第７部

特集7 INXIGNIA

Achmad Husni Thamrin、Andrey Ferriyan、阿部 涼介、鈴木 茂哉、大川 恵子

第１章　Introduction

This report outlines the updates on a digital badge platform for lifelong learning operated by SOI Asia called INXIGNIA. INXIGNIA enables organizations to issue badges to learners as proof of knowledge and skills of the learners according to specific criteria set by the organizations. Badge recipients can display their badges on social media, which may be viewed by, for example, potential employers.

Figure 1. Badges issued by INXGINIIA

SOI Asia issues several kinds of badges for learners (Figure 1). For example, APIE Camp badges are issued to learners who completed a 5-day in-person camp. Several camp participants uploaded their badges to LinkedIn to show that they completed the camp (Figure 2). Displaying such badges on LinkedIn may also increase the visibility of SOI Asia and APIE to broader audiences.

There are two versions of INXIGNIA v1, which is currently in operation, and INXIGNIA v2, the future version that is in development and will be kicked off in 2025. INXIGNIA v1 uses Open Badges, which is a popular digital badge for learning. INXIGNIA v2 uses Verifiable Credentials (VC) and Decentralized Identifiers (DID), which are under the standardization process by W3C.

第２章　INXIGNIA v1

INXIGNIA v1 (https://inxignia.soi.asia) can have multiple

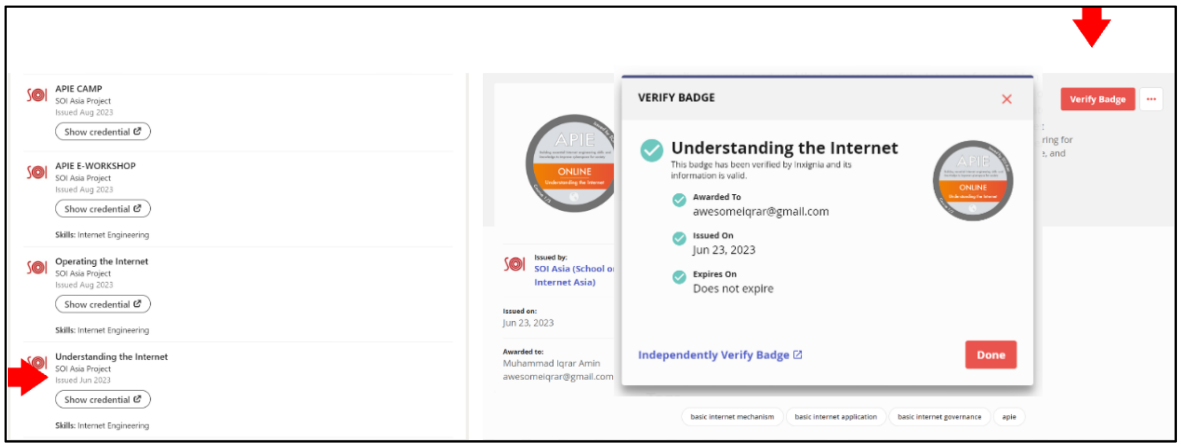

Figure 2. INXIGNIA Badges shared on LinkedIn

badge issuers, but currently, SOI Asia is the only operational issuer in INXIGNIA. Several partners have issuer accounts in INXIGNIA, and they use them to learn how to issue badges while devising organizational strategies in issuing badges, especially for their micro-credential programs.

Figure 3 shows the SOI Asia badge issuer main page. An issuer can create badges, certificates, and pathways (an experimental feature for research). INXIGNIA badges conform to Open Badges 2.0 standard, where a badge is an image with metadata that contains detailed data, such as badge name and criteria, as well as recipient name and email address. Certificates are PDF documents that show the recipient's achievements and include one or more badges. Certificates allow the recipients to have both digital and physical versions. In SOI Asia, we print the certificates and award them to the recipients in the closing ceremony of an event, such as APIE Camp. Pathway is an experimental feature that learners can use to consider related badges to get according to their learning goals.

The next iteration, which is INXIGNIA v1.1, features Single Sign On (SSO) using an identity provider. This feature allows organizations to run INXIGNIA v1 using their own SSO to issue their badges. With this feature, inxignia.soi.asia will become a choice of partner university students to store their badges after they graduate. This feature also allows better learner mobility between partner universities.

