KISTI CA Status Report

Sang-Un Ahn
for KISTI-GSDC Team

Contents

- Introduction
- KISTI CA Status
- ROOT CA Renewal
- Plan

Introduction

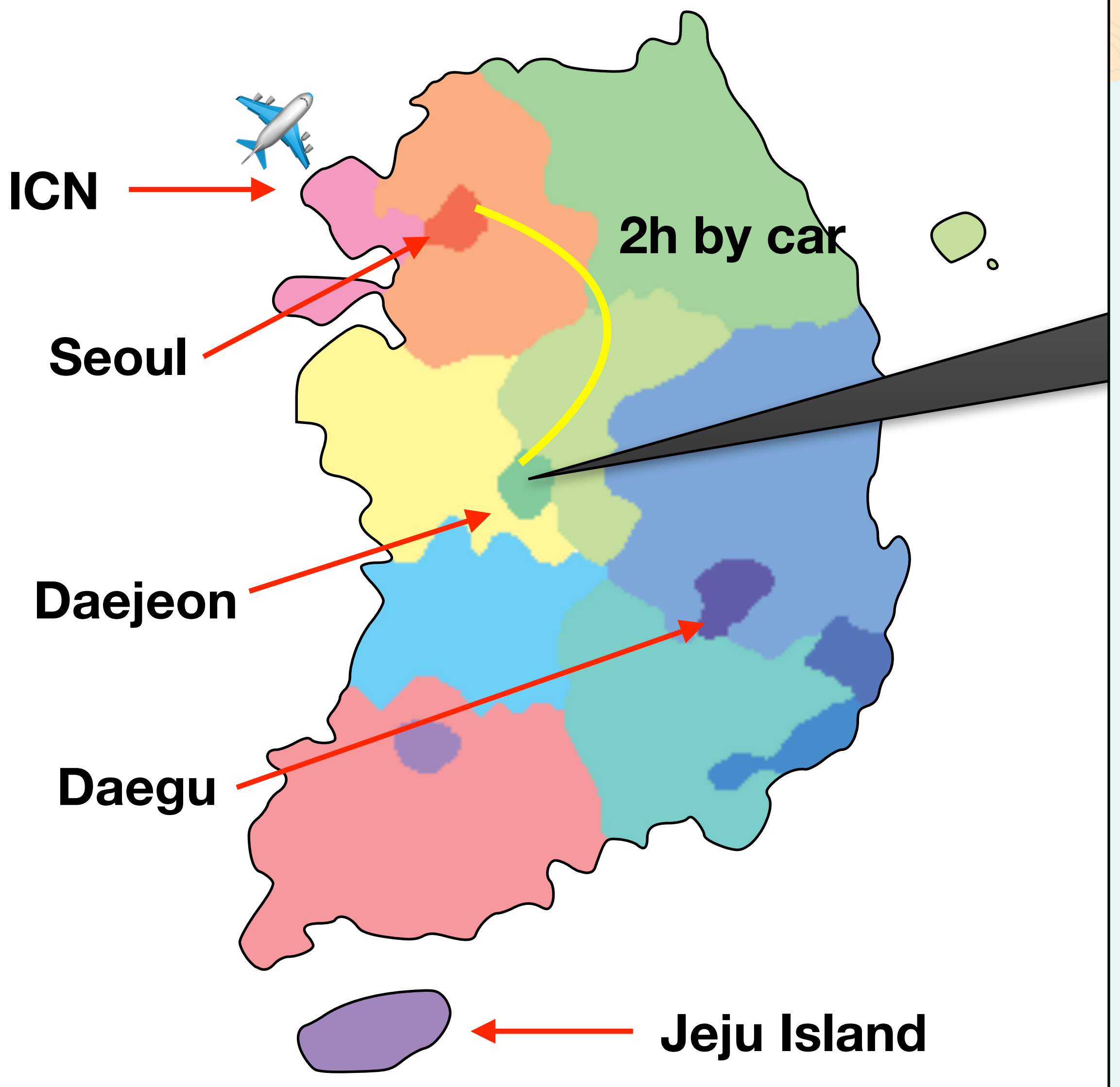
KISTI

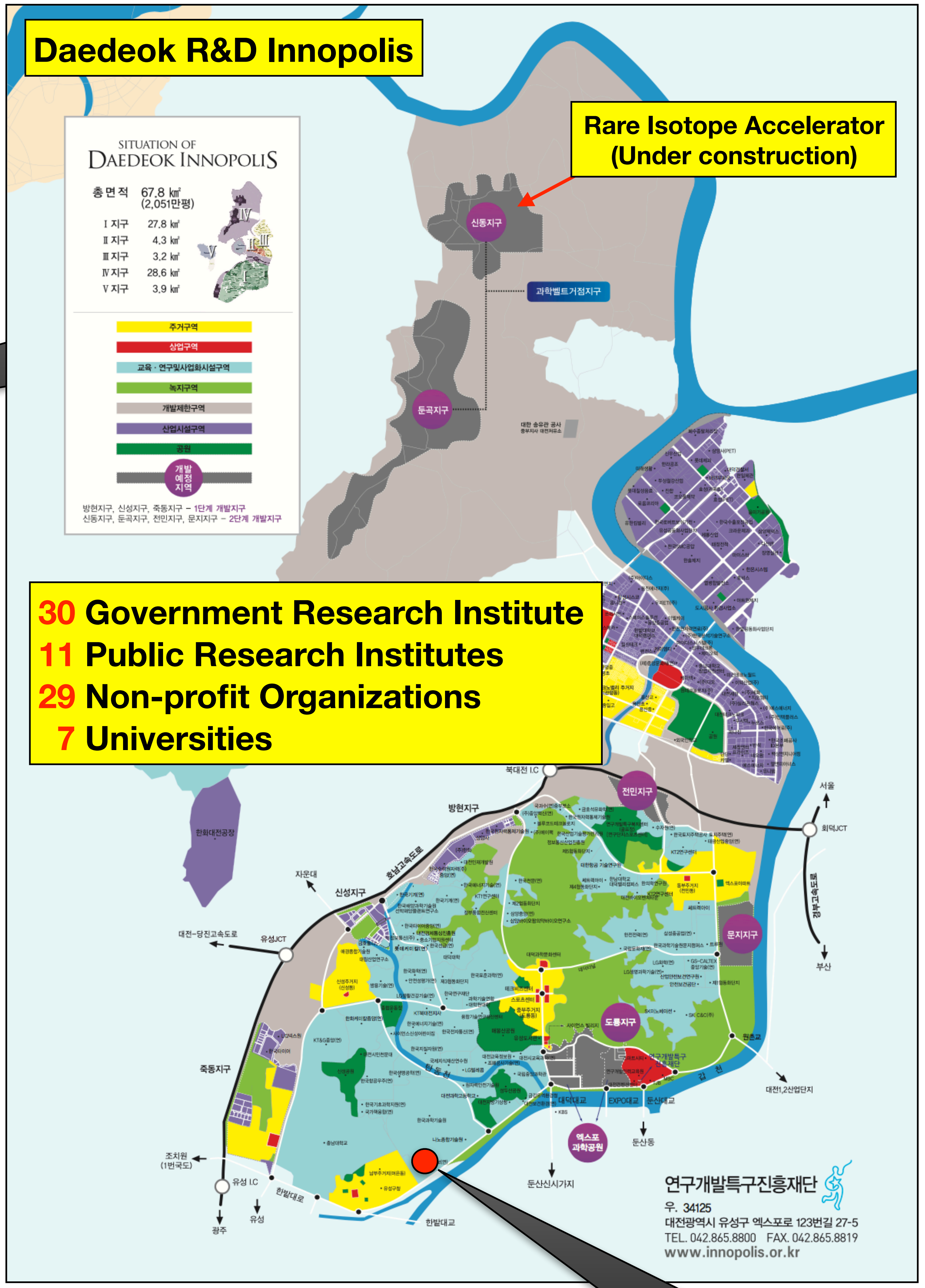
Korea Institute of Science and Technology Information

- Government-funded research institute founded in 1962 for National Information Service and Supercomputing

- **National Supercomputing Center**
    - Tachyon II system (~307.4 TFlops at peak), ranked 14th of Top500 (2009)
    - **New system coming this year (~18 PFlops at peak)**
    - **KREONet** - (Inter-)National R&E network

Map of South Korea





GSDC

Global Science experimental Data hub Center

- Government-funded project started in 2009 to **promote Korean fundamental research through providing computing power and data storage**
- **Datacenter for data-intensive fundamental research**
  - 9k cores, 8PB disk, 3PB tape
  - 6 experiments: ALICE, CMS, LIGO, Belle II, RENO and Genome project
  - New field: Structural biology based on TEM
  - 16 staff: system administration, experiment support, external-relation, management and planning

