Greetings!

Embrace Excellence @

Pos Digicert

18 September 2024

Pos Digicert is focused, committed and strives to enhance the growth of e-businesses whilst at the same time provides providing customers a seamless experience in the digital security ecosystem.

Introduction

POS Digicert

Incorporated:
12th February 1998

A wholly owned subsidiary of POS Malaysia Berhad

MSC MALAYSIA Status Company

MSC Status Company

To facilitate the migration of the **physical world economy to the internet economy**

Granted the CA Operational License in June 1999 by MCMC
(Malaysian Communications and Multimedia Commission)

Issued Approximately

Over 22mil. Digital Certificates.

● 6mil. Active Certificates.

Our Products & Solutions

We offer a full range of IT security products and services covering authentication and legally binding Digital Signing Solutions for enterprises and individuals, PKI and IT Consulting Services, Document Security Solutions and IT Project Management.

1. Digital Certificate

Prove the authenticity of a user, device, server, or website.

1.1 SSL Certificate
1.2 User Digital Certificate
1.3 e-Invoice Certificate
1.4 AATL Certificate

2. Digital ID Solution

Provide are tools and systems that enable individuals, organizations, and applications, to establish and verify their identities online.

2.1 Onboarding Identity Verification (eKYC)
2.2 Date Time Stamping (DTS)
2.3 PKI as a Service (PKIaaS) | CA Engine
2.4 IDsaya

3. Digital Signing Solution

Digital Signing Solutions Legally binding electronic signature solutions for documents signings.

3.1 Document Signing Solution (DSS)
3.2 eCredentia | e-Scroll | eTranscript
3.3 Batch Signing | Secured QR Code
3.4 Signiflow | SignMe

4. Digital Security

4.1 Data & Access Security
4.2 Application & Web Security
4.3 Threat Detection & Response
4.4 Cryptographic & Key Management

5. Professional Services

Discover unparalleled expertise and tailored solutions with us, your trusted partner in industry.

5.1 Risk Management
5.2 Business Continuity Management
5.3 Testing as a Services (TaaS)
5.4 iV&V Services

6. System Integrator (SI)

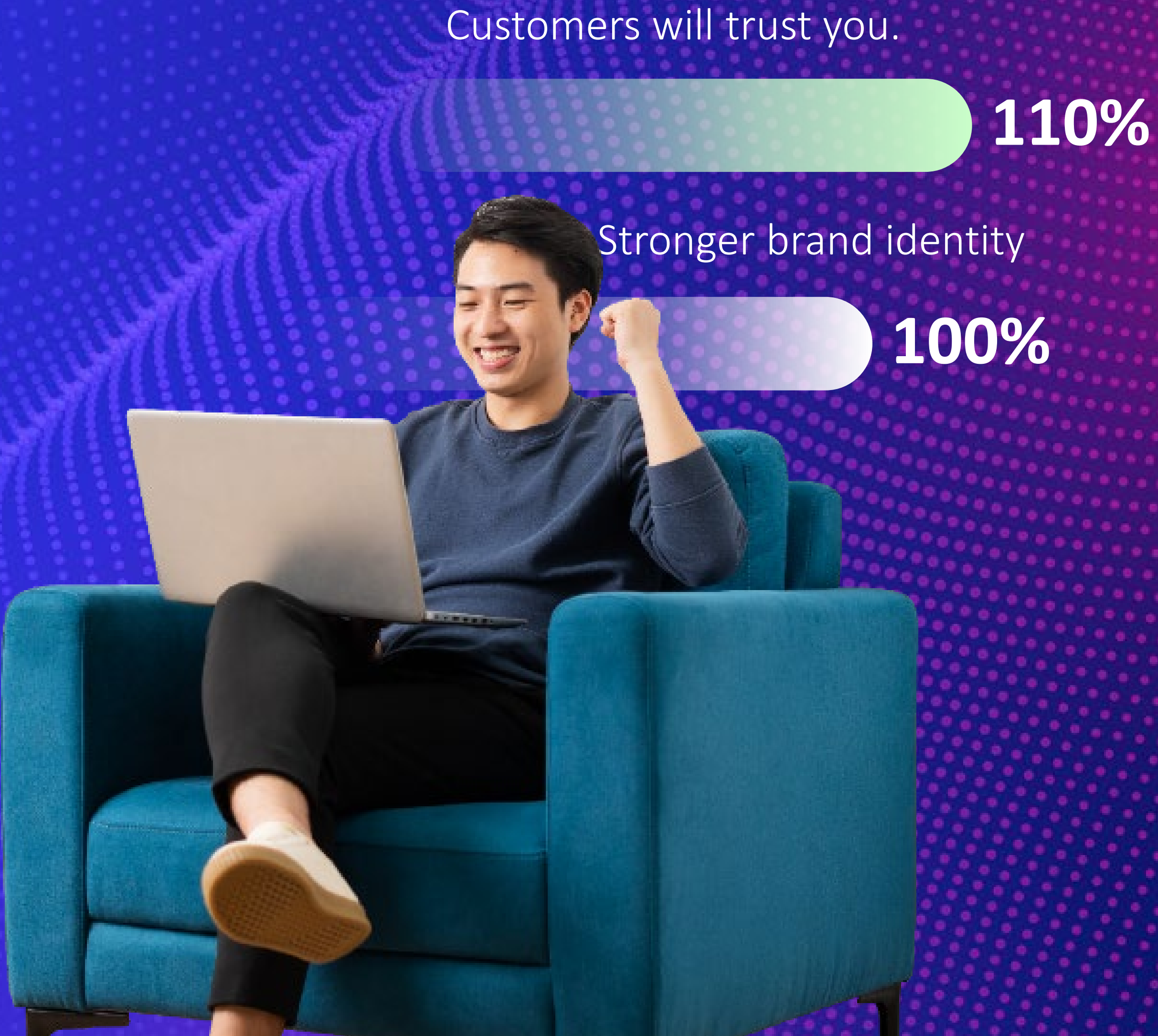
Application Development

We specialize in crafting tailored applications that drive innovation, efficiency and growth.

6.1 Custom Application Development

1

Digital Certificate



Customers will trust you.

110%

Stronger brand identity

100%

Prove the authenticity of a user, device, server or website

1.1 SSL Certificate

Show visitors you're trustworthy and authentic.

Help encrypt your site's data whether it's login information or credit card numbers. Pos Digicert gives your website a Site Seal that says your data is protected, and a trust indicator next to your domain confirms it.

Industry standard for end-to-end encryption protocol.

Helps your website search ranking with https://.

An SSL certificate eliminates the "Not Secure" browser warning.

Our SSL solutions are trusted by leading organizations worldwide. We serve a wide range of clients across various industries, including Governments, Telcos, Financial Instituition, Banks, Statutory Bodies and Private Companies

Type of SSL Certificate

Standard

The proven standard for website security. SSL certificates ensure e-commerce, communications and private information transmitted between a browser and web servers remain private and secure

Recommended : Personal sites, blogs and small forums

Multi-Domain

secure multiple domain, sub- domains or hostnames with a single certificate

Easily secures multi-application or unified communications environments that require the ability to support many domains

Recommended : larger organization needing to secure multiple domains and subdomains on one certificate.

