

Sachbericht BIG-FuE

Smartes WLAN IP-Telefon: Dual-Fon

Akronym: Dual-Fon

Projektlaufzeit: 01.10.2023 bis 30.09.2024 (12 Monate)

Benjamin Ziebarth (Inhaber)
Marke: GEQUUDIO
TGZ PM, Raum 830
Potsdamer Str. 18a, 14513 Teltow

Kurzinformation zum Unternehmen

Unternehmensgegenstand

Die Firma GEQUDIO mit Sitz in Berlin und Teltow entwickelt und vertreibt Produkte der Telekommunikation. GEQUDIO wurde 2008 in Berlin gegründet, 2021 wurde eine Niederlassung in Teltow eröffnet. Zu den Kernprodukten von GEQUDIO zählen Headsets und IP-Telefongeräte sowie komplette Telefonanlagen. Weiterhin werden Programme/Applikationen entwickelt, die die Verwendung verkaufter Hardware unterstützen. Die Vermarktung erfolgt unter der registrierten Unionsmarke: „GEQUDIO“. Aktuell vertreibt GEQUDIO seine Produkte hauptsächlich über den Onlinehandel, wobei ein bedeutsamer Absatzmarkt im deutschsprachigen Raum liegt.

Gesellschafter- und Beteiligungsstrukturen mit Firmenorganigramm

Das Unternehmen wird als Personengesellschaft (Einzelunternehmer) unter dem natürlichen Namen (Benjamin Ziebarth) geführt. Es existieren keine weiteren Gesellschafter und es gibt keine Beteiligungen. Die Hauptniederlassung befindet sich in 14513 Teltow, gemeldet im Gewerbeamt der Stadt Teltow. Die Betriebsstätte in 14513 Teltow stellt den überwiegenden Teil der gewerblichen Aktivität da. Dort sind die Unternehmensführung, das Lager, sowie die Vertriebsaktivitäten inklusive Logistik und Versand. Hier besteht ein gewerbliches Mietverhältnis. Beginn der angemeldeten Tätigkeit in 14513 Teltow ist der 01.04.2021.

Portfolio

Die Firma GEQUDIO entwickelt und verkauft Headsets, IP-Telefone und Telefonanlagen mit entsprechendem Zubehör. Es gehören sowohl kabelgebundene als auch kabellose Bluetooth Headsets zum Portfolio. Kabel-Headsets sind mit Wechselanschlüssen ausgestattet, so dass diese sowohl mit Telefonen als auch PCs und Smartphones verbunden werden können. Der besondere Fokus der Headsets von GEQUDIO liegt auf der Sprachqualität, die durch die Hardwarekonfiguration besonders hochwertig und klar ist und dem hohen Tragekomfort, was für das Langzeittragen in Büros oder Home Office von prinzipieller Bedeutung ist.

Das Produktportfolio umfasst zurzeit die nachfolgenden Artikel:



1. Kabelgebundene Headsets: 14 Varianten
2. Bluetooth Headsets: 2 Varianten
3. Voice-over-IP Telefone
4. Netzteile, Zubehörartikel
5. Cloud Telefonanlagen
6. Reparatur, Reklamation, Konfektionierung

Des Weiteren bietet GEQUDIO die passende Software und Applikationen für die Integration von Telefonen für die vorhandene IT-Infrastruktur an, u.a. Telefonbuch Konverter und Software für Windows/Mac. Die Beratung und der Support der entsprechenden Produkte und Applikationen gehört ebenfalls zum Portfolio des Unternehmens.

Ein weiteres Standbein ist die Vermittlung von Telefonanlagen der Firma foncloud GmbH & Co.KG.

Kunden, Märkte

Die Märkte der Firma GEQUDIO liegen vor allem im Bereich der Büro-Telekommunikation sämtlicher Branchen (siehe Abb. 1 und 2) und werden über verschiedene E-Commerce-Marktplätze bedient. Die Hauptabsatzmärkte im E-Commerce-Bereich liegen in Deutschland mit ca. 90 % Umsatzanteil. Der Anteil der Privatkunden, welche z.B. über die Plattform „Amazon“ bedient werden, liegt bei ca. 68 %. Die Geschäftskunden machen ca. 32 % der Kunden insgesamt aus. Ein geringerer Teil des Verkaufs (ca. 5 %) wird über den Fachhandel abgewickelt.

In Brandenburg bestellen kommunale Behörden, Selbständige wie Agenturen und KMU-Unternehmen unsere Produkte der Marke GEQUDIO. In der Pandemiezeit haben mehrere Gesundheitsämter die Kabel-Headsets erworben.

Beschreibung des Vorhabens

Darstellung des Gesamtziels

Gesamtziel des Projekts ist die Entwicklung und der anschließende Vertrieb eines neuartigen IP-Telefons mit integrierter kabelloser Schnittstelle (WLAN) sowie „smarten“ Zusatzfunktionen, welches das existierende GEQUDIO-Portfolio der kabelgebundenen IP-Telefone mit neuen Funktionen erweitert.

Vorteile eines im Gerät verbauten WLAN-Moduls:

Funktionserweiterung: Das WLAN-Protokoll erweitert den Funktionsumfang der Telefone. Neben der Mobilität und Flexibilität ermöglicht dies unter bestimmten Bedingungen auch den Einsatz in Krisenszenarien bspw. bei Ausfällen der Globalen Netze (Mobilfunk, 5G etc..).

In Abgrenzung zur üblichen WLAN-Verschlüsselung WEP/WPA/WPA2, basierend auf dem OSI-Referenzmodell (ITU-T X.200 (07/1994)) der Schicht 2 (Sicherheitsschicht), wird eine zusätzliche, darauf aufbauende Verschlüsselung auf einer höheren Schicht desselben Modells angestrebt.

Smarte Nutzungsszenarien: Das Modul ermöglicht „smarte Funktionen“ wie Kontakt-Synchronisation, Steuerung von Smart-Home Hardware, Übertragung von Klingeltönen etc. Mit den standardmäßigen analogen bzw. DECT-Schnittstellen anderer IAD (Integrated Access Device) Geräte wie Telekom Speedport oder AVM FRITZ!Box ist das nicht möglich.

Stabilität und Zuverlässigkeit: Ein im Gerät fest verbautes WLAN-Modul, bietet eine stabilere Verbindung, da es direkt mit dem Motherboard des Geräts verbunden ist.

Besseres Antennendesign für höhere Reichweite: Ein integriertes WLAN-Modul ermöglicht eine bessere Platzierung der Antenne und dadurch eine Reichweitenerhöhung, was besonders in größeren Wohnungen oder Gebäuden von Vorteil ist.

Bessere Signalqualität: Aufgrund der internen Bauweise kann das WLAN-Modul eine bessere Signalqualität bieten, da sie weniger durch physische Hindernisse beeinträchtigt wird.

Integration und Ästhetik: Da das WLAN-Modul fest im Gerät integriert ist, ergibt sich eine sauberere ästhetische Erscheinung ohne herausragende und Komponenten wie bei einem USB-WLAN-Stick.

Standortunabhängige WLAN-Tisch Telefone sind durch die Nutzung des kabellosen Internet-Protokolls für viele Szenarien interessant, unter anderem für:

Flexible Arbeitsumgebungen: In modernen, flexiblen Büroumgebungen oder Coworking Spaces kann es schwierig sein, Kabelverbindungen für jedes IP-Telefon bereitzustellen. WLAN-fähige IP-Telefone ermöglichen es den Mitarbeitern, ihre Telefone beliebig zu platzieren, ohne sich um physische Verkabelung kümmern zu müssen. Dies ist besonders nützlich, wenn Arbeitsplätze häufig umgestaltet oder umorganisiert werden.

Mobiles Arbeiten und Homeoffice: Mit der Zunahme des mobilen Arbeitens und der Homeoffice-Szenarien benötigen Mitarbeiter die Möglichkeit, ihre IP-Telefone außerhalb des Büros zu verwenden.

