Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.02

Kryptographie

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Zweck dieser Regelung ist die Definition von Prinzipien und Anforderungen / Rahmenbedingungen für die Verwendung und den Umgang von Kryptographie (z.B. Verschlüsselung) bei der AUDI BRUSSELS. Des Weiteren definiert diese Regelung organisatorische Anforderungen für die Etablierung und den Betrieb einer Public Key Infrastruktur (PKI), sowie Anforderungen an Registrierstellen (Registration Authority).

1. Verschlüsselung

1.1. Ziel

Bei AUDI BRUSSELS werden Systeme und Applikationen verwendet, die sensible Informationen in unterschiedlichen Umgebungen verarbeiten und speichern. Um die Vertraulichkeit und die Integrität der Informationen zu schützen ist es notwendig kryptographische Verfahren einzusetzen.

Ziel dieses Kapitel ist die Definition von Prinzipien und Anforderungen für die Verwendung und den Umgang mit Verschlüsselung.

Das Kapitel spezifiziert die Kriterien für den verpflichtenden Einsatz von kryptographischen Verfahren und definiert:

- Kriterien wann kryptographische Verfahren verwendet werden müssen oder sollen
- Anforderungen an die Verwendung kryptographischer Verfahren und Produkte
- Anforderungen für die Auswahl von kryptographischen Verfahren und Produkten
- Anforderungen an das Schlüsselmanagement

1.2. Prinzipien/Schutzziele

Kryptographischen Verfahren werden verwendet um

- Vertraulichkeit
- Integrität
- Authentizität
- Nachweisbarkeit

sicherzustellen.

1.2.1 Verschlüsselungstechniken

Generell ist eine Unterscheidung zwischen symmetrischer und asymmetrischer Verschlüsselung vorzunehmen.

Die Verschlüsselung muss in der Form gewählt werden, dass die Schutzziele solange gegen Angriffe gewahrt bleiben, wie dies erforderlich ist. Während der Lebensdauer der Lösung muss die Schlüssellänge oder der eingesetzte Algorithmus als sicher gelten, ansonsten ist Wechseln (Schlüssel und/oder Algorithmus) vorzusehen. Sofern ein Wechsel aus anderen

Sicherheitsgründen unterbunden wird, ist dies mit der verantwortlichen Stelle[1] individuell abzustimmen.

Symmetrische Verfahren verwenden denselben Schlüssel für die Verschlüsselung und Entschlüsselung. Dieser Schlüssel muss allen Beteiligten bekannt sein. Beispiele für symmetrische Verfahren sind DES und AES

Asymmetrische Verfahren (auch als Public Key Verfahren bekannt) nutzen ein Schlüssel-Paar, das sich aus einem privaten und einem öffentlichen Schlüssel zusammensetzt. Die Sicherheit asymmetrischer Verfahren basiert auf dem Theorem, dass eine Rekonstruktion des privaten Schlüssels über den öffentlichen Schlüssel äußerst schwierig (mit aktuellen Technologien aufgrund von Zeitfaktoren unmöglich) ist. Beispiele für asymmetrische Verfahren sind RSA und elliptische Kurven.

Asymmetrische Verfahren werden oft mit digitalen Zertifikaten verwendet. Ein digitales Zertifikat ist vergleichbar mit einem digitalen Ausweis. Die Ausweisstelle (als vertrauenswürdig eingestuft) garantiert, dass die Daten auf dem Ausweis tatsächlich der Person gehören, deren Foto sich auf dem Ausweis befindet.

Ein Zertifikat beinhaltet Informationen über den Namen seines Eigentümers, dessen öffentlichen Schlüssel, eine Seriennummer, einen Gültigkeitszeitraum, den Namen der Zertifizierungsstelle. Diese Daten sind mit dem privaten Schlüssel der Zertifizierungsstelle signiert und können durch den öffentlichen Schlüssel der Zertifizierungsstelle verifiziert werden (Verifizierung der Authentizität und Integrität). Im Falle einer hierarchischen Architektur von Zertifizierungsstellen wird die Authentizität durch die Signatur einer höherrangigen Zertifizierungsstelle sichergestellt. Diese "Zertifizierungskette" endet am bzw. an den Stammzertifikaten (root certificate), welche durch gegenseitige Bestätigungen mittels Signaturen durch die privaten Schlüssel der Stammzertifizierungsstellen (root certification authorities) signiert sind.

1.2.1.1 Symmetrische Verschlüsselung

Hauptmerkmale symmetrischer Verschlüsselung:

- Komplizierte Schlüsselverteilung (sofern kein vertrauenswürdiges Austauschmedium zur Verfügung steht).
- Alle Teilnehmer ein und derselben Kommunikation verwenden denselben Schlüssel. Für jede neue Kommunikationsinstanz muss ein neuer Schlüssel generiert werden: n Instanzen benötigen $\frac{n*(n-1)}{2}$ Schlüssel.
- Schnelle Verschlüsselung von Massendaten.
- Das einzige bewiesene sichere Verfahren ist die Vernam-Chiffre/One-Time-Pad.
- Sofern keine Quantenkryptographie verwendet wird, ist eine spontane verschlüsselte Kommunikation ohne vorherige Vertrauensbeziehung (mindestens zum Schlüsselaustausch) nicht möglich.

1.2.1.2 Asymmetrische Verschlüsselung

Hauptmerkmale asymmetrischer Verschlüsselung:

[1] Siehe Anhang B.1.1

- Für voneinander unabhängige verschlüsselte Kommunikationskanäle wächst die Zahl der Schlüssel linear mit der Zahl der Teilnehmer (bei symmetrischer Verschlüsselung wächst die Zahl wesentlich schneller mit der Zahl der voneinander unabhängigen Kommunikationsinstanzen).
- Im Vergleich zu symmetrischen Verfahren mit vergleichbarer Schlüssellänge sind alle bekannten asymmetrischen Verfahren sehr langsam. Zur Erreichung der gleichen Sicherheit, ist die benötigte Schlüssellänge gewöhnlich länger als bei symmetrischen Verfahren
- Digitale Signaturen sind möglich.
- Einfacher Schlüsselaustausch, private Schlüssel werden nicht ausgetauscht.
- Nicht geeignet für größere Datenmengen.

1.2.1.3 Hybride Verschlüsselung

Der Ausdruck hybride Verschlüsselung bezeichnet eine Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren um die Vorteile beider Verfahren zu nutzen. In der Praxis werden Nachrichten symmetrisch mit einem Sitzungsschlüssel verschlüsselt. Dieser Schlüssel muss lang genug sein, um einen erfolgreichen Brute-Force-Angriff auf den kompletten Schlüsselraum zu verhindern. Im Anschluss wird der Sitzungsschlüssel mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt und als Anlage an die verschlüsselte Nachricht mit angehängt.

