

Web Development Brief

AIT DPI University Grant — Call for Proposals Page and Submission Portal

Sep 28, 2026 · @SML - Kyi

1. Project Overview

Client: Asian Institute of Technology (AIT) **Project Name:** DPI University Grant — Call for Proposals

Deliverable: (1) A public-facing Call for Proposals web page, and (2) an online submission portal for university applicants.

Purpose

AIT is opening a grant call for university research partners in Asia-Pacific. The web page will announce the call publicly. The submission portal will allow eligible universities to submit their proposals online.

Primary Audience

University leaders, research deans, and academic staff at universities in the following countries: Bangladesh, Bhutan, Indonesia, Laos, Nepal, Pakistan, Papua New Guinea, Philippines, Singapore, Sri Lanka, and Vietnam.

Key Dates to Note

Activity	Date
Page must be live	15 October 2026
Submission portal opens	15 October 2026
Submission portal closes	30 November 2026, 5:00 PM ICT

Language

All content is in **English only**.

2. Website Page Requirements

The Call for Proposals page must be a single, scrollable public web page integrated into the existing AIT website. *It should be accessible from the AIT homepage via a clear link or banner.*

Required Sections (in order)

#	Section	Content Summary
1	Hero / Banner	Page title: "Call for Proposals — AIT Digital Public Infrastructure University Research Partnership". Short tagline. Deadline countdown or prominent deadline date. A clear "Apply Now" button linking to the submission portal.
2	Programme Overview	Two short paragraphs: (a) what AIT is offering, and (b) why this partnership matters. AIT is the lead institution and sponsor.
3	Background and Challenges	<i>Bullet list of 5 regional DPI challenges (as written in the content document).</i>

#	Section	Content Summary
4	What Partners Will Do	Table of 5 expected outcomes with evidence of achievement. Followed by a bullet list of additional responsibilities.
5	What Partners Will Receive	Bullet list of benefits: funding (up to USD 100,000), 18-month grant, capacity building, sandbox access, annual events, community membership.
6	Research Themes	Six Research Themes - Website Requirements - ai4dpi.ait.ac.th - Call for Pro...
7	Eligibility Criteria	Sub-section 1: list of 11 eligible countries. Sub-section 2: numbered list of 3 eligibility requirements. Include a note box: "Both technical capacity and a government relationship are required."
8	Evaluation Framework	Table with 5 criteria, each weighted at 20%, with what evaluators look for.
9	Key Dates	Timeline table (as per the approved dates). Highlight the application deadline in bold or a distinct colour.
10	How to Apply	Submission requirements, file format, and a prominent "Submit Your Proposal" button linking to the portal. Brief explanation of Stage 1 and Stage 2.
11	Information Sessions	Table of 3 session dates (27–29 October 2026). Note that details on time and registration will follow.
12	Contact / Questions	Contact name, email, and question deadline. (<i>Placeholders — to be filled by AIT.</i>)
13	Footer / Disclaimer	AIT logo, standard disclaimer, and copyright.

Navigation

- Include a **sticky navigation bar** at the top with anchor links to each section.
- Include a **"Back to Top"** button on the right side of the page.
- The **"Apply Now" / "Submit Your Proposal"** button must appear at minimum in the hero section and in Section 10 (How to Apply).

Downloadable Documents

Provide a clearly visible download link for:

- The full **Call for Proposals document** (PDF)
- The **Proposal Template** (Word .docx) (*to be provided by AIT*)
- The **Budget Template** (Excel .xlsx) (*to be provided by AIT*)

3. Submission Portal Requirements

The submission portal is an online form embedded in the AIT website (or hosted as a separate secured page linked from the main Call for Proposals page). It must be open from **15 October 2026** and close automatically at **30 November 2026, 5:00 PM ICT (UTC+7)**.

Form Fields

All fields are required unless marked optional.

Section A — Applicant Institution

Field	Type	Notes
University / Institution Name	Text	
Country	Dropdown	Show only the 11 eligible countries
University Website	URL	
Primary Contact Name	Text	
Primary Contact Title / Position	Text	
Primary Contact Email	Email	System sends confirmation to this email
Primary Contact Phone	Text	Optional

Section B — Research Proposal

Field	Type	Notes
Research Pillar	Dropdown	AI for DPI / Facial Verification and Open-Source PAD / Wallets and Credentials
Proposed Project Title	Text	Max 150 characters
Brief Summary of Proposal	Textarea	Max 500 words. Plain text only.

Section C — File Uploads

File	Format	Max Size	Notes
Proposal Document (PDF)	.pdf	20 MB	Required
Proposal Document (Word)	.docx	20 MB	Required
Budget (Excel)	.xlsx	5 MB	Required
Letter of Support from National ID Authority	.pdf	5 MB	Optional at Stage 1; required at Stage 2
Additional Supporting Documents	.pdf	10 MB	Optional. Max 1 file.

Section D — Declaration

- Checkbox: *"I confirm that the information provided in this application is accurate and complete."* (Required)
- Checkbox: *"I confirm that this university meets all eligibility criteria stated in the Call for Proposals."* (Required)

- Checkbox: *"I have read and understood the terms of this Call for Proposals."* (Required)

Validation Rules

- Country field must only allow selection from the 11 eligible countries. If the user selects an ineligible country, display a message: *"We are sorry. Applications from your country are not accepted in this call."*
- Email field must validate correct email format.
- All three declaration checkboxes must be ticked before submission is allowed.
- The portal must display a clear error message for any missing required fields before submission.
- File types must be validated on upload. Only accepted formats (.pdf, .docx, .xlsx) are allowed.

Submission Confirmation

- After successful submission, display an on-screen confirmation message: *"Thank you. Your application has been received. A confirmation email has been sent to [applicant email]. Please keep this for your records."*
- Send an automatic confirmation email to the applicant's primary contact email. The email must include:
 - o Application reference number (auto-generated)
 - o University name and research pillar selected
 - o Date and time of submission
 - o List of files successfully uploaded
 - o Key dates (shortlist notification, interview, final selection)
 - o Contact email for enquiries

Portal Closure

- The portal must close automatically at the deadline. After closure, display a message: *"The submission deadline has passed. This portal is now closed. Please contact [contact email] if you have questions."*
- Do not allow any new submissions after the deadline, even if a session was started before it.

4. Submission Guidelines (On-Portal Content)

The following guidelines must be displayed clearly on the submission portal page — above or alongside the form — so applicants understand what is required before they submit.

Before You Apply

Display this checklist prominently at the top of the portal:

Please ensure you have the following ready before you begin:

- Your university is located in one of the 11 eligible countries.
- Your university has an existing working relationship with your national digital identity authority.
- Your university has technical expertise in at least one relevant area (DPI, digital identity, PAD, or verifiable credentials).
- A completed proposal in English (PDF and Word format).
- A completed budget in USD (Excel format).
- All files are within the size limits stated below.

File Requirements

Display this table next to the upload section:

Document	Format	Max File Size
Proposal (PDF)	.pdf	20 MB
Proposal (Word)	.docx	20 MB
Budget	.xlsx	5 MB
Letter of Support (Optional)	.pdf	5 MB
Additional Documents (Optional)	.pdf	10 MB

Important Notes

Display these as a highlighted note box:

- Proposals must be written in **English**.
- The budget must be in **USD (United States Dollars)**.
- Late submissions will **not** be accepted. The portal closes automatically at the deadline.
- An invitation to Stage 1 does not constitute a commitment by AIT to award funding.
- AIT reserves the right to amend the terms of this call or cancel the process at any stage.

Help and Support

Display a visible help section at the bottom of the portal:

*For technical issues with the portal, contact: **[IT SUPPORT EMAIL — TO BE CONFIRMED]** For questions about the Call for Proposals, contact: **[PROGRAMME CONTACT — TO BE CONFIRMED]** Information sessions: **27, 28 and 29 October 2026***

5. Technical and Design Requirements

Design

- Follow **AIT's brand and style guide** (colours, fonts, logo placement).
- The page must be **mobile-responsive** (display correctly on desktop, tablet, and mobile phone).
- Use a **clean, professional layout** appropriate for an academic and government audience.
- Use AIT's institutional colours as the primary palette. Use white backgrounds for body content.
- All tables must be legible on mobile (horizontal scroll if needed).
- The **application deadline** must be visually prominent — consider a countdown timer or a highlighted date box.

