SignDex



FOR MINISTRIES AND AGENCIES OF THE GOVERNMENT OF MALAYSIA

Trusted digital signing and eKYC for the Government of Malaysia

Secure SaaS, hosted in Malaysia with full data residency.

Crest Infosolutions Sdn Bhd,
Malaysia

Chris Chang Pei Shan || November 2026

Executive summary

THE CHALLENGE

Paper approvals slow public services

Wet-ink approvals, couriered documents and manual identity checks add days to services for citizens and businesses.

OUR PROPOSAL

Trusted signing as a Malaysian SaaS

Multi-CA digital signatures, eKYC and MyDigital ID, hosted in Malaysia and integrated through OpenAPI.

THE DECISION WE ASK FOR

A pilot with a lead agency

Start with internal approvals and one high-volume citizen service. Agree the discovery workshop date.

Outcome: faster public services, verified identity, and records that stay in Malaysia under agency control.

Digital government needs trusted identity and signatures

10 million

MyDigital ID accounts by February 2026, with 17 million targeted by end of 2026

RM458 million

Losses from e-financial fraud in 2025, up from RM65 million in 2024

Cloud first

The National Cloud Computing Policy (2025) moves public services to cloud, with data sovereignty

SignDex brings verified identity and licensed digital signatures to government services, hosted in Malaysia.

Sources: Malay Mail (12 Feb 2026); Ministry of Digital, National Cloud Computing Policy (Aug 2025).

From paper files to a same-day digital process

TODAY

Printed for approval → Physical file routing → Wet-ink signature → Courier or counter visit → Manual filing

Days to weeks per document, with files that can be delayed or lost

WITH Digital Signing

Generated by agency system → Routed by workflow → Sent securely online → Verified and digitally signed → Stored securely with evidence

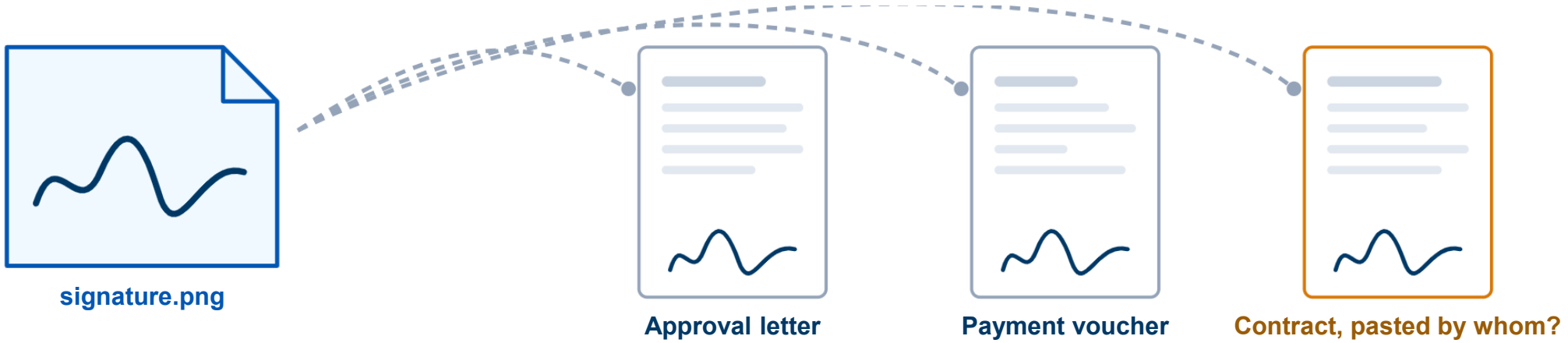
Can complete the same day, with a full audit trail

Fewer counter visits and courier runs, and faster decisions for citizens and businesses.

ANOTHER FAMILIAR STORY

The copy-paste signature

To save time, a manager keeps a picture of their signature and pastes it into PDFs. Every PDF they send out now carries that picture, ready for anyone to reuse.



⚠ All three look identical. Nobody can prove who actually signed.

