HPCI CA Update

32nd APGridPMA Meeting
August 24th 2023
Colombo, Sri Lanka

SAKANE, Eisaku
National Institute of Informatics
Japan

National Institute of Informatics

Overview

- HPCI CA issues certificates to end-entities in Japan's High Performance Computing Infrastructure (HPCI) for access to supercomputers and distributed file storage.
- The production level operation started in September 2012.
  - approved by IGTF as a MICS CA in August 2014.

National Institute of Informatics

Operation System

	A	B	C	D
Security Officer	◎			
CA Operator		◎	◎	
Log Manager				◎
Helpdesk Staff	◎	◎	◎	◎

National Institute of Informatics

Current Status

- Certificate statistics as of 2023/08/24
  #valid (#issued)
  - Client certificates: 183 (3,607)
  - Server certificates: 244 (2,997)
    host: 80 (1030)
    service (gfsd): 164 (1,967)

Support for OCSP and IPv6

- SHA-2 based certificates and CRLs
  - working
- OCSP support
  - working since June 22 2016
- CRL downloads over IPv6
  - working since October 18 2016
  - establishing the IPv6 connection with L2VPN in the building where the CA repository is.

National Institute of Informatics

Work in Progress

- GSI support
  - Docker image for GSI-OpenSSH client.
    - An alternative to GSI-SSHTerm.
    - The license of Docker Desktop was changed.
  - macOS native binary for GSI-OpenSSH.
  - Support for WSL2 (without docker)
- NAREGI-CA development
  - minor fixes will be released.
- Post GSI
  - Token-based AA system
    - OAuth-SSH (SciTokens SSH), KeyCloak, odic-agent

National Institute of Informatics

Self-audit Report

Self-audit

- HPCI CA is based on the IGTF MICS profile.
- We conducted an internal audit for FY2023 based on
  - AssuranceAssessment-v04-20190124.xlsx
  - IGTF-CAs-Auditing_v1.xlsx
  - HPCI CA CP/CPS version 9.0
- Actually, since the situation surrounding the CA is unchanged, the result of the self-audit is the same as the previous one.

National Institute of Informatics

Result of Self-Audit

- Assurance assessment (AA) matrix v04

#Items	Score				
	A	B	C	D	X
48	46	0	0	0	2

The items scored X is No. 30 and 36.

- IGTF CAs auditing v1

Authority	#Items	Score				
		A	B	C	D	X
CA (IA)	50	49	0	0	0	1
RA	10	10	0	0	0	0

The item scored X is (2) in Sec. 3.1.1 CP/CPS.

The obsolete CA check items (20), (21), (26), (37), and (44) in Sec.3.1 are omitted.

The obsolete RA check items (8) and (11) in Sec. 3.2 are also omitted.

National Institute of Informatics

Item that became scored A

3.1.2 CA System

(12) For CAs that issue end-entity certificates the lifetime of the CA certificate must be no less than two times of the maximum lifetime of an end-entity certificate and should not be more than 20 years.

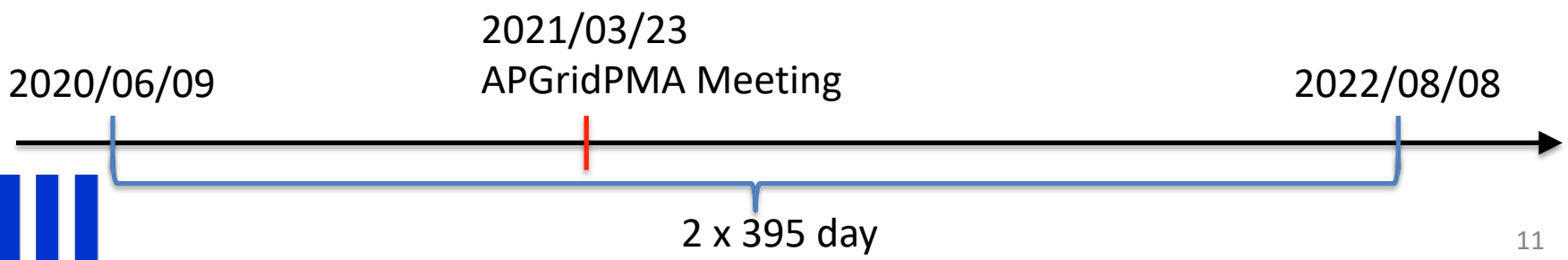
Two times of the maximum lifetime of an end-entity certificate:

2 x 395 day

Not after of HPCI CA (as of 2021/10/25) :

Not After : Aug 08 09:00:00 2022,

HPCI CA had violated PKI Tech Guideline since 2020/06/09.



National Institute of Informatics

Item that became scored A (Cont'd)

Timeline

2020/06/09	HPCI CA violated PKI Tech Guideline.
2021/03/23	27th APGridPMA meeting HPCI CA did not recognize the violation.
2021/10/28	HPCI CA extended the self-signed certificate. Not after : Aug 07 2032
2022/03	The new self-signed certificate is included in the IGTF Trust Anchor Distribution v1.115.

National Institute of Informatics