Figure 3 illustrates how INXIGNIA v1.1 works for Alice. Alice officially takes credit courses at two partner universities, A and B; hence, Alice has SSO accounts at both. Both partner universities, A and B, run their own INXIGNIA instances, and they have the policies to only issue badges to SSO accounts with their domains (a.edu and b.edu). Alice wants to keep her

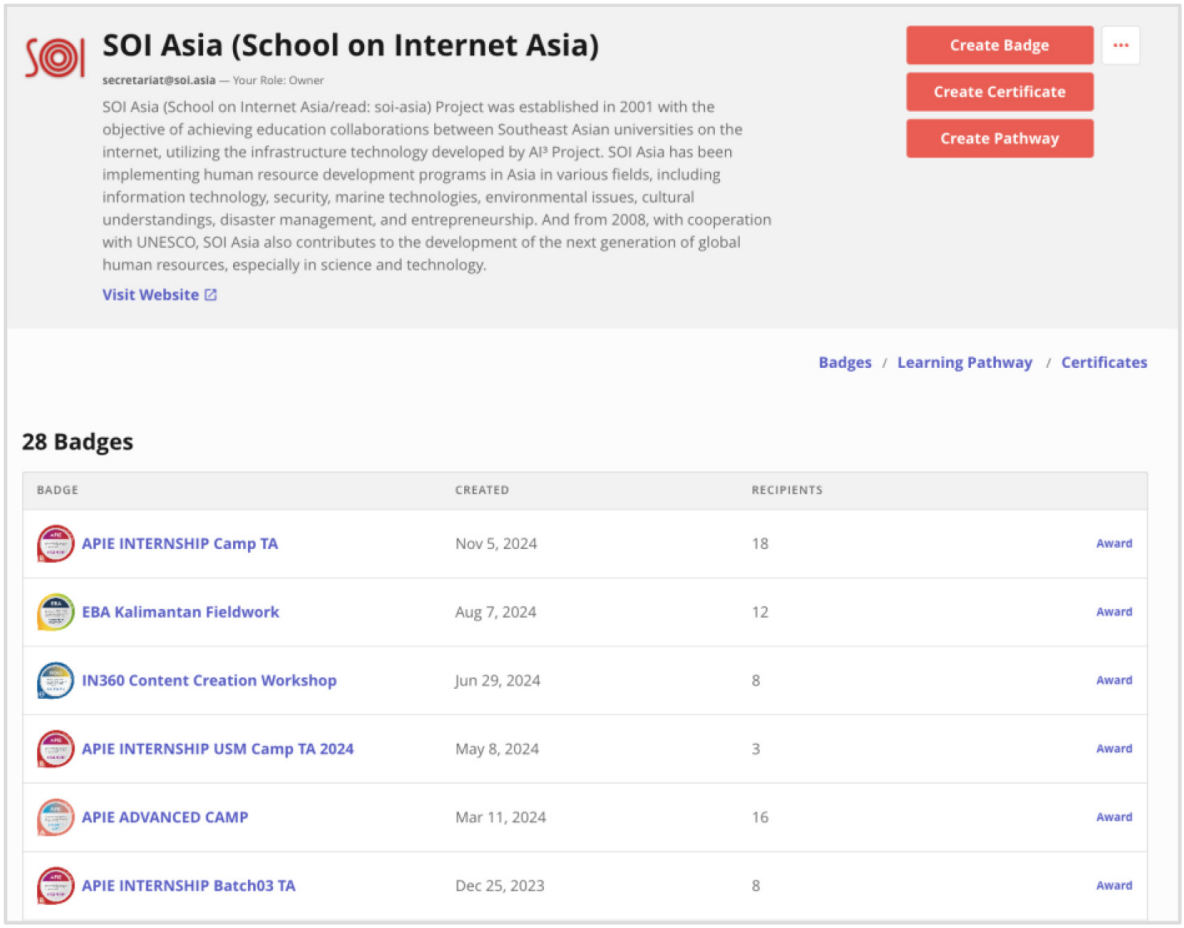

Figure 3. SOI Asia as an issuer in INXIGNIA.

badges for a long time, so she creates an account at INXIGNIA SOI Asia using her personal email address alice@example.com, adds her email address in A and B to INXIGNIA SOI Asia, then imports her badges to her account there. Alice can now keep her badges after she no longer has SSO Accounts at A and B.

We are promoting partners to run their own INXIGNIA v1 instances to realize such a scenario illustrated in Figure 3 with the aim of deployment in 2025. The main benefits for partners in running their instances are keeping their branding and flexibility in deployment to suit their needs.

We are testing INXIGNIA v1.1 with Institut Teknologi Bandung (ITB), Indonesia, for their deployment. The following partners, as well as other related universities in Southeast Asia, show their interest in deploying INXIGNIA: Universiti Sains Malaysia (USM), Universiti Malaysia Sarawak (UNIMAS), University of Philippines (UP), Ateneo de Manila University (ADMU), Universitas Brawijaya (UB), Universitas Sam Ratulangi (UNSRAT), and Universitas Syiah Kuala (USK).

