Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

SICHERHEITSEMPFEHLUNGEN FÜR BEHÖRDEN

TEIL 1: KRYPTOGRAPHISCHE METHODEN

VERSION 1.2 – 15.02.2016.

Thomas Zefferer – thomas.zefferer@a-sit.at
Bernd Prünster – bernd.pruenster@a-sit.at

Zusammenfassung: Die Wahl geeigneter kryptographischer Algorithmen und Schlüssellängen spielt für sicherheitskritische Anwendungen eine zentrale Rolle. Dies gilt gleichermaßen für Anwendungen des privaten und des öffentlichen Sektors. Um letzteren bei der Wahl geeigneter kryptographischer Algorithmen und Schlüssellängen zu unterstützen, gibt dieses Dokument einen Überblick über gängige kryptographische Verfahren und empfohlene Schlüssellängen. Dazu werden in einem ersten Schritt in Österreich wirksame gesetzliche Vorgaben und Spezifikationen aufgelistet, um den relevanten Rahmen dieses Dokuments zu definieren und jene Algorithmen zu identifizieren, die für die österreichische Infrastruktur relevant sind bzw. durch Standardkomponenten zur Anwendung kommen. Anschließend werden vorhandene Vorgaben und Empfehlungen zur Verwendung von Algorithmen und Schlüssellängen gesammelt und analysiert. Basierend auf den Ergebnissen dieser Analyse und unter Berücksichtigung der für Österreich relevanten Aspekte werden schließlich entsprechende Empfehlungen abgeleitet. Dabei wird auf eine detaillierte Erklärung der einzelnen Verfahren bewusst verzichtet, sondern ausschließlich geeignete Algorithmen und zugehörige Parameter wie Schlüssellängen gelistet. Konkret ergeben sich damit folgende Empfehlungen zur Verwendung kryptographischer Algorithmen und entsprechender Schlüssellängen im behördlichen Umfeld:

Empfohlen werden als Mindest-Schlüssellängen bzw. Hash-Funktionen

- Symmetrische Verfahren: Standardverfahren mit mindestens 100 Bit effektive Schlüssellänge. Das heißt in der Praxis z.B. **3DES (min. 112 Bit)** bzw. **AES (min. 128 Bit)**
- Asymmetrische Verfahren: **RSA (min. 1536 Bit für bestehende und min. 2048 Bit für zukünftige Systeme)** bzw. **ECDSA (min. 192 Bit für bestehende und min. 224 Bit für zukünftige Systeme)**
- Hash-Funktionen: Verfahren der **SHA-2**-Familie

Insgesamt kann dieses Dokument damit einerseits als Grundlage für die Wahl geeigneter kryptographischer Methoden und Schlüssellängen verwendet werden. Andererseits kann dieses Dokument auch als Sammlung relevanter einschlägiger Referenzen zu weiterführender Literatur zu dieser Thematik betrachtet werden. In jedem Fall kann dieses Dokument von Behörden des öffentlichen Sektors als Entscheidungshilfe für die adäquate Verwendung kryptographischer Methoden zum Schutz nicht-klassifizierter Informationen verwendet werden. Der Schutz klassifizierter Informationen wird in diesem Dokument nicht näher betrachtet, da für klassifizierte Informationen in der Regel eigene Vorgaben gelten. Dieses Dokument umfasst eine aktualisierte Version der 2014 veröffentlichen Empfehlungen [1] unter Berücksichtigung aktueller Entwicklungen.

Revision History

Version	Datum	Autor	Anmerkungen
0.1	29.05.2014	Thomas Zefferer	Initialversion
0.2	18.06.2014	Herbert Leitold	Interner Review
1.0	18.06.2014	Thomas Zefferer	Finalversion
1.1	07.10.2014	Thomas Zefferer	Überarbeitung Finalversion
1.2	15.02.2016	Bernd Prünster	Aktualisierung 02.2016

Inhaltsverzeichnis

1. Einleitung

1.1. Motivation und Ziele

Kryptographie spielt für sicherheitskritische Anwendungen, die vertrauliche Daten verarbeiten oder speichern, eine zentrale Rolle. Die Verwendung geeigneter kryptographischer Methoden erlaubt die Wahrung der Vertraulichkeit, Integrität und Authentizität dieser Daten und stellt somit die Basis sicherheitskritischer Anwendungen dar. Damit spielt Kryptographie auch für Behörden, die für interne Prozesse oder für Interaktionen mit Bürgerinnen und Bürgern auf derartige Anwendungen zurückgreifen, eine wichtige Rolle.

Bei der Verwendung kryptographischer Verfahren und Methoden spielt die Wahl geeigneter kryptographischer Algorithmen und deren Parametrisierung eine zentrale Rolle. Ein wichtiger Parameter bei der Verwendung kryptographischer Algorithmen ist die Schlüssellänge. Hier gilt prinzipiell, dass mit steigender Schlüssellänge auch die Sicherheit des kryptographischen Verfahrens und dessen Resistenz gegen Brute-Force-Angriffe zunehmen. Zugleich steigt mit einer wachsenden Schlüssellänge jedoch auch die Komplexität der mathematischen Berechnungen, die im Zuge der Abarbeitung des zugrundeliegenden Algorithmus durchgeführt werden müssen. Bei der Wahl geeigneter Schlüssellängen muss daher stets ein geeigneter Kompromiss zwischen Sicherheit und Performance gefunden werden.

Eine weitere Herausforderung in Bezug auf die Wahl geeigneter Schlüssellängen ist der Umstand, dass die verfügbare Rechenleistung stetig ansteigt, was die Durchführung von Brute-Force-Angriffen erleichtert. Somit müssen empfohlene und verwendete Schlüssellängen im Laufe der Jahre stets nach oben korrigiert werden, um ein entsprechendes Sicherheitsniveau auch für zukünftige Anwendungen garantieren zu können. Weiters kann nicht ausgeschlossen werden, dass neue Attacken auf etablierte Algorithmen bekannt werden, wodurch vormals als empfehlenswert eingestufte Verfahren kompromittiert werden können. In den meisten Fällen zeichnen sich derartige Entwicklungen jedoch über einen längeren Zeitraum ab. Dementsprechend sollten Empfehlungen bezüglich kryptographischer Methoden auch in Anbetracht entsprechender Vorzeichen im Anlassfall korrigiert werden.

Ziel dieses Dokuments ist es, einen kurzen Überblick über aktuell empfohlene kryptographische Methoden und Verfahren zu geben und für diese geeignete Parametrisierungen zu bestimmen. In der Literatur finden sich zahlreiche Publikationen, die sich dieser Thematik widmen und entsprechende Empfehlungen formulieren. Dieses Dokument baut auf diesen Publikationen auf, vergleicht die darin definierten Empfehlungen und leitet daraus ein Gesamtbild ab, das einen allgemeinen Überblick über den aktuellen Stand empfohlener kryptographischer Algorithmen und Parametrisierungen verschiedener Kategorien erlaubt. Hauptaugenmerk wird dabei vor allem auf jene Verfahren gelegt, die für den öffentlichen Sektor in Österreich auf Grund geltender gesetzlicher Bestimmungen und aktueller Spezifikationen von Relevanz sind.