WLAN-fähige IP-Telefone ermöglichen es ihnen, sich nahtlos von zu Hause oder anderen Standorten aus in das Firmennetzwerk einzuloggen und geschäftliche Anrufe zu tätigen, als wären sie im Büro.

Konferenzräume und Besprechungen: In Besprechungsräumen oder Konferenzbereichen ist die Verwendung kabelgebundener Telefone unpraktisch. WLAN-fähige IP-Telefone ermöglichen es den Teilnehmern, ihre Telefone einfacher zu platzieren und drahtlos mit dem Netzwerk zu verbinden. Dies vereinfacht die Einrichtung von Konferenzgesprächen und Präsentationen, ohne dass zusätzliche Verkabelung erforderlich ist.

Telefonie bei Blackouts: Bei großflächigen Stromausfällen ist es mit WLAN möglich, innerhalb geschlossener Infrastrukturen (z.B. Behördenetz, Verwaltungsnetz, Bahn-Netz, etc.) weiter zu telefonieren, sofern die Telefone dort weiter mit Strom versorgt werden. Aufgrund der Notstromversorgung bspw. in Krankenhäusern ist das ein realistisches Szenario. Für den WLAN-Call benötigt man keine Apps, wie WhatsApp, Skype oder ähnliches. Der Gesprächspartner kann ganz normal über die Telefonfunktion angerufen werden. Der Verbindungsaufbau über ein WLAN-Netz ist schneller als über das gewohnte Mobilfunknetz. Das liegt daran, dass das Gerät nicht innerhalb des LTE-Netzes wechseln muss. WLAN-Call bietet eine klare Tonqualität während der Verbindung.

Ziel des Dual Fon Projekts ist es, die technische Schnittstelle der kabelgebundenen Telefonie über ein im Telefon integriertes WLAN-Modul umzusetzen und zusammen mit der dazugehörigen Applikation (App-Store) als neues Gerät mit smarten Funktionen zu entwickeln. Am Markt bestehende Lösungen wie „ContactsPush“ von der Gigaset Communications GmbH funktionieren nur mit IP-Basisstationen, also nicht direkt mit den Telefonen. Die FRITZ!App Fon der AVM GmbH bindet den Kunden an ihre Komplettlösung. Viele Kunden der Netzbetreiber eigenen IAD können diese Lösung nicht nutzen. Eine von kabelgebunden IP-Netzwerken unabhängige Lösung mit Funk-Schnittstelle und smarten Zusatzfunktionen ist eine Erweiterung des bestehenden Sortiments. Das neue Gerät soll über zwei Netzwerkbuchsen verfügen um damit eine noch flexiblere Nutzung im LAN ermöglichen (daher der Name „Dual Fon“).

Beschreibung des/der angestrebten neuen bzw. verbesserten Produktes, Verfahrens oder Dienstleistung (Lösungsansatz, -weg, ggf. Neuartigkeit)

Die WLAN-Technologie ist ein etablierter, globaler und offener Funkstandard.

Ein zur Verringerung der Markteintrittsbarrieren sehr häufig geäußelter Wunsch ist eine vereinfachte Installation, ohne komplizierte Einstellungen für Serveradressen und Transportprotokolle. Alle jetzigen am Markt befindlichen IP-Telefone können nur durch Fachpersonal oder die Bereitstellung umfangreicher Schritt-für-Schritt-Anleitungen (Status-quo) realisiert werden. Daher soll durch die Entwicklung sogenannter Vorlagen die Installation dramatisch vereinfacht werden:



Abb. 3: Konzept für die Installation durch Vorlagen

Bei Nutzung der Vorlagen muss lediglich der Benutzername und das Kennwort eingegeben werden. Sämtlich andere Einstellungen werden automatisch gesetzt, wie: Zeiteinstellungen, Toneinstellungen, Serveradresse, Transportprotokolle und Einstellungen für Anrufbeantworter. Dieses Vorgehen substituiert 15 Seiten der derzeit vorhandenen, komplizierten Installationsanleitungen.

Das Marktsegment der Smart Home Geräte und Applikationen wächst in den nächsten Jahren deutlich. (siehe: Angaben zur wirtschaftlichen Verwertung der Ergebnisse/Beschreibung des Marktes). Der Smart Home Monitor der Splendid Research GmbH beschreibt exemplarisch die Sorgen und Befürchtungen, die aktuell noch Hemmnisse für den Einsatz von Smart Home Lösungen darstellen. Neben den Kosten werden dabei hauptsächlich Sicherheitsbedenken benannt.

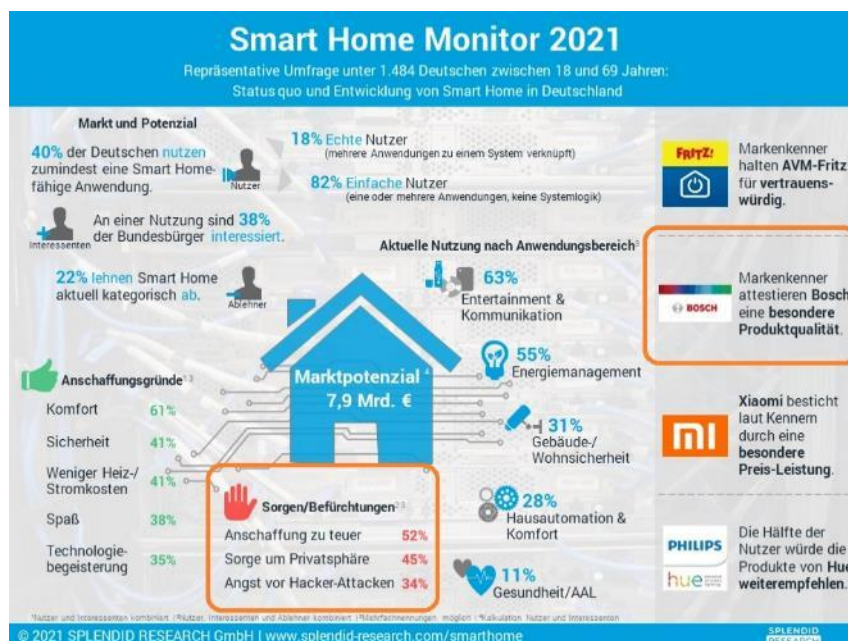


Abb. 3: Quelle: <https://www.splendid-research.com>

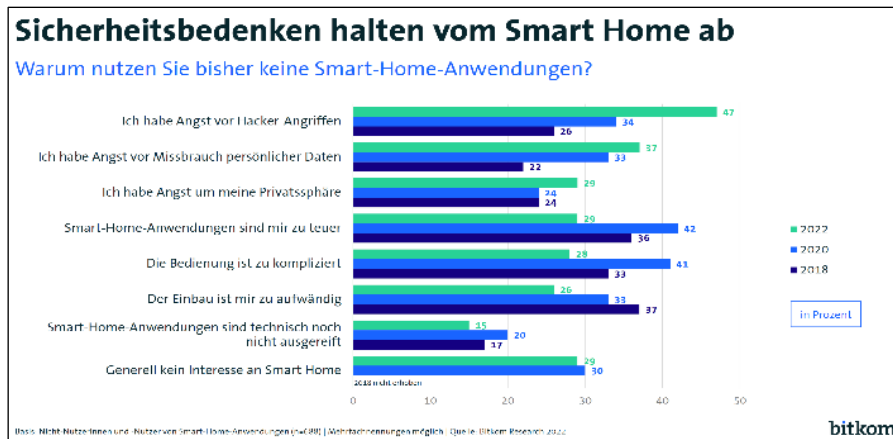


Abb. 4: Quelle Bitkom Research 2022

Zu einem ähnlichen Ergebnis kommt der Bitkom-Studienbericht “Das Intelligente zu Hause-Smart Home 2022“ vom September 2022. Aus der Analyse der weiteren Befragung ergeben sich als die Hauptursachen für Ausfälle der Smart Home Anwendungen Störungen der Internetverbindung.

