Vorstellung System BlueSecur

Inhalt

1 Scope / Anwendungsbereich 3
2 Systemvoraussetzungen Smartphone 3
3 BlueSecur-fähige Produkte 3
4 Grundfunktionen der App BlueSecur 3
4.1 HET/S24-BLE 3
4.2 Antriebe SupraMatic 4 und RollMatic 2 3
5 Technischer Aufbau 3
5.1 Bluetooth Low Energy 3
5.2 Internetverbindung 4
5.3 Speicherung im Empfänger / Antrieb 4
5.4 Uhrzeit des Empfängers / Antriebs 4
6 Zugriffsrechte / Permissions 5
7 Schlüsselinformationen 6
7.1 Schlüsselarten 6
7.2 Schlüssel kaufen + Schlüssel teilen 6
7.3 Schlüssel entfernen 7
7.4 Schlüssel-Status 8
8 Registrierung, Login, Account 9
9 Backup 9
9.1 Zweck 9
9.2 Gespeicherte Daten 9
10 Datenschutz + Datenanalyse 10
11 Reset HET, SupraMatic 4 & RollMatic 2 11
12 Fehler / Meldungen / Hinweise 12
13 Apple Watch 12

1 Scope / Anwendungsbereich

Dieses Dokument dient der Beschreibung des Systems BlueSecur und kann als Nachschlagewerk verwendet werden.

BlueSecur ist ein System bestehend aus der App Hörmann BlueSecur und Empfängern. Empfänger sind entweder der externe Zubehör-Empfänger HET/S24-BLE, oder in den Antrieben SupraMatic 4 und RollMatic 2 integrierte Empfänger. Kommuniziert wird über den Funk Bluetooth Low Energy.

Neben der Hörmann BlueSecur App, gibt es noch die OEM`s Garador, Tubauto, Steinau und Berner. Funktional sind die Apps identisch, lediglich das App-Icon unterscheidet sich und die URL`s die zum Backend führen sind unterschiedlich.

2 Systemvoraussetzungen Smartphone

- iOS: Ab Betriebssystemversion 12 -> ab AppleWatch 13
- Android: Ab Betriebssystemversion 5

3 BlueSecur-fähige Produkte

- Externer Bluetooth Empfänger „HET/S24-BLE“
- SupraMatic 4
- RollMatic 2

4 Grundfunktionen der App BlueSecur

Mit der App BlueSecur ist es möglich, Befehle per BLE an den HET-BLE, oder an die Antriebe SupraMatic 4 und RollMatic 2 zu senden.

4.1 HET/S24-BLE

- Impuls an die beiden Relais des HET-BLE
- Widgets erstellen
- Relaiseinstellungen: Schaltend und Tastend sowie Einstellen der Relaishaltezeit

4.2 Antriebe SupraMatic 4 und RollMatic 2

- Einstellen der Kanäle Impuls, Auf, Zu, Licht, Teilöffnung und Lüftungsposition
- Abruf der Diagnosedaten Torlaufzyklen, Betriebsstunden, Letzter Werksreset, Anzahl Werksreset, Letzte Lernfahrten und Letzte Fehler
- Widgets erstellen

5 Technischer Aufbau

5.1 Bluetooth Low Energy

Für die folgenden Aktionen muss sich der User in BLE Reichweite befinden:

- Für das Senden eines Befehls
- Admin 2 beim Importieren des empfangenen Zugangsrecht

- Schlüssel entfernen / blockieren
- Abrufen der Diagnosedaten

Technische Daten:

- Reichweite: ca. 2-10 Meter.
    - Zur Steigerung der Reichweite kann eine externe Bluetooth-Antenne angeschlossen werden. Diese muss in der App in den Einstellungen aktiviert werden.

  Diese hängt allerdings stark von mehreren Faktoren ab. Wie sind die örtlichen Gegebenheiten, welches Smartphone, wie ist das Wetter, gibt es Störfaktoren im Umfeld…
- Frequenz: 2,4 GHz
- Dauer der BLE Verbindung: ca. 1-2 Sekunden bis ein Befehl ausgeführt wurde.

5.2 Internetverbindung

Für die folgenden Aktionen wird eine Internetverbindung benötigt:

- Für das Teilen einer Zugangsberechtigung
- Für das Empfangen einer Zugangsberechtigung
- Für das Kaufen von Schlüsselprodukten
- Für das Erstellen eines Backups

Zudem wird eine Internetverbindung benötigt, um Daten an das Daten-Dashboard zu senden. Dies ist allerdings nur für Hörmann interessant und wichtig.

