Informationssicherheit

Netzwerk

Regelung Nr. 03.02.01

Funknetzwerke

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Der Zweck dieser Regelung ist die Definition von Sicherheitsanforderungen für den Einsatz von Wireless LAN (WLAN), Bluetooth-Anbindungen und von Ein- und Ausgabegeräten.

Im Sinne dieser Regelung bedeutet der Begriff „Informationssicherheit“ IT-Sicherheit als Bestandteil einer ganzheitlichen Informationssicherheit.

1. Sicherer Einsatz von WLAN

1.1. Ziel

Der Zweck dieser Regelung ist die Definition von Sicherheitsanforderungen an Wireless LAN (WLAN) nach dem Standard IEEE 802.11. Ein WLAN ist definiert als ein Local Area Network (LAN), welches eine nicht-kabelgebundene Kommunikation zwischen den Geräten ermöglicht.

1.2. Grundsätze

1.2.1 Rahmenbedingungen

- Die zuständige Stelle[1] ist der Betreiber der WLAN Infrastruktur.
- Die zuständige Stelle[2] muss ein Betriebskonzept zur infrastrukturellen Nutzung von WLANs definieren. Dieses Konzept ist die technische Basis für WLANs.Die zuständige Stelle[3] muss ein technisches Umsetzungskonzept erstellen, welches den Einsatz von starker Verschlüsselung[4] („Zwangsverschlüsselung“) sicherstellt.

1.2.2 Allgemeine Anforderungen

- Die WLAN Infrastruktur darf ausschließlich durch die zuständige Stelle[5] verwaltet werden.
- Die durch AUDI BRUSSELS bereitgestellte WLAN Infrastruktur darf nur von Konzernmitarbeitern, zugelassenen Dienstleistern oder produktionstechnischen Systemen/Anlagen (shop floor) genutzt werden. Eine Ausnahme bildet, vom Konzernnetz separierte WLAN Infrastruktur, für Gäste.
- Es dürfen nur drahtlose Endgeräte betrieben werden, die durch die zuständige Stelle[6] freigegeben wurden. Dies ist über einen Zertifizierungsprozess für WLAN fähige Endgeräte sicherzustellen.

[1] Siehe Anhang B.1.2

[2] Siehe Anhang B.1.1

[3] Siehe Anhang B.1.2

[4] Siehe Anhang A.1.1

[5] Siehe Anhang B.1.2

[6] Siehe Anhang B.1.3

- Der Einsatz von WLAN ist nur im Infrastruktur-Modus zulässig. Die erforderlichen WLAN-Komponenten (z. B. Access Points) müssen durch die zuständige Stelle[7] freigegeben, implementiert und zentral verwaltet werden. Es dürfen keine Peer-to-Peer-WLANs (so genannte Ad-hoc-Netzwerke) von Audi betrieben werden.
- Andere Kommunikationsprotokolle als IP Version 4 oder höher müssen durch die betreibende Stelle[8] freigegeben werden. Neue Infrastrukturen müssen ausschließlich dieses Protokoll unterstützen. Andere Protokolle müssen so herausgefiltert werden, dass ausschließlich IP in das Konzernnetzwerk gelangen kann.
- Aufstellung und Übertragungsstärke der Accesspoints bzw. Antennen muss so gewählt werden, dass ausschließlich das gewünschte Gebiet funktechnisch abgedeckt wird.
- Es müssen Technologien oder Prozesse umgesetzt werden, die das Erkennen von “wilden” Access Points (rogue access points) ermöglichen, sofern dies nicht die Funktion des WLAN beeinträchtigt. Erkannte „wilde“ Access Points (rogue access points) müssen entfernt werden.
- Wenn eine Filterung am Netzübergang zwischen WLAN und kabelgebundenem LAN nötig ist, müssen mobile Geräte im WLAN in eigenen Layer 3 Domänen (eigenständiges Segment oder VLAN mit Funktion einer Broadcastdomain) angeschlossen werden.
- Gesellschaftsspezifische Regelungen[9] bzgl. der Frequenzen, die im Rahmen von WLAN im Infrastruktur Modus verwendet werden, müssen beachtet werden.
- Ein gleichzeitiger Anschluss von WLAN Clients an ein anderes Netzwerk ist nicht zulässig, wenn das andere Netzwerk andere Schutzanforderungen hat.
- Der Einsatz von Funkbrücken[10] ist nur zulässig, wenn während der Funkübertragung eine gleichwertige Verschlüsselung der Verbindung und gleichwertige Authentisierungstechniken umgesetzt sind.
- Network Address Translation (NAT) darf auf Access Points nicht eingesetzt werden.