ALICE

CMS Compact Muon Solenoid

WLCG Worldwide LHC Computing Grid

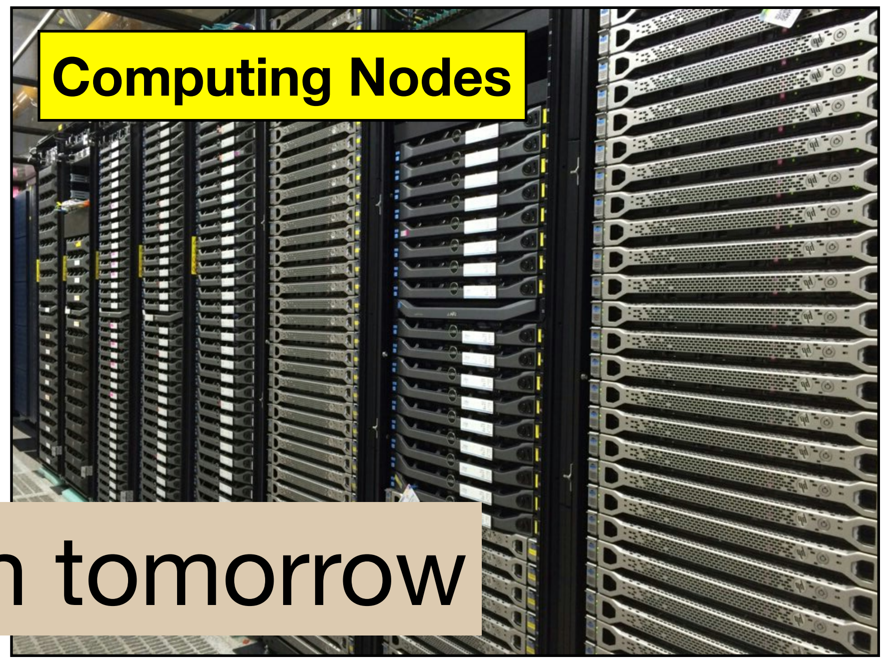
Belle II

RENO ν θ13

International Cancer Genome Consortium

LIGO

GLOBAL SCIENCE EXPERIMENTAL DATA HUB CENTER GSDC 글로벌대용량실험데이터허브센터



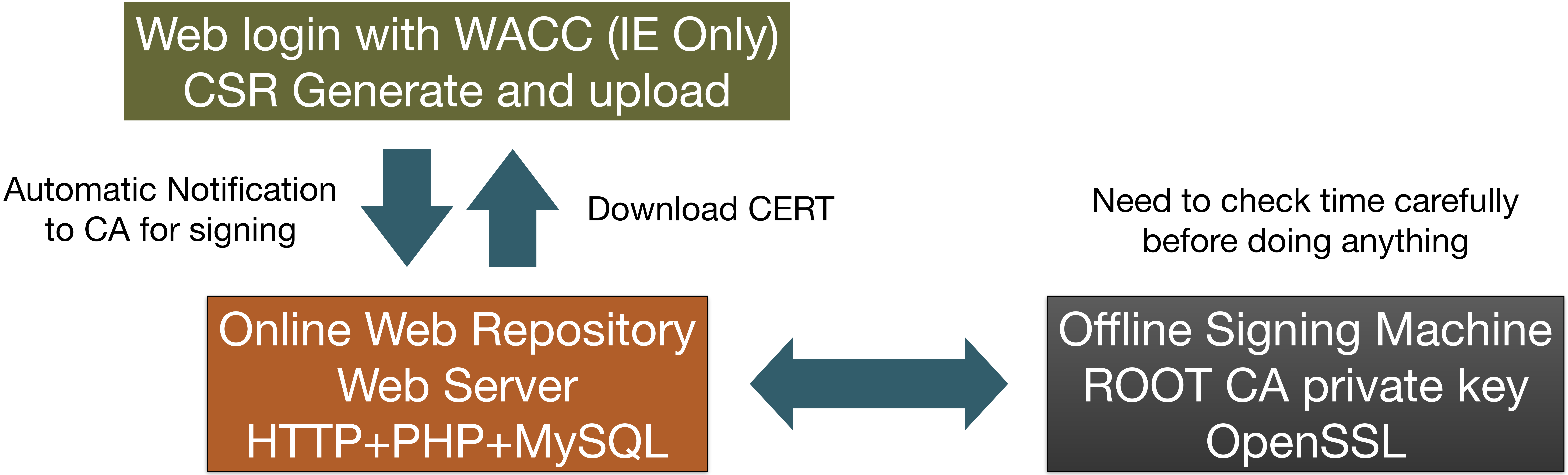
More information about GSDC system and WLCG Tier-1 operations will be given tomorrow

