**MIDTERM PROJECT: REPORT**

**Prof. Kristen Macdonald**

Group 4

**Contents**

[**Overview** 3](#_Toc137063054)

[**Benefits and Drawbacks of PKI infrastructure** 3](#_Toc137063055)

[**Best practises** 4](#_Toc137063056)

[**Why implement this technology?** 4](#_Toc137063057)

[**Consideration for MOJO Inc** 5](#_Toc137063058)

[1. Two-tier hierarchy 5](#_Toc137063059)

[2. Enterprise CA 7](#_Toc137063060)

[3. Auditing 7](#_Toc137063061)

[4. Autoenrollment 8](#_Toc137063062)

[**References** 10](#_Toc137063063)

# **Overview**

For secure digital communication and data security, cryptographic technologies like Certificate Services and Public Key Infrastructure (PKI) are used. The management and distribution of digital certificates which act as the digital identities of entities are part of certificate services. To confirm the legitimacy and integrity of digital communication, these certificates are issued by a reputable Certificate Authority (CA). An organisation that you can trust, referred to as a certificate authority or certification authority, validates websites and other entities so that you always know with whom you are dealing with. Their goal is to increase both user and organisation security on the internet. This indicates that they are crucial to digital security. The infrastructure that supports the production, transfer, and administration of digital certificates is PKI.

It makes use of asymmetric cryptography, in which each entity has a set of public and private keys. While the private key is kept secret, the public key is widely distributed. A chain of trust is created by PKI by building a hierarchy of CAs that issue and sign certificates. Secure web communication, email security, and other applications needing secure authentication and data integrity all depend on this infrastructure. Organizations may build trust, safeguard sensitive data, and abide by legal obligations by adopting these technologies correctly and following best practices. This eventually improves their entire security posture in the digital environment.

**Benefits and Drawbacks of PKI infrastructure**

**Pros:**

* The PKI’s helps in providing secure method of exchanging data over the internet by authenticating the user.
* The PKI primarily offers methods for user, user system, or organization authentication via digital certificates or independent CAs.
* The PKI’s help in authenticating the authenticity of a particular transaction.
* Encryption is used by the PKI to facilitate secure communication while ensuring privacy and safeguarding against threats.

**Cons**:

* PKI implementation and management are difficult and time-consuming tasks that demand skilled individuals with experience.
* As there are many certificates being made and used. It is difficult for an organization handle or control manually all these certificates.
* The PKI infrastructure is challenging to establish and maintain, particularly for large organizations.
* It will take a long time and be difficult to revoke the certificate, which might leave the system open to attacks for a while.
* Microsoft Active Directory Certificate Services can be an acceptable solution for managing certificates for Windows-based servers and devices, it can not help with non-Windows devices.

**Best practises**

* The Active directory certificate services should not be kept on same server as domain controller.
* Root CAs should be kept offline and locked in a secured room.
* Enterprise CA are recommended so that automate the enrollment and issuing certificates.
* To keep track of the stored certificates, organisations must maintain a certificate inventory.
* Always stay current with security patches and protocols. To keep it secure, keep your PKI updated at all times.
* Infrastructure for public keys should never be static. It is vital to rotate and inspect certifications on a regular basis. To prevent threats, a proactive system should be in place for revocation and suspension of outdated or expired certificates.

# **Why implement this technology?**

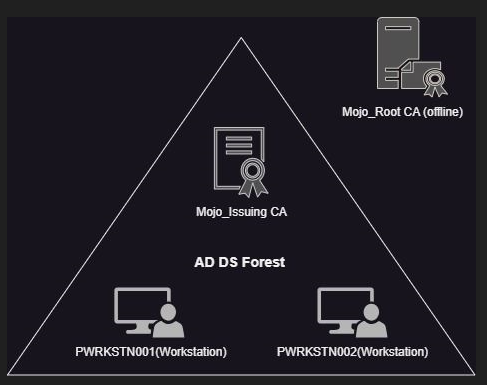
Cybersecurity is a critical component of companies’ technology infrastructures. It is a priority for any organization to protect any form of data it handles. The information that a company handles ranges from customer information or even their own intellectual property. Businesses profit significantly when there is better confidence among the many stakeholders and transparency about the cybersecurity programmes of the companies.