5.3 Speicherung im Empfänger / Antrieb

Der Empfänger und die Antriebe verfügen über einen Speicher, in dem die BlueSecur User gespeichert werden.

Der erste User, der sich per QR Code Scan als Admin am Empfänger / Antrieb einlernt wird mit einer eindeutigen Kennung auf dem Empfänger / Antrieb gespeichert. Daher weiß der Empfänger / Antrieb auch, dass bereits ein Admin eingelernt ist.
Erstellt der Admin nun weitere Schlüssel für einen Empfänger / Antrieb, erhalten auch diese Schlüssel eine eindeutige Identifikation, die auf der Kennung des ersten Admins aufbaut. So weiß der Empfänger, dass der verteilte Schlüssel berechtigt ist den Empfänger / Antrieb zu bedienen.

5.4 Uhrzeit des Empfängers / Antriebs

Der Empfänger / die Antriebe verfügen über eine interne Uhr. Somit können vom Admin Benutzerschlüssel mit einer definierten Gültigkeit erstellt und geteilt werden.
Ist die Gültigkeit eines Schlüssels abgelaufen, wird dies vom Empfänger / Antrieb erkannt und die Bedienung verweigert.
Sollte der Empfänger / der Antrieb stromlos sein, ist die Uhrzeit des Empfängers / des Antriebs nicht mehr korrekt. Es kann kein Abgleich mehr mit zeitlich begrenzten Schlüsseln stattfinden. In diesem Fall kann ein zeitlich begrenzter Schlüssel, trotz noch eigentlich vorhandener Gültigkeit den Empfänger / den Antrieb nicht mehr bedienen.
Adminschlüssel, oder dauerhafte Benutzerschlüssel haben weiterhin Zugriff.

Mit einem Befehl eines Admins, oder eines dauerhaften Benutzerschlüssels wird die Uhrzeit des Empfängers / des Antriebes wieder korrekt gesetzt. Anschließend haben auch wieder zeitlich begrenzte Benutzerschlüssel Zutritt.

6 Zugriffsrechte / Permissions

Zur Bereitstellung unserer Dienste über die APP benötigen wir Zugriff auf folgende Funktionen des Handys:

- Standortdaten:
  - Die Standortdaten gelten nur für das Betriebssystem Android bis zur Version 11.
  - Datenzugriff (Access):
  - Datenverwendung (Usage): Standortberechtigungen werden benötigt, um per Bluetooth Low Energy zu ermitteln, ob ein Gerät in Bluetooth Reichweite ist. Mit einer erteilten Standortberechtigung können Sie Ihre Geräte bedienen.
  - Datensammlung (Collect): Es werden keine Standortberechtigungen gespeichert.
  - Datenweitergabe (Share): Es werden keine Standortberechtigungen mit weiteren Personen, oder Diensten geteilt.

  Ab Android 12 lautet die Berechtigung „Gerät in der Nähe“.

- Hintergrund-Standortdaten:
  - Gilt nur für Android 10 und 11 und werden auch nur bei diesen Betriebssystemversionen explizit abgefragt. Zudem werden Sie nur im Rahmen der Widgets genutzt.
  - Datenzugriff (Access):
  - Datenverwendung (Usage): Die Standort Hintergrundberechtigung wird benötigt, um mit Ihren bluetoothfähigen Geräten zu interagieren, auch wenn Ihre App geschlossen ist. Die App verwendet Hintergrund-Standortberechtigungen nur, wenn Sie Widgets verwenden möchten. Mit diesen Berechtigungen wird die Funktion aktiviert, die feststellt, ob sich ein Bluetooth Low Energy-fähiges Gerät in Reichweite befindet oder nicht und ermöglicht die Interaktion mit diesem Gerät, auch wenn die App geschlossen ist oder sich im Hintergrund befindet.
  - Datensammlung (Collect): Es werden keine Hintergrund-Standortberechtigungen gespeichert.
  - Datenweitergabe (Share): Es werden keine Hintergrund-Standortberechtigungen mit weiteren Personen, oder Diensten geteilt.
- Kamera:
  - Datenzugriff (Access): Zugriff auf die Kamera, um einen mitgelieferten QR Code zu scannen. Durch diesen Scanvorgang werden kompatible Geräte in der App eingelernt.
  - Datenverwendung (Usage): QR-Code einlesen
  - Datensammlung (Collect): Es werden keine Kameraaufnahmen gespeichert.
  - Datenweitergabe (Share): Es werden keine Kameraaufnahmen mit weiteren Personen, oder Diensten geteilt.