KISTI CA Status

KISTI Grid Certificate Authority

- KISTI GRID CA v2.0
  - Subject: C=KR, O=KISTI, O=GRID, CN=KISTI Grid Certificate Authority
  - Valid from Jul 12, 2007 until **Aug 1, 2017 (less than 5 months left for the renewal)**
  - Signature algorithm: **SHA2** (Key size: 2048 bits)
- Online repository: http://ca.gridcenter.or.kr

Issuing Process



Web login with WACC (IE Only)
CSR Generate and upload

Automatic Notification
to CA for signing

Download CERT

Need to check time carefully
before doing anything

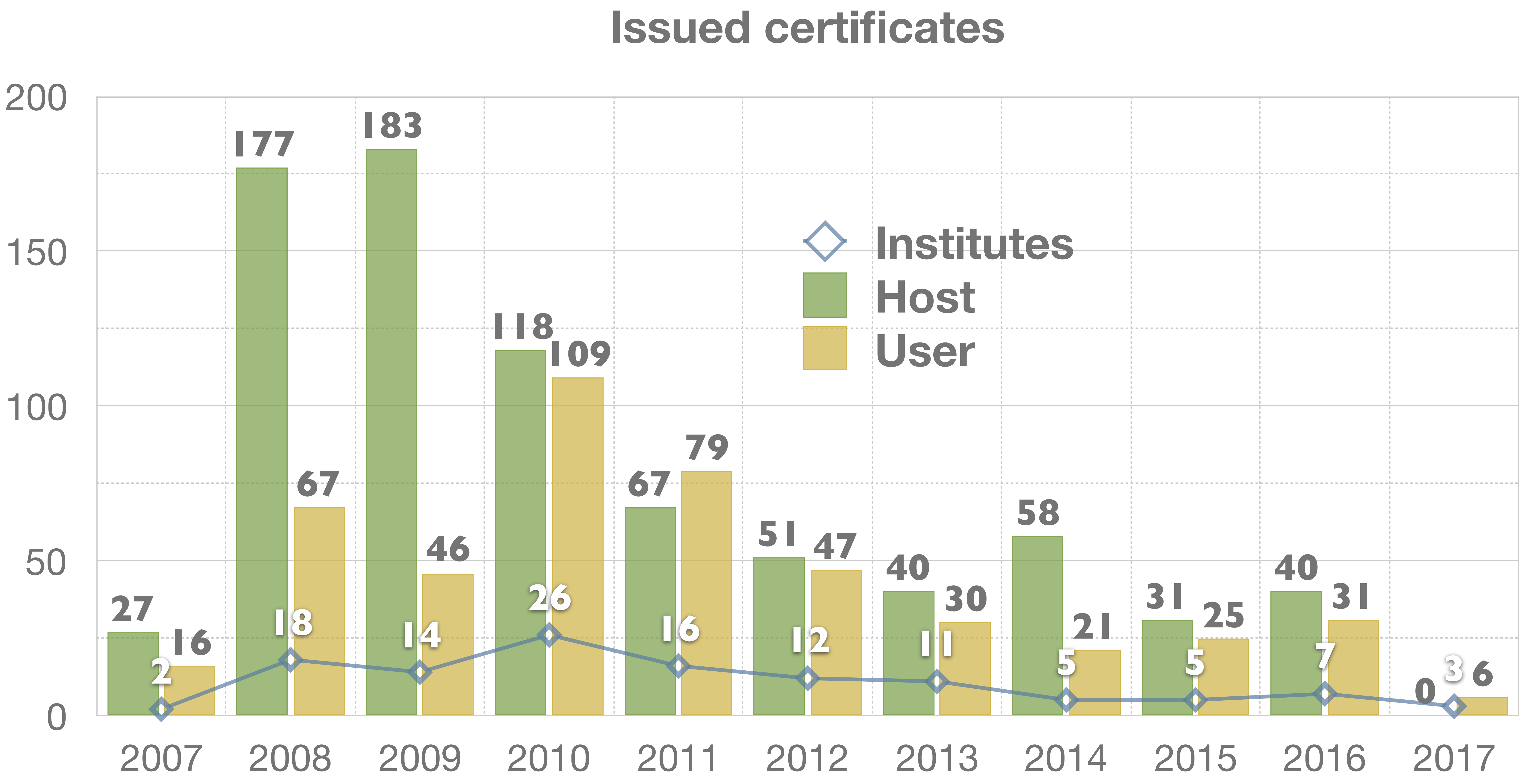
Online Web Repository
Web Server
HTTP+PHP+MySQL