1.2.3 Authentifizierung, Autorisierung und Auditierung

- Es ist eine NAC Lösung zu implementieren, die das blockieren von unbekannten Endgeräten ermöglicht.
    - Gegenseitige Authentifizierung gemäß des Standards IEEE 802.1X und mit EAP-TLS muss über einen Authentifizierungsserver implementiert werden.
    - Zertifikate für Authentifizierung dürfen nur durch Zertifikatsstellen (certification authorities) des Konzerns ausgestellt werden und müssen zentral verwaltet werden.
    - Sollte es technisch nicht möglich sein die gegenseitige Authentifizierung gemäß IEEE 802.1X zu implementieren, ist es zulässig WPA2/WPA2-PSK (Wireless Protected Access with Pre Shared Keys) mit AES-Verschlüsselung zwischen

[7] Siehe Anhang B.1.3

[8] Siehe Anhang B.1.2

[9] Siehe Anhang B.1.4

[10] Dies beinhaltet auch WLAN Repeater und Client-Brücken

WLAN Client und access point zu verwenden. Dabei sind folgende Bedingungen zu erfüllen:

- Die zuständige Stelle[11] überprüft die technischen Anforderungen
- Die zuständige Stelle hat den Einsatz von WPA2-PSK dokumentiert und freigegeben
- Festlegung und Dokumentation einer Person, die für das WLAN der Abteilung verantwortlich ist
- Diese Person ist verantwortlich für:
  - Management der PSKs
  - Sichere Speicherung der PSKs
  - Schutz vor unberechtigtem Zugriff
- Verwenden verschiedener PSKs pro use-case
- Länge des PSK: Mindestens 20 Zeichen und entsprechend der Komplexitätsanforderungen der zuständigen Stelle.

o Sollten diese Anforderungen nicht erfüllt werden können, müssen zusätzliche Maßnahmen zur Sicherstellung des Sicherheitsniveaus getroffen werden. Hierzu ist gemäß dem Ausnahmeprozess zu verfahren.

- Alle Authentifizierungen und Authentifizierungsversuche (erfolgreich / nicht erfolgreich) müssen entsprechend der Logging-Regelung protokolliert werden.

1.2.4 Verschlüsselung

- Jede Kommunikation über WLAN muss starke Verschlüsselung[12] verwenden.
- Dynamische Schlüssel müssen für jeden Nutzer und jede Verbindung unter Verwendung von 802.1x und EAP-TLS verwendet werden.

1.2.5 Management

- Vor der Implementierung im Netzwerk müssen alle Passwörter und Default-Schlüssel geändert werden.
- Passwörter müssen gemäß der Passwortregelung für systembezogene Benutzerkennungen[13] gesetzt werden.
- Die Access Points müssen zentral erfasst werden.
- Die Access Points sollten in ein zentrales Netzwerk-Managementsystem eingebunden sein.
- Die Access Points sollten über ein Netzwerk-Managementsystem konfiguriert werden.
- Access Points müssen über eine kabelgebundene LAN Verbindung konfiguriert werden.

[11] Siehe Anhang B.1.3

[12] Siehe Anhang A.1.1

[13] Siehe Anhang A.1.4

- Wireless LAN Infrastruktur darf nur durch die zuständige Stelle[14] betrieben werden. Der Betrieb durch andere Stellen muss durch die zuständige Stelle genehmigt werden.
- WLANs müssen kontinuierlich überwacht und überprüft werden, um nicht autorisierte Nutzung frühestmöglich zu erkennen oder zu verhindern.