REAL EXAMPLES, OPENED IN ADOBE ACROBAT

Same look, Different proof

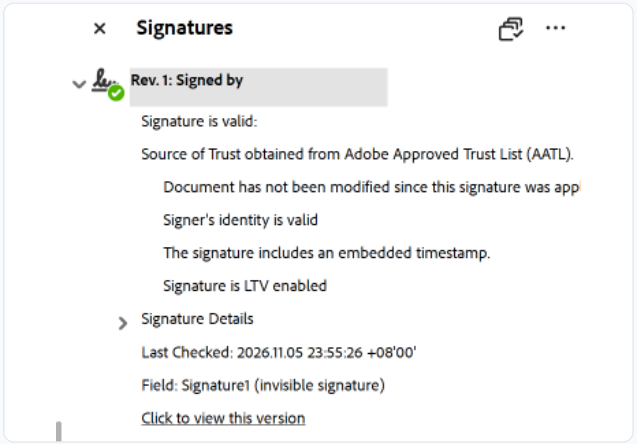
Image only



No certificate. Nothing for Adobe to check.

Can be copied, and edits go unnoticed.

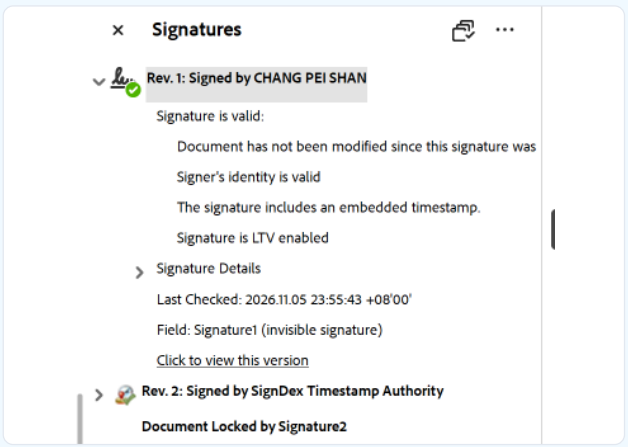
Platform certificate



Signed by: the platform.

Shows the document is unchanged, but not who signed.

Signer's own certificate



Signed by: the signer, with a trusted digital ID in Malaysia.

Proves who signed and that nothing changed. This is SignDex.

SignDex: One platform for identity, signature and evidence

Verify

eKYC with MyKad or passport, liveness detection, and MyDigital ID

Sign

Long-term validation (LTV) digital signatures with certificates from licensed CAs

Prove and store

Sealed evidence and signed PDFs, stored in Malaysia

Delivered as SaaS in a commercial cloud in Malaysia, with full data residency and privacy.

Enterprise capabilities, ready out of the box

Send and track

Requests with routing, reminders and live status

Flexible workflows

Sequential, parallel, approval and quorum

Templates

Controlled forms with preset signature fields

Identity policies

TOTP, SSO, eKYC or MyDigital ID by document

Evidence and audit

Tamper-proof logs of every signing event

OpenAPI REST APIs

Integrate any agency application, with webhooks

Verified identity for every signer

Capture

MyKad, passport or driving licence

Validate

Document checks and data extraction

Liveness

Confirms a live person, not a photo

MyDigital ID

National digital identity sign-in (in progress)

Assurance matched to risk

LEVEL 4	Licensed-CA digital certificate
LEVEL 3	eKYC or MyDigital ID
LEVEL 2	Advanced OTP
LEVEL 1	Secure email link

Each agency sets the level per document and risk.

