Dohatec

DOHATEC NEW MEDIA

Independent software vendor, custom development, system integrator, certifying authority

www.dohatec.com | Excellence, always...

Our Vision

Be a world standard software source
fueled by professional competence and national pride
in a networked world, enhancing earnings from the global marketplace
and enriching the workforce intellectually, professionally and economically

Excellence, always...

SELECTED PROJECTS

Our Developed Projects

1 PQcal OMS

Order Management System (OMS) for NASDAQ exchanges

2 e-GP System, Government of Bhutan and Nepal

National Electronic Government Procurement System — Public Procurement Monitoring Office (PPMO)

3 e-Government Procurement, Bangladesh

Online PMIS for IMED, Ministry of Planning; e-GP, MIS and Online Advertisement Information System

4 Electronic Construction Permitting System (ECPS)

RAJUK • Urban Resilience Project — digital governance and BNBC compliance for Dhaka

Dohatec

Dohatec CA
Certifying Authority

Bangladesh Certifying Authority & National PKI

Regulation • Trust infrastructure • Digital certificates • Applications

NATIONAL PKI

Bangladesh's Digital Trust Ecosystem

1 Regulator

CCA sets the regulatory and supervisory framework for licensed CAs and national PKI.

2 Trust Infrastructure

Bangladesh Root CA and subordinate CA certificates support a common trust chain.

3 Service Delivery

Licensed CAs provide certificates and trust services for people, organisations and systems.

Objective: trusted electronic transactions — authenticity, integrity, confidentiality, non-repudiation.

Dohatec

Legal Foundation & the Role of CCA

Legal & regulatory foundation

- ICT Act, 2006 — electronic records, digital signatures, CCA oversight
- Amendments (2009, 2013)
- IT (Certifying Authority) Rules, 2010 — CA licensing, certification, compliance
- CCA policies and guidelines turn the law into technical, operational and audit requirements

CCA: regulator & national PKI authority

- License, suspend or revoke CA licences
- Supervise CAs; set standards and personnel qualifications
- Maintain PKI policies, guidelines and quality controls
- Oversee national PKI trust infrastructure and certificate repository
- Coordinate PKI audits and enforcement

NATIONAL PKI

How the National PKI Trust Model Works

1 Bangladesh Root CA

National trust anchor

2 Licensed Certifying Authorities

Subordinate CA certificates under the national framework

3 Subscribers

Individuals • officials • organisations • devices

Outcome: signed documents • authenticated access • trusted digital services

Dohatec

Digital Certificate Lifecycle

1 Enrol

Application and identity validation

2 Issue

Key pair / CSR processing and issuance

3 Use

Signing, authentication or encryption

4 Validate

Chain, signature, expiry and revocation checks

5 Renew / Revoke

Lifecycle control and status publication

Trust depends on the complete lifecycle — not simply on issuing a certificate.

Core Activities of Licensed CAs

1 Identity & Registration

Onboarding, identity proofing, approval workflows, RA controls

2 Certificate Operations

Issuance, renewal, suspension, revocation, publication

3 Security Operations

HSM controls, key ceremonies, access management, backup and DR

4 Validation Services

OCSP / CRL status, relying-party support, chain validation

5 Governance & Audit

CPS / CP, policies, logs, incident response, audits

6 Customer & Ecosystem

Support, integration guidance, awareness, interoperability

Certificate & Trust-Service Categories

1 Signing certificates

Individual / organisational — authenticate signer, protect integrity

2 Encryption certificates

Confidentiality through public-key encryption

3 SSL/TLS certificates

Authenticate websites, secure connections

4 System / device certificates

Machine identity, secure system-to-system communication

5 Code-signing certificates

Verify publisher identity and code integrity

6 Supporting services

OCSP, CRL, timestamping, remote signing, e-sign APIs

REFERENCE

CCA Policies & Guidelines

1. DSC Interoperability Guidelines, 2025
2. PKI Enabled Application Guideline
3. CA Personnel (Qualification & Experience) Guideline
4. CA Licensing Guideline
5. PKI Auditing Guideline
6. Bangladesh Root CA CP & CPS
7. CCA e-Sign API Specification for online e-KYC

Dohatec

Trust, Assurance & Priorities

Foundational controls

- Strong identity proofing
- Secure key generation and HSM custody
- Separation of duties, controlled access
- Independent audits
- Reliable OCSP / CRL publication
- Incident response and continuity

Forward priorities

- Wider adoption across public and private services
- Consistent relying-party validation
- Interoperability and user experience
- Remote / cloud signing governance
- Awareness and skills
- Crypto-agility, post-quantum readiness

A trusted PKI is a shared responsibility of regulator, CAs, subscribers, application owners and relying parties.

Dohatec e-Sign

DohatecCA Certifying Authority

Dohatec CA Updates

Dongle and Browser based DSC

The Private key generated is to be protected and kept secret. The responsibility of the secrecy of the key lies with the owner

The key is secured using

- Smart Cards
- Hardware Tokens

• The Private key is generated in the crypto module residing in the smart card.