Performance

- Page load time must be under **3 seconds** on a standard broadband connection.
- All downloadable files (PDF, Word, Excel) must be hosted on AIT's server, not a third-party service.

Accessibility

- The page must comply with **WCAG 2.1 Level AA** accessibility standards.
- All images must have alt text.
- Form fields must have visible labels.
- Error messages must be descriptive and clearly linked to the relevant field.

Security (Submission Portal)

- The portal must use **HTTPS** (SSL certificate required).
- File uploads must be scanned for malware before storage.
- Submitted data and files must be stored securely on AIT's server or an approved cloud storage provider.
- Access to submitted applications must be restricted to authorised AIT staff only.
- The system must not share or expose applicant data to third parties.

Browser Compatibility

The page and portal must function correctly on:

- Google Chrome (latest version)
- Mozilla Firefox (latest version)
- Microsoft Edge (latest version)
- Safari (latest version, macOS and iOS)

Integrations

Function	Tool / Approach
Automatic confirmation email	Email service (e.g. SendGrid, Mailchimp, or AIT's mail server)
File storage for submissions	AIT server or approved cloud storage (e.g. AIT SharePoint / Google Drive restricted folder)
Admin access to submissions	Password-protected admin dashboard or secure shared folder
Portal closure automation	Auto-close at deadline — no manual action required

6. Admin and Backend Requirements

AIT staff must be able to manage all submitted applications through a secure backend. The following functions are required.

Admin Dashboard

- A password-protected admin view accessible only to authorised AIT staff.
- Display all submissions in a sortable table with the following columns:
 - o Application reference number
 - o Date and time of submission
 - o University name
 - o Country
 - o Research pillar selected
 - o Primary contact name and email
 - o Files submitted (with download links)
 - o Status (e.g. Received / Under Review / Shortlisted / Not Shortlisted)
- Allow AIT staff to update the status of each application.
- Allow AIT staff to add internal notes to each application (not visible to the applicant).

Export Function

- Allow AIT staff to **export the full list of submissions** as an Excel (.xlsx) or CSV file, including all fields above.
- Allow bulk download of all uploaded files for a selected application or all applications.

Notifications to AIT

- Send an automatic email notification to a designated AIT inbox every time a new submission is received.
- The notification must include: applicant name, university, country, research pillar, and submission date/time.

Data Retention

- All submitted data and files must be retained for a minimum of **3 years** after the portal closes.
- AIT must be able to request a full data export at any time.

Access Control

- Admin access must require username and password login.
- Only AIT-designated staff accounts may access submitted applications.
- Access logs must be maintained (who accessed what, and when).

7. Pending Information from AIT

The following items must be confirmed by AIT before the page can go live. Please fill these in and return to the web team.

#	Item	Notes
1	Submission email or portal URL	Where applicants submit their proposals. Required for Sections 8 and 9 of the content page.
2	Programme contact name and email	For applicant enquiries. Required for the Contact section and the portal Help section.
3	Question submission deadline	The deadline for applicants to send questions. Required for the Contact section.
4	IT support contact email	For technical issues with the portal.
5	Proposal Template (.docx)	To be provided by AIT for download on the page.
6	Budget Template (.xlsx)	To be provided by AIT for download on the page.
7	Information session details	Time, platform (Zoom / Teams / etc.), and registration link for the 3 sessions (27–29 October 2026).

#	Item	Notes
8	Admin email for submission notifications	The AIT inbox that receives a copy of each new submission.
9	AIT brand and style guide	To be shared with the designer for colour, font, and logo consistency.

Action required: Please provide the above items to the web development team no later than **8 October 2026** to allow time for build and testing before the 15 October 2026 launch.

Audience : Academics and university leadership

needs to read carefully and find specific information quickly — eligibility, criteria, funding, and how to apply. A scrollable page with a sticky top navigation bar lets them jump to the section they need. It is professional, clean, and works well on both desktop and mobile.

Page Sections

1. Header
2. About the Programme
 - a. Brief background — what this grant aims to achieve, and AIT's role as regional hub
3. What partners will do
 - a. Key responsibilities: hub role, research, capacity building, community participation
 - b.
4. What partners will receive
 - a. Up to USD 100,000 funding, training (25+ people), hub membership, sandbox access, hackathon hosting
5. Eligibility
 - a. The 8 eligibility criteria (clear checklist format)
6. Selection Criteria
 - a. 5 weighted criteria (C1–C5) with percentages, and the 2-stage process
7. Key Dates / Timeline
 - a. Milestone dates from Oct 2026 to Apr 2029
 - b.
8. How to apply - portal
 - a. Stage 1 and Stage 2 steps, documents required.??
 - b. Link of the proposal document and template to download
 - c. Submission link >>
 - i. To consider how we can get their documents
 - ii.
9. FAQ session
10. Footer
 - a. Links ?? - to some specific requirements
 - b. Contact person email for the enquires

Contents - Call for Proposals	2
1. Programme Overview	2
Background	2
The Role of Universities	2
2. What Partners Will Do	3
3. What Partners Will Receive	4
4. Research Themes	4
5. Eligibility Criteria	5
5.1 Eligible Countries	5
5.2 Eligibility Requirements	5
6. Evaluation Framework	6
7. Key Dates	6

8. How to Apply	7
Submission Requirements	7
Where to Submit	7
Selection Process	7
9. Contact and Information Sessions	8
Information Sessions	8
Questions and Enquiries	8

Contents - Call for Proposals

AIT Digital Public Infrastructure University Research Partnership

Sep 24, 2026 · @Kyi - Draft Version

1. Programme Overview

The Asian Institute of Technology (AIT) invites universities in the Asia-Pacific region to apply for a **Digital Public Infrastructure (DPI) University Research Partnership**.

AIT is the lead institution and sponsor of this programme. Through this partnership, AIT will fund selected universities to conduct locally relevant DPI research, support their national governments, and contribute to a growing regional academic community.

Background

Countries across Asia-Pacific have made strong progress in issuing national IDs. However, most citizens do not yet use digital ID to access services online. This gap remains a key challenge for the region.

Key challenges include:

- **Vendor dependency.** Governments often rely on a single private vendor to build and maintain identity systems. This raises data sovereignty, cost, and long-term control concerns.
- **High cost of proprietary technologies.** Proprietary face verification and liveness detection tools are expensive, slowing digital ID adoption in several countries.
- **Limited awareness of open-source options.** Many governments are unaware that mature open-source alternatives exist, or lack the technical capacity to evaluate them.
- **Technical complexity.** Open-source systems can be difficult to deploy, especially for institutions with limited technical staff.
- **Inclusive use cases.** Effective use cases — such as subsidies for smallholder farmers, gender-intentional KYC for women entrepreneurs, or portable health records for elderly and migrant communities — require direct engagement with the people they serve.

The Role of Universities

Universities are uniquely positioned to address these challenges. As independent institutions, they can produce open, vendor-neutral knowledge, provide independent technical advice to national ID authorities, and build local expertise that reduces reliance on external vendors.

Through this Call for Proposals, AIT invites universities to become research partners. Selected partners will produce and disseminate localised DPI knowledge within their own countries, conduct applied research, and validate findings in a technical sandbox environment.

2. What Partners Will Do

Each selected partner university is expected to achieve five outcomes in its country.

Expected Outcome	Evidence of Achievement
1. Locally relevant research completed	The university completes research in one of three areas: AI for DPI; face verification and Presentation Attack Detection (PAD); or digital wallets and credentials. Findings are published openly, and any software is released under the Apache 2.0 open-source licence.
2. Independent advice provided to the national identity authority	The university provides evidence-based, vendor-neutral technical advice to help the national identity authority assess suitable technologies and implementation options.
3. National evidence strengthened	The university completes a local DPI adoption survey and works with government or community stakeholders to design at least one use case suited to the country's needs.
4. DPI knowledge included in university teaching	At least one module on DPI or open-source digital identity is incorporated into an existing computer science or data science programme.
5. Regional academic collaboration strengthened	The university actively contributes research, knowledge, and experience to the Asia-Pacific DPI academic community and continues participating beyond the individual research activity.