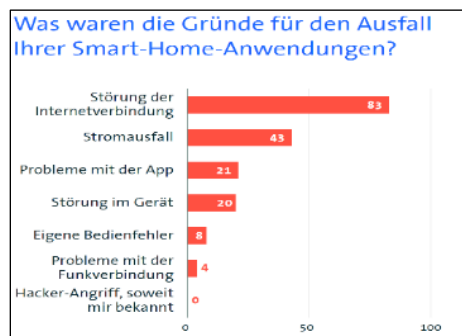


Abb. 5: Quelle: Bitkom Research 2022

Die smarten Zusatzfunktionen des Dual Fons adressieren die in den Studien benannten Defizite als Entwicklungsziele: Sicherheit und Funktion unabhängig vom Internet.

Konkrete Ziele sind:

- (1) Ein lokaler HTTP-Server auf einem Rechner im sicheren lokalen Netzwerk stellt die Schnittstelle für die Einbindung von Smart Home Anwendungen zur Verfügung. Das Dual Fon dient als permanente Bedien- und Anzeigeeinheit (Display/Tasten) für Smart Home Applikationen. Im ersten Schritt werden das Bosch-Smart-Home Applikationen sein. Die Anwendungen weiterer Anbieter werden später integriert. Die Programmierung der smarten Endgeräte wird über bereitgestellte API (Application Programming Interfaces oder Programmierschnittstellen) bestehend aus mehreren Definitionen und Protokollen zur Entwicklung und Integration von Anwendungssoftware realisiert. Eine API ist eine Schnittstelle, die es unabhängigen Anwendungen ermöglicht, miteinander zu kommunizieren und Daten auszutauschen.
 Programmiersprache: Python und Xcode mit den APIs (Programmierschnittstellen) der jeweiligen Smart-Home Geräte-Hersteller.
- (2) Persönliche Daten, wie Kontakte mit Rufnummern möchten viele Privatanwender und Unternehmen nicht auf Cloud-Speichern ablegen, teilweise gibt es auch erhebliche (rechtliche) Vorbehalte wegen der Datenschutz-Grundverordnung (DSGVO). Daher soll der zuvor erwähnte

HTTP-Server diese Dienste – der sicheren Datenübertragung – über ein lokales Netzwerk bereitstellen. Diese isolierte Verbindung zwischen Geräten und Dual Fon in einem sicheren Umfeld Nähe genießt - anders als Cloud Applikationen - hohes Vertrauen, da Anwender Ihre Geräte selbst konfigurieren und das Netzwerkwerk über eine Firewall vom Internet-Router geschützt ist. Es gibt hier keine Anfälligkeit von Abhörversuche, weil keine Übertragung über das öffentliche Internet stattfindet.

Sachbericht

Beschreibung der projektbezogenen Arbeitspakete

Arbeitspaket 1: Schaltplan Entwicklung (Elektronik)

Die Auswahl des WLAN-Moduls fiel auf die Lösung von Murata Type 1DX (Wi-Fi + Bluetooth Combo Module), Datenblatt: <https://www.murata.com/products/productdata/8813651165214/type1dx.pdf>

Type 1DX Wi-Fi® + Bluetooth® Module

Infineon CYW4343W Chipset for 802.11b/g/n + Bluetooth

5.1 Datasheet - Rev. W

- Design Name: Type 1DX

- Module P/N: LBEE5KL1DX-883

Das Murata Type 1DX ist ein kompaktes und leistungsstarkes Wi-Fi + Bluetooth Combo Modul, das für IoT- und Embedded-Anwendungen entwickelt wurde. Dieses Modul zeichnet sich durch eine Kombination aus robuster Konnektivität, Energieeffizienz und Vielseitigkeit aus, was es besonders für platz- und stromsparende Anwendungen interessant macht. Hier sind die Haupteigenschaften und Vorteile des Moduls im Detail beschrieben:

Haupteigenschaften:

Dual-Band Wi-Fi Unterstützung (802.11ac): Das Murata Type 1DX unterstützt sowohl 2,4 GHz als auch 5 GHz Wi-Fi-Frequenzen nach dem 802.11ac-Standard. Dies ermöglicht schnellere Datenübertragungen und eine stabilere Verbindung, insbesondere in Umgebungen mit vielen Störquellen. Der 802.11ac-Standard sorgt für eine verbesserte Netzwerkperformance und größere Reichweiten im Vergleich zu älteren Wi-Fi-Standards.

Integriertes Bluetooth 4.1: Neben Wi-Fi bietet das Modul integriertes Bluetooth 4.1, was es ideal für Geräte macht, die sowohl Wi-Fi als auch Bluetooth-Konnektivität benötigen. Bluetooth kann für die einfache Kopplung von Geräten, die Datenübertragung auf kurze Distanz oder für BLE (Bluetooth Low Energy)-Anwendungen genutzt werden. Die Kombination von Wi-Fi und Bluetooth in einem Modul spart Platz und vereinfacht die Entwicklung von vernetzten Produkten.

Kompakte Bauweise: Das Modul ist besonders klein und hat Abmessungen von etwa 10 mm x 8 mm x 1,3 mm, was es perfekt für platzbeschränkte Anwendungen macht. Es kann in kompakten IoT-Geräten, tragbaren Technologien oder kleinen Sensoren verwendet werden, ohne den Formfaktor des Endprodukts zu beeinträchtigen.

Stromsparendes Design: Ein wichtiges Merkmal des Murata Type 1DX ist sein stromsparendes Design. Dies macht es ideal für batteriebetriebene Anwendungen, bei denen eine lange Betriebsdauer erforderlich ist. Der niedrige Stromverbrauch trägt dazu bei, die Lebensdauer der Batterie zu maximieren, insbesondere in IoT-Geräten, die oft nur gelegentlich Daten übertragen müssen.

Integrierte Sicherheitsfeatures: Das Modul unterstützt fortschrittliche Verschlüsselungstechnologien, darunter WPA3, WPA2-Enterprise und WPA2. Damit erfüllt es moderne Sicherheitsanforderungen und bietet eine sichere Kommunikation, insbesondere bei sensiblen Anwendungen im IoT-Bereich. Die Unterstützung von TLS/SSL für verschlüsselte Verbindungen über das Internet macht es noch sicherer für Datentransfers und Cloud-basierte Anwendungen.

Vielseitige Einsatzmöglichkeiten: Die Kombination aus Wi-Fi und Bluetooth in einem Modul ermöglicht eine breite Palette von Anwendungen. Entwickler können sowohl schnelle Datenübertragung über Wi-Fi als auch energiesparende, lokale Verbindungen über Bluetooth nutzen. Dies macht das Modul ideal für Anwendungen wie vernetzte Sensoren, intelligente Geräte oder Gateways, die mehrere Funktechnologien erfordern.

Zukunftssicherheit dank 802.11ac und WPA3: Durch die Unterstützung von modernem 802.11ac Wi-Fi und dem fortschrittlichen Sicherheitsstandard WPA3 ist das Modul zukunftssicher und erfüllt die aktuellen und künftigen Anforderungen an Netzwerkeffizienz und -sicherheit. Dies ist entscheidend in Umgebungen, in denen hohe Sicherheitsanforderungen gestellt werden, wie etwa in der industriellen Automatisierung, dem Gesundheitswesen oder dem IoT-Bereich.

Energieeffizienz für längere Batterielaufzeit: Dank des stromsparenden Designs ist das Murata Type 1DX ideal für batteriebetriebene Geräte. Dies bedeutet, dass es in IoT-Geräten oder tragbaren Geräten über längere Zeiträume hinweg betrieben werden kann, ohne häufige Batterieaufladungen oder -wechsel.

Wichtig ist Betrachtung der Verschlüsselungsmöglichkeiten. WPA3 (Wi-Fi Protected Access 3) ist der neueste Sicherheitsstandard für drahtlose Netzwerke und wurde entwickelt, um die Sicherheitslücken früherer Protokolle (insbesondere WPA2) zu schließen. WPA3 bietet eine robustere Verschlüsselung und erweiterte Sicherheitsfunktionen, die moderne Anforderungen an Datenschutz und Netzwerksicherheit erfüllen. Hier sind die wichtigsten Eigenschaften und Vorteile von WPA3 im Detail:

Eigenschaften von WPA3: Verbesserte Verschlüsselung

Individuelle Verschlüsselung (Personalized Encryption): WPA3 verwendet standardmäßig 128-Bit-Verschlüsselung für WPA3-Personal und 192-Bit-Verschlüsselung für WPA3-Enterprise. Dies bietet ein höheres Sicherheitsniveau als WPA2, das 128-Bit-AES als Standard verwendet.

