Kanton Bern
Canton de Berne

Weisung

über den

Grundschutz für die Informations- und Cybersicherheit (ICSGW)

Beschlussdatum	26.08.2024
Version	3.1
Status	abgenommen
Klassifizierung	Nicht klassifiziert
Autoren	Sascha Tarli / Daniel Lörtscher
Dateiname	Weisung über den Grundschutz für die Informations- und Cyber.docx
Dokumentenummer	432393
Geschäftsnummer	2024.KAIO.76

Herausgeber: Amt für Informatik und Organisation des Kantons Bern (KAIO)

Das Amt für Informatik und Organisation (KAIO),

gestützt auf Artikel 12 Absatz 1 Buchstabe c der Direktionsverordnung vom 3. Januar 2011 über Informationssicherheit und Datenschutz (ISDS DV)[1] i.V.m. Artikel 11d Absatz 3 der Verordnung über die Organisation und die Aufgaben der Finanzdirektion (Organisationsverordnung FIN; OrV FIN)[2]

beschliesst:

Art. 1 Gegenstand und Zweck

[1] Diese Weisung legt die Anforderungen an den Grundschutz nach Artikel 5 Absatz 4 ISDS DV für die ICT-Mittel, Informationen und Personendaten der kantonalen Behörden zwecks Gewährleistung der Informations- und Datensicherheit fest.

[2] Wenn erhöhte ISDS-Anforderungen bestehen, sind neben dem Grundschutz zusätzlich die im ISDS-Konzept beschriebenen Schutzmassnahmen umzusetzen.

Art. 2 Geltungsbereich und Verwendung

[1] Diese Weisung gilt für die kantonalen Behörden nach Artikel 4 Absatz 2 des Gesetzes vom 7. März 2022 über die digitale Verwaltung (DVG)[3].

[2] Diese Weisung gilt auch für andere kantonale Träger öffentlicher Aufgaben, sofern sie ICT-Mittel der kantonalen Behörden nach Artikel 32 Absatz 1 DVG einsetzen.

[3] Beschaffen die Behörden ICT-Mittel bei beauftragen Dritten (nachfolgend Leistungserbringerinnen), sind diese grundsätzlich vertraglich und unter Verwendung der im konkreten Fall relevanten Bestimmungen der Anhänge 2 bis 6, insbesondere der AGB ISDS BE, zur Gewährleistung des Grundschutzes zu verpflichten.

[4] Sofern Absatz 3 infolge der Marktstellung des Anbieters nur teilweise umsetzbar ist oder dieser den Grundschutz durch andere als in den Anhängen 2 bis 6 verlangten Massnahmen gewährleisten will, sind die entsprechenden Risiken in der ISDS-Analyse sowie im ISDS-Konzept auszuweisen. Dabei ist auf den Grundschutznachweis des Anbieters zum Zeitpunkt seiner Offerte zu basieren (Art. 5 Abs. 4), worin die Gewährleistung des Grundschutzes trotz seinen Abweichungen von der ICSGW zu belegen ist. Die Risiken sind durch geeignete Massnahmen auf ein tragbares Mass zu senken. Die Restrisiken sind gemäss ISDS-Konzept nach Artikel 5 Absatz 5 ISDS DV von den Führungspersonen der verantwortlichen Behörde nachweisbar zu akzeptieren.

Art. 3 Anhänge

[1] Diese Weisung verfügt über die folgenden Anhänge, welche die Anforderungen an den Grundschutz des Kantons Bern beschreiben:

Anhang 1: Schutzobjekte, Klassifizierung und Schutzniveaus;
Anhang 2: Anforderungen an den Grundschutz von ICT-Mitteln, Informationen und Personendaten (Grundschutz);
Anhang 3: Grundschutz Auftragsdatenbearbeitung;

[1] ISDS DV; BSG 152.040.2
[2] OrV FIN; BSG 152.221.171
[3] DVG; BSG 109.1

Anhang 4: Allgemeine Geschäftsbedingungen des Kantons Bern über die Informationssicherheit und den Datenschutz (AGB ISDS BE);
Anhang 5: Umgang mit Authentisierungsmerkmalen;
Anhang 6: Kryptographische Verfahren.

Art. 4 Begriffe

a) **ICT-Mittel:** Güter und Dienstleistungen der Informations- und Telekommunikationstechnik (ICT), einschliesslich Hardware und Software (Art. 4 Abs. 3 Bst. a DVG).

b) **Informationen:** Angaben in beliebiger Form über Sachverhalte, jedoch ohne Personendaten.

c) **Personendaten:** Angaben in beliebiger Form über eine bestimmte oder bestimmbare natürliche oder juristische Person (Art. 2 Abs. 1 KDSG).

d) **Informations- und Datensicherheit:** Zustand, womit die Vertraulichkeit, Verfügbarkeit und Integrität von ICT-Mittel, Informationen und Personendaten sowie die Nachvollziehbarkeit ihrer Bearbeitung gewährleistet sind.

e) **Authentisierungsmittel:** Ein materielles oder digitales Objekt, das von einer natürlichen Person kontrolliert und für den Nachweis ihrer Identität (Authentisierung) eingesetzt wird; z.B. ein kryptographischer Schlüssel, ein Geheimnis oder ein biometrisches Merkmal.

f) **Sicherheitsvorfall:** Ein Ereignis, welches die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der ICT-Mittel, Informationen oder Personendaten gefährdet.

g) **Schwachstelle:** Eine Schwäche oder ein Fehler eines ICT-Mittels, welche das Potential hat, einen Sicherheitsvorfall zu ermöglichen.

Art. 5 Feststellung und Erfüllung der Grundschutzanforderungen

[1] Die Behörden stellen die einzelnen Grundschutzanforderungen an ein ICT-Mittel anhand einer ISDS-Analyse nach Artikel 5 Absatz 2 ISDS DV fest.

[2] Ergibt die ISDS-Analyse, dass ein ICT-Mittel über den Grundschutz hinausgehende Anforderungen erfüllen muss, so werden diese erhöhten ISDS-Anforderungen in einem ISDS-Konzept beschrieben.

[3] Nicht oder teilweise erfüllte Grundschutzanforderungen müssen ebenfalls im ISDS-Konzept als Risiken ausgewiesen und deren Vermeidung, Verminderung oder Akzeptanz beschrieben werden.

[4] Die Behörden sowie ihre Leistungserbringerinnen müssen die Erfüllung der Grundschutzanforderungen nachweisen können.

[5] Die Behörden verwenden für die ISDS-Analyse und das ISDS-Konzept die vom KAIO beschlossenen und publizierten Vorlagen.

Art. 6 Schutzniveau

[1] Die ICT-Mittel, Informationen und Personendaten sind Werte, deren Schutz genug stark sein muss, um ihrer Bedeutung und Bedrohung zu genügen (Schutzniveau).

[2] Die ICT-Mittel, Personendaten und Informationen sind aufgrund ihrer Bedeutung und Bedrohung durch die Behörden zu klassifizieren. Je nach Klassifizierung ist das Schutzniveau 0 bis 3 erforderlich. Der Grundschutz gewährleistet das Schutzniveau 0 und 1 (s. Anhang 1).

[3] Das Erfüllen eines bestimmten Schutzniveaus setzt die entsprechenden technischen, organisatorischen, physischen und personellen Schutzmassnahmen voraus.

Art. 7 Klassifizierung von Informationen

[1] Die Klassifizierung von Informationen schützt die folgenden öffentlichen und privaten Interessen:

a) Die Entscheidungs- und Handlungsfähigkeit der Behörden,
b) Die öffentliche Ordnung und Sicherheit.

[2] Die Behörden klassifizieren Informationen, deren Kenntnisnahme durch Unberechtigte die öffentlichen Interessen gemäss Absatz 1 beeinträchtigen kann. Sie erfolgt in den folgenden Stufen:

a) «INTERN», wenn die öffentlichen Interessen aufgrund der Kenntnisnahme durch Unberechtigte beeinträchtigt werden können,
b) «VERTRAULICH», wenn die öffentlichen Interessen aufgrund der Kenntnisnahme durch Unberechtigte erheblich beeinträchtigt werden können,
c) «GEHEIM», wenn die öffentlichen Interessen aufgrund der Kenntnisnahme durch Unberechtigte schwerwiegend beeinträchtigt werden können.

[3] Die Klassifizierung ist auf das erforderliche Mindestmass zu beschränken und möglichst zeitlich zu begrenzen.

[4] Die pro Klassifizierung erforderlichen Schutzniveaus werden in Anhang 1 definiert.

Art. 8 Übergangsbestimmung für bestehende ICT-Mittel und Verträge

[1] Die Behörden passen bestehende ICT-Mittel und Verträge bei der nächsten Neubeschaffung oder Änderung, spätestens aber vier Jahre nach dem Inkrafttreten dieser Weisung an die Grundschutzanforderungen an.

Art. 9 Aufhebung von Weisungen

[1] Die Ausführungsweisung des KAIO über die Direktionsverordnung über Informationssicherheit und Datenschutz (AW-ISDS) vom 18. März 2024 wird per 31. Dezember 2024 aufgehoben.

[2] Die Weisungen des KAIO

a) über den Umgang mit Authentisierungsmerkmalen vom 25. August 2021 (IWS 1.3.004) sowie
b) zu kryptographischen Verfahren vom 28. Juni 2022

werden per 31. Dezember 2024 aufgehoben.

Art. 10 Inkrafttreten

[1] Diese Weisung tritt per 1. Januar 2025 in Kraft.

Bern

Amt für Informatik und Organisation

Beat Jakob
27.10.2026 14:42
Geregeltes elektronisches Siegel · www.be.ch/signatur
Cachet électronique réglementé · www.be.ch/signature

Beat Jakob, Amtsleiter

Dokument-Protokoll

Freigabekontrolle

Version	Name	Datum	Bemerkungen
0.5	GS FIN	20.03.2024	Genehmigung Entwurf z.H. Konsultation
0.44	GL KAIO	26.08.2024	Beschlossen, vorbehältlich Prüfung DSA
0.44	Ueli Buri	04.09.2024	Prüfung DSA
1.0	Beat Jakob	05.09.2024	Unterzeichnung
2.0	GL KAIO	16.12.2024	Beschluss mit Anhang 5 und 6
3.0	Thomas Fischer	09.07.2025	Redaktionelle Anpassung Anhang 4 an AGB DVS
3.1	Beat Jakob	19.10.2026	Redaktionelle Anpassung Anhang 4 an KDSG

Kanton Bern
Canton de Berne

Anhang 1 zur ICSGW:

Schutzobjekte, Klassifizierung und Schutzniveaus

Beschlussdatum	16.12.2024
Version	2.0
Dokument Status	abgenommen
Klassifizierung	Nicht klassifiziert
Autor	Sascha Tarli
Dateiname	ICSGW Anhang 1 Schutzniveaus
Dokumentnummer	432425
Geschäftsnummer	2024.KAIO.76

Herausgeber: Amt für Informatik und Organisation des Kantons Bern (KAIO)

Die Behörden haben die Informations- und Datensicherheit durch die erforderlichen organisatorischen, technischen, personellen und physischen Sicherheitsmassnahmen sicherzustellen. Jedes Schutzobjekt, also ein ICT-Mittel, eine Information oder Personendaten, ist auf dessen Schutzbedarf zu überprüfen. Dieser ist sodann mit dem entsprechenden Schutzniveau, einem Bündel aus verschiedenen Schutzmassnahmen, zu decken.

Die Schutzniveaus sind sowohl für die Informations- als auch für die Datensicherheit die gleichen. Sie umfassen die Stufen 0 bis 3 (so auch nach der Inkraftsetzung des Gesetzes über die Informations- und Cybersicherheit [ICSG][1] sowie der Verordnung über die Informations- und Datensicherheit [IDSV][2]).

Informations- und Cybersicherheitsgesetz ICSG (Entwurf)		**Informations- und Datensicherheitsverordnung IDSV (Entwurf)**	**Datenschutzgesetz KDSG**
Schutz der Interessen des Staates		**Massnahmen für die Informations- und Datensicherheit**	**Schutz der Interessen natürlicher Personen**
ICT-Mittel	Informationen	Schutzmassnahmen nach Stand der Technik	Personendaten
Sehr hoher Schutz	GEHEIM	Schutzniveau 3	Personendaten als schwere Gefahr für die Sicherheit Einzelner (Leib, Leben, Freiheit)
Hoher Schutz	VERTRAULICH	Schutzniveau 2	Besonders schützenswerte Personendaten und Personendaten mit besonderer Geheimhaltung (Berufs-, Steuergeheimnis etc.)
Grundschutz	INTERN	Schutzniveau 1	Allgemeine Personendaten
	Nicht klassifiziert	Schutzniveau 0	Nicht personenbezogene Daten (ausserhalb des Schutzbereichs des KDSG)
Personensicherheitsprüfung (PSP) nach ICSG durch anstellende Behörde		Vollzugsvorschriften für ICSG und KDSG	Prüfung der Vertrauenswürdigkeit nach Personalgesetz durch anstellende Behörde

Die Schutzziele des ICSG und des KDSG sind zu unterscheiden:

a) Das ICSG schützt den Staat vor ungesetzlichem Stören seiner Entscheidungsfreiheit und seines Handelns.
b) Das KDSG schützt die Menschen vor ungesetzlichen Eingriffen in ihre Persönlichkeit.

Die beiden Schutzziele werden mit der Ermittlung des Schutzbedarfs pro Schutzobjekt, der entsprechenden Kennzeichnung bzw. Klassifizierung nach Art. 7 ICSGW sowie der Umsetzung der Schutzniveaus[3] erreicht.

[1] ICSG, Referendumsfassung, Ablauf Referendumsfrist 2. Oktober 2025
[2] Entwurf zur IDSV, zurzeit zu Illustrationszwecken zusammen mit dem ICSG in der Beratung des Grossen Rates (Stand Dezember 2024)
[3] Spezialfall: Informationen und Personendaten haben das Schutzniveau 0, wenn sie von einer Behörde veröffentlicht wurden oder dazu bestimmt sind. Beispiel: Angaben zur Parteizugehörigkeit eines Grossratsmitglieds in einem Vorstoss oder im Protokoll des Grossen Rates.

Dokument-Protokoll

Freigabekontrolle

Version	Name	Datum	Bemerkungen
0.5	GS FIN	20.03.2024	Genehmigung Entwurf z.H. Konsultation
0.17	GL KAIO	26.08.2024	Beschluss, vorbehältlich Prüfung DSA
0.17	Ueli Buri	04.05.2024	Prüfung DSA
1.0	Beat Jakob	05.09.2024	Unterzeichnung KAIO
2.0	GL KAIO	16.12.2024	Beschluss mit Anhang 5 und 6

Kanton Bern
Canton de Berne

Anhang 2 zur ICSGW:

Anforderungen an den Grundschutz von ICT-Mitteln, Informationen und Personendaten (Grundschutz)

Beschlussdatum	16.12.2024
Version	2.0
Dokument Status	abgenommen
Klassifizierung	Nicht klassifiziert
Autor	KAIO
Dateiname	ICSGW Anhang 2 Anforderungen an den Grundschutz von ICT-Mittel, Informationen und Personendaten.docx
Dokumentnummer	432426
Geschäftsnummer	2024.KAIO.76

Herausgeber: Amt für Informatik und Organisation des Kantons Bern (KAIO)

1. Generelle Anforderungen an den Grundschutz

Die Behörden haben diese Anforderungen umzusetzen oder beim Bezug von ICT-Leistungen bei beauftragten Dritten (nachfolgend Leistungserbringerinnen) vertraglich für deren Umsetzung zu sorgen (Art. 2 Abs. 1 und 2 ICSGW).

