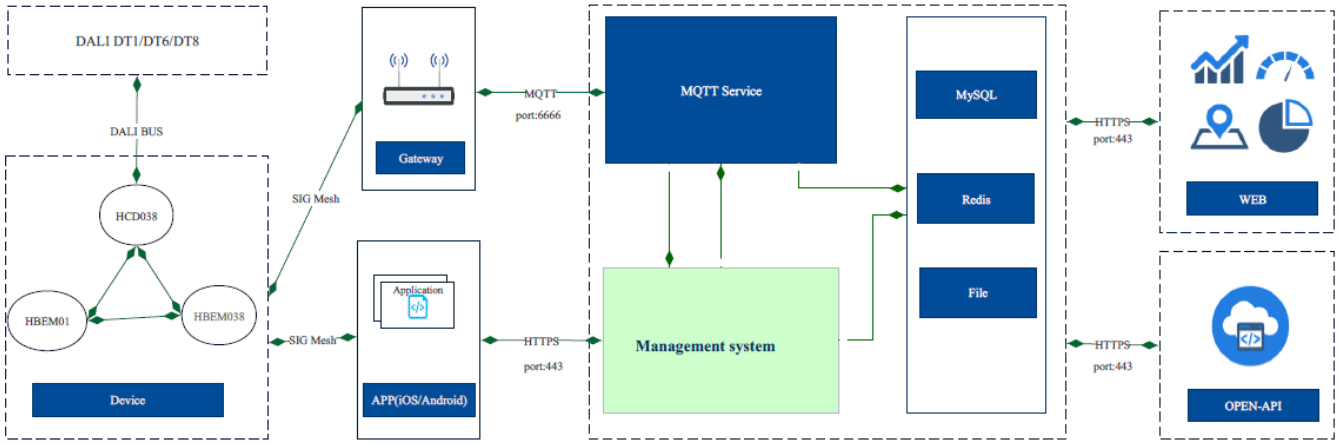
Das Alurays-Mesh-System basiert auf einer drahtlosen Funktechnologie "Bluetooth Low Energy" (BLE) und der internationalen Spezifikation IEEE 802.15.1. Das System verwendet den BLE SIG 5.0 Nordic nRF52832-Chipsatz mit Authentifizierungsidentifikationsnummer mit einem 128-Bit-Sicherheitsschlüssel unter Verwendung von SIG Mesh Version 1.0.1.

Der Rest der Koolmesh-Architektur kann für das DALI-Protokoll nachgelagert und für die Cloud- und API-Funktionen wie folgt dargestellt werden:




**Netzwerksicherheit:**
Die Netzwerksicherheit des Alurays-Mesh-Systems wird in zwei Hauptbereichen eingeteilt:

- **Bereich 1: Das BLE-Mesh:**

Dies ist im Wesentlichen die Bluetooth-"Schicht". Der BLE SIG 5.0 Standard regelt unter anderem die Anforderungen an die Datenver- und -entschlüsselung, das Datenformat und die Berechtigung zur Signatur ("Signieren"). Das Alurays-Mesh-System ist vollständig konform mit dem SIG 5.0-Standard in den Bluetooth-Layern. Der SIG 5.0 Standard gewährleistet eine kontinuierliche Überwachung potenzieller Sicherheitsbedrohungen. Wenn daher eine potenzielle Bedrohung für das aktuelle SIG 5.0-Protokoll erkannt wird, wird das Protokoll aktualisiert, und Alurays wird dies anpassen und das Protokoll sofort aktualisieren. Bei Bedarf kann ein Update für ein bestehendes Netzwerksystem über ein "Over the Air"-Upgrade (OTA) durch die Smartphone Applikation für das Standortnetzwerk implementiert werden.

- **Bereich 2: Die Internetverbindung (von der Alurays-Mesh-App zum Cloud-Server):**

  Alle Datenpakete des Alurays-Mesh-Knotens können nur von der Alurays-Mesh-App und/oder dem Alurays-Mesh Gateway verschlüsselt oder entschlüsselt werden. Es gibt keine andere Methode, 3rd-Party-Geräte oder Software, die die Mesh-Datenpakete umsetzen kann. Alle Datenformate und Verschlüsselungsmethoden sind auf das Alurays-Mesh-System zugeschnitten und werden nicht durch andere verwendet oder an Dritte weitergegeben. Das Alurays-Mesh-System verfügt über zwei sehr wichtige Elemente, um die Daten bei der Übertragung auf den Cloud-Server zu schützen:

  1. **Element 1: "Token":**
     Wenn sich der Benutzer anmeldet, gibt die Person Benutzerauthentifizierungsinformationen (z. B. Konto und Passwort Details) an den Server; und der Server gibt nach der Authentifizierung ein "Token" an das Konto des Clients zurück. Wenn der Benutzer erneut Informationen sendet / anfordert, wird dieser Token damit verbunden. Wenn der Token empfangen wird, werden die Daten zurückgegeben.

2. **Element 2: Nachrichtensignatur ("Zeichen"):**
   Dabei wird ASCII-Code, einschließlich des ersten "Token"-Elements, unter Verwendung der MD5-Verschlüsselung ("Fingerabdruckdatei") verwendet, um eine sekundären "Sign"-Signatur zu generieren; und jedes Mal, wenn das System nach der Anmeldung nach Benutzerinformationen "aufruft", verwendet das System sowohl die Parameter "Token" als auch "Sign" für die Authentifizierung.

