TECHNICAL GUIDE FOR ESTEID2025 LDAP USAGE

This guide describes the LDAP directory service provided for querying digital identity certificates issued by Zetes Estonia. The service enables client applications to retrieve certificate entries using standard directory access protocols.

The service supports both LDAP (plaintext) and LDAPS (TLS-encrypted) protocols. Use of LDAPS is strongly recommended for all production integrations to ensure the confidentiality and integrity of directory queries in transit.

The test environment is intended for integration development and test certificate validation. It mirrors the production service behaviour but operates on a separate infrastructure. Production credentials and certificates must not be used against the test environment.

Service connectivity

- Production
    - LDAPS via ldaps://ldap.eidpki.ee port 636
    - LDAP via ldap://ldap.eidpki.ee port 389
- Test Services
    - LDAPS via ldaps://ldap-test.eidpki.ee port 636
    - LDAP via ldap://ldap-test.eidpki.ee port 389

Service Restrictions

The following limitations apply to all queries against the production service:

- Search fields. Directory searches are restricted to two attributes: the personal identity number field (serialNumber) and the common name field (CN). Queries against other attributes are not supported.
- Result set size. A maximum of 50 certificate entries will be returned per query. If a query matches more than 50 entries, only the first 50 will be returned. Client applications should construct queries specific enough to stay within this limit.
- Rate limiting. The service enforces a limit of 60 requests per hour per source IP address. Clients exceeding this threshold will receive an error response until the rate limit window resets. Applications should implement appropriate request throttling and caching to avoid hitting this limit under normal operating conditions.

Example Queries

Production environment

Base DN: *dc=ldap,dc=eidpki,dc=ee*

Search by personal identity number (serialNumber):

```
ldapsearch -H ldaps://ldap.eidpki.ee -x \
  -b "dc=ldap,dc=eidpki,dc=ee" \
```

```
  "serialNumber=PNOEE-***********"
```

Search by common name (CN):

```
ldapsearch -H ldap://ldap.eidpki.ee -x \
  -b "dc=ldap,dc=eidpki,dc=ee" \
  "cn=SURNAME,GIVENNAME,***********"
```

Test Services environment

Base DN: *dc=eidpki,dc=ee*

Note: The base DN for the test environment differs from production — dc=ldap is not present.

Search by personal identity number (serialNumber):

```
ldapsearch -H ldaps://ldap-test.eidpki.ee -x \
  -b "dc=eidpki,dc=ee" \
  "serialNumber=PNOEE-***********"
```

Search by common name (CN):

```
ldapsearch -H ldap://ldap-test.eidpki.ee -x \
  -b "dc=eidpki,dc=ee" \
  "cn=SURNAME,GIVENNAME,***********"
```

Schema for production environment