ID	Anforderung	Beschreibung
1	Organisatorische Sicherheit	
1.1	Organisation	
1.1.1	Informationssicherheitsleitlinien	Die Geschäftsleitungen der Behörde sowie deren Leistungserbringerinnen müssen Informationssicherheitsleitlinien (analog ISO 27001) beschlossen und die Verantwortlichkeiten für die Informations- und Datensicherheit definiert haben. Mitarbeitende beider Parteien sowie allfällige Subunternehmen der Leistungserbringerinnen müssen darüber in Kenntnis gesetzt sein. Die Leitlinien sind jährlich zu überprüfen.
1.1.2	Trennen von unvereinbaren Aufgaben (Segregation of Duties)	Die Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) müssen so strukturiert sein, dass infolge Interessenskonflikten unvereinbare Aufgaben, z.B. Betriebsaufgaben sowie deren Kontrolle, auf verschiedene Personen verteilt sind. Für unvereinbare Aufgaben muss die Trennung festgelegt und dokumentiert sein.
1.1.3	Management von Sicherheitsvorfällen	Es sind wirksame Verfahren und eindeutige AKV festgelegt und dokumentiert, um eine schnelle, wirksame Reaktion auf Sicherheitsvorfälle sicherzustellen. Die Behörden und die Leistungserbringerinnen bezeichnen eine Kontaktstelle für Sicherheitsvorfälle und definieren deren Erreichbarkeit.
1.1.4	Meldepflicht bei Sicherheitsvorfällen oder Schwachstellen	Ein Sicherheitsvorfall gemäss Art. 4 Bst. f ICSGW ist insbesondere in den folgenden Fällen meldepflichtig, (analog Art. 74d ISG[1] i.V.m. Art. 18 CSV[2]): 1. infolgedessen Mitarbeitende oder Dritte von Unterbrüchen der ICT-Mittel betroffen sind, 2. die betroffene Behörde oder die Leistungserbringerin ihre Tätigkeit nur noch im Notbetrieb aufrechterhalten können, 3. geschäftsrelevante Informationen durch Unbefugte verändert oder offengelegt werden, 4. er zu einer Manipulation oder zu einem Abfluss von Informationen geführt hat, 5. er mehr als 90 Tage unentdeckt blieb, insbesondere wenn Anzeichen bestehen, dass er zur Vorbereitung eines Cyberangriffs ausgeführt wurde,

[1] Informationssicherheitsgesetz des Bundes (ISG, SR 128)
[2] Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV, SR 128.51)

		6. er mit Erpressung, Drohung oder Nötigung verbunden ist, sich also gegen die Behörde oder die Leistungserbringerin inkl. deren Mitarbeitenden richten. Sicherheitsvorfälle und Schwachstellen müssen spätestens innert 24 Stunden seit Entdeckung über die kantonale Meldeplattform gemeldet werden.
1.1.5	Umzug der Datenhaltung und/oder Datenprozessierung	Ein Umzug der Datenhaltung und/oder Datenprozessierung darf nur in ein Land mit einem angemessenen Datenschutz gemäss Anhang 1 zur Verordnung des Bundes vom 31. August 2022 über den Datenschutz (Datenschutzverordnung, DSV)[3] erfolgen. Andernfalls muss der Umzug von der Leistungserbringerin mindestens 60 Tage vor der vertraglichen Kündigungsfrist der Behörde gemeldet werden.
1.2	**Informationsmanagement**	
1.2.1	Klassifizierung von Informationen	Die Informationen und Personendaten sind durch die Behörden nach Art. 7 ICSGW zu klassifizieren und gemäss dem erforderlichen Schutzniveau nach Anhang 1 zur ICSGW mit organisatorischen, technischen, personellen und physischen Massnahmen, namentlich gemäss diesem Anhang, zu schützen.
1.2.2	Sichere Entsorgung von Datenträgern	Vor der Entsorgung von Datenträgern muss nachweisbar sichergestellt sein, dass alle Informationen und Personendaten nicht wieder herstellbar gelöscht wurden. Die Entsorgung hat dem Schutzbedarf der Informationen entsprechend (mindestens Schutzklasse 2 nach DIN 66399) oder einem gleichwertigen Standard zu erfolgen.
1.2.3	Sicherer Wechsel der Speichermedien	Beim Wechsel der Speichermedien zu Wartungszwecken, auf Verlangen der auftraggebenden Behörde oder bei Beendigung des Vertragsverhältnisses hat sichere Löschung gemäss Ziff. 1.2.3 oben der Inhalts- und Randdaten der auftraggebenden Behörde zu erfolgen, einschliesslich allfälliger Backups. Diese Datenlöschung ist mit einem Report nachzuweisen.
1.2.4	Archivierung und Löschung	Die Archivierung und Löschung von Informationen und Personendaten erfolgt gemäss den vertraglich vereinbarten Regeln. Fehlen solche, so hat sich die Leistungserbringerin vor der Löschung von Daten über das Archivierungs- und Löschkonzept und allfällige gesetzliche Auflagen bei der auftraggebenden Behörde zu informieren.

[3] DSV Anhang 1; SR 235.11

		Nicht mehr erforderliche oder zweckentfremdete Daten sind nachweislich und nicht wiederherstellbar zu löschen.
1.3	**Verträge**	
1.3.1	Informations- und Datensicherheit in Verträgen mit Leistungserbringerinnen	Den Leistungserbringerinnen sind die Anforderungen an die Informations- und Datensicherheit vertraglich zu überbinden, und sie sind zu verpflichten, die Anforderungen auch ihren Subunternehmen zu übertragen.
1.4	**ICT-Service-Continuity-Management**	
1.4.1	Sicherstellen der Geschäftskontinuität	Die Behörden sowie deren Leistungserbringerinnen haben sicherzustellen, dass für die von ihnen verantworteten ICT-Mittel ein ICT-Service-Continuity-Management-Konzept besteht. Dieses stellt sicher, dass die ICT-Mittel auch bei ausserordentlichen Lagen so lange wie nötig in Betrieb bleiben. Bei Unterbrüchen stellt das Konzept sicher, dass die Wiederinbetriebnahme so rasch wie nötig erfolgt.
2	**Personensicherheit**	
2.1	**Sicherheit des Personals**	
2.1.1	Eignung und Vertrauenswürdigkeit der Mitarbeitenden und Leistungserbringerinnen	Die Behörden und deren Leistungserbringerinnen setzen nur geeignete und vertrauenswürdige Fachpersonen ein. Die Behörden und Leistungserbringerinnen überprüfen die Personen bei der Anstellung bzw. Beauftragung gemäss einem schriftlich festgelegten Rekrutierungsprozess anhand der Lebensläufe und Qualifikationsnachweise der in Frage kommenden Personen. Sie überprüfen die Vertrauenswürdigkeit des eingesetzten Personals vor der Anstellung bzw. Beauftragung und später in regelmässigen Abständen. Der Umfang und die Periodizität der Prüfung richtet sich nach dem Risiko, der mit dem Personaleinsatz verbunden ist.
2.1.2	Vertraulichkeitserklärungen	Bevor Mitarbeitende von Leistungserbringerinnen (inkl. deren Subunternehmen) Zugang zu ICT-Mittel, Informationen oder Personendaten mit Schutzniveau 2 gemäss Anhang 1 zu Art. 6 ICSGW erhalten, sind sie von der Behörde mit einer Vertraulichkeitserklärung oder -vereinbarung pro Person zur Geheimhaltung zu verpflichten und über die Folgen bei deren Verletzung zu instruieren. Mitarbeitende von Behörden sind von ihren Vorgesetzen in nachvollziehbarer Form auf das von Gesetzes wegen geltende Amtsgeheimnis aufmerksam zu machen (Art.

		58 Personalgesetz des Kantons Bern[4], Art. 320 Strafgesetzbuch[5]).
2.2	**Schulung**	
2.2.1	Befähigung des Personals zur Informationssicherheit und zum Datenschutz	Die Behörden und die Leistungserbringerinnen haben sicherzustellen, dass die Mitarbeitenden und Leistungserbringerinnen regelmässig, aufgaben- und stufengerecht für die Gewährleistung der Informationssicherheit und des Datenschutzes geschult werden.
3	**Physische Sicherheit**	
3.1	Schutz von ICT-Mitteln, Informationen und Personendaten	ICT-Mittel, Informationen und Personendaten, welche durch die Leistungserbringerin für die Behörde eingesetzt werden, sind nach dem Stand der Technik (ISO 27'002:2022, Ref. 7.1 bis 7.9, s. Kapitel 3 dieses Anhangs) zu schützen. Ist dies nicht möglich, ist die Sicherheit mit anderen Massnahmen zu gewährleisten und der verantwortlichen Behörde anzuzeigen.
4	**Technische Sicherheit**	
4.1	**Zugriffskontrolle**	
4.1.1	Beschränkung des Zugriffs und sichere Anmeldeverfahren	Zugriffe auf ICT-Mittel setzen die dem Schutzniveau entsprechende Anmeldeverfahren (Authentifizierung) voraus (s. Kapitel 2, Sicherheitsstufen für Authentisierungsmittel). Zugriffe dürfen nur aufgrund eines rollenbasierten Berechtigungskonzepts erfolgen. ICT-Mittel sind technisch so zu bauen, dass sie die definierten Passwortvorschriften gemäss Anhang 5, Umgang mit Authentisierungsmerkmalen, erzwingen. Für Authentifizierungen von Maschine zu Maschine sind zertifikatsbasierende Authentifizierungsverfahren anzuwenden.
4.1.2	Überprüfung der Zugriffsrechte	Zugriffsrechte auf ICT-Mittel, insbesondere die privilegierten Rechte der Leistungserbringerinnen, sind mittels eines dokumentierten Prozesses zu verwalten und aktuell zu halten. Nutzende und mit Administratorenrechten ausgestattete Personen dürfen nur über die Rechte verfügen, die für ihre Aufgaben nötig sind (Least-Privilege-Prinzip). Die Zugriffsrechte sind jährlich auf deren Zweckmässigkeit, Notwendigkeit und Eignung zu überprüfen. Nicht mehr benötigte Rechte sind aufzuheben.

[4] PG, BSG 153.01
[5] StGB, SR 311.0

		Die Leistungserbringerinnen legen schriftlich fest und auf Verlangen der Behörde hin offen, welche Personen mit Administratorenrechte auf die ICT-Mittel Zugriff haben (Berechtigungskonzept).
4.1.3	Umgang mit Authentisierungsmerkmalen	Es gilt Anhang 5, Umgang mit Authentisierungsmerkmalen,.
4.1.4	Benutzer-Authentifizierung Applikationen Zone «Internet»	Wenn eine Authentifizierung über das Internet erfolgt (z.B. bei Software as a Service), ist eine mehrstufige Benutzerauthentisierung (Minimum zwei Faktoren) einzusetzen.
4.1.5	Fernzugriffe von Leistungserbringerinnen	Ein Fernzugriff von Leistungserbringerinnen auf ICT-Mittel ist unter folgenden Voraussetzungen zulässig: a) Der Zugriff erfolgt über ein persönliches Benutzerkonto; b) Die Authentifikation erfolgt über ein Authentisierungsmittel mindestens Schutzniveau 1 gemäss nachfolgendes Kapitel 2 zu diesem Anhang, Sicherheitsstufen für Authentisierungsmittel; c) Das Benutzerkonto einer Leistungserbringerin Beauftragten ist zeitlich begrenzt und bzw. oder dessen Nutzung wird aufgezeichnet und die Protokollierung periodisch überprüft; d) Der Zugriff erfolgt über einen sog. Jump-Host (vorgelagerter Server zur Authentisierung); e) Die Netzwerkverbindung für den Zugriff ist nach dem aktuellen Stand der Technik verschlüsselt. Abweichungen sind der Behörde anzuzeigen.
4.1.6	Administratoren-Konto	Administratorenkonten, a) müssen mit minimal notwendigen Rechten konfiguriert sein; b) dürfen nur für Administratoren-Tätigkeiten verwendet werden (zweckgebunden); für andere Tätigkeiten ist ein Standardkonto zu verwenden; c) sind jährlich auf deren Zweckmässigkeit, Notwendigkeit und Geeignetheit zu überprüfen; d) müssen einer einzigen, identifizierten sowie überprüften natürlichen Person zugeordnet werden können; e) müssen aufgezeichnet, überwacht und ausgewertet werden; f) haben ein verschlüsselt gespeichertes Passwort, welches vertraulich zu behandeln ist.
4.1.7	Service-Benutzerkonto	Unpersönliche Service-Benutzerkonten für automatisierte Prozesse

		a) müssen mit minimal notwendigen Rechten konfiguriert sein, b) dürfen nur für die Tätigkeiten des definierten Service verwendet werden, c) sind jährlich auf ihre Zweckmässigkeit, Notwendigkeit und Geeignetheit zu überprüfen, d) sind mit den folgenden Angaben nachvollziehbar zu dokumentieren: • Zweck des Service-Kontos; • für das Konto verantwortliche Person; • deren Stellvertretung; • die Zugriffsberechtigten. e) Es gelten die gleichen Passwortanforderungen, wie für die Administratoren-Konten. Wenn eine jährliche Passwortänderung technisch nicht möglich ist, muss die Passwortlänge auf mindestens 32 Stellen erhöht werden.
4.1.8	Test-Benutzerkonten	a) Müssen als solche identifizierbar und mit dem Namen der verantwortlichen Person gekennzeichnet sein; b) Dürfen zu keiner Zeit Zugriff auf produktive Daten der Kantonsverwaltung ermöglichen; c) Dürfen keine privilegierten Rechte umfassen.
4.2	**Kryptografie**	
4.2.1	Verwendung von kryptographischen Verfahren	Die Anforderungen gemäss Anhang 6, Kryptographische Verfahren, sind zu erfüllen. Der Grad der Vertraulichkeit und Integrität muss dem Schutzbedarf der ICT-Mittel, Informationen oder Personendaten entsprechen. Sie müssen unter Berücksichtigung des Einsatzortes mit adäquaten kryptografischen Verfahren gesichert sein.
4.3	**Sicherheit im Betrieb**	
4.3.1	Dokumentation	Für ICT-Mittel muss den Behörden eine aktuelle Dokumentation in der geforderten Sprache und einfach lesbarer Form vorgelegt werden. Werden die ICT-Mittel von Leistungserbringerinnen geliefert oder betrieben, so ist die Dokumentation – auch der Leistungen von Subunternehmen – vertraglich sicherzustellen. Die Dokumentation muss die gesamte Lebensdauer der ICT-Mittel abdecken und folgende Inhalte ausweisen: a) Die Netzwerk- und Systemarchitektur; b) Die sicherheitsrelevanten Komponenten, Funktionen und Einstellungen; c) Die Schlüsselverwaltung beim Einsatz kryptografischer Verfahren; d) Die Prozesse bei Changes, Wartung, Reparaturen, Entsorgung und Verlust;

