

OIDs des Bundesministeriums für Inneres und deren Verwendung im Verantwortungsbereich des BMI Trustcenters

Dieses Dokument dient als Überblick über den für das BMI Trustcenter relevanten Teil des globalen OID Baumes und die Verwendung von OIDs in den Zertifizierungsstellen (CAs) des Trustcenters. Die aktuelle Version dieses Dokumentes ist unter <https://trustcenter.bmi.gv.at/ref/OID.pdf> abrufbar.

Grundlagen und Standards

Um Certificate Policies voneinander unterscheiden zu können, ist jeder Policy eine weltweit eindeutige OID zugeordnet.

In der "*Certificate Policies Certificate Extension*" kann eine oder mehrere OIDs angegeben werden. Zwei optionale Felder zur Certificate Policy sind vorgesehen: eine "*User Notice*", die die Policy kurz beschreibt, und ein Link auf das "*Certificate Practice Statement (CPS)*". Beide Möglichkeiten können, müssen aber nicht vom BMI Trustcenter genutzt werden.

Implementierung und Status

Die offiziellen OID-Nummern von "Certificate Policy"-Dokumenten des BMI Trustcenters werden im Allgemeinen unter dem Baum 1.2.40.0.10.1.2.3 angelegt.

OID	Bezeichnung
1	iso
1.2	iso member body
1.2.40	Austria (ÖNORM Institut)
1.2.40.0.10	Österreichische Verwaltung
1.2.40.0.10.1	Organisation
1.2.40.0.10.1.2	Bundesministerium für Inneres
1.2.40.0.10.1.2.1.1.1	eReisepass Policy
1.2.40.0.10.1.2.1.1.2	EAC-Policy
1.2.40.0.10.1.2.3	Standarddokumente des BMI-Trustcenters
1.2.40.0.10.1.2.3.1	CPS (Certificate Practice Statement) Portalverbund-CA (Generation 1) - ab Generation 2 mit Schema JJJJ.MM
1.2.40.0.10.1.2.3.1.2018.11	CPS (Certificate Practice Statement) Portalverbund-CA (Generation 2)
1.2.40.0.10.1.2.3.2	CP (Certificate Policy) Portalverbund-CA (Generation 1) - ab Generation 2 mit Schema JJJJ.MM
1.2.40.0.10.1.2.3.2.2018.11	CP (Certificate Policy) Portalverbund-CA (Generation 2)
1.2.40.0.10.1.2.3.3.2018.11	CP (Certificate Policy) BMI Kunden CA, ab Generation 2 mit Versionsnummer nach Schema JJJJ.MM

Sollten Versionsnummern nötig werden, so sind diese an die entsprechenden Basis OIDs anzuhängen. Dabei ist die momentan bevorzugte Möglichkeit die Nutzung des Schemas JJJJ.MM mit Jahreszahl und Monat.

Änderungen der Policy während der Lebensdauer einer CA werden nicht angestrebt, sind aber nicht vollständig auszuschließen, in diesem Fall kann es zur Neuausstellung von CA Zertifikaten zu bestehenden CA Schlüsseln kommen, um die entsprechenden OIDs eintragen zu können. Unwesentliche Änderungen an einem Dokument und Änderungen um Unklarheiten hinsichtlich der tatsächlichen Vorgehensweisen des BMI Trustcenters auszuräumen bedürfen keiner neuen OID.