Multi-CA platform, built for Malaysia's trust ecosystem

INTEGRATED

Trustgate CA

Licensed certification authority under the Digital Signature Act 1997

IN PROGRESS

Pos Digicert CA

Licensed certification authority under the Digital Signature Act 1997

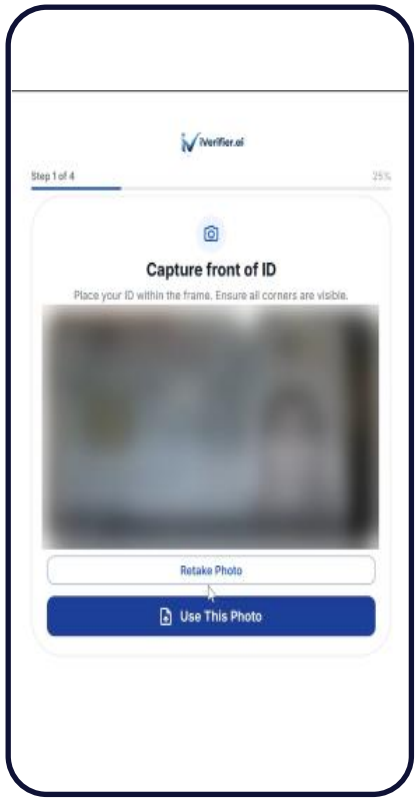
IN PROGRESS

MyDigital ID

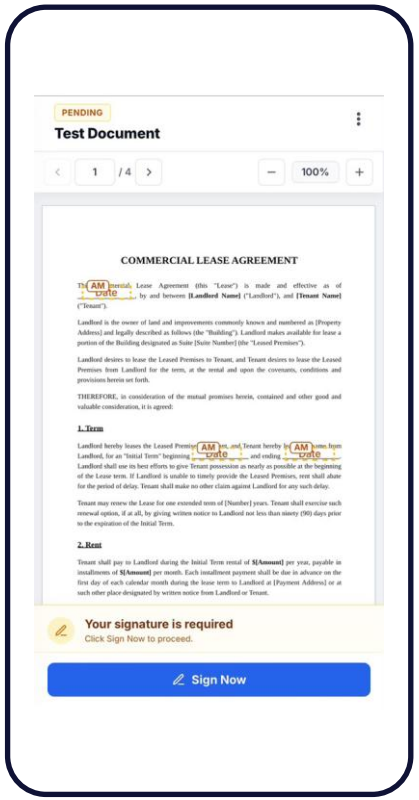
National digital identity, verified against National Registration Department records

Agencies choose the CA per document type or policy, through one workflow and one API, with no lock-in.

