

- READY
- ALARM
- MESSAGE

IT-Dienstleistungszentrum des Freistaats Bayern **Gruppenrichtlinie zur Verteilung von Wurzelzertifikaten für Behörden außerhalb des Bündnisforests**

1. Vorbetrachtung.....	3
2. Konfiguration der Richtlinie	4

1. Vorbetrachtung

Das IT-Dienstleistungszentrum beim Landesamt für Digitalisierung, Breitband und Vermessung (LDBV) betreibt für die Bayerischen Verwaltungsbehörden eine kryptographische Infrastruktur bzw. Public Key Infrastruktur (PKI). Ziel dieser Infrastruktur ist die Bereitstellung von kryptographischem Schlüsselmaterial, elektronischen Zertifikaten und Zertifikatsstatusinformationen, um ein hohes Maß an Sicherheit für verschiedene IT-Verfahren der bayerischen Verwaltung zu gewährleisten.

Damit die hierbei eingesetzten Zertifikate über die Bayerische Verwaltung hinaus wirken können, ordnet sich die Zertifizierungsstelle der B-VPKI der zentralen Verwaltungs-PKI des Bundesamts für Sicherheit in der Informationstechnik (BSI) unter. Das BSI betreibt die zentrale Wurzelzertifizierungsstelle und generiert die Zertifikate der angeschlossenen Zertifizierungsstellen der einzelnen Verwaltungs-PKIs. Durch die zentralen Vorgaben des BSIs, zu deren Einhaltung sich die Betreiber der Verwaltungs-PKIs verpflichten, wird ein einheitliches Sicherheitsniveau geschaffen, so dass über die Grenzen der eigenen PKI hinaus auch automatisch Vertrauen zu den Zertifikaten anderer Verwaltungs-PKIs aufgebaut werden kann.

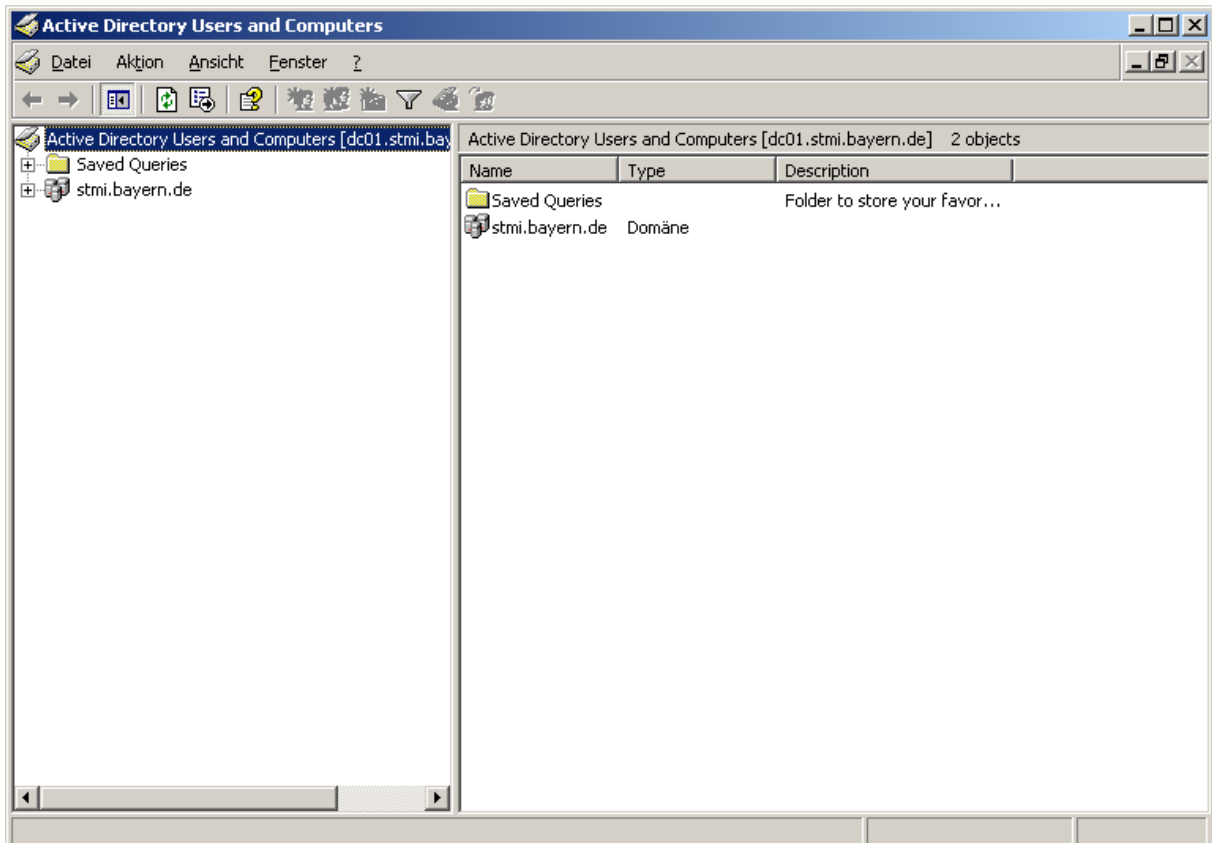
Um die Vertrauensstellung technisch zu realisieren, müssen den Clients die Wurzelzertifikate der Verwaltungs-PKI bekannt sein. Dies kann in Einzelarbeit durch den Anwender oder durch eine Gruppenrichtlinie erfolgen. Da das BSI jedes Jahr ein neues Wurzelzertifikat herausbringt, bedeutet es einen gewissen administrativen Aufwand die Liste der Wurzelzertifikate aktuell zu halten.

