# Spezifikation Sicherheitsklassen für den Zugriff von Benutzern auf Anwendungen	Konvention SecClass 2.1 14~~22~~.12~~0~~.2007 Ergebnis der AG

Kurzbeschreibung:	Die Definition und Abbildung von Sicherheitsklassen ermöglicht es einer Anwendung zu prüfen, ob ein Benutzer die für die Nutzung der Anwendungsfunktion erforderlichen Sicherheitsauflagen erfüllt, auch wenn für Benutzer und Anwendungsbetreiber unterschiedliche Sicherheitsnormen gelten. Der Schutzbedarf von Anwendungen einerseits und Sicherheitsmaßnahmen der Benutzer und ihrer Systeme andererseits wird in einem Schema mit 4 Sicherheitsklassen kategorisiert, welches Auflagen im Bereich der Authentifizierung, der Netzsicherheit, der räumlichen Sicherheit und anderen Bereichen beinhaltet.		
Autor:	Rainer Hörbe (Q-PV)	Projektteam / Arbeitsgruppe:	Arbeitsgruppe Q-PV
Beiträge von:	Hildegard Freidl Peter Pfläging		

Vorgelegt am **TT.MM.JJJJ**

Abgelehnt von:
Zur Kenntnis genommen von:
Anregungen von:
Angenommen von: *(mit der Option von allen bzw. allen übrigen Ländern bei ablehnenden Stellungnahmen)*

Inhalt

1 Ziele für die Definition von Sicherheitsklassen

Die Sicherheitsanforderungen an Betreiber und Benutzer einer Anwendung sind abhängig von verarbeiteten Daten und sind daher von Anwendung zu Anwendung sehr unterschiedlich. Für die Erfüllung der Sicherheitsanforderungen ist der Auftraggeber einer Datenanwendung[1] verantwortlich.

Der Zugriff auf schützenswerte Daten hat im Rahmen einer Sicherheitsvereinbarung oder –verordnung zu erfolgen, wenn Maßnahmen durch die Anwendung nicht ausreichen. Allgemeine Sicherheitsvereinbarungen (wie die Portalverbund-vereinbarung) können durch anwendungsspezifische Sicherheitsvereinbarungen ergänzt werden.

Die Vereinbarung und Prüfung der Sicherheitsvereinbarungen soll zum Zeitpunkt des Zugriffs automatisch erfolgen und einfach zu verwalten sein. Dazu sind die Sicherheitserfordernisse in Sicherheitsklassen zu kategorisieren, welche mit Maßnahmen in folgenden Bereichen zu erfüllen sind:

1. Bereich der Benutzer
    - Authentisierungssicherheit
    - IT-Grundschutz (Netzwerksicherheit, Schutz von Maleware, ..)
    - Räumliche und physische Sicherheit
    - Personelle Maßnahmen (Schulung, Verpflichtungserklärung, ..)
2. Bereich der Anwendungen
3. Bereich der Kommunikation vertrauenswürdiger Geräte und Netzwerke

Durch die Übermittlung einer aus allen Maßnahmen des Benutzers abgeleiteten Sicherheitsklasse kann die Anwendung sicherstellen, dass der Benutzer mindestens die Anforderungen der von der gewünschten Anwendungsfunktion vorgegebenen Sicherheitsklasse erfüllt. Wenn nun eine Anwendungsfunktion eine höhere Sicherheitsstufe verlangt als der Benutzer hat, muss der Zugriff abgelehnt werden.

Die Vereinbarung von Sicherheitsklassen gewährleistet eine adäquate Sicherheit für die Anwendungen bei Auftrennung der Verantwortung für Anwendungs- und Benutzersicherheit.

Die Sicherheitsklassen sind auf einer allgemeinen Ebene spezifiziert, und müssen von den jeweiligen Organisationen im Detail spezifiziert werden. Damit sollen unterschiedliche Sicherheitsnormen (ISO 27000, BSI, [IT-SHB]) umgesetzt und zertifiziert werden können.

Nichtziele
In diesem Kontext werden die Anforderungen der Anonymität oder Pseudonymität von Benutzern nicht betrachtet, da die Nachvollziehbarkeit des Zugriffs auf personenbezogene Daten wichtiger ist.

[1] Im Portalverbund wird die Erfüllung von benutzerseitigen Sicherheitsanforderungen von den am Stammportal vertretenen Organen der öffentlichen Verwaltung wahrgenommen.

2 Referenz

Österreichisches IT-Sicherheitshandbuch [IT-SIHB], herausgegeben von der IKT-Stabsstelle des Bundes in der Version 2.2 (November 2004).