- Kontaktliste:
  - Datenzugriff (Access): Es wird auf die „Kontakte“-Anwendung des Endgerätes zugegriffen, um weiteren Personen Öffnungsberechtigungen weiterzugeben.
  - Datenverwendung (Usage): Weitergabe von Öffnungsberechtigungen

- Datensammlung (Collect): Es werden keine Kontakte gesammelt.
- Datenweitergabe (Share): Es werden keine Kontakte mit weiteren Personen, oder Diensten geteilt.

Diese Zugriffrechte werden bei Bedarf von der App abgefragt und eingefordert.
Werden diese abgelehnt, können sie nachträglich noch in den Systemeinstellungen des Smartphones aktiviert werden.

7 Schlüsselinformationen

7.1 Schlüsselarten

-  **Adminschlüssel**:
  Der Nutzer der das Gerät einlernt ist automatisch der erste Admin. Dieser kann exakt nur einen weiteren Adminschlüssel teilen.
  Mit einem Adminschlüssel können Sie weitere Benutzerschlüssel teilen und Einstellungen am Gerät vornehmen.
  Es können maximal zwei Admins je Gerät erstellt werden.
-  **Benutzerschlüssel:**
  Dieser Schlüssel kann mit, oder ohne zeitliche Begrenzung geteilt werden. Ein Benutzerschlüssel kann keine Einstellungen am Gerät vornehmen.
  Je Admin können ca. 250 Benutzerschlüssel erstellt werden.
-  **Einmalschlüssel**:
  Dieser Schlüssel kann exakt einmal benutzt werden. Nach der Verwendung ist er nicht mehr gültig. Der Einmalschlüssel hat eine maximale Gültigkeit von einem Monat. Dieser Schlüssel ist kostenfrei.
  Je Admin können 15 Einmalschlüssel gleichzeitig erstellt werden.

7.2 Schlüssel kaufen + Schlüssel teilen

- Um Schlüssel zu teilen müssen zuvor Schlüssel via InAppKauf gekauft werden.
- 1 Schlüssel = 8,99 €
- 5 Schlüssel = 34,99 €
- Der Schlüsselkauf findet außerhalb der BlueSecur App statt. Der Kauf wird von Google oder Apple abgewickelt.
- Gekaufte Schlüssel können für den Admin-, als auch für die Benutzerschlüssel verwendet werden. Beim Schlüsselkauf wird nicht zwischen Admin- und Benutzerschlüssel unterschieden.
- Im Schlüsselkontingent können die Schlüssel gekauft werden.
- Die Schlüssel können für die eingelernten Geräte erstellt und via Messengerdienste (E-Mail, Whatsapp, usw.) geteilt werden.
- Für das Teilen kann ein unverschlüsselter, oder ein verschlüsselter Weg gewählt werden.
- Der verschlüsselte Weg verläuft nach dem TAN-Prinzip. Per SMS wird eine TAN an den Benutzer gesendet, der den Schlüssel empfangen soll. Wird die TAN korrekt eingegeben, ist die Authentifizierung erfolgreich und der Schlüssel wird zugestellt.

7.3 Schlüssel entfernen

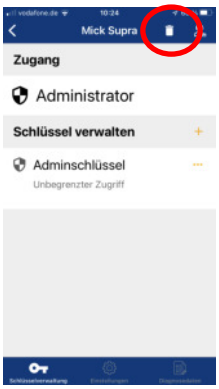
- **Adminschlüssel:**

Bitte gehen Sie in die Bluetooth-Reichweite Ihres Gerätes.

Sie haben einen Adminschlüssel geteilt:

WICHTIG: Damit der Schlüssel gutgeschrieben werden kann, müssen Sie zwingend eingeloggt / registriert sein!

Löschen Sie Ihr Gerät aus der App.



