Education Cloud CA System
Wenshan Yang and Wuzheng Tan
Koal Software Co., Ltd, Shanghai, China

Keywords: Commercial cryptography infrastructure, Technology system, Criterion system, Detection system, Trust-internet system, Cipher application.

Abstract. This paper proposed vision and thought about Education Cloud CA System[1] [2], The cloud computing platform at the ministerial level deploys the cloud certificate certification system of the ministry of education, Certificate integrated management system, Cipher server, VPN And so on, CDS, supported by CA system, seamlessly connects with CA system to provide resource management, certificate management, terminal management, certificate issuing strategy configuration and certificate issuing statistics. CDS provides online certificate life cycle management for educational management institutions, schools and teachers in the form of cloud services.

Overall Architecture

The cloud computing platform at the ministerial level deploys the cloud certificate certification system of the ministry of education, Certificate integrated management system, Cipher server, VPN And so on system, Cipher machine provides cipher service for educational cloud CA and CDS through cloud network technology. The provincial service center communicates with the ministerial-level CA system through the VPN tunnel, and provides certificate services for the educational institutions and school users in the province.

The ministerial-level CA center and provincial-level RA center can provide certificate issuing and business handling services for institutional or school users through RA or LRA offline acceptance points. Certificates can also be issued and managed online through the CDS system.

Figure 1. Overall Architecture Sketch map

Copyright © 2019, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).
CDS, supported by CA system, seamlessly connects with CA system to provide resource management, certificate management, terminal management, certificate issuing strategy configuration and certificate issuing statistics. CDS provides online certificate life cycle management for educational management institutions, schools and teachers in the form of cloud services. Certificates are issued to support hardware media such as USBkey and TF CARDS, as well as certificate assistants on mobile terminals such as mobile phones and pads. Certificate assistants adopt hardware-based security technology and take security and convenience into consideration.

**Development Scheme**

The cloud CA system construction of the ministry of education is divided into two phases. The first phase is the construction of the ministerial-level cloud CA system, which provides certificate download and online self-service management services for national educational institutions, schools and education users; The second phase includes provincial RA system, education management institution RA system, institutions of higher learning RA system and higher vocational/secondary vocational college RA system. After completion, each RA system will provide certificate download and certificate online self-service management services for the unit and its subordinate units. The following is the content of phase I construction:

**Logical Structure**

The cloud CA of the ministry of education carries out the system structure design in accordance with the relevant requirements of the PKI system. In terms of the certificate business process, it adopts the method of external service to integrate the certificate life cycle management process and business.

The construction contents include: education cloud CA system[1] [2], cloud KM system[1] [2], cloud RA system[1] [2], certificate issuing and inquiring system[1] [2], CDS and certificate acceptance point LRA system.

The education cloud CA system, as the core part of the entire e-cert certification system, is responsible for issuing certificates and CRL, and responding to requests made by other modules. The issuing system plays a leading role in the whole e-cert certification system and enjoys a high level of security.

The cloud KM system provides the key service for the cloud CA system. It is the key generation and management organization of double-certificate users and realizes the key management based on the SM2 algorithm. It has the same or higher security level as the issuing system.

The cloud CA system, as the core part of the entire e-cert certification system, is responsible for issuing certificates and CRL, and responding to requests made by other modules. The issuing system plays a leading role in the whole e-cert certification system and enjoys a high level of security.

RA certificate registration system as a certificate application registration, audit institutions, is an important part of the system, can complete the user application information input, audit, query and
other management functions. Mainly provide certificate operation service for Intranet users.

Comprehensive management system to provide the resources management certificate, certificate management, terminal management, issuance policy configuration, issuance statistics, provide detailed certificate life cycle management, according to choose the deployment in the network or the net outside, supported by a CA system, the seamless docking with the CA system, support the traditional USBkey, TF card hardware such as media and mobile phone, PAD, and other forms of mobile software certificate storage way; The LRA and the RA certificate registration system have the same functions, and provide services for Intranet certificate users, which can be deployed according to the actual needs.

The publishing system is responsible for interacting with the end user and providing a query download service for the user's public key certificate and certificate revocation list (CRL). The certificates and CRL are published in a lightweight directory server supporting x.500 protocol standard, which adopts the technology of LDAP and LDAP distribution point to provide external authentication blacklist service. The directory service system is constructed in a master-slave manner, and the service is provided externally by the slave directory service system.

Online certificate status query system (OCSP) mainly provides real-time and online certificate status query service for certificate-based business systems.

**Network Topology**

In education within the cloud computing platform education cloud CA system deployment, CDS, and certificate issuing and online query service system, using the cloud to logical partitioning of network, network technology using firewall Settings access control policy between different areas, using the cloud platform security mechanism, guarantee the security of the CA system of cloud to cloud service mode of the national education management institutions and schools provide certificate service. Schematic diagram of system deployment network topology is as follows:

KM, CA and RA systems use cloud network technology to directly connect with the server logic of private cipher machine. CDS provides users with online certificate download and online certificate management services. SLDAP/OCSP and single sign-on gateway provide users with certificate query and authentication services.