Wildcard

Wildcard SSL certificates secure an entire domain and all of its subdomains with a single certificate. For example:

YourDomainName.com

- www.**YourDomainName**.com
- mail.**YourDomainName**.com

Recommended : Single website and all its sub-domains.

Extended Validation Multi-domain

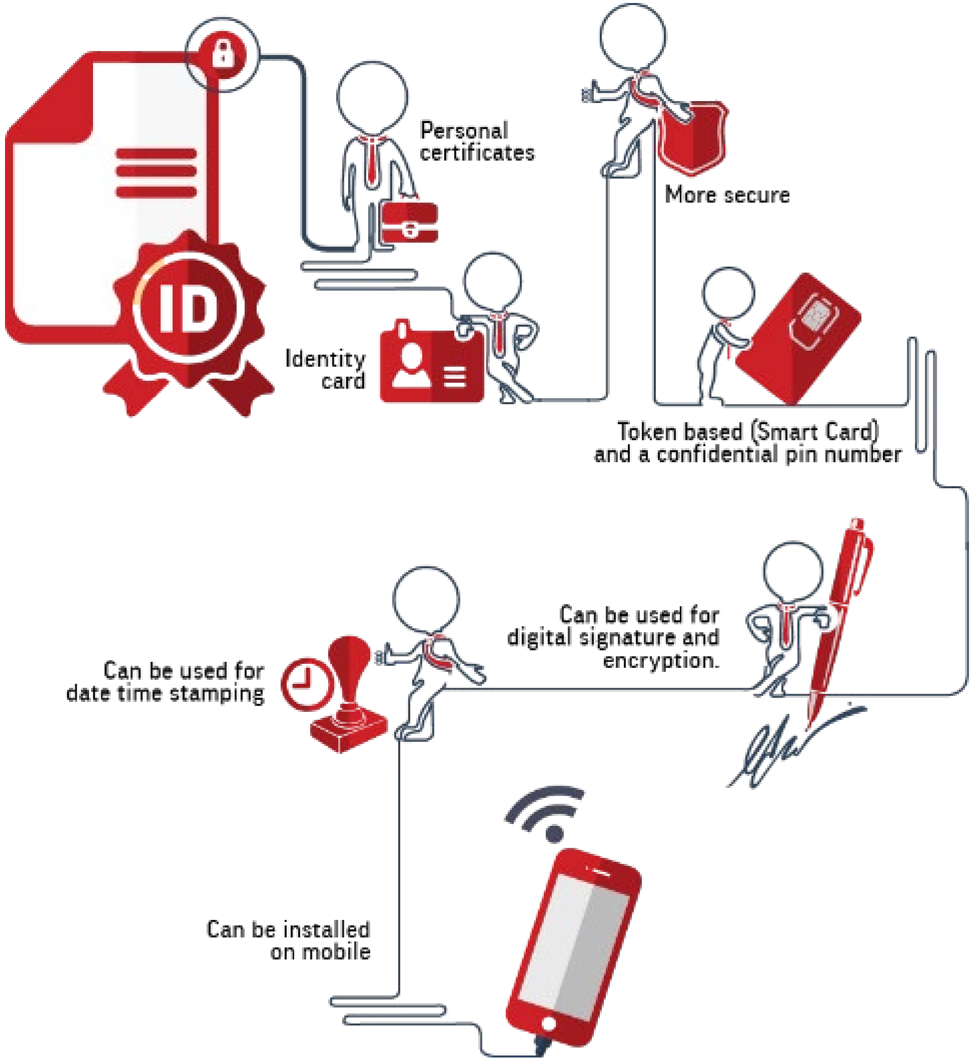
(Ev Multi-domain)

provides the customers with the highest degree of assurance by verifying the identity of the company they are transacting with.

Recommended : eCommerce websites and industries that may require higher security.

1.2 User Digital Certificate

- Personal certificates used for online authentication, digital signature and encryption for individuals;
- It is more secure than username / password mechanism or it can be used as an additional method for authentication;
- Can utilises the ATM concept of a token based (USB Token) and a confidential pin number;
- The digital signature is legally recognised under Digital Signature Act 1997


Personal certificates
More secure
Identity card
Token based (Smart Card) and a confidential pin number
Can be used for digital signature and encryption.
Can be used for date time stamping
Can be installed on mobile

1.2 User Digital Certificate

a. PKI Roaming Certificate

POS DIGICERT's 2048-bit certificate is store and protected by Hardware Security Module (HSM) at Pos Digicert Key Management Centre (KMC).

Features:-

- Centralize management user certificates
- Token-less solution
- Access and use of certificate with NOT limited by;
  - Operating system
  - Browser
  - Devices – support all devices that have internet connectivity and standard browser. - PC, tablet, mobile phone ..etc

Our PKI Roaming Certificate clients : Governments, State Governments, -IPTA, IPTS, Banks, Statutory Bodies and Private Companies

b. Soft Certificate

Software digital certificate that can be stored directly on a computer.

Features:-

- P.12 format
- Exportable and can be copied to other PC

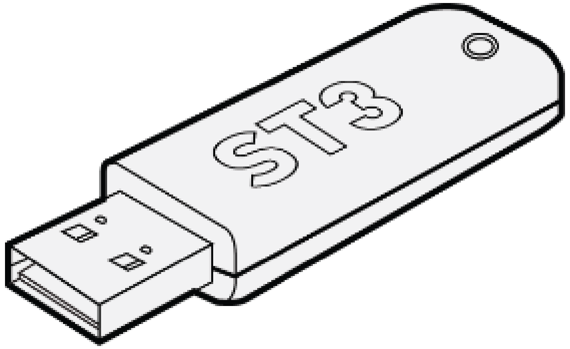
Our Soft Certificate clients : Governments, Law Firms

User Digital Certificate

c. PKI Token Package: PKI Token ST3

PKI Token ST3 is an auto-install model that combines both high speed and high security with 32-bit microprocessor and 128K (64K usable) memory plus 2MB flash memory for auto-installer facility for middleware and token manager tool.

POS DIGICERT’s 2048-bit user certificate is generated in the ST3 USB Token.



Our PKI Token Package clients : Governments, State Governments, and Private Companies

1.3 e-Invoice Certificate

Stay Compliant with Malaysia's e-Invoice Rollout

What is e-Invoice?

e-Invoice is an advanced method for businesses to send and receive invoices electronically, streamlining the process compared to traditional paper invoicing. This digital approach enhances efficiency and reduces manual errors, making it easier for businesses to manage their invoicing tasks.

Provide 2 package options:	**Soft Certificate**	**Roaming Certificate**
Location	Should be placed on the same server as your ERP or middleware.	Stored securely at Pos Digicert's HSM.
Accessibility	Your ERP server / middleware should read the soft certificate file in .p12 format.	Via API.
Integration	No integration needed, but the ERP server must locate the certificate.	Required.
Suitable for	Any organization.	Appointed Tax Agents / Intermediaries.
Certificate validity	1 Year	

Our e-Invoice Certificate clients : Private Companies, Financial Institutions, Manufacturers, retailers, e-commerce platforms, and service providers and businesses

1.3 e-Invoice Certificate *(Cont..)*

Mandatory Information in the Certificate

Mandatory Field	Description	Value Example
Common Name (CN)	The organization name	Pos Digicert Sdn Bhd
Country (C)	The country of the organization - 2-letter ISO code.	MY
Email (E)	An email for the organization.	einvoice@posdigicert.com.my
Organization (O)	The organization name	Pos Digicert Sdn Bhd
Organization identifier	The Tax Identification Number of the organization (TIN)	C1041895804
Serial number (serialNumber)	The business registration number (BRN) of the organization that is linked to the TIN provided above.	199801001482

1.5 AATL Certificate

What is AATL?