1.2.6 WLANs von Dritten auf dem Firmengelände

- Peer to peer WLANS (die nicht durch Audi betrieben werden) müssen in Verträgen mit Mitarbeitern und Anbietern reglementiert werden oder in einer generellen Regelung zum akzeptierten Umgang mit Ad-hoc-Netzwerken erfasst sein. Ad-hoc-Netzwerke in Produktionsumgebungen (shop floor) dürfen nur nach vorheriger Genehmigung der zuständigen Stelle[15] betrieben werden.
- Infrastruktur WLANs von Dritten auf dem Firmengelände müssen registriert und von der verantwortlichen Stelle freigegeben werden. Die verantwortliche Stelle darf diese Netzwerke nur unten den folgenden Bedingungen freigeben:
    - Es ist eine angemessene Dokumentation des WLANS vorhanden
    - Es gibt keine Verbindung zwischen dem WLAN und dem Konzernnetzwerk
    - Das WLAN verwendet die von der verantwortlichen Stelle[16] zugeteilten Kanäle
    - Jegliche Kommunikation über das WLAN muss Verschlüsselung nach den Vorgaben der Regelung Kryptographie[17] verwenden
    - Audi Mitarbeiter dürfen nicht in der Lage sein, sich mit diesen WLANs zu verbinden (beispielsweise durch eine erzwungene Authentifizierung)
- Die Kommunikation muss durch WPA2 oder äquivalente Technologien verschlüsselt sein.

[14] Siehe Anhang B.1.3

[15] Siehe Anhang B.1.3

[16] Siehe Anhang B.1.3

[17] Siehe Anhang A.1.1

2. Bluetooth

Bluetooth ist ein offener Standard zur Kommunikation über kurze Distanz per Funktechnik. Bluetooth wird überwiegend zum Aufbau drahtloser personal area Netzwerke verwendet. Der Standard bietet momentan keine ausreichenden Sicherheitsmaßnahmen für Authentifizierung, Autorisierung und Verschlüsselung. Dies ist vor dem Einsatz von Bluetooth-Verbindungen zu beachten. Wenn möglich, sollten andere Kommunikationswege mit besseren Sicherheitsvorkehrungen verwendet werden.

Die Anforderungen an Bluetooth-Verbindungen unterscheiden sich zwischen:

- Geräten mit Bluetooth-Funktionalitäten
  z.B. Mobiltelefone, Smartphones, Laptops, etc.
- Peripheriegeräte mit Bluetooth-Funktionalitäten
  z.B. Maus, Keyboard, Headset, etc.

Der Zweck von Bluetooth-Peripherie wird durch die Art des Designs festgelegt. Beispielsweise kann ein Bluetooth-Headset rein zur Sprachübertragung genutzt werden und eine Bluetooth-Tastatur als reines Eingabegerät. Andererseits können Geräte für eine Vielzahl von Zwecken genutzt werden. Ein Mobiltelefon kann z.B. über Bluetooth die Funktion eines Modems für ein Laptop bereitstellen. Ebenso kann Datenaustausch zwischen zwei Geräten über Bluetooth stattfinden.

2.1. Geräte mit Bluetooth Verbindungen

2.1.1 Ziel

In diesem Kapitel werden Sicherheitsanforderungen an Bluetooth-Verbindungen von Geräten (e.g. Notebooks, Smartphones, Laptops, etc.) definiert.

2.1.2 Grundsätze

Aktive Bluetooth-Module können die Leistung und Verfügbarkeit anderer Funkverbindungen und Systeme im Konzern beeinträchtigen.

- Rechtliche Vorgaben für Funkverbindungen müssen beachtet werden.
- Eine direkte Verbindung zum Konzernnetzwerk über Bluetooth-Infrastruktur ist nicht zulässig.
  - Überprüfung der Verträglichkeit eines Bluetooth Netzwerks bezüglich der Funkverbindung und/oder Störeinflüssen mit sich in der Nähe befindenden WLANs. Bluetooth-Übertragungen dürfen WLAN-Zugang nicht unterbrechen.
  - Um Störeinflüsse mit anderen Funknetzen (besonders WLAN) zu vermeiden und das Risiko von Angriffen auf Bluetooth Netzwerke zu senken wird empfohlen nur Geräte der Bluetooth Klassen[18] 2 oder 3 zu verwenden.
  - Die entsprechenden Regelungen[19, 20] zur Speicherung oder weiteren Verarbeitung von Daten auf Bluetooth-Geräten sind zu beachten.

[18] Siehe Anhang B.2.2

[19] Siehe Anhang A.1.3

[20] Siehe Anhang A.1.4

    - Geräte sollten “adaptive frequency hopping (AFH)” und “optimized paging and inquiry” unterstützen.
- Geräte sollten Bluetooth V2.4 (oder höher) verwenden. Neue Geräte müssen V2.4 oder höher verwenden.