		e) Die Leistungen und deren Sicherheitsrelevanz von Subunternehmen; f) Den Zugriff der Behörden auf die Dokumentation muss auch beim Ausfall der ICT-Mittel gewährleistet sein.
4.3.2	Change Management	Ein geplanter Change muss durch die auftraggebende Behörde auf dessen Auswirkungen auf die Informations- und Datensicherheit beurteilt, in einem Genehmigungsverfahren freigegeben und seine Umsetzung nachvollziehbar aufgezeichnet werden. Ungeplant umgesetzte Changes sind umgehend zu überprüfen und zu dokumentieren.
4.3.3	Kapazitätsmanagement	Die benötigen Kapazitäten der ICT-Mittel müssen prognostiziert, überwacht, mit den auftraggebenden Behörden abgestimmt sowie rechtzeitig bereitgestellt werden.
4.3.4	Trennung von Entwicklungs-, Test-, Integrationsumgebung von der Produktivumgebungen	Die produktive Umgebung der ICT-Mittel muss von unproduktiven Umgebungen getrennt sein. Die entsprechenden Massnahmen zur Trennung sind nachvollziehbar dokumentiert.
4.3.5	Schutz vor Schadprogrammen	Die ICT-Mittel müssen vor Schadprogrammen (Malware) geschützt werden. Die dazu verwendete Lösung ist laufend auf dem aktuellen Stand der abzuwehrenden Angriffe zu halten. Betreiber von ICT-Mitteln (Behörden oder Leistungserbringerinnen) müssen über ein Malwareschutzkonzept verfügen, in welchem geregelt ist: a) Prozesse und Verantwortlichkeiten; b) Aktualisierung der Software zum Malwareschutz; c) Festlegung der Schwerpunkte und Periodizität des Scannens (z. B. Clients, Server, Datenspeicher); d) Technische Umsetzung; e) Vorgehen für Beseitigung von Malware und Beurteilung des Schadensausmasses.
4.3.6	Protokollierung sicherheitsrelevanter Aktivitäten und Ereignisse	Sicherheitsrelevante Ereignisse müssen nachvollziehbar aufgezeichnet und vor unbefugter Bearbeitung gesichert werden. Die Aufzeichnungen müssen so aufbewahrt werden, dass sie ausgewertet werden können.
4.3.7	Dokumentierte Datensicherungs- und Wiederherstellungsverfahren	Die für ICT-Mittel verantwortlichen Behörden stellen sicher, dass definierte und getestete Verfahren zur Sicherung und Wiederherstellung einzelner Daten, des ICT-Mittels und der jeweiligen Konfigurationen eingesetzt werden und nachweisbar sind. Die Backup-Strategie muss ein Mehrgenerationen-Prinzip (Tages-, Wochen- oder Monatsbackup) vorsehen.

		Die Wiederherstellbarkeit und Konsistenz der Backups müssen regelmässig und nachweisbar getestet werden. Ein Datenverlust nach einer Datenwiederherstellung ist in einem Report auszuweisen und der auftraggebenden Behörde zur Verfügung zu stellen.
4.3.8	Sicherung von geschäftskritischen Daten	Wenn ein Datenverlust für die Behörden und deren Aufgabenerfüllung schwerwiegende Folgen haben kann, ist die Datensicherung mit Mehrgenerationen-Prinzip und eine Offline-Speicherung mittels «Write once read many» (WORM) oder mit physischer Entkopplung vom Netzwerk vorzunehmen. Die gesicherten Daten müssen auch im Falle von Ransomware-Angriffen verfügbar und deren Integrität sichergestellt sein.
4.3.9	Systemzeit	Die Systemzeit muss zentral synchronisiert und darf nur von der hierfür verantwortlichen Person verändert werden.
4.3.10	Integritätsschutz	Die Integrität der auf den ICT-Mitteln eingesetzten Softwarekomponenten muss sichergestellt sein, z.B. mit Hilfe von digitalen Signaturen oder Prüfsummen.
4.3.11	Keine unautorisierten Installationen und Ausführungen von Software auf ICT-Endgeräten	Nur geprüfte und freigegebene Software darf auf ICT-Endgeräten (Notebooks, Computer, Server etc.) installiert und ausgeführt werden können. Die Ausführung von ungeprüfter Software ist auf den ICT-Endgeräten zu unterbinden.
4.3.12	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	Für ICT-Mittel sowie ihre Komponenten (z.B. Software-Bibliotheken, Firmware, Treiber, Middleware und Betriebssysteme) muss während der ganzen Nutzungsdauer eine grundsätzlich zeitnahe, nachweisbar regelmässige Wartung und Pflege sichergestellt sein. Darunter fällt insbesondere auch das Einspielen von regelmässigen betrieblichen oder sicherheitstechnischen Updates und Fehlerkorrekturen (Patches). Es müssen Prozesse implementiert sein, die ein Testing und eine zeitgerechte Fehlerkorrektur sicherstellen. Das Installieren sicherheitsrelevanter Patches in bestehenden Services/auf bestehenden Systemen erfolgen risikobasiert und unter Berücksichtigung vertraglich vereinbarter Wartungsfenster. Solange keine entsprechenden Patches zur Verfügung stehen, müssen je nach Schwachstelle oder Bedrohung, andere geeignete Schutzmassnahmen getroffen werden.

4.3.13	Prüfung auf Schwachstellen und Verwundbarkeiten	ICT-Mittel sind vor und in Betrieb nach Massgabe des Schutzbedarfs und der Exposition gegenüber dem Internet regelmässig auf Schwachstellen zu prüfen und nötigenfalls zu verstärken.
4.3.14	Einsatz von mobilen Endgeräten	Der Zugriff auf ICT-Mittel und die Datenbearbeitung durch die Leistungserbringerin ist nur mit sicheren und verwalteten Geräten erlaubt (z.B. End Point Protection – Zugriffsschutz, Disk-Verschlüsselung, Remote Wipe, Malware-Schutz, Sicherheitsupdates). Der Verlust von mobilen Geräten ist gemäss eines geregelten Sicherheitsprozesses zu behandeln.
4.3.15	Ausfallzeiten	Bei ungeplanten Ausfällen ist den auftraggebenden Behörden das Ereignis umgehend zu melden und diese mit regelmässigen Statusupdates auf dem Laufenden zu halten. Nach der Wiederherstellung ist innerhalb angemessener Frist mit einem Bericht über das Ereignis zu informieren.
4.4	**Netzwerksicherheit**	
4.4.1	Ausrichtung	Der Netzwerkverkehr hat, wenn das eingesetzte Protokoll die Möglichkeit bietet (wie z.B. https, ldaps, sftp, ssh), immer verschlüsselt zu erfolgen und unterliegt der Network Security Policy des Kantons Bern.
4.4.2	Netzwerke zur Administration	Administrative Zugriffe auf ICT-Systeme der auftraggebenden Behörde haben aus einem dedizierten Netz zu erfolgen und sind über Jump-Hosts oder sind mittels Multi-Faktor Authentifizierung abgesichert. Administrative Zugriffe sind zu protokollieren und der auftraggebenden Behörde auf Anfrage auszuweisen. Die Aufbewahrungsdauer richten sich nach Art. 4 RDV[6] für bewirtschaftete Daten.
4.5	**Entwicklung und Wartung**	
4.5.1	Entwicklung	Bei der Entwicklung von Applikationen muss sichergestellt sein, dass a) der Quellcode sicher aufbewahrt wird, indem der Zugriff auf die entsprechenden Repositories klar geregelt und nachvollziehbar kontrolliert wird; b) die Build-Prozesse überwacht werden, und Änderungen an der Build-Pipeline nur kontrolliert erfolgen können; c) die Software regelmässig auf Schwachstellen und Funktionalität getestet wird;

[6] Randdatenverordnung des Kantons Bern (RDV, BSG 153.011.5)

		d) die Integrität der Software jederzeit sichergestellt ist (z.B. mit Hilfe von digitalen Signaturen); e) Die Anpassbarkeit bzw. Austauschbarkeit der verwendeten kryptografischen Verfahren muss sichergestellt sein. f) Für Office-Makros gelten c) und d).
4.5.2	Konfiguration und Einstellung	ICT-Mittel müssen vor der ersten Inbetriebnahme so konfiguriert und eingestellt sein, dass sie a) vor unberechtigtem Zugriff geschützt sind; b) technisch gehärtet sind; c) in einer zur Aufgabenerfüllung erforderlichen, vom Benutzer nicht veränderbaren Minimalkonfiguration betrieben werden (d.h. nicht genutzte Schnittstellen, Module und Funktionen müssen deaktiviert sein).
4.5.3	Verwendung von Produktivdaten in Test-, Schulungs- und Entwicklungssystemen	In Test-, Schulungs- und Entwicklungssystemen sind grundsätzlich keine Kopien von Informationen und Personendaten aus produktiven Systemen zu verwenden. Ausnahmen müssen mit Massnahmen zur Risikobehandlung im ISDS-Konzept beschrieben und in die Vorabkontrolle gebracht werden. Die Leistungserbringerinnen stellen sicher, dass Datendateien nach der Übergabe (Kopien), wie auch Daten auf Testsystemen kurz nach Testabschluss gemäss einem standardisierten Prozess gelöscht werden.
4.5.4	Überprüfte Software	Software darf nur dann auf ICT-Endgeräten (Notebooks, Computer, Server etc.) installiert werden, wenn diese aus vertrauenswürdigen Quellen stammt und auf Sicherheitslücken und Malware überprüft wurde.
4.5.5	Geplante Wartung	Geplante Wartungsfenster sind den auftraggebenden Behörden mindestens 30 Arbeitstage vorher mitzuteilen.

2. Sicherheitsstufen für Authentisierungsmittel

Grundsätzlich sind die ICT-Standards[7] des Kantons Bern betr. «Single-Sign-On», Authentisierungsmethoden und der «Anbindung an Identity-Provider (IdP)» einzuhalten. Die genannten Beispiele sind nicht abschliessend zu verstehen und in der Tabelle summarisch zusammengestellt.

Schutzniveau nach ICSGW	Mögliche Authentisierungsmittel
0	• Benutzername und Passwort • «Bearer-Token» (z. B. Cookies)
1	• Benutzername und Passwort mit SMS-Verifikationscode[8] • Benutzername und Passwort mit Gerätebindung (TPM oder kryptographischer Token) • OTP (One-Time Password)-Software-Lösung (z. B. Microsoft Authenticator-App) • Software-Zertifikat • Kerberos-Tickets der Ressourcen-Forests • Per SAML (Security Assertion Markup Language) oder OIDC (OpenID Connect) / OAuth (Open Authorization) übertragene «Bearer-Token» wie JSON Web Token (JWT)
2	• OTP-Token (z. B. RSA, Vasco) • OTP-Lösung auf der Basis eines TPM (z.B. Single-Sign-On des BE-KWP) • FIDO2-Token • Swisscom Mobile ID • SwissID
3	• Eigene PKI-Lösung oder PKI-Lösung des Bundes

3. Physische Sicherheit

Die in der Norm ISO 27002:2022: Ref. 7.1 bis Ref. 7.9. detailliert beschriebenen Anforderungen umfassen die folgenden Themen (zur Orientierung auch die Kapitel aus der alten Version):

Version 2022	Alte Version 2013	Thema
7.1	11.1.1	Physische Sicherheitsperimeter
7.2	11.1.2, 11.1.6	Physische Zutrittssteuerung
7.3	11.1.3	Sichern von Büros, Räumen und Einrichtungen
7.4	keine Referenz	Überwachung der physischen Sicherheit
7.5	11.1.4	Schutz vor physischen und umweltbedingten Bedrohungen
7.6	11.1.5	Arbeiten in Sicherheitsbereichen
7.7	11.2.9	Aufgeräumte Arbeitsumgebung und Bildschirmsperren
7.8	11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln
7.9	11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten ausserhalb der Räumlichkeiten

[7] ICT-Standards des Kanton Bern
[8] Grundsätzlich sollten SMS-basierte Authentifikationsverfahren nur noch eingesetzt werden, wenn es keine bessere Alternative gibt.

Dokument-Protokoll

Freigabekontrolle

Version	Name	Datum	Bemerkungen
0.2	GS FIN	20.03.2024	Genehmigung Entwurf z.H. Konsultation
0.41	GL KAIO	26.08.2024	Beschluss, vorbehältlich Prüfung DSA
0.41	Ueli Buri	04.09.2024	Prüfung DSA
1.0	Beat Jakob	05.09.2024	Unterzeichnung
2.0	GL KAIO	16.12.2024	Beschluss mit Anhang 5 und 6

Kanton Bern
Canton de Berne

Anhang 3 ICSGW:

Grundschutz Auftragsdatenbearbeitung

Beschlussdatum	16.12.2024
Version	2.0
Dokument Status	abgenommen
Klassifizierung	Nicht klassifiziert
Autoren	Daniel Lörtscher / Sascha Tarli
Dokumentnummer	432427
Geschäftsnummer	2024.KAIO.76

Herausgeber: Amt für Informatik und Organisation des Kantons Bern (KAIO)

1. Gegenstand

Dieser Anhang 3 zur ICSGW bestimmt die Anforderungen an die Bearbeitung von Informationen und Personendaten durch von den Behörden beauftragte Dritte (nachfolgend Leistungserbringerinnen). Die von den Leistungserbringerinnen eingesetzten ICT-Mittel müssen die Anforderungen der ICSGW inkl. Anhänge erfüllen.

Die Bedag Informatik AG ist im Eigentum des Kantons Bern. Ihre Pflichten insbesondere zur Informations- und Datensicherheit sind vorab und separat in der Eignerstrategie 2024 Bedag Informatik AG sowie den Ausführungsbestimmungen zur Eignerstrategie 2024, beide vom 13. Dezember 2023, als Teil des Regelwerks der ICT der Kantonsverwaltung verbindlich beschrieben. Sie gehen den vertraglichen Bestimmungen vor.

2. Sicherheitsanforderungen

Die Sicherheitsanforderungen werden pro Schutzniveau gemäss Anhang 1 ICSGW beschrieben.

Die in den Spalten Schutzniveau 0 und 1 beschriebenen Massnahmen stellen die Anforderungen an den Grundschutz bei Auftragsdatenbearbeitung dar. Auf die generell-abstrakte Festlegung der Anforderungen des Schutzniveaus 3 wird verzichtet. Diese sind ergänzend zu Schutzniveau 2 risikobasiert im ISDS-Konzept zu definieren.

ID	Sicherheitsanforderung	Schutzniveau 0	Schutzniveau 1	Schutzniveau 2
1	Ort der Datenbearbeitung und -speicherung (auch im Redundanzfall und Backups)	Weltweit	Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz gemäss Anhang 1 der Verordnung des Bundesrates vom 31. August 2022 über den Datenschutz (DSV)[1]	
2	Gerichtsstand und anwendbares Recht	Keine Anforderung	Schweiz	
3	Angaben zu Ermittlungsanfragen staatlicher Stellen	Keine Anforderung	Leistungserbringerinnen und deren Subunternehmen müssen ihre gesetzlichen Verpflichtungen, Daten an ausserkantonale oder ausländische Behörden bekanntzugeben, offenlegen.	
4	Angaben zu vorhandenen Zertifizierungen und Auditberichten	Keine Anforderung	Bereitstellung der vorhandenen Zertifikate und Auditberichte. Mindestens: Nachweis Einhaltung Grundschutz gemäss ICSGW oder ISO/IEC 27001 Nur die ISO27001 Zertifizierung ohne den Nachweis unseres Grundschutzes ist nicht geleichwertig und muss in der Risikoanalyse behandelt werden.	Bereitstellung der vorhandenen Zertifikate und Auditberichte. Mindestens: Nachweis Einhaltung Grundschutz gemäss ICSGW oder ISO/IEC 27001 ISO 27017 ISO 27018 Nur die ISO Zertifizierungen ohne den Nachweis unseres Grundschutzes ist nicht geleichwertig und muss in der Risikoanalyse behandelt werden.