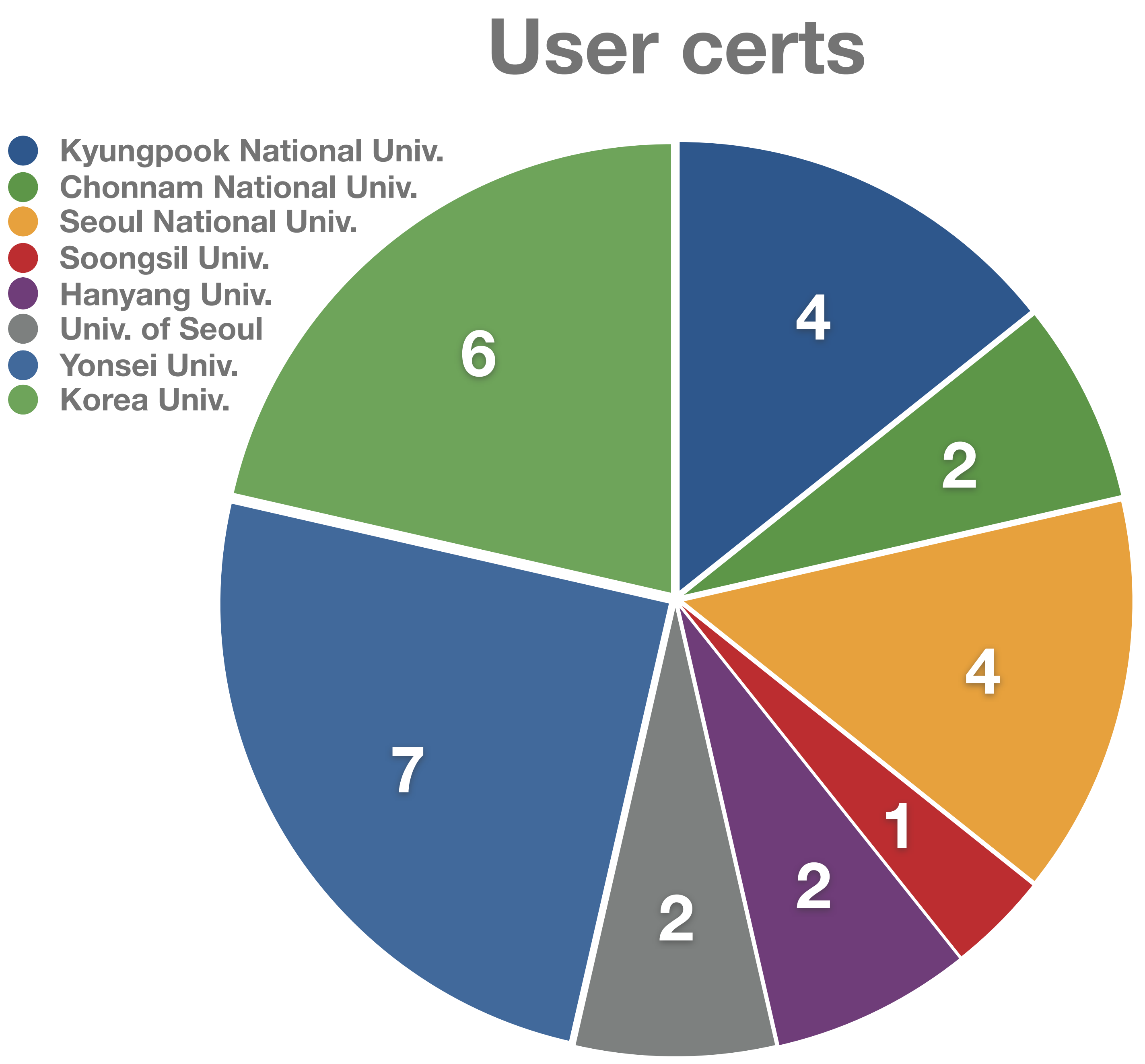
Offline Signing Machine
ROOT CA private key
OpenSSL