1.2.2 Digitale Signaturen und Hash Funktionen

1.2.2.1 Digitale Signaturen

Durch die Verwendung digitaler Signaturen können folgende Punkte gewährleistet werden:

- Authentizität des Datenursprungs:

  Ermöglicht es dem Empfänger zu verifizieren, dass die Nachricht vom erwarteten Sender stammt.

- Datenintegrität:

  Ermöglicht es dem Empfänger zu verifizieren, dass die Nachricht auf dem Übertragungsweg nicht verändert wurde.

Es werden asymmetrische Verschlüsselungsverfahren genutzt[2].

Ein Teilnehmer, der eine digitale Signatur für ein Dokument erstellen möchte, muss ein Schlüsselpaar besitzen. Er verwendet seinen privaten Schlüssel zur Erstellung der Signatur. Der Empfänger verwendet dann den öffentlichen Schlüssel des Senders um die Korrektheit der Signatur zu verifizieren.

1.2.2.2 Hash Funktionen

Hash-Algorithmen generieren aus einer Nachricht ein verkürztes Abbild. Ein Hash-Algorithmus erlaubt es einem Nutzer eine Veränderung an der Originalnachricht zu erkennen, da der Hash-Algorithmus bei einer Veränderung ein wesentlich anderes Abbild liefert. Diese Algorithmen kommen bei hybriden Verfahren zum Einsatz. Allerdings sind nur sogenannte kryptographische Hash-Algorithmen geeignet und sicher. Ein kryptographischer Hash-Algorithmus verfügt über spezielle Kriterien: Es ist nahezu unmöglich einen passenden

[2] Siehe Kapitel 1.2.1.2

Datenauszug zu einem gegebenen Hash-Wert zu finden. Es ist zudem auch nahezu unmöglich zwei unterschiedliche Datenauszüge zu finden, die denselben Hash-Wert ergeben. Ein Beispiel für einen kryptographischen Hash-Algorithmus ist SHA-256.

Notwendige Eigenschaften eines Hash-Algorithmus sind:

- Kollisionsfreiheit:
  Es darf nicht in einer effizienten Art und Weise möglich sein zwei „verwendbare“ Eingaben zu finden, die denselben Hash-Wert erzeugen.
- Einwegfunktionalität:
  Es darf nicht in einer effizienten Art und Weise möglich sein, zu einem gegebenen Hash-Wert eine passende Eingabe zu finden.
- Kompression:
  Die Ausgabe ist ein Wert mit stets gleicher Länge.
- Pseudozufälligkeit:
  Ähnliche Texte müssen völlig unterschiedliche Hash-Werte ergeben.

1.3. Anwendung und Auswahl kryptographischer Verfahren und Produkte

1.3.1 Anwendung kryptographischer Verfahren

Die Entscheidung zur Verwendung kryptographischer Verfahren muss immer auf der Informationsklassifikation, dem Schutzbedarf und den relevanten rechtlichen Vorgaben basieren[3].

Entsprechend der Unternehmensrichtlinie „Informationssicherheit URLB_024“ sind die Informationen entsprechend zu klassifizieren und die Einhaltung der Vertraulichkeit, Integrität und Nachweisbarkeit sicherzustellen. Sofern dies nicht durch physikalische Abgrenzungen oder andere geeignete Verfahren sichergestellt werden kann, müssen

- als "vertraulich" klassifizierte Informationen bei der elektronischen Übertragung verschlüsselt übertragen werden. Zudem sollte eine verschlüsselte Ablage der Daten auf persistenten Speichermedien erfolgen. Bei Nutzung von Cloud-Umgebungen muss dies zwingend erfolgen.
- als "geheim" klassifizierte Informationen bei der elektronischen Übertragung verschlüsselt übertragen werden. Auch die Ablage der Daten hat verschlüsselt zu erfolgen.[4]. Die verwendeten Algorithmen müssen mindestens die definierte minimale Schlüssellänge[5] unterstützen.

[3] Siehe Anhang A.1.2

[4] Siehe Anhang A.1.2

[5] Siehe Anhang C.1

Die Verwendung kürzerer als der im Anhang[6] definierten Schlüssellängen, ist nur in berechtigten Ausnahmefällen nach Genehmigung durch die verantwortliche Stelle[7] erlaubt.

1.3.2 Auswahl kryptographischer Verfahren

Es müssen kryptographische Verfahren verwendet werden, deren Sicherheit und Stärke von Experten[8] bewertet und bestätigt wurde. Bei der Entscheidung für ein kryptographisches Verfahren muss der aktuelle Stand der Technik, die vorgesehene Anwendung und der entsprechende Zeitraum, in dem die Informationen geschützt werden sollen, beachtet werden. Im Besonderen muss die Stärke des kryptographischen Algorithmus und eine ausreichende Schlüssellänge beachtet werden. Weitere Informationen über geeignete Algorithmen und Protokolle finden sich im Anhang[9].

Im Anhang[10] sind kryptographische Algorithmen aufgeführt die als sicher für die Verwendung innerhalb der AUDI BRUSSELS angesehen werden. Die Verwendung von anderen Algorithmen muss durch die verantwortliche Stelle[11] genehmigt werden.

Es dürfen nur dokumentierte und für Sicherheitsüberprüfungen öffentlich verfügbare kryptographische Verfahren genutzt werden. Des Weiteren muss bewertet werden, ob für den benötigten Zweck symmetrische, asymmetrische oder hybride Verschlüsselungsverfahren geeignet sind.

Für unterschiedliche Schutzziele müssen unterschiedliche kryptographische Verfahren verwendet werden:

Vertraulichkeit:

- Symmetrische Verschlüsselungsverfahren
- Asymmetrische Verschlüsselungsverfahren
- Hybride Verschlüsselungsverfahren

Integrität:

- Hash-Algorithmen um Hash-Werte zu generieren
- Hash-Algorithmen bei denen ein symmetrischer Schlüssel in die Berechnung integriert ist, sogenannte Message Authentication Codes (MACs), können die Integrität sicherstellen
- Asymmetrische Signaturverfahren können die Integrität sicherstellen

Nachweisbarkeit:

- Asymmetrische (Signatur) Verfahren können die Nachweisbarkeit sicherstellen

---

[6] Siehe Anhang C.1

[7] Siehe Anhang B.1.1

[8] Siehe Anhang B.1.1

[9] Siehe Anhang A.3.1 und A.3.2

[10] Siehe Anhang C.1

[11] Siehe Anhang B.1.4

- Die Nachweisbarkeit kann durch die Verwendung von Signaturen mit gültigen digitalen Zertifikaten sichergestellt werden

Es gibt keine kryptographischen Verfahren, welche die Verfügbarkeit verbessern oder sicherstellen können. Dennoch ist es beim Einsatz von Kryptographie wichtig, dass die Verfügbarkeit und Erreichbarkeit nicht mehr als nötig beeinträchtigt werden.