1.2. Methodik

Um die oben definierten Ziele dieser Studie zu erreichen, wurde folgende Methodik gewählt: In einem ersten Schritt wird in Abschnitt 2 der relevante Rahmen dieser Studie definiert, indem derzeit in Österreich geltende gesetzliche Vorgaben und Spezifikationen hinsichtlich der Verwendung kryptographischer Verfahren analysiert werden. Aus diesen Resultaten werden in Abschnitt 3 schließlich relevante Kategorien kryptographischer Verfahren identifiziert. Unter Berücksichtigung der identifizierten Kategorien werden in Abschnitt 4 vorhandene Publikationen, die sich der Ermittlung geeigneter kryptographischer Verfahren und Parametrisierungen widmen, gesammelt und analysiert. Dabei werden Resultate entsprechender Forschungsprojekte, einschlägige Publikationen von Organisationen und Institutionen sowie wissenschaftliche Arbeiten berücksichtigt. Aus den gesammelten Resultaten werden schließlich in Abschnitt 5 unter Berücksichtigung der österreichischen Infrastruktur entsprechende Empfehlungen abgeleitet.

2. Österreichische Infrastruktur

In diesem Abschnitt wird ein kurzer Überblick über relevante Komponenten österreichischer Infrastrukturen des öffentlichen Sektors gegeben. Hauptaugenmerk wird dabei auf jene Infrastrukturen gelegt, die im engen Zusammenhang mit E-Government- und Signaturlösungen stehen. Dadurch soll einerseits ein Überblick über aktuelle Infrastrukturkomponenten und die von diesen Komponenten verwendeten kryptographischen Algorithmen und Schlüssellängen gegeben und andererseits der relevante Rahmen dieses Dokuments definiert und eingegrenzt werden. Dazu werden im Folgenden gesetzliche Vorgaben, Standards und Spezifikationen, denen relevante Infrastrukturkomponenten zugrunde liegen, gelistet und überblicksmäßig beschrieben.

2.1. Gesetzliche Vorgaben

In Österreich regeln eine Reihe von Gesetzen und Verordnungen den Umgang mit sicherheitskritischen elektronischen Daten. In einigen Fällen werden über diese gesetzlichen Vorgaben auch Anforderungen bezüglich der Verwendung und Implementierung geeigneter kryptographischer Methoden zum Schutz dieser Daten definiert. In anderen Fällen wird hingegen lediglich ein entsprechendes Sicherheitsniveau gefordert, ohne jedoch konkrete technische Vorgaben zu machen. Im Folgenden werden einige der in Österreich geltenden relevanten gesetzlichen Bestimmungen überblicksmäßig beschrieben. Der Fokus wird dabei vor allem auf jene Bestimmungen gelegt, die für Behörden von Relevanz sind.

2.1.1. E-Government-Gesetz

Das österreichische E-Government-Gesetz [1] stellt die rechtliche Grundlage von E-Government in Österreich dar. Darin werden grundlegende Konzepte, auf denen E-Government-Lösungen in Österreich beruhen, definiert. So definiert das E-Government-Gesetz unter anderem die Funktion der Bürgerkarte, die Verwendung von Stammzahlen und bereichsspezifischer Personenkennzeichen (bPK) zur Identifikation von Bürgerinnen und Bürgern oder auch die Verwendung und die rechtliche Grundlage von Amtssignaturen.

Obwohl das österreichische E-Government-Gesetz grundlegende Konzepte der österreichischen E-Government-Infrastruktur beschreibt und diese Konzepte mitunter auf kryptographischen Verfahren beruhen, definiert das E-Government-Gesetz selbst keine Vorgaben bezüglich der für diese Verfahren einzusetzenden Algorithmen oder Schlüssellängen. Für die Berechnung von Stammzahlen und bereichsspezifischer Personenkennzeichen wird etwa lediglich auf die Stammzahlenregisterbehörde verwiesen. Diese ist laut E-Government-Gesetz angehalten, die für die Berechnung der Stammzahl verwendeten kryptographischen Algorithmen festzulegen und im Internet zu veröffentlichen. Selbiges gilt für kryptographische Methoden, die zur Berechnung von bereichsspezifischen Personenkennzeichen verwendet werden. Nähere Informationen zu den von der Stammzahlenregisterbehörde veröffentlichten Algorithmen werden in Abschnitt 2.1.2 erläutert. Für die Umsetzung der Amtssignatur definiert das E-Government-Gesetz lediglich, dass diese einer fortgeschrittenen Signatur im Sinne des Signaturgesetzes entspricht. Konkrete Anforderungen bezüglich der dafür zu verwendenden Algorithmen werden durch das E-Government-Gesetz jedoch nicht definiert.

2.1.2. Vorgaben der Stammzahlenregisterbehörde

Zu den Aufgaben der Stammzahlenregisterbehörde gehört unter anderem die Vergabe von Stammzahlen und von bereichsspezifischen Personenkennzeichen (bPK). Gemäß E-Government-Gesetz ist die Stammzahlenregisterbehörde zudem dafür verantwortlich, mathematische Verfahren zur Bildung von Stammzahlen und bPK festzulegen und zu publizieren. Dem kommt die Stammzahlenregisterbehörde auf ihrer Website [3] nach. Dort sind folgende kryptographische Verfahren veröffentlicht:

- Bildung von Stammzahlen: Triple-DES im CBC-Modus
- Bildung von OwPK: Triple-DES im CBC-Modus
- Bildung von bPK: SHA-1
- Bildung des wbPK: SHA-1

2.1.3. Signaturgesetz

Das österreichische Signaturgesetz [4] setzt die EU Signaturrichtlinie auf nationaler Ebene um und stellt damit die Grundlage für die Verwendung elektronischer Signaturen in Österreich dar. Die EU Signaturrichtlinie definiert ein Rahmenwerk für die Verwendung elektronischer Signaturen in Europa, legt jedoch keine zu verwendenden kryptographischen Algorithmen oder Schlüssellängen fest.

Auch das österreichische Signaturgesetz folgt im Wesentlichen diesem Ansatz. So werden in diesem Gesetz zwar einige technische Sicherheitserfordernisse definiert, es werden jedoch keine konkreten kryptographischen Methoden, Algorithmen oder gar Schlüssellängen vorgegeben. Für die nähere Spezifikation näherer Anforderungen an technische Komponenten verweist das Signaturgesetz in §25 lediglich auf eine vom Bundeskanzler zu erlassende Signaturverordnung.

Mit 01.07.2016 werden die Signaturrichtlinie und auch das österreichische Signaturgesetz durch die eIDAS-Verordnung [5] ersetzt.

2.1.4. Signaturverordnung

Die Signaturverordnung [6], deren Notwendigkeit im Signaturgesetz definiert ist, legt weitere Details zur Verwendung elektronischer Signaturen in Österreich fest. Im Gegensatz zum Signaturgesetz beschreibt die Signaturverordnung unter anderem sehr ausführlich geeignete Algorithmen und Parameter, die im Zuge der Erstellung und Verwendung qualifizierter elektronischer Signaturen zur Anwendung kommen dürfen. Konkret definiert die Signaturverordnung kryptographische Algorithmen und Parameter für die Erstellung von Signaturen, das Bilden von Hashwerten, das Padding von Daten und die Erzeugung von Zufallszahlen.

Aus Gründen der Übersichtlichkeit wird auf eine vollständige Wiedergabe aller in der Signaturverordnung definierten Algorithmen und Parameter in diesem Dokument verzichtet. Stattdessen werden im Folgenden für jede Kategorie von kryptographischen Verfahren nur einige der wichtigsten Vorgaben entsprechend der in der Signaturverordnung definierten Terminologie exemplarisch angeführt.