Adobe Approved Trust List or AATL, is a program that allows users to create digital signatures that are trusted whenever the signed document is opened in Adobe® Acrobat® or Reader® software. Digital signatures created with a Digital ID that has been issued under any of the trustworthy certificates published in the AATL will appear as trusted in Acrobat and Acrobat Reader.

A. User AATL Digital Certificate
B. Organisational AATL Digital Certificate

Is Pos Digicert's digital certificate AATL enabled?

Approved Trust List
MEMBER

Pos Digicert Sdn Bhd is a member of AATL via the commercial public trust root. Any signatures applied with Pos Digicert certificates that trace back to Pos Digicert AATL Root CA will be automatically trusted in Adobe products.

Our AATL Certificate clients : State Government , IPTA, IPTS, Financial Institutions and Statutory bodies

2

Digital ID Solution

Provide tools and systems that enable individuals, organisations and applications to establish and verify their identities online.

2.1 Onboarding Identity Verification (eKYC)

Pos Digicert offers a mobile and web-enabled solution that leverages on-device technology, biometric authentication (such as facial recognition and liveness detection) and compliant machine learning to achieve accurate identity results in a digital environment

Product Features

MyKad, Passport and Driver's license Verification

Capture the front and back of the ID document and data extracted via optical character recognition (OCR) is verified for authenticity.

Liveness Check & ID Face Match Check

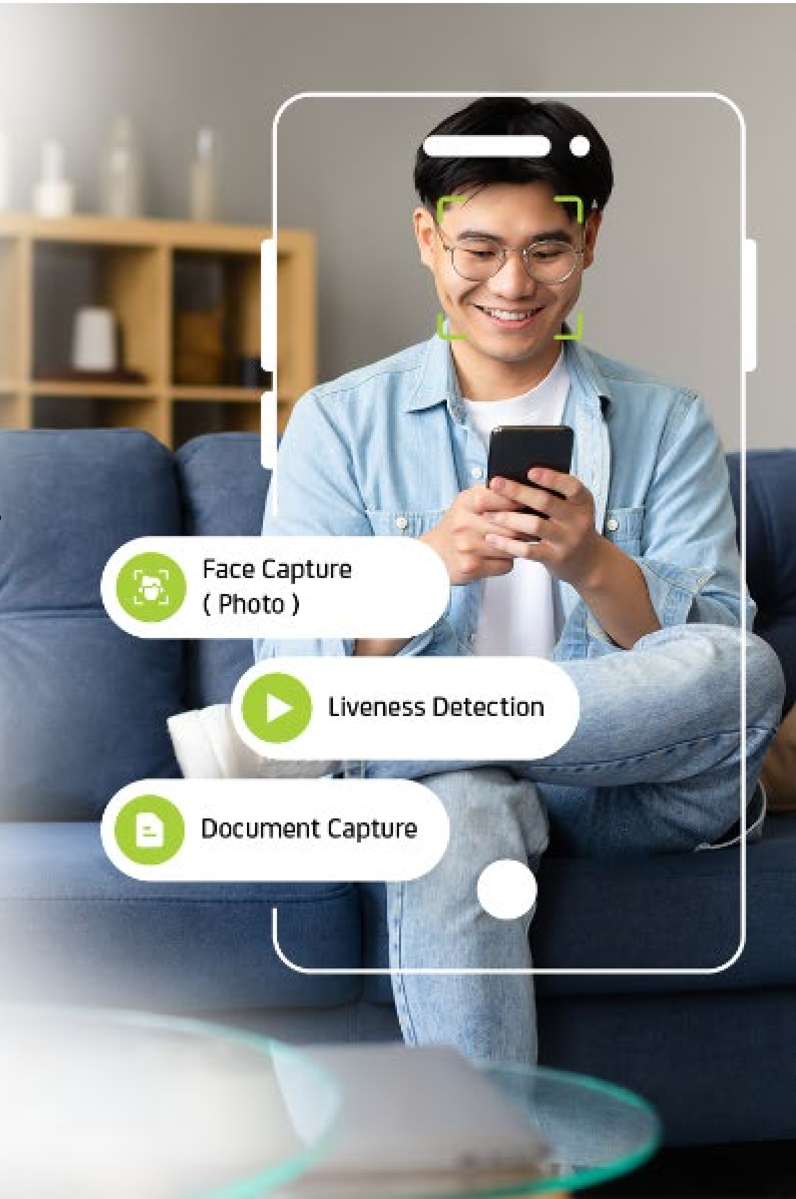
Analysing selfie videos for micro expressions and facial features effectively to identify if the customer is a real person.

Verification Result & Full Verification Report

Verify a user’s identity in real-time by using advance facial matching algorithms with industry leading accuracy and speed.

BNM e-KYC Reporting

User-oriented, State of the Art Proprietary Manual Review Tools and e-KYC Reporting Format (BNM e-KYC Guideline Compliant)



Our eKYC clients : Banks, Statutory bodies, Service Provider, System Integrator and Financial Instituitions

2.2 Date Time Stamping (DTS)

Pos Digicert offers Time-Stamp Service which cryptographically seals electron-ic data and documents. This is achieved by applying a tamperproof digital signature and an accurate time from an auditable Universal Time Coordinated (UTC) source i.e.: SIRIM Malaysia who is the Malaysian National Time Authority.

Our DTS solution provides a cost effective solution for organisations seeking to reinforce data integrity and non-repudiation in the tracking, storage, archiving and submission of electronic records in applications, document management systems, or transactional websites.

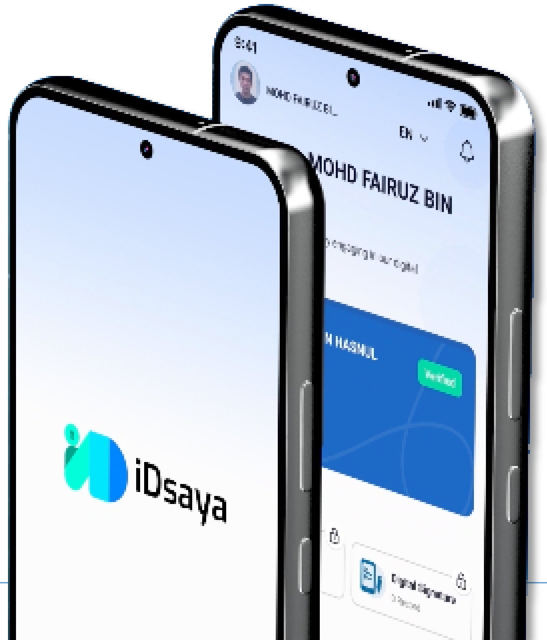
Digital ID Solution

2.3 iDsaya

POS Digicert

Product Features:

1. A digital identity solution which has the capability to ensure the right user is using the phone, by leveraging AI technology.
2. During digital onboarding, user will just need to perform eKYC (facial and MyKad verification).
3. Once verified, via the verified IC number, user will be allowed/not allowed to perform to scan the Secured QR on MITI and MIDA Trustmarks.