Forward Secrecy: WPA3 führt eine sogenannte „Vorwärtsgeheimhaltung“ ein, die verhindert, dass frühere Kommunikation entschlüsselt werden kann, auch wenn ein späterer Schlüssel kompromittiert wird. Dies schützt insbesondere vor Angriffen, bei denen Angreifer versuchen, alte Datenpakete zu entschlüsseln.

Simultaneous Authentication of Equals (SAE):

Widerstandsfähigkeit gegen Passwortangriffe: WPA3 ersetzt den Pre-Shared-Key (PSK) durch das SAE-Protokoll (Simultaneous Authentication of Equals), das deutlich sicherer ist. SAE verhindert Brute-Force-Angriffe, bei denen Angreifer wiederholt verschiedene Passwortkombinationen ausprobieren. Selbst bei schwachen Passwörtern wird die Sicherheit dadurch erhöht.

Schutz gegen Offline-Angriffe: SAE schützt effektiv vor Offline-Wörterbuchangriffen, bei denen Angreifer versuchen, Passwörter durch Ausprobieren bekannter Kombinationen zu knacken.

Einfachere Verbindungen für IoT-Geräte (Wi-Fi Easy Connect):

Verbesserter Schutz in offenen Netzwerken (OWE):

Opportunistic Wireless Encryption (OWE): WPA3 bietet eine Verschlüsselung auch in öffentlichen WLANs, die üblicherweise keine Passwörter verwenden (z. B. in Cafés, Flughäfen). OWE verschlüsselt

die Verbindung zwischen dem Gerät und dem Access Point, auch ohne dass ein Passwort erforderlich ist. Dadurch wird verhindert, dass Dritte den Datenverkehr einfach abhören können.

Unterstützung für Netzwerke mit hohen Sicherheitsanforderungen (WPA3-Enterprise):

192-Bit-Verschlüsselung: WPA3-Enterprise bietet eine noch stärkere Sicherheitsarchitektur mit einer 192-Bit-AES-Verschlüsselung, die vor allem in sensiblen Bereichen wie Finanzsektor, Regierungsstellen und Unternehmen mit hohen Sicherheitsanforderungen eingesetzt wird.

Schutz von Management-Frames (PMF):

WPA3 enthält einen obligatorischen Schutz für Management-Frames, bekannt als Protected Management Frames (PMF). Diese Frames sind wichtige Steuerinformationen in Wi-Fi-Netzwerken. Ohne den Schutz können Angreifer in WPA2-Netzwerken diese Nachrichten manipulieren und z. B. „Deauth“-Angriffe durchführen, bei denen Geräte unerwartet vom Netzwerk getrennt werden.

Vorteile von WPA3:

Erhöhte Sicherheit bei der Nutzung schwacher Passwörter:

Mit dem SAE-Protokoll bietet WPA3 besseren Schutz, selbst wenn ein Nutzer ein schwaches Passwort verwendet. Im Gegensatz zu WPA2 macht WPA3 es deutlich schwieriger für Angreifer, Passwörter durch Brute-Force- oder Wörterbuchangriffe zu knacken.

Besserer Schutz in öffentlichen WLAN-Netzwerken:

In offenen Netzwerken, die typischerweise keine Verschlüsselung haben, bietet WPA3 durch OWE eine automatische Verschlüsselung des Datenverkehrs. Dies verhindert, dass Dritte den unverschlüsselten Datenverkehr abhören und vertrauliche Informationen stehlen können.

Erweiterte Sicherheit für Unternehmen:

WPA3-Enterprise bietet durch die 192-Bit-Verschlüsselung und weitere Sicherheitsverbesserungen einen hohen Schutz für Netzwerke mit besonders sensiblen Daten. Dies ist wichtig für Branchen wie Finanzen, Gesundheitswesen und Regierungsstellen, die hohen Sicherheitsanforderungen unterliegen.

Zukunftssicherheit:

WPA3 ist ein zukunftssicherer Standard, da er moderne Verschlüsselungsmethoden und Sicherheitsmechanismen nutzt, die auf die wachsenden Bedrohungen der digitalen Welt reagieren. Der Einsatz von WPA3 in neuen Geräten und Netzwerken garantiert, dass diese Systeme vor den neuesten Angriffstechniken geschützt sind.

Verbesserte Benutzerfreundlichkeit:

Dank der Unterstützung für Wi-Fi Easy Connect ist es einfacher, IoT-Geräte und andere „kopflose“ Geräte (also Geräte ohne Bildschirm oder Eingabemöglichkeiten) sicher mit einem Netzwerk zu verbinden. Dies ist besonders nützlich in Smart Homes oder Smart Offices, wo viele Geräte miteinander vernetzt sind.

Schutz gegen Deauth-Angriffe:

Mit PMF (Protected Management Frames) wird das Risiko von Deauthentication-Angriffen deutlich reduziert. Solche Angriffe, die in WPA2-Netzwerken häufig vorkommen, trennen Geräte gewaltsam vom Netzwerk und können von Angreifern genutzt werden, um weitere schädliche Aktionen durchzuführen. WPA3 macht diese Angriffe wesentlich schwieriger.

WPA3 ist bereits ein vorhandener Standard, daher soll diese Technologie kombiniert werden, damit der Anspruch in Bezug auf Sicherheit und Verschlüsselung erfüllt wird.

WPA3 arbeitet auf der Sicherungsschicht (Layer 2) des OSI-Modells und schützt die drahtlose Kommunikation zwischen Geräten im Netzwerk durch Authentifizierung und Verschlüsselung. Um die Sicherheit weiter zu erhöhen, kann WPA3 mit einer zusätzlichen Verschlüsselungsart auf einer höheren OSI-Schicht kombiniert werden, insbesondere auf der Transportschicht (Layer 4) oder der Anwendungsschicht (Layer 7).

Die am häufigsten verwendete Verschlüsselungsmethode auf diesen höheren Schichten ist TLS (Transport Layer Security).

TLS (Transport Layer Security) – Transportschicht (Layer 4) / Anwendungsschicht (Layer 7):
Eigenschaften von TLS:

TLS ist das gängigste Protokoll zur Sicherung von Verbindungen auf der Transportschicht (Layer 4) und der Anwendungsschicht (Layer 7) des OSI-Modells.

Es wird verwendet, um Daten während der Übertragung über das Internet zu verschlüsseln, und wird typischerweise in Protokollen wie HTTPS, SMTP, IMAP, FTPS und anderen genutzt.

TLS bietet Ende-zu-Ende-Verschlüsselung, Authentifizierung und Datenintegrität.

Kombination von WPA3 und TLS:

WPA3 sorgt für eine sichere Verbindung zwischen einem Gerät und dem Access Point auf der Sicherungsschicht. Es verschlüsselt den Datenverkehr über das WLAN und schützt vor Angriffen auf diese Verbindungsebene.

TLS sorgt dafür, dass die Daten, die über das Internet oder das Intranet gesendet werden, verschlüsselt und authentifiziert sind, unabhängig davon, ob das Netzwerk sicher oder unsicher ist. Selbst wenn ein Angreifer Zugriff auf das lokale Netzwerk erhält, kann er durch die TLS-Verschlüsselung die übertragenen Daten nicht entschlüsseln.

Vorteile der Kombination:

Doppelte Sicherheit: WPA3 sichert die drahtlose Kommunikation zwischen Gerät und Access Point, während TLS die Daten auf der Transportschicht verschlüsselt. Dies bietet zusätzlichen Schutz vor Angriffen auf unterschiedlichen Netzwerkebenen.