- Zulässige Signaturalgorithmen: rsa, dsa, ecdsa-Fp, ecdsa-F2m, ecgdsa-Fp, ecgdsa-F2m
- Zulässige Hashverfahren: sha1, ripemd160, sha224, sha256, sha384, sha512, whirlpool
- Zulässige Padding-Verfahren: emsa-pkcs1-v1_5, emsa_pss, emsa-pkcs1-v2_1, iso9796ds2, iso9796-din-rn, iso9796ds3

Selbst wenn diese Algorithmen in der Signaturverordnung genannt sind, ist gemäß §3(2) der Signaturverordnung auch der Stand der Technik zu berücksichtigen, d.h. ein allenfalls kompromittierter Algorithmus nicht zu verwenden. Unter diesem Gesichtspunkt ist auf Grund aktueller Entwicklungen im Bereich Kryptoanalyse [7] von der Verwendung von SHA-1 abzuraten, da das Finden von Kollisionen für diesen Algorithmus erwartet wird.

2.1.5. Informationssicherheitsgesetz

In Bezug auf die Sicherheit schützenswerter Daten spielt in Österreich auch das Informationssicherheitsgesetz [8] eine wichtige Rolle. Dieses regelt im Wesentlichen die Handhabung von und den Zugang zu klassifizierten Daten, für welche das Gesetz die Klassifizierungen EINGESCHRÄNKT, VERTRAULICH, GEHEIM und STRENG GEHEIM definiert. Vorgaben bezüglich kryptographischer Methoden und Verfahren zum Schutz klassifizierter Informationen werden im Informationssicherheitsgesetz jedoch nicht definiert.

Ähnlich dem Signaturgesetz verweist auch das Informationssicherheitsgesetz auf eine entsprechende Verordnung, in der weitere Details zu den im Gesetz relativ abstrakt gehaltenen Vorgaben definiert werden. Konkret verweist das Informationssicherheitsgesetz dazu auf die Informationssicherheitsverordnung. Auf diese wird in Abschnitt 2.1.6 näher eingegangen.

2.1.6. Informationssicherheitsverordnung / Geheimschutzordnung

Die Informationssicherheitsverordnung [9] definiert weitere Details der grundsätzlichen Vorgaben, die im Informationssicherheitsgesetz festgelegt sind. So spezifiziert die Informationssicherheitsverordnung unter anderem auch die elektronische Verarbeitung und Übermittlung klassifizierter Informationen. Allerdings spezifiziert auch die Informationssicherheitsverordnung dafür keine konkreten kryptographischen Algorithmen und Methoden. Es wird festgelegt, dass die Übermittlung von klassifizierten Informationen ab der Klassifizierungsstufe VERTRAULICH gemäß den Vorgaben der Informationssicherheitskommission zu schützen bzw. etwa unter Einsatz qualifizierter Signatur bzw. bei automatischer Übermittlung mit technisch gleichwertigen Sicherheitsanforderungen zu protokollieren ist.

Die Geheimschutzordnung des Bundes trifft Regelungen zum Umgang mit Informationen mit besonderem Schutzbedarf. Es werden Anforderungen zur Verwahrung oder Verarbeitung klassifizierter Informationen gegeben, wobei zu den IKT-Systemen und Algorithmen auf die Vorgaben der Informationssicherheitskommission verwiesen wird.

2.1.7. Sektorielle Vorgaben

Die bisher genannten gesetzlichen Vorgaben gelten in der Regel unabhängig vom jeweiligen Bereich und stellen somit allgemein gültige Richtlinien dar. Daneben existieren noch sektorielle Vorgaben, deren Gültigkeit auf einen bestimmten Anwendungsbereich begrenzt ist. Beispielhaft und stellvertretend für andere sektorielle Vorgaben wird hier die Gesundheitstelematikverordnung (GTeIV) [36] genannt.

Die Gesundheitstelematikverordnung (GTeIV) konkretisiert Datensicherheitsanforderungen und legt Rollen von Gesundheitsdiensteanbietern fest. Damit ergänzt die GTeIV Vorgaben des Gesundheitstelematikgesetzes (GTelG) [37], welches auch die elektronische Gesundheitsakte (ELGA) behandelt, und definiert unter anderem zulässige kryptographische Algorithmen. Dabei verweist die Gesundheitstelematikverordnung einerseits auf die Signaturverordnung und die darin festgelegten Verfahren. Andererseits definiert die GTeIV explizit folgende symmetrische Verfahren als geeignet:

- AES mit Schlüssellängen von 128, 192 oder 256 Bit im CBC- oder CTR-Modus
- 3DES mit einer effektiven Schlüssellänge von mindestens 112 Bit im CBC- oder CTR-Modus

2.2. Spezifikationen

Neben gesetzlichen Vorgaben definieren in Österreich auch diverse Spezifikationen die Verwendung von kryptographischen Methoden und Verfahren im öffentlichen Sektor und in der Kommunikation zwischen Behörden und Bürgerinnen und Bürgern. Im Folgenden werden einige der relevantesten Spezifikationen überblicksmäßig beschrieben und deren Vorgaben bezüglich der Verwendung kryptographischer Verfahren beleuchtet.

2.2.1. Bürgerkartenspezifikation

Die Spezifikationen zur Bürgerkarte sind unter [10] öffentlich verfügbar. Diese definieren nicht nur relevante Funktionen und Schnittstellen der Bürgerkarte bzw. der Bürgerkartenumgebung, sondern auch die Verwendung kryptographischer Verfahren. Konkret werden Vorgaben bezüglich der Verwendung von kryptographischen Verfahren für CMS-Signaturen, XML-Signaturen, CMS-Verschlüsselung, XML-Verschlüsselung und für die Berechnung von Hashwerten durch die Spezifikationen der Bürgerkarte definiert. Auf diese Vorgaben wird im Folgenden getrennt eingegangen.

- CMS-Signaturen: Bezüglich der Erstellung von CMS-Signaturen schreibt die Bürgerkartenspezifikation für die Berechnung des Message Digests bzw. für die Erstellung der elektronischen Signatur die Verwendung von gemäß Signaturverordnung zulässigen Algorithmen vor. Zusätzlich wird empfohlen, von einer Verwendung von SHA-1 Abstand zu nehmen. Diese Empfehlung wird an dieser Stelle bestätigt, da auf Grund aktueller

Entwicklungen im Bereich Kryptoanalyse [7] das Finden von Kollisionen für diesen Algorithmus erwartet wird.

