NUNTIUS

Bedienungs- und Funktionsanleitung

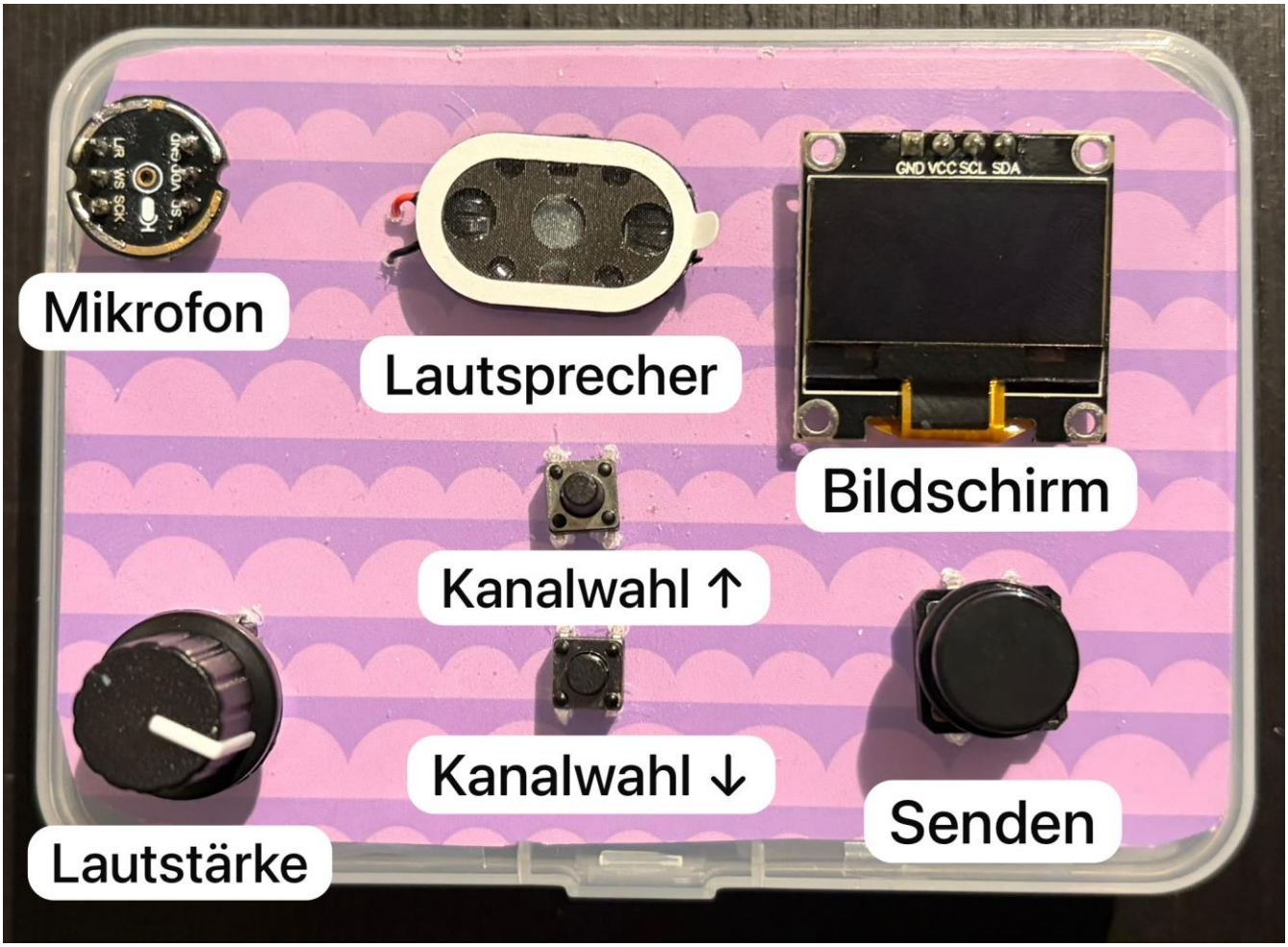
Digitaler Sprechfunk zur Förderung von Freundschaften

Gewidmet an Papst Leo XIV

1. Bedienelemente am Nuntius-Gerät

Das Gerät besitzt vier zentrale Bedienelemente. Die Bedienung ist auf eine einfache Push-to-Talk-Nutzung ausgelegt. Die Übertragung funktioniert über WLAN und ist weltweit möglich.