• The key is kept in the memory of the smart card.

• The key is highly secured as it doesn't leave the card, the message digest is sent inside the card for signing, and the signatures leave the card.



Hardware Token



Smart Card

Dohatec

Dohatec eKYC: 4 Escalating Layers of Trust

1 Phase 1: Contact verification

Mobile number and email input with OTP retrieval — dual-factor anchor

2 Phase 2: Identity proof

Real-time NID capture with OCR extraction of name, date of birth and ID number

3 Phase 3: Liveness

Face verification and liveness check matched against government records

4 Phase 4: Secure the future

Profile confirmation, residential data and 6-digit PIN creation

The 6-digit PIN acts as the cryptographic key — every future signature is bound to the verified individual.

e-Sign Signing Workflow

1 Login

Email or mobile credentials

2 Dashboard

Credits, usage metrics, tools

3 Upload

Drag-and-drop PDF, 6MB limit

4 Place signature

Preview and position block

5 Designation

Designation and institution

6 Crypto package

Choose algorithm

7 Enter PIN

Authorises key use

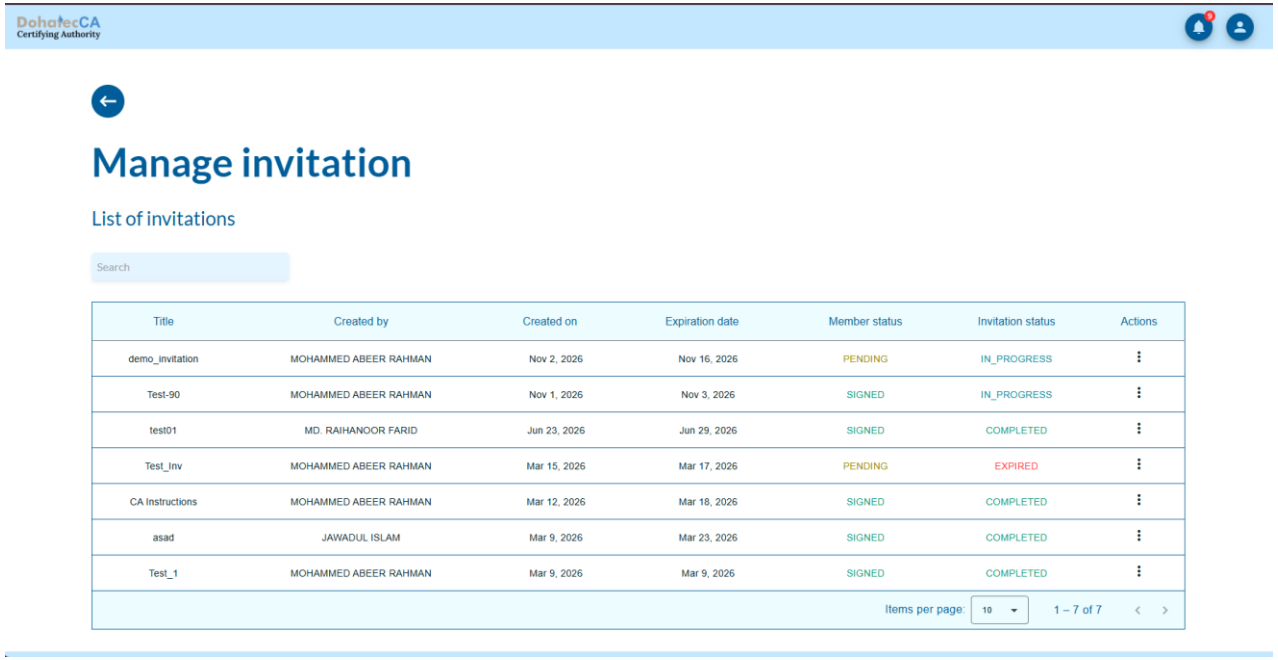
8 Sign

Cert generated, signature applied

9 Result

Success with audit trail

Organisation Invitations & Management



1 Invite & add members

Name the invitation, set expiry, add members by name, phone and email

2 Manage invitations

Track and manage existing invitations in one list

Dohatec

Visible Digital Seal (e-Seal)

The modern, tamper-proof official stamp that bridges digital trust and physical printed paper across Bangladesh.

SIMPLE LIFECYCLE

How It Works in Everyday Practice

1 Issue with e-Seal

STEP 01

The organization generates the document (certificate, permit, or trade license). The system automatically embeds an encrypted e-Seal QR code on the page.

2 Distribute Anywhere

STEP 02

The document can be downloaded as a PDF or printed on standard paper. The digital seal retains full mathematical integrity across both formats.

3 Scan & Verify

STEP 03

A bank officer, employer, or government official scans the QR code. The app instantly shows the exact original data and confirms the authentic issuing authority.

Think of it like an unbreakable digital notary stamp: Even if an imposter changes a grade or number on the printed sheet, scanning the QR code reveals the genuine government truth in under 3 seconds.

Dohatec

Dohatec

Thank You

Dohatec New Media • www.dohatec.com • Excellence, always...