In addition, each partner university is expected to:

- Lead its approved research and maintain the government relationship required for the work.
- Conduct local engagement and adoption surveys.

- Host or participate in local hackathons.
- Attend hackathons and conferences organised by AIT.
- Develop its teaching contribution and share findings openly.
- Identify staff responsible for delivery and grant administration.

3. What Partners Will Receive

Selected partner universities will receive the following support from AIT:

- **Research funding of up to USD 100,000.** The final award is determined by AIT based on its review of the proposed activities and budget.
- **Grant duration of up to 18 months**, from January 2027 to July 2028.
- **Train-the-Trainer capacity building**, with at least 25 people from each university involved.
- **Membership in the MOSIP Asia-Pacific Regional Hub** governance structure.
- **Access to AIT's technical sandbox environment** for validating research and use cases.
- **Participation in annual convenings** and hackathons organised by AIT.
- **Access to a community-governed GitHub organisation**, mailing list, and communication channel for Asia-Pacific DPI developers.
- **Rotating hackathon hosting and community leadership** responsibilities from Phase 3 onwards.

4. Research Themes

Applicants must propose research under one of the following three pillars. The fourth pillar, Academic Community, is a shared responsibility of all partners and is not a research topic.

Pillar	Focus
AI for DPI	Research on how artificial intelligence tools and agents can be integrated into digital public infrastructure. This includes developing and testing open-source tools that monitor, maintain, and automate the health of a deployed digital identity platform. Research should result in a white paper and an implementation playbook.
Facial Verification and Open-Source PAD	Development and certification of an open-source face verification and Presentation Attack Detection (PAD) module. PAD detects attempts to deceive an identity system using a photograph, video, or mask. The module should be tested using datasets that represent populations across the Asia-Pacific region, and guidance should be published for integrating it with open-source digital wallets.

Wallets and Credentials

Research on how open-source digital wallets can be used for remote identity verification — allowing people to prove their identity online without visiting an office. Research should also address how these wallets can work with national identity systems that do not use open-source identity platforms.

Applicants should explain the local problem, the research question, the proposed activities, and the evidence that will show whether the approach works. The research should be achievable within the available funding and the agreed schedule.

5. Eligibility Criteria

5.1 Eligible Countries

Applications are accepted from universities in the following countries:

1. Bangladesh
2. Bhutan
3. Indonesia
4. Laos
5. Nepal
6. Pakistan
7. Papua New Guinea
8. Philippines
9. Singapore
10. Sri Lanka
11. Vietnam

5.2 Eligibility Requirements

An applicant university must meet **all** of the following criteria:

1. **Eligible location.** The university must be located in one of the countries listed above.
2. **Institutional relationship.** The university must have a substantive, pre-existing working relationship with its national identity authority. This relationship must be established **before** the execution of a Memorandum of Understanding (MoU) or Memorandum of Agreement (MoA) with AIT.
3. **Technical expertise.** The university must demonstrate expertise in at least one of the following areas:
 - Digital Public Infrastructure
 - Digital Identity Systems
 - Presentation Attack Detection
 - Verifiable Credentials

Note: Technical capacity alone does not compensate for the absence of an established government relationship. Both are required.

6. Evaluation Framework

Applications will be evaluated using AIT's Selection Scorecard. The scorecard assesses two dimensions jointly: the technical quality of the proposal and the strength of the institutional and government relationship.

Criterion	Weight	What Evaluators Look For
1. Expected Outcomes and Impact	20%	Alignment with national ID authority strategy; clear beneficiaries; scalability and replicability; sustainability of impact after the grant period.
2. Project KPIs	20%	KPIs that are specific, measurable, and tied to outcomes; realistic baseline and target values; alignment with programme deliverables.
3. Workable Plan and Activities	20%	Logical results chain from activities to outputs and outcomes; realistic timeline; proportionate budget; concrete curriculum integration plan; identified risks and mitigation strategies.
4. Strong Project Team and Institutional Support	20%	Named faculty with relevant expertise; administrative readiness; documented relationship with the national ID authority; evidence of local government and community engagement.
5. Finance	20%	Realistic and well-justified budget; demonstrated financial management capacity; track record in managing and reporting on externally funded grants.

Shortlisted applicants will be invited to an interview. One university will be selected per eligible country. The Terms of Reference (TOR) are published openly, and any eligible university may apply on equal terms.

7. Key Dates

Activity	Date
----------	------

Call Opens	15 October 2026
Information Sessions	27, 28 and 29 October 2026
Application Deadline	30 November 2026, 5:00 PM ICT (UTC/GMT +7)
Shortlisted Applicants Notified	15 December 2026
Interview for Shortlisted Candidates	3 January 2027
Final Selection Announced	10 January 2027
Partnership Agreement (MoU/MoA) Executed	January 2027
Grant Period Begins	January 2027
Grant Period Ends	July 2028

8. How to Apply

Submission Requirements

Applicants must submit the following by **30 November 2026 at 5:00 PM ICT (UTC+7)**:

- A completed proposal in **English**
- Both a **PDF version** and an **editable Word (.docx) version**
- A **budget prepared in USD** (United States Dollars)

Where to Submit

Submit your proposal to: **[SUBMISSION EMAIL OR PORTAL — TO BE CONFIRMED]**

Selection Process

Stage 1 — Shortlist. Applications are assessed on publicly verifiable indicators of institutional record. Three candidates per country will be shortlisted. Shortlisted applicants will be notified by 15 December 2026.

Stage 2 — Selection. Shortlisted applicants will attend an interview on 3 January 2027. A formal letter of support from the national ID authority endorsing the university is required at this stage. The final selection will be announced on 10 January 2027.

Note: An invitation to Stage 1 does not confer any entitlement or commitment by AIT.

9. Contact and Information Sessions

Information Sessions

AIT will hold three information sessions to answer questions about this call. All eligible universities are encouraged to attend.

Session	Date
---------	------

Session 1	27 October 2026
-----------	-----------------

Session 2	28 October 2026
-----------	-----------------

Session 3	29 October 2026
-----------	-----------------

Details on format, time, and registration will be shared separately.

Questions and Enquiries

Direct all questions to: **[CONTACT NAME / TEAM AND EMAIL — TO BE CONFIRMED]**

Deadline for submitting questions: **[QUESTION DEADLINE, TIME AND TIME ZONE — TO BE CONFIRMED]**

URLs

- Temporary link: <https://vdr.hqp.mybluehost.me/>
- Domain: ai4dpi.ait.ac.th

Call for Proposal requirements

Yes. For your **AIT DPI project**, I would design the Call for Proposal (CfP) as a **small grant/proposal-management platform**, rather than simply a Google Form with email attachments.

Since you want proposals from **international universities** for several technical areas—AI assistants, face verification/PAD, and verifiable credentials—the system should handle the entire lifecycle:

Discover → Register → Ask questions → Submit → Validate → Review → Clarify → Shortlist → Approve → Contract → Track implementation → Final reporting.

A useful reference point is the EU's Horizon Europe model: applicants create an institutional profile, select a call, submit through an online form, and can track/manage their proposals; some calls also use a two-stage concept-note/full-proposal process.

1. What AIT should publish

I would make **one master Call for Proposal document** plus **separate Technical Challenge Briefs**.

A. Master Call for Proposal

This should answer:

Section	What prospective universities need to know
About AIT DPI	Project background, objectives, Gates-funded program context
Purpose of CfP	Why AIT is inviting universities
Eligible applicants	Universities, research institutes, labs, consortiums
Geographic eligibility	Countries/regions permitted
Thematic areas	AI Assistant, Face Verification/PAD, VC, etc.
Expected outputs	Research prototype, benchmark, API, integration, report, open-source contribution, etc.
Duration	?
Funding	Maximum grant per proposal, eligible costs
Application stages	Concept note → full proposal, if you want two-stage selection
Evaluation criteria	Technical, research, DPI relevance, team, feasibility, etc.
IP policy	Ownership, licensing, foreground/background IP

Open-source requirements	What must be released and under which license
Data policy	What data can/cannot be used
Security/privacy	Especially important for biometrics
DPI interoperability	MOSIP, Inji, eSignet, VC ecosystem, APIs, standards
Deliverables	Expected outputs and milestones
Reporting	Technical/financial reporting
Payment	Milestone-based payment structure
Timeline	Opening, Q&A, submission, review, notification, contracting
Contact	Official CfP email and portal
Submission procedure	Explicit instructions

2. Create a separate Technical Challenge Brief for each area

This is particularly important for your project.

