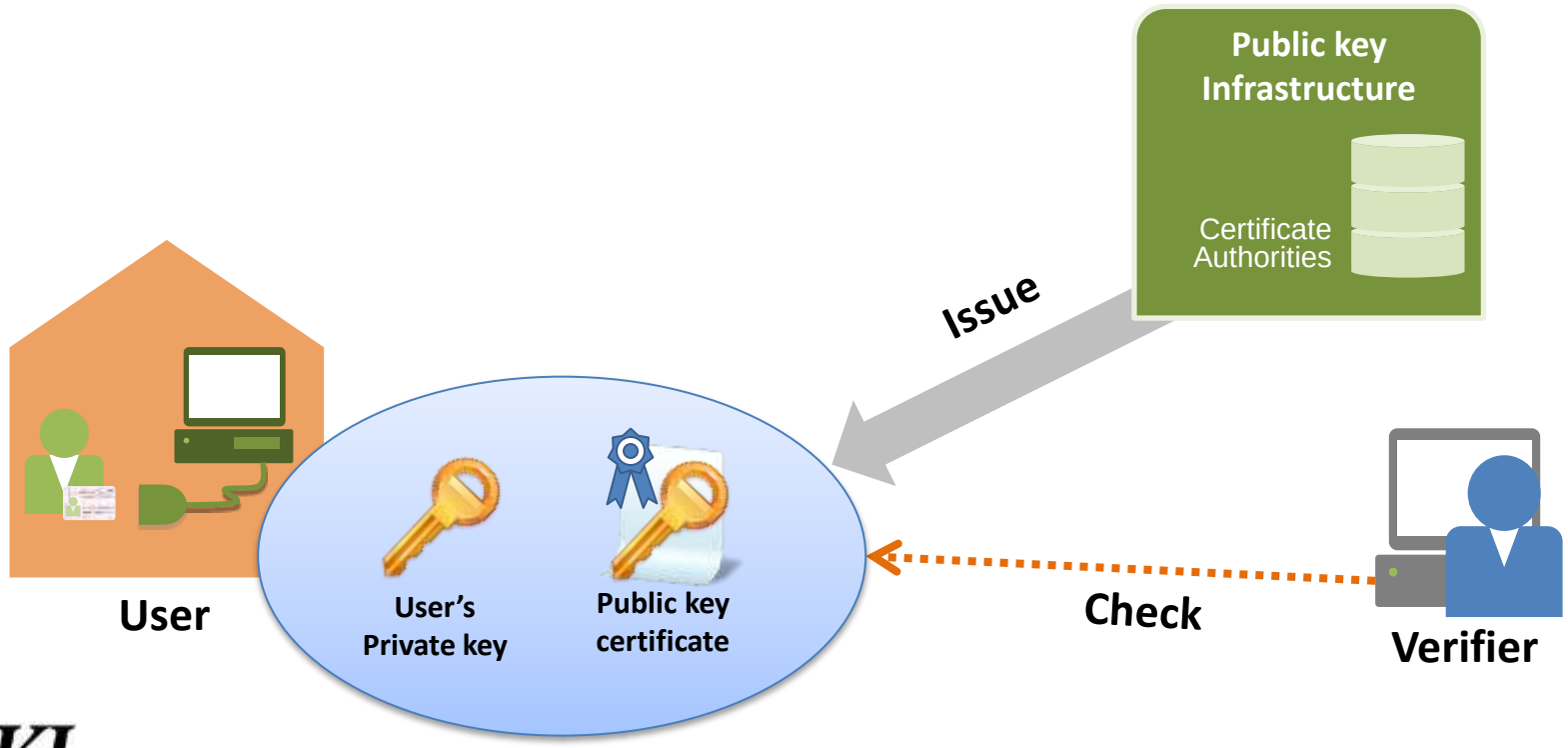
Public Key Infrastructure in Georgia

DAVID KURDGELAIDZE

David.Kurdgelaidze@cra.gov.ge

What is PKI?

