ISSN 2962–5688
Website :
jurnal.umj.ac.id/index.php/TripleA
Email : triplea@umj.ac.id

TRIPLE A
Jurnal Pendidikan Teknologi Informasi

PENERAPAN KONFIGURASI DASAR PKI DUA TINGKAT: ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS)

Mahbubul Wathoni[1*)], Rabiatul Nurhasanah [*)], Deva Shela[3*)]
[1,2,3)]Pendidikan Teknologi Informasi, Fakultas Ilmu Pendidikan, Universitas Muhammadiyah Jakarta, Jl. K.H. Ahmad Dahlan, Cireundeu, Kec. Ciputat Timur., Kota Tangerang Selatan, Banten 15419

[*]*mahbubul.wathoni@umj.ac.id*

ABSTRACT

The two-tier hierarchy of public key infrastructure (PKI) is a system for managing and distributing digital certificates and public key encryption. In a PKI hierarchy, there are typically two levels of certification authority (CA): the root CA at the top level and one or more intermediate CAs at the root kedua.CA level are the highest level of trust in the PKI hierarchy. It issues a self-signed certificate that is used to certify the intermediate CA. Intermediate CAs, in turn, issue certificates to end entities such as individuals or devices. In a two-tier PKI hierarchy, the root CA is typically offline and stored in a secure location, whereas the intermediate CA is online and handles the day-to-day task of issuing and revoking certificates. This separation of duties helped ensure the security and integrity of the PKI hierarchy. There are several benefits to using a two-tier PKI hierarchy. This allows for greater flexibility and scalability, as it is easier to add additional intermediate CAs as needed. It also provides a higher level of security, as the root CA is not directly connected to the network and is less vulnerable to attacks.
Keywords*: Cryptography , Public Key Infrastructure, Certificate Authority, Cryptography, Information Technology*

ABSTRAK

Hierarki infrastruktur kunci publik (PKI) dua tingkat adalah sistem untuk mengelola dan mendistribusikan sertifikat digital dan enkripsi kunci publik. Dalam hierarki PKI, biasanya ada dua tingkat otoritas sertifikasi (CA): CA root di tingkat atas dan satu atau lebih CA menengah di tingkat kedua. CA akar adalah tingkat kepercayaan tertinggi dalam hierarki PKI. Ini mengeluarkan sertifikat yang ditandatangani sendiri yang digunakan untuk mengesahkan CA perantara. CA perantara, pada gilirannya, menerbitkan sertifikat untuk entitas akhir seperti individu atau perangkat. Dalam hierarki PKI dua tingkat, CA root biasanya offline dan disimpan di lokasi yang aman, sedangkan CA perantara sedang online dan menangani tugas sehari-hari untuk menerbitkan dan mencabut sertifikat. Pemisahan tugas ini membantu memastikan keamanan dan integritas hierarki PKI. Ada beberapa manfaat menggunakan hierarki PKI dua tingkat. Ini memungkinkan fleksibilitas dan skalabilitas yang lebih besar, karena lebih mudah untuk menambahkan CA perantara tambahan sesuai kebutuhan. Ini juga memberikan tingkat keamanan yang lebih tinggi, karena CA root tidak terhubung langsung ke jaringan dan kurang rentan terhadap serangan.
Kata Kunci: *Kriptografi, Infrastruktur Kunci Publik, Otoritas Sertifikat, Kriptografi, Teknologi Informasi*

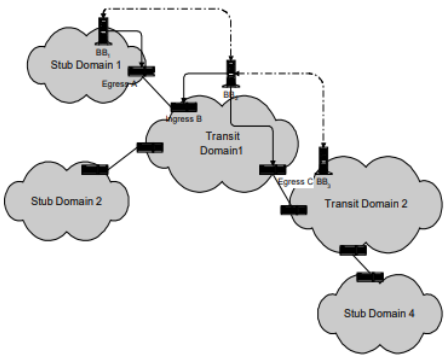
DOI:https://

PENDAHULUAN

Hierarki *Public Key Infrastructure* (PKI) dua tingkat adalah sistem untuk mengelola dan mendistribusikan sertifikat digital dan enkripsi kunci publik. Dalam hierarki PKI, biasanya ada dua tingkat otoritas sertifikasi (CA): CA root di tingkat atas dan satu atau lebih CA menengah di tingkat kedua.