1.3.3 Auswahl kryptographischer Produkte

Abhängig vom Schutzbedarf[12] der Informationen müssen zertifizierte Produkte (z. B. Common Criteria EAL 4+ oder FIPS 140-2) eingesetzt werden. Die Funktionalität und die Einhaltung des spezifizierten Bewertungslevels müssen durch Überprüfungen unabhängiger Dritter gewährleistet werden. Unabhängige Audits qualifizierter Dritter können für die Bewertung von Produkten ebenfalls herangezogen werden. Kryptographische Produkte müssen insofern Benutzerfreundlich sein, dass alle Mitarbeiter die Verschlüsselungssoftware problemlos nutzen können und dadurch das Risiko für Bedienfehler und potentielle Kompromittierungen minimiert wird. Während der Produktauswahl muss entschieden werden, welche Art von Komponente (software-, firmware- oder hardwarebasiert) am besten für den Einsatzzweck geeignet ist.

1.3.4 Organisatorische Anforderungen

Jeder Mitarbeiter der kryptographische Verfahren (z. B. Smartcards, Dateiverschlüsselung) spezifiziert, implementiert, betreibt oder verwendet, sollte in der Verwendung des jeweiligen kryptographischen Produkts geschult werden. Zusätzlich sollten die Mitarbeiter auf die Vorteile und die Notwendigkeit der Verwendung kryptographischer Verfahren hingewiesen werden und eine Einführung in die Grundlagen der Kryptographie erhalten.

Probleme, IT-Sicherheitsvorfälle oder vermutete Vorfälle im Zusammenhang mit kryptographischen Produkten müssen der entsprechenden Stelle[13] gemeldet werden.

Jeder Benutzer muss über die Regelungen zur Verschlüsselung[14] (abhängig von der Datenklassifikation), sowie die Berichtswege[15] für den Verlust oder die Kompromittierung von Schlüsseln oder Authentifizierungsmitteln informiert werden.

1.3.5 Technische Anforderungen

Um nach einem Systemfehler oder einer Softwareneuinstallation die Konfiguration schnell wiederherstellen zu können, muss vor der Überführung in die Produktion die gewünschte Konfiguration des kryptographischen Produkts (z. B. Schlüssellänge, Betriebsmodus, kryptographischer Algorithmus) definiert und dokumentiert werden.

Die kryptographischen Produkte für Benutzer müssen durch den Administrator so vorkonfiguriert werden, dass die benötigte Sicherheitsstufe ohne das Eingreifen des Benutzers erreicht wird.

Kryptographische Produkte müssen so implementiert werden, dass

---

[12] Bei geheimen Daten sind nur zertifizierte Produkte zulässig

[13] Siehe Anhang B.1.2

[14] Siehe Anhang A.1.2

[15] Siehe Anhang A.1.2

- der Benutzer die benötigten Grundfunktionen nicht technisch umgehen kann,
- nur die für den Betrieb verantwortliche Stelle die Konfiguration ändern kann.

Für komplexe kryptographische Produkte müssen entsprechende Handbücher vorliegen.

Der Zugang zu kryptographischen Schlüsseln von Benutzern muss durch Passwörter oder PINs geschützt werden.

1.4. Schlüssel Management

1.4.1 Einführung

Eine wesentliche Aufgabe bei der Verwendung von Kryptographie ist das Management der dazugehörigen Schlüssel. Um einen sicheren Betrieb zu gewährleisten müssen organisatorische Prozesse und technische Vorkehrungen implementiert werden. Notwendige Prozesse für das Schlüsselmanagement müssen dokumentiert werden. Es muss vor allem definiert und dokumentiert werden wer zu welchen Schlüsseln Zugang hat und wie Schlüssel vor unautorisierter Verwendung geschützt werden.

1.4.2 Schlüsselerzeugung

Die Schlüsselerzeugung sollte in einer sicheren Umgebung unter Verwendung von geeigneten kryptographischen Schlüsselgeneratoren[16], die unvorhersagbare, statistisch gleichverteilte Zufallssequenzen unter Nutzung des kompletten zur Verfügung stehenden Schlüsselraums erzeugen, erfolgen. Falls für die Schlüsselerzeugung Benutzereingaben verwendet werden, sollten diese schwierig vorhersagbar sein und durch geeignete technische Maßnahmen unterstützt werden.

1.4.3 Schlüsselseparierung

Sofern möglich, sollten kryptographische Schlüssel nur für einen Einsatzzweck verwendet werden. Verschlüsselungs- und Signaturschlüssel sind zu trennen, d.h. diese sind unterschiedlich zu wählen. Damit soll sichergestellt werden, dass der Signaturschlüssel vom Benutzer nur bewusst verwendet werden kann.

1.4.4 Schlüsselverteilung

Die Schlüsselverteilung muss durch Maßnahmen (z. B. Verschlüsselung, persönliche Zustellung, Versenden per Einschreiben), die dem Schutzbedarf entsprechen, gesichert werden.

1.4.5 Schlüsselinstallation

Während der Schlüsselinstallation muss sowohl die Authentizität, als auch die Integrität, des Schlüsselmaterials verifiziert werden.

1.4.6 Schlüsselspeicherung

Kryptographische Schlüssel müssen so gespeichert werden, dass sie vor unautorisiertem Zugriff geschützt sind.

Systeme, die Schlüsselmaterial speichern, müssen angemessen geschützt sein. Der Zugang muss auf eine kleine Gruppe autorisierter Personen eingeschränkt sein Der private Schlüssel muss verschlüsselt gespeichert werden und darf nicht exportierbar sein.

[16] Siehe Anhang A.3.1

Ein Backup der Schlüssel sollte regelmäßig durchgeführt und an Speicherorten, die den oben genannten Anforderungen entsprechen, gespeichert werden.

1.4.7 Schlüsselarchivierung und -ablage

Schlüssel dürfen nur unter folgenden Bedingungen abgelegt (bzw. archiviert) werden:

- Der Zugriff ist auch notwendig, wenn der Originalschlüssel nicht verfügbar ist (z. B. wenn ein Mitarbeiter das Unternehmen verlässt oder aufgrund von Krankheit abwesend ist).
- Die Schlüssel werden nur zur Verschlüsselung verwendet.
- Private Schlüssel dürfen niemals archiviert werden.

