Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

5th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2024)

SEPTEMBER 5-6th, 2024

Efficient Implementation of Entity On-Boarding and Authentication in Zero-Trust Systems

Paper ID - 95

Presented by

Jayashree Rana

Author Name

Jayashree Rana(PhD Scholar), Rojalina Priyadarshini (Professor), Pramod Kumar Meher (Professor), and K Pratyush(B.tech Student)

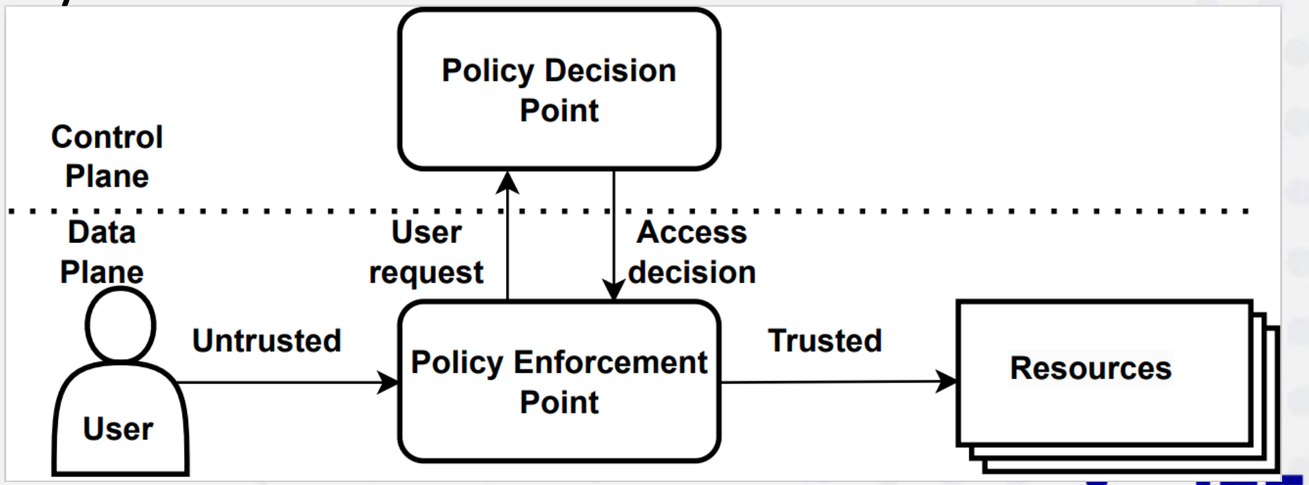
OVERVIEW

1. **INTRODUCTION:**
   - Zero-Trust Architecture
   - Public Key Infrastructure
   - Digital Certificate
2. **PROPOSED WORK**
   - Building a Self-Signed Certificate Authority
   - Certificate Generation
   - User Registration in Zero-Trust Network
   - User Authentication using Public Key Infrastructure in Zero-Trust network
3. **CONCLUSION**
4. **REFERENCE**

INTRODUCTION

Zero-Trust Architecture (ZTA)

- ZTA based on a security model which is proactive dynamic and real-time security model
- It does not trust any entity by default
- The traditional security model trust the insider object by default
- National Institute of Standards and Technology (NIST) give the concept of ZTA
- ZTA is different from traditional security architecture



[A Logical View of ZTA [1]]

Public Key Infrastructure (PKI)

- Provide a framework
- Manage digital keys and certificates [3]
- Secure the communications over the network [2]
- Verify identities of entities over the network

Key components of PKI:

1. **Public and Private Keys:** Use for encryption [2]
2. **Certificate Authority (CA):** Validate user's identity, generate and manage digital certificates [2]
3. **Registration Authority (RA):** Intermediary between entities and the CA [2]
4. **Certificate Repository:** Stores and manages digital certificates [3]
5. **Certificate Revocation List Distribution Unit:** Check validity of certificates [3]
6. **Key Management System :** Generates, stores, and manage keys [3]

Digital Certificate

- Ensure the authenticity of the entities

Digital Certificate

- **Owner's Name**
- **Validity Period**
- **Issuing CA**
- **Owner's Public Key**
- **Digital Signature of CA**