CA akar adalah tingkat kepercayaan tertinggi dalam hierarki PKI. Ini mengeluarkan sertifikat yang ditandatangani sendiri yang digunakan untuk mengesahkan CA perantara. CA perantara, pada gilirannya, menerbitkan sertifikat untuk entitas akhir seperti individu atau perangkat. Dalam hierarki PKI dua tingkat, CA root biasanya offline dan disimpan di lokasi yang aman, sedangkan CA perantara sedang online dan menangani tugas sehari-hari untuk menerbitkan dan mencabut sertifikat. Pemisahan tugas ini membantu memastikan keamanan dan integritas hierarki PKI.

Ada beberapa manfaat menggunakan hierarki PKI dua tingkat. Ini memungkinkan fleksibilitas dan skalabilitas yang lebih besar, karena lebih mudah untuk menambahkan CA perantara tambahan sesuai kebutuhan. Ini juga memberikan tingkat keamanan yang lebih tinggi, karena CA root tidak terhubung langsung ke jaringan dan kurang rentan terhadap serangan.



Gambar 1. Two-Tier Hierarchy

TINJAUAN PUSTAKA

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) adalah sistem manajemen kunci publik yang mengelola daftar penting kunci publik dan memastikan keandalannya, biasanya untuk entitas dalam jaringan. PKI memungkinkan kunci publik ditautkan ke identitas (seperti nama pengguna atau organisasi). PKI memberikan jaminan bahwa kunci publik yang diperoleh melaluinya dapat dipercaya *secara apriori*, tetapi itu bukan CA. Arsitektur dapat didasarkan pada otoritas sertifikasi tetapi juga dapat menggunakan mekanisme lain seperti blockchain. PKI mengelola siklus hidup sertifikat keamanan untuk mengaitkan entitas dengan kunci publik. Ini menanggapi permintaan untuk verifikasi sertifikat dan mengelola pencabutan sertifikat.

Active Directory (AD)

Ada banyak komponen yang terlibat dalam menjalankan jaringan berbasis sertifikat. Anda perlu membuat server tepercaya dan otoritas sertifikat (CA), memastikan perangkat dapat mendaftar untuk sertifikat, mengautentikasi pengguna, mengelola siklus hidup sertifikat, mengelompokkan pengguna untuk kebijakan grup yang berbeda, dan banyak lagi.Microsoft menawarkan CA mereka sendiri sehingga lingkungan berbasis Microsoft dapat menerapkan Infrastruktur Kunci Publik (PKI). PKI menjadi lebih populer di bidang keamanan jaringan karena mereka memungkinkan alur kerja elektronik dan menyediakan server SSL dan keamanan email, hanya untuk menyebutkan beberapa.

Certificate Authority

Dalam kriptografi, Certificate Authority (CA) adalah unit yang menerbitkan sertifikat digital untuk digunakan oleh pihak lain.

Certificate Authority adalah pihak tepercaya yang terpasang di semua perangkat keras dan perangkat lunak yang memerlukan komunikasi aman antara klien dan server. PKI mengikuti struktur hierarkis dengan dua jenis otoritas sertifikat: CA root dan CA intermediate. CA yang lebih tinggi dalam hierarki diberi wewenang untuk mengeluarkan sertifikat ke CA lain yang lebih rendah dalam hierarki, untuk memungkinkan CA yang lebih rendah dalam hierarki untuk menerbitkan sertifikat kepada pengguna. Certificate Authority biasanya dipilih oleh vendor aplikasi atau sistem operasi. Sistem PKI terdiri dari beberapa komponen, termasuk CA, registration authority, direktori untuk menyimpan dan mengindeks kunci dan sertifikat, dan sistem manajemen sertifikat.

