HKU Grid Certificate Authority (HKU Grid CA)

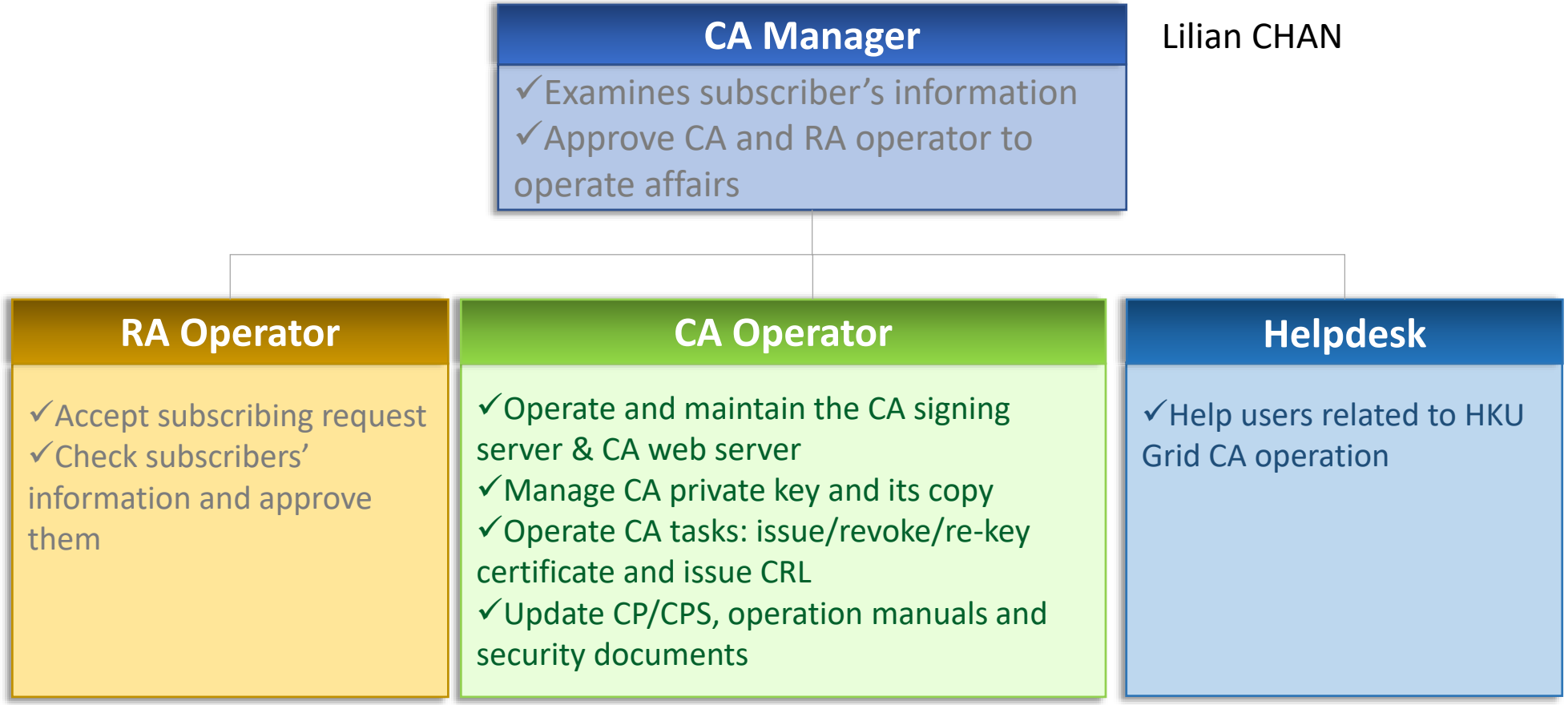
Self Audit & Status Report

Mar 21, 2023

INFORMATION TECHNOLOGY SERVICES
The University of Hong Kong

Operating Organization

HKU Grid CA ~ Classical offline CA operates since 2009



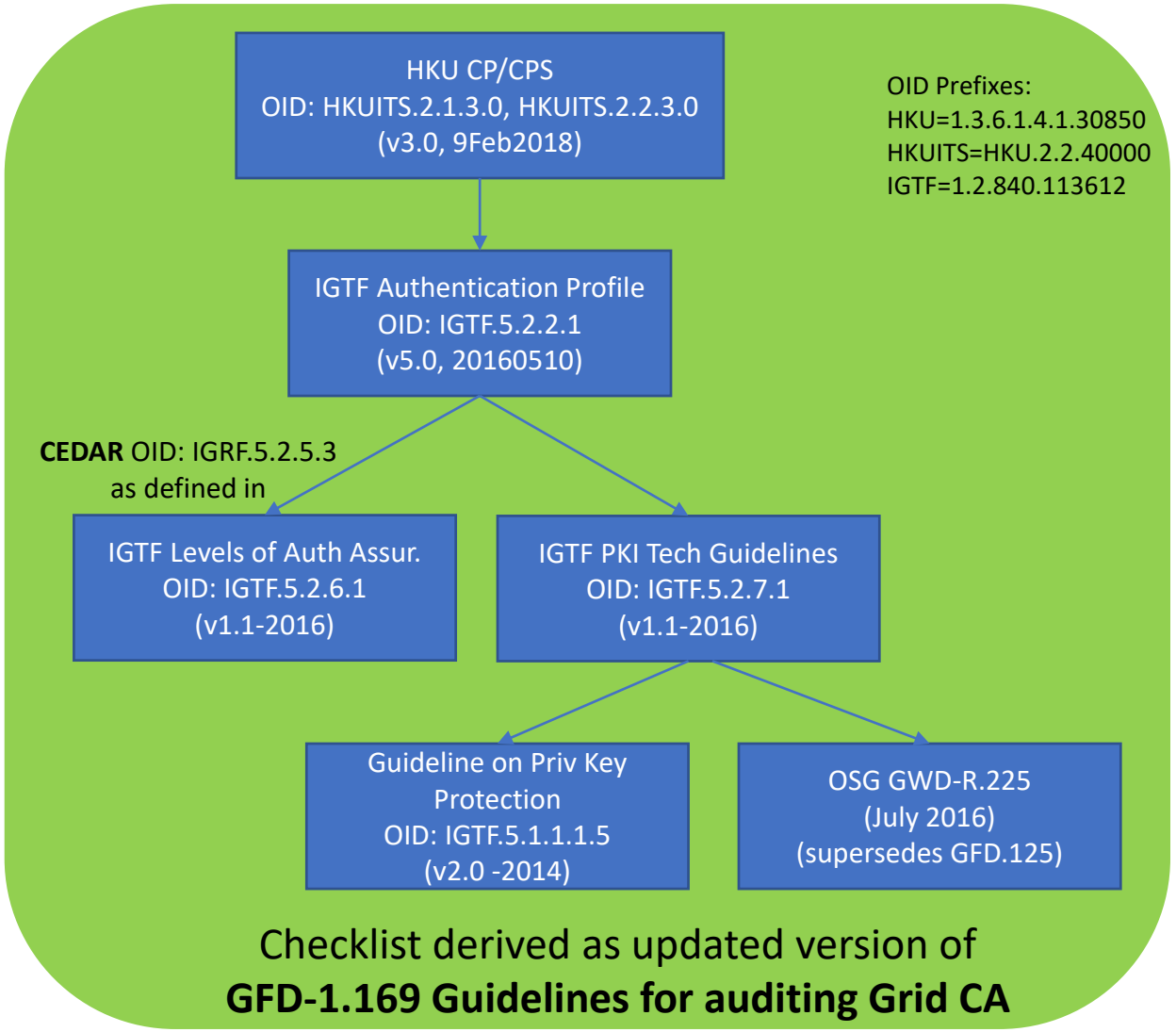
Issued Certificates

(As of 20th March, 2023)			
HKU GridCA 2	User Certificates	Valid	3
		Expired/Revoked	24
	Host Certificates	Valid	46
		Expired/Revoked	115

The previous root certificate “HKU GridCA” retired in 2019.
Physical machine are disposed, but the hard disks are stored in safe location.
Planned to be destroyed **this year**.

Materials Used for Auditing

- Guidelines for auditing Grid CAs version 1.1
- Relevant IGTF Authentication Profile version 5.0
- HKU Grid CA CP/CPS v3.0 (RFC 3647)
- CA Repository:
  - http://ca.grid.hku.hk/
  - CA Certificate, CRL, End-Entity certificates
- Document published on the web repository:
  - Certificate application procedure
  - Certificate renew and revocation procedure



Footnote: GFD-1.169 is at v1.0 but the checklist in Excel form was updated and called “v1.1”

Operation Inspection Items

- CA room
  - Located in HKU ITS server room.
  - Access restricted to authorized persons and all events are recorded.
- RA and CA machines
  - Both are running on dedicated machines.
  - CA signing machine is dedicated to CA operation and is completely offline.
- Backup media of the CA private key and its place
- Media storage of archived logs and other documents and their place
  - Locked in safe deposit box which is located at another room where access control is restricted.
- Logs of RA and CA servers
- Records of operation of the RA and CA
- Access log on the CA room

Summary of Self Audit Result

Score A (Good)	71
Score B (Minor Change)	2
Score C (Major Change)	0
Score D (Must Change)	0
Score X (Could not evaluate)	3

Items with Result "B"

- CA-(5): Whenever there is a change in the CP/CPS the OID of the document **must** change.

- Current Situation: Section 9.2: New OID will be assigned to major changes and will not be assigned to minor changes.

Items with Result "B"

- CA-(6): All versions of the CP/CPS under which valid Certificates are issued **must** be available on the web.

- Current Situation: Requirement met but not guaranteed by CP/CPS

Thank You