Additional Services:

1. User can perform passwordless authentication to login into the system.
2. User can perform signing using his/her digital certificates, seamlessly.
3. Can be integrated with counter system for counter registration/queuing purposes without the needs to handover MyKad/Driving License at counter.
4. Can leverage digital ‘Business Card’ with QR features – can eliminate the use of physical business card.
5. Multi-Factor Authentication is also provided to strengthen the digital signing capability.

POS Digicert

2.4 PKI as a Service PKIaaS

PKI as a Service is a scalable way to deploy PKI. Key factor of PKIaaS combines expert-managed PKI and certificate lifecycle automation into a single, cloud-delivered platform. There is an indispensable need for compliance with regulatory standards such as SOX, PCI DSS, GDPR.

1 | On cloud implementation. Support and Maintenance remotely

2 | Minimal investment cost to setup Certification Authority

3 | Deploy faster. It's turnkey PKI without hassle to setup large scale infra

4 | Minimum team required to operate and support

5 | Scale without limits with secure PKI designed

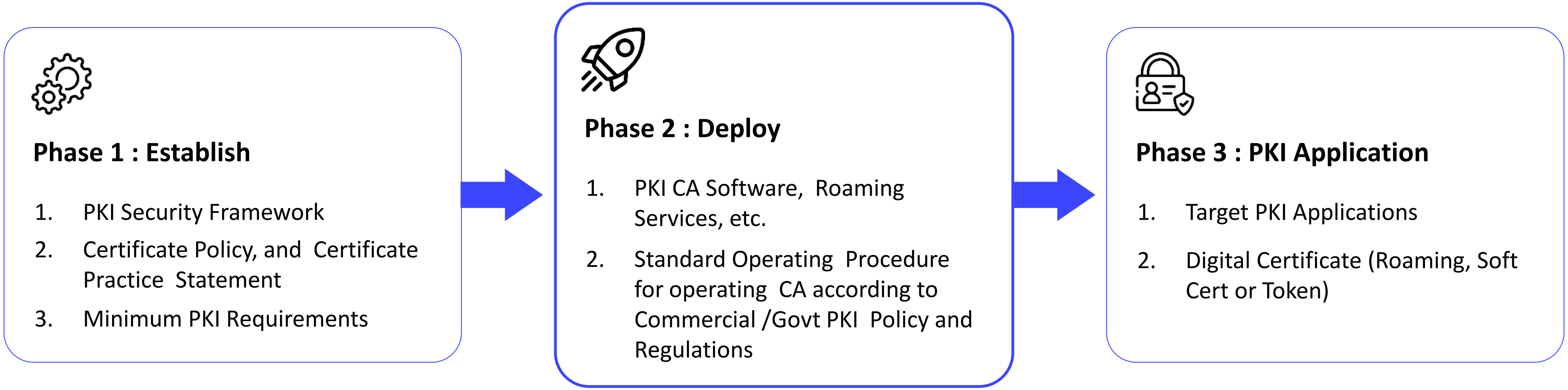
6 | Secure it to the highest level while retain full visibility of access to root CA key material.

7 | Seamless and automated managed services with extensive digital connectivity

8 | Expedite the implementation of systems and services

PKIAAS clients : NITA - Uganda

2.4 PKI as a Service PKIaaS *(Cont..)*



Phase 1 : Establish

1. PKI Security Framework
2. Certificate Policy, and Certificate Practice Statement
3. Minimum PKI Requirements

Phase 2 : Deploy

1. PKI CA Software, Roaming Services, etc.
2. Standard Operating Procedure for operating CA according to Commercial /Govt PKI Policy and Regulations

Phase 3 : PKI Application

1. Target PKI Applications
2. Digital Certificate (Roaming, Soft Cert or Token)

2.4 PKI as a Service PKIaaS *(Cont..)*

PKIaaS and CA Components

Pos Digicert Root CA ⟶ **Government CA**

Key Ceremony at Pos Digicert Secure Facility. Creation of a dedicated "Security World" via its own Hardware Security Module (HSM).

Registration Authority (RA)

Registration Authority (RA)

- A unit performing the processes of application, verification of user; issuance, unblocking and revocation of digital certificates.
- All the process at RA will be audited annually by either PWC, E&Y, Deloitte or KPMG.

PKI as a Service

OCSP Service : The OCSP protocol allows a client to query the status of one or more certificates and get up to date information on their revocation status.

CRL Service : Certificate Revocation List Service for user to revoke their certificate.

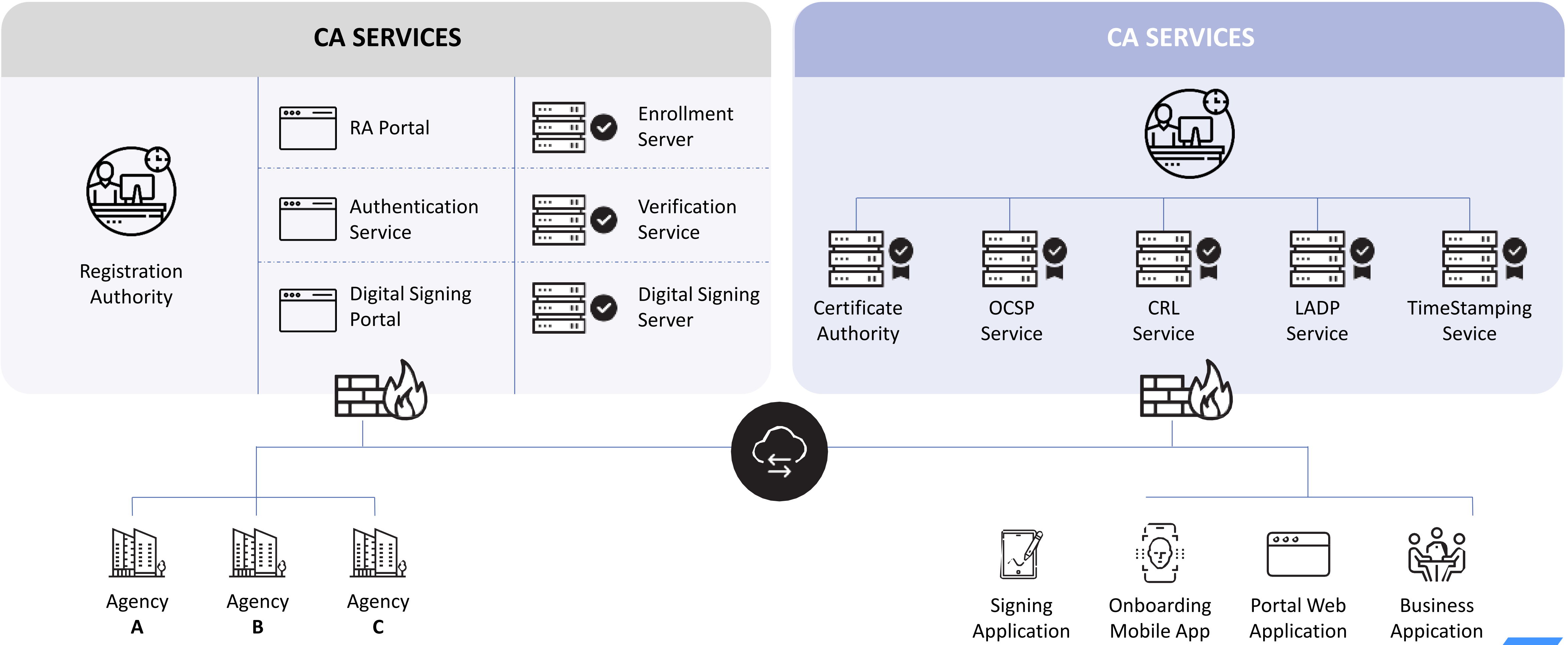
Timestamping Service : Time used in time stamp is a National Standard Time, which is maintained and managed by National Time Authority and can be used to countermeasure for settlement as a presumption.