Domain Name System (DNS)

DNS adalah elemen dasar komunikasi IP, yang merupakan salah satu protokol paling terkenal di Internet. DNS juga menyediakan alat untuk meningkatkan kegunaan aplikasi IP, misalnya mencegah pengguna memasukkan alamat IP secara langsung ke aplikasi seperti browser web dan mengizinkan server web untuk melayani halaman web yang disusupi dengan berbagai konten tertaut. Untuk berkomunikasi melalui jaringan IP, perangkat IP harus mengirim paket IP ke tujuan yang dituju; dan setiap header paket IP memerlukan alamat IP sumber dan tujuan. DNS juga memiliki fungsi utama menerjemahkan nama domain yang dapat dibaca manusia ke alamat IP yang sesuai, proses terjemahan dilakukan dengan DNS query antara client dan server DNS (resolver).

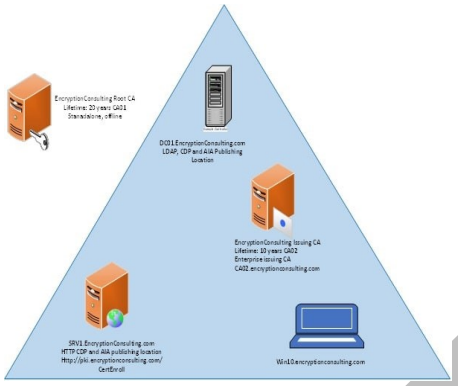
Certificate Revocation List (CRL)

Certificate Revocation List (CRL) adalah daftar berstempel waktu di mana semua informasi sertifikat yang telah dicabut atau digantung terdaftar, dikeluarkan oleh otoritas sertifikasi CA dan diterbitkan secara berkala. CRL berisi dua bidang: tanggal pembaruan saat ini dan tanggal pembaruan berikutnya. Pengguna dapat menentukan apakah CRL saat ini adalah yang terbaru dari dua informasi tanggal, dan CRL berisi tanda tangan CA. Jadi CRL dapat disimpan di node mana pun di jaringan. Untuk memeriksa validitas sertifikat, pemverifikasi memulai permintaan ke server direktori LDAP yang menghosting CRL yang sesuai dengan parameter pengidentifikasi CA yang mengeluarkan sertifikat.

METODE PENELITIAN

Ada lima komputer/mesin yang terlibat dalam lab hierarki PKI dua tingkat ini.

1. Ada satu pengontrol domain (DC01) yang juga menjalankan Layanan Nama Domain (DNS) terintegrasi Direktori Aktif. Komputer ini juga akan menyediakan lokasi Lightweight Directory Access Protocol (LDAP) untuk CDP dan titik AIA untuk konfigurasi PKI.
2. Satu CA Root Offline Mandiri (CA01).
3. CA Penerbit Satu Perusahaan (CA02).
4. Satu Server Web (SRV1) (HTTP CDP/AIA) dan
5. Satu komputer Klien Windows 10 (Win10).



Gambar 2. Root AD DS

Virtual Machine	Roles	OS Type	IP Address	Subnet mask	Preferred DNS server
DC01.encryption con- pti.com	DC & DNS - LDAP CDP/AIA	Windows Server 2019	192.168.1.10	255.255.255.0	192.168.1.10
CA01	Standalone Offline Root CA	Windows Server 2019	NA	NA	NA
CA02.encryption con- pti.com	Enterprise Issuing CA	Windows Server 2019	192.168.1.12	255.255.255.0	192.168.1.10
SRV1.encryption con- pti.com	Web Server - HTTP CDP/AIA	Windows Server 2019	192.168.1.13	255.255.255.0	192.168.1.10
WIN10.encryptio n- pti.com	Windows Client Computer	Windows 10	192.168.1.14	255.255.255.0	192.168.1.10

Langkah Utama

Ada delapan tahap utama dalam konfigurasi dasar seperti yang tercantum di bawah ini (masing-masing mencakup beberapa subtugas).