Instead of making the university read one enormous document, give them:

Track 1 — AI Assistant

For example:

Problem

Develop an AI assistant that can support users of a DPI ecosystem through natural-language interaction.

Then specify:

- target users
- languages
- expected use cases
- LLM requirements
- RAG requirements
- tool/function calling
- privacy requirements
- hallucination evaluation

- security
 - deployment environment
 - API requirements
 - expected integration with DPI components
 - expected demonstration
 - evaluation dataset
 - evaluation metrics
 - deliverables
-

Track 2 — Face Verification + Liveness/PAD

This needs to be much more technically precise.

For example:

Objective

Develop and evaluate a face verification and presentation-attack-detection solution suitable for remote identity verification.

Require applicants to address:

- face detection
- face quality assessment
- face embedding
- 1:1 verification
- liveness/PAD
- replay attacks
- printed-photo attacks
- screen attacks
- mask/partial-face attacks
- injection attacks
- demographic performance
- FAR/FMR
- FRR/FNMR
- ROC/DET
- latency
- mobile/web deployment
- on-device vs server-side processing
- privacy
- model licensing
- training-data provenance

For PAD, I would explicitly reference **ISO/IEC 30107** terminology and testing methodology. NIST's current digital identity guidance also explicitly addresses facial PAD and points to ISO/IEC 30107-3 testing.

That prevents universities from submitting proposals that simply say *"we will develop a liveness model"* without defining how it will actually be tested.

Track 3 — Verifiable Credentials

Here I would specify the interoperability target rather than simply asking:

"Develop a VC solution."

For example:

Objective

Research and develop interoperable Verifiable Credential capabilities that can integrate with an open-source DPI ecosystem.

Applicants should address:

- credential issuance
- credential holding
- presentation
- verification
- revocation/status
- selective disclosure
- privacy
- cryptographic integrity
- interoperability
- wallet integration
- issuer/verifier interfaces
- standards compliance
- API design
- security
- implementation/deployment

Since **W3C Verifiable Credentials Data Model 2.0** became a Recommendation in May 2025, you can explicitly reference VCDM 2.0 as a baseline.

3. Give applicants a "Proposal Pack"

I would create a downloadable **AIT DPI CfP Proposal Pack**.

Something like:

AIT-DPI-CFP-2026/

|

|— 01_Call_for_Proposal.pdf

|

|— 02_AI_Assistant_Challenge.pdf

|

- |— 03_Face_Verification_PAD_Challenge.pdf
- |
- |— 04_Verifiable_Credentials_Challenge.pdf
- |
- |— 05_Proposal_Template.docx
- |
- |— 06_Budget_Template.xlsx
- |
- |— 07_Technical_Requirements.pdf
- |
- |— 08_Evaluation_Criteria.pdf
- |
- |— 09_IP_and_Licensing_Framework.pdf
- |
- |— 10_Data_Privacy_and_Security_Requirements.pdf
- |
- |— 11_Declaration_of_Eligibility.docx
- |
- |— 12_FAQ.pdf

This makes the call feel like a **serious international research program**, rather than an informal university survey.

4. Don't make them upload one giant proposal blindly

I would structure the **online submission into sections**.

Applicant registration

First:

Institution

- University name
- Country
- University website
- Faculty/school
- Department
- Research laboratory
- Institutional address

Principal Investigator

- Name
- Position
- Email

- ORCID
- CV

Institutional representative

- Name
- position
- email

Technical lead

- Name
- email
- expertise

Team members

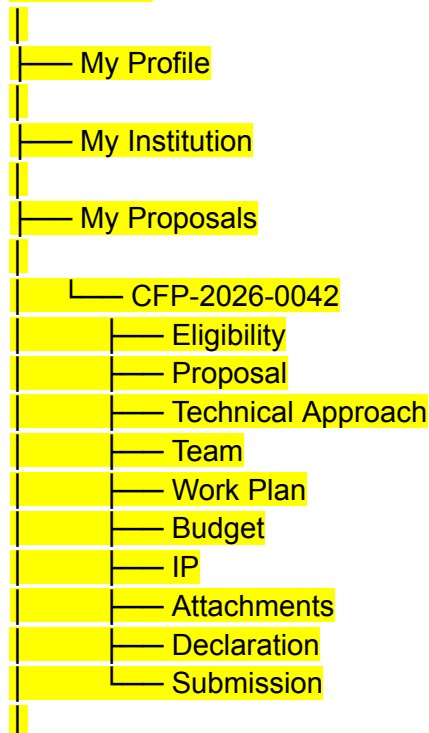
- Name
 - role
 - expertise
 - institution
-

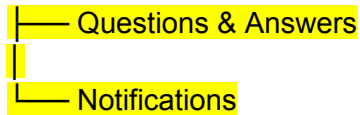
5. Then create a proposal workspace

After registration:

AIT DPI Proposal Portal

Dashboard





This is much better than sending attachments by email.

6. Use **Save-and-Continue**

This is extremely important for international universities.

They should be able to:

Save draft → leave → return tomorrow → continue.

The system should show:

Proposal completion: 72%

For example:

Proposal: Face Verification & PAD

- ✓ Applicant information
- ✓ Institution
- ✓ PI information
- ✓ Team
- ✓ Problem statement
- ✓ Technical approach
- ✓ Work packages
- ✓ Evaluation methodology
- ✓ Budget
- ✓ IP
- △ Declaration
- △ Final submission

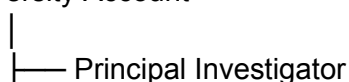
72% complete

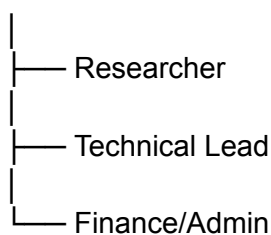
7. Allow multiple people from one university

For example:

University X

University Account





The PI should be able to invite team members.

Then permissions can be:

Role	Access
PI	Full proposal
Technical Lead	Technical sections
Researcher	Technical sections
Finance	Budget
Institutional Admin	Submission/official documents
AIT Administrator	Administrative review
AIT Technical Reviewer	Assigned proposals only
AIT Evaluation Committee	Assigned evaluation
Super Admin	Everything

8. Authentication should be stronger than ordinary email/password

For international institutions, I would support:

Option A — Email verification

Minimum requirement:

Email + password + email OTP

Option B — Institutional SSO

Where practical:

Google / Microsoft / institutional SSO

Option C — MFA

For sensitive actions:

- login
- changing PI
- submitting proposal
- withdrawing proposal

use MFA.

The principle should be:

Authentication establishes who the user is; authorization determines what that user is allowed to see or change.

9. Institution verification

This is particularly important.

Don't allow someone to register:

"Oxford University"

using a Gmail account and submit a proposal.

You could require:

Institutional verification

Institution

University of XYZ

Institutional domain

@xyz.edu

Institutional representative

professor@xyz.edu

Institution website

https://xyz.edu

Verification

Pending → Verified

For institutions that don't use a .edu-type domain, AIT can manually verify them.

10. Proposal status tracking

This is one of the biggest advantages of building a portal.

The applicant should see:

SUBMITTED



Eligibility Check



Administrative Review



Technical Review



Committee Evaluation



Clarification / Q&A



Shortlisted



Final Approval



Contracting



Project Initiated

But **don't expose internal reviewer details or confidential comments.**

Applicants should see something like:

Technical Review – In Progress

rather than:

"Reviewer 3 gave you 67/100."

unless your governance model explicitly intends to disclose scores.

11. Internal AIT workflow

On the AIT side, I would have a completely different dashboard.

