

	Richtlinie der Freien und Hansestadt Hamburg zur Authentisierung von Personen und technischen Entitäten (Authentisierungsrichtlinie - RAuPE)	Version 1.1 Stand: 29.08.2024
---	---	--

Inhaltsverzeichnis

1.	Zielsetzung	2
2.	Gegenstand und Geltungsbereich.....	2
3.	Regelungen	2
3.1	Identitätsprüfung	2
3.2	Faktoren der Authentisierung.....	2
3.3	Authentisierung.....	3
3.4	Umgang mit Konten	3
3.5	Nutzung von Passwörtern	4
3.6	Nutzung von Token und Hardware-Authentisierungsmittel.....	6
3.7	Nutzung der Biometrie	6
3.8	Nutzung von digitalen Zertifikaten	6
3.9	Ausnahmen	6
4.	Mitgeltende Vorschriften	7
5.	Kontrolle der Richtlinie	7
6.	Inkrafttreten und Geltungsdauer.....	7
	Anlage 1 – Begriffsdefinitionen.....	8

1. Zielsetzung

- (1) Ziel der Richtlinie ist es, durch die Verwendung von Passwörtern und weiteren Authentisierungsformen bei konsequenter und adäquater Nutzung einen unbefugten Zugang zu den [IT-Systemen](#) zu verhindern und die Sicherheit zu gewährleisten.
- (2) Die nachfolgenden Regelungen orientieren sich an den Anforderungen des Identitätsmanagements nach IT-Grundschutz des BSI-Standards des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung.

2. Gegenstand und Geltungsbereich

- (1) Diese Richtlinie definiert mittels Vorgaben einen Mindeststandard für die Authentisierung von Personen und technischen Entitäten als Voraussetzung für den Zugang zu IT-Systemen der Freien und Hansestadt Hamburg, sowie Vorgaben für die Handhabung und Gestaltung von Passwörtern, Token oder biometrischen Verfahren, die zum Nachweis der Identität von berechtigten Nutzern eingesetzt werden.
- (2) Technische Details dieser Richtlinie werden von dem IT-Architekturboard beschlossen.
- (3) Diese Richtlinie gilt für alle Dienststellen, Landesbetriebe und Einrichtungen der Freien und Hansestadt Hamburg, für die der Senat oberste Dienstbehörde ist und für die Organisationseinheiten, die die IT-Infrastruktur der FHH nutzen.
- (4) Soweit andere Regelwerke strengere Vorschriften zur Passwortsicherheit beinhalten, so gelten diese zusätzlich.

3. Regelungen

3.1 Identitätsprüfung

- (1) Vor Einrichtung von Nutzerberechtigungen hat der Verantwortliche nachweisbar sicherzustellen, dass die tatsächliche Identität der Nutzenden initial mit geeigneten Methoden nachgewiesen wurde.

3.2 Faktoren der Authentisierung

- (1) Für den Identitätsnachweis an einem IT-System ([Authentisierung](#)) können drei Faktoren genutzt werden:
 1. Wissen (z.B. Passwort oder PIN)
 2. Besitz (z.B. Chipkarte)
 3. Biometrische Merkmale (z.B. Fingerabdrücke, Gesichtsgeometrie, Stimmfarbe)
- (2) Für eine [Multifaktor-Authentisierung \(MFA\)](#) müssen mindestens zwei der oben genannten Faktoren kumulativ verwendet werden.

3.3 Authentisierung

- (1) Für den Zugang zu IT-Systemen der FHH ist mindestens eine [Ein-Faktor-Authentisierung](#) zu verwenden.
- (2) Bei Benutzerkennungen mit besonderen Rechten und Aufgaben (z.B. Systemverwaltung, Sicherheitsfunktionen oder Anwendungen mit sensiblen Daten) ist die Verwendung eines weiteren Faktors (MFA) angezeigt¹.
- (3) Die Faktoren Besitz und Biometrie müssen durch einen weiteren Faktor abgesichert werden. Die Faktoren Besitz und Biometrie müssen jedoch nicht zwingend zusammenhängend zur Authentisierung verwendet werden.
- (4) Die Mechanismenstärke der Authentisierung mittels Art und Anzahl der zu nutzenden Authentisierungsfaktoren ist durch die jeweils fachlich verantwortliche Stelle, insbesondere bei Schutzbedarf „hoch“ und „sehr hoch“, festzulegen.
- (5) Die Authentisierungsverfahren können je nach genutzter Umgebung variieren und sind einzeln freizugeben.

