emudhra
Trust Delivered

Concept Note

Empowering Security and Digital Transformation in Defense

Introduction

Cryptography has been an essential part of defense and warfare for the greater part of a century. With the use of computers to manage data storage, authorization, procurement, and more, identity management and secure transactions have never been more important to defense organizations than it is today. PKI (Public Key Infrastructure) helps defense organizations to secure their systems in a more robust way by enabling fool-proof identity management, integrity of transactions, and mitigating the risk of surveillance through SSL activity.

eMudhra has helped defense organizations enable robust security policies through an internal PKI ecosystem that relies on internal trust rather than external trust provided by global trust providers. Further, the system enables organizationsto enhance their authentication standard and streamline procurement processes by facilitating the creation and use of digital signatures to internal stakeholders which are secured through a self-destructible crypto-device.

Understanding Private PKI

Overview

Private PKI (Enterprise PKI) is about enabling the benefits of asymmetric cryptography to solve problems in an internal enterprise ecosystem (i.e. Army, Navy, Air Force) or even units within a large enterprise ecosystem (i.e. Army Procurement and Maintenance, etc). PKI is widely used in the form SSL's (or TLS) which are typically issued by global trust service providers. These providers are technologically trusted by the prominent web browser organizations of today to enable secure trusted communication between a web-server and the website. The communication leverages upon asymmetric cryptography and globally trusted identity to securely identify endpoints in a fool-proof manner, and encrypt data between the two endpoints using advanced encryption once the trusted communication channel has been established.

Private PKI is really about leveraging the benefits of this concept and utilizing the same internally to identify and secure communication that occurs constantly between multiple servers, applications, internal sites, and people, within an organization. This is done through setting up an internally trusted Certifying Authority system capable of issuing signature certificates as explained below:

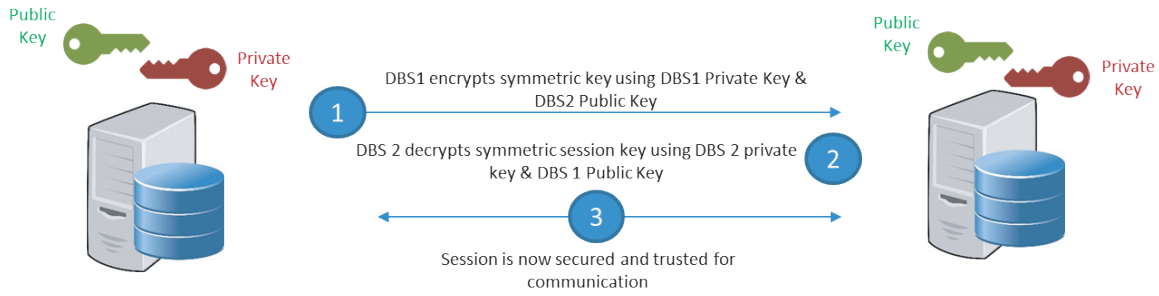
Certificate Type	Use Case
Server Certificates	Used to identify servers and establish trusted & encrypted communication channels amongst servers
SSL (Private)	Private SSL's help in building internal trust ecosystems within an organization for web assets that require trusted access but are not generally exposed to the public
User Certificates	User certificates are digital signature certificates issued to members of an organization and are often used as an advanced form of authentication to access applications and to sign documents in a manner that ensures data integrity, confidentiality, and non-repudiation. User certificates are Typically issued on a crypto-device

	(client side signing) to the end user or saved in a secure Hardware Security Module and retrieved for usage (server side signing)
Code Signing Certificates	These certificates are meant to protect the integrity of any sensitive piece of code and establish a legal identity to the code (and hence, the IP)
Document Signer Certificates	Document signer certificates are certificates that are issued to an organization at large to enable one-sided signing of documents in bulk to maintain integrity of document data at all times
IoT Certificates	These certificates are issued to IoT devices which typically carry low processing power to enable trusted identity of such

How PKI Works

PKI works on the premise of asymmetric cryptography whereby a private key (private to a user or device) and a corresponding public key (available in a public registry and unique to a single private key) are used to securely identify a given user or device.