Das Sicherheitshandbuch wurde als Grundlage gewählt, weil es gegenüber anderen Normen, wie ITSEC, CC, BSI-Handbuch, BS7799 etc. folgende Vorteile hat:

- deutsche Sprache
- Anpassung an ÖNORM (Brandschutz, ..)
- Anpassung an österreichischen Gesetze
- deutlich gekürzter Umfang

3 Begriffsbestimmung

Benutzer	Physische oder juristische Personen, welche für den Zugriff auf Datenanwendungen berechtigt sind. Das schließt öffentliche Zugriffsrechte für anonyme Benutzer ein.~~Bedienstete oder sonstige von einer zugriffsberechtigten Stelle beauftragte physische Personen, welchen Zugriffsrechte auf Datenanwendungen zugeordnet sind.~~
Authentifizierung	Überprüfung der Identität eines Benutzers im Zuge des Anmeldevorganges
Autorisierung	von einem Stammportal für den Zugriff auf eine bestimmte Datenanwendung bestätigtes Rechteprofil eines Benutzers
zugriffsberechtigte Stelle	Einrichtung, der aufgrund ihrer gesetzlichen Aufgaben und der Vorgaben des Anwendungsverantwortlichen Zugriffsrechte auf eine oder mehrere Datenanwendungen eingeräumt wurden.

4 Klassifikation von Anwendungen

Es wurden 4 Sicherheitsklassen definiert, die für Anwendungen relevant sind. Dieses Dokument gibt vor, wie die minimalen Sicherheitsanforderungen durch den Anwendungsverantowrtlichen zu ermitteln sind.

Die Klassifizierung nach einer kombinierten Risikoanalysestrategie (IT-SIHB Teil 1) ist aufwändig: Für IT-Systeme der Schutzbedarfs-Kategorie "niedrig bis mittel" ~~wird~~ kann auf eine detaillierte Risikoanalyse verzichtet -und auf die im Folgenden beschriebene Klassifizierung nach DSG zurückgegriffen werden. Dies erlaubt eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus. Wenn eine Anwendung vertrauliche, nicht personenbezogene Daten verarbeitet, ist auch eine Riskioanalyse durchzuführen.
IT-Systeme der Schutzbedarfskategorie "hoch bis sehr hoch" sind einer detaillierten Risikoanalyse zu unterziehen. Die Sicherheitsklasse wird als Maximum der beiden Klassifizierungen (Risikoanalysestrategie sowie DSG) ermittelt.

Klassifizierung nach einer kombinierten Risikoanalysestrategie (IT-SIHB Teil 1/4.4.1)	**Sicherheitsklasse**
Schutzbedarfskategorie "niedrig bis mittel"	Ermittlung nach DSG ~~wie unten~~oder eigene Risikoanalyse
Schutzbedarfskategorie "hoch bis sehr hoch"	Eigene Risikoanalyse

Klassifizierung der Daten nach DSG und Vertraulichkeit (Sensibilitätsklasse)	**Sicherheitsklasse**			
	0	**1**	**2**	**3**
Frei verfügbare Informationen	X			
Abfrage von personenbezogenen Daten, die für jedermann zugänglich ist (z.B. Meldeauskunft nach §16.(1) MeldeG), oder Abfrage auf eingeschränkte Daten		X		
Transaktion[2] auf personenbezogene Daten (§ 4 (1) DSG 2000)			X	
Transaktion auf sensible Daten (§ 4 (2) DSG 2000)				X

[2] Transaktion i.S. von Abfrage, Verknüpfung, Eingabe, Änderung und Löschung von Daten

Übersicht zur Ermittlung der Schutzbedarfskategorien

(Abschnitt 4.4.1, IT-SIHB V2.2 Teil 1)

	Schutzbedarfskategorie "niedrig bis mittel"	Schutzbedarfskategorie "hoch bis sehr hoch"
1. Verstoß gegen Gesetze, Vorschriften oder Verträge	○ Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen ○ Geringfügige Vertragsverletzungen mit geringen Konventional-strafen ○ Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen	○ Schwere Verstöße gegen Gesetze und Vorschriften (Strafverfolgung) ○ Vertragsverletzungen mit hohen Konventionalstrafen oder Haftungsschäden ○ Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen ○ (Verlust der Vertraulichkeit oder Integrität sensibler Daten)
2. Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich	Eine über Bagatelle-verletzungen hinausgehende Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden

3. Beeinträchtigung der Aufgabenerfüllung	○ Es kann zu einer leichten bis maximal mittelschweren Beeinträchtigung der Aufgabenerfüllung kommen ○ Eine Zielerreichung ist mit vertretbarem Mehraufwand möglich	○ Es kann zu einer schweren Beeinträchtigung der Aufgabenerfüllung bis hin zur Handlungsunfähigkeit der betroffenen Organisation kommen ○ Bedeutende Zielabweichung in Qualität und/oder Quantität
4. Vertraulichkeit der verarbeiteten Information	Es werden nur Daten der Sicherheitsklassen OFFEN und EINGESCHRÄNKT verarbeitet bzw. gespeichert	Es werden auch Daten der Sicherheitsklassen VERTRAULICH, GEHEIM und/oder STRENG GEHEIM verarbeitet bzw. gespeichert[3]
5. Dauer der Verzichtbarkeit	Die maximal tolerierbare Ausfallszeit der Anwendung beträgt mehrere Stunden bis mehrere Tage (d.h. die Anwendung ist in Verfügbarkeitsklasse 2 oder 3 lt. Bsp. in Kap. 2.2.6 eingestuft)	Die maximal tolerierbare Ausfallszeit des Systems beträgt lediglich einige Minuten (Verfügbarkeitsklasse 1 lt. Bsp. in Kap. 2.2.6)
6. Negative Außenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten	Eine breite Beeinträchtigung des Vertrauens in die Organisation oder ihr Ansehen ist zu erwarten
7. Finanzielle Auswirkungen	Der finanzielle Schaden ist kleiner als (z.B.) € 100.000.-	Der zu erwartende finanzielle Schaden ist größer als (z.B.) € 100.000.-

[3] Definition entsprechend InfoSIG 2003 §2(2)

5 Sicherheitsklassen aus der Sicht von Benutzern

Die Sicherheitsklasse einer Client-Transaktion ist aus Benutzersicht von folgenden Faktoren abhängig:

- Client-Device (z.B. Arbeitsplatzrechner)
- Ort (Außendienst, Telearbeitsplatz, Amtsgebäude mit Zutrittskontrolle)
- Netzwerkanbindung (Intra- versus Internet)
- Registrierungsprozess
- Authentifizierungsfaktoren (z.B. Wissen und Besitz)

Die folgende Tabelle definiert, in welchen Bereichen von der jeweiligen Organisation des Benutzers detaillierte Sicherheitsanforderungen definiert werden müssen:
In der Tabelle bedeutet ‚X' erforderlich, ‚E' empfohlen.

	Sicherheitsklasse			
	0	**1**	**2**	**3**
Client-Authentifizierung				
Anonym	X			
Authentifiziert durch Wissen (UserID/Passwort)		X		
Authentifiziert durch Wissen und Besitz (SW-Zertifikat, HW-Token, Bürgerkarte, Einmalpasswort) ODER Authentifiziert durch Wissen an in einem geschützten Bereich[4] betriebenen Gerät ODER Authentifiziert durch Wissen und Eigenschaft (biometrisch)			X X X	
Authentifiziert durch Wissen und Eigenschaft an in einem geschützten Bereich betriebenen Gerät ODER Authentifiziert durch Wissen und Besitz an in einem geschützten Bereich4 betriebenen Gerät ODER Authentifiziert durch Wissen und Besitz an einem mobilen Endgerät mit erhöhtem Grundschutz[5]				X X X
IT-Grundschutz				
Passwortsicherheit		X	X	
Session Timeout[6]		X	X	X
Keine (Zwischen-) Speicherung von Anwendungsdaten am Client		X	X	X
Schutz vor Schadprogrammen (Viren etc.)		X	X	X
Physische Sicherheit			X	X
Netzwerkidentifikation (IP Netzwerk- oder Host-Adresse[7] oder Gerätezertifikat)				E
Restriktives Gerätemanagement[8]			X	X

[4] siehe unten die Definition „Geschützter Bereich"
[5] siehe unten die Definition "mobiles Endgerät mit erhöhtem Grundschutz"
[6] Ein Session Timeout erfordert eine neue Authentifizierung nach eine Inaktivitätsperiode
[7] Die Sinnhaftigkeit derPrüfung von IP-Adressen ist nur gegeben, wenn sichergestellt wird, dass keine fremden Devices, etwa drahtlos, mittels gültige IP-Adressen Zugriff bekommen können.
[8] z.B. Einschränkung für Benutzer selbst Software oder Devices zu installieren