- XML-Signaturen: Bezüglich der Erstellung von XML-Signaturen schreibt die Bürgerkartenspezifikation für die Berechnung des Message Digests bzw. für die Erstellung der elektronischen Signatur die Verwendung von gemäß Signaturverordnung zulässigen Algorithmen vor. Zusätzlich wird empfohlen, von einer Verwendung von SHA-1 Abstand zu nehmen. Diese Empfehlung wird an dieser Stelle bestätigt, da auf Grund aktueller Entwicklungen im Bereich Kryptoanalyse [7] das Finden von Kollisionen für diesen Algorithmus erwartet wird

- CMS-Verschlüsselung: In Bezug auf CMS-Verschlüsselungen definiert die Bürgerkartenspezifikation Algorithmen für den Schlüsseltransport und für die Datenverschlüsselung, die für diese Aufgaben verwendet werden können. Auf Grund der derzeitigen Verbreitung empfiehlt die Bürgerkartenspezifikation eine Verwendung von PKCS#1 v1.5 für den Schlüsseltransport und von Triple-DES im CBC-Modus für die Datenverschlüsselung. Folgende Algorithmen stehen laut Spezifikation prinzipiell zur Auswahl:

    - Schlüsseltransport:
        - PKCS#1 v1.5
        - RSAES-OEAP

    - Datenverschlüsselung:
        - Triple-DES (CBC-Modus)
        - AES-128 (CBC-Modus)
        - AES-256 (CBC-Modus)

- XML-Verschlüsselung: In Bezug auf XML-Verschlüsselungen definiert die Bürgerkartenspezifikation Algorithmen für den Schlüsseltransport, die Schlüsselvereinbarung, die Schlüsselverschlüsselung und für die Datenverschlüsselung (Blockverschlüsselung), die für diese Aufgaben verwendet werden können. Auf Grund der derzeitigen Verbreitung empfiehlt die Bürgerkartenspezifikation eine Verwendung von RSA Version 1.5 für den Schlüsseltransport und von AES-128 im CBC-Modus für die Datenverschlüsselung. Folgende Algorithmen stehen laut Spezifikation prinzipiell zur Auswahl:

    - Blockverschlüsselung:
        - Triple-DES (Blockverschlüsselung)
        - AES-128 im CBC-Modus (Blockverschlüsselung)
        - AES-256 im CBC-Modus (Blockverschlüsselung)

    - Schlüsseltransport:
        - RSA Version 1.5 (Schlüsseltransport)
        - RSA-OAEP (Schlüsseltransport)

    - Schlüsselverschlüsselung:
        - CMS Triple DES Key Wrap
        - AES KeyWrap 128 Bit
        - AES KeyWrap 256 Bit

    - Schlüsselvereinbarung:
        - Diffie-Hellman Key Agreement

- Hashwert-Berechnung: In Bezug auf die Berechnung von Hashwerten definiert die Bürgerkartenspezifikation, dass die Bürgerkartenumgebung alle Algorithmen unterstützen muss, die im Rahmen der XML-Signaturprüfung unterstützt werden.

2.2.2. Sicherheitsklassen gemäß PVP und verwandten Standards

Neben den Bürgerkarten-Spezifikationen gibt es noch eine Reihe weiterer Spezifikationen, die den Umgang mit Daten in sicherheitskritischen Bereichen des öffentlichen Sektors definieren und daher potentiell für diese Studie von Relevanz sein können. Eine dieser Spezifikationen, die hier beispielhaft genannt werden soll, ist die Spezifikation von Sicherheitsklassen im Rahmen des Portalverbundprotokolls (PVP) [11]. In diesem Dokument werden Sicherheitsklassen aus der Sicht von Benutzerinnen und Benutzern, Sicherheitsklassen für Anwendungen und Sicherheitsklassen für die Verbindung zwischen vertrauenswürdigen Geräten und Netzwerken definiert. In jeder Kategorie werden dabei vier verschiedene Sicherheitsklassen (0-3) definiert.

Trotz ihres direkten Bezugs zum Schutz von sicherheitskritischen und privaten Daten definiert diese Spezifikation jedoch keine konkreten zu verwendenden Algorithmen oder Schlüssellängen. Lediglich für die beiden höchsten Sicherheitsklassen wird im Rahmen der Datensicherheit eine starke Verschlüsselung vorgeschrieben und für diese bei symmetrischen Verfahren eine Mindestschlüssellänge von 100 Bit definiert.

2.3. Eigenschaften aktuell im Einsatz befindlicher Systeme und Zertifikate

Neben gesetzlichen Vorgaben und verbindlichen technischen Spezifikationen zeichnen auch aktuell im Einsatz befindliche Zertifikate, sowie gültige Bescheinigungen kryptographischer Komponenten ein Bild der aktuellen Infrastruktur in Österreich. Eine Auswertung der im Rahmen dieser Studie erhobenen Daten wird in den folgenden Abschnitten dargelegt.

2.3.1. Übersicht aktuell gültiger elektronischer Zertifikate

Über den Verzeichnisdienst von Zertifizierungsstellen können digitale Zertifikate, die beispielsweise für elektronische Signaturen zum Einsatz kommen, abgerufen werden. Durch eine statistische Auswertung von Zertifikatseigenschaften und einem Abgleich mit veröffentlichten Produktbeschreibungen der unterschiedlichen Zertifikatstypen lassen sich Aussagen über das Sicherheitsniveau von elektronischen Signaturen bzw. Datenverschlüsselung im öffentlichen, privaten und geschäftlichen Umfeld treffen. Relevant sind in diesem Zusammenhang die Root– und Intermediate-Zertifikate von Zertifizierungsstellen, welche qualifizierte Zertifikate ausstellen, wobei durchwegs RSA mit Schlüssellängen von 2048 bzw. 4096 Bit zum Einsatz kommt. Nicht sinnvoll hingegen ist beispielsweise eine Auswertung von SSL/TLS-Zertifikaten, da deren Parameter vom Kunden und nicht von der Zertifizierungsstelle festgelegt werden.

2.3.2. Bescheinigungen kryptographischer Komponenten

Abgesehen von digitalen Zertifikaten lassen auch gültige Bescheinigungen kryptographischer Komponenten wie Bankkarten oder Signaturkarten Schlüsse über die aktuelle Situation der Infrastruktur in Österreich zu. Im Folgenden sollen daher eine Reihe bescheinigter Komponenten und die von diesen Komponenten verwendeten kryptographischen Funktionen aufgelistet werden. Als Grundlage für die folgende Auflistung dienen veröffentlichte Bescheinigungen der Bestätigungsstelle A-SIT [12] (Stand: Februar 2016).

- Sichere Signaturerstellungseinheit der A-Trust für die Handy-Signatur bestehend aus HSM und HSM Server
    - Signaturerstellung:
        - ECDSA mit einer Schlüssellänge von 256 Bit
    - Hashwertberechnung:
        - SHA-256
- SSCD Protect & Sign Personal Signature, version 4.1
    - Signaturerstellung:
        - RSA mit einer Schlüsellänge von 2048 Bit
    - Hashwertberechnung:
        - SHA-256

- SSCD AliasLab CryptoAccelerator, release 3.4.3
    - Signaturerstellung:
        - RSA mit einer Schlüssellänge von 2048 oder 4096 Bit
    - Hashwertberechnung:
        - SHA256
- SSCD PkBox, Versionen 3.0.3, 3.0.5
    - Signaturerstellung:
        - RSA mit einer Schlüssellänge von 2048 oder 4096 Bit
    - Hashwertberechnung:
        - SHA-256
        - SHA-348
        - SHA-512
- Sichere Signaturerstellungseinheit CardOS V5.3 QES, V1.0
    - Signaturerstellung:
        - ECDSA mit einer Schlüssellänge von 256 oder 348 Bit
        - RSA mit einer Schlüssellänge von 2048 – 4096 Bit
    - Hashwertberechnung:
        - SHA-256
        - SHA-348
        - SHA-512

3. Identifikation relevanter Kategorien

Aus dem gegebenen Überblick wird ersichtlich, welche kryptographischen Verfahren und Methoden von Komponenten und Lösungen der österreichischen E-Government-Infrastruktur hauptsächlich verwendet werden. Basierend auf diesem Überblick kann daher eine Vorauswahl von relevanten kryptographischen Verfahren, Methoden und Algorithmen getroffen werden, auf die im Rahmen dieser Studie in weiterer Folge der Fokus gelegt werden soll.