Machine identification lies at the core of cybersecurity strategy implementation. Digital certificates known as machine IDs are used to verify the legitimacy of machines on networks. It authenticates each application and device before providing access to communicate, assisting in the detection of outside and internal threats as well as the eradication of hostile actors' lateral movement within the network. A lifecycle of discovery, monitoring, renewals, revocation, and provisioning is often involved in managing digital certificates. By using spreadsheets and proprietary software, organisations have traditionally managed the certificate lifetime manually. The large digital footprint of today, however, has made manual certificate management more difficult. Organisations struggle to manually monitor and manage the hundreds of thousands of certificates that are dispersed across hybrid, multi-cloud, and containerized environments. As a result, certificates frequently expire, applications go down, and the danger of a cyberattack rises. Having a Public-Key Infrastructure (PKI) setup today has undeniably become the standard for authentication and encryption of data. It should be followed unquestionably by all the devices, servers, applications, and users. (*Sectigo*, n.d.)

Because PKI offers a framework and infrastructure to safeguard data, user, and device identities, and assure that the integrity of the data has remained intact and is authentic, it enhances trust on the internet. Digital certificates that confirm the identification of users, devices, or services can be issued using PKI. These certificates can be used to authenticate devices connecting to your VPN, Wiki, Wi-Fi, and other private internal services as well as public web pages.

**Consideration for MOJO Inc**

The company MOJO Inc considered for the project is a product-based company and the organization provides solutions and services to their customers, and it becomes inevitable to envision cybersecurity strategies that will ensure the protection of customer data. PKI being a standard is widely used in enterprise IT and is essential for securing communications between groups of people, teams, and organisations. MOJO Inc has opted for self-managed PKI, and it uses an internal root CA as PKI’s trust anchor. (Archiveddocs, 2016)

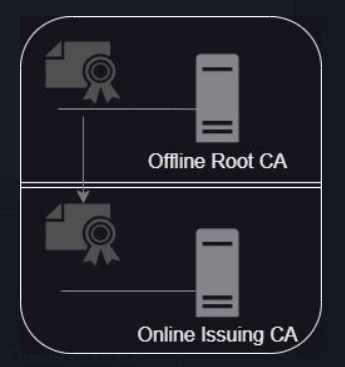


Fig(1) MOJO infrstructure

In this project below are the considerations made at the infrastructure level:

1. Two-tier hierarchy:

All our CAs are under the domain MOJOINC.domain. The two-tier hierarchy is used because it enhances the level of security as the root and issuing certificates are separated. Also, it can help the company in terms of scalability and flexibility as the company is focussing on expansion as well.



Fig(2) 2-tier hierarchy

* Root CA – MOJOROOTCA :

This server will act as a root CA which will be kept offline (in our case powered off). Keeping the root CA offline will also help in keeping the private key protected.

* Subordinate CA’s (Issuing CA) – MOJO\_IssuingCA:

In this scenario, the subordinate CA are the issuing CAs. They are used to sign end-entity certificates, such as SSL/TLS certificates for web servers, and are signed by the root certificate, which is stored safely offline. This establishes a chain of trust that extends back to the root CA, preventing the disastrous necessity of revoking every certificate ever issued by the root CA in response to the compromise of a subordinate certificate, no matter how horrible that may be.

A screenshot of a computer

Description automatically generated

Fig(3) Root and subordinate CA configuration

1. Enterprise CA:

The CA server is integrated with the Active Directory design.

1. Auditing:

Enabling auditing will give us the ability to record any activity at the certificate services end. In this case we are enabling auditing where it can log any start\stop of the certificate services, any revocation of the certificate performed, any rows deleted from the certificate database and so on. All these events will be reflected in the event logs, a few of the event ids are listed below. (Gopal, 2022)

A screenshot of a computer

Description automatically generated with low confidence

Fig(4) Sample Event ID details for auditing

*Source: serverbrain.org*

A screenshot of a computer

Description automatically generated with medium confidence

Fig(5) Auditing enabled results

1. Autoenrollment:

The issue of certificates to the Microsoft certificate store on Windows PCs and servers is automated through auto-enrollment. It is configured so that certificates to the users and devices are issued automatically without being requested and it will be a faster process.

A screenshot of a computer

Description automatically generated with medium confidence

Fig(6) Autoenrollment configured for the user cert\_1 demo

# **References**

*Sectigo*. (n.d.). <https://www.positivessl.com/uploads/resources/Whitepaper_PKI_Financial-V1.pdf>

Archiveddocs. (2016, August 31). *Securing PKI: Monitoring Public Key Infrastructure*. Microsoft Learn. <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786432(v=ws.11)?redirectedfrom=MSDN>

Gopal. (2022). Enable certification Authority Advanced Audit Filter to create a secure architecture in your organization. *Encryption Consulting*. <https://www.encryptionconsulting.com/how-to-enable-certification-authority-advanced-audit-filter>

*Enabling Auditing at the CA - Certificate Security Windows Server 2003*. (2023, February 2). Windows Server Brain. <https://www.serverbrain.org/certificate-security-2003/enabling-auditing-at-the-ca.html>