Für die Anforderungen an die Speicher von Schlüsselmaterialen werden grundlegend 2 Arten von Anwendungsfällen unterschieden:

- Schlüssel zur Sicherstellung der Identität/Vertraulichkeit (private Schlüssel)
- Schlüssel zur Sicherstellung der Authentizität/Validität (öffentliche Schlüssel)

Der Schlüsselspeicher für private Schlüssel:

1. Muss eine abgesicherte API besitzen, die die privaten Schlüssel für kryptographische Aufgaben nutzt (keine Herausgabe des privaten Schlüssels)
2. Darf NICHT auslesbar sein, bzw. darf KEINE Schnittstelle „Schlüsselherausgabe“ enthalten (gilt für den Ablage-Speicher UND den Verarbeitungsspeicher/-prozess)
3. Muss gegen alle aktuell bekannten Site-Channel-Attacken geschützt sein (Timing, Power-Analysis, Abstrahlung – optisch; thermisch; akustisch; magnetisch; statisch, Input-Datenbasiert, etc.)
4. Muss, falls erforderlich, das Einbringen eines temporären Schlüsselmaterials für Verschlüsselung, für einen definierten Zeitraum (Zeit/Eventbasiert) ermöglichen; Das Einbringen von Schlüsseln zum Zwecke der Signatur/Authentisierung darf NICHT möglich sein, auch dann nicht, wenn dieser Schlüssel für Verschlüsselung genutzt wird.

Der Schlüsselspeicher für öffentliche Schlüssel:

1. MUSS solange schreibgeschützt sein, bis bestimmte autorisierende Rahmenbedingungen erfüllt sind, die die spezifische API zum Schlüsseltausch freigeben.
2. Muss eine API besitzen um nachvollziehbare kryptographische Aktionen mit den Public-Keys durchführen können
3. Muss in einen sicheren Prozess zur Validierung der Authentizität eingebunden sein
4. Muss authentische Antworten für den Anfragenden liefern, die der Anfragende selbst prüfen kann

1.4.8 Schlüsselwechsel

Um potentiellen Kompromittierungen zu begegnen, müssen Schlüssel regelmäßig gewechselt werden. Bei der Einführung des kryptographischen Verfahrens muss die Häufigkeit des Schlüsselwechsels durch die für den Betrieb verantwortliche Stelle definiert werden. Die Häufigkeit des Schlüsselwechsels hängt von verschiedenen Parametern ab:

- Gerätetyp oder Medium (z. B. Langzeitdatenspeicher, Datenübertragungsmedium)
- Kryptographischer Algorithmus
- Schlüssellänge
- Feststellung von Angriffen (z. B. Diebstahl oder Verlust des Schlüssels)
- Schutzbedarf der Daten
- Häufigkeit der Verwendung des Schlüssels
- Umfang der verschlüsselten Daten
- Relevantes Bedrohungspotential
- Sicherheit der Schlüsselspeicherung

Bei einer bestätigten Kompromittierung oder dem Verdacht darauf muss die für den Betrieb verantwortliche Stelle[17] sofort den Schlüsselaustausch unter Berücksichtigung der Rahmenbedingungen wie „Schwachstelle wurde behoben“ veranlassen. Sofern technisch und rechtlich möglich sollten alle von der Gesellschaft zur Verfügung gestellten oder gespeicherten Daten, die mit dem kompromittierten Schlüssel verschlüsselt sind, sicher gelöscht, mit einem neuen Schlüssel verschlüsselt und erst dann wieder zur Verfügung gestellt werden.

1.4.9 Schlüsselzerstörung

Schlüssel die nicht länger benötigt werden (z. B. abgelaufene Schlüssel) müssen sicher gelöscht oder zerstört werden (z. B. durch mehrfache Löschung/Überschreibung und/oder mechanische Zerstörung des Speichermediums). Hierbei ist darauf zu achten, dass Verschlüsselungsschlüssel für zum Beispiel Backups über den eigentlichen Verwendungszeitraum hinaus benötigt werden. Dies kann auch für andere Anwendungsfälle erforderlich sein.

1.4.10 Schlüsselschutz

Schlüssel müssen gegen Veränderung, Diebstahl, ungeplanten Verlust und mutwillige Zerstörung gesichert werden. Mitarbeiter und externe Partner sind verpflichtet die für sie ausgestellten Schlüssel sorgfältig zu behandeln. Private Schlüssel, die einer Person gehören (unabhängig davon ob es sich um einen Verschlüsselungs- oder Signaturschlüssel handelt), dürfen nicht mit anderen geteilt werden. Hardware die für die Schlüsselerzeugung, -verteilung, -speicherung und -archivierung verwendet wird, muss gegen unautorisierten Zugriff, Verlust, Diebstahl oder Beschädigung durch geeignete physische Maßnahmen geschützt werden.

[17] Siehe Anhang B.1.3

2. PKI

2.1. Ziel

Eine Public Key Infrastructure (PKI) verwendet kryptographische Verfahren und kann verwendet werden um den Sicherheitsanforderungen[18] von Systemen und Applikationen Rechnung zu tragen.

Das Ziel dieses Kapitels ist die Definition der notwendigen organisatorischen Anforderungen für die Implementierung und den Betrieb einer PKI in der AUDI BRUSSELS sowie die Bereitstellung von weiterführenden Informationen diesbezüglich.

Insgesamt gilt es hierbei das Vertrauen im elektronischen Austausch innerhalb der AUDI BRUSSELS / Audi-VW-Konzern und mit Partnerunternehmen zu sichern.

Detaillierte technische Maßnahmen sind in diesem Kapitel nicht enthalten.

2.2. Generelle Prinzipien

Die folgenden Grundsätze gelten für eine im Netzwerk der AUDI BRUSSELS betriebe PKI:

- Alle PKI Certificate Authority (CA) Installationen müssen an eine der bereitgestellten Root CAs „VW-PKI“, „MOD CA“ oder „Product PKI“ der VW-Group angebunden werden.
- Für jede CA (Root-CA und Sub-CA) ist durch den jeweiligen Betreiber eine Certificate Policy (CP) und ein Certification Practice Statement (CPS) zu erstellen und zu publizieren.

Jede Konzerngesellschaft, die in ihrem Bereich Zertifikate und Schlüsselträger ausgeben will, muss die Funktionen einer Registration Authority (RA), gemäß den Anforderungen der verwendeten CA[19], umsetzen.