2.1.3 Datenklassifikation und Sicherheitsanforderungen

Geschäftsbereiche, die Bluetooth-Geräte verwenden, müssen ihre Daten klassifizieren. Sicherheitsanforderungen an Bluetooth-Verbindungen basieren auf der Datenklassifikation.

2.1.3.1 Interne Daten

Es gelten die folgenden Anforderungen:

- Der Anwender muss die Authentizität des Kommunikationspartners überprüfen.
- Jegliche Kommunikation sollte verschlüsselt erfolgen[21] (sofern möglich).

2.1.3.2 Vertrauliche Daten

Zusätzlich zu 2.1.3.1:

- Jegliche Kommunikation hat verschlüsselt zu erfolgen[22].
- Die Übermittlung vertraulicher Daten über Bluetooth-Verbindungen ohne ausreichende zusätzliche Sicherheit (z.B. Datenverschlüsselung[23]) auf Applikationsebene ist nicht zulässig.

2.1.3.3 Geheime Daten

Geheime Daten dürfen nicht über Bluetooth-Verbindungen übertragen werden.

2.1.4 Bluetooth Konfiguration

- Es dürfen nur benötigte Profile aktiviert werden. Andere Profile müssen deaktiviert werden.
- Der operating mode sollte non-discoverable, non-connectable und non-pairable oder non-bondable sein. Sollte einer dieser modi aktiviert sein müssen, so ist dies nur für einen definierten Zeitraum zulässig.
    - Der Discoverable Mode sollte eine Zeitbegrenzung haben. Nach Ablauf der Zeit sollte das Gerät automatisch in den Non Discoverable Mode schalten.
    - Der Pairing Mode sollte eine Zeitbegrenzung haben. Nach Ablauf der Zeit sollte das Gerät den Pairing Mode automatisch abschalten.
    - Die Zeitbegrenzung soll 3 Minuten nicht überschreiten.

[21] Siehe Anhang A.1.1

[22] Siehe Anhang A.1.1

[23] Siehe Anhang A.1.1

2.1.5 Kopplung der Geräte (Pairing)

- Die Kopplung (Pairing) der Bluetooth Geräte muss in einer sicheren Umgebung durchgeführt werden, um ein Abhören während der Eingabe der PINs zu verhindern.
- Wenn beide Geräte mindestens Bluetooth-Spezifikation 2.1 + EDR unterstützen, sollte Secure Simple Pairing[24] (oder sicherere Verfahren) verwendet werden.
- Die PIN zum Pairing sollte 16 Zeichen lang sein.
- Die Verwendung von Master Key und Geräteschlüssel (Unit Key) ist nicht zulässig.

2.1.6 Allgemeiner Umgang

- Der Zugang zu der Konfiguration eines jeden Bluetooth Gerätes muss mindestens durch eine PIN geschützt sein.
- Unterstützt das Gerät die Änderung von PINs, muss der Anfangsschlüssel (PIN) vom Benutzer unmittelbar nach der Übergabe geändert werden.
- Die Liste der vertrauenswürdigen Kommunikationspartner muss regelmäßig durch den Benutzer überprüft werden.
- Benutzer müssen darauf achten, dass immer nur eine einzige Netzwerkverbindung gleichzeitig aktiv ist (z.B. Bluetooth-Verbindung zu einem Netzwerk oder Gerät vs. LAN, welches möglicherweise split tunneling ermöglicht).

2.1.7 Verwendung in Produktionsumgebungen (Shop Floor Areas)

- Geräte mit aktiviertem Bluetooth dürfen auf Grund möglicher Beeinträchtigungen anderer Funkübertragungen (WLAN, etc.) nicht in oder in der Nähe von Produktionsumgebungen (Shop Floor) betrieben werden.
- Ausgenommen sind Bluetooth Geräte, die Teil der Produktionsumgebung sind oder erforderlich sind, um Komponenten (z. B. Anlagen) der Produktionsumgebung zu administrieren.

2.2. Peripheriegeräte mit Bluetooth-Verbindungen

2.2.1 Ziel

Der Zweck dieser Regelung ist die Definition von Sicherheitsanforderungen für den Einsatz von Ein- und Ausgabegeräten (Peripherie) mit Funkanbindungen (z.B. Maus, Keyboards, Headsets…).