AIT ADMIN PORTAL

Open Calls: 1

Applications: 37

Eligibility Pending: 5

Under Review: 18
Shortlisted: 8
Clarification Required: 4
Approved: 3

Click:

Face Verification/PAD

and see:

Proposa I	Institution	Status	Reviewer 1	Reviewer 2	Conflict
FV-001	University A	Review	Assigned	Assigned	No
FV-002	University B	Review	Assigned	—	No
FV-003	University C	Conflict	—	—	Yes

12. Conflict-of-interest management

For an international research call, I would make this a **mandatory part of the platform**.

Before reviewing:

I declare that I have no conflict of interest with this applicant.

Then:

Accept

or

Declare conflict

If conflict:

Reviewer



Declares COI



Proposal removed from reviewer queue



Administrator assigns another reviewer

This is particularly important because you are dealing with universities, research groups, potentially competing technologies, and IP.

13. Blind technical review can be considered

Depending on AIT/Gates governance, you could separate:

Administrative information

from

Technical proposal

For technical evaluation, reviewers might initially see:

Proposal ID: DPI-FV-017

Technical proposal

Team expertise

Methodology

Work plan

Evaluation

Budget

rather than unnecessary applicant information.

Whether you actually use blind review depends on the funding/governance requirements.

14. Use structured evaluation rather than PDFs alone

This is important.

Instead of reviewer downloading the proposal and sending an Excel sheet back, give reviewers an online evaluation form.

For example:

Technical merit

- Problem understanding
- Technical approach
- Novelty
- Scientific rigor
- Feasibility
- Evaluation methodology
- DPI interoperability

- Security/privacy
- Team capability
- Sustainability

And then:

Reviewer recommendation

- ☐ Recommend
- ☐ Recommend with conditions
- ☐ Do not recommend

Comments

[_____]

The actual scoring/weighting should be established in your approved AIT/Gates evaluation framework.

15. Clarification workflow

This is something I strongly recommend.

Instead of:

"Please email us if you have questions."

have:

Proposal #DPI-024

AIT:

Please clarify whether your proposed PAD model requires cloud inference.

Applicant:

Response...

AIT:

Thank you. Please upload revised methodology.

Applicant:

Uploaded v2.

Every communication becomes part of the proposal's **audit trail**.

16. Version control

Never overwrite proposals.

You want:

Proposal v1
Proposal v2
Proposal v3
Final Submitted Version

and:

Submitted:
28 Sept 2026
10:32 UTC+5:45

Submitted by:
Dr. XYZ

Document hash:
xxxxxxxxx

This becomes very useful if there is ever a dispute about what was actually submitted.

17. Audit trail

The system should record:

User logged in
Proposal created
Team member added
Budget modified
Document uploaded
Reviewer assigned
Reviewer accessed proposal
Reviewer submitted evaluation
COI declared
Clarification requested
Applicant responded
Proposal resubmitted
Final approval

with:

- user
- timestamp

- action
 - proposal ID
 - IP/device information where appropriate
-

18. File upload requirements

For each document, specify:

Allowed formats

- PDF
- DOCX
- XLSX
- ZIP where necessary

Maximum size

For example:

- Proposal: 20 MB
- CV: 5 MB
- Technical annex: 20 MB
- Code: repository link or ZIP

I'd actually prefer **GitHub/GitLab repository links** for source code rather than massive ZIP files.

19. Don't ask universities to upload unnecessary sensitive data

This is especially important for the biometric track.

The initial proposal should **not require real biometric datasets**.

Instead, ask:

Describe the datasets you intend to use, their provenance, licensing, demographic composition, and ethical/legal basis.

Then, after selection, establish a separate:

Data Access Agreement

if actual biometric data needs to be provided.

20. Technical requirements for Face Verification/PAD should be unusually detailed

Because otherwise proposals will be impossible to compare meaningfully.

I'd require reporting of things such as:

Face verification

- FMR
- FNMR
- ROC/DET
- threshold
- demographic breakdown
- image/video quality conditions
- latency
- compute requirements

PAD

- attack types
- APCER
- BPCER
- ACER where appropriate
- IAPAR where applicable
- attack instruments
- replay attacks
- print attacks
- screen attacks
- 3D mask/material attacks
- injection attacks

NIST's current guidance, for example, specifies facial PAD and provides quantitative performance expectations, while referencing ISO/IEC 30107 testing. Your CfP doesn't necessarily have to copy NIST's thresholds, but it should require **standardized reporting and reproducible testing**.

21. For VC, define interoperability explicitly

I'd include a table like:

Area	Requirement
Data model	W3C VCDM
Credential format	Applicant proposes
Proof mechanism	Applicant proposes
Issuer	Required
Holder	Required
Verifier	Required
Wallet	Required/optional depending on track
Revocation/status	Required
Selective disclosure	Required/desired
API	Required
Documentation	Required
Open-source	Define required components
Interoperability testing	Required

W3C describes VC as a three-party ecosystem involving **issuer, holder and verifier**, and VCDM 2.0 is now a Recommendation.

22. What should be public vs private?

I'd divide information into three levels.

Public

- Call
- technical challenge
- eligibility
- deadlines
- FAQ
- evaluation criteria
- templates
- funding information
- announcements

Applicant-only

- draft proposal
- budget
- uploaded CVs
- clarification discussions
- submission status
- institutional documents

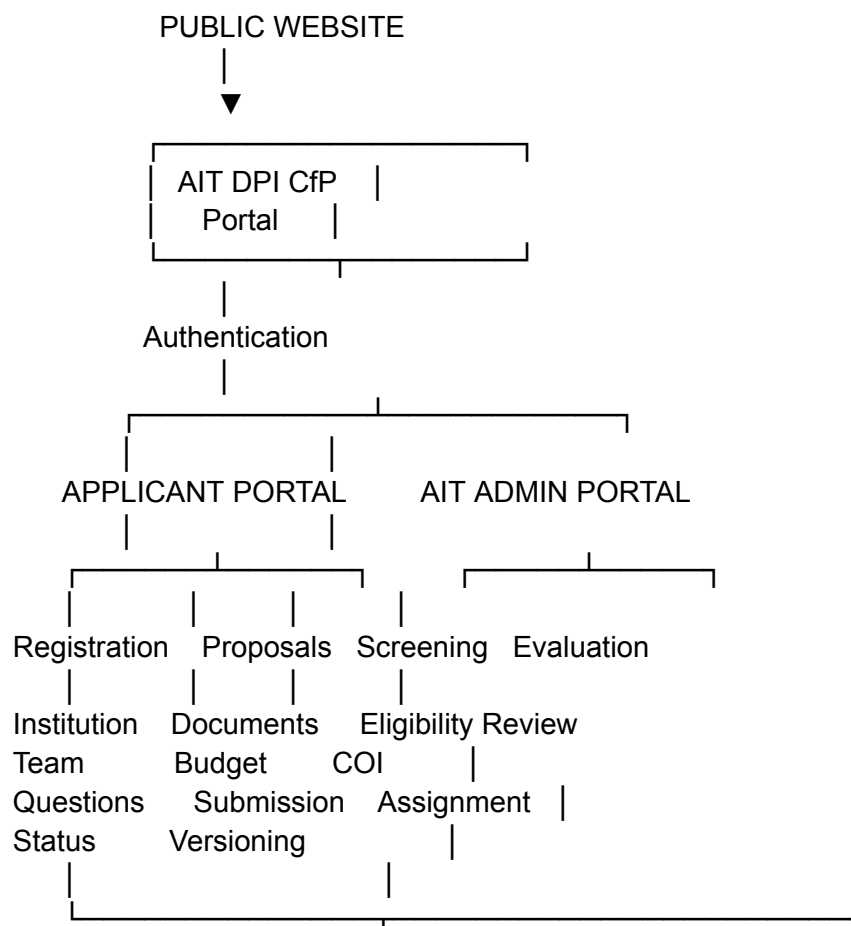
AIT-internal

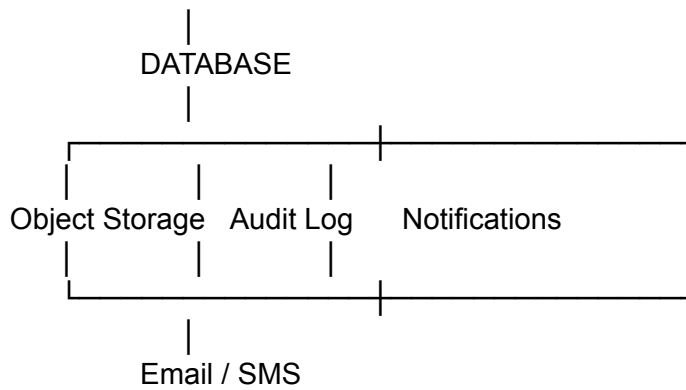
- reviewer assignments
- reviewer comments
- scores
- COI
- committee discussions
- internal recommendations
- approval decisions before announcement

This separation is essential.