Bedienelement	Funktion
Senden	Taste gedrückt halten, um das Mikrofon zu aktivieren und Sprache zu übertragen. Beim Loslassen endet die Übertragung und das Mikrofon schaltet ab.
Kanalwahl ↑	Wechselt zum nächsten verfügbaren Kanal.
Kanal ↓	Wechselt zum vorherigen verfügbaren Kanal.
Lautstärke	Regelt die Wiedergabelautstärke des Lautsprechers.



2. Sprechen und Hören

Nuntius arbeitet nach dem Prinzip Push-to-Talk. Das bedeutet: Das Mikrofon wird nicht dauerhaft für die Übertragung verwendet. Erst während des Drückens der Senden-Taste wird Audio aufgenommen und übertragen.

Beim Loslassen der Senden-Taste endet die eigene Übertragung. Das Mikrofon wird anschließend nicht weiter für die Funkübertragung abgehört bzw. übertragen.

Eingehende Sprache funktioniert dagegen automatisch: Befindet sich ein anderer Teilnehmer auf demselben Kanal und sendet, wird das empfangene Audiosignal vom Gerät automatisch über den Lautsprecher wiedergegeben. Es ist dafür kein Tastendruck erforderlich.

Kurz: Drücken = sprechen; nicht drücken = zuhören bzw. auf eingehende Übertragungen warten.

3. Wie Kanäle funktionieren

Ein Kanal ist eine logische Gesprächsgruppe. Geräte, die denselben Kanal ausgewählt haben, können miteinander kommunizieren. Gesendete Sprache wird dem jeweiligen Kanal zugeordnet und an die dafür vorgesehenen Teilnehmer weitergeleitet.

Ein Kanalwechsel ändert damit die Gesprächsgruppe, in der das Gerät sendet und von der es Audio empfängt. Mit Kanal Auf und Kanal Ab kann zwischen den verfügbaren Kanälen gewechselt werden.

Die Verfügbaren Kanäle können je nach Nutzer abweichen. Wenn sie Zugang zu einem bestehenden Kanal erhalten wollen oder einen neuen Kanal für sich und andere Nutzer erstellen kontaktieren sie bitte den Betreiber. Dies ist mit keinen Kosten verbunden. Die E-Mail für den Kontakt lautet: nuntius@kheuer.de

4. Audioübertragung

Die Nuntius-Geräte übertragen digitales Audiosignal über das Netzwerk. Das System verwendet für Sprache eine Abtastrate von 16 kHz und Mono-Audio mit 16 Bit pro Sample.

Die Übertragung erfolgt paketweise. Beim Empfang werden die Audiopakete wieder zusammengesetzt und automatisch über den Lautsprecher ausgegeben.

5. Weboberfläche

Die Primäre Verwendung zwecks der Kommunikation erfolgt über die physischen Geräte.

Alle Einstellungen sind auch über das Webportal vernehmbar, dieses ist über das Internet unter der Adresse https://nuntius.kheuer.de/ erreichbar.

Es ist dort auch möglich über den Webbrowser an der Kommunikation teilzunehmen. Die Kommunikation ist hier aber weniger flüssig, besonders auf iPhone und iPad Geräten, die von der Firma Apple fabriziert wurden

6. Sichere Kommunikation und Verschlüsselung

Nuntius verwendet kryptografische Schlüssel sowohl für die Authentifizierung von Geräten als auch für die Verschlüsselung der Audiopakete.

Ein Kanalschlüssel ist ein zufällig erstellter und einzigartiger 256-Bit-Schlüssel. Der Schlüssel gehört zum jeweiligen geschützten Kanal und ist auf allen Geräten gespeichert, die zur Nutzung des jeweiligen Kanals berechtigt sind. Geräte verschlüsseln und entschlüsseln jedes Paket vor und nach Empfang.

Ein Zentraler Server verwaltet die Kanalmitgliedschaften und sendet die Verschlüsselten Pakete an andere Nutzer des Kanals weiter, ohne die Pakete zu bearbeiten oder zu entschlüsseln.

Die Geräteauthentifizierung verwendet einen separaten geheimen Geräteschlüssel, der ebenfalls auf dem Gerät gespeichert ist. Dieser Schlüssel dient dazu, sicherzustellen, dass ein Gerät gegenüber dem Server als berechtigtes Gerät authentifiziert werden kann. So wird garantiert das unberechtigte Personen weder zuhören noch mitreden können.