Physical access through console by CA Managers
CSR or CERT or CRL with hand-carrier media

Statistics

As of 28 Feb 2017

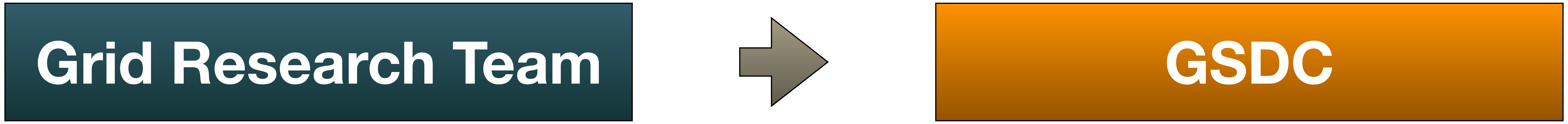




Type	User	Host	Total
Valid	37(28)	32(3)	69(31)
Expired	403	689	1,092
Revoked	37	71	107
Total	477	792	1,269

Average number of issued certificates is around 70 for the last 5 yrs
Now mostly are WLCG related certs, LDG and B2CG will bring more

CA Management Transfer



Grid Research Team → GSDC

ca@gridcenter.or.kr

CA
- **Sangwan Kim**
- Soonwook Hwang

RA
- Sangwan Kim
- Soonwook Hwang
- Kihyeon Cho

kisti-grid-ca@kisti.re.kr

CA
- **Sang-Un Ahn**
- Ilyeon Yeo

RA
- Each experiment support contact
- ALICE, CMS, LIGO, Belle II

System & security admins

Thanks to Sangwan Kim for his devoted work last 10 years !!!

Sangwan Kim has joined the project of developing supercomputing system for KISTI

True Story is …

- CRL was not updated within its lifecycle (30days) in September last year
- About 15 hours was taken for the recovery from the notice of failure since it happened in the middle of national holidays
- Authentication failure affected the stop of key services for grid operations led to the fall of almost 0.5% of overall availability of GSDC in the WLCG monitoring framework (achieved 99.3% availability in 2016)
- Since then we started discussion on management transfer of CA operations
  - Most of issued host certificates is used at GSDC for grid operations
  - Also GSDC grid admins rely on KISTI CA to enable grid services

We could do nothing in the situation we cannot control, we just try to avoid it

ROOT CA Renewal

CP/CPS Change Summary

- Keep the current CP/CPS with minor changes to maintain the certification signing policy and its practical procedure until the ROOT CA renewal
  - Replacing contact information plus mailing list for CA managers
  - Different subject name should be used for new ROOT CA following common naming convention
    - (Current) C=KR, O=KISTI, O=GRID, CN=KISTI Grid Certificate Authority
    - (New) C=KR, O=KISTI, CN=KISTI Grid Certification Authority
  - Avoid using “GRID” term repeatedly throughout the document, i.e. simply KISTI CA
  - OID should be updated accordingly
  - Correcting typos, deleting duplication

Certificate vs. Certification ?