Ende-zu-Ende-Verschlüsselung: Während WPA3 den lokalen Drahtlosverkehr sichert, stellt TLS sicher, dass Daten auf ihrem gesamten Weg vom Sender zum Empfänger verschlüsselt bleiben. Diese Kombination schützt die Daten während der gesamten Übertragungskette.

Schutz vor Man-in-the-Middle-Angriffen: Während WPA3 den drahtlosen Datenverkehr gegen Abhören schützt, verhindert TLS, dass ein Angreifer, der möglicherweise auf das Netzwerk zugreift, die über das Internet gesendeten Daten entschlüsseln oder manipulieren kann.

Typische Anwendungsfälle:

HTTPS (HTTP über TLS) ist eine typische Anwendung, bei der TLS zusammen mit WPA3 verwendet wird. Die Kommunikation zwischen einem Client (z. B. ein Smartphone) und einem Webserver wird über WPA3 geschützt, und die darauf folgenden Webanfragen und -antworten werden zusätzlich über TLS verschlüsselt.

VPNs (Virtual Private Networks): Oftmals wird WPA3 mit VPN-Protokollen kombiniert, die auf der Transportschicht zusätzliche Verschlüsselung bieten. Die VPN-Verbindung verschlüsselt alle Daten zwischen einem Gerät und einem VPN-Server und bietet eine weitere Sicherheitsschicht.

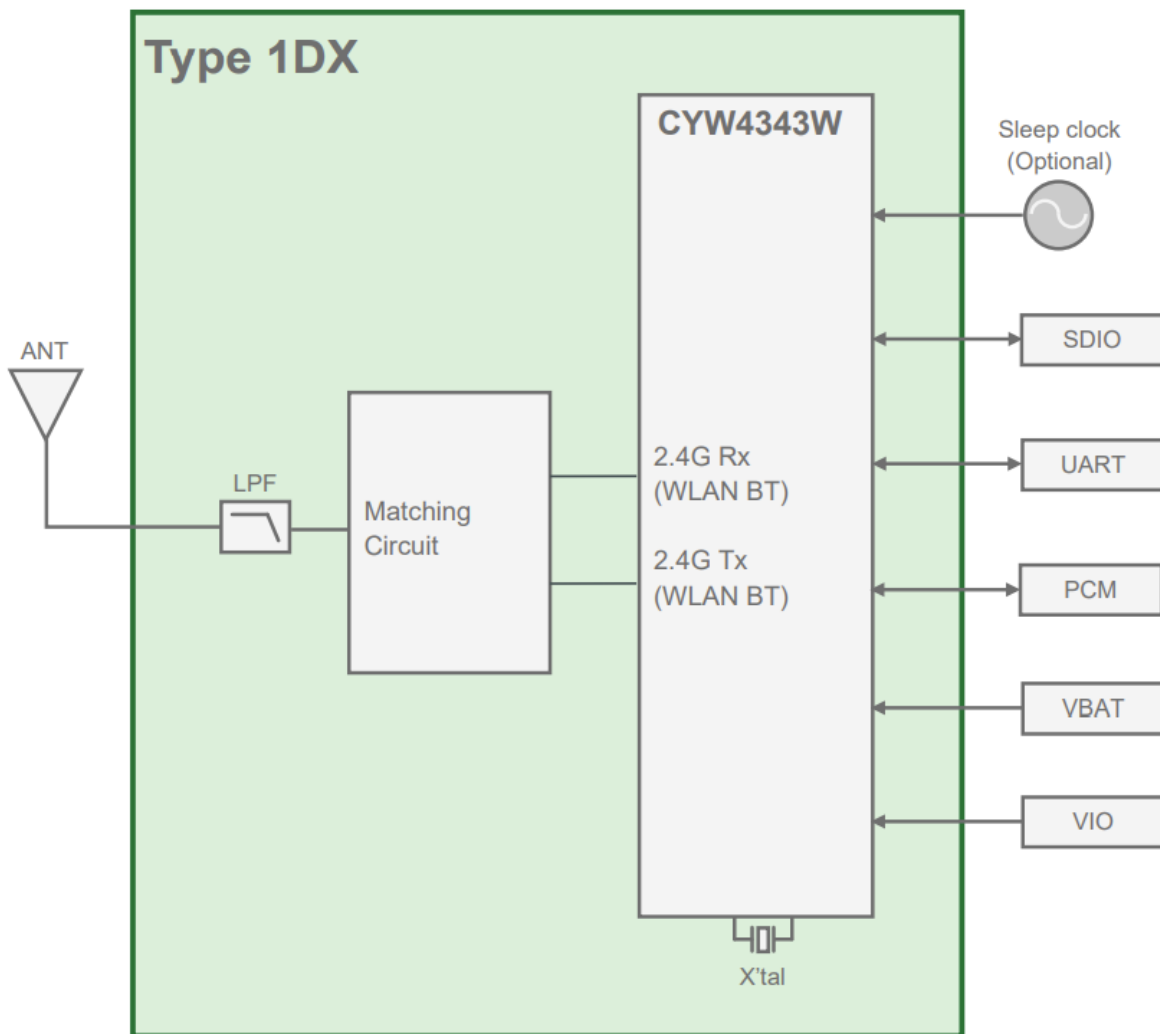


Abb. 6: [Blockdiagramm von muRata aus dem Datenblatt]

Arbeitspaket 2: Firmware Entwicklung (Telefon):

Nachfolgend ist eine ausführliche Tabelle mit technischen Produktanforderungen für die Firmware-Entwicklung eines Telefons mit WPA3-verschlüsselter Technologie:

Anforderung	Beschreibung	Ziel
Sicherheitsprotokolle	Implementierung von WPA3 zur Sicherstellung sicherer WLAN-Verbindungen.	Gewährleistung, dass alle WLAN-Verbindungen die neuesten Sicherheitsstandards erfüllen.
Datenverschlüsselung	Nutzung von 128-Bit- oder 192-Bit-Verschlüsselung für sichere Datenübertragung.	Schutz der übertragenen Daten vor unbefugtem Zugriff.

Forward Secrecy	Unterstützung für Forward Secrecy zur Sicherstellung, dass frühere Kommunikationsschlüssel nicht kompromittiert werden können.	Erhöhung der Datensicherheit über längere Zeiträume hinweg.
Benutzeroberfläche	Intuitive und benutzerfreundliche Einstellungen für WLAN-Sicherheit.	Erleichterung der Konfiguration für Endbenutzer.
Kompatibilität	Unterstützung älterer WPA/WPA2-Standards für Rückwärtskompatibilität.	Sicherstellung, dass das Gerät mit bestehenden WLAN-Netzwerken und Routern funktioniert.
Zertifizierung	Zertifizierung gemäß den neuesten Wi-Fi-Allianz-Richtlinien.	Gewährleistung, dass das Gerät alle erforderlichen Sicherheitsstandards erfüllt.
Leistungsoptimierung	Minimierung des Energieverbrauchs während der WPA3-Authentifizierung.	Verlängerung der Akkulaufzeit des Geräts.
Optimierung der Verbindungszeiten	Optimierung der Verbindungszeiten und der Signalstabilität während der WPA3-Authentifizierung.	Verbesserung der Benutzererfahrung durch schnellere und stabilere Verbindungen.
Updates und Wartung	Möglichkeit zur Aktualisierung der Firmware über Over-the-Air (OTA).	Regelmäßige Bereitstellung von Sicherheitsupdates und Bugfixes.
Regelmäßige Sicherheitsüberprüfungen	Durchführung regelmäßiger Sicherheitsüberprüfungen und -updates.	Aufrechterhaltung eines hohen Sicherheitsniveaus und Reaktion auf neu auftretende Bedrohungen.