3.4 Umgang mit Konten

- (1) Es werden personalisierte Benutzerkonten und Dienstkonten zur Regelung der Zugangsberechtigung zu einem IT-System eingesetzt.

3.4.1 Personalisierte Benutzerkonten

- (1) Personalisierte Benutzerkonten müssen jeweils über einen eindeutigen Namen einer natürlichen Person zugeordnet sein und dürfen nur von dieser zugeordneten Person für die Authentisierung genutzt werden.
- (2) Eine Kontosperrung durch mehrere fehlgeschlagene Anmeldeversuche kann dazu führen, dass ohne den Zugang zu den IT-Systemen eine Administration (z.B. der [ADs](#) oder anderer [TDC-Dienste](#)) be- oder verhindert werden kann. Es ist zulässig, entsprechende Konten nach Ablauf einer durch das ITAB festgelegten Frist automatisiert zu entsperren. Voraussetzung dafür ist, dass Konten auf missbräuchliche Sperrung überwacht und im Rahmen geordneter Prozesse auf entsprechende Alarme reagiert wird.

3.4.2 Dienstkonten

- (1) Dienstkonten dürfen nur aus zwingenden technischen Gründen eingerichtet werden, wenn die Funktionalität des IT-Systems mit anderen Mitteln in wirtschaftlich vertretbarem Umfang nicht herstellbar ist.
- (2) Dienstkonten dürfen nicht von Personen benutzt werden.

¹ Eine Entscheidungshilfe als „Varianten der sicheren Authentisierung / Vor- und Nachteile“ wird in der [Sicherheitspyramide des InSiMa](#) bereitgestellt.

- (3) Sie dürfen nur in automatisierter Weise von einer Anwendung aktiviert werden.
- (4) Jedes Dienstkonto muss durch einen verantwortlichen Mitarbeitenden oder Vertretenden verwaltet werden.
- (5) Aus dem Gesamtzusammenhang der Protokollierung auf allen Ebenen (Anwendungs-, Middleware- und Systemprotokollierung) muss die vom Dienstkonto ausgeführte Datenverarbeitung feststellbar sein.

3.5 Nutzung von Passwörtern

3.5.1 Allgemeine Vorgaben

- (1) Die nachfolgenden Regeln für Passwörter beziehen sich auf die Absicherung des Zugangs zu IT-Systemen, die Daten bis einschließlich Schutzbedarf „normal“ speichern und verarbeiten.
- (2) Für IT-Systeme mit Schutzbedarf „hoch“ ist grundsätzlich die Verwendung eines weiteren Faktors angezeigt. Die Entscheidung liegt bei der fachlich verantwortlichen Stelle.
- (3) Für IT-Systeme mit Schutzbedarf „sehr hoch“ ist grundsätzlich die Verwendung einer MFA angezeigt. Die Entscheidung liegt bei der fachlich verantwortlichen Stelle.
- (4) Benutzerkennungen mit besonderen Rechten und Aufgaben sollen mit einer MFA, z. B. mit kryptografischen Zertifikaten, Chipkarten oder Token, geschützt werden.
- (5) Wenn ein Passwortwechsel notwendig ist, dürfen die letzten 6 Passwörter vor dem aktuellen Wechsel nicht erneut verwendet werden.
- (6) Pro IT-System muss ein Passwort verwendet werden, es dürfen keine unterschiedlichen Anmeldungen mit dem gleichen Passwort getätigt werden können.²
- (7) Nach Überschreitung von 5 erfolglosen Authentisierungsversuchen sperrt das IT-System bzw. die IT-Anwendung die Benutzerkennung.
- (8) Der in der FHH etablierte [Passwort-SelfService](#) ist von jedem Nutzer zur (späteren) Identifikation und zum Rücksetzen des Passwortes einzurichten. Zum automatisierten selbstständigen Rücksetzen von Passwörtern kann der Passwort-SelfService ebenso verwendet werden. Vergleichbare Systeme sind grundsätzlich zulässig (z.B. bei Fachanwendungen).

3.5.2 Geheimhaltung

- (1) Passwörter sind geheim zu halten. Sie sind verdeckt einzugeben. Die Weitergabe von Passwörtern ist untersagt.