1. Sie haben einen SupraMatic Serie 4 mit integriertem Bluetooth Empfänger.

    - Drücken und halten Sie die Taste PRG am Antrieb bis 00 angezeigt wird.
    - Drücken Sie die Taste Pfeil hoch so oft bis 19 angezeigt wird.
    - Drücken Sie die Taste PRG **ein**mal, 00 blinkt.
    - Drücken Sie 2-mal auf die Taste Pfeil hoch, 02 wird angezeigt.
    - Drücken und halten Sie die Taste PRG, 02 blinkt, blinkt dann schneller, 19 wird angezeigt.
    - Lasse Sie die Taste PRG los.
    - Drücken Sie so oft auf die Taste Pfeil runter bis 00 angezeigt wird.
    - Drücken Sie die Taste PRG **ein**mal, ein Strich wird angezeigt.
    - Aktivieren Sie die Bluetooth Funktion am Antrieb, indem Sie die Bluetooth Taste **ein**mal drücken, das Bluetooth Symbol blinkt rot.
    - Nun können Sie den QR Code des Antriebs mit der BlueSecur App erneut einscannen, um den Antrieb neu in Betrieb zu nehmen.

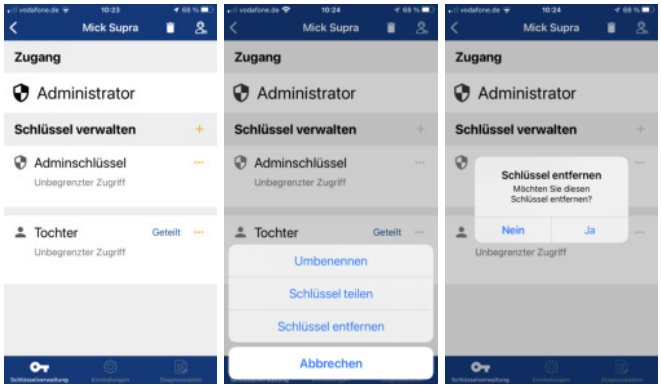
2. Sie haben einen externen HET/S 24 BLE Empfänger:

    - Öffnen Sie den Deckel des HET/S 24 BLE.
    - Auf der Platine befindet sich eine Taste, drücken und halten Sie diese Taste.
    - Die LED fängt an blau zu blinken.
    - Die LED blinkt schneller blau, lassen Sie die Taste los.
    - Nun können Sie den QR Code des HET/S 24 BLE erneut mit der BlueSecur App scannen.

- **Geteilten Benutzerschlüssel**

Bitte gehen Sie in die Bluetooth-Reichweite Ihres Gerätes.

- Sie gehen in die Ansicht „Schlüsselverwaltung“ und entfernen die Schlüssel die Sie zuvor geteilt und versendet hatten. Dies machen Sie über das 3-Punkte-Menü am Schlüssel.
- Nun werden diese entfernten Schlüssel wieder Ihrem Schlüsselkontingent gutgeschrieben.
- Jetzt müssen Sie den Schlüssel teilen Prozess leider erneut durchführen. D.h. Sie erstellen erneut die Schlüssel und teilen diese mit den gewünschten Personen.



- **Ungeteilten Benutzerschlüssel**

Um einen ungeteilten Benutzerschüssel zu löschen, muss man sich **nicht** in Bluetooth-Reichweite des Gerätes befinden.

Der Prozess einen ungeteilten Schlüssel zu entfernen ist ansonsten analog zu einem geteilten Benutzerschlüssel.

7.4 Schlüssel-Status

- **Ungeteilt** = Sie haben einen Schlüssel erstellt, diesen aber noch nicht geteilt
- **Geteilt** = Sie haben einen Schlüssel mit einem weiteren Nutzer innerhalb der letzten 24 Stunden geteilt, dieser hat den Schlüssel aber noch nicht vom Server abgeholt.
- **Abgelaufen** = Sie haben einen Schlüssel geteilt, dieser wurde aber nicht innerhalb von 24 Stunden durch einen anderen Nutzer vom Server abgeholt.
- **Aktiviert** = Sie haben einen Schlüssel geteilt und dieser wurde innerhalb von 24 Stunden durch einen anderen Nutzer importiert
- **Ungültiger Schlüssel:**
  - Der Antrieb wurde resettet.
  - Der Schlüssel wurde vom Admin wieder entzogen.
  - Der Antrieb war stromlos und die Uhr ist davon gelaufen -> aber nur bei Schlüssel mit zeitlicher Begrenzung.

