Missing replies	reply
Maximum expiration time of OCSP responses	10 minutes
EV Test Results	atttached
non sequentiel serial numbers and entropy in cert	random number in SERIALNUMBER field in subject (12 digits, ~39 bits)
URL to info about publicly disclosed subCA certs	https://www.a-trust.at/docs/SSL-Hierarchy-Gen05.pdf B) extensions for a-sign-SSL-EV-05 and a-sign-SSL-05
Externally operated SubCAs	no
Cross-signing	none
Technical Constraints on Third-party Issuers	not applicable
	https://cert.webtrust.org/SealFile?seal=1753&file=pdf, https://cert.webtrust.org/SealFile?seal=1754&file=pdf with Links to Management Assertions
Baseline Requirements	
	CPS: https://www.a-trust.at/docs/cps/a-sign-ssl-ev/a-sign-ssl-ev_cps.pdf - translated sections attached
SSL Verification	No challenge - response mechanism available
Organization Verification Procedures	translated sections attached
Multi-Factor authentication	Issuance is only possible using a smart card with PINs
	regular Network security checks are performed and monitored by Austrian Authorities since the Austrian
Network Security	citizen card, which is used for E-Government is also issued by A-Trust. Additional Audit conducted by
Document Handling of IDNs in CP/CPS	Manual handling, addressed in next WebTrust Audit
Issuing SSL Certificates for Internal Domains	only domains succesfully verified through a NIC-database are accepted
DNS names go in SAN	every DNS name in SAN, additionaly one DNS name in Subject
Domain owned by a Natural Person	SSL certificates are only issued to organizations (SSL and SSL EV)
	Non EV certificates issued by the new root certificate will have
Long-lived DV certificates	a maximum validity of 36 months (3 years)
Wildcard DV SSL certificates	Every issued SSL certificate is validated using OV
	no email challenge-response mechanism to verify domain control is used domains are validated by
Email Address Prefixes for DV Certs	identifying individual domain owners who are mentioned in trustworthy whois-databases
Delegation of Domain / Email validation to third parties	no third parties / RAs are involved in issuing SSL and SSL EV certificates
Allowing external entities to operate subordinate CAs	not used with SSL certificate roots
Distributing generated private keys in PKCS#12 files	keys are always generated by the subscriber

	certificates are only issued for external hostnames that can be
Certificates referencing hostnames or private IP addresses	verified - no IP adresses, no internal hostnames
Issuing SSL Certificates for Internal Domains	certificates are only issued for external hostnames that can be verified - no IP adresses, no internal hostnames old certificates have been audited, every used domain name in our certificates has been verified against the database or our national registration service
SHA-1 Certificates	the new root certificate will only be used to issue SHA-256 certificates existing certificates (using another root) will be migrated, once the new root certificate has been deployed
Lack of Communication With End Users	as A-Trust issues the Austria citizen signature card, there are many ways of contact available (7x24 Call center available)
Backdating the notBefore date	certificates are never backdated