² Zugriffe auf IT-Systeme unter [Single Sign-On](#) sind von dieser Regelung ausgenommen.

- (2) Passwörter dürfen nicht auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden.
- (3) Ein Passwort für Dienstkonten darf nur für eine Hinterlegung im Notfall schriftlich fixiert und sicher verwahrt werden. Dies ist nur zulässig, wenn eine einfache Änderung oder eine Hinterlegung im IT-System nicht möglich sind.

3.5.3 Komplexität und Lebensdauer

- (1) Es gelten folgende Kriterien bei der Passwortvergabe:
 - a. Die Länge beträgt mindestens 10 Stellen.
 - b. Passwörter müssen Groß- und Kleinbuchstaben und mindestens ein Sonderzeichen und eine Ziffer enthalten.
 - c. Einstiegs- und Übergangspasswörter sind unverzüglich nach Erhalt durch eigene Passwörter zu ersetzen.
 - d. Die Lebensdauer eines Passworts wird nicht beschränkt, solange keine Kompromittierung vorliegt, es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.
 - e. Es müssen sichere Passwörter verwendet werden, die sich an den Vorgaben des BSI³ orientieren.

3.5.4 Übermittlung

- (1) Vor der Übermittlung des Passwortes ist die Identität der Person mit geeigneten Methoden zu überprüfen.
- (2) Die elektronische Übermittlung von Zugangsdaten, wie Passwort und Benutzerkennung, an Personen bzw. innerhalb von vernetzten IT-Systemen, darf ausschließlich kryptografisch unter Berücksichtigung der technischen Richtlinie zu kryptographischen Verfahren (BSI TR-02102-1) des Bundesamtes für Sicherheit in der Informationstechnik in der gültigen Fassung gesichert erfolgen.
- (3) Steht eine solche Verbindung nicht zur Verfügung, sind alternative Kommunikationswege zu nutzen, die eine unberechtigte Kenntnisnahme dieser Zugangsdaten ausschließen.

3.5.5 Speichertools für Benutzer

- (1) Für die toolgestützte sichere Hinterlegung und Verwaltung von Zugangsdaten (zum Beispiel Benutzerkennung und Passwort) für personalisierte Benutzerkonten und Dienstkonten oder zur Speicherung von komplexen Passwörtern können, die von der für die IT zuständigen Behörde freigegebenen Verfahren⁴ genutzt werden.

³ [BSI - Bundesamt für Sicherheit in der Informationstechnik - Sichere Passwörter - Faktenblatt](#)

⁴ Bei der Nutzung wird die Verwendung eines Hauptpasswortes mit mehr als 10 Zeichen empfohlen, um die Sicherheit zu erhöhen.

3.6 Nutzung von Token und Hardware-Authentisierungsmittel

- (1) Über den Einsatz von [Token](#) oder Hardware-Authentisierungsmitteln für ein IT-Verfahren entscheidet die jeweils fachlich verantwortliche Stelle.
- (2) Technische Details zur Authentisierung mittels Tokens sind durch die fachlich verantwortliche Stelle in Absprache mit dem IT-Dienstleister zu definieren. Arbeitshilfen zur Anwendung sind den Nutzern zur Verfügung zu stellen. Für die technischen Vorgaben bei Einsatz von Token ist die [PIN](#) Policy der Freien und Hansestadt Hamburg zu berücksichtigen.
- (3) Hardware-Authentisierungsmittel (z.B. Smartcard, Magnet-, Chipkarte), die zur Authentisierung verwendet werden, sind so zu handhaben, dass die Benutzung durch Unbefugte ausgeschlossen ist. Zu Benutzung, Verlust oder Diebstahl können die zuständigen Stellen besondere Regelungen treffen. Verlust oder Diebstahl ist unverzüglich zu melden.

3.7 Nutzung der Biometrie

- (1) Über den Einsatz von biometrischer Authentisierung für ein IT-Verfahren entscheidet die jeweils fachlich verantwortliche Stelle.
- (2) Technische Details zur Authentisierung mittels Biometrie sind durch die fachlich verantwortliche Stelle in Zusammenarbeit mit dem IT-Dienstleister zu definieren. Arbeitshilfen zur Anwendung sind den Nutzern zur Verfügung zu stellen.
- (3) Für die technischen Vorgaben bei Einsatz biometrischer Verfahren sind die Biometrie-Vorgaben der Freien und Hansestadt Hamburg zu berücksichtigen.