第３章　INXIGNIA v2

In addition to INXIGNIA v1, we are developing INXIGNIA v2 as the future of digital badging platforms. INXIGNIA v2 uses the Verifiable Credentials (VC) and Decentralized Identifiers (DID) ecosystem, which are now under the standardization process, mainly in W3C. The objective of using DID/VC is to ensure that learners can manage their credentials for the long term in a secure and privacy-preserving manner.

We are developing two applications: Wallet and INXIGNIA. Wallet is a mobile application that generates DIDs, holds VCs, and presents VCs to other entities. Wallet stores the DID private keys securely to ensure no breach. INXIGNIA is a web application that generates its own DIDs and issues VCs.

Figure 4 illustrates a simplified flow of how University A and University B use INXIGNIA to issue VCs and how Alice uses Wallet to control her identifiers as well as to receive and present VCs.

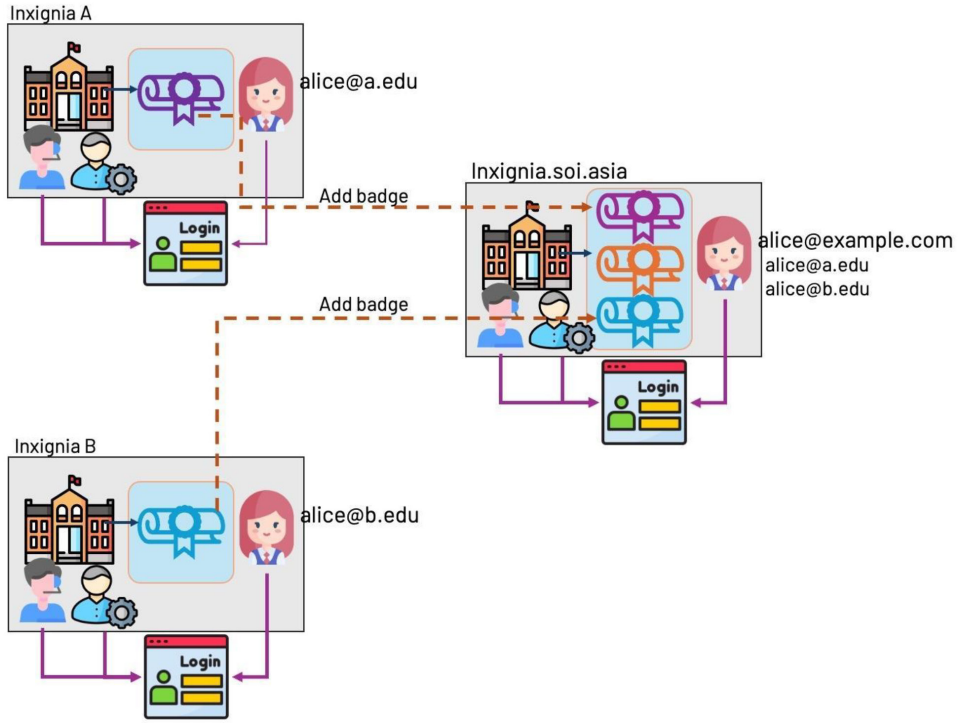

Figure 4. Alice uses INXIGNIA SOI Asia to keep her badges for the long term after graduating from A and B.

Alice has a Wallet app on her smartphone. Before she graduates from A, she generates a DID, Alice_X123, and gives the public key part to A. A issues a bachelor's degree certificate as a VC to Alice, and Alice stores the VC in her Wallet. In this flow, INXIGNIA A takes the role of the issuer and Alice's Wallet as the holder.

Alice then continues her education in B. Before she graduates, Alice generates a new DID, Alice_Z987, and uses it to receive her master's degree certificate from B. Alice then applies for a job at Major Company (M). She generates another DID, Alice_W456, bundles her bachelor's and master's degree VCs and other related VCs from her Wallet application, and presents them as a Verifiable Presentation (VP) to M, which takes the role of a verifier.

M has to verify whether the VCs it receives are in the valid format and not tampered with, and also, all DIDs in the VCs correctly point to the corresponding entities. First, M queries the corresponding Verifiable Data Registry (VDR, not shown in the figure 5) to get the public key of each DID in the VCs and to confirm, for example, that DID UA belongs to University A, and all Alice's DIDs belong to Alice. Then, M uses the public keys to verify that all the VCs are not modified cryptographically. M will accept the VP from Alice after the verification process is completed without any issues.

