

<h2>Spezifikation Spezifikation Sicherheitsklassen</h2> <p>im Portalverbund-System</p>		Konvention	
		SecClass 1.1.1/22.01.04	
		Empfehlung	
Kurzbeschreibung:	<p>Die Definition und Abbildung von Sicherheitsklassen im Portalverbund ermöglicht es einer Anwendung zu prüfen, ob ein Benutzer die für die Nutzung der Anwendungsfunktion erforderlichen Sicherheitsauflagen erfüllt.</p> <p>Der Schutzbedarf von Anwendungen einerseits und Sicherheitsmaßnahmen der Benutzer und Benutzer-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.</p>		
Autor(en):	Rainer Hörbe (BMI-ITMS)	Projektteam / Arbeitsgruppe:	Arbeitsgruppe behördenübergreifende Autorisierungssysteme  Hildegard Freidl/Land Stmk. Franz Grandits/ Land Stmk. Rainer Hörbe/BMI Ludwig Moser/BMF Peter Pfläging/Mag. Wien

Stelle:	vorgelegt am:	angenommen am:
IKT-Board		
Städtebund		
Gemeindebund		
Länder		

## 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.

Um diese Sicherheitsanforderungen abdecken zu können, sind Maßnahmen erforderlich im:

- Bereich der Anwendung
- Bereich der Anwender
  - Authentisierungssicherheit
  - IT-Grundschutz (Netzwerksicherheit, Virenschutz, ..)
  - Räumliche und physische Sicherheit
  - Personelle Maßnahmen (Schulung, Verpflichtungserklärung, ..)

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

Zur Vereinfachung des Portalverbundes werden die Sicherheitserfordernisse in Sicherheitsklassen kategorisiert.

Dieses Dokument behandelt Sicherheitsanforderungen für folgende Bereiche:

1. Sicherheitsklassen aus Anwendungssicht.
2. Sicherheitsklassen aus Anwendersicht. Definiert Anforderungen an Stammportal und Benutzer um sicherzustellen, dass der Anwender mindestens die Sicherheitsanforderungen einer von der gewünschten Anwendungsfunktion vorgegebenen Sicherheitsklasse erfüllt. Wenn nun eine Anwendung eine höhere Sicherheitsstufe verlangt, als das Stammportal für einen bestimmten Anwender übermittelt, erhält der Anwender eine Fehlermeldung.
3. Sicherheitsklassen aus der Sicht des Anwendungsportals

Die Vereinbarung von Sicherheitsklassen gewährleistet eine adäquate Sicherheit für die IT-Anwendungen bei Auftrennung der Verantwortung für Anwendungs- und Benutzersicherheit. Darüber hinaus wird durch die Standardisierung der Maßnahmen zu den einzelnen Sicherheitsklassen eine einfache und effiziente Sicherheitspolitik ermöglicht.

Die Sicherheitsklassen sind auf einer groben Ebene spezifiziert, um so eine Schnittstelle zu den verschiedenen Sicherheitsrichtlinien der Verwaltungsorganisationen zu ermöglichen.

## **Begriffsbestimmung**

Die Begriffe sind in [PVV 1.0] definiert.

## **Kommunikation von Sicherheitsklassen zwischen Portalen**

Die Form der Übermittlung der Sicherheitsklasse ist im Dokument „PortalVerbundProtokollVx.x“ der AG Autorisierungssysteme definiert.

## **Referenz**

IT-Sicherheitshandbuch für die öffentliche Verwaltung, herausgegeben vom BMÖLS in der Version 2 (September 2001).

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

# 1. Sicherheitsklassen aus Anwendungssicht

- Es wurden 4 Sicherheitsklassen definiert, die für Webanwendungen relevant sind.

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

Klassifizierung nach einer kombinierten Risikoanalysestrategie (SIHB Teil 1/3.4.1)	Sicherheitsklasse
Schutzbedarfskategorie "niedrig bis mittel"	Ermittlung nach DSGVO wie unten
Schutzbedarfskategorie "hoch bis sehr hoch"	Eigene Risikoanalyse

Klassifizierung der Daten nach DSGVO 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, <i>oder Abfrage auf vertrauliche Daten</i>		X		
Transaktion <sup>1</sup> auf personenbezogene Daten (§ 4 (1) <a href="#">DSG 2000</a> )			X	
Transaktion auf sensible Daten (§ 4 (2) <a href="#">DSG 2000</a> )				X

<sup>1</sup> Transaktion i.S. von Abfrage, Verknüpfung, Eingabe, Änderung und Löschung von Daten