3.8 Nutzung von digitalen Zertifikaten

- (1) Über den Einsatz von [digitalen Zertifikaten](#) entscheidet die jeweils zuständige fachlich verantwortliche Stelle.
- (2) Digitale Zertifikate, die zur Authentisierung verwendet werden, sind so zu handhaben, dass die Benutzung durch Unbefugte ausgeschlossen ist. Zu Benutzung, Verlust oder Diebstahl können die für die IT zuständigen Stellen in den Organisationseinheiten besondere Regelungen treffen. Verlust oder Diebstahl ist unverzüglich zu melden.

3.9 Ausnahmen

- (1) Ausnahmen sind durch das [Ausnahmenmanagement](#) des Informationssicherheitsmanagement der Freien und Hansestadt Hamburg zu genehmigen.

4. Mitgeltende Vorschriften

(1) Folgende Vorschriften⁵ gelten ergänzend:

- PIN Policy der Freien und Hansestadt Hamburg
- Biometrie Vorgaben der Freien und Hansestadt Hamburg
- Dataport-Richtlinie „Namenskonvention Verzeichnisdienst“

5. Kontrolle der Richtlinie

(1) Die Vorgaben der Richtlinie sind regelmäßig durch die für die IT zuständige Behörde auf Wirksamkeit und Aktualität zu überprüfen.

6. Inkrafttreten und Geltungsdauer

(1) Diese Richtlinie tritt am 01.05.2024 in Kraft und ersetzt die Richtlinie zur Verwaltung von Passwörtern (Passwortrichtlinie – Passwort-RL) vom 10.10.2007 (MittVw, Seite 96). Die Richtlinie gilt bis zum Erscheinen einer neuen Version bzw. bis auf Widerruf.

Änderungshistorie

Version	Änderungs-Datum	Gliederungs-punkt	Erläuterung der Änderung	Autor/in
0.1	27.04.2021	Gesamter Inhalt	Entwurfserstellung	Wonneberger
0.10	07.01.2022	Gesamter Inhalt	Entwurfsfortsetzung	Hintz
0.11	10.06.2022	Gesamter Inhalt	Entwurfsfortsetzung	Harm
0.12	04.08.2022	Gesamter Inhalt	Überarbeitung Entwurf	Hintz
0.13	05.01.2023	Gesamter Inhalt	Überarbeitung Entwurf	Hintz
0.14	21.02.2023	Gesamter Inhalt	Finalisierung Entwurf	Hintz, Wonneberger, Taruttis, Pfau
0.15	28.06.2023	3.4.4	Identitätsnachweis vor Übermittlung ergänzt	Hintz
0.16	05.09.2023	Gesamter Inhalt	Einarbeitung der Anmerkungen der InSiBe und weitere Finalisierung	Hintz
0.2	12.09.2023	Gesamter Inhalt	Finalisierung Formatierung	Hintz
1.0	16.04.2024		Finale Version	Hintz
1.1	29.08.2024		Aktualisierung Inhaltsverzeichnis, Schärfung Def. PSS	Hintz

⁵ [SharePoint Bereich für die FHH geltenden IT-Vorschriften](#)

Anlage 1 – Begriffsdefinitionen

AD

Active Directory (AD) ist der zentrale Verzeichnisdienst (engl. directory für Verzeichnis), der die in einer Domäne vorhandenen Objekte verwaltet (Benutzer- und Gerätekennungen, Berechtigungsgruppen).

Administrator

Ein Administrator, auch Admin, ist ein Benutzer mit erweiterten Rechten in IT-Systemen zur Wartung und Verwaltung dieser IT-Systeme.

Ausnahmemanagement

Die IT-Stellen der Organisationseinheiten sind über den Ausnahmeprozess informiert und finden den Prozess über den BASIS-Kundenportal des IT-Dienstleisters. Beantragte Ausnahmen werden im Zuge des Ausnahmegenehmigungsprozesses mit Dataport und dem Informationssicherheitsmanagement der Freien und Hansestadt Hamburg bewertet und gegebenenfalls genehmigt. Über eine Befristung von Ausnahmen entscheidet das Informationssicherheitsmanagement der Freien und Hansestadt Hamburg.