[1] DSV; SR 235.11

5	Angaben zu Servicebedingungen (Terms of Service)	Für alle Endbenutzer als Terms of Service online abrufbar.		
6	Umgang mit Randdaten	Keine Anforderung	Transparente Angaben über alle anfallenden Log- und Telemetriedaten des Services und der Nutzer, deren Nutzungszwecke, die zugriffsberechtigten Gruppen und deren Aufbewahrungsorte und -zeiten	
7	Daten für Support und Tests	Keine Anforderung	Daten für Support und Tests müssen - auch bei Supportorganisationen, die dem Follow-the- Sun-Prinzip folgen - immer in Ländern mit einem angemessenen Datenschutz gemäss Anhang 1 DSV erfolgen. Test- und Supportdaten müssen nach ihrer Zweckerfüllung umgehend und nicht wiederherstellbar gelöscht werden.	
8	Separierung der Daten von anderen Kunden und technische Ausgestaltung des Cloud Services	Die Leistungserbringerinnen können aufgrund der gewählten Architektur und den zur Verfügung gestellten Dokumentationen nachweisen, dass der angebotene Service eine angemessene Trennung gegenüber anderen Kunden sicherstellt. Konzepte, Architekturen und Dokumentationen werden auf Anfrage von den Leistungserbringerinnen kostenlos zur Verfügung gestellt.		
9	Standort Identity-Store	In Ländern mit einem angemessenen Datenschutz gemäss Anhang 1 DSV.		
10	Zugriffsberechtigungen	Bei temporär nötigen Zugriffen der Leistungserbringerinnen werden diese Zugriffsberechtigungen zeitnah, aber spätestens nach 14 Tagen angepasst oder entzogen.		
11	Speicherverschlüsselung der Inhaltsdaten («Data at Rest»)	Keine Anforderung	Alle Inhaltsdaten müssen verschlüsselt abgelegt werden.	Alle Inhaltsdaten werden verschlüsselt gespeichert. Wenn die für die Verschlüsselung verwendeten privaten Schlüssel nicht ausschliesslich der Behörde bekannt sind, müssen sich die Leistungserbringerinnen vertraglich verpflichten, die privaten Schlüssel nur mit der ausdrücklichen Zustimmung der Behörde zu verwenden.
12	Netzwerksicherheit	Anwendung von Firewalls und IDS/IPS-Systemen (Intrusion Detection System / Intrusion Prevention System). Bei einer erhöhten Verfügbarkeitsanforderung ist zusätzlich ein DDoS-	Anwendung von Firewalls und IDS/IPS-Systemen sowie einer Application Level Firewall (XML/WAF) oder eines Zero-Trust-Modells. Bei einer erhöhten Verfügbarkeitsanforderung ist zusätzlich ein DDoS-Schutz vorzusehen.	

		Schutz (Distributed Denial of Service) vorzusehen.	
13	Verschlüsselte Kommunikation	Die Datenübermittlung sowie jede andere Kommunikation zwischen den Leistungserbringerinnen und der Behörde, zwischen und in den Cloud-Standorten sowie mit allfälligen Subunternehmen der Leistungserbringerinnen hat gemäss Anhang 6, Kryptographische Verfahren, zu erfolgen.	
14	Portabilität – Bereitstellung von Daten	In regelmässigen Abständen und bei Vertragsende muss die Möglichkeit bestehen, die Daten unter Beibehaltung aller logischen Relationen in einem anwendbaren Standardformat exportieren zu können. Allfällige Zusatzkosten sind offenzulegen. Der Service verfügt über eine Funktionalität, wodurch Snapshots von Systemen/Containern oder der Datenexport ohne Beteiligung der Leistungserbringerinnen über standardisierte oder offengelegte Schnittstellen (API (Application Programming Interface) und Protokolle) erfolgen kann.	
15	Backup ausserhalb Cloud	Bereitstellung einer Schnittstelle, um ein Backup der Daten oder Snapshots von Systemen/Containern auf einen anderen On-Prem- oder Cloud-Speicher durchführen zu können.	

Dokument-Protokoll

Freigabekontrolle

Version	Name	Datum	Bemerkungen
0.2	GS FIN	20.03.2024	Genehmigung Entwurf z.H. Konsultation
0.24	GL KAIO	26.08.2024	Beschluss vorbehältlich Prüfung DSA
0.24	Ueli Buri	04.09.2024	Prüfung DSA
1.0	Beat Jakob	05.09.2024	Unterzeichnung
2.0	GL KAIO	16.12.2024	Beschluss mit Anhang 5 und 6

Allgemeine Geschäftsbedingungen des Kantons Bern

über die

Informationssicherheit und den Datenschutz

AGB ISDS BE

vom 26.08.2024
revidiert 16.12.2024 / 09.07.2025 / 27.10.2026
Version 3.1

Inhaltsverzeichnis

1. Zweck ... 2
2. Begriffe ... 2
3. Unterstellung unter das Datenschutzgesetz des Kantons Bern ... 3
4. Verhältnis zum Vertrag sowie zu den AGB DVS ... 3
5. Informations- und Datensicherheit ... 3
6. Datenbearbeitung ... 4
7. Beizug von Subunternehmen ... 4
8. Audits ... 5
9. Meldepflicht und Sofortmassnahmen bei Sicherheitsvorfällen und Schwachstellen ... 6
10. Personaleinsatz, Geheimhaltung und Konventionalstrafen ... 6
11. Rückgabe und Löschung bei Vertragsende ... 7

1. Zweck

1.1 Diese Allgemeinen Geschäftsbedingungen über die Informationssicherheit und den Datenschutz (AGB ISDS BE) bezwecken die Gewährleistung der Informations- und Datensicherheit und damit auch des Datenschutzes bei der Beschaffung und beim Einsatz von ICT-Mitteln durch die Behörden des Kantons Bern.

1.2 Mit der Umsetzung der AGB ISDS BE sowie der Anforderungen gemäss der Weisung über den Grundschutz für die Informations- und Cybersicherheit (ICSGW) wird der Grundschutz für die ICT-Mittel, Informationen und Personendaten auch durch die Leistungserbringerinnen sichergestellt.

2. Begriffe

In diesen AGB ISDS BE bedeuten:

2.1 **Behörden:** Auftraggebende kantonale Behörden, die Gemeindebehörden sowie die Träger öffentlicher Aufgaben des Kantons und der Gemeinden unabhängig von ihrer Rechtsform (Art. 4 Abs. 1 und 2 des Gesetzes vom 7. März 2022 über die digitale Verwaltung (DVG)[1]).

2.2 **Leistungserbringerin**: Eine natürliche oder juristische Person, welche im Auftrag einer Behörde diese mit ICT-Mitteln versorgt.

2.3 **ICT-Mittel:** Güter und Dienstleistungen der Informations- und Telekommunikationstechnik (ICT), einschliesslich Hardware und Software (Art. 4 Abs. 3 Bst. a DVG).

2.4 **Informationen:** Angaben in beliebiger Form über Sachverhalte, jedoch ohne Personendaten (Art. 4 Bst. b ICSGW).

2.5 **Personendaten:** Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person (Art. 2 Bst. a des Kantonalen Datenschutzgesetzes vom 3. Dezember 2025, [KDSG][2]).

2.6 **Informations- bzw. Datensicherheit:** Zustand, womit die Vertraulichkeit, Verfügbarkeit und Integrität von ICT-Mitteln, Informationen und Personendaten sowie die Nachvollziehbarkeit ihrer Bearbeitung gewährleistet sind (Art. 4 Bst. d ICSGW).

2.7 **Bearbeiten:** Jeder Umgang mit Personendaten, unabhängig von den angewendeten Mitteln und Verfahren, insbesondere deren Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten. (Art. 2 Bst. f KDSG).

2.8 **Bekanntgeben:** Das Übermitteln und Zugänglichmachen von Personendaten wie das Einsichtgewähren, Auskunftgeben, Weitergeben oder Veröffentlichen. (Art. 2 Bst. g KDSG).

2.9 **Sicherheitsvorfall:** Ein Ereignis, welches die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der ICT-Mittel, Informationen oder Personendaten gefährdet (Art. 4 Bst. f ICSGW) .

[1] DVG; BSG 109.1
[2] KDSG; BSG 152.04

3. Bearbeitung von Personendaten durch Leistungserbringerin

3.1 Die Leistungserbringerin nimmt zur Kenntnis, dass sie als beauftragte Dritte gemäss Artikel 12 KDSG die Personendaten nur so bearbeiten darf, wie es die auftraggebende Behörde selbst tun dürfte. Insbesondere bedarf die Bekanntgabe der Personendaten an weitere Dritte der ausdrücklichen Zustimmung der Behörde (s. Ziff. 7.1, Art. 12 Abs. 3 KDSG).

3.2 Die Leistungserbringerin darf die Personendaten nur im vertraglich vereinbarten Umfang und zum Zweck der Vertragserfüllung bearbeiten.

3.3 Erbringt die Leistungserbringerin Leistungen für Strafverfolgungsbehörden oder -gerichte mit Verzeichnispflicht nach Artikel 22 KDSG, so muss die Leistungserbringerin ebenfalls ein Verzeichnis führen (Art. 8 Abs. 1 KDSV).

4. Verhältnis zum Vertrag sowie zu den AGB DVS

4.1 Die AGB ISDS BE sind Teil des Vertrages zwischen der Leistungserbringerin und der Behörde. Vorbehalten bleiben abweichende Vereinbarungen.

4.2 Die Allgemeinen Geschäftsbedingungen für IKT-Leistungen der Digitalen Verwaltung Schweiz (AGB DVS)[3], Ausgabe März 2025, sind ebenso Teil des Vertrages, gehen aber diesem sowie den AGB ISDS BE nach.

5. Informations- und Datensicherheit

5.1 Verantwortung

5.1.1 Die Behörde behält die Verfügungsmacht an den in ihrem Auftrag bearbeiteten Informationen und Personendaten; dies gilt sowohl für Inhaltsdaten als auch für Randdaten nach Artikel 1 Absatz 1 Buchstabe a und b der Randdatenverordnung vom 20. November 2019 (RDV)[4]. Sie bleibt für deren Schutz verantwortlich und weisungsberechtigt (Gewährleistungsverantwortung, Art. 8 Abs. 1 KDSG).

5.1.2 Die Leistungserbringerin hat im Rahmen ihres Herrschaftsbereichs für die Sicherheit der ihr anvertrauten ICT-Mittel, Informationen und Personendaten zu sorgen.

5.1.3 Die Leistungserbringerin erwirbt an den bearbeiteten Informationen und Personendaten keine Rechte. Sie hat die ISDS-Massnahmen wirksam umzusetzen und die Weisungen der Behörde zu befolgen (Umsetzungsverantwortung).

5.2 Umsetzung des Grundschutzes

5.2.1 Die Leistungserbringerin hat die Grundschutzmassnahmen gemäss der ICSGW, zum Stand des Vertragsschlusses, umzusetzen und nachweisbar auf ihre Wirksamkeit zu prüfen. Leistungsspezifische Präzisierungen sind im Vertrag geregelt.

[3] AGB DVS, Ausgabe März 2025
[4] RDV; BSG 153.011.5

5.3 Umsetzung des erhöhten Schutzes gemäss ISDS-Analyse und -Konzept

5.3.1 Führt die ISDS-Analyse der Behörde zum Ergebnis, dass für die zu bearbeitenden Informationen und Personendaten ein erhöhter Schutzbedarf besteht, so sind die dazu erforderlichen und vertraglich, gemäss ISDS-Konzept vereinbarten Massnahmen von der Leitungserbringerin umzusetzen und nachweisbar auf ihre Wirksamkeit zu prüfen (Art. 5 ISDS DV[5]: ISDS-Analyse und -Konzept).

6. Datenbearbeitung

6.1 Zweckbindung

6.1.1 Die Informationen und Personendaten dürfen nur durch diejenigen Mitarbeitenden der Leistungserbringerin bearbeitet werden, welche die Informationen und Personendaten zur Erfüllung des Vertrages benötigen. Die Bearbeitung der Informationen und Personendaten darf ausschliesslich zum vertraglich festgelegten Zweck erfolgen.

6.2 Bearbeiten und Bekanntgabe von Informationen oder Personendaten

6.2.1 Die Leistungserbringerin darf Informationen oder Personendaten der Behörde ohne anderslautende Ermächtigung nur für die Behörde bearbeiten oder bekanntgeben. Begehren von Privaten oder anderen Behörden um Datenbekanntgabe sind unverzüglich der Behörde weiterzuleiten.

6.2.2 Vorbehalten sind gesetzlich vorgesehene prozessuale Zwangsmassnahmen anderer zuständiger Behörden. Auch in diesen Fällen ist, soweit gesetzlich zulässig, an die Behörde zu verweisen, oder diese ist unverzüglich zu informieren.

6.3 Ort der Bearbeitung von Informationen und Personendaten

6.3.1 Soweit der Vertrag nichts anderes vorsieht, darf die Bearbeitung der Informationen und Personendaten nur in der Schweiz oder in einem Staat mit einem angemessenen Datenschutz gemäss Anhang 1 der Verordnung des Bundesrates vom 31. August 2022 über den Datenschutz (DSV)[6] erfolgen.

7. Beizug von Subunternehmen

7.1 Der Vertrag regelt, ob und unter welchen Umständen die Leistungserbringerin Subunternehmen beiziehen darf, welche bei direkter Ausübung der ihnen von der Leistungserbringerin übertragenen wesentlichen Leistungen selbst in den Anwendungsbereich der AGB ISDS BE fallen würden. Soweit bei Vertragsschluss bekannt, werden diese Subunternehmen im Vertrag aufgeführt und deren Einsatz von der Behörde genehmigt.

7.2 Die Leistungserbringerin verpflichtet die Subunternehmen gemäss Ziff. 7.1 vertraglich, die Sicherheitsmassnahmen gemäss Hauptvertrag, ISDS-Konzept sowie gemäss den AGB ISDS BE als auch AGB SIK umzusetzen.

[5] ISDS DV, BSG 152.040.2
[6] DSV; SR 235.11

8. Audits

8.1 Rechtmässigkeitsprüfung

8.1.1 Die Leistungserbringerin räumt folgenden unabhängigen staatlichen Aufsichtsstellen im Rahmen deren gesetzlichen Aufgaben zur Überprüfung der rechtmässigen Leistungserbringung ein Audit- und Kontrollrecht ein:

a) der zuständigen Datenschutzbehörde;
b) dem zuständigen Finanzaufsichtsorgan.

Die Leistungserbringerin ist im Rahmen der gesetzlichen Grundlagen der Aufsichtsstellen zur Mitwirkung und insbesondere zur Herausgabe der erforderlichen Informationen und Unterlagen verpflichtet.

8.2 Leistungsüberprüfung

8.2.1 Die Behörde kann im Zusammenhang mit den vertraglich vereinbarten Leistungen Audits im Bereich der Informationssicherheit, des Datenschutzes, der Prozesse und der Rechnungsstellung durchführen.