1. Instal *Active Directory Forest*
2. Persiapkan server web untuk publikasi CDP dan AIA
3. Instal Standalone Offline Root CA
4. Lakukan langkah-langkah konfigurasi pasca penginstalan pada CA root offline mandiri
5. Instal Subordinate Issuing CA
6. Lakukan konfigurasi pasca-instalasi pada CA penerbit bawahan
7. Instal dan konfigurasikan responden online
8. Verifikasi kesehatan hierarki PKI.

HASIL DAN PEMBAHASAN

Instal *Active Directory Forest*

- Mengonfigurasi Nama Server dan Pengaturan Jaringan
- Instal forest baru dengan menggunakan Server Manager
- HTTP Web Server: Publikasi CDP dan AIA
- Instal Peran Server Web (IIS)
- Buat Folder CertEnroll dan berikan Izin Berbagi & NTFS ke grup Cert Publishers
- Buat Direktori Virtual CertEnroll di IIS
- Aktifkan Pelarian Ganda di Server IIS
- Membuat CNAME (pki. Enkripsi Pti.com) dalam DNS

Instal *Standalone Offline Root CA*

- Buat CAPolicy.inf untuk *Standalone Offline Root CA*
- Menginstal *Standalone Offline Root CA*

Lakukan konfigurasi pasca instalasi untuk Root CA

- Mengaktifkan pengauditan pada CA Akar
- Konfigurasikan AIA dan CDP
- Mengonfigurasi AIA
- Konfigurasikan CDP

Instal Perusahaan Menerbitkan CA

- Bergabunglah dengan CA02 ke domain
- Buat CAPolicy.inf untuk Enterprise Root CA
- Menerbitkan Sertifikat Root CA dan CRL
- Instal CA Penerbit Bawahan
- Kirim Permintaan dan Terbitkan EncryptionConsulting yang menerbitkan sertifikat CA
- Instal Konsultasi Enkripsi yang Menerbitkan Sertifikat CA di CA02

Melakukan tugas konfigurasi pasca instalasi pada CA penerbit bawahan

- Mengonfigurasi Pencabutan Sertifikat dan Masa Berlaku Sertifikat CA
- Mengaktifkan Pengauditan pada CA yang Menerbitkan
- Mengonfigurasi AIA
- Konfigurasikan CDP

Menginstal dan mengonfigurasi layanan peran responder online

- Instal Layanan Peran Responder Online di SRV1
- Tambahkan URL OCSP ke CA Penerbit Konsultasi Enkripsi
- Mengonfigurasi dan menerbitkan sertifikat penandatanganan respons

OCSP pada CA penerbit konsultasi enkripsi

- Mengonfigurasi konfigurasi pencabutan pada responden online
- : Konfigurasikan Kebijakan Grup untuk Menyediakan URL OCSP untuk CA Penerbit EncryptionConsulting

Verifikasi Kesehatan Hierarki PKI

- WIN10
  1. Masuk ke WIN10 sebagai administrator lokal.
  2. Klik Mulai, ketik ncpa.cpl dan tekan ENTER.
  3. Di sambungan jaringan, klik kanan sambungan area lokal dan kemudian klik Properti.
     - Jika ada lebih dari satu ikon Local Area Connection di Network Connections, Anda ingin memodifikasi salah satu yang terhubung ke segmen jaringan yang dibagikan oleh semua komputer yang telah Anda instal untuk lab ini.
  4. Klik Internet Protocol Version 4 (TCP/IPv4) dan kemudian klik Properti.
  5. Pilih Gunakan alamat IP Berikut. Konfigurasikan alamat IP, Subnet mask, dan gateway Default dengan tepat untuk jaringan pengujian Anda.
     - Alamat IP: 192.168.1.14
     - Subnet mask: 255.255.255.0
     - Gateway default: <opsional>
  6. Pilih Gunakan alamat server DNS berikut. Konfigurasikan server DNS Pilihan sebagai alamat IP pengontrol domain Anda. Klik Close.
     - Server DNS pilihan: 192.168.1.10.
  7. Klik Start, ketik sysdm.cpl dan tekan ENTER. Klik Ubah. (Pastikan nama komputer sudah diatur ke WIN10 - jika tidak ubah)
  8. Di Anggota dari, pilih Domain, lalu ketik EncryptionPti.com. Klik Oke.
  9. Di Keamanan Windows, masukkan Nama pengguna dan kata sandi untuk akun administrator domain. Klik Oke.
  10. Anda akan disambut di domain EncryptionConsulting. Klik Oke.
  11. Ketika diminta bahwa restart diperlukan, klik OK. Klik Restart Now.