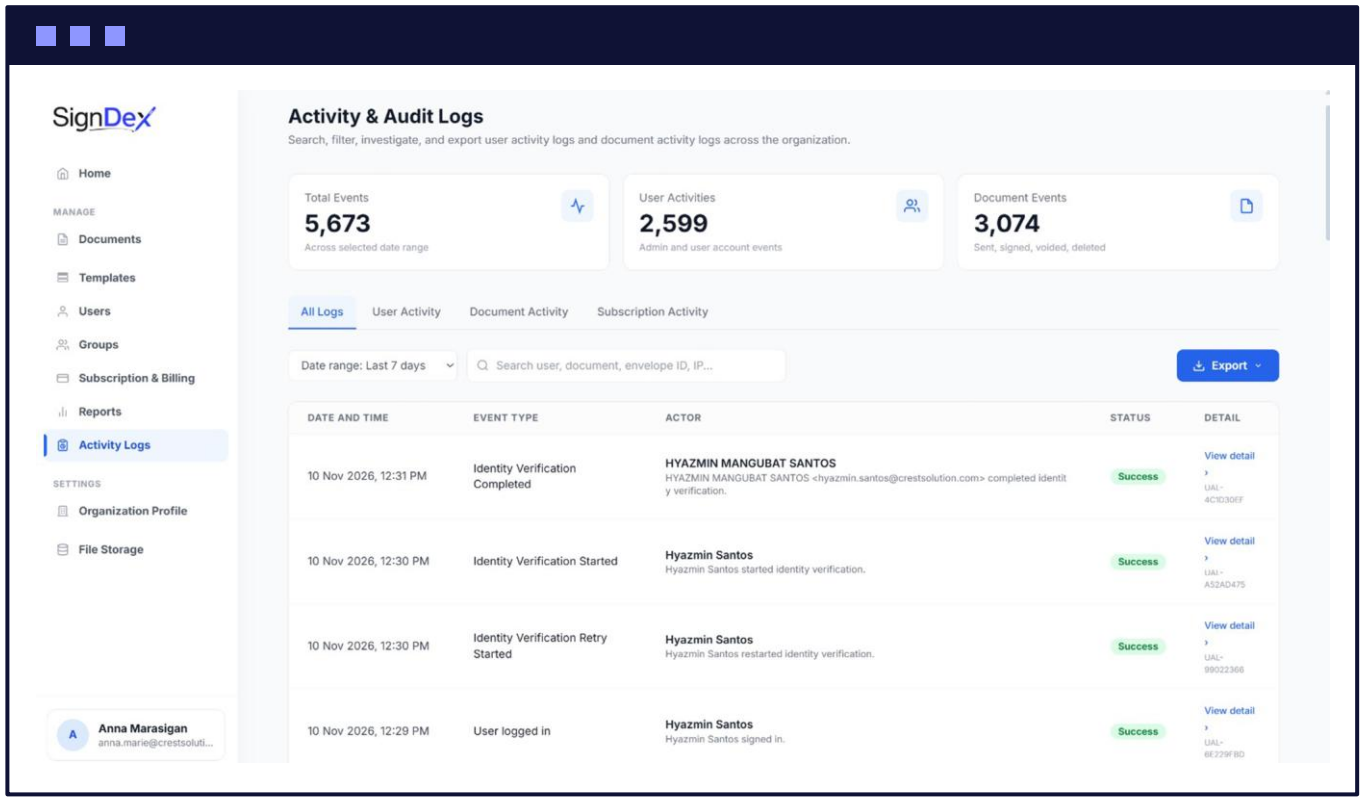
SignDex in action



eKYC with MyKad



Mobile signing



Admin console: workflows and audit trail

Use cases across ministries and agencies

Internal approvals
Approval memos, circulars and meeting minutes

Licences and permits
Digitally signed licences, permits and certificates

Citizen and business services
Applications and declarations signed online with eKYC

Contracts and procurement
Vendor contracts, letters of award and acceptances

HR and administration
Offer letters, staff declarations and approvals

Inter-agency correspondence
Official letters signed and exchanged securely

Suggested start: internal approvals and one high-volume citizen service, then expand.

From request to sealed evidence in six steps

1

Initiate

From the agency system via API, or the console

2

Notify

Secure link with reminders and status

3

Verify

eKYC, MyDigital ID or OTP, by policy

4

Sign

Digital signature with a licensed-CA certificate

5

Seal

PAdES B-LTA signature level and trusted timestamp

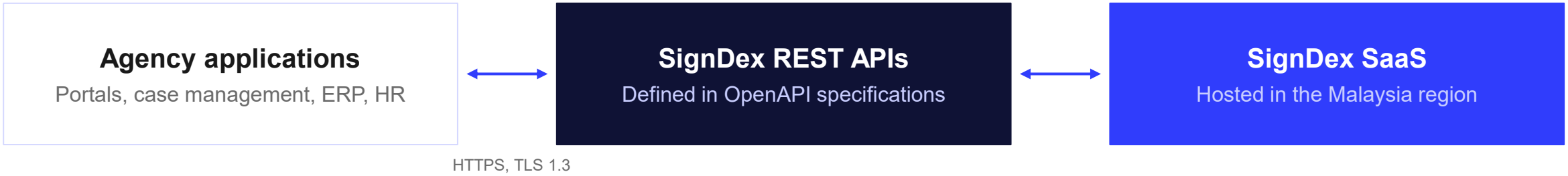
6

Store

PDF and evidence kept in Malaysia

Workflows: sequential, parallel, approval and quorum. Citizens and vendors need no account.

Integrate any agency application through OpenAPI



OpenAPI specification

A machine-readable contract; generate clients in any language.

Core operations

Create requests, add signers, track status, download signed PDFs and evidence.

Webhooks

Status events pushed back to agency systems in real time.

Sandbox tenant

Build and test integrations before go-live.

One integration pattern for every ministry and agency, with no infrastructure to install.