All educational institutions, schools and education users across the country can obtain digital
certificates through offline certificate acceptance points or CDS online certificate download form. Online support USBkey, TF card and mobile terminal certificate assistant form certificate download and certificate management. The use of the USBkey certificate is consistent with the original educational management information system identity authentication.

**Differences from Norms**

GM/T 0034-2014 certificate authentication system password and related security technical specifications based on SM2 cryptographic algorithm.


**Physical Security: Electromagnetic Shielding**

**The Differences.** In the cloud room mode, the drift characteristics of host devices will increase the uncontrollability of many hosts. And the cloud center IDC room of electromagnetic leakage measures can not meet the requirements of the specification.

**Considering Solution.** (1) Shielding machine room shall be constructed according to the specifications

The advantages are that the shielding effect can meet the requirements, strict management; The downside is that when cloud centers migrate, they need to be rebuilt.

(2) Adopt shielding cabinet

Advantages are easy to move, reusable, small capital investment; The disadvantage is that the shielding effect is slightly worse than that of the shielding room. It can only meet the level C requirements of bmb19-2006 "technical requirements and test methods of electromagnetic leakage emission shielding cabinet", and cannot achieve the requirements of double doors. The management needs to rely on monitoring and other facilities in the cloud center.

**Physical Security: Divide the Area**

**The Differences.** Due to the characteristics of cloud computing, the system drifts in the cloud environment, and the region is divided into logical divisions, which cannot be physicalized or identified.

**Considering Solution.** By using virtual firewall to realize network layer, the layered deployment of the system can be guaranteed, and the database and business software can be deployed separately. With the help of multi-tenancy and virtual firewall, the uniqueness of the connection between database and business software can be guaranteed. Encryption machine is separately deployed in the shielding cabinet, with the help of the network firewall to achieve the uniqueness of the connection between business software and encryption machine, forming a logical area.

**Network Security**

**The Differences.** Due to the characteristics of cloud computing, the virtualization deployment of network equipment and network security equipment belongs to the basic technical route of the cloud center. Therefore, the switch, firewall and intrusion detection deployed separately will be converted into virtual deployment, and the security strategy of access control will not change. But the cipher machine cannot connect directly to the server.

**Considering Solution.** The cipher machine is deployed in the shielding cabinet, and by means of firewall device access control strategy and encryption machine whitelist technology, the controllable logic pass-through connection between encryption machine equipment and CA software is realized.

**Certificate Operation Process**

**The Differences.** Cloud, largely to the Internet application certificate for the CA system and the traditional CA counter each user identity real-name audit process is different, the Internet application is to provide bulk user data in advance, according to the business of real-time elastic to
provide timely and certificate business, the traditional CA system based on the individual one by one approval process appeared a lot of limitations.

**Safety Management System**

**The Differences.** The security management system needs to be revised according to the cloud environment mode, and the operation of the system shall be undertaken by the cloud platform and CA operation team in the trust service mode of Shared responsibility.

**Compensatory Design**

**Physical Reinforcement**

In cloud room set for the CA system drift zone, through the limit of host shift strategy, make the CA system in the process of initialization is limited within the particular cloud computer room, in the process of performance expansion, to limit the scope of the expansion and the host also will CA system involved in the host lock in a fixed room inside, so as to achieve relatively host position fixed and risk control; About CA management on the other hand, because of the strict access management of cloud room, especially the certificate for the CA system business daily management of conflict, therefore the establishment of a specialized management center, through the special line connected to the cloud room CA system, at the same time in accordance with the standards of the secret room requirements for safety design management center.

**Network Environment Reinforcement**

On the one hand, tenant isolation is adopted to separate the cloud CA system from other services on the cloud in terms of host, network, data and exchange, so as to create an independent computing environment for CA tenants. On the other hand, the virtual private network technology is adopted to integrate the cloud cipher machine equipment and management center with the CA system, strengthen the key communication process, and isolate the network through the security group firewall technology.

**Business Process Hardening**

Users are classified into internal network users and external network users. The process of internal network users still adopts the traditional mode. After external network users provide identity certificates, they are directly accepted by CA system and online certificate service is provided.

**Management System Adjustment**

In the case of keeping the original management mode unchanged, the system requirements for cloud platform management should be increased, especially the institutional constraints on various behaviors of administrators of CA's virtual private network.

**Conclusion**

This paper proposed Education Cloud CA System, The cloud computing platform at the ministerial level deploys the cloud certificate certification system of the ministry of education, Certificate integrated management system, Cipher server, VPN And so on, CDS, supported by CA system, seamlessly connects with CA system to provide resource management, certificate management, terminal management, certificate issuing strategy configuration and certificate issuing statistics. CDS provides online certificate life cycle management for educational management institutions, schools and teachers in the form of cloud services.

**Reference**