Establish Shared Security Services

Enable a dedicated Shared Security (PKI) Services for Government. Provide centralized security services including Document Signing, onboarding Mobile Apps, Validation services and others for public's easy access.

2.4 PKI as a Service PKIaaS *(Cont..)*

PKIaaS and CA Components



3

Digital Signing Solution

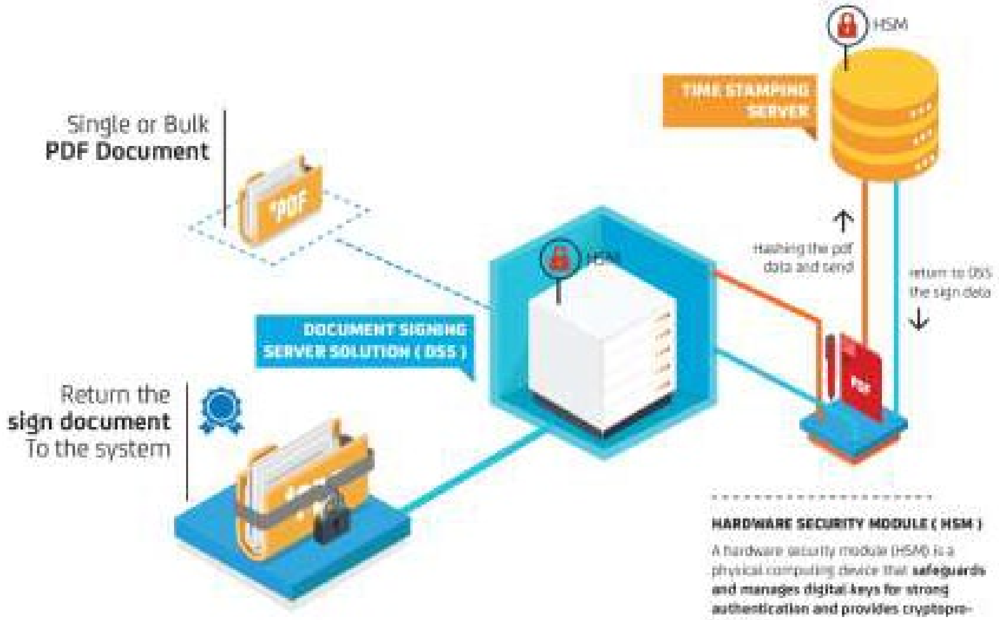
Digital Signing Solutions with legally binding digital certificate for digital document signings

3.1 Document Signing Solution (DSS)

- Convert and embed important data into Encrypted QR Code
- Support Date Time Stamping services (based on RFC 6131)
- Support User Authentication with Digital Certificate
- Support International Standard
  - PAdES , AdeS & LTV (Long Term Validation)

It is a Server-based product that digitally signs documents (a substitute for traditional handwritten signatures) like PDF files, Web Form and XML documents by using the user's legal binging digital certificate. The end product can be verified not modified and tampered with.

DSS can integrate into any online application that requires digital signing capabilities with our easy and reliable APIs


HSM
TIME STAMPING SERVER
Single or Bulk PDF Document
PDF
HSM
Hashing the pdf data and send
return to DSS the sign data
DOCUMENT SIGNING SERVER SOLUTION (DSS)
Pdf
Return the sign document To the system

HARDWARE SECURITY MODULE (HSM)

A hardware security module (HSM) is a physical computing device that **safeguards and manages digital keys for strong authentication and provides cryptoprocessing.**

DSS clients : Government Agencies, State Government, Financial Institutions, IPTA, IPTS, System Integrator and Private Companies

3.1 Document Signing Solution (DSS)

DSS FEATURES

SIGNING PDF, XML & WEB FORMS

Certify PDFs to prove authorship, contents, and secure against future tampering.

EASY TO USE APIs

DSS comes with set of APIs for easy integration.

BATCH SIGNING

Allows bulk signing on numbers of PDF document.

MULTIPLE SIGNERS

Multiple signers can sign onto the PDF.

VARIOUS STORAGE MEDIUMS

For signing, user can use various type of certificate storage medium such as USB Token, Smart Card , HSM and Roaming Certificate.

SUPPORTS USER AUTHENTICATION

Support User Certificate-based verification and authentication.

SUPPORTS DATE TIME STAMPING (DTS)

Documents signed by DSS will be Date Time Stamped based on International RFC 3161 standard.

SUPPORTS INTERNATIONAL STANDARD

- **PAdES**
- **AdeS**
- **LTV** (Long Term Validation)

3.2 Secured QR Code

Verify and validate the authenticity of physical digitally signed documents

Tamper Proof & Secure QR

This Secure QR code solution from Pos Digicert serves as the definitive method to verify and authenticate the physical copy of the digitally signed documents. QR codes embedded within the document are securely linked and protected by industry standards' encryption.

Only Pos Digicert's eValidator mobile app is capable of decoding the document, guaranteeing its authenticity. This initiative is designed to uphold the integrity and authenticity of the document.

Our Secured QR Code clients : State Government, Government Agencies and Private Companies

Benefits

Encrypted QR Code Generator At Server Side

Creates information encryption to generate Secure QR codes

Pos Digicert eValidator App

A mobile app installed on smartphones designed to securely display encrypted information contained within the issued QR code

Verification of Digital Certified True Copy

Easily verify printed copies of Digital Certified True Copy (CTC) document

3.3 eCredentia / eScroll / eTranscript

The unique and preferred solution for securing professional certificates & education scrolls issued by higher education institutions & professional institution in Malaysia

What is eCredentia

- eCredentia empowers higher education institutions in managing records including transcripts, certificates and official letters to be digitally signed and securely stored, giving students and graduates direct access to their records
- eCredentia offers significant benefits to higher education institutions, graduates, employers, government agencies or any other recipients of credentials documents

Secured QR Code clients : IPTA, IPTS and Government Agencies

3.3 eCredentia / eScroll / eTranscript *(Cont..)*

Benefits

✓ **Secure! - It utilises digital signature and date time stamping technology**

Unlike the traditional paper-based certificates or scrolls which is can be easily forged, our eCredentia uses digital certificates to sign and time stamp the digital document. This is made possible by using the Public Key infrastructure (PKI) which has been proven worldwide to be tamper proof

✓ **Convenient! Instantaneous verification by any relying parties**

Relying parties can verify the authenticity of the eCredentia instantaneously using Adobe PDF reader

✓ **Save Paper & Hassle Free! Just retrieve and share the eCredentia!**

No more hard copy printing! Graduates can easily send their eCredentia to their future employers by providing anywhere, anytime access and the ability to retrieve and share documents with employers, universities and other parties with whom they choose

✓ **Secured QR Code – Verification of Digital Certified True Copy**

Receiving organisations will also be able to rely on the authenticity of the documents and be less concerned about potential fraud

- Creates information encryption to generate secure QR codes
- Legally protected under the Malaysian Digital Signature Act 1997
- Tamper proof and instant verification
- Easily validated via online portal or the eValidator App
- Date Time Stamped
- Modern signature technology

3.4 SignMe

Go paperless, Grow your business with SignMe

Faster than paper

Accelerate signing processing by up to 80%.