8 Registrierung, Login, Account

Mit einer E-Mailadresse und einem Passwort können sich User in der App registrieren.
Optional kann auch die Mobilfunknummer hinzugefügt werden.

Nachdem sich ein User registriert hat, hat dieser einen Account erstellt.
In seinem Account wird ein Backup mit seinen Daten hinterlegt.
Das Backup befindet sich auf einem Server, welcher von der easy-smarthome GmbH (Bertelsons) gehostet wird.

Möchte ein Kunde sein Passwort ändern, kann er dies in seinem Account in der App vornehmen.
Hat ein Kunde sein Passwort vergessen und möchte ein neues erstellen, kann er sich per E-Mail Anweisungen zuschicken lassen. Hat der Kunde auch eine Mobilnummer hinterlegt, können die Anweisungen auch per SMS erfolgen.

9 Backup

9.1 Zweck

- Wenn Sie Geräte eingelernt und Schlüssel geteilt haben, können diese problemlos wiederhergestellt werden, z.B. bei einem Wechsel Ihres Smartphones. Nach einer Registrierung kann eine Sicherheitskopie (Backup) der Geräte erstellt werden.
- Wenn Sie Schlüssel gekauft haben, können diese problemlos wiederhergestellt werden, z.B. bei einem Wechsel Ihres Smartphones. Nach einer Registrierung kann eine Sicherheitskopie (Backup) der Geräte erstellt werden.
- Sollten Sie einmal Ihr Smartphone wechseln ist der Umstieg kinderleicht. Melden Sie sich auf dem neuen Smartphone einfach mit Ihrem Account an und Sie nehmen alle Ihre bereits gekauften Schlüssel sowie eingelernten Geräte mit auf das neue Smartphone.
- Sollte ein Reset am Antrieb oder am HET durchgeführt werden, sind die Daten nach dem Reset weiterhin vorhanden.

9.2 Gespeicherte Daten

- E-Mailadresse
- Anzahl gekaufter Schlüssel
- Alle eingelernten Geräte
- Alle erstellten Schlüssel
- Alle geteilten Schlüssel
- Diagnosedaten des Antriebes

Die Daten werden dauerhaft gespeichert. Sollen diese gelöscht werden, muss der Kunde dies bei uns anfordern.

Ein User hat keine Möglichkeit sich per Web-Oberfläche in seinen Account einzuloggen und dort Veränderungen an seinem Account vorzunehmen.

Wenn zu einem Token (E-Mailadresse) schon ein Backup existiert wird dieses "überschrieben". Wenn es ein neues Backup mit einem neuen Token ist, wird dieses auch neu erstellt. Es können also durchaus mehrere Backups existieren.

10 Datenschutz + Datenanalyse

Ab der BlueSecur Version xxx möchten wir mit Hilfe der App Daten einsammeln und auf einem Dashboard visualisieren.

Der User wird gefragt, ob er den Datenschutzbestimmungen inkl. der Datenanalyse zustimmt. Per Default ist diese Funktion deaktiviert.
Sollte der User zustimmen und möchte dies nachträglich widerrufen, gibt es unter dem Menüpunkt „Rechtliches“ das Untermenü „Einwilligung zur Datenanalyse“ Hier kann der Haken nachträglich entfernt werden.
Die Daten werden bei einem Systemstart, oder bei einem Befehl per Widget oder aus der App an den Server gesendet.

Alle Daten werden in Deutschland verwaltet, sodass wir den Datenschutzrichtlinien entsprechen.

Folgende Daten werden eingesammelt:

Folgende **Antriebsdaten** / **HET-Daten** können erhoben werden:

- Menüeinstellungen
- Fehler
- Power On Zähler
- Betriebsstunden
- Betriebsstunden seit Wartung
- Anzahl Wartungen
- Vollständige Torzyklen
- Vollständige Torzyklen seit Wartung
- Unvollständige Torzyklen
- Unvollständige Torzyklen seit Wartung
- Zeitpunkt Erstinbetriebnahme
- Zeitpunkt Werksreset
- Anzahl Werksreset
- Zeitpunkt Nachlernfahrt Kraft
- Zeitpunkt Nachlernfahrt Position
- Torzyklen Nachlernfahrt Kraft
- Torzyklen Nachlernfahrt Position
- Anzahl Fahrbefehle
- Anzahl Reversierfahrten
- Antriebslaufzeit in Sekunden
- Antriebslaufzeit seit letzter Wartung in Sekunden
- Relaiseinstellungen (HET)