Here's an example of how PKI works in the realm of trusted communication of data:



When the key pair is signed by a trusted Certifying Authority (CA), a new file type is created which is termed as the 'Digital Signature Certificate.' The function of the CA is to provide the keys to a trusted identity to enable other applications in the organization to trust the transactions originating from a certain set of keys.

PKI is also widely used to sign documents and pieces of data which are another critical form of user to user communication in today's world. In this case, a hash is created out of each document and is encrypted using the sender's private key. The encrypted hash is digitally signed using a certificate from a trusted source.

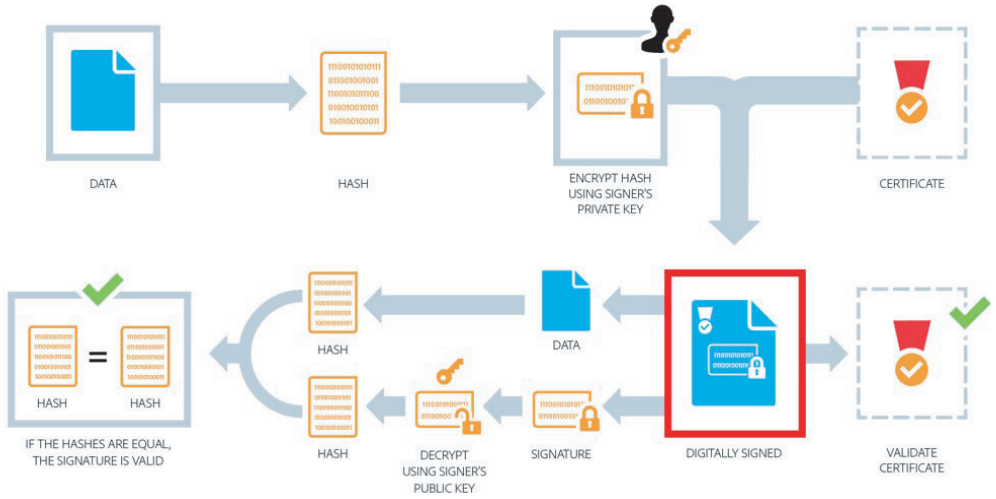
The digitally signeddocument consists of two components:

a) A digital signature, which is a signed and encrypted hash value
b) The original piece of data itself

The receiving application would essentially decrypt the signature file using the sender's public key. Simultaneously, the original data is again converted into a hash using globally accepted algorithms. When the two hash values match, we confirm that the signed document is valid and integrity of data is maintained.

The certificate is validated by the application to ensure it is a trusted certificate and that the identity of the signer as claimed can be trusted.

Here's a small diagram outlining how it works:



Value Proposition

Contextual Value Proposition

While there are many ways in which a private PKI can help, below are a few areas in which a PKI system can add

Problem Area	Risks Addressed	Benefits
Trusted communication across & within organizations	Private PKI can ensure that each server, user, and device, is given a fool-proof identity which is then used to communicate. Further, it is also used for encryption of data between trusted endpoints to ensure high levels of security in communication. As a result, it can help in following ways: • Prevent man-in-the-middle and browser-in-the-middle attacks • Prevent phishing and other risk arising out of fraudulent sites that can pose as valid websites • Protect sensitive data and limit the amount of information passed outside of the defense agency	The benefits of private PKI in enabling trusted communication are many. With evolving technologies like IoT and blockchain, PKI becomes an important component to establish identity and trust in these ecosystems. eMudhra's emCA is optimally catered to enhance your IT ecosystem. Some of the benefits of emCA are: • Issuance of IoT certificates to track movement of sensitive inventory with zero-risk of hacking • Enhance mobility and use of digital assets within the organization without compromising security • Have a tamper proof record of all communication activity (data and documents; not radio) available at all