PROPOSED WORK
Generation of Self-Signed Certificate Authority

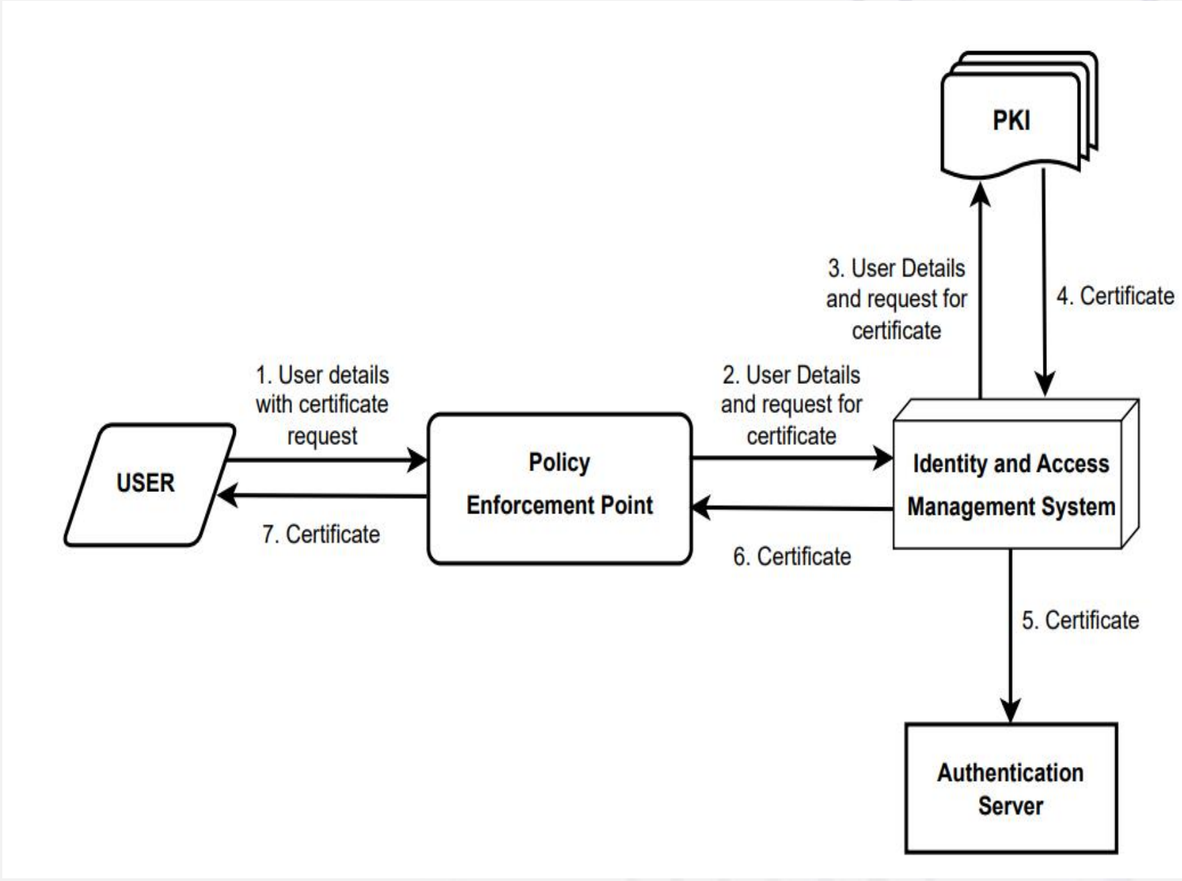
- Use of Open Source Secure Sockets Layer (OpenSSL) tool
- Generation of the private and public key of the CA
- Command to generate private key: **openssl genpkey -algorithm RSA-out ca.key -aes256**
- Generation of self-signed certificate for CA
- Certificate is valid for 365 days

Certificate Generation

- User generates private-public key pair using Rivest-Shamir-Adleman (RSA) algorithm
- User creates a Certificate Signing Request (CSR) including its public key and identity information
- Command to generate CSR: **openssl req -new -key client.key -out client.csr**
- CSR is provided to the CA
- Then CA checks the user details and publish the certificate