A PKI (Public Key Infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange sensitive data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.



Why we need PKI?

For issuing eID we need PKI.
Each eID card included two certificates:

- **Authentication CA;**
- **Signing CA**

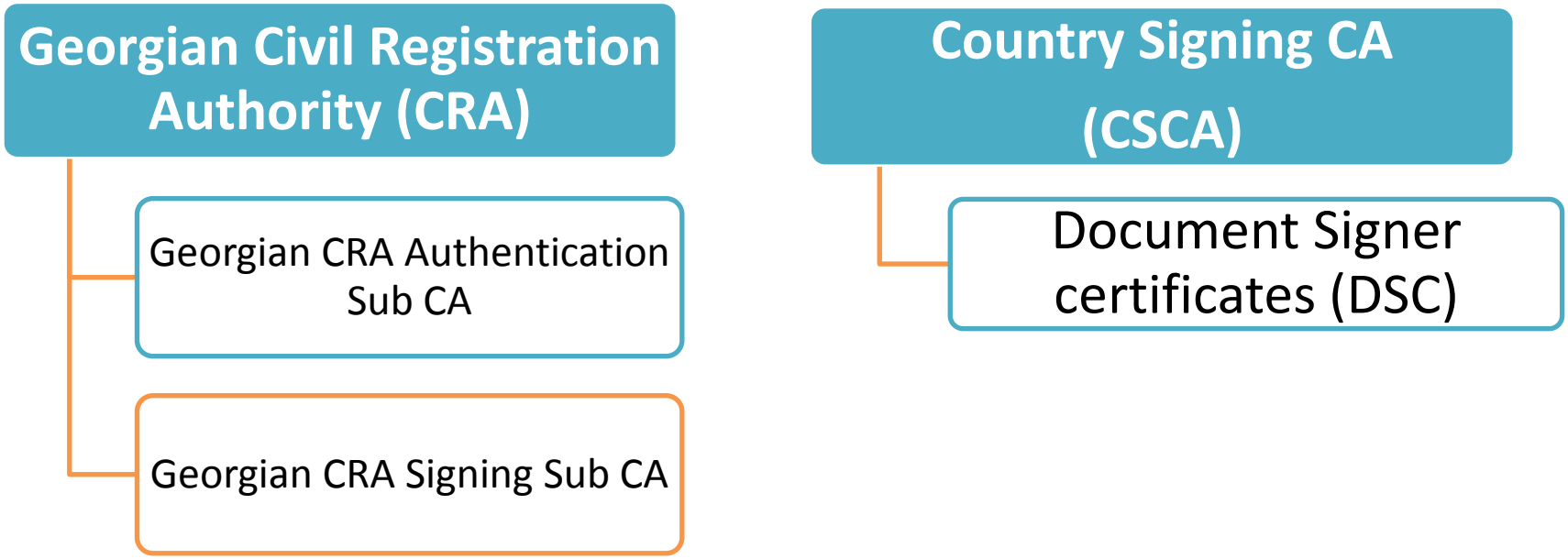
During printing of eID must be Country Signing CA (CSCA), that issues Document Signer certificates (DSC).

- **DSC provided personal data security and integrity.**

Certificate Authorities hierarchy

Certificate Authorities hierarchy

The Certificate Authorities to be installed are:



The public key infrastructure includes

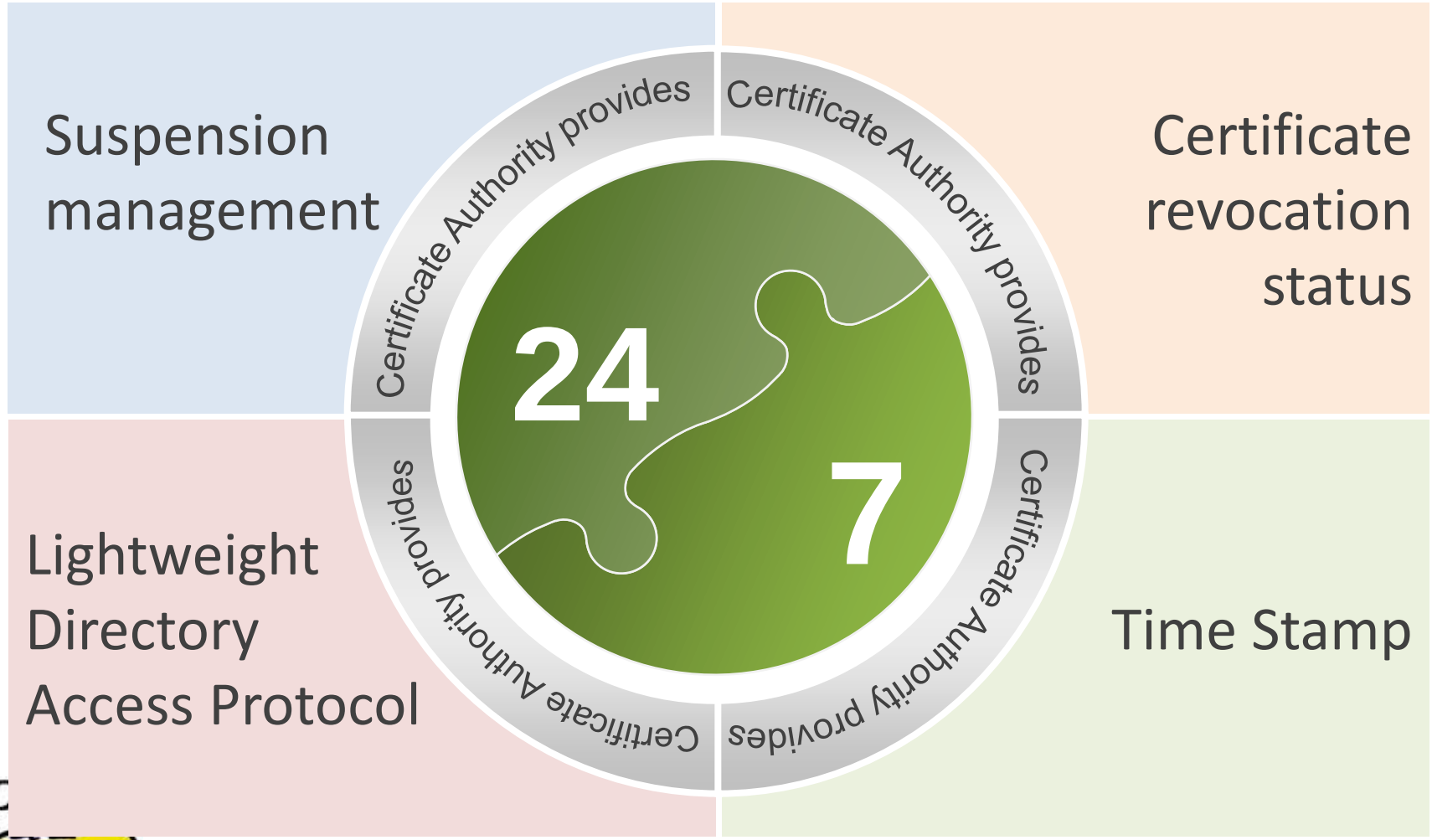
A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key