8.3 Durchführung der Audits

8.3.1 Der Behörde obliegt die Leitung des Audits. Sie bestimmt nach Anhörung der Leistungserbringerin

a) die Auditobjekte, wie z.B. Prozesse, Core Services, Software, Datensammlungen, Dokumentationen und Quellcode, Leistungsabrechnungen;
b) die mit dem Audit beauftragte Organisation, wobei es sich nicht um einen direkten Konkurrenten der Leistungserbringerin handeln darf, und
c) das Verfahren und die Einzelheiten des Audits.

8.3.2 Die Behörde wird die Ausübung der Auditrechte grundsätzlich mindestens einen Monat im Voraus ankündigen, unter Darlegung des Auditthemas und –zeitplans. Bei Sicherheitsvorfällen kann die Frist verkürzt werden.

8.3.3 Die Leistungserbringerin wirkt beim Audit gemäss den Weisungen der Behörde oder der mit dem Audit beauftragten Organisation auf eigene Kosten mit. Sie gewährt deren Mitarbeitenden oder Beauftragten den nötigen Zugang, gewährt ihnen die nötige Einsicht und beantwortet die von ihnen gestellten Fragen.

8.3.4 Die Behörde verpflichtet die mit dem Audit beauftragte Organisation und ihre Mitarbeitenden oder Beauftragten zur Verschwiegenheit.

8.4 Kosten

8.4.1 Die Kosten für ein Audit infolge eines hierzu beauftragten Dritten werden grundsätzlich von der Behörde übernommen. Im Übrigen tragen die Parteien die ihnen infolge des Audits angefallenen Kosten grundsätzlich selbst.

8.4.2 Stellt sich anlässlich des Audits heraus, dass gesetzliche oder vertragliche Vorschriften verletzt wurden und von der auditierenden Behörde Feststellungen mittlerer oder hoher Bedeutung gemacht wurden, so gilt jedoch, dass die Leistungserbringerin

a) die infolge nicht gehöriger Vertragserfüllung und der demzufolge zu viel bezogenen Vergütungen, zuzüglich Zins zu 5 %, und

b) alle internen und externen Kosten, die der Behörde im Zusammenhang mit dem Audit entstanden sind,

innert 30 Tagen nach Vorliegen des von der auditierenden Behörde genehmigten Schlussberichts dem Kanton schuldet.

8.4.3 Die Kosten zur Behebung der im Audit festgestellten Mängel gehen zu Lasten der Leistungserbringerin.

9. Meldepflicht und Sofortmassnahmen bei Sicherheitsvorfällen und Schwachstellen

9.1 Die Leistungserbringerin hat die Behörde über Sicherheitsvorfälle oder Schwachstellen gemäss Art. 4 Bst. f und g ICSGW zu informieren und mit der Behörde zusammenzuarbeiten, insbesondere wenn

a) ein Sicherheitsvorfall oder eine Schwachstelle gemäss ICSGW, Anhang 2, Ziff. 1.1.4, vorliegt, oder
b) eine andere ausserkantonale oder ausländische Behörde bei der Leistungserbringerin Kontrollhandlungen und Massnahmen durchführt, soweit sie Informationen, Personendaten oder ICT-Mittel gemäss Vertrag betreffen, oder
c) ICT-Mittel bei der Leistungserbringerin durch Pfändung, Konkurs oder andere Zwangsvollstreckungsmassnahmen oder durch sonstige Ereignisse oder Massnahmen Dritter entzogen werden. Die Leistungserbringerin wird alle hierfür Verantwortlichen unverzüglich darüber informieren, dass die Verfügungsmacht über die Informationen und Personendaten gemäss Vertrag allein bei der Behörde liegt.

Die vorgenannten Sicherheitsvorfälle oder eine Schwachstelle müssen spätestens innert 24 Stunden seit Entdeckung über die Meldeplattform BE gemeldet werden.

9.2 Die Leistungserbringerin wird in den vorgenannten Fällen umgehend diejenigen Sofortmassnahmen ergreifen, die rechtlich und nach dem aktuellen Stand der Technik erforderlich sind, um die Informationen und Personendaten und die für deren Bearbeitung eingesetzten ICT-Mittel zu sichern und nachteilige Folgen bestmöglich zu verhindern bzw. zu minimieren.

9.3 Die Leistungserbringerin dokumentiert zu Handen der Behörde die Vorfälle und allfällige Verletzungen der Informations- und Datensicherheit. Zudem ergreift und dokumentiert sie diejenigen Massnahmen, welche nach dem aktuellen Stand der Technik erforderlich sind, um eine Wiederholung der Verletzung zu verhindern.

10. Personaleinsatz, Geheimhaltung und Konventionalstrafen

10.1 Es gelten die Ziff. 8, und15 und 22 der AGB DVS, insbesondere auch die dort beschriebenen straf- und privatrechtlichen Sanktionen.

11. Rückgabe und Löschung bei Vertragsende

11.1 Mit Beendigung des Vertrages hat die Leistungserbringerin sämtliche in ihrem Herrschaftsbereich liegenden Informationen und Personendaten im vereinbarten oder einem weiterverarbeitbaren Format gemäss aktuellem Stand der Technik der Behörde unentgeltlich auszuhändigen.

11.2 Durch die Leistungserbringerin bearbeitete Informationen oder Personendaten hat sie gemäss Weisung der Behörde unentgeltlich und gemäss Anforderungen des Anhangs 2 zur ICSWG, Ziff. 1.2.3, nicht wiederherstellbar zu löschen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf erste Aufforderung der Behörde vorzulegen.

* * *

Dokument-Protokoll

Freigabekontrolle

Version	Name	Datum	Bemerkungen
0.5	GS FIN	20.03.2024	Genehmigung Entwurf z.H. Konsultation
0.31	GL KAIO	26.08.2024	Beschluss vorbehältlich Prüfung DSA
0.31	Ueli Buri	04.08.2024	Prüfung DSA
1.0	Beat Jakob	05.09.2024	Unterzeichnung KAIO
2.0	GL KAIO	16.12.2024	Beschluss mit Anhang 5 und 6
3.0	Thomas Fischer	09.07.2025	Redaktionelle Anpassung an AGB DVS
3.1	Sascha Tarli	01.10.2026	Anpassungen an neue/s KDSG und KDSV
3.1	Ueli Buri	16.10.2026	Prüfung und Ergänzung

Kanton Bern
Canton de Berne

Anhang 5 ICSGW:

Umgang mit Authentisierungsmerkmalen

Beschlussdatum	16.12.2024
Version	1.0
Dokument Status	abgenommen
Klassifizierung	Nicht klassifiziert
Autor	KAIO
Dokumentnummer	432568
Geschäftsnummer	2024.KAIO.76

Herausgeber: Amt für Informatik und Organisation des Kantons Bern (KAIO)

1. Gegenstand, Zweck und Begriffe

Gegenstand und Zweck

Art. 1 Dieser Anhang regelt die Handhabung von Authentisierungsmerkmalen zwecks deren einheitlichen Anwendung bei der Nutzung von ICT-Mitteln

Begriffe

Art. 2 In diesem Anhang bedeuten:

a *Authentisierung:* Eine Person oder ein technischer Benutzer weist die digitale Identität nach, indem sie den Datensatz der digitalen Identität ins ICT-Mittel eingeben, z.B. ihren Benutzernamen und das zugehörige Passwort.

b *Authentifizierung:* Das ICT-Mittel überprüft die von der Person oder vom technischen Benutzer gemachten Angaben mit denjenigen auf der zugehörigen Datensammlung. Bei deren Übereinstimmung wird die Berechtigung für das ICT-Mittel erteilt (Autorisierung).

c *Authentisierungsmerkmal:* Eigenschaft, mit der gegenüber einem ICT-Mittel der Nachweis der Identität erbracht wird.

d *Passwort:* Authentisierungsmerkmal, bestehend aus einer Zeichenkette.

e *Persönliche Identifikationsnummer PIN:* Authentisierungsmerkmal, bestehend aus einer Zeichenkette, die an ein bestimmtes Gerät oder Token gebunden ist und nie im Klartext über Netzwerke übertragen wird.

f *Biometrisches Merkmal:* Authentisierungsmerkmal, bestehend aus einer individuellen und unveränderlichen Eigenschaft des menschlichen Körpers.

g *Token:* Ein ICT-Mittel, das zwecks Authentisierung ein Einmalpasswort erzeugt oder ein komplexes Authentisierungsmerkmal (z.B. ein Zertifikat) bereitstellt.

h *Administratorkonto:* Zugang zu einem ICT-Mittel, über welchen Änderungen am ICT-Mittel vorgenommen werden können, die sich auf die Nutzenden auswirken, und Einsichtsrechte gewährt, die über diejenigen der Nutzenden hinausgehen.

i *Service-Benutzerkonto:* Zugang zu einem ICT-Mittel, welches von einem anderen ICT-Mittel genutzt wird.

j *Integriertes Administratorkonto*: Ein vom ICT-Mittel nicht entfernbares Administratorkonto.

2. Vorschriften für die Benutzerinnen und Benutzer

Grundsatz

Art. 3 [1] Passwörter, PIN und Token sind vertraulich und zudem persönlich. Sie dürfen anderen Personen nicht bekannt gegeben oder anvertraut werden.

[2] Die berechtigte Person ist für die sichere Aufbewahrung und Handhabung der Passwörter, PIN und Token verantwortlich.

[3] Erhält eine andere Person, auch nur mutmasslich, Kenntnis eines Passworts oder eines PIN, so ist das Passwort oder der PIN unverzüglich zu ändern.

[4] Geht ein Token oder ein mit einem PIN oder Passwort gesichertes Gerät verloren, ist der Sicherheitsvorfall unverzüglich dem Service Desk des KAIO zu melden.

Unberechtigte Benutzung

Art. 4 [1] Wer vermutet, dass unberechtigte Personen versuchen, mit dem Passwort einer Drittperson zu arbeiten, informiert unverzüglich die vorgesetzte oder die für das ICT-Mittel verantwortliche Person.

[2] Konnten unberechtigte Personen die Eingabe von Passwörtern oder PIN beobachten, sind diese geschützt zu ändern.

Umgang mit Authentisierungsmerkmalen

Art. 5 [1] Passwörter und PIN müssen verschlüsselt gespeichert werden (z.B. mit dem Passwortmanager «KeePass» auf dem kantonalen Arbeitsplatz).

[2] Nach dem Stand der Technik vor der Entwendung zu schützen sind:

a Passwörter,

b PIN,

c Token,

d mobile Geräte, die zur Authentisierung benützt werden.

Passwortwahl

Art. 6 Passwörter und PIN

a sind grundsätzlich automatisch zu generieren und in einem Passwortmanager gemäss Art. 5 zu speichern,

b dürfen nicht für mehrere ICT-Mittel gleich lauten,

c sind so zu wählen, dass sie nicht in einer bekannten Analogie oder Beziehung zur benutzenden Person stehen und damit auf einfache Art erraten werden können.

3. Anforderungen an Systeme und Anwendungen

Grundsatz

Art. 7 [1] Das Recht für einen Zugang via eines Administratorkontos muss durch mindestens zwei unabhängige Authentisierungsmerkmale (Faktoren) überprüft werden.

[2] Sie müssen mindestens aus zwei der folgenden Gruppen gewählt werden:

a Wissen: z.B. Passwort oder PIN,

b Besitz: z.B. Laptop, Token oder Smartphone,

c Körper: ein biometrisches Merkmal (z.B. der Fingerabdruck).

Allgemeine Bestimmungen

Art. 8 Anwendungen haben die folgenden Anforderungen zu erfüllen:

a Jede Person kann das eigene Passwort jederzeit ändern und zurücksetzen

b Die Anwendung verdeckt das eingegebene Passwort;

c Sie verhindert eine Wiederverwendung der zuletzt verwendeten Passwörter;

d Die Passwörter sind in der Anwendung verschlüsselt gespeichert;

e Die Anwendung kann einen Passwortwechsel initiieren;

f Das Authentifizierungsverfahren ist dokumentiert und entspricht einem aktuell gültigen Industriestandard.

PINs

Art. 9 [1] Der Einsatz von PINs ist zulässig, wenn

a zur Authentisierung zusätzlich ein Token oder ein biometrisches Merkmal eingesetzt wird, oder

b die Authentisierung mit der PIN nur auf einem bestimmten Gerät erfolgen kann; in diesem Fall gilt dieses als Token.

[2] In Fällen von Absatz 1 Buchstabe b ist eine zusätzliches Authentisierungsmerkmal gemäss Artikel 7 vorzusehen für den Zugriff über das mobile Gerät auf

a als VERTRAULICH oder höher klassifizierte Informationen,

b besonders schützenswerte Personendaten, oder

c Personendaten, die einer besonderen Geheimhaltungspflicht unterstehen.

[3] Werden PINs eingesetzt, kann ihre wiederholte Eingabe durch ein biometrisches Merkmal ersetzt werden.

Passwortkomplexität

Art. 10

[1] Passwörter müssen

a mindestens zehn Zeichen lang sein,

b Gross- und Kleinschreibung unterscheiden, und

c mindestens ein Zeichen aus mindestens drei der folgenden Zeichengruppen enthalten:

1. Grossbuchstaben,
2. Kleinbuchstaben,
3. Ziffern,
4. andere Zeichen.

[2] Passwörter für Konten mit erweiterten Berechtigungen oder Administratorkonten müssen mindestens fünfzehn Zeichen lang sein.

[3] Passwörter für Service-Benutzerkonten oder integrierte Administratorenkonten müssen mindestens sechsundzwanzig Zeichen lang sein.

[4] PINs müssen mindestens acht Zeichen lang sein.

Passwortwechsel

Art. 11

[1] Passwörter und PINs sind grundsätzlich unbeschränkt gültig.

[2] Passwörter für Konten mit erweiterten Berechtigungen oder Administratorkonten sind mindestens halbjährlich zu ändern.

[3] Passwörter für Service-Benutzerkonten oder integrierte Administratorenkonten sind mindestens jährlich zu ändern. Wenn eine jährliche Passwortänderung technisch nicht möglich ist, muss die Passwortlänge auf mindestens 32 Stellen erhöht werden.

[4] Das neue Passwort darf nicht in einfacher Weise aus dem alten abgeleitet werden können.

[5] Wenn Hinweise darauf vorliegen, dass Passwörter oder PINs Unbefugten zugänglich gemacht wurden, müssen die System- und Anwendungsverantwortlichen die Passwörter oder PINs der potenziell betroffenen Benutzerinnen und Benutzer unverzüglich zurücksetzen.

Erstanmeldung

Art. 12 Für die Erstanmeldung neuer Benutzerinnen und Benutzer sind Einmalpasswörter zu vergeben, die nach dem ersten Gebrauch nicht mehr verwendet werden können.

Verschlüsselte Übertragung von Authentisierungsmerkmalen

Art. 13 Authentisierungsmerkmale (z.B. Benutzername, Passwort) dürfen nur getrennt und in Netzen nur verschlüsselt übertragen werden. Dies gilt nicht für Einmalpasswörter.

Passwortsperrung

Art. 14 [1] Nach fünfmaliger fehlerhafter Eingabe des Passworts oder der PIN muss eine Sperrung erfolgen.

[2] Diese Sperrung kann grundsätzlich nur von den System- und Anwendungsverantwortlichen aufgehoben werden. Sie kann auch durch die Berechtigten selbst aufgehoben werden, nachdem sich diese mit einem anderen Passwort oder durch die korrekte Beantwortung mehrerer Sicherheitsfragen identifiziert haben.

[3] Eine automatische Entsperrung nach mindestens 30 Minuten ist zulässig.