Eine PKI besteht aus:

- organisatorischen
- technischen
- administrativen

Maßnahmen zur sicheren

- Erstellung
- Verteilung
- Pflege

von

- Zertifikaten
- Schlüsseln

[18] Siehe Kapitel 1

[19] Siehe Kapitel 2.3

- Schlüsselträgern (Chip-Karten, Dateien oder maschinell lesbaren Datenträger)

für asymmetrische Verschlüsselungsverfahren, sowie aus einer CA, die eine richtige Zuordnung von Zertifikaten zu deren Inhabern gewährleistet.

Der Betreiber der PKI hat sicherzustellen, dass die hierfür notwendigen Prozesse etabliert sind und bei Bedarf auditiert werden können.

2.3. Certification Authorities / Trust Center

2.3.1 Einführung

Wenn über PKI diskutiert wird, werden meist nur die technischen Bestandteile betrachtet (die Verwendung der Public Key Kryptografie und deren Systeme, um folgende Funktionen zu ermöglichen: starke Authentisierung, Datenintegrität, Unbestreitbarkeit und Vertraulichkeit).

Diese unterstützenden Funktionen erfordern jedoch eine Infrastruktur (das "I" in PKI).

Diese Infrastruktur umfasst mehr als nur kryptografische Technologien. Sie beinhaltet auch die Richtlinien, die die Verwendung der PKI regeln.

Um die bestehenden, traditionellen Transaktionsverfahren durch PKI-Techniken zu unterstützen kann es zusätzlich notwendig sein, Änderungen an Geschäftsprozessen vorzunehmen.

2.3.2 Betroffene Parteien

Die PKI-Implementierungen stellen die Basis für die Umsetzung der Regelungen dar, die auf die Netzwerke und integrierte, schnell-verarbeitenden Vertrauensapplikationen angewendet werden müssen.

Wie auch bei traditionellen Vertrauensmodellen (z. B. Notar), existieren mehrere Parteien, Interessens- und Regelungsfragen.

An der PKI beteiligte Parteien:

- Person oder Organisation, die durch das Zertifikat identifiziert wird (Subjekt oder Abonnent).
- Aussteller des Zertifikates, welcher die Identität der im Zertifikat enthaltenen Subjektinformationen garantiert.
- Organisation, die den Nutzern die Zertifikats- und/oder Validierungsinformationen bereitstellt.
- Gesellschaft, Agentur oder das Individuum, welche dem Zertifikat vertraut (vertrauende Partei).

2.3.3 Certificate Policy (CP) - „was muss ich tun“

Die Policy für eine CA wird in einer CP dokumentiert und ist für andere vertrauende Parteien einsehbar. Hiermit deklariert die CA den zugedachten Zweck des Zertifikates gegenüber einer vertrauenden Partei, die das Zertifikat verarbeiten möchte.

Praktisch gesehen ist eine “vertrauende Partei” jemand, der bei der Verwendung des Zertifikates “Wert generiert”. Daher hat die vertrauende Partei ein erhebliches Interesse an der CP, die die Erstellung und Verwendung des Zertifikates regelt.

Mit den höher werdenden Sicherheitsanforderungen einer Transaktion werden auch die Anforderungen an die Zuverlässigkeit der CA und der dafür angewandten Verfahren höher. Diese Anforderungen variieren abhängig vom Zweck der Zertifikatsnutzung.

Die Anforderungen, die die Erstellung und Verwendung der Public Key Zertifikate regeln, werden „Certificate Policy“ genannt. Gemäß der IETF (Internet Engineering Task Force) Framework Definition ist eine Certificate Policy „eine definierte Regelgruppe, welche die Anwendbarkeit eines Zertifikates für eine bestimmte Personengruppe und/oder Applikationsklasse regelt, die gemeinsamen Sicherheitsanforderungen unterliegen.“

2.3.4 Certification Practice Statement (CPS) - „wie muss ich es tun“

Das IETF Framework definiert das Certification Practice Statement als die „Feststellung des Verfahrens, das eine CA bei der Erstellung von Zertifikaten einsetzt“.

Ein Certification Practice Statement wird oft mit einer Certificate Policy verwechselt, aber es spiegelt die Feststellung der Verfahren wieder, die notwendig sind, um den jeweiligen Anforderungen einer oder mehrerer CPs zu entsprechen oder um vertrauenden Parteien und Abonnenten die Überprüfung der Vertrauensstärke einer CA und deren erstellten Zertifikaten zu ermöglichen.

2.3.5 Die Unterstützung einer CP mit weiteren Dokumenten

Zusammen mit den notwendigen unterstützenden rechtlichen Dokumenten (z. B. Vereinbarung mit vertrauenden Parteien und Erklärung zum Datenschutz) besitzt eine PKI-Policy Regelung wenig Wert ohne explizite Einbindung in die bestehenden regulatorischen und geschäftlichen Infrastrukturen, Geschäftsvorfälle und Applikationen.

2.4. Zertifikat-Validierung

Im Rahmen der Zertifikatsbasierten Authentifizierung müssen alle Anwendungen beim Verbindungsaufbau die Server-Zertifikate auf Authentizität prüfen. Dabei sind alle Zertifikate der gesamten Zertifikat-Kette (Zertifikat-Pfad) zu prüfen.

Im Prüfumfang für die Sub-CA-Zertifikate und Blatt-Zertifikate sind immer:

1. Zeitliche Gültigkeit aller Zertifikate
2. Kryptograpische Korrektheit der Signaturen
3. Prüfung auf Zertifikat-Revozierung (in Abhängigkeit von Kritikalität CRL oder OCSP)
4. Korrektheit der erwarteten CN- und Issuer-Einträge
5. Korrektheit der erwarteten Zertifikat-Kette

Es ist sicherzustellen, dass sich die erforderliche RootCA der Zertifikat-Kette im Trust-Store des Gerätes befindet. Ggf. ist hier ein RootCA-Zertifikat-Deployment auszuarbeiten, welches die Einbringung ohne Anwendungsdeployment ermöglicht.

Sofern für die Anwendungen eine Datenklassifikation von „geheim“ erfolgt ist, ist in der Anwendung eine RootCA-CN-Festlegung und SubCA-Pfad-CN-Festlegung einzusetzen. Hierbei ist allerdings darauf zu achten, dass immer ein AdHoc-RootCA-Tausch möglich ist und dass eine alternative RootCA-CN inkl. CA-Pfad fest integrierter Bestandteil des Deployment ist. (Mindestens zwei zulässige Root-CA-Pfade inkl. Sub-CAs). Alternativ dürfen in diesen Fällen auch Technologien wie DNS-DANE eingesetzt werden.

In jedem Fall ist die Prüfung auf

- Zeitliche Gültigkeit der Zertifikate,
- die Prüfung auf Zertifikat-Revozierung und
- die Korrektheit der erwarteten Zertifikat-Kette

durchzuführen.