Easy and intuitive

Simplify signing for everyone, tech-savvy or not.

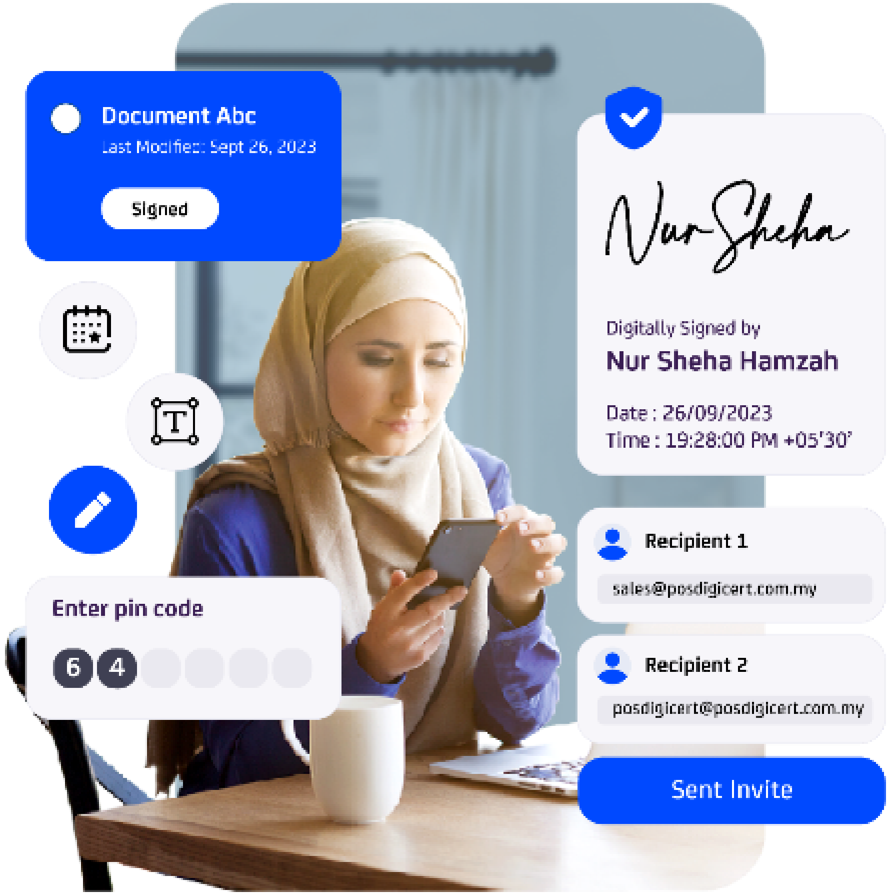
Legally Binding

(By complying with Malaysia Digital Signature Act 1997 & Electronic Commerce Act 2006)

Strong audit trails offer conclusive evidence of document access, review, and signature actions.

Secure and reliable

Safely sign and request signatures for your most important documents.



SignMe clients : Government Agencies, Financial Instituitions, IPTA, Statutory Bodies

3.4 SignMe (cont..)

POS Digicert

SignMe Value Proposition

SignMe can run on both web and mobile phone. The solution is available for deployment on cloud or on any preferred on-premise locations.

API Integration - CRM, DMS, ERP, etc

Multi-language *(including Bahasa Malaysia)*

Pos Digicert eKYC - Digital ID Verification

Compliance with Digital Signature Act 1997 & Electronic Commerce Act 2006

Integration with Roaming Certificate *(No Token required)*

Cloud based (Roaming) Signing

Compliant with Bank Negara Malaysia (BNM) eKYC policy.

WorkThow Automation

Hosted or On-premise

In-Country (Malaysia) & Global Support 24/7

Process Digitisation

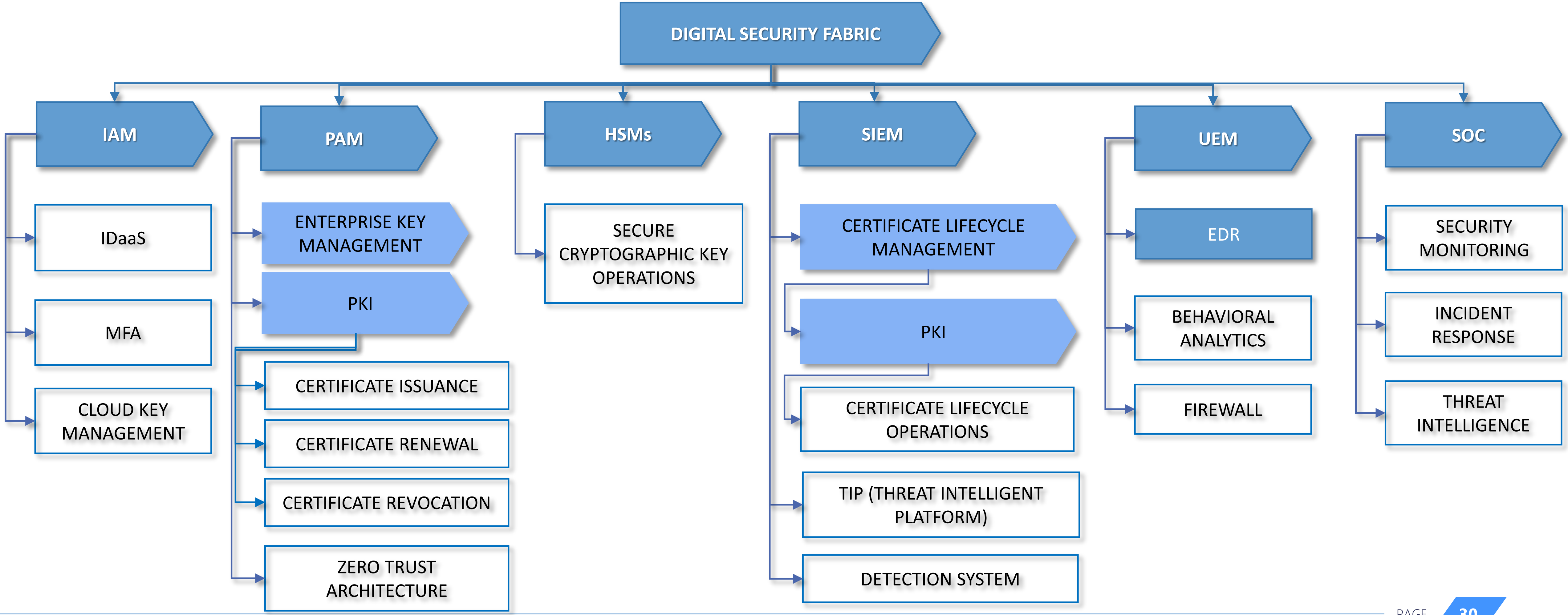
4

Digital Security

Protects and manages confidential systems, networks, data and identities in physical and digital

4.0 DIGITAL SECURITY

Digital Security is the fundamental part of access and the entry point for most digital securities issues



4.1 DATA & ACCESS SECURITY

Data Management

- **Encryption:** Utilizes advanced encryption standards (AES), end-to-end encryption, and homomorphic encryption to secure data both at rest and in transit.
- **Data Loss Prevention (DLP):** Deploys machine learning and AI-driven DLP solutions to detect and prevent data breaches, ensuring sensitive data is not lost, misused, or accessed by unauthorized users.
- **Database Security:** Implements database activity monitoring (DAM) and database firewalls to secure databases against compromises and unauthorized access.