	Current	**New**
0. Title of CP/CPS	Korea Institute of Science and Technology Information (KISTI) Certificate Policy and Certification Practice Statement	KISTI GRID Certification Authority Certificate Policy and Certification Practice Statement
1.1 Overview	-	Korea Institute of Science and Technology Information (KISTI) is a government-funded research institute located in Daejeon, Republic of Korea.
	This document is structured according to the RFC3647 (RFC3647 obsolete RFC2527).	This document is structured according to the RFC3647
1.2 Document name and Identification		
Document title	KISTI GRID CA Certificate Policy and Certification Practice Statement	KISTI CA Certificate Policy and Certification Practice Statement
Document version	2.0	3.0 OR 2.1
Document date	July 20, 2007	February 17, 2017
OID	1.3.6.1.4.1.14305.1.1.1.2.0	1.3.6.1.4.1.14305.1.2.1.3(2).0(1)
	1 (KISTI GRID CA)	2 (KISTI CA)
	2 (Major Version)	3 (Major Version) OR 2(Major).1(Minor)
1.3.3 Subscribers (End Entities)	· Grid projects in collaboration with KISTI · Programs involved in KISTI supercomputing research · LCG/EGEE-related projects/programs in Korea · International or domestic collaboration in Grid computing area	· International or domestic research projects/programs involved in WLCG Project or grid infrastructure related projects · Grid projects in collaboration with KISTI · Programs involved in KISTI supercomputing research
1.3.4 Relying parties	KISTI GRID CA's relying parties includes the following: - Employees of KISTI or research institutes in Korea - Employees of international research institutes which collaborate with KISTI in Grid computing area - Resource-sharing organizations with KISTI Supercomputing Center	KISTI CA's relying parties includes the following: - Employees of KISTI or research institutes in Korea - Employees of international research institutes which collaborate with KISTI - Collaborating organizations with KISTI Supercomputing Center

	Current	New
1.4 Prohibited certificate uses	Certificates issued by the CA must not be used for: Electronic commerce. Any application requiring fail-safe performance, including those associated with, but not limited to: The operation of nuclear facilities; Air traffic control systems; Aircraft navigation systems; Hospital life support systems; Municipal water treatment plants; Weapons control systems; or Any other system whose failure could lead to injury, death, damage to property or environmental damage. Transactions where applicable law prohibits the use of digital signatures for such transactions or where otherwise prohibited by law; or Unless supported by other appropriate security mechanisms and procedural safeguards, the protection of: Information that, if compromised, could cause extremely grave injury outside the national interest; or Classified information.	No Stipulation
1.5.1. Organization administering the document	KISTI GRID CA is managed by Grid Technology Research Team, KISTI.	KISTI CA is managed by Global Science experimental Data hub Center, KISTI.
1.5.2. Contact person	Sangwan Kim Soonwook Hwang	Updated accordingly Added new mailing list (kisti-grid-ca@kisti.re.kr)
3.1.6. Recognition, authentication, and role of trademarks	Duplicate	Remove duplication
3.2.2. Authentication of organization identity	The KISTI GRID CA verifies the identity of organizations by checking that the organization is known to the grid computing communities.	No Stipulation

	Current	**New**
5.3.3. Training requirements	The CA shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as security requirements, operational responsibilities and associated procedures	Internal training is given to KISTI CA and RA operators
5.3.4. Retraining frequency and requirements	The CA shall review and update its training program at least once a year to accommodate changes in the CA system.	No Stipulation
6.1.5. Key sizes	The minimum key length for user or host/service certificate is 1024 bits. The CA key length is 2048 bits.	The minimum key length for user or host/service certificate is 2048 bits. The CA key length is 2048 bits.
6.3.1. Public key archival	The CA shall retain all public key certificates it generates.	Public key archival is not supported.
7.1.3. Algorithm object identifiers	Signature Algorithm: sha1WithRSAEncryption(2048 bits)	Signature Algorithm: sha2WithRSAEncryption(2048 bits)

References

- RFC3647
- APGrid PMA CP/CPS Requirement

Milestones

	2016			2017							
	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
☑ CA Management Transfer Meeting	18.10.2016										
☑ CA Management Transfer				10.01.2017							
☑ Internal CP/CPS Revision					17.02.2017						
☑ Review request to APGrid PMA					21.02.2017						
□ Review & feedback (multiple rounds expected)						🟧	🟧				
□ Generate new ROOT CA and publish onto repository								▨			
□ Re-issue certificates with new ROOT CA									▨	▨	
□ Revoke certificates signed by old ROOT CA											▨

↑ ROOT CA Expiration

Plan

CA System Upgrade

- Old hardware replacement of online repository and CA signing machine
- Supporting not only IE for certificate request but also Firefox, Safari, Chrome, etc. upon various OS
- Under investigation to Dog-tag certificate system (open-source version of Red Hat Certificate system)

Appropriate?

- Under investigation to Hardware Security Module (FIPS 140-2 level 3 validated)
- Automation of certificate issue process
    - User enrollment must(?) be done with a F2F meeting

Can it be done with appropriate identification process?

- In order to deploy the new system in production after validation, CP/CPS shall be updated accordingly and published with approval of PMA

Thank you

Questions?