Alle OTA-Updates für die Firmware sind durch das Alurays-Mesh-Protokoll geschützt, und nur die Alurays-Mesh-App oder das Alurays-Mesh-System-fähige Gateway kann auf den Alurays-Firmware-Server zugreifen, um ein Update anzufordern. Die gesamte Firmware wird sowohl auf der Anwendungs- als auch auf der Netzwerkseite verschlüsselt. Jedes Mal, wenn der Benutzer ein Update über die App anfordert, sendet er den Token des Benutzers und signiert dies am Server, um den Zugriff zu autorisieren. Wenn die Autorisierung genehmigt wurde, sendet der Server die verschlüsselten Updates über das Internet an die App. Die App überprüft das Zeichen und das Token erneut, bevor das Update entschlüsselt und auf dem Gerät installiert wird.

3. **Element 3: Cloud-Server**

Der Alurays-Cloud-Server basiert auf AWS-Diensten und wir auf der Instanz in Frankfurt umgesetzt. Sicherheit und Größenänderung finden Sie unter folgendem Link:
Sicheres und größenveränderbares Cloud-Computing – Amazon EC2 – Amazon Web Services

Amazon Web Services ermöglicht es Alurays, bei Bedarf die Anwendung schnell zu skalieren sowie Speicher und Leistung zu erhöhenKontobesitz, Berechtigungsverwaltung und Autorisierungsebenen der Installation (Fortsetzung):

Im Alurays-Mesh-System gibt es drei Kontoidentitäten oder "Ebenen" für ein einzelnes Mesh-Netzwerk:

- Administrator
- Installateur
- Unterbenutzer (Gast)

**Administrator:**
Diese Identität/Ebene hat vollen Zugriff auf das Netzwerk, einschließlich der Möglichkeit, Installateure zum Netzwerk hinzuzufügen oder zu löschen. Unterbenutzer hinzufügen oder löschen; und den Unterbenutzern unterschiedliche Ebenenberechtigungen für Netzwerkfunktionen geben. Ein Mesh-Netzwerk hat nur ein Konto auf Administratorebene, kann aber beliebig viele Installateure oder Unterbenutzer haben. Wenn der Administrator das Netzwerk nicht mehr verwalten möchte, kann er das Eigentum an einen anderen Benutzer übertragen, indem er einen eindeutigen QR-Code erstellt (mit verschlüsseltem Schlüssel, wie bereits erwähnt). Dann verschwindet das Netzwerk bei der Übertragung aus dem Konto des Administrators. Der Administrator kann die Berechtigungsstufen des Unterbenutzers verwalten, z. B. nur den Kontrollzugriff für den Unterbenutzer öffnen, ihm jedoch nicht erlauben, die in Auftrag gegebenen Einstellungen oder Szeneneinstellungen des Sensors zu ändern. Diese Berechtigungen können im Abschnitt Alurays-Mesh-App-Berechtigungsmanager festgelegt werden.

**Installateur:**
Diese Identität / Ebene ist dazu gedacht, das Netzwerk in Betrieb zu nehmen, hat also vollen Zugriff auf das Netzwerk und verwaltet das Netzwerk, einschließlich des Hinzufügens oder Entfernens von Knoten aus dem Netzwerk; Ändern von Mesh-Einstellungen oder Einstellungen einzelner Geräte und Durchführen von OTA-Upgrades (in der Regel während der Inbetriebnahmephase). Wenn das Installationsprogramm, das das Mesh-

Netzwerk erstellt hat nicht an einen anderen Benutzer auf Administratorebene überträgt, kann dieses Installationsprogramm diesem Netzwerk ein neues Installationsprogramm hinzufügen. Sie können jedoch keine Unterbenutzer (Gäste) hinzufügen, da dies von der Admin-Ebene abgedeckt wird (in der Regel nach Abschluss der Inbetriebnahmephase).

Wenn der Installateur diesem Netzwerk ein neues Installateurkonto hinzufügt, generiert die App einen QR-Code und einen verschlüsselten, zufälligen Schlüssel (bleibt offen und 1 Stunde gültig). So kann der neue Installateur die Alurays-Mesh-App verwenden, um diesen QR-Code zu scannen oder den verschlüsselten zufälligen Schlüssel einzugeben, um Zugriff auf dasselbe Netzwerk zu erhalten. Der gesamte Autorisierungsprozess wird in der Alurays-Mesh-App durchgeführt.

Nachdem der Installateur die Inbetriebnahme vor Ort abgeschlossen hat, kann er das Eigentum an dem Netzwerk auf das Admin-Konto "übertragen", indem er die gleiche Methode wie "Installateur hinzufügen" verwendet. Sie müssen ihr Kontopasswort eingeben, um diesen Vorgang abzuschließen. Nachdem die "Eigentumsübertragung" abgeschlossen ist, verschwindet dieses Netzwerk aus dem Konto des Installateurs und wird stattdessen im Konto des Administrators angezeigt.

**Unterbenutzer (Gast):**
Die vom Benutzer auf Administratorebene verwaltete Unterbenutzeridentität / -ebene verfügt normalerweise nicht über den vollen Zugriff und die Berechtigungen für das Netzwerk. Diese Ebene kann keine Installationsprogramme übertragen oder hinzufügen. Auch diese Identität kann von der Admin-Ebene autorisiert werden, um verschiedene Layer-Berechtigungen zu haben, z. B. nur die Ein-/Aus-Steuerung der Leuchten zu erlauben.

Alle Autorisierungsprozesse sind durch das Alurays-Mesh-Protokoll geschützt, und alle Verschlüsselungsschlüssel werden zufällig generiert und nicht wiederholt (wie oben beschrieben). Alle Kontodaten werden verschlüsselt und gespeichert, mit Backup auf den Cloud-Servern.