23. The overall architecture I'd recommend

For your AIT project:





24. What technology should you use?

For a **first AIT DPI CfP**, I wouldn't build everything from scratch unless the project itself is intended to demonstrate a platform.

You essentially have three choices:

Option 1 — Google Forms + Drive

Very easy.

But weak for:

- multi-user proposal editing
- institutional accounts
- workflow
- reviewer assignment
- audit trail
- versioning
- applicant status
- authorization

I'd use this only for a **simple preliminary expression of interest**.

Option 2 — WordPress + forms/workflow

This could be a reasonable middle ground.

You can build:

AIT DPI Website

+

WordPress

+

Application/Form plugin

+

File storage
+
Workflow
+
Authentication

Good for getting the CfP online quickly.

But once you have sophisticated reviewer permissions, institutional accounts, conflict-of-interest management and audit trails, you need to be careful about plugin security and architecture.

Option 3 — Dedicated CfP portal

For your particular project, this is the architecture I would **design toward**:

Frontend
React / Next.js

Backend
FastAPI / Django

Database
PostgreSQL

Object Storage
S3-compatible storage

Authentication
OIDC / OAuth2 + MFA

Authorization
RBAC

Email
Institutional SMTP / transactional email

Document processing
PDF/DOCX validation

Audit
Immutable audit log

Deployment
AIT infrastructure / secure cloud

This also gives you something potentially reusable for future DPI research calls.

25. I would actually use a two-stage CfP

For international universities, this can reduce everyone's workload.

Stage 1 — Concept Note

Perhaps 3–5 pages.

Ask for:

- institution
- PI
- problem
- proposed solution
- innovation
- relevant experience
- preliminary methodology
- team
- approximate budget
- expected outcomes

Then AIT screens these.

Stage 2 — Full Proposal

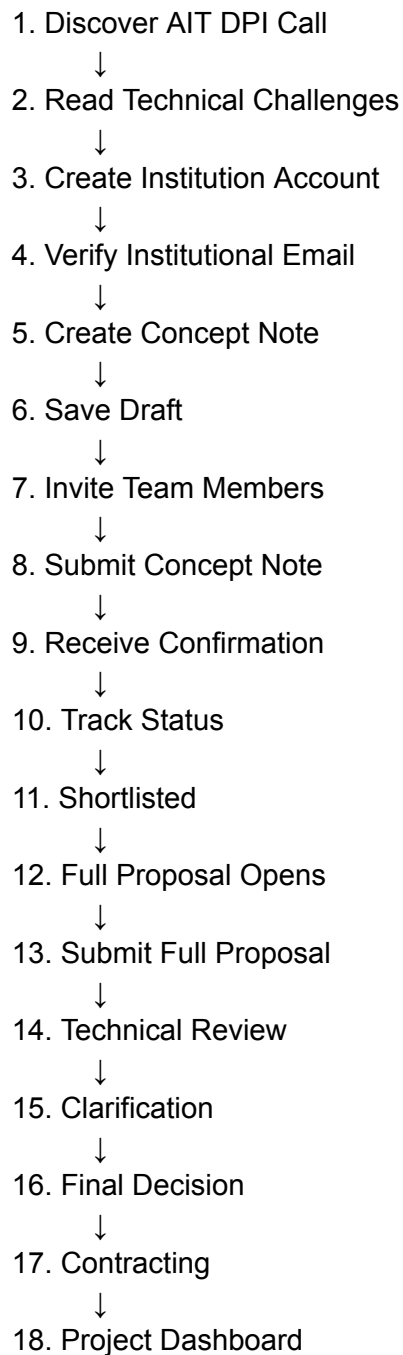
Only shortlisted applicants submit:

- detailed architecture
- methodology
- work packages
- milestones
- evaluation plan
- datasets
- security
- ethics
- IP
- open-source
- detailed budget
- team CVs
- implementation plan

This is essentially the same general pattern used by some major research funding calls; Horizon Europe explicitly supports two-stage applications for some calls.

26. Suggested applicant journey

The whole experience should feel like this:



And after selection, **the same portal should ideally become the project-management portal.**

That means the system evolves:

CfP Portal → Proposal Portal → Grant/Research Management Portal.

27. One important design decision for your AIT DPI project

I would separate the **technical challenge** from the **implementation contract**.

For example:

Challenge document

We want to solve this problem.

Proposal

This is how our university proposes to solve it.

Evaluation

This is how AIT evaluates it.

Contract

These are the agreed deliverables, IP, payment, reporting and ownership.

Project management

This is how the selected university executes it.

This prevents the CfP itself from becoming an enormous 50-page legal/technical document.

My recommended AIT structure

I would therefore create **five components**:

1. AIT DPI CfP Website

Public information and call documents.

2. Applicant Portal

Registration, proposal creation, document upload, team management, submission and status.

3. Reviewer Portal

Assigned proposals, conflict declaration, evaluation forms and recommendations.

4. AIT Admin Portal

Eligibility, assignment, workflow, committee management, approvals and audit.

5. Project Management Portal

For selected universities: milestones, deliverables, technical reviews, payments, reports and final evaluation.

The most important point is that **authentication, authorization, workflow, audit trail and document versioning should be designed from day one**. Don't bolt those onto a Google Form later.

For your particular DPI work, I'd also make the **technical challenge briefs extremely precise**, especially for **Face Verification/PAD** and **VC**, because otherwise you may receive proposals that sound impressive but cannot be compared technically. The W3C VC standards and ISO/NIST biometric terminology give you a good standards-based foundation for doing that.

If you want to implement this quickly, a good next step would be to design the **actual AIT DPI CfP portal specification**—including the database entities, applicant/reviewer/admin roles, workflow/status machine, proposal form fields, document templates, and a WordPress-vs-custom-portal decision.

RESEARCH TRACKS

Six open research tracks

Select the track that best matches your team's expertise and your country's DPI context. Proposals must address a real national or sub-national need.

DPI Needs Assessment

01

Map the digital ID and DPI landscape in your country. Identify barriers to adoption, infrastructure gaps, and the needs of marginalised populations.

Digital ID Establishment

02

Research and prototype open-source digital identity systems, with a focus on interoperability, inclusivity, and alignment with national digital ID strategy.

Attack Dataset Development

03

Develop datasets of biometric spoofing and identity fraud attacks to support security research and testing of DPI authentication systems.

Presentation Attack Detection (PAD)

04

Build and validate machine learning models to detect spoofing attacks on biometric systems used in national digital ID programmes.

Verifiable Credentials (VC) Use Cases

05

Design and pilot verifiable credential applications for education, employment, healthcare, or financial services using open DPI standards.

AI Agents for DPI

06

Explore how AI agents can improve citizen access to DPI-enabled government services, with attention to safety, privacy, and equity.

Research Tracks

Tracks are organised from foundational to advanced research. Each profile sets out the focus of the track, followed by its results chain from output to outcome to impact.

Needs Assessment and DPI Readiness

Track 1: Needs Assessment

Foundational research

Partner universities are expected to (1) map their country's identity ecosystem, including institutions, laws, policies, and technology, (2) engage key stakeholders (e.g., ID authority, relevant ministries, service providers, and target populations) through interviews, surveys, or focus groups, (3) identify priority gaps, inclusion barriers, and candidate use cases, and (4) assess readiness for open-source DPI adoption using a documented scorecard.

Output

Needs assessment report with a stakeholder map, prioritized gaps and use cases, and a DPI readiness scorecard.



Outcome

Knowledge: Evidence-based understanding of country-specific needs, inclusion gaps, and readiness for open-source DPI adoption.



Impact

National ID authorities and DPI implementers are guided in prioritizing DPI investments and use cases through a published needs assessment report.