Sollten sich aufgrund von Aktualisierungen ein Kettenglied der SubCA-Zertifikate (gleicher CN und Issuer-Eintrag) geändert haben und damit die Hashwerte verschieden sein, so ist zu prüfen, ob die RootCA noch als Vertrauensanker vorhanden ist und es ist die vollständige Zertifikat-Prüfung der gesamten Kette durchzuführen. (Mindestens bis zum nächsten validen Kettenstück in Richtung RootCA.)

Da für die CNs von RootCAs und SubCAs im Allgemeinen keine DNS-Namen eingesetzt werden, kann in Einzelfällen davon ausgegangen werden, dass bei der Prüfung nur ein fest vorgegebener Teil des CN verglichen werden muss/darf. (Einzelfallentscheidung, die Dokumentiert und begründet werden muss!)

Für die Prüfung ist im Allgemeinen die vom Server-System gelieferte Information zu verwenden und die Entwickler für die Client-Anwendungen können/dürfen davon ausgehen, dass entsprechend des TLS-Kommunikationsstandard der Server immer die gesamte zu validierende Zertifikat-Kette an den Client versendet, gegen die zu prüfen ist.

Ein Zertifikat-Pinning in der Form, dass die Hash-Werte der Sub- und/oder Blatt-Zertifikate oder die Public-Keys mit der Anwendung verteilt werden, ist ein erhebliches Sicherheitsrisiko, da diese Werte viel leichter durch einen Angreifer ausgetauscht werden könnten, als eine Root-CA. Zudem entspricht diese Vorgehensweise einem Public-Private-Key-Verfahren, bei dem Revozierungen nicht durchgeführt werden. Umsetzungen nach RFC7469 und entsprechenden sind nicht zulässig.

3. Registrierstellen

3.1. Ziel

Dieses Kapitel definiert Anforderungen an die Infrastruktur und den Betrieb von Registrierstellen (registration authority – RA) innerhalb der AUDI BRUSSELS.

3.2. Einführung

Eine Registrierstelle der Volkswagen PKI im Sinne dieser Regelung ist jede Stelle, Person oder Organisationseinheit, welche Zertifikate ausgibt, die von einer Volkswagen Certification Authority stammen, d.h. als Stammzertifizierungsstelle (root CA) die Volkswagen PKI haben.

Registrierstellen sind innerhalb der Volkswagen PKI für die korrekte Registrierung von PKI Benutzern und die korrekte Verteilung von Schlüsselträgern (z. B. Smartcards) an die Benutzer verantwortlich. Aufgrund dessen haben Registrierstellen die Hauptverantwortung für die Vertrauenswürdigkeit von Zertifikaten.

Ein Mitarbeiter einer Registrierstelle wird als Registration Authority Officer bezeichnet.

3.3. Generelle Anforderungen

Zertifikate können für Personen, Geräte oder Services ausgestellt werden und dürfen nur für genehmigte Anwendungsfälle[20] durch autorisierte Registration Authorities, z.B. Officers der Volkswagen PKI, erstellt werden.

Gemäß ISO-C-Beschluss vom 13. Juli 2000, müssen bei der Nutzung von Zertifikaten innerhalb des Konzerns, Zertifikate einer der im Konzern zugelassenen Public Key Infrastrukturen eingesetzt werden. Dies können neben den internen PKI-Landschaften auch öffentliche akkreditierte Certificate Authorities sein, die durch die IT-Sicherheit bestätigt wurden.

Die verantwortliche Stelle[21] muss Prozesse, Anwendungsfälle und technische Anforderungen für die Erstellung von Zertifikaten definieren.

Der Aufbau von Registrierstellen muss in Abstimmung mit und unter Zustimmung der verantwortlichen Stelle[22] erfolgen.

Die Funktion des Registration Authority Officers kann durch einen Dienst übernommen werden. Die Art und Funktionsweise eines solchen Dienstes ist mit der zuständigen Stelle[23] abzustimmen.

Zertifikate, die der starken Authentifizierung der Anwender dienen, dürfen nur von internen Mitarbeitern der jeweiligen Konzerngesellschaft in der Rolle des Registration Authority Officers erstellt werden.

Zertifikate für Geräte dürfen nur erstellt werden, wenn diese den Vorgaben des IT-Sicherheitsregelwerks entsprechen.

---

[20] Siehe Anhang B.3.1

[21] Siehe Anhang B.3.1

[22] Siehe Anhang B.3.1

[23] Siehe Anhang B.3.1

Missbräuchlich oder falsch erstellte Zertifikate müssen entzogen werden.

3.3.1 Betriebliche Anforderungen

Die folgenden Anforderungen für den Betrieb von Registrierstellen müssen eingehalten werden:

- Das Personal muss ausgebildet sein (Ausbildungsnachweis, regelmäßige Auffrischungsseminare).
- Das Personal muss vertrauenswürdig sein.
- Jede Änderung des Personalumfanges (Zugänge, Abgänge) muss den verantwortlichen Personen der RA oder CA mitgeteilt werden. Die Berichte müssen aufbewahrt werden. (Für diese Mitarbeiter müssen in der PKI besondere Berechtigungen eingerichtet werden.)
- RAs müssen im Audi-Intranet betrieben werden. Eine Einwahl von außen (z. B. über das Internet oder Telefonverbindungen) ist für RAs nicht zulässig.
- RAs müssen von den jeweiligen Gesellschaften betrieben werden.
- Die Systeme und die Hardware der RA müssen gegen Viren und Angriffe aus dem Netz geschützt werden.
  - Arbeitsplatz-Rechner dürfen nicht verwendet werden (keine Office-Suite, kein Internet-Zugang, keine Entwicklungsumgebung, keine Spiele).
  - Virenscanner
  - Personal Firewall
  - Es sind nur Anwendungen zur Erstellung der Smart-Cards und Zertifikate (inkl. evtl. Ausweiserstellung) erlaubt.
  - Es sind nur Netzwerkverbindungen zu benötigten Netzkomponenten erlaubt.
- Die CA muss ein Installationsmedium für die RA-Rechner bereitstellen.
- Die Ausgabe von Schlüsselträgern muss protokolliert werden. Protokolle sind zu archivieren.
- Die Rechner der RAs dürfen nur von autorisiertem Personal im Rahmen der RA Funktionen genutzt werden. Autorisiertes Personal sind:
  - RA-Officer,
  - Personen, die mit der Produktion von Ausweiskarten betraut sind,
  - Administratoren für die Rechner der RAs.
- Die Rechner der RAs müssen vom RA-Betreiber gegen unautorisierten Zugriff, Verlust, Diebstahl oder Zerstörung durch geeignete physische Maßnahmen geschützt werden.