Insgesamt können dabei die drei in den folgenden Unterabschnitten kurz beschriebenen Kategorien identifiziert werden. Für jede dieser Kategorien werden wo möglich und sinnvoll Einschränkungen in Bezug auf die betrachteten kryptographischen Algorithmen definiert.

3.1. Symmetrische Verfahren

Symmetrische Verfahren werden vorwiegend zur Verschlüsselung großer Mengen an Nutzdaten eingesetzt. Im Laufe der Zeit wurde eine Vielzahl symmetrischer Verfahren entwickelt.

In Österreich kommen überwiegend die beiden etablierten Verfahren Triple-DES (3DES) und AES mit zum Teil unterschiedlichen Schlüssellängen zur Anwendung. Die Betrachtung symmetrischer Verfahren in dieser Studie soll daher auf diese beiden Algorithmen beschränkt bleiben.

3.2. Asymmetrische Verfahren

Asymmetrische kryptographische Verfahren machen den Austausch gemeinsamer kryptographischer Schlüssel unnötig, sind in Implementierung und Ausführung jedoch komplexer als symmetrische Verfahren. Asymmetrische Verfahren sind daher für eine Anwendung auf große Daten eher ungeeignet, kommen aber vor allem bei der Umsetzung elektronischer Signaturlösungen oder für den sicheren Austausch symmetrischer Schlüssel zur Anwendung.

In Österreich kommen im Rahmen asymmetrischer kryptographischer Verfahren vor allem die beiden Verfahren RSA und ECDSA zur Anwendung. Im Rahmen dieser Studie wird der weitere Fokus daher auf diese beiden Verfahren gelegt.

3.3. Verfahren zur Hashwert-Berechnung

Hash-Verfahren bilden große Datenmengen auf einen Hash-Wert konstanter Länge ab. Die Verfahren sind so entworfen, dass von einem gegebenen Hashwert nicht mehr auf die Ausgangsdaten rückgeschlossen werden kann. Außerdem ist es praktisch nicht möglich, gezielt andere Daten zu finden, die auf denselben Hashwert abgebildet werden. Erreicht werden diese Eigenschaften durch die Verwendung geeigneter mathematischer Einweg-Funktionen.

Im Laufe der letzten Jahre wurde eine Vielzahl von Verfahren zur Berechnung von Hashwerten entwickelt. In Österreich kommen dazu vor allem Verfahren aus der SHA-Familie zur Anwendung. Weiters wird RIPEMD der österreichischen Signaturverordung als zulässiges Verfahren geführt. Die Betrachtung von Verfahren zur Hashwert-Berechnung soll in dieser Studie daher auf die Verfahren der SHA- bzw. RIPEMD-Familie beschränkt bleiben.

4. Analyse bestehender Vorgaben und Empfehlungen

Die Identifizierung und Definition geeigneter kryptographischer Algorithmen und Schlüssellängen für verschiedene Anwendungsszenarien ist eine wiederkehrende Problemstellung. Dementsprechend sind bereits zahlreiche Publikationen verfügbar, in denen diese Problematik von verschiedenen Gesichtspunkten aus betrachtet wird und die entsprechende Vorgaben und Empfehlungen formulieren. Im Folgenden soll ein kurzer Überblick über derartige Publikationen gegeben werden. Betrachtet werden dabei Resultate einschlägiger Projekte, welche die Identifizierung und die Definition geeigneter Algorithmen und Schlüssellängen zum Ziel hatten, veröffentlichte Dokumente verschiedener Organisationen und Institutionen zu diesem Thema sowie aktuelle wissenschaftliche Publikationen. Aus letzteren soll vor allem der aktuelle Stand der Forschung in Bezug auf die Analyse aktueller kryptographischer Algorithmen klar werden.

Als Startpunkt für die Analyse bestehender Vorgaben bietet sich die Website *BlueCrypt – Cryptographic Key Length Recommendation* [35] an. Diese stellt ein einfaches webbasiertes Tool zur Verfügung, über das Empfehlungen unterschiedlicher Quellen direkt miteinander verglichen werden können. Für das Jahr 2016 liefert dieses Tool beispielsweise die in Tabelle 1 aufgeführten Schlüssellängen, die für die einzelnen kryptographischen Operationen empfohlen werden.

Tabelle 1: Empfohlene Schlüssellängen für das Jahr 2016 gemäß BlueCrypt – Cryptographic Key Length Recommendation [35].

Method	Date	Symmetric	Factoring Modulus	Discrete Logarithm		Elliptic Curve	Hash
				Key	Group		
Lenstra / Verheul	2016	83	1664 1312	146	1664	155	165
Lenstra Updated	2016	79	1273 1392	158	1273	158	158
ECRYPT II	2016 - 2020	96	1776	192	1776	192	192
NIST	2011 - 2030	112	2048	224	2048	224	224
ANSSI	2014 - 2020	100	2048	200	2048	200	200
BSI	2016	128	2048	256	2048	256	256

Entsprechende Tabellen lassen sich über das von BlueCrypt zur Verfügung gestellte webbasierte Tool auch für zukünftige Zeitpunkte berechnen. Gemäß der Annahme, dass in Zukunft auf Grund der Verfügbarkeit größerer Rechenleistung in der Regel größere Schlüssellängen notwendig sein werden, ergeben sich dabei entsprechend größere empfohlene Schlüssellängen.

Um dies zu verdeutlichen, zeigt Tabelle 2 beispielhaft die von verschiedenen Quellen empfohlenen Schlüssellängen für das Jahr 2020.

Tabelle 2: Empfohlene Schlüssellängen für das Jahr 2020 gemäß BlueCrypt – Cryptographic Key Length Recommendation *[35].*

Method	Date	Symmetric	Factoring Modulus	Discrete Logarithm		Elliptic Curve	Hash
				Key	Group		
Lenstra / Verheul	2020	86	1881 1472	151	1881	161	171
Lenstra Updated	2020	82	1387 1568	163	1387	163	163
ECRYPT II	2016 - 2020	96	1776	192	1776	192	192
NIST	2011 - 2030	112	2048	224	2048	224	224
ANSSI	2014 - 2020	100	2048	200	2048	200	200
BSI	2017 - 2021	128	3072	256	3072	256	256

Wie aus Tabelle 1 und Tabelle 2 ersichtlich, vergleicht BlueCrypt Vorgaben sechs verschiedener Quellen. Diese und andere potentielle Quellen für Empfehlungen zur Verwendung kryptographischer Verfahren werden in den folgenden Abschnitten näher beschrieben.

4.1. Relevante Projekte

Die Identifizierung und Definition geeigneter kryptographischer Algorithmen und Schlüssellängen war unter anderem das Ziel verschiedener Forschungsprojekte. Eine Auswahl dieser Projekte und ein Überblick über die in diesen Projekten erzielten Resultate sollen im Folgenden gegeben werden. Fokus wird dabei auf die Projekte NESSIE, ECRYPT/ECRYPT II und CRYPTREC gelegt.