	Sicherheitsklasse			
	0	**1**	**2**	**3**
Datensicherheit				
Unverfälscht (MAC/Hashwert im SSL[9])	X	X	X	X
Einer Person zuordenbar (über Protokolle)		X	X	X
Nicht bestreitbar (über Protokolle oder Signatur)		X	X	X
Stark verschlüsselt (SSL, symmetrischer Schlüssel mindestens 100 Bit)			X	X
Personelle Maßnahmen				
~~Identifikation (Registrierung) mit amtlichem Lichtbildausweis oder durch persönliche Bekanntschaft~~Identifikation (Registrierung) entsprechend den Erfordernissen für qualifizierte Zertifikate oder durch persönliche Bekanntschaft			X	
~~Identifikation (Registrierung) mit amtlichem Lichtbildausweis entsprechend den Erfordernissen für qualifizierte Zertifikate~~Identifikation (Registrierung) entsprechend den Erfordernissen für qualifizierte Zertifikate				X
Regelungen für Mitarbeiter		X	X	X

Anmerkung zur Authentifizierung durch Besitz: bis zur Einführung von HW-Token können auch SW-Zertifikate in der Sicherheitsklasse 2 verwendet werden. Bei der Gestaltung der konkreten Sicherheitsrichtlinien ist darauf zu achten, dass die schwächere Authentifizierung durch andere Maßnahmen wie verbesserte Schulung ausgeglichen wird.

Definition "Geschützer Bereich"
Die zugriffsberechtigte Stelle hat in ihrer Sicherheitsrichtline festzulegen, wie die physische und netzwerktechnische Kontrolle umzusetzen ist. Mit der physischen Kontrolle muss verhindert werden, dass unbekannte oder nicht vertrauenswürdige Personen Zutritt zum Gerät haben. Mit der netzwerktechnischen Kontrolle ist möglichst zu unterbinden, dass unerlaubte Zugriffe überhaupt das Gerät erreichen, etwa durch den Einsatz von Firewalls und Content-Filtern.

Anmerkung zur „Identifikation entsprechend den Erfordernissen für qualifizierte Zertifikate"
SigG § 8. (1) ~~verlangt, dass „die Identität von Personen, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines amtlichen Lichtbildausweises zuverlässig festzustellen [ist]."~~Ein ZDA oder eine in seinem Auftrag tätige Stelle hat die Identität von Personen, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines amtlichen Lichtbildausweises oder durch einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis, festzustellen.
Der Nachweis darüber ist ~~durch die Ablage einer Ausweiskopie oder die Niederschrift der Ausweisdaten zu erbringen~~zu dokumentieren.

[9] SSL, TLS, IPSec oder äquivalente kryptografische Verfahren

Definition "Mobiles Endgerät mit erhöhtem Grundschutz"
In der Sicherheitsrichtline ist festzulegen, wie in der jeweiligen Organisation mobile Geräte stark geschützt werden. Als mindestes Erfordernis müssen die Daten auf den Massenspeichern durch einen Schlüssel auf einem HW-Token verschlüsselt werden. Eine Entfernung des HW-Tokens muss die Entschlüsselung der Daten zuverlässig verhindern. Dieser Schlüssel muss ein anderer Schlüssel sein als zu Signatur verwendet wird. Er darf von anderen Benutzern des Endgeräts ebenfalls verwendet werden, muss dann aber auf einem anderen HW-Token gespeichert sein und mit einem unterschiedlichen Passwort gesichert sein. Wird das mobile Endgerät außerhalb von physisch geschützten Bereichen betrieben, muss dafür gesorgt werden, dass der HW-Token immer in der unmittelbaren Umgebung des Benutzers verbleibt.

Die Definition für das mobile Endgerät kann auch für stationäre Geräte angewendet werden, die nicht in einem geschützten Bereich betrieben werden.

Übergangsregelung für die Implementierung der Sicherheitsklasse 3 bis ~~Ende~~ 30. 9. 2008
Die ursprünglich bis Ende 2006 geplant Einführung von elektronischen Dienstausweisen ~~mit Bürgerkartenfunktion~~auf Zertifikatsbasis kann wegen der technischen und organisatorischen Schwierigkeiten in einigen Organisationen noch nicht umgesetzt werden. Um in der Zwischenzeit den Betrieb im Portalverbund zu ermöglichen und die mit der 3270-Kommunikation verbundenen Sicherheitsprobleme zu eliminieren, können Benutzer der Sicherheitsklasse 2 in einem geschützten Bereich in der Sicherheitsklasse 3 geführt werden. Diese Übergangsregelung ist bis Ende 2007 befristet und bedarf der Zustimmung des jeweiligen Anwendungsverantwortlichten.