A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor

One or more directories where the certificates (with their public keys) are held

A certificate management system

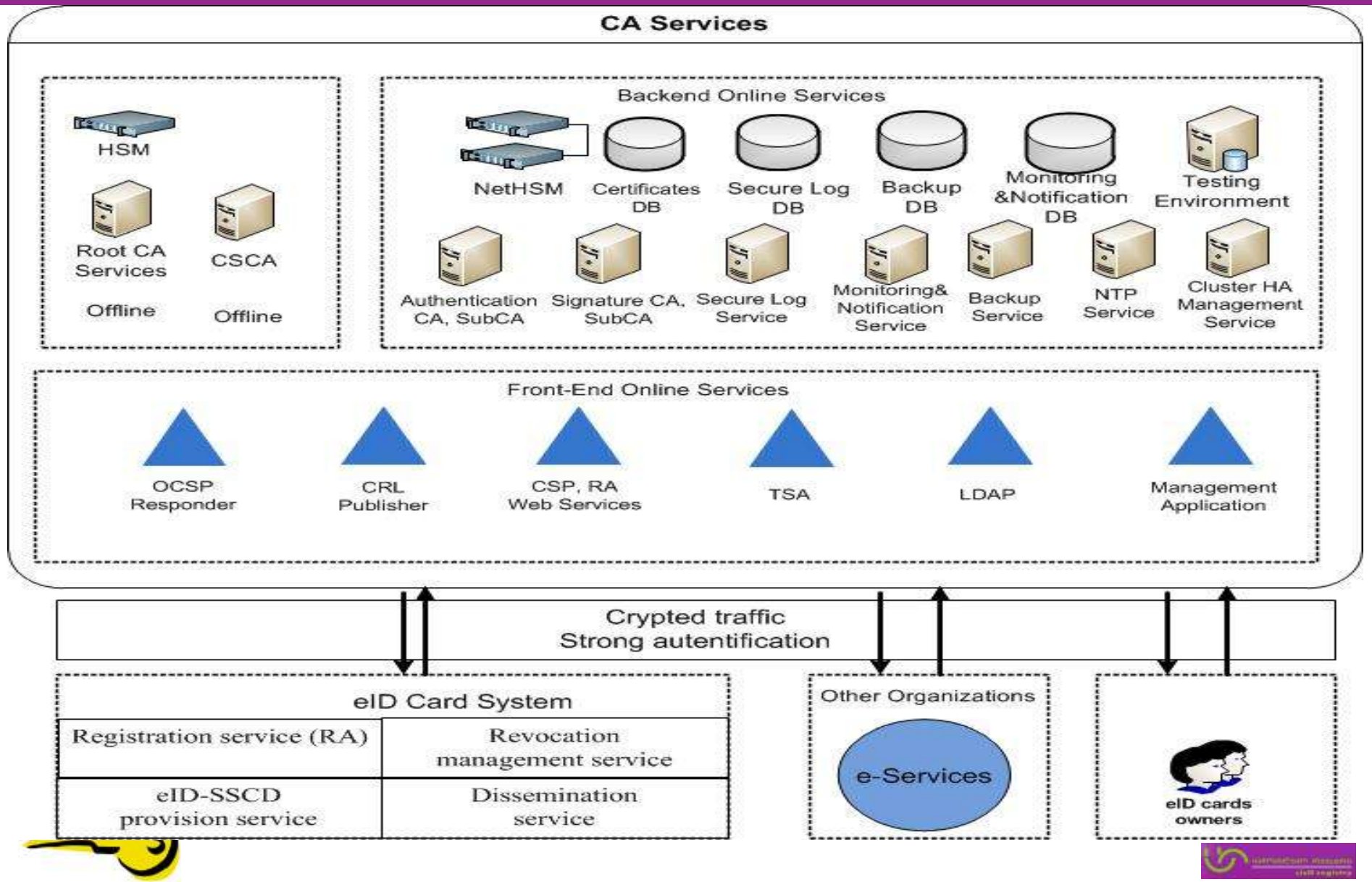
Certificate Authority provides



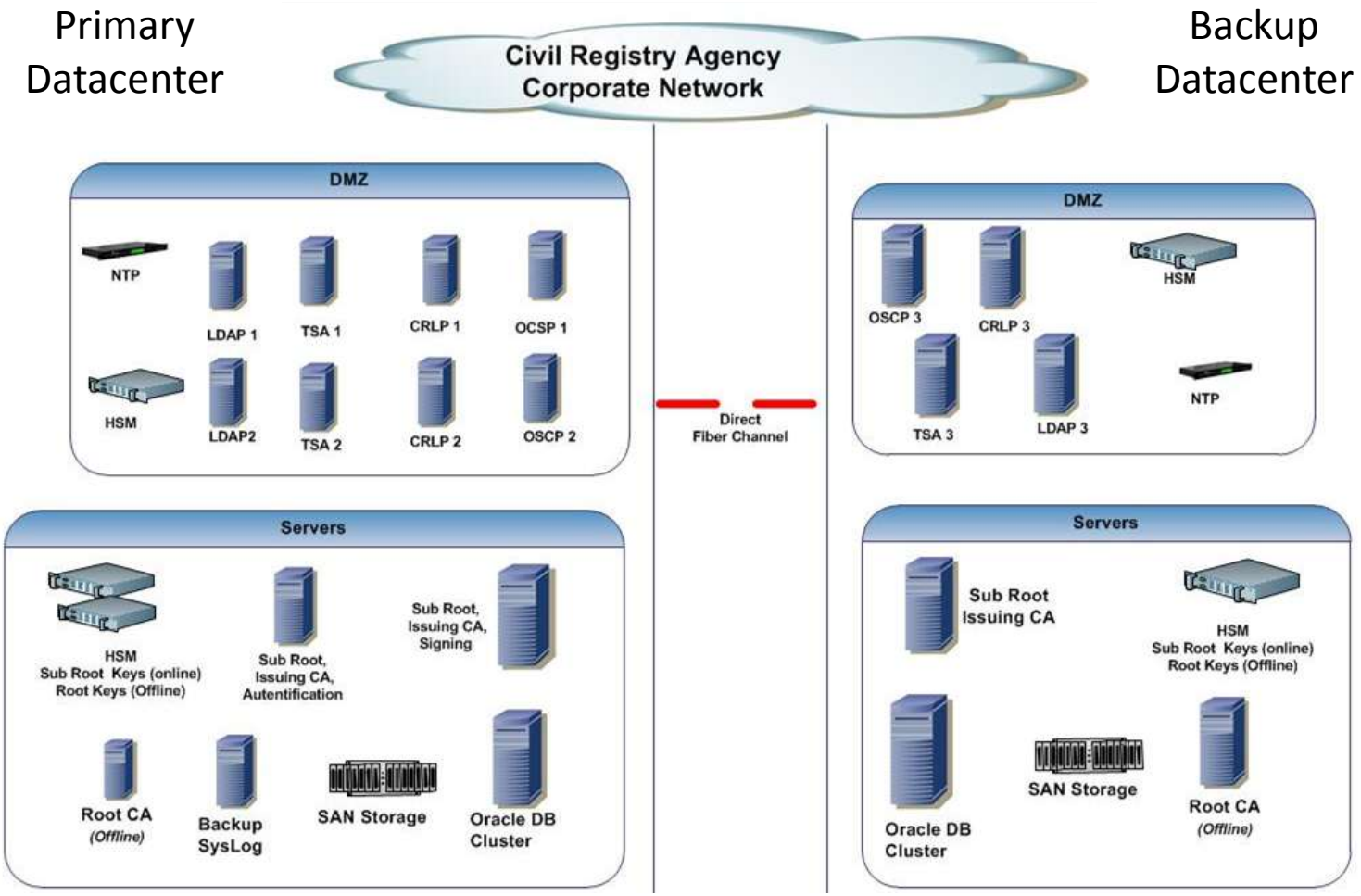
Online Services provided by CA in CRA

- eID Certificate generation services
- Revocation status: OCSP & CRL
- 24/7 suspension management service
- 24/7 Certificate revocation status service, provide both CRL and OCSP certificate revocation status services
- Time Stamp – TSA
- Lightweight Directory Access Protocol-LDAP

Certificate Authority Services



CRA's CA Infrastructure



Future Planes

- In 2 years to become a trusted CSP of Web Trust in order to be trusted in MS-Windows, Linux operational system;
- Implement Country Verification CA (CVCA) to provide ePassport verification service around the Georgia;
- To be trust from International PKI Directory;
- Implement Sub Root Servers to provide different type of the certificates;

Thank You