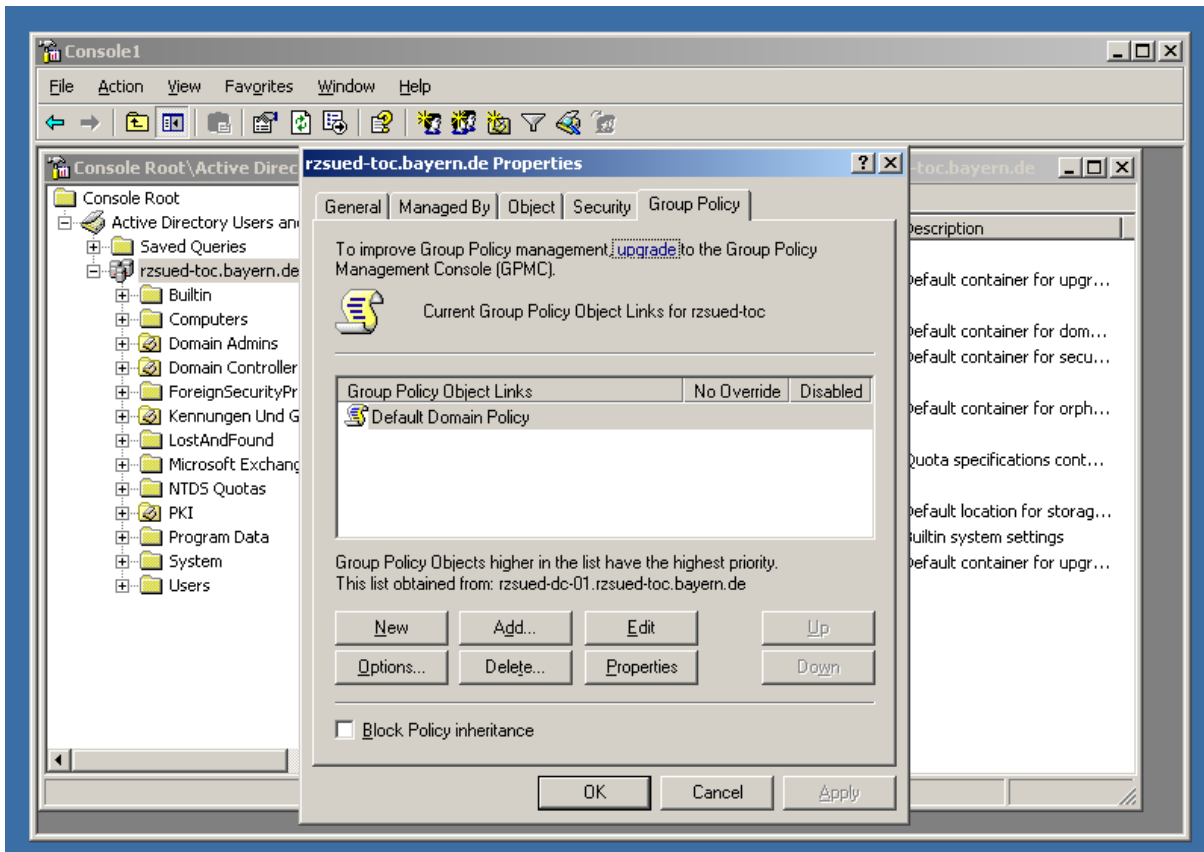
Das LDBV stellt im folgenden Kapitel die Dokumentation zur Verfügung, wie die windowsseitige Gruppenrichtlinie angepasst wird.

