



Zuverlässiger Schutz für die elektronische Kommunikation

Für die elektronische Kommunikation ist die Sicherstellung der Vertraulichkeit eine Grundvoraussetzung. Dies gilt einerseits zwischen den Behörden der Berliner Verwaltung untereinander und zwischen Behörden und Bürgern andererseits – gerade im Hinblick auf die neuen bürgerfreundlichen Entwicklungen im Rahmen von eGovernment.

Um Ihren Daten- und Dokumentenaustausch jederzeit zuverlässig vor fremdem Zugriff zu schützen, hat das ITDZ Berlin bereits vor Jahren eine hauseigene Public Key Infrastructure (PKI) aufgebaut.

Eine Kette des Vertrauens – Struktur der PKI des ITDZ Berlin

Die im ITDZ Berlin ausgestellten Zertifikate entsprechen den international gängigen Sicherheitsanforderungen und basieren auf einer hierarchischen Vertrauensstruktur mit verschiedenen Zertifizierungsinstanzen sowie Aufgaben.

Als Zertifizierungsstelle beglaubigt das ITDZ Berlin die Gültigkeit des öffentlichen Schlüssels eines Zertifikatnehmers mit den dazugehörigen Identifikationsmerkmalen (wie Schlüsselinhaber, beglaubigende Stelle, Gültigkeitszeitraum etc.) durch ihre elektronische Signatur.

Gleichzeitig ist das ITDZ Berlin Registrierungsstelle (Registration Authority; RA) und damit zuständig für die Identitätsprüfung der Zertifikatnehmer, die Weiterleitung geprüfter Anträge an die

jeweilige Zertifizierungsinstanz und die Übergabe der Zertifikate an die Teilnehmer. Für Mitarbeiter des Landes Berlin liegt der Identitätsnachweis beim ITDZ Berlin bereits vor, eine weitere Identitätsprüfung ist in diesem Falle nicht mehr nötig.

Außerdem hat sich das ITDZ Berlin mit einer zusätzlichen Zertifizierungsstelle der bundesweiten PKI angeschlossen. Diese bezieht sich auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgebaute zertifikatsbasierte Schlüsselinfrastruktur und deren Sicherheitsrichtlinien für die Wurzelzertifizierungsinstanz der „Verwaltung für sichere E-Mail-Kommunikation“. Somit wird die Zertifizierungsstelle des ITDZ Berlin zum Bestandteil der PKI dieser Bundesverwaltung.

Kontakt

Gern unterbreiten wir Ihnen ein individuelles Angebot.

Kontaktieren Sie uns unter:

Telefon: +49 30 90222 (intern 9222) 6167
eMail: info@itdz-berlin.de

IT-Dienstleistungszentrum Berlin

Anstalt des öffentlichen Rechts
Berliner Straße 112–115
10713 Berlin
Internet: www.itdz-berlin.de
Intranet: www.itdz.verwalt-berlin.de

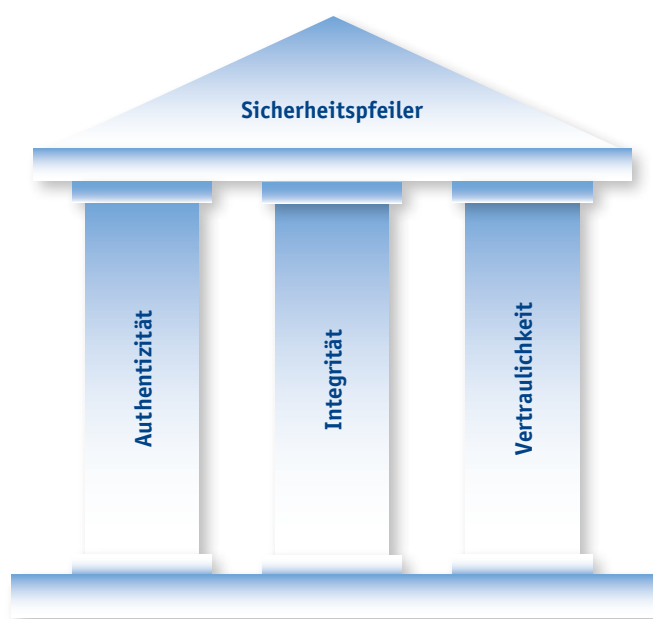
Stand: Frühjahr 2010

Doppelter Schutz – Verschlüsselung und elektronische Signatur

Um die Vertraulichkeit der Kommunikation zu gewährleisten, werden die Daten verschlüsselt übertragen. Die Verschlüsselung erfolgt über digitale Zertifikate, die auch die Echtheit eines öffentlichen Schlüssels und seinen zulässigen Geltungsbereich bestätigen.

Die elektronische Signatur entspricht der persönlichen Unterschrift unter einem Dokument und liefert den Nachweis über die Authentizität des angegebenen Kommunikationspartners und über die Integrität der Daten, d. h. darüber, dass die Daten unverändert beim Empfänger ankommen.

Die PKI erstellt, verteilt und prüft die digitalen Zertifikate und bildet damit die Grundlage für Verschlüsselung und elektronische Signatur.



Angebote im Rahmen unserer PKI

Zur Absicherung folgender Kommunikationswege generiert unsere PKI die entsprechenden Zertifikate für Sie:

■ eMail-Kommunikation (S/MIME-Zertifikate)

eMail-Zertifikate reduzieren die Risiken vor dem Zugriff durch Fremde. Eine gültig signierte eMail gibt zusätzlich die Sicherheit, dass die Nachricht wirklich vom angegebenen Absender kommt.

■ Server-Client-Kommunikation (SSL-Zertifikate)

Bei der verschlüsselten Kommunikation mit einem von unserer PKI zertifizierten Server können Sie sicher sein, dass es sich wirklich um den angegebenen Server handelt.

■ VPN (IPSec-Zertifikate)

Zum Aufbau von virtuellen privaten Netzen (VPN) werden IPSec-Zertifikate für eine verschlüsselte Verbindung zwischen VPN-Gateways eingesetzt, die die gesicherte Daten- und Informationsübertragung über öffentliche Netze garantieren. Durch die Zertifikate lassen sich verschlüsselte und authentifizierte Kommunikationskanäle (sogenannte Tunnel) zwischen einem Arbeitsplatz-PC und einem Anwendungsserver an verschiedenen Standorten aufbauen.

■ Windows Logon (Windows-Anmelde-Zertifikate)

Windows-Anmelde-Zertifikate garantieren die sichere Anmeldung zum System sowie zum Active Directory. Die Zertifikate stehen ab Anfang 2010 bereit.