This year, we focused on the following: 1) introducing INXIGNIA v2 and DID/VC ecosystem to partners, 2) designing the Wallet application, and 3) designing how to onboard partners to INXIGNIA v2, as the concept of DID/VC ecosystem is pretty new and we plan to lower the barrier to the development and deployment in SOI Asia community.

We introduced INXIGNIA v2 to our community on several occasions in 2024: monthly seminars, two AI3/SOI Asia Meetings hosted by the University of San Carlos (USC) and Bangladesh University of Engineering and Technology (BUET), and a MicroCASA Project meeting hosted by ADMU and UP. The responses from the community, in general, are positive and forward-looking. At the same time, they are reasonably curious on how the DID/VC ecosystem works and what the benefits are offered by INXIGNIA v2 compared to INXIGNIA v1.

For the Wallet, the "Delight" student research group in Keio University SFC is mainly in charge of the development. We are developing the Wallet using Dart and Flutter, so we have a code shared for both IOS and Android platforms. The Wallet uses the secure element embedded in smartphones to store

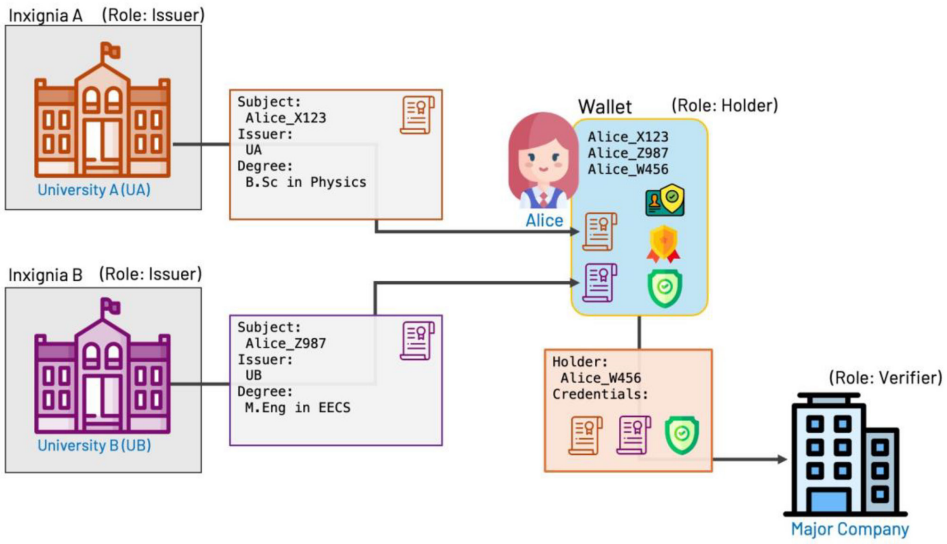

Figure 5. An illustration of how universities, a learner, and a company interact with each other using INXIGNIA and Wallet.

private keys and to perform cryptographic operations for security purposes.

INXIGNIA v2 will be developed on top of INXIGNIA v1, leveraging SOI Asia identity provider as the INXIGNIA Data Registry (IDR) to store DID public keys and the badge metadata of INXIGNIA v1 to be included as the claims in Verifiable Credentials issued by INXIGNIA v2. We plan to do the initial deployment using the Trusted Platform Module (TPM) to store private keys and perform the related cryptographic operations securely.

We are designing a Key Signing Party (KSP) to onboard partner organizations into INXIGNIA v2 during the SOI Asia 59th Meeting on March 6, 2025. The main idea is to translate the human trust network built in the community over the years into a web of trust among DIDs using a procedure similar to PGP.

In performing a KSP, Participant X shows his passport page and business card and uses his Wallet to show the QR Code of his personally identifiable information (PII) data signed using his private key to Participant Y. Y scans the QR Code and verifies the PII data by matching X's passport and business card with the PII data and performing cryptographic verification of the signed PII data. Y then certifies X and creates a corresponding QR Code of the certification to be scanned by X.

X performs a similar procedure with several participants from different organizations. After receiving the required number of certifications, X uploads his PII data and the certifications to IDR for onboarding to INXIGNIA. The KSP is complete for X, and his organization after IDR receives the PII data of everyone who issued the certification for X. INXIGNIA may issue VCs for the members of X's organization in the future.

第4章　Future Plans

We will migrate to INXIGNIA v1.1 for full-fledged operation and promote the deployment in partner organizations. For INXIGNIA v2, we will start the development in full swing in 2025, and we aim to prepare to form INXIGNIA Consortium with partner organizations for sustainable development and operation of both INXIGNIA v1 and v2.