2.2.2 Grundsätze

- Landesspezifische, gesetzliche Vorschriften für Funkverbindungen müssen eingehalten werden.
- Bluetooth-Übertragungen dürfen durch Funkübertragung WLAN-Zugänge nicht unterbrechen oder stören.

[24] Siehe Anhang B.2.1

- Um anderer Funkverbindungen (speziell WLAN) nicht zu beeinträchtigen und das Risiko von Angriffen auf Bluetooth-Netzwerke zu senken, wird empfohlen nur Bluetooth der Klasse 2 oder 3[25] zu verwenden.
- Die entsprechenden Regelungen[26,27] zur Speicherung oder weiteren Verarbeitung von Daten auf Bluetooth-Geräten sind zu beachten.
    - Jegliche Kommunikation muss verschlüsselt erfolgen[28].
    - Ein-/Ausgabegeräte mit Funkanbindung (wie Keyboards, Lautsprecher, etc.) sollten nicht in Bereichen, in denen geheime Daten verarbeitet werden, eingesetzt werden.
    - Bei der Reparatur oder Verschrottung des Ein-/Ausgabegerätes müssen notwendige Sicherheitsaspekte beachtet werden (z. B. Löschen von Speichern).
    - Nach einer Reparatur eines Ein-/ Ausgabegerätes oder vor der Wiederverwendung durch einen neuen User muss der Schlüssel bzw. die PIN geändert werden.
    - Nach Verlust oder Diebstahl eines Geräts müssen sämtliche Paarungseinträge auf anderen Geräten, die das gestohlene Gerät betreffen, gelöscht werden

2.2.3 Bekanntmachen der Geräte (Pairing)

- Das Bekanntmachen (Pairing) der Bluetooth Geräte muss in einer sicheren Umgebung durchgeführt werden, um ein Abhören während der Eingabe der PINs zu verhindern.
- Die Verwendung von Master Key und Geräteschlüssel (Unit Key) ist nicht zulässig.

[25] Siehe Anhang B.2.2

[26] Siehe Anhang A.1.3

[27] Siehe Anhang A.1.4

[28] Siehe Anhang A.1.1

II. Verantwortlichkeiten

II.I Kapitel 1: Sicherer Einsatz von WLAN

Diese Regelung ist von allen Betreibern von WLANs und WLAN Endgeräten einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.II Kapitel 2: Bluetooth Anbindungen

Diese Regelung ist von allen Stellen, die für die Beschaffung, den Einsatz und den Betrieb von Bluetooth zuständig sind einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

A.1.2 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.3 Informationssicherheit Regelung Nr. 03.05.01 Physischer Schutz

A.1.4 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.5 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

A.2 Anlagen

A.2.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.3 Abkürzungen und Definitionen

Abkürzung / Bezeichnung	Erläuterung
Connectable Device	Ein Gerät, welches auf Anfragen über Netzwerkprotokolle antwortet wird als Connectable Device bezeichnet. Ein Verbindungsaufbau ist möglich.
Discoverable	Geräte die Discoverable sind, senden ihre Kennung auf ein Inquiry.
Inquiry	Allgemeine Kennungsabfrage von Geräten.
Page	Gezieltes Ansprechen eines Gerätes mittels der Bluetooth Adresse.
Pairable	Ein Gerät, das ein neues Vertrauensverhältnis mit einem anderen Kommunikationspartner eingehen kann.

A.4 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 06.08.2021

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[29].

A.5 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht

[29] Siehe Anhang A.2.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Sicherer Einsatz von WLAN

B.1.1 IT-Services

B.1.2 IT-Services

B.1.3 IT-Services

B.1.4 Siehe Dokument „Strategiepapier_100908_Audi_241008“ (Regulierung zu Frequenzen bei Audi), verfügbar bei IT-Services

B.2 Kapitel 2: Bluetooth

B.2.1 Bluetooth Security Mode

All definitions in this document refer to Bluetooth specification 2.1 + EDR.

(https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=241363&_ga=2.21023026.840818434.1503314562-1851474613.1493733113)

B.2.2 Bluetooth Device Classes of Power Management

Type	Max Power Level	Operating Range
Class1	100mW (20 dBm)	Up to 100 meter
Class2	2.5mW (4 dBm)	Up to 10 meter
Class3	1mW (0 dBm)	1 meter

dBm: decibles referenced to one milliwatt