Identity & Access Management (IAM)

- **Authentication:** Verifies user identities using next-gen MFA (e.g., biometric, behavioral biometrics), single sign-on (SSO), and adaptive authentication.
- **Authorization:** Controls access levels and permissions using dynamic role-based access control (RBAC) and attribute-based access control (ABAC).
- **Identity Governance and Administration (IGA):** Manages the identity lifecycle with AI-powered identity analytics, ensuring users have appropriate access rights and maintaining compliance with policies and regulations.
- **Privileged Access Management (PAM):** Secures, manages, and monitors privileged access using just-in-time (JIT) access, zero trust principles, and session monitoring to prevent unauthorized access and potential breaches.

4.2 APPLICATION & WEB SECURITY

Application Delivery Controller (ADC)

- **Load Balancing:** Uses intelligent load balancing and auto-scaling to distribute network or application traffic across multiple servers, ensuring high availability and performance.
- **Application Acceleration:** Enhances performance with SSL/TLS offloading, content caching, and HTTP/2 support.
- **Application Security:** Protects applications with next-gen WAF, runtime application self-protection (RASP), and integrated DDoS protection.

Web Application Firewall (WAF)

- **Signature-based Detection:** Utilizes automated rule updates and threat intelligence feeds to identify and block known threats.
- **Behavioral Detection:** Uses AI and machine learning to detect and respond to anomalous behavior and zero-day attacks.
- **Bot Mitigation:** Employs advanced bot management solutions, including behavioral analysis, CAPTCHA, and challenge-response mechanisms to prevent automated bot attacks.

4.3 THREAT DETECTION & RESPONSE

Threat Detection & Response

- **Intrusion Detection Systems (IDS):** Monitors network or system activities using AI-enhanced anomaly detection and signature-based detection for malicious actions or policy violations.
- **Security Information and Event Management (SIEM):** Provides real-time analysis of security alerts with big data analytics, machine learning, and threat intelligence integration.
- **Endpoint Detection and Response (EDR):** Uses behavioral analysis, AI-driven threat hunting, and automated remediation to identify, investigate, and mitigate suspicious activities on endpoints.

Next Generation Firewall (NGFW)

- **Advanced Threat Protection:** Incorporates deep packet inspection, AI-based malware detection, and sandboxing to identify and block advanced threats.
- **Application Awareness:** Offers granular application control and user identity tracking to enhance security.
- **Integrated Intrusion Prevention System (IPS):** Prevents and detects threats in real-time with signature-based and anomaly-based detection powered by AI.

Network Intrusion Prevention System (NIPS)

- **Signature-based Detection:** Uses threat intelligence feeds and AI to identify known attack patterns.
- **Anomaly-based Detection:** Detects unknown threats by identifying deviations from normal behavior using machine learning algorithms.
- **Policy Enforcement:** Analyzes and filters network traffic to enforce security policies and ensure compliance.

4.4 ENTERPRISE KEY MANAGEMENT (EKM)

Cloud Key Management (CKM)

- **Key Generation:** Securely creates symmetric and asymmetric cryptographic keys using quantum-resistant algorithms.
- **Key Distribution:** Ensures secure exchange and distribution of keys with zero-trust key exchange protocols.
- **Key Storage:** Utilizes Hardware Security Modules (HSM) and cloud-based key management solutions to securely store cryptographic keys.

Hardware Security Module (HSM)

- **Key Management:** Provides secure storage and lifecycle management of cryptographic keys with tamper-resistant hardware.
- **Cryptographic Operations:** Facilitates secure encryption, decryption, and digital signature processes, compliant with FIPS 140-3 and Common Criteria (CC) standards.
- **Compliance and Certification:** Ensures adherence to industry standards and regulatory requirements, providing robust security for critical cryptographic operations.

Certificate Lifecycle Management (CLM)

- **Certificate Issuance:** Manages the creation and issuance of digital certificates through a scalable Public Key Infrastructure (PKI) and trusted Certificate Authorities (CA).
- **Certificate Renewal:** Automates the renewal process with AI-driven expiration monitoring to maintain continuous security.
- **Certificate Revocation:** Uses real-time Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) to revoke and check the status of certificates.

5

Professional Service

Discover unparalleled expertise and tailored solutions with us, your trusted partner in industry

5.1 Risk Management – Consultancy Services

Risk management consultancy services help businesses identify, assess, and mitigate risks. These services can be tailored to a specific business or industry, and can address a wide range of risks, including:

a) Strategic risks, such as changes in market conditions or competition
b) Operational risks, such as disruptions to production or IT systems
c) Financial risks, such as fluctuations in currency exchange rates or interest rates
d) Compliance risks, such as violations of laws or regulations
e) Reputational risks, such as negative publicity or product recalls

Risk management consultancy services can help businesses to:

a) Improve their risk management culture
b) Develop a risk management framework
c) Identify and assess risks
d) Develop and implement risk mitigation strategies
e) Monitor and report on risks

By helping businesses to identify and mitigate risks, risk management consultancy services can help businesses to improve their overall performance and achieve their strategic objectives.

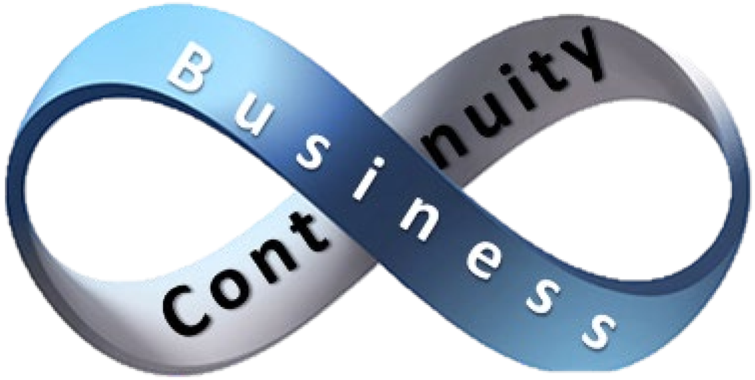
Risk Management Consultancy Services clients : Government and Government Agencies

5.2 Business Continuity Management (BCM)

Business continuity consultancy services focus on helping organizations prepare for and recover from disruptive events. These events can be anything from natural disasters like floods or fires to cyberattacks or even power outages.