Security and trust agencies can defend

AES-256

Data at rest

TLS 1.3

Data in transit

LTV

PAdES B-LTA signature level

Multi-CA

Licensed Malaysian CAs

Every signing event is captured in a sealed, tamper-evident audit trail.

Aligned with

- Digital Signature Act 1997
- Electronic Commerce Act 2006
- Electronic Government Activities Act 2007
- Cyber Security Act 2024
- Personal Data Protection Act 2010

ISO 9001 | ISO 27001

Crest Infosolutions: certified quality and information security management

Full data residency and privacy in Malaysia

Hosted in Malaysia

Documents, evidence, backups and logs stay in the Malaysia region.

Isolated per agency

Each agency has its own tenant, users, policies and audit trail.

Dedicated keys

AES-256 encryption with keys per agency; TLS 1.3 in transit.

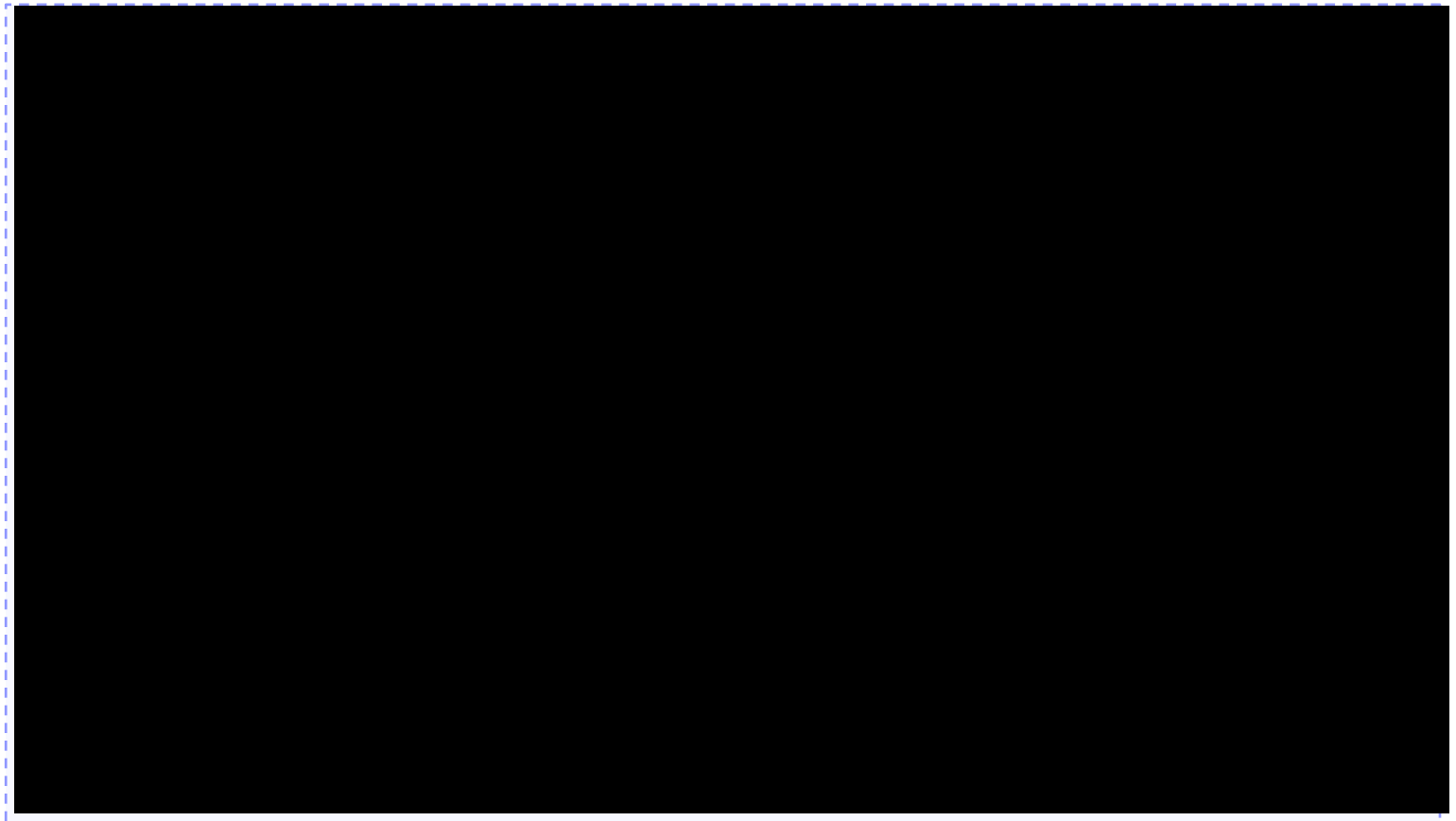
Privacy by design

Data minimisation, retention rules and full access logging.

Supports data sovereignty under Malaysia's National Cloud Computing Policy.

Cloud provider and region are confirmed in the service agreement.

Live demo



Suggested demo flow

1. Agency system creates a request via API
2. Applicant verifies with MyKad and liveness
3. Officer signs with a Trustgate certificate
4. Review evidence and the signed PDF

QR

Scan to try eKYC on your own phone

SaaS service model: Crest runs it, each agency controls it

CREST RUNS

- 24x7 monitoring and incident response
- Patching, upgrades, backup and DR
- CA connections and certificate lifecycle
- L1 to L3 support

TOGETHER

- Service levels and reports
- Quarterly service reviews
- Change approvals
- Security reviews and audits

AGENCY CONTROLS

- Users, roles and SSO
- Templates and workflows
- Signing and identity policies
- Retention rules

One shared platform: each agency onboards to its own tenant, with no infrastructure to buy or run.

Illustrative scope. Service hours, SLAs and responsibilities are finalised in the service agreement.

Indicative onboarding for each agency

Discover	Configure	Integrate	Go live
Weeks 1 to 2	Weeks 3 to 4	Weeks 5 to 8	Week 9 onward
• Use-case workshop • Security and data review • CA and identity choices	• Agency tenant and SSO • Roles and policies • Templates and workflows	• OpenAPI integration in sandbox • User acceptance testing • Officer training	• Production launch • Add services in waves