4.1.1. NESSIE

Das Projekt NESSIE [15], an dem in den Jahren 2000-2003 aktiv gearbeitet wurde, hatte zum Ziel, geeignete sichere kryptographische Primitive zu identifizieren. Auf Grund der relativ langen Zeit seit Abschluss dieses Projekts ist dieses für diese Studie nur mehr von beschränkter Bedeutung und hier primär aus Gründen der Vollständigkeit erwähnt.

4.1.2. ECRYPT/ECRYPT II

Das internationale Forschungsprojekt ECRYPT wurde 2004 als Nachfolgeprojekt von NESSIE gestartet und hatte zum Ziel, die Zusammenarbeit europäischer Forscherinnen und Forscher in den Bereichen IT-Sicherheit, Kryptographie und Digitale Wasserzeichen zu fördern. Nach Beendigung des Projekts wurde im Jahr 2008 das Nachfolgeprojekt ECRYPT II mit ähnlichen Zielen gestartet.

Die für diese Studie relevantesten Resultate von ECRYPT II sind jährliche Berichte zu Algorithmen und Schlüssellängen. Derartige Berichte wurden jährlich zwischen 2009 und 2012 veröffentlicht und können nach wie vor von der Projekt-Website [13] bezogen werden.

4.1.3. CRYPTREC

CRYPTREC steht für Cryptography Research and Evaluation Committees und wurde von der japanischen Regierung als Äquivalent zu den europäischen Projekten NESSIE und ECRYPT/ECRYPT II ins Leben gerufen. Ziel von CRYPTREC ist die Evaluierung kryptographischer Methoden und die Erstellung von Empfehlungen zur Verwendung bestimmter geeigneter Verfahren in Industrie und im öffentlichen Sektor. Empfehlungen zu kryptographischen Methoden, Algorithmen und Schlüssellängen können der CRYPTREC Website [14] entnommen werden.

4.2. Dokumente von Organisationen und Institutionen

In den letzten Jahren wurden zahlreiche Dokumente von verschiedenen Organisationen und Institutionen publiziert, in denen Empfehlungen zur Verwendung kryptographischer Methoden definiert sind. Im Folgenden werden einige dieser Publikationen etwas näher beleuchtet.

4.2.1. BRZ Sicherheitsarchitektur

Dieses von der Bundesrechenzentrum GmbH erstellte Dokument [16] enthält Vorgaben bezüglich anzuwendender Methoden, Standards und Technologien bei der Umsetzung von technischen Sicherheitsmaßnahmen. Dabei wird im Speziellen auf verschiedene Sicherheitsfunktionen eingegangen.

Entsprechende kryptographische Algorithmen werden beispielsweise für die Sicherheitsfunktion Sichere Datenhaltung gelistet und bewertet. Für jedes identifizierte Verfahren werden in diesem Dokument bekannte Stärken und Schwächen analysiert und entsprechende Rückschlüsse auf empfohlene Schlüssellängen gezogen.

4.2.2. ENISA: Algorithms, Key Size and Parameters Report

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) veröffentlichte im Oktober 2013 sowie im November 2014 den Algorithms, Key Size and Parameters Report [17]. Ziel dieses Reports ist es unter anderem, ein Nachfolgedokument für die zwischen 2009 und 2012 jährlich erscheinenden Reports des Projekts ECRYPT II zu liefern. Dementsprechend ähneln sich auch die

Inhalte der jährlichen ECRYPT II-Berichte und der von der ENISA veröffentlichten Dokumente; beide definieren Empfehlungen zur Verwendung kryptographischer Primitive und entsprechender Schlüssellängen. Konkret spezifiziert ENISA Empfehlungen zur Verwendung von Blockchiffren, Hash-Funktionen, Stromchiffren, und Public-Key-Verfahren.

4.2.3. NIST Cryptographic Toolkit

Das National Institute of Standards and Technologies (NIST) stellt ein sogenanntes Cryptographic Toolkit [18] zusammen, das zum Ziel hat, US-Behörden bei der Verwendung entsprechender kryptographischer Methoden und Verfahren zum Schutz kritischer Daten zu unterstützen. Dementsprechend enthält dieses Toolkit Empfehlungen zur Verwendung kryptographischer Algorithmen und geeigneter Schlüssellängen.

4.2.4. ANSSI Empfehlungen

Empfehlungen zur Verwendung von kryptographischen Verfahren und Methoden wurden auch von der französischen Organisation Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) definiert. Diese Empfehlungen sind unter [19] verfügbar.

4.2.5. Fact Sheet NSA Suite B Cryptography

NSA Suite B Cryptography bezeichnet eine Liste kryptographischer Algorithmen und zugehöriger Schlüssellängen, die von der National Security Agency (NSA) erstellt wurde. Je nach Geheimhaltungsstufe (SECRET, TOP SECRET) werden dabei mitunter unterschiedliche Parameter (Schlüssellängen) definiert. Suite B Cryptography zugeordnete Algorithmen und zugehörige Parameter sind auf der Website der NSA [20] veröffentlicht.

4.2.6. RFC 3766

Die Stärke von verwendeten kryptographischen Schlüsseln wird auch in RFC 3766 behandelt. Dieses Dokument fokussiert sich vor allem auf die Verwendung von Public-Key-Kryptographie für den Austausch symmetrischer Schlüssel und auf verschiedene Aspekte, die bei der Wahl entsprechender Schlüssellängen betrachtet werden müssen. RFC 3766 ist unter [21] öffentlich verfügbar.

4.3. Wissenschaftliche Publikationen

In diesem Abschnitt soll schließlich noch ein kurzer Überblick über aktuelle Forschungstätigkeiten im Bereich der Kryptoanalyse und der Analyse geeigneter Schlüssellängen gegeben werden. Dadurch soll ein rudimentärer Überblick über den aktuellen Stand der Forschung und über die Sicherheit aktueller kryptographischer Verfahren aus akademischer Sicht erarbeitet werden. Fokus wird dabei ausschließlich auf die mathematische Analyse der unterschiedlichen Algorithmen gelegt. Implementierungsattacken, die weniger den Algorithmus selbst also vielmehr dessen Umsetzung angreifen, werden hier nicht näher betrachtet, da für diese die Wahl von Schlüssellängen und anderen Parametern nur bedingt von Relevanz ist.

4.3.1. Symmetrische Verfahren

Kryptoanalyse symmetrischer Verfahren wie AES oder DES hat in den letzten Jahren nur wenige Fortschritte gemacht. Teilerfolge konnten in den letzten Jahren zumeist nur erzielt werden, wenn Angriffen entsprechende Modelle zu Grunde gelegt wurden, die die Durchführung von Angriffen vereinfachen. Ein Beispiel für ein derartiges Modell sind beispielsweise Related-Key Attacken, denen die Annahme zu Grunde liegt, dass ein Angreifer Cipher-Operationen mit verschiedenen Schlüsseln beobachten kann und diese Schlüssel eine bestimme Beziehung zueinander haben. Eine Kryptoanalyse basierend auf dieser Annahme wurde beispielsweise im Jahr 2009 von Biryukov et al. [23] vorgestellt. Einige der besten Resultate ohne die Notwendigkeit entsprechender Annahmen über verwendete Schlüssel wurden bisher von Bogdanov et al. [24] publiziert. Jedoch liegt auch diesem Angriff eine derart hohe Komplexität zu Grunde, dass die sichere praktische Verwendung von AES in keiner Weise gefährdet ist. Insgesamt kann also festgehalten werden, dass praktikable Angriffe auf derzeit in Verwendung befindliche symmetrische Verfahren auch aus akademischer Sicht bei entsprechenden Schlüssellängen nicht möglich sind.