Foundational Digital ID

Track 2: Digital ID Establishment

Foundational research

Intended for partner universities in countries without a digital ID system. Partner universities are expected to (1) analyse the civil registration and identification landscape, including legal and data protection prerequisites, (2) co-design a reference architecture and phased roadmap with the relevant government authority using open-source platforms, (3) develop a sandbox-based POC of enrolment, ID issuance, and authentication (e.g., on the AIT sandbox), and (4) evaluate the POC for feasibility, cost, inclusion, and privacy.

Output

Reference architecture, phased roadmap, and a sandbox-based POC of a foundational digital ID system.

→

Outcome

Knowledge: Evidence-based lessons on establishing foundational digital ID using open-source DPI in countries without an existing digital ID system.

→

Impact

Governments without digital ID are guided in establishing inclusive, vendor-neutral foundational ID systems through a published playbook and roadmap.

Facial Verification and Open-Source PAD

Track 3: Attack Dataset

Applied research

Partner universities are expected to build presentation attack datasets that represent their populations, for use in testing the PAD module (Track 4). They are also expected to document and validate their data collection protocol, including how dataset quality is assessed, guidelines on how the dataset should be used, and which evaluation protocol the dataset serves.

Output

Dataset, with a documented and validated data collection protocol and usage guidelines.

→

Outcome

Knowledge: Evidence-based lessons on collecting attack data.

→

Impact

The national ID authority and system integrators can test and select PAD solutions against a locally representative attack dataset, ensuring that face verification works reliably for the country's population. Supported by a published data collection playbook.

Facial Verification and Open-Source PAD

Track 4: Model

Applied research

Partner universities are expected to develop an open-source face Presentation Attack Detection (PAD) module. PAD helps detect attempts to deceive an identity system using a photograph, video, mask, or similar method. They are also expected to benchmark the model, document the total project cost broken down by category (for example, GPU costs), and analyse the model's weaknesses.

Output

Open-source PAD model with benchmark results, a cost breakdown by category, and an analysis of the model's weaknesses.



Outcome

Knowledge: Evidence-based lessons on building face PAD models.



Impact

The national ID authority has a benchmarked, open-source PAD option to inform its procurement and deployment decisions, reducing reliance on proprietary solutions. Supported by a published PAD development playbook.

Wallets and Credentials

Track 5: VC Use Case

Applied research

Partner universities are expected to research, identify, pilot and evaluate VC use cases for marginalized populations in their country.

Output

Validated POC/MVP: VC use case piloted with a small group of users in their region.



Outcome

Knowledge: analysis of what works and what does not in using open-source digital wallets for remote identity verification for marginalised populations.



Impact

The national ID authority or relevant government agency is positioned to scale the piloted VC use case, extending remote identity verification to marginalised populations nationwide. Supported by a published implementation playbook.

AI agent for DPI

Track 6: Consent Framework and Trust Architecture

Advanced research

Partner universities are required to propose (1) consent frameworks, (2) trust architecture, (3) one relevant use case, (4) develop a prototype as a demonstrator of the framework, and (5) evaluate the prototype (framework) with a focus on effectiveness, cost, security, governance, and risks.

Output

Validated and evaluated POC/MVP of the framework.



Outcome

A secure and robust AI agent that operates reliably across various DPI systems and use cases evaluated through a prototype in one relevant DPI use case.



Impact

National identity authorities and corresponding public institutions are guided in adopting the consent framework and trust architecture for AI agents through a white paper/playbook.

Contents of the Website

About the Programme

ABOUT THE PROGRAMME

Building a regional network of DPI expertise

Digital Public Infrastructure (DPI) — open-source systems for digital identity, data exchange, and digital payments — is reshaping how governments deliver services to citizens. Asia Pacific countries are at different stages of DPI adoption, and many lack the local research capacity and technical community to build and sustain these systems.

The AIT DPI University Grant Programme, funded by the Gates Foundation, brings universities into this ecosystem. Selected universities will conduct original research, train the next generation of DPI practitioners, and connect with a growing regional network managed by AIT.

This is the first call in a series. Universities that join now become founding members of the AIT DPI University Network — participating in shared knowledge, regional events, and future collaboration through to 2029.

GRANT AT A GLANCE

PROGRAMME	Advancing Open Source Digital Public Infrastructure in Asia Pacific
FUNDED BY	Gates Foundation
MANAGED BY	Asian Institute of Technology (AIT), Thailand
PERIOD	January 2027 – January 2029 (24 months)
MAXIMUM	USD 100,000 per university
OPENS	15 October 2026
DEADLINE	30 November 2026, 5:00 PM ICT

Building a regional network of DPI expertise

Digital Public Infrastructure (DPI) — open-source systems for digital identity, data exchange, and digital payments — is reshaping how governments deliver services to citizens. Asia Pacific countries are at different stages of DPI adoption, and many lack the local research capacity and technical community to build and sustain these systems.

The AIT DPI University Grant Programme, funded by the Gates Foundation, brings universities into this ecosystem. Selected universities will conduct original research, train the next generation of DPI practitioners, and connect with a growing regional network managed by AIT.

This is the first call in a series. Universities that join now become founding members of the AIT DPI University Network — participating in shared knowledge, regional events, and future collaboration through to 2029.

Eligible countries:

ELIGIBILITY

Open to 10 countries in Asia Pacific

Applicants must be degree-granting universities with active programmes in computer science, information technology, or related fields.

 Bangladesh

 Bhutan

 Indonesia

 Laos

 Nepal

 Pakistan

 Papua New Guinea

 Philippines

 Sri Lanka

 Vietnam

One application per university. A consortium of departments within the same institution is permitted. Joint applications across two or more universities are not accepted under this call.

Mandatory components

There are 3 mandatory components:

- 1. Component 1 : Research
- 2. Component 2:
- 3. Component 3:

MANDATORY COMPONENTS

Every proposal must address all three components

No single component may exceed 60% of the total budget. Activities across all three must be clearly described in your proposal. Select a component to see the full requirements.



COMPONENT 1

Research & Development

Original research, prototyping, and technical development tied to your chosen track. Outputs must be open-source and openly published.

6 research tracks available ↓



COMPONENT 2

Capacity Building

Training, workshops, and curriculum development to build DPI knowledge and skills among students, faculty, and local practitioners.

See full requirements ↓



COMPONENT 3

Community & Ecosystem Engagement

Connecting with government, civil society, and the regional DPI network. Includes events, publications, and contributing to open communities.

See full requirements ↓

Component 1 - Research Tracks

For the research tracks, I want to show the 6 research tracks overall and links to the details.
Research Track

RESEARCH TRACKS

Six open research tracks

Select the track that best matches your team's expertise and your country's DPI context. Proposals must address a real national or sub-national need.

DPI Needs Assessment

01

Map the digital ID and DPI landscape in your country. Identify barriers to adoption, infrastructure gaps, and the needs of marginalised populations.

Digital ID Establishment

02

Research and prototype open-source digital identity systems, with a focus on interoperability, inclusivity, and alignment with national digital ID strategy.

Attack Dataset Development

03

Develop datasets of biometric spoofing and identity fraud attacks to support security research and testing of DPI authentication systems.

Presentation Attack Detection (PAD)

04

Build and validate machine learning models to detect spoofing attacks on biometric systems used in national digital ID programmes.

Verifiable Credentials (VC) Use Cases

05

Design and pilot verifiable credential applications for education, employment, healthcare, or financial services using open DPI standards.

AI Agents for DPI

06

Explore how AI agents can improve citizen access to DPI-enabled government services, with attention to safety, privacy, and equity.

Details

Tracks are organised from foundational to advanced research. Each profile sets out the focus of the track, followed by its results chain from output to outcome to impact.

Needs Assessment and DPI Readiness

Track 1: Needs Assessment

Foundational research

Partner universities are expected to (1) map their country's identity ecosystem, including institutions, laws, policies, and technology, (2) engage key stakeholders (e.g., ID authority, relevant ministries, service providers, and target populations) through interviews, surveys, or focus groups, (3) identify priority gaps, inclusion barriers, and candidate use cases, and (4) assess readiness for open-source DPI adoption using a documented scorecard.