PKI Authentication, STRONG user authentication management	Digital Signatures can be issued to individuals within an organization from a Private PKI Root. Such signatures can be stored in smart cards, crypto tokens, or even on the server (to be retrieved for use when needed). These signatures can mitigate risks in following ways: • DSC authentication significantly reduces risk associated with false authentication • Since it signs the authentication transaction with a time stamp, the authentication activity can never be refuted by the user thus bringing greater accountability • It can provide a tamperproof log of not only application level access but also domain level access helping reduce risk and manage the digital ecosystem effectively	PKI Authentication has been the standard in multiple defense organizations, and broadly speaking, for sensitive government applications and eCitizen actions. The key criteria for PKI to be used lies in the nature of technology which does not allow for any technological compromise. What this means, is that inappropriate access would not be possible unless the rightful user has shared their credentials. Hence, there is a significant level of accountability placed on the user and the importance that they give in managing their credentials. Some benefits of this application include: • Non-repudiation of user actions in any domain level or application level activity • Dynamic management of user authentication through effective duration and key policies • Secure access to digital archives • Ability to detect unwanted access or access by illegal persons through the CRL & OCSP
Document signing, ensuring valid identity, document integrity, confidentiality, and user accountability in going paperless	The signature certificates issued to users through a Private PKI have yet another important use case that can significantly streamline and protect your organization's intelligence and activities. Intelligence quite often is in written form which generally poses a high level of risk of theft, copy, loss, etc. The same goes for approvals, authorizations, signed documents, etc. that are exchanged between teams every day. Document signing using Digital Signatures can help reduce risk in following ways: • Reduce the amount of physical paper that needs to be transported, created, stored, etc. • Reduce risk associated with data tampering in archived documents and in current documents (exchanged within organization) • Reduce risk associated with unauthorized approvals and unauthorized communication	There are many benefits associated with going paperless in a secure fashion. Security lies at the center of any true paperless office initiative to ensure that digital transformation can actually be worthwhile for Defense organizations. eMudhra's emSigner can benefit your organization in following ways: • Significantly reduce costs associated with paper, storage, transport, etc. • Enable digitization in procurement and document movement in the organization • Complete traceability of all documents managed through the system • Securely storing documents in the form of hash values which can only be retrieved by the application • Paired with STRONG authentication and AD/LDAP (or inbuilt access management) to ensure that only trusted users have access. • Bring accountability in the minds of your employees to enhance the user mindset towards security at the work environment

Use cases

Use Case	Description	Status
Domain level access authentication	Using user's Digital Signature to authenticate user and sign the event every time user logs into any given domain. *eMudhra is not privy to the full details of the domain as portions of the same were handled by the customer	**Deployed on live instances**
Application level access authentication	Using user's Digital Signature to authenticate user each time he/she log into application(s) within the organization. *eMudhra provided API stack to customer who then did various integrations with level 2 support from eMudhra	**Deployed on live instances**
Paperless procurement	Entire procurement process was converted to a paperless process using digital signatures. Certificates were stored in the HSM and retrieved though user authentication. Sensitive use cases required some users to carry crypto devices also.	**Deployed on live instances**
ERP/HRMS integration (recruitment, accounts, inter team communication, etc.)	Integration with ERP to manage digital communication across all nodes, branches, and users of the ecosystem. Use cases are envisaged to go beyond procurement into accounts, inventory management, maintenance, recruitment, and more	**Deployed on live instances**
Inventory management on blockchain	Hyperledger fabric envisaged to create a distributed ledger ecosystem for storing inventory records to protect against single point risk	**Proof of Concept facilitation**

The Solution Ecosystem

The solution ecosystem will have to consist of multiple modules that function together effectively to address the security requirements of a defense organization. The solution components must primarily address the creation of digital signatures. Then, this must be supplemented with the ability to validate the same and broadly, the ability to use the same in document workflows.

eMudhra, as a firm focused on empowering digital transformation through PKI, has the entire framework of solutions required to make secure digital transformation in Defense a reality. The deployment details below are standard architectures. However, eMudhra has helped defense organizations right from defining the data centers, customizing the deployment architecture, all the way to implementing a robust and comprehensive PKI solution and PKI dependent application ecosystem.