## Übersicht zur Ermittlung der Schutzbedarfskategorien (Abschnitt 3.4.1, SIHB Teil 1)

	Schutzbedarfskategorie "niedrig bis mittel"	Schutzbedarfskategorie "hoch bis sehr hoch"
1. Verstoß gegen Gesetze, Vorschriften oder Verträge	<ul style="list-style-type: none"> <li>○ Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen</li> <li>○ Geringfügige Vertragsverletzungen mit geringen Konventionalstrafen</li> </ul>	<ul style="list-style-type: none"> <li>○ Schwere Verstöße gegen Gesetze und Vorschriften (Strafverfolgung)</li> <li>○ Vertragsverletzungen mit hohen Konventionalstrafen oder Haftungsschäden</li> <li>○ Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen</li> <li>○ Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen</li> <li>○ (Verlust der Vertraulichkeit oder Integrität sensibler Daten)</li> </ul>
2. Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich	Eine über Bagatelleverletzungen hinausgehende Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden

3. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> <li>○ Es kann zu einer leichten bis maximal mittelschweren Beeinträchtigung der Aufgabenerfüllung kommen</li> <li>○ Eine Zielerreichung ist mit vertretbarem Mehraufwand möglich</li> </ul>	<ul style="list-style-type: none"> <li>○ Es kann zu einer schweren Beeinträchtigung der Aufgabenerfüllung bis hin zur Handlungsunfähigkeit der betroffenen Organisation kommen</li> <li>○ Bedeutende Zielabweichung in Qualität und/oder Quantität</li> </ul>
4. Vertraulichkeit der verarbeiteten Information	Es werden nur Daten der Sicherheitsklassen <small>OFFEN</small> und <small>VERTRAULICH</small> verarbeitet bzw. gespeichert	Es werden auch Daten der Sicherheitsklassen <small>GEHEIM</small> und/oder <small>SENSIBEL</small> verarbeitet bzw. gespeichert
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.-

## 2. Sicherheitsklassen aus der Sicht von Benutzersessions

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

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

Authentifizierung (z.B. Wissen und Besitz)

Die folgende Tabelle enthält, in welchen Bereichen von der jeweiligen Organisation des Benutzers detaillierte Sicherheitsanforderungen definiert werden müssen.

	Sicherheitsklasse			
	0	1	2	3
<b>Client-Authentifizierung</b>				
Anonym	X			
Authentifiziert durch Wissen (UserID/Passwort)		X		
Authentifiziert durch Wissen und Besitz (SW-Zertifikat, HW-Token, Einmalpasswort) ODER Authentifiziert durch Wissen an in einem geschützten Bereich <sup>2</sup> betriebenen Gerät			X	
Authentifiziert durch Wissen und Eigenschaft (biometrisch) ODER Authentifiziert durch Wissen und Besitz (HW-Token, Einmalpasswort) an in einem geschützten Bereich betriebenen Gerät <sup>2</sup> ODER Authentifiziert durch Wissen und Besitz (HW-Token) an einem mobilen Endgerät mit erhöhtem Grundschutz <sup>3</sup>				X
<b>IT-Grundschutz</b>				
Passwortsicherheit		X	X	X
Session Timeout <sup>4</sup>		X	X	X
Keine (Zwischen-) Speicherung von Anwendungsdaten am Client		X	X	X
Schutz vor Schadprogrammen (Viren etc.)			X	X
Physische Sicherheit			X	X
Netzwerkidentifikation (IP Netzwerk- oder Host-Adresse)				X
Gerätemanagement			X	X
<b>Datensicherheit</b>				
Unverfälscht (MAC/Hashwert im SSL <sup>5</sup> )	X	X	X	X
Einer Person zuordenbar (über Protokolle)		X	X	X

<sup>2</sup> siehe unten die Definition „Geschützter Bereich“

<sup>3</sup> siehe unten die Definition „mobiles Endgerät mit erhöhtem Grundschutz“

<sup>4</sup> Ein Session Timeout erfordert eine neue Authentifizierung nach eine Inaktivitätsperiode

<sup>5</sup> SSL, TLS, IPSec oder äquivalente kryptografische Verfahren

Nicht bestreitbar (über Protokolle oder Signatur)		X	X	X
Stark verschlüsselt (SSL, symmetrischer Schlüssel mindestens 100 bit)			X	X
Personelle Maßnahmen				
Identifikation mit amtlichem Lichtbildausweis (Registrierung)			X	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 "Geschützter Bereich"**

In der Sicherheitsrichtlinie ist festzulegen, wie in der jeweiligen Organisation 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.

#### **Definition "Mobiles Endgerät mit erhöhtem Grundschutz"**

In der Sicherheitsrichtlinie 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. Dieser Schlüssel muss ein anderer Schlüssel sein als zu Signatur und Authentifizierung 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 Anwenders verbleibt.

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

### 3. Sicherheitsklassen für die Verbindung zwischen Anwendungs- und Stammportal

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

#### Referenzen

[PVV 1.0]

Connert, Grandits, Kotschy, Posch, Siegl: Vereinbarung über die einzuhaltenden Rahmenbedingungen bei der Einrichtung und Benützung eines E-Government Portalverbundsystems (21.11.2002)  
<http://reference.e-government.gv.at> ⇒ Empfehlungen

[PVP]

Hörbe, Rainer: Portalverbund-Protokoll (16.10.2002)  
<http://reference.e-government.gv.at> ⇒ Empfehlungen

#### Funktionelle 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“

#### 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.“