Die Sicherheit hängt in der Praxis auch von der sicheren Verwarnung der Geräte ab. Wenn eine nicht vertrauenswürdige Person physischen Zugriff auf das Gerät erhält, kann diese sich als sie ausgeben, solange sie das Gerät besitzt.

Eine Staatlicher Akteur wie z.B. der BND hat vermutlich auch die Möglichkeit die Sicherheitsschlüssel auszulesen und gefälschte Geräte mit ihrer Identität herzustellen, sofern sie den physischen Zugriff auf ihr Gerät an diesen Akteur verlieren.

Es folgt eine Nachricht vom Entwickler des Systems:

Die Sicherheit und Privatsphäre von allen Nutzern ist mir sehr wichtig, aktuell ist der Quellcode noch privat, ich plane allerdings ihn zu veröffentlichen, sobald das System stabil ist und ich es nichtmehr aktiv weiterentwickle. Wenn sie den Quellcode bereits zuvor einsehen möchten, kontaktieren sie mich wirklich sehr gerne, ich habe dazu die E-Mail-Adresse nuntius@kheuer.de eingerichtet.

Zwecks des Ersatzes von Geräten bei Beschädigung und Diebstahl und um in Zukunft neu Geräte zu bestehenden Kanälen hinzuzufügen, speichere ich die Authentifizierungsschlüssel von Geräten und allen Kanälen, außerdem speichere ich den Scrypt Hashwert des Nutzerpasswortes zwecks des Nutzervalidierung auf der Website. Dadurch ist es für mich theoretisch möglich ihre privaten Gespräche mitzuhören oder mich als sie auszugeben, ich verspreche davon keinen Nutzen zu machen aber nur Gott im Himmel kann validieren das ich dieses Versprechen halte, sie müssen mir Vertrauen. Das Mithören und Fälschen von Nachrichten sind den Betreibern der Server von WhatsApp, Skype, Teams etc. übrigens auch möglich, selbst wenn diese das Gegenteil behaupten, da sie nicht kontrollieren können welcher Code wirklich auf dem Server läuft.

Wenn sie das Wünschen können sie eine Kopie des Quellcodes für Geräte erhalten und ein Gerät von ihren eigenen PC aus flashen, ich bin dabei auch gerne behilflich. Sie können auch einen Kanal erstellen dessen

Sicherheitsschlüssel nicht bei mir gespeichert ist, dann ist es für mich unmöglich nachträglich weitere Nutzer dem Kanal hinzuzufügen, aber es besteht auch eine Kryptographische Garantie dafür das ich die geheime Kommunikation nicht mithören kann.

Sie können auch gerne ihren eigenen Nuntius Server betreiben und ein separates Netzwerk selbst kontrollieren. Dann müssen alle Nutzer dieses Netzwerkes nicht mir, sondern ihnen Vertrauen.

7. Neue WLAN Verbindungen einrichten

Das Gerät kann mehrere WLAN-Netzwerke speichern. Beim Einschalten versucht das Gerät zunächst, sich automatisch mit bekannten Netzwerken zu verbinden.

Ist kein bekanntes WLAN erreichbar, wechselt das Gerät in den Konfigurationsmodus. Dabei stellt es ein eigenes WLAN zur Verfügung. Mit einem Smartphone, Tablet oder Computer können sie sich mit diesem WLAN verbinden und anschließend die Konfigurationsseite des Nuntius öffnen.

Dort können die Zugangsdaten eines neuen WLAN-Netzwerks eingetragen und gespeichert werden. Nach dem Speichern startet das Gerät neu und versucht, sich mit dem neu hinterlegten Netzwerk zu verbinden.

Der Name des WLAN Netzwerks dazu lautet: Nuntius gefolgt von ihrem Gerätenamen, z.B. Nuntius_Carlo. Das Passwort wird zufällig generiert und die Adresse zum vornehmen der Konfiguration lautet 192.168.4.1, das können sie in einem Browser, so wie eine URL eingeben.

Diese Informationen werden auf dem Bildschirm des Gerätes erscheinen, falls keine Verbindung zum Internet hergestellt werden kann.

Die Geräte unterstützen nur Wi-Fi Verbindungen auf der 2.4 GHz Frequenz, 5 GHz Verbindungen werden nicht unterstützt.