Output

Needs assessment report with a stakeholder map, prioritized gaps and use cases, and a DPI readiness scorecard.



Outcome

Knowledge: Evidence-based understanding of country-specific needs, inclusion gaps, and readiness for open-source DPI adoption.



Impact

National ID authorities and DPI implementers are guided in prioritizing DPI investments and use cases through a published needs assessment report.

Foundational Digital ID

Track 2: Digital ID Establishment

Foundational research

Intended for partner universities in countries without a digital ID system. Partner universities are expected to (1) analyse the civil registration and identification landscape, including legal and data protection prerequisites, (2) co-design a reference architecture and phased roadmap with the relevant government authority using open-source platforms, (3) develop a sandbox-based POC of enrolment, ID issuance, and authentication (e.g., on the AIT sandbox), and (4) evaluate the POC for feasibility, cost, inclusion, and privacy.

Output

Reference architecture, phased roadmap, and a sandbox-based POC of a foundational digital ID system.



Outcome

Knowledge: Evidence-based lessons on establishing foundational digital ID using open-source DPI in countries without an existing digital ID system.



Impact

Governments without digital ID are guided in establishing inclusive, vendor-neutral foundational ID systems through a published playbook and roadmap.

Facial Verification and Open-Source PAD

Track 3: Attack Dataset

Applied research

Partner universities are expected to build presentation attack datasets that represent their populations, for use in testing the PAD module (Track 4). They are also expected to document and validate their data collection protocol, including how dataset quality is assessed, guidelines on how the dataset should be used, and which evaluation protocol the dataset serves.

Output

Dataset, with a documented and validated data collection protocol and usage guidelines.



Outcome

Knowledge: Evidence-based lessons on collecting attack data.



Impact

The national ID authority and system integrators can test and select PAD solutions against a locally representative attack dataset, ensuring that face verification works reliably for the country's population. Supported by a published data collection playbook.

Facial Verification and Open-Source PAD

Track 4: Model

Applied research

Partner universities are expected to develop an open-source face Presentation Attack Detection (PAD) module. PAD helps detect attempts to deceive an identity system using a photograph, video, mask, or similar method. They are also expected to benchmark the model, document the total project cost broken down by category (for example, GPU costs), and analyse the model's weaknesses.

Output

Open-source PAD model with benchmark results, a cost breakdown by category, and an analysis of the model's weaknesses.



Outcome

Knowledge: Evidence-based lessons on building face PAD models.



Impact

The national ID authority has a benchmarked, open-source PAD option to inform its procurement and deployment decisions, reducing reliance on proprietary solutions. Supported by a published PAD development playbook.

Wallets and Credentials

Track 5: VC Use Case

Applied research

Partner universities are expected to research, identify, pilot and evaluate VC use cases for marginalized populations in their country.

Output

Validated POC/MVP: VC use case piloted with a small group of users in their region.



Outcome

Knowledge: analysis of what works and what does not in using open-source digital wallets for remote identity verification for marginalised populations.



Impact

The national ID authority or relevant government agency is positioned to scale the piloted VC use case, extending remote identity verification to marginalised populations nationwide. Supported by a published implementation playbook.

AI agent for DPI

Track 6: Consent Framework and Trust Architecture

Advanced research

Partner universities are required to propose (1) consent frameworks, (2) trust architecture, (3) one relevant use case, (4) develop a prototype as a demonstrator of the framework, and (5) evaluate the prototype (framework) with a focus on effectiveness, cost, security, governance, and risks.

Output

Validated and evaluated POC/MVP of the framework.



Outcome

A secure and robust AI agent that operates reliably across various DPI systems and use cases evaluated through a prototype in one relevant DPI use case.



Impact

National identity authorities and corresponding public institutions are guided in adopting the consent framework and trust architecture for AI agents through a white paper/playbook.

Component 2 - Capacity Building

COMPONENT 2

Capacity Building

Develop DPI knowledge and practical skills in your institution and local community – from students and faculty to government officials and practitioners.

**Student Curriculum**

Develop or integrate DPI content into existing courses. Target undergraduate and postgraduate students in computer science, information technology, or related fields.

**Government Training**

Deliver workshops or training programmes for government staff, policymakers, or regulators working on national DPI implementation.

**Practitioner Development**

Run bootcamps, hackathons, or short courses for developers, engineers, and technologists building or maintaining DPI systems.

Minimum expectation: At least 30 individuals trained or upskilled through Component 2 activities over the 24-month grant period.

Component 3 - Community & Ecosystem Engagement

Proposal Evaluation

How to Apply

- Step 1: read the call for proposals
- Step 2: complete the proposal templates
 - Main Proposal template
 - *Financial template*
 - *Technical template*
- Step 3: Gather supporting documents
- Step 4: Submit via the online portal
 - discuss more

E.g

HOW TO APPLY

Four steps to submit

All four documents in the submission package are required. Incomplete applications will not be considered.

1

Read the Call for Proposals

Download and read the full Call for Proposals, including eligibility, scope, and evaluation criteria, before preparing your application.

2

Complete the proposal template

Fill in all sections (A–G) of the official Grant Proposal Template. Do not alter the template structure or delete any section.

3

Gather supporting documents

Prepare CVs for the PI and key team members, evidence of government engagement (MoU or letter), and optionally a letter from the national ID authority.

4

Submit via the online portal

Submit your complete application package through the official online portal (Google Form). Only submissions received before 30 Nov 2026, 5:00 PM ICT will be accepted.



Information Sessions — 27, 28 & 29 October 2026

Join our free online sessions to learn about the programme, ask questions, and connect with the AIT team before submitting.

Platform: Zoom · Meeting ID: [TO BE CONFIRMED] · Passcode: [TO BE CONFIRMED]

[Register Interest](#)

[Submit Application \(Google Form\) ↗](#)

Portal opens 15 October 2026 · Deadline 30 November 2026, 5:00 PM ICT

Key Dates

Call timetable

Activity	Date
Call Opens	15th of October 2026
Information sessions	27th, 28th and 29th October 2026
Application Deadline	30th November 2026, 5:00 PM ICT (UTC/GMT +7)
Shortlisted applicants notified	15th December 2026
Interview for the shortlisted candidates	4th January 2027
Final selection announced	10th January 2027

KEY DATES

15 OCTOBER 2026

Call for Proposals opens

Call document and official template available for download

27-29 OCTOBER 2026

Information Sessions (Online via Zoom)

Join our live Q&A sessions to learn more about the programme and ask questions.

Zoom Meeting ID: [TO BE CONFIRMED] | Passcode: [TO BE CONFIRMED]

Registration: [ZOOM REGISTRATION LINK]

30 NOVEMBER 2026, 5:00 PM ICT

Application Deadline

Submit via the online portal. Late submissions will not be accepted.

15 DECEMBER 2026

Shortlisted applicants notified

Shortlisted institutions will be contacted directly by the programme team

4 JANUARY 2027

Interviews with shortlisted candidates

Online interviews conducted by the independent review panel

10 JANUARY 2027

Final selection announced

Successful universities notified and onboarded into the AIT DPI University Network

Downloads Applications Package

- Call for Proposal
 - Please contact Kyi for the final pdf version
- Grant Proposal Template
 - Please contact Kyi for the final pdf version

DOWNLOADS

Application package

Both documents must be submitted. Use only the official template — submissions in other formats will not be accepted.



Call for Proposals

Full programme document. Covers eligibility, research scope, evaluation rubric, grant conditions, and submission requirements.

[Download PDF ↓](#)



Grant Proposal Template

Official application form (MS Word, .docx). Complete Sections A–G. Submit both the Word file and a PDF export of the completed document.

[Download Template ↓](#)

CFP - Page

- About the Program
- Eligibility
- Mandatory components
 - Component 1 - Research Tracks
 - For the research track -
 - quick overview of the tracks
 - Details for each track
 - Component 2
 - Component 3
- Proposal Evaluation
- How to Apply
 - Step 1: read the call for proposals
 - Step 2: complete the proposal templates
 - Main Proposal template
 - *Financial template*
 - *Technical template*
 - Step 3: Gather supporting documents
 - Step 4: Submit via the online portal
 - discuss more
- Key Dates
- Download session
 - the proposal
 - Proposal template