2. Konfiguration der Richtlinie

Zuerst wird die MMC „Users and Computers“ gestartet.

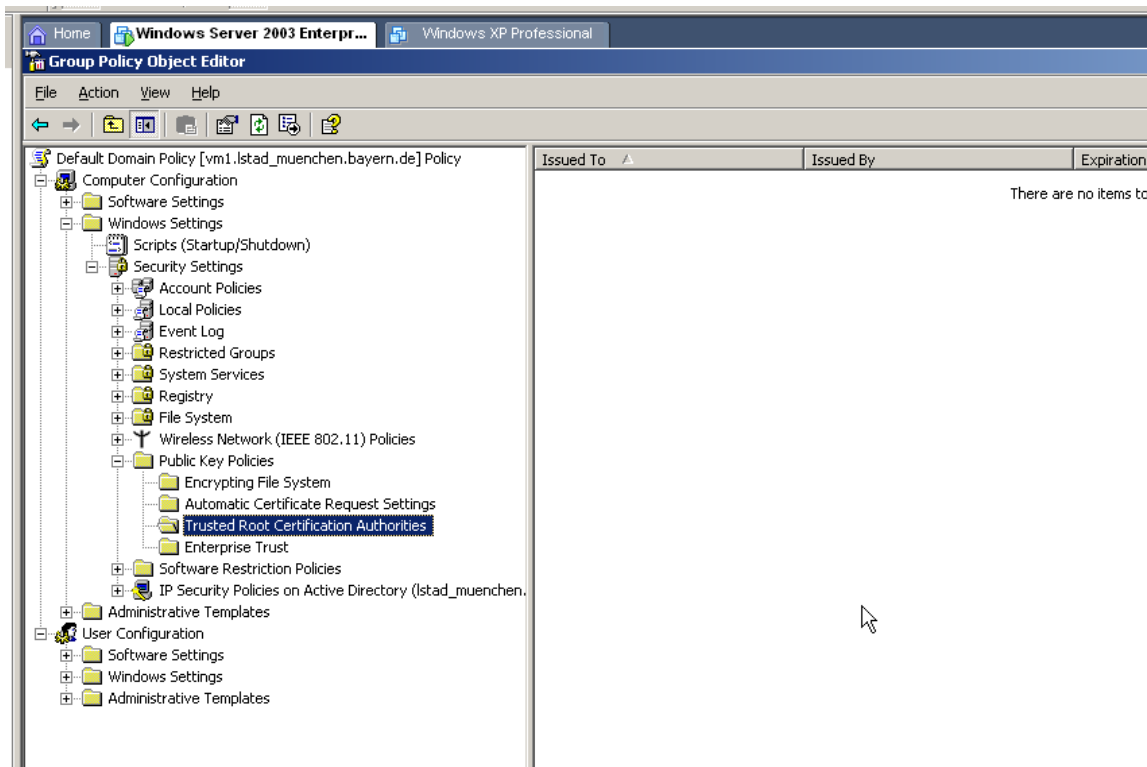
Wählen Sie den Ordner (Domäne / Organizational Unit) auf den die Gruppenrichtlinie wirken soll. Dies sollte die Domäne sein, mindestens aber die OU in der sich die Client PCs befinden. Klicken Sie dort mit der rechten Maustaste auf Eigenschaften (Properties) und dann auf den Reiter Group Policy / Gruppenrichtlinie.





Der genaue Pfad befindet sich unter:

→ **Group Policy** → **Computer Configuration** → **Windows Settings** → **Security Settings** → **Public Key Policy** → **Trusted Root Certification Authorities**



Dort können Sie mittels Klick auf die rechte Maustaste die übergeordneten Root-Zertifikate importieren. Diese können Sie vorher über einen Link auf unserer Webseite beziehen:

www.pki.bayern.de

- Allgemeine Informationen
 - Infrastruktur
 - CA Zertifikate
 - Link: Wurzelzertifikate

Die Richtlinie bezieht sich nun auf alle untergeordneten Rechner und bewirkt, dass dem lokalen Microsoft Zertifikatsspeicher die Wurzelzertifikate der Verwaltungs-PKI im Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ ergänzt werden. Andere Einstellungen werden durch diese Richtlinie nicht vorgenommen.