[4] Im Enterprise Mobility Management (EMM) werden nach zehnmaliger fehlerhafter Eingabe die geschäftlichen Daten gelöscht. Wenn es technisch möglich ist, bleiben die privaten Daten erhalten.

4. Missbrauch und Ausnahmen

Missbrauch

Art. 15 Bei Meldungen über unberechtigte Benutzung klären die System- und Anwendungsverantwortlichen ab, ob tatsächlich und durch wen ein Missbrauch erfolgte. Sie leiten die entsprechenden Massnahmen ein.

Ausnahmen

Art. 16 [1] Ausnahmen von diesem Anhang sind in den folgenden Fällen zulässig, wenn das damit geschaffene Risiko vertretbar bleibt:

a falls die Einhaltung in bestehenden Anwendungen nur mit unverhältnismässig grossem Aufwand möglich wäre;

b falls das eingesetzte System die Umsetzung nicht vollständig unterstützt; oder

c falls Stellvertretungsregeln nicht anders als durch eine gemeinsame Identifikation gelöst werden können.

[2] Ausnahmen dauern höchstens ein Jahr. Sie können erneuert werden.

[3] Zuständig zum Entscheid über Ausnahmen ist die für den Datenschutz verantwortliche Behörde (Art. 8 Abs. 1 KDSG). Sind mehrere Behörden verantwortlich, ist die für den Datenschutz insgesamt sorgende Behörde zuständig (Art. 8 Abs. 2 KDSG).

[4] Die System- und Anwendungsverantwortlichen dokumentieren,

a wer über die Ausnahme entschieden hat,

b von welchen Bestimmungen dieses Anhangs aus welchem Grund und in welchem Umfang abgewichen wird,

c welche ICT-Mittel, Personen oder Personengruppen die Ausnahme betrifft, und

d wie lange die Ausnahme dauert.

[5] Die System- und Anwendungsverantwortlichen teilen die Ausnahme mit den vorstehenden Angaben der oder dem Informationssicherheitsverantwortlichen (I-SIVE) mit. Diese oder dieser teilt die Ausnahme der oder dem Sicherheitsbeauftragten des Kantons (SIBE) mit.

Dokument-Protokoll

Freigabekontrolle

Version	Name	Datum	Bemerkungen
1.0	GL KAIO	16.12.2024	Beschluss mit ICSGW, Version 2.0

Kanton Bern
Canton de Berne

Anhang 6 ICSGW:

Kryptographische Verfahren

Beschlussdatum	16. Dezember 2024
Version	1.0
Dokument-Status	abgenommen
Klassifizierung	Nicht klassifiziert
Autor	Anton Jurt
Dokumentnummer	432567
Geschäftsnummer	2024.KAIO.76

Herausgeber: Amt für Informatik und Organisation des Kantons Bern (KAIO)

Inhaltsverzeichnis

1. Allgemeine Bestimmungen ... 3
Art. 1 Gegenstand ... 3
Art. 2 Begriffe ... 3

2. Schlüsselverwaltung ... 3
Art. 3 Speicherung und Archivierung ... 3
Art. 4 Sitzungsschlüssel (Ephemer-Schlüssel) ... 4
Art. 5 Lebensdauer ... 4
Art. 6 Zufallszahlen ... 4

3. Kryptographische Algorithmen und Schlüssellängen ... 5
Art. 7 Symmetrische Verfahren ... 5
Art. 8 Klassische asymmetrische Verfahren ... 6
Art. 9 Quantensichere, asymmetrische Verfahren ... 6
Art. 10 Hashfunktionen ... 7
Art. 11 Datenauthentisierung ... 7
Art. 12 Quantensichere Signaturverfahren ... 8
Art. 13 Schlüsseltransport und Schlüsseleinigung ... 8

4. Kryptographische Protokolle ... 8
Art. 14 Transport Layer Security (TLS) ... 8
Art. 15 Datagram Transport Layer Security (DTLS) ... 10
Art. 16 Secure Shell (SSH) ... 10
Art. 17 Internet Key Exchange (IKE) und Internet Protocol Security (IPsec) ... 11
Art. 18 Messaging Layer Security (MLS) ... 14

5. Weitere Sicherheitsmassnahmen ... 15
Art. 19 Festplattenverschlüsselung ... 15
Art. 20 Bluetooth ... 15
Art. 21 WLAN ... 15
Art. 22 PKI Zertifikate ... 16

6. Abkürzungsverzeichnis ... 16

7. Schlüsseltypen (Tabelle Art. 5) ... 17

8. Referenzierte Dokumente ... 19

Dokument-Protokoll ... 20

1. Allgemeine Bestimmungen

Art. 1 Gegenstand

[1] Dieser Anhang regelt die einheitliche und sichere Verwendung von kryptografischen Verfahren beim Einsatz von ICT-Mittel.

[2] Dieser Anhang wurde auf Basis der referenzierten Dokumente ([1], [2], [3], [4]) mit dem Bedürfnis nach Konsolidierung und der Möglichkeit zur zeitnahen Anpassung, wie auch Abbildung kantonaler Spezialitäten, erstellt.

Art. 2 Begriffe

1. Cipher Suiten	Definierte Sammlungen kryptographischer Verfahren zur sicheren Kommunikation. Über Cipher Suiten (Chiffrensammlung) wird festgelegt, welche Verschlüsselungsalgorithmen ein Webserver für die Datenübertragung akzeptiert.
2. Datenauthentisierung	Kryptographische Verfahren, welche garantieren, dass versendete oder gespeicherte Daten nicht verändert wurden und tatsächlich vom Urheber stammen.
3. Ephemer-Schlüssel	Bei Ephemer-Schlüssel handelt es sich um ein Schlüsselpaar, welches für jede neue Verbindung erzeugt und verwendet wird.
4. Perfect Forward Secrecy (PFS)	Methode der Schlüsseleinigung kryptografischer Verfahren, die nachträgliche Entschlüsselung durch Bekanntwerden des Hauptschlüssels verhindert.
5. Hashfunktion	Umwandlung einer Zeichenfolge in einen normalerweise kürzeren, numerischen Wert oder Schlüssel mit fester Länge. Der numerische Wert ist der Hashwert und eine andere Darstellung der ursprünglichen Zeichenfolge. Er kann nicht rückwärts aufgelöst werden.
6. Hybridisierung	Einsatz eines quantensicheren Verschlüsselungsverfahrens in Kombination mit einem klassischen Verschlüsselungsverfahren.
7. Secure Shell (SSH)	Kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ungesicherte Netzwerke.
8. Hardware Securtity Module (HSM)	Internes oder externes Peripheriegerät für die sichere Ausführung kryptographischer Operationen oder Applikationen.

2. Schlüsselverwaltung

Art. 3 Speicherung und Archivierung

[1] Schlüssel für die Kryptographie müssen sicher verwaltet werden. Insbesondere sind sie vor Kopieren, missbräuchlicher Nutzung und Manipulation zu schützen.
[2] Eine sichere Schlüsselspeicherung muss durch die Verwendung zertifizierter Hardware (Chipkarte, HSM) gewährleistet sein.
[3] Die öffentlichen Schlüssel müssen vor Veränderungen geschützt gespeichert werden.

Art. 4 Sitzungsschlüssel (Ephemer-Schlüssel)

[1] Alle Ephemer-Schlüssel sind nach ihrer Verwendung unwiderruflich zu löschen.
[2] Es ist sicherzustellen, dass keine Kopien dieser Schlüssel erzeugt werden.
[3] Ephemer-Schlüssel dürfen nur für eine Verbindung benutzt und nicht persistent abgespeichert werden.

Art. 5 Lebensdauer

[1] Die Tabelle definiert die Lebensdauer verschiedener Schlüsseltypen.
[2] Die Lebensdauer darf nicht überschritten werden.

Lebensdauer Schlüssel

Schlüsseltyp (Beschreibun in Kap. 7))		**Lebensdauer**	
		Ausstellernutzungsdauer Originator-Usage Period (OUP)	Empfängernutzungdauer Recipient-Usage Period (RUP)
1.	Privater Signatur-Schlüssel	1 bis 3 Jahre	
2.	Öffentlicher Signatur-Prüfschlüssel	Mehrere Jahre (abhängig von der Schlüsselgrösse)	
3.	Symmetrischer Authentifizierungsschlüssel	≤ 2 Jahre	≤ OUP + 3 Jahre
4.	Privater Authentifizierungsschlüssel	1 bis 2 Jahre	
5.	Öffentlicher Authentifizierungsschlüssel	1 bis 2 Jahre	
6.	Symmetrische Datenverschlüsselungsschlüssel	≤ 2 Jahre	≤ OUP + 3 Jahre
7.	Symmetrischer Key Wrapping Key	≤ 2 Jahre	≤ OUP + 3 Jahre
8.	Symmetrischer Master Key[1]	1 Jahr	-
9.	Privater Schlüsseltransportschlüssel	≤ 2 Jahre[2]	
10.	Öffentlicher Schlüsseltransportschlüssel	1 bis 2 Jahre	
11.	Symmetrischer Schlüsseleinigungsschlüssel	1 bis 2 Jahre[3]	
12.	Private statische Schlüsseleinigungsschlüssel	1 bis 2 Jahre[4]	
13.	Öffentliche statische Schlüsseleinigungsschlüssel	1 bis 2 Jahre	
14.	Privater Ephemer-Schlüsseleinigungsschlüssel	eine Schlüsseleinigungstransaktion	
15.	Öffentlicher Ephemer-Schlüsseleinigungsschlüssel	eine Schlüsseleinigungstransaktion	
16.	Symmetrischer Autorisierungsschlüssel	≤ 2 Jahre	
17.	Privater Autorisierungsschlüssel	≤ 2 Jahre	
18.	Öffentlicher Autorisierungsschlüssel	≤ 2 Jahre	

Art. 6 Zufallszahlen

[1] Für die Erzeugung von Zufallszahlen für kryptographische Schlüssel oder die Signaturerzeugung muss ein überprüfter, hardware-basierter Zufallsgenerator, sog. True-Random-Number-Generator (TRNG), eingesetzt werden.
[2] Weiter sind Zufallszahlengeneratoren aus einer der Klassen DRG.3, DRG.4, PTG.3 oder NTG.1 [9] zur Nutzung erlaubt.

[1] Auch «key-derivation key» genannt.
[2] In E-Mail-Anwendungen, in denen empfangene Nachrichten gespeichert und zu einem späteren Zeitpunkt entschlüsselt werden, kann die Lebensdauer des privaten Schlüssel Transportschlüssels die Lebensdauer des öffentlichen Schlüssel Transportschlüssels überschreiten.
[3] In E-Mail-Anwendungen, in denen empfangene Nachrichten gespeichert und zu einem späteren Zeitpunkt entschlüsselt werden, kann die «Recipient-Usage Period» des Schlüssels die «Originator-Usage Period» überschreiten.
[4] In E-Mail-Anwendungen, bei denen empfangene Nachrichten gespeichert und zu einem späteren Zeitpunkt entschlüsselt werden, kann die Lebensdauer des privaten statischen Schlüsselvereinbarungsschlüssels die Lebensdauer des öffentlichen statischen Schlüsselvereinbarungsschlüssels überschreiten.

3. Kryptographische Algorithmen und Schlüssellängen

Art. 7 Symmetrische Verfahren

[1] Für die symmetrische Verschlüsselung wird der Advanced Encryption Standard (AES) vorgegeben.
[2] Blockchiffren haben die folgenden Anforderungen zu erfüllen:

a *Schlüssellänge*
Wenn möglich 256 Bit, mindestens aber 128 Bit. Die zulässigen Blockchiffren sind in Ziffer 1 der nachfolgenden Tabelle aufgeführt.

b *Betriebsarten*
Die zulässigen Betriebsarten sind in Ziffer 2, Zulässige Betriebsarten, aufgeführt.

c *Betriebsbedingungen*
Für die aufgeführten Betriebsarten sind die Bedingungen in der mittleren Spalte zwingend.

d *Paddingverfahren*
Der Cipher Block Chaining-Modus (CBC-Modus) benötigt einen zusätzlichen Padding-Schritt. Um den letzten Klartextblock auf die Blockgrösse der eingesetzten Chiffre aufzufüllen, sind die Paddingverfahren in Ziffer 3 zulässig.

[3] Stromchiffren dürfen nicht eingesetzt werden. Der AES im Counter-Modus ist davon ausgenommen.

1. Zulässige Blockchiffren

a)	**AES-128**
b)	**AES-192**
c)	**AES-256**

2. Zulässige Betriebsarten

Betriebsarten, die Authenticated Encryption with Associated Data (AEAD) bieten, sind grundsätzlich zu verwenden. Ausnahmen sind zu begründen.

Betriebsart	Bedingungen	AEAD
a) Counter with Cipher Block ChainingMessage Authentication (CCM)	Initialisierungsvektoren dürfen sich innerhalb einer Schlüsselwechselperiode nicht wiederholen.	Ja
b) **Galois/Counter-Mode (GCM)**		Ja
c) **Counter Mode (CTR)**		Nein
d) Counter with Cipher Block ChainingMessage Authentication (CCM)	Die Länge der Authentisierungstags muss mindestens 64 Bit betragen	Ja
e) Cipher-Block Chaining (CBC)	Initialisierungsvektoren müssen unvorhersagbar sein. Ein möglicher Angreifer darf also nicht in der Lage sein, zukünftig eingesetzte Initialisierungsvektoren herauszufinden oder die Wahl des Initialisierungsvektors zu beeinflussen. Für die Erzeugung von unvorhersagbaren Initialisierungsvektoren sind folgende Verfahren zu verwenden: – **Verschlüsselte Initialisierungsvektoren:** Nutzen eines deterministischen Verfahrens zur Erzeugung von Prä-Initialisierungsvektoren (z.B. einem Zähler). Verschlüsselung des Prä-Initialisierungsvektors welcher den einzusetzenden Blockchiffre und den einzusetzenden Schlüssel und den Chiffretext als Initialisierungsvektor nutzt. – **Zufällige Initialisierungsvektoren**: Erzeugen einer zufälligen Bitfolge der Länge n und diese als Initialisierungsvektor nutzen. Die Entropie der zufälligen Bitfolge muss dabei mindestens 95 Bit betragen.	Nein

3. Zulässige Paddingverfahren

a)	**ISO-Padding gemäss ISO/IEC 9797-1:2011**
b)	**Padding gemäss RFC 5652**
c)	**ESP-Padding gemäss RFC 4303**

Art. 8 Klassische asymmetrische Verfahren

[1] Es dürfen ausschliesslich die in der nachfolgenden Tabelle aufgeführten Verfahren für eine asymmetrische Verschlüsselung eingesetzt werden.
[2] Für den RSA-Verschlüsselungsalgorithmus ist das Formatierungsverfahren «EME-OAEP» zwingend.

Zulässige asymmetrische Verfahren

Verfahren	Mindestschlüssellänge [Bit]	Einsatzzweck
a) RSA	3000	Verschlüsselung, Schlüsselaustausch, Digitale Signatur
b) Diffie-Hellman (DH)	3000	Schlüsseleinigung
c) EC Diffie-Hellman (ECDH)	250	Schlüsseleinigung
d) ElGamal	3000	Verschlüsselung, Schlüsseleinigung
e) DSA	3000[5]	Digitale Signatur
f) ECDSA	250	Digitale Signatur
g) DLIES	3000	Hybrides Verschlüsselungsverfahren
h) ECIES	250	Hybrides Verschlüsselungsverfahren

Art. 9 Quantensichere, asymmetrische Verfahren

Es dürfen ausschliesslich die in der nachfolgenden Tabelle aufgeführten Verfahren für eine quantensichere, asymmetrische Verschlüsselung eingesetzt werden.