Logging und Monitoring	Implementierung von Protokollierungsfunktionen für Sicherheitsergebnisse und Unterstützung von Netzwerkanalyse-Tools.	Ermöglichung der Überwachung der Verbindungssicherheit und schnelle Reaktion auf Sicherheitsvorfälle.
Interoperabilität	Sicherstellung der Interoperabilität mit verschiedenen WLAN-Routern und Access Points, die WPA3 unterstützen.	Gewährleistung einer nahtlosen Benutzererfahrung, unabhängig von der verwendeten Infrastruktur.
Benutzersupport	Bereitstellung von Dokumentation und Support für Endbenutzer zur Konfiguration und Fehlerbehebung bei WPA3-Verbindungen.	Unterstützung der Benutzer bei der effektiven Nutzung der Sicherheitsfunktionen des Geräts.
Ressourcenschonung	Minimierung des Speicher- und Rechenaufwands während der WPA3-Authentifizierung.	Gewährleistung eines reibungslosen Betriebs des Telefons ohne Beeinträchtigung der Leistung.
Funknetzwerk-Management	Unterstützung von Funktionen zur Analyse der Funknetzwerk-Umgebung zur Optimierung der Verbindung.	Verbesserung der Verbindungsqualität und Reduzierung von Interferenzen.

Systemarchitektur für die Firmware-Entwicklung

1. Benutzerschnittstelle (UI)

- Einstellungen für WLAN: Benutzer kann WLAN konfigurieren, WPA3 aktivieren/deaktivieren.
- Statusanzeige: Anzeige des Verbindungsstatus und der Sicherheitseinstellungen.

2. Anwendungs- und Middleware-Schicht

- WLAN-Manager:
 - Verwaltung von WLAN-Verbindungen.
 - Implementierung von WPA3-Authentifizierungsprotokollen.

- Sicherheitsmodule:
 - Unterstützung für Verschlüsselung (z.B. AES) und Authentifizierung (z.B. SAE).
 - Fehlerbehandlung:
 - Protokollierung und Benachrichtigung von Sicherheitsereignissen.
3. Firmware- und Treiberschicht
- Netzwerk-Treiber:
 - Implementierung der WLAN- und Bluetooth-Treiber.
 - Hardware-Abstraktionsschicht (HAL):
 - Bereitstellung einer Schnittstelle zur Hardware (z.B. Antenne, Chipsatz).
4. Hardware
- Mikrocontroller (MCU):
 - Steuert die WLAN- und Bluetooth-Funktionalität.
 - WLAN/Bluetooth-Modul (z.B. Murata Type 1DX):
 - Hardware-Implementierung der WLAN- und Bluetooth-Verbindungen.
 - Sensoren:
 - Integrierte Sensoren zur Unterstützung von IoT-Funktionen.
5. Netzwerk- und Cloud-Integration
- Cloud-Backend:
 - Datenmanagement und -synchronisierung.
 - Sicherheitsüberprüfungen:
 - Regelmäßige Updates zur Sicherheit der Firmware.
6. Monitoring und Logging
- Protokollierungsdienste:
 - Aufzeichnung von Verbindungsereignissen und Sicherheitsprotokollen.
 - Analyse-Tools:
 - Überwachung der Netzwerksicherheit und der Verbindung.

Testplan für WPA3-verschlüsselte Firmware, hier beschränkt auf die sogenannte Top-Level Darstellung.

Testfall-ID	Testfallbeschreibung	Testkategorie	Erwartetes Ergebnis
TC-001	Überprüfung der WPA3-Authentifizierung	Funktionalität	Erfolgreiche Verbindung zu einem WPA3-Netzwerk
TC-002	Verbindung zu einem WPA2-Netzwerk	Kompatibilität	Verbindung wird hergestellt, WPA3 deaktiviert
TC-003	Test der Passwortsicherheit (Brute-Force-Angriff)	Sicherheit	Schutz gegen Passwortangriffe
TC-004	Überprüfung der Datenverschlüsselung	Funktionalität	Daten werden während der Übertragung verschlüsselt
TC-005	Test der Benutzeroberfläche für WLAN-Einstellungen	Usability	Intuitive Benutzeroberfläche mit klaren Anweisungen
TC-006	Test der OTA-Updates	Wartbarkeit	Erfolgreiche Installation von Firmware-Updates

TC-007	Protokollierung von Sicherheitsereignissen	Sicherheit	Alle sicherheitsrelevanten Ereignisse werden protokolliert
TC-008	Analyse der Verbindungsstabilität	Leistung	Stabilität der Verbindung über einen längeren Zeitraum
TC-009	Test der Rückwärtskompatibilität zu WPA/WPA2	Kompatibilität	Erfolgreiche Verbindung mit WPA/WPA2 Geräten
TC-010	Überprüfung der Sensorintegration	Funktionalität	Sensoren funktionieren einwandfrei über die WLAN-Verbindung
TC-011	Sicherheitstests für Forward Secrecy	Sicherheit	Früherer Sitzungsschlüssel kann nicht kompromittiert werden
TC-012	Performance-Test der WPA3-Authentifizierung	Leistung	Akzeptable Authentifizierungszeiten unter Last

Arbeitspaket 3: Applikationsentwicklung für den HTTP-Server/

Arbeitspaket 4: Integration und Benutzerfreundlichkeit:

Die Darstellung erfolgt beispielhaft für die Steuerung von Lampen (Smart-Home)

Verfügbare LEDs (Lampen) einer FRITZ!Box werden automatisch abgerufen und in der SmartHome-FB.txt Datei gespeichert. In diesem Beispiel zeigen wir, wie Sie die Schlafzimmer Lampe steuern, Sie heißt hier „LED1“.

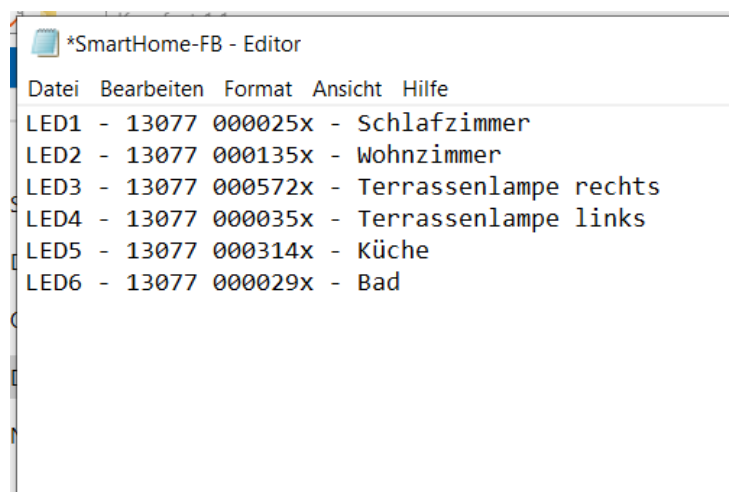


Abb. 7: [Beispiel: Smart-Home Lampen]

Voraussetzung ist die Einrichtung, hier am Beispiel an einer FRITZ!Box.

GEQUDIO
Deutsch

Funktionstaste
Side Key
Flexibel belegbare Taste
Fortgeschritten

- > Systemmenü
- > Netzwerk
- > Leitung
- > Telefon Einstellungen
- > Telefonbuch
- > Anrufliste
- > Funktionstaste
- > Anwendung
- > Sicherheits
- > Gesprächsprotokoll

Funktionstasteneinstellungen

DSS-Taste weiterleiten
Modus: Blindes weiterleiten

Dsskey Home Page: None

Dsskey Edit: Short Press/Lor

Übernehmen

Seite1
Seite2
Seite3
Seite4
Seite5

Löschen
Neue Seite hinzufügen

Taste	Art	Name	Wert	Wert2	Unterart	Leitung	Anruf Hohlen Nummer	Icon Color
DSS Key 1	Action URL	Schlafzimmer-ein	3.38:8080/LED1-ein		HTTP(s) Get	AUTO		Default Green
DSS Key 2	Action URL	Schlafzimmer-aus	.38:8080/LED1-aus		HTTP(s) Get	AUTO		Default Green
DSS Key 3	Keine				Keine	AUTO		Default Green
DSS Key 4	Keine				Keine	AUTO		Default Green
DSS Key 5	Keine				Keine	AUTO		Default Green
DSS Key 6	Keine				Keine	AUTO		Default Green

Übernehmen

Version: 2.4.9.0

Abb. 8: [Zuweisung zu programmierbaren Tasten]