- Cek Kesehatan PKI dengan PKI Enterprise

  Untuk menggunakan konsol PKI Enterprise untuk memeriksa kesehatan PKI:
  1. Pada CA02. EncryptionConsulting.com, pastikan Anda masuk sebagai EncryptionConsu\Administrator.
  2. Buka Manajer Server.
  3. In pohon konsol, di bawah Peran dan Layanan Sertifikat Direktori Aktif, klik PKI Perusahaan.
  4. Alternatively, Anda dapat menjalankan Enterprise PKI dengan menjalankan PKIView.msc dari prompt perintah administratif.
  5. Klik kanan PKI Perusahaan lalu klik Kelola Kontainer AD.
  6. Verifikasi sertifikat CA Penerbit EncryptionConsulting muncul dengan status OK.
  7. Pada tab AIA Container, verifikasi bahwa sertifikat EncryptionConsulting Root CA

dan EncryptionConsulting Issuing CA hadir dengan status OK.

8. Pada tab Kontainer CDP, verifikasi EncryptionConsulting Root CA base CRL, EncryptionConsulting Issuing CA base, dan Delta CRLs hadir dengan status OK.
9. Pada Wadah Otoritas Sertifikasi, verifikasi sertifikat EncryptionConsulting Root CA hadir dengan status OK.
10. Pada Kontainer Layanan Pendaftaran, verifikasi sertifikat CA Penerbitan EncryptionConsulting hadir dengan status OK.

- Mengonfigurasi distribusi sertifikat pada CA penerbit konsultasi enkripsi
  Untuk menerbitkan sertifikat untuk komputer di perusahaan:
  1. Pada CA02. EncryptionConsulting.com, pastikan Anda masuk sebagai EncryptionConsu\Administrator.
  2. In konsol Certification Authority, pastikan EncryptionConsulting Issuing CA diperluas.
  3. Klik kanan Template Sertifikat pilih Baru dan pilih Template Sertifikat untuk Diterbitkan.
  4. Pada kotak dialog Aktifkan Template Sertifikat, klik Workstation Authentication, halaman dan kemudian klik OK.

- Dapatkan Sertifikat Menggunakan WIN10 dan Verifikasi PKI Health
  Untuk mendapatkan sertifikat untuk WIN10 dan memverifikasi kesehatan PKI:
  1. Masuk ke Win10. EncryptionPti.com sebagai EncryptionPti\Administrator. (Pastikan Anda mengalihkan pengguna untuk masuk sebagai EncryptionConsu\Administrator)
  2. Klik Mulai, ketik mmc lalu tekan ENTER.
  3. Klik File, lalu klik Tambah/Hapus Snap-in

SIMPULAN

Berikut adalah simpulan yang dapat ditarik dari penilitian ini:

1. Hierarki *Public Key Infrastructure* (PKI) dua tingkat adalah sistem untuk mengelola dan mendistribusikan sertifikat digital dan enkripsi kunci publik. Dalam hierarki PKI, biasanya ada dua tingkat otoritas sertifikasi (CA): CA root di tingkat atas dan satu atau lebih CA menengah di tingkat kedua.
2. *Public Key Infrastructure* (PKI) adalah sistem manajemen kunci publik yang mengelola daftar penting kunci publik dan memastikan keandalannya, biasanya untuk entitas dalam jaringan. PKI memungkinkan kunci publik ditautkan ke identitas (seperti nama pengguna atau organisasi).
3. Dalam kriptografi, Certificate Authority (CA) adalah unit yang menerbitkan sertifikat digital untuk digunakan oleh pihak lain
4. DNS adalah elemen dasar komunikasi IP, yang merupakan salah satu protokol paling terkenal di Internet.
5. Certificate Revocation List (CRL) adalah daftar berstempel waktu di mana semua informasi sertifikat yang telah dicabut atau digantung terdaftar, dikeluarkan oleh otoritas