Zulässige quantensichere Verfahren

a) FrodoKEM-976, FrodoKEM-1344

b) mceliece460896, mceliece6688128, mceliece8192128

c) mceliece460896f, mceliece6688128f, mceliece8192128f

Den quantensicheren Verfahren, die hier aufgeführt sind, wird im Allgemeinen noch nicht das gleiche Vertrauen entgegengebracht, wie den etablierten klassischen Verfahren, da sie beispielsweise in Hinblick auf Seitenkanalresistenz und Implementierungssicherheit nicht gleich gut untersucht sind. Deshalb soll der Einsatz eines quantensicheren nur in Kombination zusammen mit einem klassischen Verfahren erfolgen. Die zulässigen Hybridisierungsverfahren sind:

CatKDF, CasKDF

[5] Wegen geringer Verbreitung und Abkündigung nur noch bis 2029 empfohlen.

Art. 10 Hashfunktionen

[1] Es dürfen nur die in Ziffer 1 aufgeführten, kryptographisch starken Hashfunktionen eingesetzt werden.
[2] Um aus einem Passwort einen kryptographischen Schlüssel zur Verschlüsselung zu erzeugen, oder um ein Passwort zu speichern, sind nur die Passwort-Hashfunktionen in Ziffer 2 zugelassen.
[3] Der Einsatz von SHA1 ist nicht erlaubt.

1. Zulässige Hashfunktionen

In der ersten Zeile der Tabelle handelt es sich um SHA2 (die Nummer wird bei der Version 2 nicht ausgeschrieben).

a)	SHA-256, SHA-512/256, SHA-384 und SHA-512
b)	SHA3-256, SHA3-384, SHA3-512

2. Zulässige Passwort-Hashfunktionen

a)	Argon2
b)	bcrypt
c)	scrypt
d)	PBKDF2

Art. 11 Datenauthentisierung

[1] Anforderungen an das MAC-Verfahren:
a Die in Ziffer 1 aufgeführten MAC-Verfahren dürfen unter Berücksichtigung der minimalen Schlüssel- und Taglängen eingesetzt werden.
b Der Schlüssel für den MAC darf nicht derselbe sein wie für die Chiffrierung.
[2] Anforderungen an digitale Signaturen:
Die in Ziffer 2 aufgeführten Signaturverfahren mit den entsprechenden Schlüssellängen sind zulässig.

1. Zulässige MAC-Verfahren

Verfahren	**Mindestschlüssellänge [Bit]**	**Mindesttaglänge [Bit]**
a) CMAC	256	96
b) HMAC	256	128
c) KMAC256	256	96
d) GMAC	256	96

2. Zulässige Signaturverfahren

Verfahren	**Mindestschlüssellänge [Bit]**
a) RSA	3000
b) DSA	3000[6]
c) ECDSA	250

[6] Wegen geringer Verbreitung und Abkündigung nur noch bis 2029 empfohlen.

Art. 12 Quantensichere Signaturverfahren

[1] Der Einsatz quantensicherer Signaturverfahren muss grundsätzlich in Kombination mit klassischen Signaturverfahren erfolgen. Diese Hybridisierung soll der noch nicht gleich fortgeschrittenen Erforschung der Implementierungssicherheit entgegen wirken.

Art. 13 Schlüsseltransport und Schlüsseleinigung

[1] Perfect Forward Secrecy (PFS):
Nur mit asymmetrischen Schlüsseleinigungsverfahren ist die Sicherheitseigenschaft Perfect Forward Secrecy erreichbar. Zur Verhinderung von Man-in-the-Middle-Attacken muss der Schlüsselaustausch authentisiert ablaufen, z.B. per Signierung (Art.11, Ziffer 2).

[2] Symmetrische Verfahren:
Zum Transport von Sitzungsschlüssel sind alle im Art. 7 aufgeführten symmetrischen Verschlüsselungsverfahren zulässig. Die Kombination mit einem, im Art. 12, Tabelle Ziff. 1, aufgeführten MAC-Verfahren ist zwingend notwendig. Die Schlüsseleinigungsverfahren in Ziffer 1 sind zulässig.

[3] Asymmetrische Verfahren:
Zum Transport neuer Sitzungsschlüssel sind ausschliesslich die in Art. 8 aufgeführten klassischen asymmetrischen Verschlüsselungsverfahren zulässig. Für die Schlüsseleinigung müssen die in Ziffer 2 aufgeführten Verfahren eingesetzt werden.

1. Zulässige Schlüsseleinigungsverfahren (Symmetrische Verfahren)

Key Establishment Mechanism 5 gemäss ISO/IEC 11770-2:2018

2. Zulässige Schlüsseleinigungsverfahren (Asymmetrische Verfahren)

a) Elliptic Curve Key Agreement of ElGamal Type (ECKA-EG)

b) Instanzauthentisierung mit RSA und Schlüsselvereinbarung mit RSA

c) MTI/A0 (Two-pass Diffie-Hellman)

4. Kryptographische Protokolle

Art. 14 Transport Layer Security (TLS)

[1] Es sind die in Ziffer 1 aufgeführten TLS-Versionen als Mindeststandard zu verwenden. Stärkere Protokollversionen sind zu bevorzugen. Schwächere Protokollversionen von TLS oder Versionen des SSL Protokolls dürfen nicht verwendet werden, auch nicht als Fallback.

[2] Verwendung von Cipher Suiten:
a *TLS 1.2:* Die in Ziffer 2 aufgeführten Cipher-Suiten für die Protokollversion 1.2 sind zugelassen. Wenn immer möglich sollten Cipher-Suiten mit Perfect Forward Secrecy eingesetzt werden.

b *TLS 1.3:* Die in Ziffer 3 aufgeführten Cipher-Suiten für die Protokollversion 1.3 sind zugelassen.

[3] Die Mindestschlüssellänge für TLS müssen den Vorgaben gemäss Kapitel 3 «Kryptographische Algorithmen und Schlüssellängen» entsprechen.

1. Zulässige TLS-Versionen

a) TLS 1.2

b) TLS 1.3

2. Zulässige Cipher-Suiten TLS 1.2

Eigenschaft	Zulässige Cipher-Suiten TLS 1.2
a) Cipher-Suiten mit Perfect Forward Secrecy	– TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 – TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 – TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_ECDSA_WITH_AES_128_CCM – TLS_ECDHE_ECDSA_WITH_AES_256_CCM – TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 – TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 – TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 – TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 – TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 – TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
b) Cipher-Suiten ohne Perfect Forward Secrecy (Verwendung bis 2026)	– TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 – TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 – TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 – TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 – TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 – TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 – TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 – TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 – TLS_DH_DSS_WITH_AES_128_CBC_SHA256 – TLS_DH_DSS_WITH_AES_256_CBC_SHA256 – TLS_DH_DSS_WITH_AES_128_GCM_SHA256 – TLS_DH_DSS_WITH_AES_256_GCM_SHA384 – TLS_DH_RSA_WITH_AES_128_CBC_SHA256 – TLS_DH_RSA_WITH_AES_256_CBC_SHA256 – TLS_DH_RSA_WITH_AES_128_GCM_SHA256 – TLS_DH_RSA_WITH_AES_256_GCM_SHA384
c) Cipher-Suiten für die Schlüsseleinigung mit vorab ausgetauschten Daten (Pre-Shared Key)	– TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 – TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384 – TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256 – TLS_DHE_PSK_WITH_AES_128_CBC_SHA256 – TLS_DHE_PSK_WITH_AES_256_CBC_SHA384 – TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 – TLS_DHE_PSK_WITH_AES_256_GCM_SHA384 – TLS_DHE_PSK_WITH_AES_128_CCM – TLS_DHE_PSK_WITH_AES_256_CCM

3. Zulässige Cipher-Suiten TLS 1.3

a) TLS_AES_128_GCM_SHA256

b) TLS_AES_256_GCM_SHA384

c) TLS_AES_128_CCM_SHA256

Art. 15 Datagram Transport Layer Security (DTLS)

[1] Da DTLS auf TLS basiert, gelten die Vorgaben gemäss Art. 14. Beim Einsatz von DTLS muss vorgängig abgeklärt werden, welche der vorgegebenen Cipher Suiten mit DTLS kompatibel sind. Die in der Tabelle aufgeführten DTLS-Versionen sind zulässig.

1. Zulässige DTLS-Version
TLS 1.2

Art. 16 Secure Shell (SSH)

[1]Ausschliesslich die in Ziffer 1 aufgeführten SSH-Versionen sind zulässig.

[2] Ausschliesslich die in Ziffer 2 aufgeführten Methoden für den Schlüsselaustausch (Key Exchange) sind zulässig.

[3] Es dürfen die in Ziffer 3 aufgeführten Verschlüsselungsalgorithmen eingesetzt werden.

[4] Wird ein Cipher nicht im GCM-Modus betrieben, muss die Integrität zusätzlich durch die Verwendung eines MAC-Verfahrens sichergestellt werden. Ausschliesslich die in Ziffer 4 aufgeführten Verfahren dürfen eingesetzt werden.

[5] Zulässige Authentisierungen:

a *Server-Authentisierung*
Ausschliesslich die in Ziffer 5 aufgeführten Verfahren sind für die Server-Authentisierung zugelassen.

b *Client-Authentisierung*
Wenn clientseitig Schlüssel zur Authentifizierung eingesetzt werden (Public Key Authentication) müssen die in Ziffer 6 aufgeführten Schlüsseltypen verwendet werden. Die Minimalschlüssellänge für den RSA-Verschlüsselungsalgorithmus ist in Art. 8 definiert.

1. Zulässige SSH-Versionen
SSH-2

2. Zulässige Key-Exchange-Methoden
a) diffie-hellman-group-exchange-sha256
b) diffie-hellman-group15-sha512
c) diffie-hellman-group16-sha512
d) ecdh-sha2-nistp256
e) ecdh-sha2-nistp384
f) ecdh-sha2-nistp521

3. Zulässige SSH-Ciphers

a) AEAD_AES_128_GCM

b) AEAD_AES_256_GCM

c) aes128-ctr

d) aes192-ctr

e) aes256-ctr

4. Zulässige Verfahren zur MAC-Sicherung

a) hmac-sha2-256

b) hmac-sha2-512

5. Zulässige Verfahren für die Server-Authentisierung

Verfahren	Mindestschlüssellänge [Bit]
a) ecdsa-sha2-nistp384	250
b) ecdsa-sha2-nistp521	250
c) x509v3-ecdsa-sha2-nistp256	250
d) x509v3-ecdsa-sha2-nistp384	250
e) x509v3-ecdsa-sha2-nistp521	250

6. Vorgeschriebene Schlüsseltypen

a) RSA

b) Ed25519

Art. 17 Internet Key Exchange (IKE) und Internet Protocol Security (IPsec)

[1] Anforderungen an den IKE

a *Versionen*
Ausschliesslich die in Ziffer 1 aufgeführten IKE-Versionen sind zulässig. Für die gegenseitige Authentisierung ist die Verwendung von Zertifikaten vorgeschrieben. Werden Pre-Shared Keys (PSK) eingesetzt, müssen sie Buchstaben, Zahlen und Sonderzeichen enthalten und mindestens 20 Zeichen lang sein.

b *Verschlüsselungsverfahren*
Die Verschlüsselung der im IKE_AUTH-, CREATE_CHILD_SA- sowie INFORMATIONAL-Exchange ausgetauschten Nachrichten muss nach einem der in Ziffer 2 aufgeführten Verfahren erfolgen.

c *Integritätsschutzverfahren*
Für den Schutz der Integrität, der im IKE_AUTH-, CREATE_CHILD_SA- sowie INFORMATIONAL-Exchange ausgetauschten Nachrichten, sind ausschliesslich die in Ziffer 3 aufgeführten Verfahren zulässig.

d *Schlüsselerzeugung*
Die Erzeugung von Schlüsselmaterial muss nach einem in Ziffer 4 aufgeführten Verfahren erfolgen.

e *Schlüsselaustausch*
Ausschliesslich die in Ziffer 5 aufgeführten Diffie-Hellman-Gruppen sind für den Schlüsselaustausch zulässig.

f *Authentisierungsverfahren (Peer Authentication)*
Für die Authentisierung muss eines der in Ziffer 6 aufgeführten Verfahren eingesetzt werden.

[2] Anforderungen an die IPsec

a *Protokolle*
Die Verwendung des AH Protokolls ist nicht zulässig. Es ist Pflicht, die Nullverschlüsselung mit dem ESP Protokoll in Ziffer 7 anstelle des AH-Protokolls zu verwenden, wenn keine Verschlüsselung erwünscht ist.

b *ESP Paketverschlüsselung*
Für die Verschlüsselung der ESP-Pakete sind ausschliesslich die in Ziffer 8 aufgeführten Verfahren zulässig.

c *ESP Integritätsschutz*
Die Integrität von ESP-Paketen muss mit einem in Ziffer 9 aufgeführten Verfahren sichergestellt werden.

[3] Security Association Lifetime und Re-Keying
Die Lebensdauer einer Security Association (SA)[7] muss in Abhängigkeit der Sicherheitsanforderung der Anwendung festgelegt werden. In gewöhnlichen Einsatzszenarien darf die IKE-SA-Lifetime maximal 24 Stunden und die IPsec-SA-Lifetime maximal 4 Stunden betragen.

1. Zulässige IKE-Versionen für den Schlüsselaustausch

IKEv2

2. Zulässige Verschlüsselungsverfahren IKEv2

Die Verfahren ENCR_AES_CBC und ENCR_AES_CTR bieten keinen Schutz der Integrität. Sie müssen daher zwingend mit einem solchen kombiniert werden (gemäss Ziffer 3).

Verfahren	AES-Mindestschlüssellänge [Bit]
a) ENCR_AES_CBC	256
b) ENCR_AES_CTR	256
c) ENCR_AES_GCM_16	256
d) ENCR_AES_GCM_12	256
e) ENCR_AES_CCM_16	256
f) ENCR_AES_CCM_12	256

[7] IPsec gesicherte Verbindung zwischen zwei Kommunikationspartnern inkl. der zugehörigen kryptographischen Parameter, Algorithmen, Schlüssel und Betriebsmodi für diese Verbindung.

3. Zulässige Integritätsschutzverfahren

a) AUTH_AES_XCBC_96

b) AUTH_HMAC_SHA2_256_128

c) AUTH_HMAC_SHA2_384_192

d) AUTH_HMAC_SHA2_512_256

4. Vorgeschriebene Verfahren zur Schlüsselerzeugung

a) PRF_AES128_XCBC

b) PRF_AES128_CMAC

c) PRF_HMAC_SHA2_256

d) PRF_HMAC_SHA2_384

e) PRF_HMAC_SHA2_512

5. Zulässige Diffie-Hellman-Gruppen für den Schlüsselaustausch

Perfect Forward Secrecy soll, falls möglich, immer umgesetzt werden. Für die Umsetzung muss im CREATE_CHILD_SA Austausch ein erneuter Diffie-Hellman-Schlüsselaustausch unter Verwendung der zulässigen Diffie-Hellman Gruppen durchgeführt werden.