6 Sicherheitsklassen für Anwendungen

	Sicherheitsklasse			
	0	**1**	**2**	**3**
Server-Authentifizierung				
Server-Authentifizierung durch Zertifikat (für HTTPS)	X	X	X	X
Signatur von aktivem Content	X	X	X	X
Datensicherheit				
Einem Benutzer zuordenbar (über Protokolle)		X	X	X
Bestätigung von Transaktionen durch die Anwendung			X	X
Unverfälscht (MAC/Hashwert im SSL)	X	X	X	X
Nicht bestreitbar (über Protokolle oder Signatur)		X	X	X
Stark verschlüsselt (SSL, symmetrischer Schlüssel mindestens 100 bit)			X	X

7 Sicherheitsklassen für die Verbindung zwischen vertrauenswürdigen Geräten und Netzwerken

	Sicherheitsklasse			
	0	**1**	**2**	**3**
Peer-Authentifizierung				
Wahlweise: Client-Zertifikat (über SSL-Verbindung oder VPN) oder Shared Secret (VPN) oder Überprüfung der statisch zugeordneten IP-Adresse		X	X	X
Datensicherheit				
Unverfälscht (MAC/Hashwert im SSL)	X	X	X	X
Stark verschlüsselt (SSL, symmetrischer Schlüssel mindestens 100 bit)			X	X

8 Änderungen

Änderungen von Version 2.0 zu 2.1

- Änderung in 4 Klassifikation von Anwendungen: Risikoanalyse kann auch gemacht werden, wenn keine personenbezogenen Daten verarbeitet werden (z.B. Einsatzpläne beim Katastrophenschutz
- Korrektere Formulierung der Tabelle in Kapitel 5 „Personelle Maßnahmen".
- Die Übergangsfrist für die Authentifizierung mit Wissen und Besitz für die Sicherheitsklasse 3 wird auf 30.9.2008 verlängert.
- In der Übersicht zur Ermittlung der Schutzbedarfskategorien Punkt 4 wurde angemerkt, dass die Begriffe aus dem InfoSIG stammen.
- Erweiterung der Begriffsbestimmung (→ Abschnitt 3) für Benutzer (damit sind auch Bürger und private Organisationen eingeschlossen)
- Die Anmerkung „Identifikation entsprechend den Erfordernissen für qualifizierte Zertifikate" auf Seite 8 wurde der Novelle SigG 2007 angepasst.

Änderungen von Version 1.1.1 zu 2.0

- ~~Erweiterung der Definition „geschützter Bereich"~~
- Erweiterung der Definition „geschützter Bereich"
- Übergangsbestimmung für die Sicherheitsklasse 3
- Erweiterung des Geltungsbereichs auerhalb des Portalverbundes
- Klärung HW-Verschlüsselung bei mobilen Geräten mit erhöhtem Grundschutz
- Korrektur der Schutzbedarfskategorien (1. Verstoß gegen Gesetze)
- Überarbeitung von „1 Ziele für die Definition von Sicherheitsklassen"
- SecClass aus Benutzersicht/Netzwerkidentifikation: Gerätezertifikat als Alternative zu IP-Adresse definiert, Soll- statt Muss-Bestimmung.
- Authentifizierung durch Wissen und Eigenschaft ist SecClass 3 nur an in einem geschützten Bereich betriebenen Gerät
- Def. „Mobiles Gerät mit erhöhtem Grundschutz": ... Dieser Schlüssel muss ein anderer Schlüssel sein als zu Signatur ~~und Authentifizierung~~ verwendet wird.
- „Übergangsregelung für die Implementierung der Sicherheitsklasse 3 bis Ende 2007": ... bis Ende 2007 befristet und bedarf der Zustimmung des jeweiligen Anwendungsverantwortlichten.
- Differenzierung der Ausweispflicht zwischen den Sicherheitsklassen 2 und 3. (Siehe „5. Sicherheitsklassen aus der Sicht von Benutzern" -> personelle Maßnahmen). Für die Sicherheitsklasse 2 kann persönliche Bekanntschaft den Ausweis ersetzen.

Änderungen von Version 1.1.0 zu 1.1.1

keine funktionellen Änderungen
Berichtigung der Definition „geschützter Bereich": statt „Mit der physischen Kontrolle muss erreicht werden" richtig „Mit der physischen Kontrolle muss verhindert werden.
Adaptierung der Vertraulichkeitsklassen gemäß der aktuellen Version des IT-Sicherheitshandbuches (IT-SIHB V 2.2, November 2004)

Änderungen von Version 1.0.0 zu 1.1.0

- Verwendung von Authentifizierung mit Wissen und Besitz in der Sicherheitsklasse 3
- reduzierte Anforderung an Authentifizierung im geschützten Bereich nicht mehr auf Übergangsfrist beschränkt

- Detailliertere Definition von „geschütztem Bereich“ und „mobilem Endgerät mit erhöhtem Grundschutz”
-