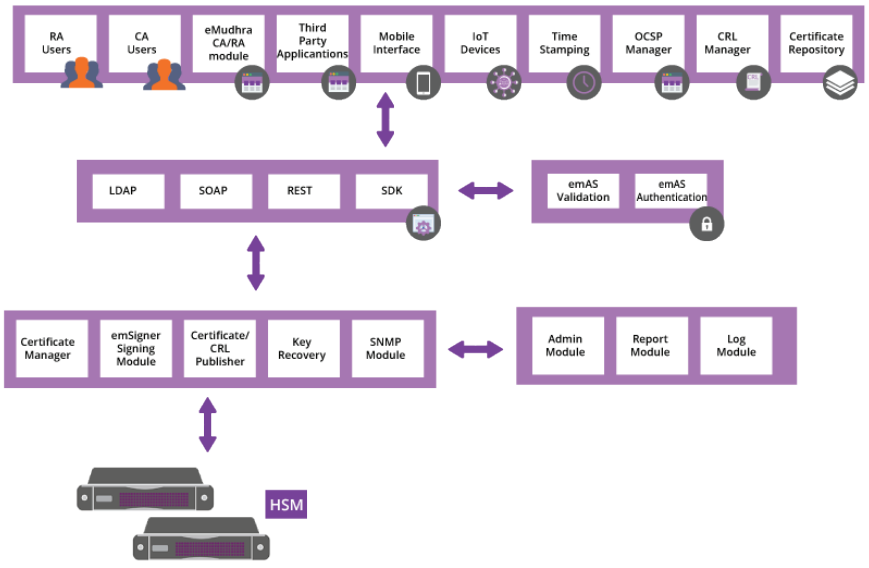
Components

Solution Name	Solution Type	Purpose of Solution
emCA – PKI Suite ***solution structure covered below***	Certificate Authority system	Used to create and manage the lifecycle and distribution of digital certificates within an organization
emAS – Identity Management	Multi Factor Authentication system	Used to validate digital signatures in multiple forms in addition to other authentication factors such as OTP, Biometric, Facial, Iris, Smart card, etc.
emSigner – Paperless Office	Signer solution	Used to leverage upon digital signatures in multiple forms to sign documents and manage workflows, DMS, OCR, and more.

Private PKI (emCA) – Solution Structure

For the purpose of this concept note, we are primarily focusing on the core solution, emCA, which enables creation and management of signature certificates in addition to managing many nuances around the same. Kindly note that deployment architectures are subject to variance from one client to another due to the variance in nuances and requirements.

Below is a pictorial representation of all the components of the core PKI system (emCA) which are required to function as an effective private PKI:



Useful Links

Title	Link
emCA Brochure	https://www.emudhra.com/download/brochures/emCA-Suite.pdf
emAS Brochure	https://www.emudhra.com/download/brochures/emAS-MFA.pdf
emSigner Brochure	https://www.emudhra.com/download/brochures/emSigner.pdf
References – eMudhra	https://www.emudhra.com/resources.html?resid=UseCases
Press - eMudhra	https://www.emudhra.com/press-releases.html

About eMudhra

eMudhra is a global entity and leading trust service provider focusing on Digital Transformation and Cybersecurity initiatives. Headquartered in Bengaluru, India, eMudhra has global offices across 5 continents catering to thousands of customers across the globe. eMudhra also holds the Vice chairmanship of Asia PKI Consortium, Chairmanship of the India PKI Consortium, an is a member of the UN council on Blockchain.

USA | INDIA | UAE | SINGAPORE