

The background of the slide is a light gray gradient with several realistic water droplets of various sizes scattered across it. The droplets have highlights and shadows, giving them a three-dimensional appearance.

KISTI CA REPORT STATUS & SELF-AUDIT

shna@kisti.re.kr

For KISTI Certification Authority

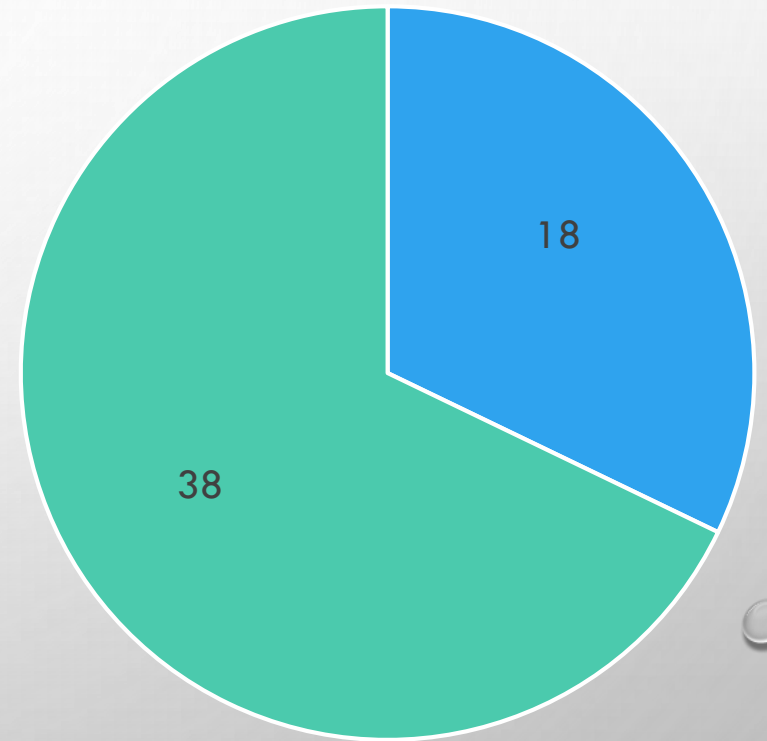
KISTI CA OVERVIEW

- Subject: C=KR, O=KISTI, CN=KISTI Certification Authority
- Valid from Apr 14, 2017 until Apr 9, 2037 (20 years)
- Signature algorithm: SHA-256 (CA Key size: 4096 bits)
- Online repository: <http://ca.gridcenter.or.kr>
 - Not deployed any more upon IPv6
 - Due to server relocation into the KISTI DMZ Zone, which is for the secure public web service, at last years.
 - The KISTI network manager do not have a plan to support IPv6 regarding public web service yet.
- Contact: kisti-grid-ca@kisti.re.kr

OPERATION STATUS

- **Subscribers**
 - Total number of subscribers: 382
 - Total number of institutes: 8
- **Certificates**
 - Total number of valid certificates: 51
 - Total number of issued certificates: 54 (user: 24, host: 30)
 - Total number of revoked certificates: 3 (user: 3)

INSTITUTE



■ University ■ Public Institute

SUMMARY OF SELF-AUDIT RESULT

- Auditing References
 - IGTF CAs auditing Checklist version 1 : CA – 50, RA – 10
 - The obsolete CA and RA items are omitted: CA – 20, 21, 26, 37, 44, RA – 8, 11
 - IGTF PKI Technology Guidelines Version 1.0-2016
- Overall Scoring

Authority	Items	Score			
		A	B	C	D (must change)
CA	50	49	1 (49)	-	1 (29)
RA	10	10	-	-	-

ITEMS REVIEW

- Item scored B – CA(49)
 - The KISTI CA CRL download had failed two times due to the network problem (Gbic adapter) and firewall policy expiration of DMZ zone.
 - Even though the web repository available 24X7 by on-call monitoring service, physical or SW issues sometimes make problems on availability. Thus we might consider finding high availability solution or adding one more CRL distribution point at external, such as cloud storage.
- Item scored D – CA(29)
 - The KISTI CA is off-line and must issue a new CRL at least 7days before the time stated in the next Update field, but we had missed CRL update one time at last April (1.096 days).
 - Currently, it relies on scheduled alarms, but it seems that a double check is needed through cooperation between CA operators.

UPDATE OF KISTI CA

- March 2021 -

- **CP/CPS 4.0 for new KISTI CA service**
 - writing a new CP/CPS documents
 - the APGridPMA reviewing until the first half of this year.
- **KISTI CA v.4 operation test**
 - we will attempt operational testing of new KISTI CA services.