Business continuity consultancy services offering:

- **Business Impact Analysis (BIA):** Consultants will work with you to identify critical business functions and assess the potential impact of disruptions on those functions. This helps prioritize recovery efforts.
- **Business Continuity Plan (BCP) Development:** They will guide you in creating a plan that outlines steps to resume critical operations after a disruption. This includes identifying backup locations, communication protocols, and data recovery procedures.
- **Incident Response Planning:** Consultants can help develop a plan for how to respond to specific incidents, ensuring a coordinated and effective response that minimizes downtime.
- **Business Continuity Management System (BCMS) Implementation:** They can assist in establishing a framework for ongoing risk assessment, plan maintenance, and testing to ensure your business continuity plan remains effective.
- **Testing and Training:** Regularly testing your BCP is crucial. Consultants can help facilitate these drills and train your staff on their roles and responsibilities during a disruption



Business Continuity Management Consultancy Services clients' : Government and Government Agencies

5.3 SW Testing as a Services (TaaS)

Pos Digicert‘s test automation service helps to automate your test cases.

Specialised tools are used to create and control the execution of your tests cases and compares the actual results against the expected result with little to no human intervention. This increases your test efficiency and coverage thus enabling for a shorter testing phase and faster deployment to production.

Test automation criteria

Repeatable

The test should be repeatable and do not undergo major changes.

Determinant

The test output or results should be determinant and not ambiguous or requires tester’s feedback.

5.3.1 Functional Testing

To helps validate if your system application is functioning as intended.

by evaluating each functions or modules with an appropriate input and verifying the output against the system application's functional requirements specification.

We can help you manage your testing activities from analysing the system or application's functional requirement specification and extracting test cases for bugs reporting, producing summary reports and improvement recommendations.

Our Test Service include:

Desktop and Mobile:

Whether it's for desktop system or a mobile application, we got it covered.

Main functions:

To test the main functions of the system / application.

Basic Usability:

To test the ease of use and accessibility of the system / application.

Error Conditions:

To test the suitability of error messages displayed (error message best practices).

Documentation:

Produce documentation and reports throughout the testing phase.

5.3.2 Performance Testing

To evaluate system’s performance and behavior under both normal and anticipated peak load conditions, measure performance against Service Level Agreements and Key Performance Indicators and identify the bottlenecks of a system.

Type of performance testing

- Load Testing
- Stress Testing
- Spike Testing
- Scalability Testing
- Volume Testing
- Endurance Testing

We can help you to identify a variety of problems before your system goes into production:

- **Server and infrastructure configuration issues**
  (Web Server, Application Server, Database Server, Load Balancer, Firewall, etc.)
- **Hardware limitation issues**
  (Excessive disk usage, I/O, CPU maximization, memory limitations, network bottleneck)
- **Database design and performance issues**

5.4 Independent Verification & Validation iV&V

Independent Verification & Validation (IV &V) means verification and validation performed by an organization that is technically, managerially, and financially independent of the development organization.

(ISO / IEC / IEEE 24765: 2010 Systems and Software Engineering – Vocabulary)

a) Participate in government IV & V tenders – critical and high Impact
b) Provide IV & V to government , private sector companies local and international market

IV& V Service Offering

Service Elements	Description
Early Testing	To inspect requirements documents such as a system requirements specification to determine whether the requirements are complete, clear, consistent, testable and maintainable. To detect and remove defects as early as possible.
Static Analysis using Tool	To analyze code that does not execute the program, and is used to detect quality and security issues before the software is released.
Risk Assessment	To identify, prioritize, mitigate, monitor, and control (test) project / product related risks and risk handling plans. Risk based testing as one of the test approaches.
Requirements traceability	The traceability matrix is used to verify that all stated and derived requirements are associated with corresponding product risks, test conditions, test cases and test procedures.
Test Automation Using Tool	Test Automation Service increases the speed, accuracy and coverage of application testing and provides a high return on investment for software projects while lowering the business risk and bringing savings in capital expenses.

6

System Integrator (SI)

Application Development

We specialize in crafting tailored applications that drive innovation, efficiency and growth

6.1 Custom Application Development

Custom application development offers a powerful way to build web services and mobile apps that perfectly integrate with your existing systems and workflows. Our team of expert developers offers unparalleled skill in Java, .NET, PHP and mobile app development. We translate your vision into reality, crafting applications that:

a) **Address Specific Needs:** Ditch off-the-shelf limitations. We design apps that perfectly integrate with your existing systems, leveraging our expertise in:
   - Java: Build robust, secure, and scalable enterprise applications.
   - .NET: Ensure seamless integration with Microsoft environments and develop high-performance web services.
   - PHP: Deliver rapid development and cost-effective solutions for web applications.
   - Mobile App Development: Create user-friendly, native apps for iOS and Android.

b) **Embrace Innovation:** Got a groundbreaking idea? Our team's deep knowledge of these programming languages and cutting-edge technologies will bring it to life.

c) **Deliver Cross-Platform Functionality:** Reach your audience on any device with apps built for web, iOS, and Android.

d) **Ensure Scalability:** Build for the future. We use technologies that can grow alongside your business.

Benefits of Custom Development with Our Expertise:

a) **Increased Efficiency:** Automate tasks and streamline processes for a more productive team.

b) **Enhanced User Engagement:** Create user-friendly and interactive experiences that keep users hooked.

c) **Data-Driven Decisions:** Gain valuable insights into user behavior with built-in analytics.

d) **Competitive Advantage:** Stand out with a unique app that offers exceptional value..

Custom Application Development Services clients : Government, Government Agencies, Financial Institutions and Private Companies

Our Award & Recognition Our Client

We are grateful when our efforts earn recognition in the important areas of service quality and internet security. The accolades we receive are thanks to the hard work and ingenuity of our dedicated Pos Digicert Team.

Award & Recognitions

WEBTRUST FOR CA

TMMI CERTICATION LEVEL 3

QUALITY MANAGEMENT SYSTEM ISO 9001:2015

INFORMATION SECURITY MANAGEMENT SYSTEM ISO/IEC 27001:2013

RECOGNISED DATE TIME STAMPING PROVIDER

ADOBE APPROVED TRUST LIST

LICENSED CA FOR REPUBLIC OF UGANDA

CLOUD SIGNING CONSORTIUM

Our Client

POS Digicert

Government

	eFiling / MyTax	GPKI	ePerolehan	eKYC /Mobile Apps	Digital CTC	PKIaaS
Use Case	Signing of Tax Submissions	Authentication and signing of data between gov. agencies	Signing of tender submissions	User Onboarding & Mobile Apps	Purchase of Company Documents which have been Digitally Certified	Digital Signing & Authentication for various gov & public applications
User	Public	Government Officers	Company	Public	Public / Company	Public (Ugandan Nationals)
Use Frequency:	Annually	Daily	Daily	Daily	Daily	Daily

Let’s Connect!

We'd love to hear from you! Whether you have questions, need more information, or are ready to take the next step, we're here to help.

☎ **Call US :** +603 8800 6000

Our team is ready to assist you with any inquiries you may have.

Email US : sales@posdigicert.com.my

Drop us an email, and we'll get back to you as soon as possible.

Visit Our Website : www.posdigicert.com.my

Explore our offerings and learn more about how we can help you.