ID	Gruppen
15	3072-bit MODP Group
16	4096-bit MODP Group
19	256-bit random ECP group
20	384-bit random ECP group
21	521-bit random ECP group
28	brainpoolP256r1
29	brainpoolP384r1
30	brainpoolP512r1

6. Zulässige Authentisierungsverfahren

Verfahren	Länge [Bit]	Hash-Funktion
a) ECDSA-256 mit Kurve secp256r1	256	SHA-256
b) ECDSA-384 mit Kurve secp384r1	384	SHA-384
c) ECDSA-512 mit Kurve secp521r1	512	SHA-512
d) ECDSA-256 mit Kurve brainpoolP256r1	256	SHA-256
e) ECDSA-384 mit Kurve brainpoolP384r1	384	SHA-384
f) ECDSA-512 mit Kurve brainpoolP512r1	512	SHA-512

g)	RSASSA-PSS	4096	SHA-384
h)	ECGDSA-256 mit Kurve brainpoolP256r1	256	SHA-256
i)	ECGDSA-384 mit Kurve brainpoolP384r1	384	SHA-384
j)	ECGDSA-512 mit Kurve brainpoolP512r1	512	SHA-512

7. Zulässige IPsec-Protokolle

Encapsulated Security Payload (ESP)

8. Zulässige ESP-Paketverschlüsselung

Bei der Verwendung von ESP muss der Tunnelmodus gegenüber dem Transportmodus bevorzugt werden.

Verfahren	AES-Mindestschlüssellänge [Bit]
a) ENCR_AES_CBC	256
b) ENCR_AES_CTR	256
c) ENCR_AES_GCM_16	256
d) ENCR_AES_GCM_12	256
e) ENCR_AES_CCM_16	256
f) ENCR_AES_CCM_12	256

9. Zulässige ESP-Integritätsschutzverfahren

a) AUTH_AES_XCBC_96

b) AUTH_AES_CMAC_96

c) AUTH_HMAC_SHA2_256_128

d) AUTH_HMAC_SHA2_384_192

e) AUTH_HMAC_SHA2_512_256

Art. 18 Messaging Layer Security (MLS)

MLS 1.0 ist zulässig.

Zulässige MLS-Cipher Suiten
a) MLS_128_DHKEMP256_AES128GCM_SHA256_P256
b) MLS_256_DHKEMP384_AES256GCM_SHA384_P384
c) MLS_256_DHKEMP521_AES256GCM_SHA512_P521

5. Weitere Sicherheitsmassnahmen

Art. 19 Festplattenverschlüsselung

Ist es bei Festplatten aus Effizienz- und/oder Platzgründen nicht möglich, eine Chiffrierung mit Authentisierung (siehe Art. 7 Lemma [2]) einzusetzen, muss XTS-AES verwendet werden.

Art. 20 Bluetooth

[1] Bei der Verwendung von Bluetooth muss mindestens die Version 4.2 mit einem aktuellen Patch Level eingesetzt werden.

[2] Im Fall von Bluetooth BR/EDR/HS muss mindestens der Security Mode 4, Level 3 (Secure Simple Pairing) und im Fall von Bluetooth LE der Security Mode 1 Level 4 eingesetzt werden.

[3] Auf die Verwendung der Methode „Just Works“ für das Pairing soll wenn immer möglich verzichtet werden.

Art. 21 WLAN

In der nachfolgenden Tabelle sind die zulässigen kryptografischen Verfahren zu WLAN beschrieben.

Kryptografische Verfahren WLAN

WLAN Modus	Bereich	Zulässige Verfahren
a) WPA3-Enterprise	Authentication	Mehrere EAP
	Encryption	AES-CCMP 128
	Key derivation & confirmation	HMAC-SHA256
	Frame protection	BIP-CMAC-128
b) WPA3-Enterprise mit 192-Bit-Modus (für den Schutz sensibler Daten)	Authentication	EAP TLS_ECDHE_EC-DSA_WITH_AES_256_GCM_SHA384
	Encryption	GCMP-256
	Key derivation & confirmation	HMAC-SHA384
	Frame protection	BIP-GMAC-256

c) WPA2-Enterprise	Falls Geräte oder Komponenten kein WPA3 unterstützen, kann auf den Mixed Mode mit WPA2-Enterprise zurückgegriffen werden.

Art. 22 PKI Zertifikate

[1] Folgende E-Government Standards sind einzuhalten:
a) eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten [5]
b) eCH-0048 PKI-Zertifikatsklassen [6]

[2] Geltende CP/CPS der CA des Kantons Bern:
a) CPCPS_Root-CA_BECH [7]
b) CP CPS Sicherheits- und Zertifizierungsrichtlinien CERT-001-BE-CH [8]

6. Abkürzungsverzeichnis

Abkürzung	Bedeutung
AEAD	Authenticated encryption with associated data
AH	Authentication Header
CCM	Counter with Cipher Block Chaining Message Authentication
CBC	Cipher-Block Chaining
CTR	Counter Mode
DH	Diffie-Hellman
DLIES	Discrete Logarithm Integrated Encryption Scheme
DRG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ESP	Encapsulated Security Payload
GCM	Galois/Counter Mode
HSM	Hardware Security Module
ICSG	Informations- und Cybersicherheitsgesetz des Kantons Bern
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
MAC	Message Authentication Code
NTG	Non-physical Random Number Generator
HMAC	Keyed-Hash Message Authentication Code
PFS	Perfect Forward Secrecy
PTG	Physical Random Number Generator
RNG	Random Number Generator
RSA	Rivest–Shamir–Adleman
SA	Security Association

SSL	Secure Socket Layer
SSH	Secure Shell Protocol
SHA	Secure Hash Algorithms
TLS	Transport Layer Security
TRNG	True Random Number Generator

7. Schlüsseltypen (Tabelle Art. 5)

Schlüsseltyp	Beschreibung
a) Privater Signatur-Schlüssel	Private Signatur-Schlüssel sind die privaten Schlüssel von asymmetrischen Schlüsselpaaren, die von Algorithmen für öffentliche Schlüssel verwendet werden, um digitale Signaturen zu erzeugen, welche für eine langfristige Verwendung bestimmt sind. Bei ordnungsgemässer Handhabung können private Signatur-Schlüssel zur Sicherstellung der Authentifizierung und Integrität, sowie der Nicht-Abstreitbarkeit von Nachrichten, Dokumenten oder gespeicherten Daten verwendet werden.
b) Öffentlicher Signatur-Prüfschlüssel	Ein öffentlicher Signaturprüfschlüssel ist der öffentliche Schlüssel eines asymmetrischen Schlüsselpaares, der von einem Algorithmus für öffentliche Schlüssel zur Überprüfung digitaler Signaturen verwendet wird, um die Identität eines Benutzers und/oder die Integrität der Daten zu verifizieren, sowie die Nicht-Abstreitbarkeit von Nachrichten, Dokumenten oder gespeicherten Daten sicherzustellen.
c) Symmetrischer Authentifizierungsschlüssel	Symmetrische Authentifizierungsschlüssel werden mit symmetrischen Schlüsselalgorithmen zur Identitäts- und Integritätsprüfung von Kommunikationssitzungen, Nachrichten, Dokumenten oder gespeicherten Daten verwendet. Zu beachten ist, dass bei Authentifizierungs-Verschlüsselungsmodi für einen symmetrischen Schlüsselalgorithmus ein einziger Schlüssel sowohl für die Authentifizierung als auch für die Verschlüsselung verwendet wird.
d) Privater Authentifizierungsschlüssel	Ein privater Authentifizierungsschlüssel ist der private Schlüssel eines asymmetrischen Schlüsselpaares, der mit einem Algorithmus für öffentliche Schlüssel verwendet wird, um die Identität einer Entität beim Aufbau einer authentifizierten Kommunikationssitzung oder der Autorisierung zur Durchführung einer Aktion zu gewährleisten.
e) Öffentlicher Authentifizierungsschlüssel	Ein öffentlicher Authentifizierungsschlüssel ist der öffentliche Schlüssel eines asymmetrischen Schlüsselpaares, der zusammen mit einem Algorithmus für öffentliche Schlüssel verwendet wird, um die Identität einer Entität sicherzustellen, wenn eine authentifizierte Kommunikationssitzung oder eine Autorisierung zur Durchführung einer Aktion aufgebaut wird.
f) Symmetrische Datenverschlüsselungsschlüssel	Diese Schlüssel werden mit symmetrischen Schlüsselalgorithmen verwendet, um die Vertraulichkeit von Daten zu schützen (d.h. Klartextdaten zu verschlüsseln). Derselbe Schlüssel wird auch zur Aufhebung des Vertraulichkeitsschutzes (d.h. zur Entschlüsselung der Daten) verwendet. Zu beachten ist, dass bei authentifizierten Verschlüsselungsmodi für einen symmetrischen Schlüsselalgorithmus ein einziger Schlüssel sowohl für die Quellenauthentifizierung als auch für die Verschlüsselung verwendet wird.
g) Symmetrischer Key Wrapping Key	Symmetrische Key Wrapping Keys (auch Schlüsselumhüllungsschlüssel genannt) werden mit symmetrischen Schlüsselalgorithmen verwendet, um andere Schlüssel zu verschlüsseln. Der Key Wrapping Key, der zur Verschlüsselung eines Schlüssels verwendet wird, wird auch zur Umkehrung des Verschlüsselungsvorgangs verwendet (d.h. zur Entschlüsselung des verschlüsselten Schlüssels).
h) Symmetrischer Master Key	Ein symmetrischer Master Key (Hauptschlüssel) wird zur Ableitung anderer symmetrischer Schlüssel (z.B. Datenverschlüsselungsschlüssel oder Key Wrapping Keys) unter Verwendung symmetrischer kryptografischer Verfahren verwendet.

i)	Privater Schlüsseltransportschlüssel	Private Schlüsseltransportschlüssel sind die privaten Schlüssel von Schlüsselpaaren mit asymmetrischen Schlüsseln, die zur Entschlüsselung von Schlüsseln verwendet werden, die mit dem entsprechenden öffentlichen Schlüssel verschlüsselt wurden. Schlüsseltransportschlüssel werden in der Regel verwendet, um symmetrische Schlüssel (z.B. Key Wrapping Keys, Datenverschlüsselungsschlüssel oder MAC-Schlüssel) und gegebenenfalls anderes Schlüsselmaterial (z.B. Initialisierungsvektoren) zu erstellen.
j)	Öffentlicher Schlüsseltransportschlüssel	Öffentliche Schlüsseltransportschlüssel sind die öffentlichen Schlüssel von Schlüsselpaaren mit asymmetrischen Schlüsseln, die zur Verschlüsselung von Schlüsseln verwendet werden. Diese Schlüssel werden verwendet, um symmetrische Schlüssel (z.B. Key Wrapping Keys, Datenverschlüsselungsschlüssel oder MAC-Schlüssel) und gegebenenfalls anderes Schlüsselmaterial (z.B. Initialisierungsvektoren) zu erstellen.
k)	Symmetrischer Schlüsseleinigungsschlüssel	Diese symmetrischen Schlüssel werden verwendet, um symmetrische Schlüssel (z.B. Key Wrapping Keys, Datenverschlüsselungsschlüssel oder MAC-Schlüssel) und optional anderes Schlüsselmaterial (z.B. Initialisierungsvektoren) unter Verwendung eines symmetrischen Schlüsselübereinstimmungsalgorithmus zu erstellen.
l)	Private statische Schlüsseleinigungsschlüssel	Private statische Schlüsseleinigungsschlüssel sind die langfristigen privaten Schlüssel von Schlüsselpaaren mit asymmetrischen Schlüsseln, die zur Erstellung symmetrischer Schlüssel (z.B. Key Wrapping Keys, Datenverschlüsselungsschlüssel oder MAC-Schlüssel) und gegebenenfalls anderen Schlüsselmaterials (z.B. Initialisierungsvektoren) verwendet werden.
m)	Öffentliche statische Schlüsseleinigungsschlüssel	Öffentliche statische Schlüsseleinigungsschlüssel sind die langfristigen öffentlichen Schlüssel von Schlüsselpaaren mit asymmetrischen Schlüsseln, die zur Erstellung symmetrischer Schlüssel (z.B. Key Wrapping Keys, Datenverschlüsselungsschlüssel oder MAC-Schlüssel) und gegebenenfalls anderem Schlüsselmaterial (z.B. Initialisierungsvektoren) verwendet werden.
n)	Privater Ephemer-Schlüsseleinigungsschlüssel	Private ephemere Schlüssel (Sitzungsschlüssel) sind die kurzzeitigen privaten Schlüssel von Schlüsselpaaren mit asymmetrischen Schlüsseln, die nur einmal verwendet werden, um einen oder mehrere symmetrische Schlüssel (z.B. Key Wrapping Keys, Datenverschlüsselungsschlüssel oder MAC-Schlüssel) und gegebenenfalls anderes Schlüsselmaterial (z.B. Initialisierungsvektoren) zu erstellen.
o)	Öffentlicher Ephemer-Schlüsseleinigungsschlüssel	Öffentliche ephemere Schlüssel (Sitzungsschlüssel) sind die kurzfristigen öffentlichen Schlüssel asymmetrischer Schlüsselpaare, die in einer einzigen Schlüsseltransaktion verwendet werden, um einen oder mehrere symmetrische Schlüssel (z.B. Key Wrapping Keys, Datenverschlüsselungsschlüssel oder MAC-Schlüssel) und gegebenenfalls anderes Schlüsselmaterial (z.B. Initialisierungsvektoren) zu erstellen.
p)	Symmetrischer Autorisierungsschlüssel	Symmetrische Autorisierungsschlüssel werden verwendet, um einer Entität mithilfe einer symmetrischen kryptografischen Methode Berechtigungen zu gewähren. Der Autorisierungsschlüssel ist der Entität bekannt, die für die Überwachung und Gewährung von Zugriffsrechten für autorisierte Entitäten verantwortlich ist, sowie der Entität, die Zugang zu Ressourcen wünscht.
q)	Privater Autorisierungsschlüssel	Ein privater Autorisierungsschlüssel ist der private Schlüssel eines asymmetrischen Schlüsselpaares, der dazu dient, das Recht des Eigentümers auf Berechtigungen zu beweisen.
r)	Öffentlicher Autorisierungsschlüssel	Ein öffentlicher Autorisierungsschlüssel ist der öffentliche Schlüssel eines asymmetrischen Schlüsselpaares, der zur Überprüfung von Berechtigungen für eine Entität verwendet wird, die den zugehörigen privaten Autorisierungsschlüssel kennt.

8. Referenzierte Dokumente

Referenz	Dokumente	Ablage
[1]	BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen" Version: 2024-01	
[2]	BSI TR-02102-2 "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)" Version: 2024-1	
[3]	BSI TR-02102-3 "Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)" Version: 2024-01	
[4]	BSI TR-02102-4 "Kryptographische Verfahren: Teil 4 – Verwendung von Secure Shell (SSH)" Version: 2024-01	
[5]	eCH-0170 "Qualitätsmodell zur Authentifizierung von Subjekten" Version 2.0	
[6]	eCH-0048 "PKI-Zertifikatsklassen" Version 2.0	
[7]	CPCPS_Root-CA_BECH	(KAIO) #166147
[8]	CP CPS Sicherheits- und Zertifizierungsrichtlinien CERT-001-BE-CH	(KAIO) #188753
[9]	BSI: Functionality classes for random number generators	

Dokument-Protokoll

Freigabekontrolle

Version	Name	Datum	Bemerkungen
1.0	GL KAIO	16.12.2024	Beschluss mit ICSGW, Version 2.0