Internal approvals can go live first, before API integration is complete.

Indicative only. Depends on agency security reviews, procurement and integration scope.

Benefits for agencies, citizens and businesses

Faster services

Approvals and applications completed online, without counter visits

Lower risk

Verified identity and tamper-evident, licensed-CA signatures

Data sovereignty

Documents and evidence stay in Malaysia

Lower cost

No infrastructure to buy; less printing, courier and storage

Measured in the pilot: turnaround time, documents signed digitally, counter visits avoided and cost per document.

No lock-in: agencies keep their records and their choice of CA

Owned by the agency

Signed documents and evidence can be exported at any time.

Verifiable anywhere

PDFs with long-term validation (LTV) stay verifiable in any PDF reader.

Choice of CA

Multi-CA support avoids dependence on a single certificate provider.

Exit, data export and handover terms are defined in the service agreement.

Why SignDex and Crest Infosolutions

Multi-CA by design

MSC Trustgate integrated; Pos Digicert and MyDigital ID in progress

Hosted in Malaysia

SaaS with full data residency and per-agency isolation

API-first

OpenAPI specifications and webhooks for any agency system

CREST
— Ideate — Innovate — Implement —

Crest Infosolutions Sdn Bhd

Local delivery and support in Malaysia

ISO 9001 | ISO 27001

Certified quality and information security

Next steps: from conversation to pilot

1. **Discovery workshop**
   Lead agency, priority services and integration points

2. **Security and compliance review**
   Data residency, privacy and cyber security requirements

3. **Pilot scope**
   Internal approvals and one citizen service

4. **Commercial agreement**
   Subscription model, service levels and support

DECISIONS NEEDED

- Lead agency and sponsor
- First services for the pilot
- Preferred CA and identity options
- Integration and security contacts

SignDex

Thank you

Next: agree the discovery workshop with a lead agency

Chris Chang Pei Shan
IT Product Manager, Crest Infosolutions

Chris.chang@crestsolution.com