4.3.2. Asymmetrische Verfahren

Wissenschaftliche Publikationen zu Angriffen auf asymmetrische Verfahren fokussierten in letzter Zeit vor allem auf die Generierung von Schlüsselpaaren und potentiell schlechte Randomness, die in der Praxis dafür verwendet wird [25].

Insgesamt kann jedoch festgehalten werden, dass in Bezug auf die grundlegenden mathematischen Probleme, auf denen die Sicherheit der meisten asymmetrischen Verfahren beruht, sich in letzter Zeit keine signifikanten Änderungen ergeben haben. Eine Ausnahme stellen hier vielleicht Verfahren, die auf DPL bzw. ECDPL beruhen, dar. Fortschritte in Bezug auf Angriffe auf diese [26] bedingen jedoch ein spezielles Setting (supersinguläre Kurven für ECDLP), das in der Praxis nur sehr beschränkt zum Einsatz kommt.

4.3.3. Hash-Verfahren

Die Kryptoanalyse von Hash-Verfahren ist nach wie vor ein zentrales Thema wissenschaftlicher Publikationen. Veröffentlichte Arbeiten zur Analyse von Hash-Verfahren fokussierten sich in den letzten Jahren unter anderem auf die SHA-Familie [7][27][28][29][30] und auf RIPEMD-160 [31]. Im Wesentlichen untermauern aktuelle Forschungsresultate zu Angriffen auf bekannte Hash-Verfahren die aktuell vorherrschende Einschätzung, dass von einer Verwendung von SHA-1 in Zukunft abzuraten ist, während andere gängige Hash-Verfahren kurz- und mittelfristig noch ein ausreichendes Maß an Sicherheit bieten dürften. Im Speziellen sind aktuelle Fortschritte bezüglich der Kollisionsresistenz von SHA-1 [7] hervorzuheben. Die hieraus gewonnen Erkenntnisse legen die Vermutung nahe, dass praxisrelevante Angriffe auf SHA-1 früher als geplant umgesetzt werden könnten. Eine qualifizierte zeitliche Abschätzung kann diesbezüglich allerdings nicht getroffen werden. Derartige Entwicklungen bekräftigen jedoch die Empfehlung von SHA-1 Abstand zu nehmen.

4.3.4. Analyse von Schlüssellängen

Aus wissenschaftlicher Sicht sind in Bezug auf empfohlene Parameter für kryptographische Algorithmen vor allem die Arbeiten von Lenstra und Verheul [32] [33] [34] von Bedeutung. In diesen analysieren die Autoren verschiedene kryptographische Methoden und leiten empfohlene Parameter für die verschiedenen Verfahren her.

5. Empfehlungen

Unter Berücksichtigung der in Abschnitt 4 überblicksmäßig beschriebenen Quellen werden in diesem Abschnitt nun Empfehlungen für die in Abschnitt 3 identifizierten für Österreich relevanten Verfahren und Algorithmen hergeleitet. Dadurch soll einerseits überprüft werden, ob die in Österreich über gesetzliche Vorgaben bzw. relevante Spezifikationen definierten kryptographischen Algorithmen nach wie vor für einen sicheren Einsatz geeignet sind und andererseits geeignete Parameter für die Verwendung dieser Algorithmen identifiziert werden.

5.1. Symmetrische Verfahren

Entsprechend den Empfehlungen der verschiedenen angeführten Quellen und unter Berücksichtigung der speziellen Situation in Österreich kann für symmetrische Verfahren derzeit bei Verwendung eines entsprechenden Algorithmus eine effektive Mindestschlüssellänge von 100 Bit empfohlen werden. Damit ergeben sich bei Verwendung von in Österreich üblichen Algorithmen wie 3DES oder AES tatsächliche empfohlene Schlüssellängen von 112 (3DES) bzw. 128 (AES) Bit.

5.2. Asymmetrische Verfahren

Entsprechend den analysierten Vorgaben verschiedener Quellen und unter Berücksichtigung der österreichischen Infrastruktur kann für asymmetrische Verfahren eine Schlüssellänge von 1500 Bit für bestehende und eine Schlüssellänge von 2000 Bit für zukünftige Systeme und Verwendungen empfohlen werden. Für RSA kann damit eine Schlüssellänge von 1536 bzw. 2048 Bit als geeignet angesehen werden. Entsprechend kann für kryptographische Verfahren basierend auf elliptischen Kurven eine Schlüssellänge von 192 Bit für bestehende, bzw. 224 Bit für zukünftige Anwendungen empfohlen werden.

5.3. Hash-Funktionen

Kryptographische Hash-Funktionen verwenden keine kryptographischen Schlüssel. Eine Empfehlung von Mindestschlüssellängen ist in dieser Kategorie daher nicht notwendig. Allerdings steigt die Komplexität von Attacken auf ein Hash-Verfahren mit der Länge des Hashwerts, der durch dieses Verfahren berechnet wird. Somit kann diese Länge als relevanter Parameter für die Sicherheit von Hash-Verfahren herangezogen werden.

Je nach Quelle wird dabei aktuell eine Länge von 155 bis 224 Bit empfohlen. Damit sind etwa SHA-1 und RIPEMD-160 mit einer Hashwertlänge von jeweils 160 Bit bereits am unteren Ende des empfohlenen Spektrums und – wie zum Beispiel im ENISA Algorithms, Key Size and Parameters Report [17] angeführt – für zukünftige Verwendungen nicht mehr zu empfehlen. Stattdessen kann die Verwendung anderer Hash-Algorithmen wie Vertreter der SHA2-Familie empfohlen werden.

An dieser Stelle ist auch das vom NIST im August 2015 standardisierte Verfahren SHA3 [38] zu erwähnen. Dieses Verfahrens wird unter anderem im ENISA Algorithms, Key Size and Parameters Report [17] für zukünftige Verwendung empfohlen. Es wird erwartet, dass SHA3 in den kommenden Jahren an Relevanz gewinnt, allerdings werden Hash-Funktionen der SHA2-Familie weiterhin von allen in diesem Dokument erwähnten Organisationen auch für zukünftige Anwendungen als ausreichend sicher klassifiziert, daher kann deren Einsatz uneingeschränkt empfohlen werden.

6. Fazit

Kryptographische Methoden und Verfahren stellen für sicherheitskritische Anwendungen ein zentrales Element zur Gewährleistung der Sicherheit von Daten dar. Die Wahl geeigneter Methoden und Algorithmen sowie die adäquate Parametrisierung dieser Algorithmen sind dabei von zentraler Bedeutung.

In diesem Dokument wurde ein Überblick über aktuell empfohlene kryptographische Algorithmen und Parametrisierungen gegeben. Dabei wurde das Hauptaugenmerk vor allem auf jene Verfahren gelegt, die im Rahmen der österreichischen Infrastruktur von Bedeutung sind. Dazu wurden derzeit in Österreich geltende gesetzliche Vorgaben und Spezifikationen näher beleuchtet und relevante Verfahren aus diesen Vorgaben identifiziert.