User Registration in Zero-Trust network

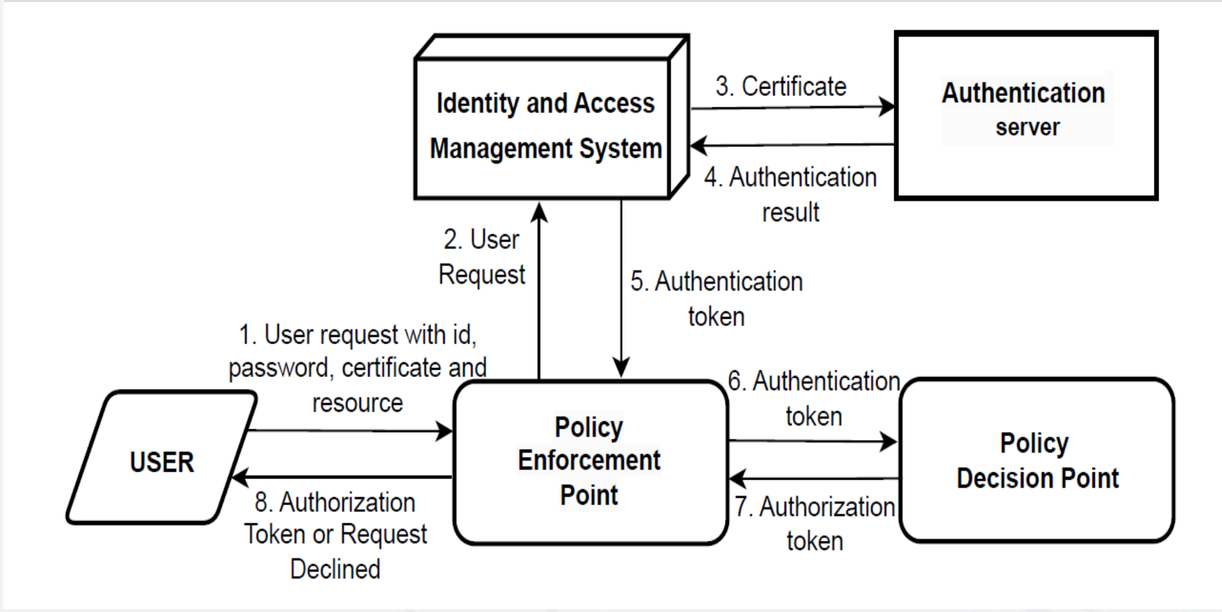
- Policy Enforcement Point (PEP) provides the user request to the Identity and Access Management System (IAMS)
- The IAMS verifies the user information
- IAMS forwards the certificate request to the PKI of the verified user and stores the user information in its database
- PKI generates the certificate and provide it to the IAMS
- AIMS forwards the certificates to the authentication server and the user



[The proposed model for user registration in the zero-trust network]

User Authentication and Authorization using Public Key Infrastructure in Zero-Trust Network

- PEP is the gateway between user and resource
- It forwards the user's request data to the AIMS
- AIMS sends the user's certificate to the authentication server
- The authentication server verifies the digital certificate and informs the result to the AIMS
- Upon successful authentication, the AIMS sends the authentication token to the PEP
- PEP forwards the authentication token to the Policy Decision Point (PDP)
- PDP take access decision through PE and sends authorization token to PEP
- Based on the authorization token PEP allow or deny the user to access the resource



[Proposed model for user authentication and authorization in zero-trust network]

CONCLUSION

- The zero-trust model ensures robust authentication
- The requesting entity in the zero-trust system must be authenticated
- The digital certificate validate the identity during the authentication process
- Generation of a self-signed CA
- Generation of digital certificate by the CA in the zero-trust enterprise systems during user registration
- Authentication performed by the PEP using IAMS integrated with the authentication server

REFERENCE

1. He, Yuanhang, et al. "A survey on zero trust architecture: Challenges and future trends." *Wireless Communications and Mobile Computing* 2022.1 (2022): 6476274.
2. Adams, Carlisle, and Steve Lloyd. *Understanding PKI: concepts, standards, and deployment considerations*. Addison-Wesley Professional, 2003.
3. Slagell, Adam, Rafael Bonilla, and William Yurcik. "A survey of PKI components and scalability issues." *2006 IEEE International Performance Computing and Communications Conference*. IEEE, 2006.
4. Siddiqui, Zeeshan, Jiechao Gao, and Muhammad Khurram Khan. "An improved lightweight PUF–PKI digital certificate authentication scheme for the Internet of Things." *IEEE Internet of Things Journal* 9.20 (2022): 19744-19756.

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

THANK YOU

https://pkiindia.in

Social Media
/pkiindia

IEEE BANGALORE SECTION