sertifikasi CA dan diterbitkan secara berkala. CRL berisi dua bidang: tanggal pembaruan saat ini dan tanggal pembaruan berikutnya.

6. Ada delapan tahap utama dalam konfigurasi dasar seperti yang tercantum di bawah ini (masing-masing mencakup beberapa subtugas).
   - Instal Active Directory Forest
   - Persiapkan server web untuk publikasi CDP dan AIA
   - Instal Standalone Offline Root CA
   - Lakukan langkah-langkah konfigurasi pasca penginstalan pada CA root offline mandiri
   - Instal Subordinate Issuing CA
   - Lakukan konfigurasi pasca-instalasi pada CA penerbit bawahan
   - Instal dan konfigurasikan responden online
   - Verifikasi kesehatan hierarki PKI

DAFTAR PUSTAKA

Berger, Harel dkk. 2021. "A wrinkle in time: a case study in DNS poisoning". *International Journal of Information Security*. Vol. 20 No. 3, p313-329

Bhutta, Muhammad Nasir Mumtaz dkk. 2016. "Public-key infrastructure validation and revocation mechanism suitable for delay/ disruption tolerant networks" . *IET Information Security*. Vol. 11 No. 1, pp. 16-22.

Chaganti, Ravikanth. 2018. *Pro PowerShell Desired State Configuration : An In-Depth Guide to Windows PowerShell DSC.* New York: Apress.

Dauti, Bekim. 2019. *Windows Server 2019 Administration Fundamentals : A Beginner's Guide to Managing and Administering Windows Server Environments*. Birmingham : Packt Publishing.

Dauti, Bekim. 2022. *Windows Server 2022 Administration Fundamentals : A Beginner's Guide to Managing and Administering Windows Server Environments*. United Kingdom : Packt Publishing.

Flaus, Jean-Marie. 2019. *Cybersecurity of Industrial System*. London : John Wiley & Sons, Ltd.

Hughes, Laurance E. 2022. Pro Active *Directory Certificate Services: Creating and Managing Digital Certificates for Use in Microsoft Networks Kindle Edition*. New York : Apress.

Maulani, Gindari dkk. 2021. Digital Certificate Authority with Blockchain Cybersecurity in Education"". *International Journal of Cyber and IT Service Management (IJCITSM*). Vol. 1.

Mirosnikov, Andrei. 2018. *Windows Security Monitoring : Scenarios and Patterns*. Indianapolis : Wiley.

Moiso, Corrado & Matteo Petracca. 2019. "PKIoT: A public key infrastructure for the Internet of Things". *Transactions on Emerging Telecommunications Technologies*. Vol. 30 No. 10.

Rooney, Timothy & Michael Dooley. 2017. *DNS Security Management*. London : John Wiley & Sons, Ltd.

Sermpinis, Thomas dkk.2020. "DeTRACT: a decentralized, transparent, immutable and open PKI certificate

framework". *International Journal of Information Security*. Vol. 20 No 4, p553-570. 18p.

Schareer, Jacob dkk. 2021. Veritaa: A distributed public key infrastructure with signature store. *International Journal of Network Management*. Vo. 32 No. 2.

Sayfan, Gigi. 2019. *Hands-On Microservices with Kubernetes : Build, Deploy, and Manage Scalable Microservices on Kubernetes*. Birmingham : Packt Publishing.

Xie, Jingxue dkk. 2022. "CR-BA: Public Key Infrastructure Certificate Revocation Scheme Based on Blockchain and Accumulator". *Security & Communication Networks*. Volume: 2022 (2022).