

# Verwendungsbereiche der unterschiedlichen Zertifikate im Bereich BMI-Portal und Portalverbund

*Im Behördenbereich kommen verschiedene private und allgemein verfügbare Zertifikatsaussteller zum Einsatz. Die Einsatzbereiche der unterschiedlichen Zertifikate sind jedoch streng abgegrenzt. (Stand 2006-03-27)*

---

## Warum Zertifikate?

Zertifikate dienen der Authentifizierung von Anwendern – genau genommen, meist der Authentifizierung eines Rechners, dessen Benutzer zu bestimmten privilegierten Zugriffen berechtigt sind.

Das Schlüsselpaar, das zu einem bestimmten Zertifikat gehört, erlaubt dabei eine zweifelsfreie Identifikation sowie die sichere Verschlüsselung der Kommunikation.

Das genau identifizierte Zertifikat wird anhand eines Verzeichniseintrags in einem LDAP-Verzeichnis mit bestimmten Rechten gleichgesetzt.

---

## Die Zertifikatsaussteller im Bereich von BMI-Portal und Portalverbund

Während prinzipiell jedes Zertifikat eines vertrauenswürdigen Ausstellers für einen gesicherten Zugang verwendet werden könnte, sind in der Praxis die Zertifikatsaussteller aus organisatorischen und wirtschaftlichen Gründen eingeschränkt.

Besonders, wenn es um eine große Zahl von Zertifikaten geht, bietet sich aus Kostengründen die Verwendung von privaten Zertifikaten an.

### **bmiCA und bmiDemoCA – die BMI-CAs der ersten Generation**

Zur Inbetriebnahme des ZMR wurden die bmiCA und bmiDemoCA eingerichtet. Der Einsatzbereich dieser CAs ist der Zugriff von Gemeinden und Behörden auf das BMI-Portal. Zur Erstverteilung wurde ein semi-automatisches System entwickelt, um eine sichere und zuverlässige Verteilung der inzwischen mehr als 60.000 Zertifikate dieser CAs (in Test und Produktion zusammengefasst) zu ermöglichen.

Diese Zertifikate sind in ihrer Verwendung ausschließlich auf Gemeinden, Gebietskörperschaften und andere Einrichtungen der regionalen Verwaltung zur Kommunikation mit dem BMI-Portal vorgesehen.

### **bmiKundenCA und bmiKundenTestCA – die BMI-CAs für Businesspartner des BMI**

Für Abfragen durch BMI-Businesspartner wurden die bmiKundenCAs eingerichtet. Auch diese Zertifikate haben einen eng umgrenzten Gültigkeitsbereich, nämlich der direkten und gesicherten Kommunikation von BMI-Kunden mit dem BMI-Portal.

Da es sich bei diesem Zertifikat auch um ein reines Client-Zertifikat handelt, kann es ausschließlich für Client-Anfragen an das BMI-Portal verwendet werden.

Diese Zertifikate werden den Businesspartnern durch die BMI-Benutzerverwaltung zur Verfügung gestellt und haben eine zweijährige

Gültigkeit. Der Businesspartner ist dazu angehalten, die Gültigkeit des verwendeten Zertifikats im Auge zu behalten: Die Erneuerung der Zertifikate erfolgt zwar automatisch, die Installation des erneuerten Zertifikats liegt jedoch in der Verantwortung des einzelnen Businesspartners.

### **Portalverbund-CA – BMI Zertifikate für Server des Portalverbundes**

Für den Einsatz im Portalverbund sind die bisher genannten Zertifikate nicht verwendbar. Im Portalverbund kommunizieren Systeme, gemeinhin Portale, und ermöglichen den gegenseitigen Zugriff auf unterschiedliche Services, die auf Behördenportalen angeboten werden. (Siehe Literatur zum Portalverbund, etwa unter <http://portal.bmi.gv.at/ref/>)

Zur Teilnahme am Portalverbund ist die Portalverbund-Vereinbarung Voraussetzung.

Zertifikate des Portalverbundes können auch von anderen Zertifizierungsdiensten erstellt werden. Voraussetzung ist, dass das sogenannte Behördenkennzeichen als Zertifikatserweiterung gesetzt ist.

Als Serverzertifikate erfordern die PVP-Zertifikate, dass der Zertifikats-CN mit dem DNS-Namen des Systems übereinstimmt, auf dem das Zertifikat installiert ist. Bei einer Verwendung ausschließlich als Client muss diese Bedingung zwar nicht erfüllt sein, dennoch muss der CN des Zertifikats einem legalen und dem PVP-Teilnehmer zugeordneten DNS-Namen entsprechen.

Für die Gültigkeit des Zertifikats ist der PVP-Teilnehmer zuständig, eine Erneuerung eines Zertifikats, das durch die Portalverbund-CA erstellt wurde, muss mit mindestens 14 Tagen Vorlaufzeit bei der Ausstellerbehörde beantragt werden.

Für kommerziell erworbene Zertifikate, die für PVP-Verwendung berechtigt sind, gelten im Allgemeinen andere Bedingungen für die Erneuerung.

Es obliegt jedoch dem PVP-Teilnehmer, das erneuerte Zertifikat in diesem Fall ldap.gv.at bekannt zu machen. (Vorerst auch direkt der BMI-Zertifikatsverwaltung).