Nachfolgende Befehle sind möglich:

LED1-ein = Lampe einschalten
 LED1-aus = Lampe ausschalten
 LED1-warm = Lampe warmweiß (2700K)
 LED1-kalt = Lampe kaltweiß (6500K)
 LED1-25 = Helligkeit auf 25%
 LED1-50 = Helligkeit auf 50%
 LED1-75 = Helligkeit auf 75%
 LED1-100 = Helligkeit auf 100%
 LED1-rot = Lampe rot
 LED1-blau = Lampe blau
 LED1-magenta = Lampe magenta
 LED1-gruen = Lampe grün
 LED1-tuerkis = Lampe türkis
 LED1-pink = Lampe pink

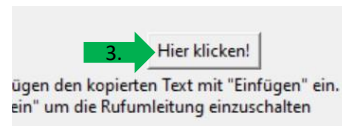
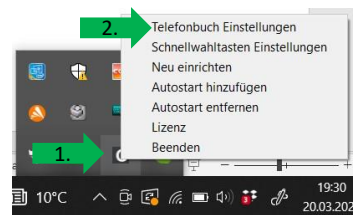
Ein weiteres Beispiel ist die Einrichtung der Telefonbuchabfragen hier zu Visualisierung über die Schnittstelle (GEQUDIO Komfort) an einem PC. Funktion kann äquivalent im IP-Telefon integriert werden.

Telefonbuchabfrage einrichten

Voraussetzungen:

- [Telefonbuch](#) in der Fritzbox eingerichtet.
- [Cloud-Telefonbücher](#) in der Fritzbox eingerichtet falls Sie diese abrufen möchten.
- Das GEQUDIO Telefon ist an der FritzBox registriert und die Ersteinrichtung der GEQUDIO Komfort Software ist erfolgreich abgeschlossen.

1. Klicken Sie mit der rechten Maustaste auf das GEQUDIO Komfort Logo
2. Klicken Sie anschließend mit der linken Maustaste auf „Telefonbuch Einstellungen“
3. Es öffnet sich ein Fenster. Klicken Sie auf den „Hier Klicke!“ Button in dem neuen Fenster um einen Text zu kopieren.

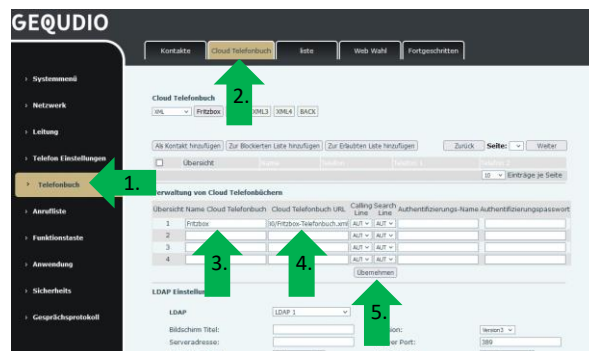


GEQUDIO

43

Telefonbuchabfrage einrichten

1. Klicken Sie im GEQUDIO Webinterface auf „Telefonbuch“
2. Dann auf „Cloud Telefonbuch“
3. Vergeben Sie hier den Namen „Fritzbox“
4. Mit der rechten Maustaste in das Feld „Cloud Telefonbuch URL“ klicken und dann „Einfügen“. Es wird folgendes eingefügt:
`http://192.168.xxx.xx:8080/Fritzbox-Telefonbuch.xml`
5. Klicken Sie auf „Übernehmen“.



GEQUDIO

44

Telefonbuchabfrage einrichten

Prüfen Sie anschließend, ob das Telefonbuch verfügbar ist:

1. Drücken Sie am Telefon die „Menü“ Taste unter dem Bildschirm.
2. Wählen Sie „Telefonbuch“ mit den Pfeiltasten aus und drücken „OK“
3. Navigieren Sie auf „Cloud Kontakte“ und bestätigen mit „OK“
4. Die Kontakte werden abgerufen und angezeigt.
5. Die Kontakte werden automatisch alle 5 Minuten von der FritzBox abgerufen.



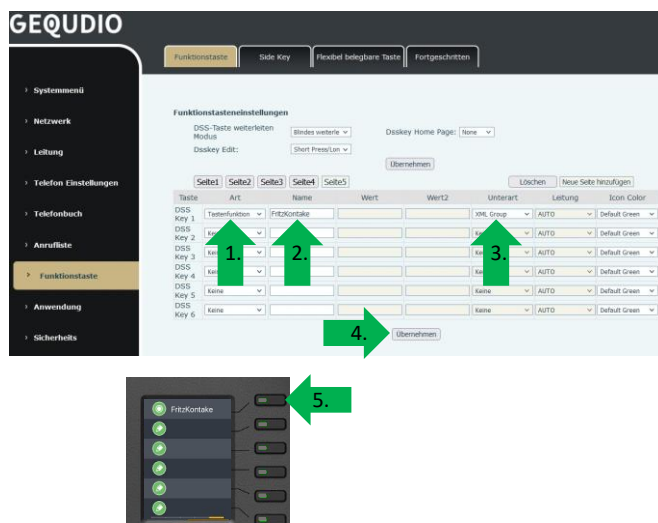
GEQUIDIO

45

Telefonbuchabfrage einrichten

Wenn Sie das Telefonbuch mit einem Tastendruck abrufen möchten, können Sie eine Schnellwahltaste dafür konfigurieren.

1. Art „Tastenfunktion“
2. Vergeben Sie einen Namen
3. Unterart „XML Group“
4. „Übernehmen“
5. Über diese Taste kann jetzt das Telefonbuch abgerufen werden



GEQUIDIO

46

Telefonbuchabfrage einrichten

Wenn die Taste unter dem Bildschirm angezeigt werden soll können Sie dafür auch eine Taste einrichten.

1. Funktionstaste
2. Flexibel belegbare Taste
3. Art „Tastenfunktion“
4. Vergeben Sie einen Namen
5. Unterart „XML Group“
6. Weiter unten auf „Übernehmen“ klicken

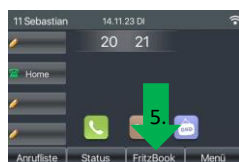
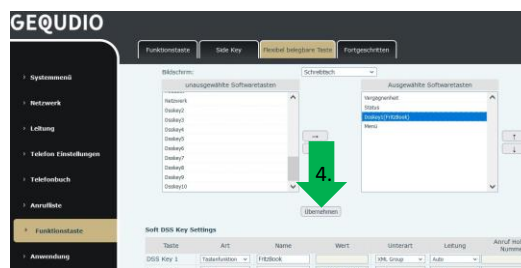
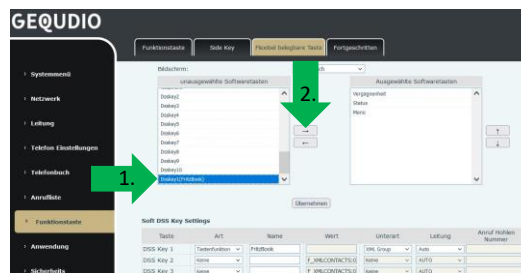


GEQUIDIO

47

Telefonbuchabfrage einrichten

1. Markieren Sie die erstellte DSS Taste in der Liste
2. Drücken Sie die Pfeiltaste nach rechts
3. Verschieben Sie die Taste an die gewünschte Position
4. Mit „Übernehmen“ abschließen.
5. Die Taste erscheint jetzt im Display



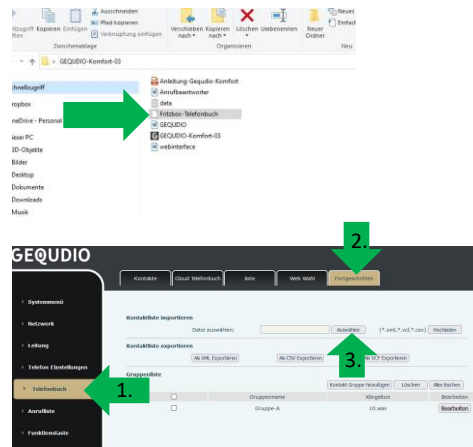
GEQUIDIO

48

Telefonbuch übertragen

Die Kontakte werden alle 5 Minuten von der FritzBox abgerufen und in der „Fritzbox-Telefonbuch.xml“ Datei abgespeichert. Diese „.xml“ Datei können Sie auch auf das Telefon hochladen, damit die Kontakte dauerhaft im Telefonbuch gespeichert sind, auch wenn Ihr PC ausgeschaltet oder GEQUDIO Komfort nicht eingeschaltet ist. Dann werden diese jedoch nicht synchronisiert.