II. Verantwortlichkeiten

II.I Kapitel 1: Verschlüsselung

Diese Regelung ist von allen Planern, Entwicklern und Betreibern von IT-Systemen anzuwenden und 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: PKI

Diese Regelung ist vom Betreiber des Trust Centers einzuhalten.

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

II.III Kapitel 3: Registrierstellen

Diese Regelung ist von allen Registration Authority Officern 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. 03.01.09 Ausnahmeprozess

A.1.2 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

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 Quellen und Referenzen

A.3.1 NIST Special Publication 800-131A Revision 1 (November 2015) Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

A.3.2 FIPS 140-2: Security Requirements for Cryptographic Modules

Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules)

Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules

A.3.3 BSI - Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen; BSI TR-02102; Bundesamt für Sicherheit in der Informationstechnik; Version 2018.01

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[24].

A.5 Dokumentenhistorie

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

[24] Siehe Anhang A.2.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Verschlüsselung

B.1.1 IT-Sicherheit

B.1.2 IT-Sicherheit

B.1.3 Systeme auf der BCAL (Business critical application list) müssen einen Schlüssel-Notfallersatzprozess im BCH-IT (Business continuity handbook – IT) definieren

B.1.4 IT-Sicherheit

B.2 Kapitel 2: PKI

-

B.3 Kapitel 3: Registrierstellen

B.3.1 Konzern Information Systems Security Organisation (ISSO)

B.3.2 Konzern Information Systems Security Organisation (ISSO)

C. Bewertung kryptographischer Verfahren

Das folgende Kapitel bewertet kryptographische Verfahren und definiert zulässige kryptographische Algorithmen und Protokolle.

Ist der Einsatz ausgeschlossener oder nicht erwähnter Algorithmen notwendig, so ist eine individuelle Bewertung und Ausnahmegenehmigung erforderlich.

C.1 Algorithmen

Die Hinweise zur "empfohlenen Schlüssellänge" ergeben sich aus technisch angemessenen und umsetzbaren Schlüssellängen. Betrachtet wurde ein Zeitraum bis 2024. Längere Schlüssellängen sind immer empfehlenswert, wenn ein System über eine längere Zeit ohne Änderungen am Algorithmus betrieben werden soll oder die Vertraulichkeit der Daten auch in weiter Zukunft sichergestellt werden muss (z.B. zukünftiges brechen der Verschlüsselung von heute aufgezeichneten Daten).

Die Verwendung eigener kryptographischer Algorithmen ist nicht erlaubt.

C.1.1 Symmetrische Verschlüsselungsverfahren

Algorithmus	**Minimale Schlüssellänge (Bit)**	**Empfohlene Schlüssellänge (Bit)**	**Bemerkung**
Advanced Encryption Standard (AES)	128	256	
Triple-DES	-	-	Einsatz nicht zulässig!
RC2	-	-	Einsatz nicht zulässig!
RC4	-	-	Einsatz nicht mehr zulässig!
RC5	32/16/16	64/20/32	mittelfristig zu ersetzen!
RC6	32/20/16	64/24/32	
Serpent	128	128	
Blowfish	256	448	zeitnah ersetzen!
Twofish	128	256	
International Data Encryption Algorithm (IDEA)	-	-	Einsatz nicht zulässig!, auch nicht mehr in TLS 1.2.
Data Encryption Standard (DES)	-	-	Einsatz nicht zulässig!
CAST	128	128	
CAST-256	128	256	

Camellia	128	256	Royalty-free-License, patentiert, für nicht-kommerzielle Zwecke kostenlos

Symmetrische Verschlüsselungsverfahren, die als Blockalgorithmus operieren, dürfen nur in einem sicheren Betriebsmodus, der angemessenen für die jeweilige Anwendung ist, betrieben werden. Beispiele für Betriebsmodi sind GCM, CCM, CBC, CTR.

C.1.2 Hash-Verfahen

Algorithmus	**Minimale Hash-Länge (Bit)**
SHA / SHA 1	Einsatz nicht zulässig!
SHA 2	Zulässig: SHA-256, SHA-384, SHA-512, SHA-512/256 Nicht zulässig: SHA-224
SHA 3 aka. Keccak	SHA3-256, SHA3-384, SHA3-512
RIPEMD-160	Sollte abgelöst werden
MD5	MUSS abgelöst werden
Whirlpool	512

Ein Wechsel von SHA-1 (mit 160 bit) zu SHA-2 (Schlüssellängen 224, 256, 384 und 512 bit) oder zu Whirlpool (512 bit) ist erforderlich. Das Verwenden von SHA-1 ist nur zulässig, wenn SHA-2 nicht für den benötigten Anwendungsfall, oder das Protokoll, zur Verfügung steht.

C.1.3 Asymmetrische Verfahren

Sofern verfügbar sind die Verfahren als „Perfect Forward Secrecy“-Verfahren umzusetzen.

Algorithmus	**Minimale Schlüssellänge (Bit)**	**Empfohlene Schlüssellänge (Bit)**
RSA	2048	4096
DSS	2048	4096
DSA	1024 (2048 wenn technisch machbar)	4096, Verfahren sollte grundsätzlich nicht mehr eingesetzt werden.
EC-DSA[25]	224	250
DH Key-Exchange	2048 with 256 Prime Order Subgroup	4096 MODP Group with >256 Prime Order Subgroup

[25] Elliptic Curve DSA

Elliptic Curve DH Key-Exchange	224	384 (512+ wenn technisch umsetzbar)

C.1.4 Message Authentication Codes (MACs)

Symmetrische (Block) Verschlüsselungsverfahren werden oft in Form von Message Authentication Codes genutzt. Es wird die Verwendung der HMAC Methode (in Anlehnung an RFC 2104) empfohlen. Symmetrische Verschlüsselungsalgorithmen müssen nach den Vorgaben des Kapitel C.1.1 ausgesucht werden.

Algorithmus	**Minimale Schlüssellänge (Bit)**	**Empfohlene Schlüssellänge (Bit)**	**Bemerkung**
Poly1305	128+128+128	128+128+128	
HMAC	128	128	Taglänge >= 96
CMAC	128	128	Taglänge >= 96
GMAC	128	128	Taglänge >= 96
GCM, CBC, CTR. OFB. CFB			Empfohlen wird primär GCM. Nicht empfohlen ECB

C.1.5 (Pseudo-) Zufallszahlengeneratoren

In der Kryptographie werden Zufallszahlen meistens für die Generierung von Schlüsseln benötigt, sie sind aber auch Bestandteil von Protokollen.