Folgende **Smartphonedaten** können erhoben werden:

- Welches Betriebssystem
- Betriebssystem Version
- Sprache

- Smartphonehersteller und –typ
- Zeitzone
- Provider

- Daten zur App-Nutzung

Folgende Daten zur App-Nutzung können erhoben werden:

- Wann welcher Befehl gesendet wird
- Wann welcher Screen aufgerufen wird
- Wann auf welchen Button geklickt wird
- Eingeloggt, oder nicht eingeloggt
- Wann Einstellungen geändert wurden
- Wann Diagnosedaten abgerufen werden
- Wann und wie häufig die App gestartet wird
- Wann Schlüsselkäufe getätigt wurden
- Welche Schlüsselkäufe getätigt wurden
- Eingeloggte User: wie viele Schlüssel der User hat
- Wie viele Geräte in der App eingelernt sind
- Welche Geräte eingelernt sind
- Welche Kanäle aktiviert sind
- Welche Aktionen genutzt werden (Tor, Tür, Licht…)(HET)
- Welche App Version installiert ist
- Welche Schlüsselarten wurden von einem Admin erstellt und geteilt
- Interne, oder externe Antenne eingestellt

Zur Analyse Ihrer Daten nutzen wir ein Daten-Dashboard.

Diese Informationen befinden sich 1:1 in der App in den Datenschutzbestimmungen.

Detaillierte Informationen können im BlueSecur_Konzept Datenanalyse nachgelesen werden.

11 Reset HET, SupraMatic 4 & RollMatic 2

Wird ein HET/S24-BLE, ein SupraMatic 4, oder ein RollMatic 2 resettet, kann das eingelernte Gerät in der App nicht mehr genutzt werden.

Nach einem Reset kann der mitgelieferte QR Code erneut gescannt werden, um das Gerät neu einzulernen.
Der QR Code befindet sich im Gehäusedeckel (HET/S24-BLE), oder auf der Antriebskufe (SupraMatic 4)

12 Fehler / Meldungen / Hinweise

- Unbekannter Fehler = Kurzer Bluetooth-Aussetzer – ähnlich BT-Kopfhörer
  - Häufig im Grenzbereich, oder grundsätzlich, wenn mal ein schwaches Signal vorhanden ist.
- 10 Minuten Sperre = 3 mal falscher Login. Der Account wird für 10 Minuten gesperrt. Anschließend kann ein neuer Eingabeversuch gestartet werden. Sollte dieser Versuch erneut falsch sein, ist das Konto erneut für 10 Minuten gesperrt.
- Login-Konflikt = Es fand ein Login auf einem zweiten Smartphone statt.
  - Ein User ist auf Smartphone 1 eingeloggt.
  - Auf Smartphone 2 erfolgt ein Login mit den gleichen Login Daten (E-Mailadresse + Passwort)
  - Auf Smartphone 1 erscheint die Meldung „Login Konflikt“
- Antrieb kann nicht eingelernt werden.
- Fehler 51 = mandatory credentials missing = Anmeldeinformationen fehlen in der Anfrage
- Fehler 63 = Token is invalid or expired = Token ist abgelaufen oder ungültig
  - Passwort Reset - E-Mail erscheint und ist nur für eine Stunde gültig. Anschließend ist der Token abgelaufen und es erscheint Fehler 63.
- BlueSecur zu viele Logins = es wurde zu oft das falsche Passwort verwendet.
- Timeout recieved = BLE Kommunikation mit dem Empfänger gescheitert. Zeit ist abgelaufen, da die Kommunikation zu lange gedauert hat.
- QR Code kann nicht gelesen werden = Der Antrieb ist bereits eingelernt. Um den Antrieb erneut einzulernen, muss dieser über das Menü 19-02 resettet werden. Anschließend kann der Antrieb in der App erneut eingelernt werden.

13 Apple Watch

- Nutzbar für Kunden ab iOS 13
- Watch OS 6 oder 8
- Funktioniert autark, d.h. das Smartphone muss nicht in der Nähe der Watch sein.
- Business-Logik wurde extra für WatchOS entwickelt.