1. Wählen Sie „Telefonbuch“
2. Dann „Fortgeschritten“
3. „Auswählen“

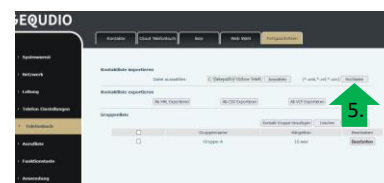
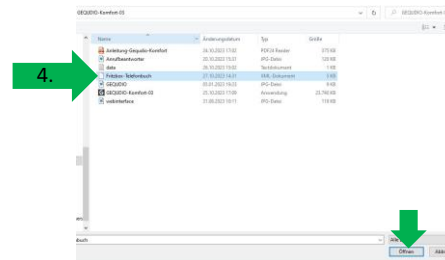


GEQUDIO

49

Telefonbuch übertragen

4. Wählen Sie die „Fritzbox-Telefonbuch.xml“ Datei aus.
5. „Hochladen“ drücken um die Datei auf das Telefon hochzuladen.
6. Die Kontakte sind dauerhaft auf dem Telefon gespeichert und können abgerufen werden, wenn GEQUDIO Komfort nicht eingeschaltet ist.



GEQUDIO

50

Abb. 9: [Beispiel: Telefonbuch übertrage]

Arbeitspaket 5: Produktion und Lieferketten

Diese Arbeitspaket wurde durch einen externen Dienstleister erbracht. Die Darstellung erfolgt hier lediglich auszugsweise.

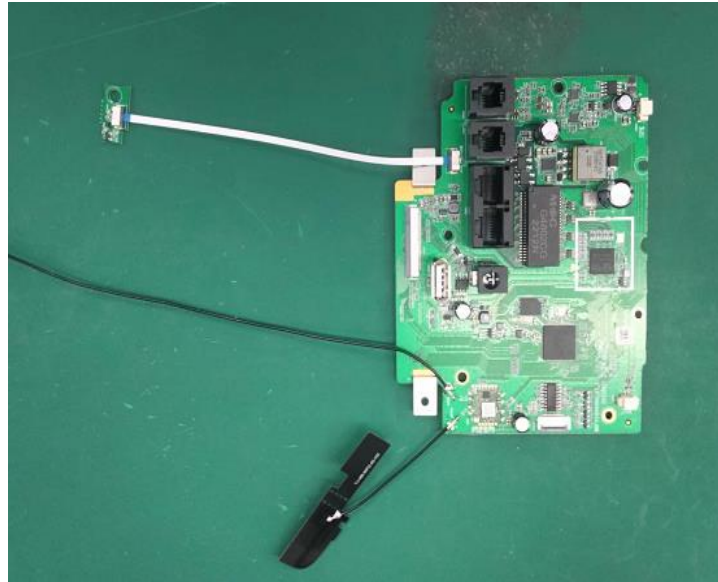


Abb. 10: [Montage der WLAN-Antennen vom GEQUDIO Modell: GZ-6]



Abb. 11: [Baugruppen-Montage vom GEQUDIO Modell: GZ-6]

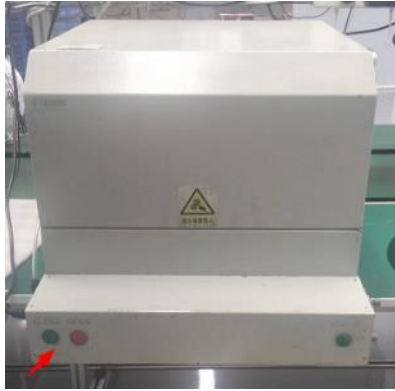


Abb. 12: [WLAN-Tastkammer vom GEQUDIO Modell: GZ-6]

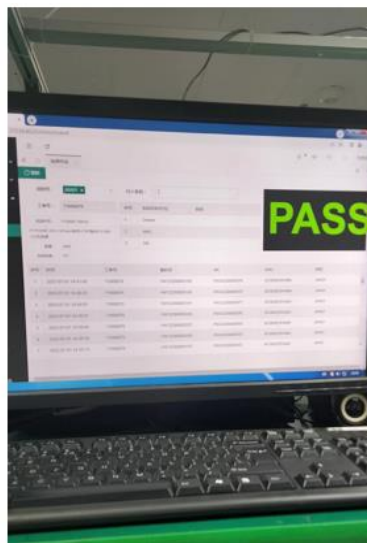


Abb. 13: [Funktions-Test vom GEQUDIO Modell: GZ-6]



Abb. 14: [Endmontage vom GEQUDIO Modell: GZ-6]



Abb. 15: [Verkaufsartikel: GEQUDIO GZ-6]

Arbeitspaket 6: Regulatorisch & Produkt-Dokumentation (4 Monate x 0,1 PM)

Für die Standard-Konformität gemäß CE-Kennzeichnung wurden die nachfolgenden Standards als zutreffend identifiziert:

Norm	Kurz-Bezeichnung	Themenbereich	Kurze Erklärung
EN 55032:2015+A11:2020	Störstrahlung	Elektromagnetische Verträglichkeit	Beschreibt die Grenzwerte für Störstrahlung, die von Informationstechnologie-Geräten (IT-Geräten) abgestrahlt werden dürfen.
EN IEC 61000-3-2:2019	Oberschwingungen	Elektromagnetische Verträglichkeit	Legt Grenzwerte für Oberschwingungen fest, die von Geräten in Niederspannungsnetzen erzeugt werden dürfen.
EN 61000-3-3:2013+A1:2019	Spannungsschwankungen	Elektromagnetische Verträglichkeit	Beschreibt die Anforderungen an Geräte, um Störungen durch Spannungsschwankungen und Flicker zu tolerieren.
EN 55035:2017+A11:2020	Störsicherheit	Elektromagnetische Verträglichkeit	Legt die Anforderungen an die Störsicherheit von Audio-, Video- und ähnlichen elektronischen Geräten fest.
EN 62368-1:2014+A11:2017	Sicherheit	Sicherheit von Informationstechnologie-Equipment	Definiert die Sicherheitsanforderungen für Informationstechnologie-Equipment (ITE) und Audio-/Video-Equipment (AV-Equipment).
ETSI EN 301 489-1 V2.2.3 (2019-11)	Funkgeräte	Funkgeräte und -systeme	Beschreibt die technischen Anforderungen an Funkgeräte und -systeme, die in Europa betrieben werden sollen.

ETSI EN 301 489-17 V3.2.4 (2020-09)	Funkgeräte	Funkgeräte und - systeme	Beschreibt spezifische Anforderungen an Funkgeräte und -systeme, z.B. für den Betrieb in bestimmten Frequenz- bändern.
--	------------	-----------------------------	---

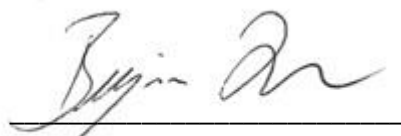
Die zutreffenden Standards für das beim IP-Telefon mitgelieferte Stecker-Netzteil werden hier nicht benannt, sind jedoch zu berücksichtigen.

Produktanleitungen und weitere Dokumente werden auf der Produktseite in der jeweils aktuellen Version zur Verfügung gestellt.

Abschluss-Betrachtung

Das Projekt mit seinen Arbeitspaketen wurde vollumfänglich und ohne Abweichungen abgeschlossen. Ich danke den involvierten Personen für die Teilnahme und Umsetzung des Projektvorhabens.

Mit freundlichen Grüßen,



Benjamin Ziebarth (02.11.2024)