Wenn möglich sollten sogenannte echte Zufallszahlengeneratoren verwendet werden. Diese Generatoren basieren auf physischen Mechanismen (z. B. Messung von Stromschwankungen an Dioden). Diese sind jedoch in Computern selten vorhanden. Aus diesem Grund werden üblicherweise pseudo Zufallszahlengeneratoren verwendet.

NIST gibt in FIPS 104-2 einen Überblick der erlaubten Generatoren die verwendet werden müssen.

C.1.6 Biometrische Verfahren

Biometrische Verfahren müssen von der IT-Sicherheit freigegeben werden.

C.1.7 Stromverschlüsselungsverfahren

Algorithmus	Minimale Schlüssellänge (Bit)	Empfohlene Schlüssellänge (Bit)	Bemerkung
A5/1	-	-	Einsatz nicht zulässig!
A5/2	-	-	Einsatz nicht zulässig!
ChaCha20 / Salsa20	256	256	20 rounds, 96 Bit Nonce, 256 Bit Schlüssellänge

C.1.8 Speichern von Passwörtern

Verfahren	Bemerkung
scrypt	[RFC7914]
PBKDF2	[RFC2898]
bcrypt	basiert auf blowfish (s. oben)

C.2 Protokolle

C.2.1 TLS

Die folgenden Standards dürfen verwendet werden:

TLS 1.2 Diffie-Hellman-Gruppen	IANA-Nr.	RFC	Verwendung bis
secp256r1	23	[RFC8422]	2025+
secp384r1	24	[RFC8422]	2025+
ffdhe3072	257	[RFC7919]	2025+
ffdhe4096	258	[RFC7919]	2025+

TLS 1.2 Signaturverfahren	IANA-Nr.	RFC	Verwendung bis
RSA	1	[RFC5246]	2025
DSA	2	[RFC5246]	2025+
ECDSA	3	[RFC5246]	2025+

TLS 1.2 Hashfunktionen	IANA-Nr.	RFC	Verwendung bis
SHA256	4	[RFC5246]	2025+
SHA384	5	[RFC5246]	2025+
SHA512	6	[RFC5246]	2025+

TLS 1.3 Handshake-Modi	IANA-Nr.	RFC	Verwendung bis
psk_ke	0	[RFC8446]	2025+
psk_dhe_ke	1	[RFC8446]	2025+

TLS 1.3 Diffie-Hellman-Gruppen	IANA-Nr.	RFC	Verwendung bis
secp256r1	23	[RFC8422]	2025+
secp384r1	24	[RFC8422]	2025+
ffdhe3072	257	[RFC7919]	2025+
ffdhe4096	258	[RFC7919]	2025+

TLS 1.3 Signaturverfahren für "signature_algorithms"-Erweiterung	IANA-Nr.	RFC	Verwendung bis
rsa_pss_rsae_sha256	0x0804	[RFC8446]	2025+
rsa_pss_rsae_sha384	0x0805	[RFC8446]	2025+
rsa_pss_rsae_sha512	0x0806	[RFC8446]	2025+
rsa_pss_pss_sha256	0x0809	[RFC8446]	2025+
rsa_pss_pss_sha384	0x080A	[RFC8446]	2025+
rsa_pss_pss_sha512	0x080B	[RFC8446]	2025+
ecdsa_secp256r1_sha256	0x0403	[RFC8446]	2025+
ecdsa_secp384r1_sha384	0x0503	[RFC8446]	2025+

TLS 1.3 Signaturverfahren für "signature_algorithms_cert"-Erweiterung	IANA-Nr.	RFC	Verwendung bis
rsa_pkcs1_sha256	0x0401	[RFC8446]	2025
rsa_pkcs1_sha384	0x0501	[RFC8446]	2025
rsa_pkcs1_sha512	0x0601	[RFC8446]	2025
rsa_pss_rsae_sha256	0x0804	[RFC8446]	2025+
rsa_pss_rsae_sha384	0x0805	[RFC8446]	2025+
ecdsa_secp256r1_sha256	0x0403	[RFC8446]	2025+
ecdsa_secp384r1_sha384	0x0503	[RFC8446]	2025+
rsa_pss_pss_sha256	0x0809	[RFC8446]	2025+
rsa_pss_pss_sha384	0x080A	[RFC8446]	2025+
rsa_pss_pss_sha512	0x080B	[RFC8446]	2025+
rsa_pss_rsae_sha512	0x0806	[RFC8446]	2025+

TLS-Ciphersuites (TLS 1.2 + TLS 1.3)	IANA-Nr.	RFC	Verwendung bis
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA9	[RFC7905]	2025+
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA8	[RFC7905]	2025+
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xc030	0xC0,0x30	[RFC5289]	2025+
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xc02f	0xC0,0x2F	[RFC5289]	2025+
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC0,0x2B	[RFC5289]	2025+
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC0,0x2C	[RFC5289]	2025+
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC0,0x31	[RFC5289]	2025+
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC0,0x32	[RFC5289]	2025+

TLS_AES_128_GCM_SHA256	0x13,0x01	[RFC8446]	2025+
TLS_AES_256_GCM_SHA384	0x13,0x02	[RFC8446]	2025+
TLS_AES_128_CCM_SHA256	0x13,0x04	[RFC8446]	2025+
TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	[RFC8446]	2025+

C.2.2 Absicherung von WLAN

- WEP: nicht erlaubt
- WPA: nicht erlaubt
- WPA2: erlaubt

Anstelle einer Authentifizierung mit statischen symmetrischen Schlüsseln (Pre-shared Keys) wird die Verwendung von Zertifikaten in Kombination mit EAP 802.1x empfohlen. Alternativ kann ein WLAN auch durch einen separat aufgebauten, kryptographisch sicheren und verschlüsselten VPN-Tunnel gesichert werden. In diesem Fall darf eine Kommunikation nur über den VPN Tunnel möglich sein.

In allen Fällen muss der statische symmetrische Schlüssel individuell zugewiesen werden.

C.2.3 SSH

SSH bietet unterschiedliche kryptographische Algorithmen:

- Es müssen in C.1 aufgeführte Algorithmen verwendet werden.

Die Sicherheit von SSH wird durch eine Zahl von kryptographischen Algorithmen für die Verschlüsselung und Authentifizierung garantiert. Es gibt zwei Versionen des SSH Protokolls: SSH-1 und SSH-2. Der Integritätscheck von SSH-1 ist verwundbar und kann für Man-in-the-Middle-Attacken ausgenutzt werden.

- Die Version SSH-2 des Protokolls muss verwendet werden.