Authentisierung/ Authentifizierung

Unter Authentisierung wird der Identitätsnachweis an einem IT-System verstanden. Die Authentisierung kann durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z.B. durch kryptografische Signaturen. Durch Verifizierung authentifiziert das IT-System anschließend den Benutzer.

Benutzerkennung

Benutzerkennung ist der Anmeldename einer natürlichen Person oder eines Dienstes, um sich an einem IT-System zu authentisieren.

Biometrie

Biometrie ist ein Messverfahren zur Wiedererkennung von Personen. Im Kontext dieser Richtlinie bezeichnet es eine Authentisierungsmethode, die zur Identifikation von Benutzern biologische Merkmale wie Fingerabdruck, Gesicht, Iris des Auges oder Stimme verwendet.

Digitales Zertifikat

Ein digitales Zertifikat ist ein Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Ein digitales Zertifikat ermöglicht unter anderem die Verwendung elektronischer Signaturen.

Ein-Faktor-Authentisierung

Hierunter wird eine Anmeldung über ein Benutzeraccount mit einem Faktor verstanden.

IT-Systeme

Ein IT-System im Sinne dieser Richtlinie besteht aus Hard- und Software sowie aus Daten, um der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten zu dienen.

Kompromittierung

Ein IT-System, eine Datenbank oder auch nur ein einzelner Datensatz wird als kompromittiert betrachtet, wenn Daten manipuliert sein könnten und wenn der Eigentümer (oder Administrator) des IT-Systems keine Kontrolle über die korrekte Funktionsweise oder den korrekten Inhalt mehr hat.

Konto

Ein Konto ist ein Mittel zur Regelung der Zugangsberechtigung zu einem IT-System. Im Sinne dieser Richtlinie gibt es zwei Arten von Konten:

- **Personalisiertes Benutzerkonto:** Benutzerkonto, welches von einer natürlichen Person genutzt wird. Die Begriffe Account, User Account werden synonym verwendet.
- **Dienstkonto:** Benutzerkonto, welches ausschließlich in automatisierter Weise von einem IT-System oder einer Anwendung genutzt wird. Dies schließt auch so genannte Roboter-Accounts auf Endgeräten ein.

Multi-Faktor-Authentisierung (MFA)

Eine Multi-Faktor-Authentisierung bezeichnet den Identitätsnachweis eines Nutzers mittels einer Kombination aus mindestens zwei unterschiedlichen und insbesondere unabhängigen Faktoren. Bei komplexen Sachverhalten können dieses aber auch drei oder vier Faktoren sein, die benötigt werden, um Zugang zu erhalten

Passwort

Ein Passwort ist ein Kennwort, mit dem sich ein Benutzer in Verbindung mit einem Benutzerkonto an einem IT-System authentisiert.

Password-SelfService

Der Password-SelfService (PSS) ermöglicht bei Basis-Arbeitsplätzen die Rücksetzung des Benutzerkonto-Passwortes ohne Hilfe von mitwirkenden IT-Abteilungen und UserHelpDesk des IT-Dienstleisters. Die selbstständige Rücksetzung durch Anwendende wird am Arbeitsplatz mit Hilfe eines Zugangs einer Kollegin oder eines Kollegen im Intranet durchgeführt⁶. Rücksetzungen bei Basis-Arbeitsplätzen im Homeoffice erfolgen über den UserHelpDesk auf Grundlage des Password-SelfServices.

PIN

Eine Persönliche Identifikationsnummer (PIN) ist eine nur einer oder wenigen bekannte Ziffernfolge, mit der sich diese gegenüber einer Maschine authentisieren können.

Single Sign-On

Single Sign-On (SSO), übersetzt Einmalanmeldung, beschreibt ein Verfahren, mit dem Benutzer über einen einzigen Authentisierungsprozess Zugriff auf verschiedene Anwendungen, Dienste oder Ressourcen erhalten.

Token

Ein Token ist eine personalisierte Hardwarekomponente (z.B. SmartCard, USB-Stick, Dongle) zur Identifikation und Authentisierung von Benutzern.

Technische Entität

Als technische Entität im Sinne dieser Richtlinie werden IT-Systeme bezeichnet, über die Informationen gespeichert oder verarbeitet werden sollen.

TDC-Dienste

TDC-Dienste sind die Dienste des Twin-Data-Center (Hauptrechenzentrum von Dataport).

⁶ [Link zum PSS](#); [WiKi zum PSS](#)