Darauf aufbauend wurden bestehende Vorgaben und Empfehlungen zur Auswahl und Parametrisierung kryptographischer Methoden analysiert. Diese Analyse zeigte, dass bereits ein breites Spektrum an entsprechenden Empfehlungen verfügbar ist. Im Rahmen dieser Studie wurden daher primär bestehende Empfehlungen gesammelt und kombiniert. Unter Berücksichtigung der zuvor für die österreichische Infrastruktur als relevant identifizierten Verfahren wurden schließlich aus bestehenden Empfehlungen Vorschläge für die Verwendung und Parametrisierung verschiedener Kategorien kryptographischer Methoden abgeleitet.

Dieses Dokument kann damit einerseits als Grundlage für die Wahl geeigneter kryptographischer Methoden und deren Parametrisierung verwendet werden. Andererseits kann dieses Dokument auch als Sammlung relevanter einschlägiger Referenzen zu weiterführender Literatur zu dieser Thematik betrachtet werden. In jedem Fall kann dieses Dokument damit als Entscheidungshilfe für die adäquate Verwendung kryptographischer Methoden verwendet werden.

7. Referenzen

[1] A-SIT: Sicherheitsempfehlungen für Behörden, Version 1.1. 10.11.2014 http://demo.a-sit.at/sicherheitsempfehlungen-fuer-behoerden/ (aufgerufen am 05.01.2016)

[2] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG). https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20003230/E-GovG%2c%20Fassung%20vom%2005.01.2016.pdf (aufgerufen am 05.01.2016)

[3] Österreichische Datenschutzbehörde – Stammzahlenregisterbehörde. http://www.stammzahlenregister.gv.at/ (aufgerufen am 05.01.2016)

[4] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/10003685/SigG%2c%20Fassung%20vom%2005.01.2016.pdf (aufgerufen am 05.01.2016)

[5] Electronic identification and trust services (eIDAS): regulatory environment and beyond. https://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond (aufgerufen am 15.02.2016

[6] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008). https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20005618/SigV%202008%2c%20Fassung%20vom%2005.01.2016.pdf (aufgerufen am 05.01.2016)

[7] Marc Stevens, Pierre Karpman, Thomas Peyrin: The SHAppening: freestart collisions for SHA-1 https://sites.google.com/site/itstheshappening/ (aufgerufen am 05.01.2016)

[8] Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz, InfoSiG). https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20001740/InfoSiG%2c%20Fassung%20vom%2005.01.2016.pdf (aufgerufen am 05.01.2016)

[9] Verordnung der Bundesregierung über die Informationssicherheit (Informationssicherheitsverordnung, InfoSiV). https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20003054/InfoSiV%2c%20Fassung%20vom%2005.01.2016.pdf (aufgerufen am 05.01.2016)

[10] Spezifikationen der Bürgerkarte. http://www.buergerkarte.at/hintergrund-informationen.html#jump8 (aufgerufen am 05.01.2016)

[11] Spezifikation Sicherheitsklassen für den Zugriff von Benutzern auf Anwendungen. http://reference.e-government.gv.at/uploads/media/SecClass_2-1-0_2007-12-14.pdf (aufgerufen am 05.01.2016)

[12] A-SIT: Bestätigungsstelle. http://www.a-sit.at/de/bestaetigungsstelle/index.php (aufgerufen am 05.01.2016)

[13] European Network of Excellence in Cryptology II. http://www.ecrypt.eu.org/ (aufgerufen am 05.01.2016)

[14] CRYPTREC. http://www.cryptrec.go.jp/english/ (aufgerufen am 05.01.2016)

[15] NESSIE - New European Schemes for Signatures, Integrity, and Encryption. https://www.cosic.esat.kuleuven.be/nessie/ (aufgerufen am 05.01.2016)

[16] BRZ: BRZ Sicherheitsarchitektur - Sicherheitsfunktionen - technische Vorgaben, Anwendung und Verbindlichkeit.

[17] ENISA: Algorithms, Key Sizes and Parameters Report – 2014 – November 2014. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014 (aufgerufen am 05.01.2016)

[18] NIST: Cryptographic Toolkit. http://csrc.nist.gov/groups/ST/toolkit/index.html (aufgerufen am 05.01.2016)

[19] Agence nationale de la sécurité des systèmes d'information: Référentiel Général de Sécurité. http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf (aufgerufen am 05.01.2016)

[20] NSA: Suite B Cryptography. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml (aufgerufen am 05.01.2016)

[21] RFC 3766: Determining Strengths For Public Keys Used For Exchanging Symmetric Keys. http://www.ietf.org/rfc/rfc3766.txt (aufgerufen am 05.01.2016)

[22] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nache dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Alogrithmen), 13.01.2014. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2014Algorithmenkatalog.pdf?__blob=publicationFile&v=1

[23] Alex Biryukov, Dmitry Khovratovich: Related-Key Cryptanalysis of the Full AES-192 and AES-256. ASIACRYPT 2009: 1-18

[24] Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger: Biclique Cryptanalysis of the Full AES. ASIACRYPT 2011: 344-371

[25] Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, Nicko van Someren: Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild. ASIACRYPT (2) 2013: 341-360

[26] Robert Granger, Thorsten Kleinjung, Jens Zumbrägel: Breaking `128-bit Secure' Supersingular Binary Curves (or how to solve discrete logarithms in $\F_{2^{4 \cdot 1223}}$ and $\F_{2^{12 \cdot 367}}$). CoRR abs/1402.3668 (2014)

[27] Marc Stevens: New Collision Attacks on SHA-1 Based on Optimal Joint Local-Collision Analysis. EUROCRYPT 2013: 245-261

[28] Florian Mendel, Tomislav Nad, Martin Schläffer: Improving Local Collisions: New Attacks on Reduced SHA-256. EUROCRYPT 2013: 262-278

[29] Maria Eichlseder, Florian Mendel, Martin Schläffer: Branching Heuristics in Differential Collision Search with Applications to SHA-512, FSE 2014.

[30] Itai Dinur, Orr Dunkelman, Adi Shamir: Self-Differential Cryptanalysis of Up to 5 Rounds of SHA-3. FSE 2013

[31] Florian Mendel, Thomas Peyrin, Martin Schläffer, Lei Wang, Shuang Wu: Improved Cryptanalysis of Reduced RIPEMD-160. ASIACRYPT 2013: 484-503

[32] Arjen K. Lenstra and Eric R. Verheul: Selecting Cryptographic Key Sizes. Journal of Cryptology, vol. 14, pp. 255-293, 1999.

[33] Arjen K. Lenstra: Key Lengths. The Handbook of Information Security, 2004.

[34] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter: Public Keys. CRYPTO 2012: 626-642

[35] BlueCrypt: Cryptographic Key Length Recommendation. http://www.keylength.com/en/compare/ (aufgerufen am 05.01.2016)

[36] Verordnung des Bundesministers für Gesundheit, mit der nähere Regelungen für die Gesundheitstelematik getroffen werden – Gesundheitstelematikverordnung 2013 (GTelV 2013). https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008732 (aufgerufen am 05.01.2016)

[37] Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verwendung elektronischer Gesundheitsdaten (Gesundheitstelematikgesetz 2012 – GTelG 2012). https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120 (aufgerufen am 05.01.2016)

[38] National Institute of Standards and Technologies: SHA-3 Standardization http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html (aufgerufen am 05.01.2016)