REPUBLIC OF THE PHILIPPINES
PHILIPPINE STATISTICS AUTHORITY
BATANES PROVINCIAL STATISTICAL OFFICE

BAGONG PILIPINAS

Reference No. 202509-081

11204

DEPARTMENT OF EDUCATION
SDO - BATANES
MAR 10 2025
RECEIVED
BY: Fed TIME: 10:45

10 March 2025

ALFREDO B. GUMARU JR., EdD, CESO V
Schools Division Superintendent
Department of Education
Schools Division Office Batanes
Brgy. Kaychanarianan, Basco, Batanes

SUBJECT: Invitation to Leverage the National ID Authentication Services

Dear SDS Gumaru:

Greetings from the Philippine Statistics Authority (PSA)!

We extend our formal invitation on the availability of the National ID Authentication Services, which the Department of Education- Schools Division Office Batanes (SDO) may adopt to securely authenticate individuals (e.g. transacting clients or students). These authentication services provide a higher level of assurance in identity verification, enhancing both trust and security in the process.

The National ID Authentication Services comes in two tier levels: the **Basic Online Authentication Service (Tier I)** and the **electronic Know Your Customer (eKYC) (Tier II)**. The Basic Online Authentication Service offers a "match" or "no match" upon verification while the eKYC service offers a more comprehensive verification response by providing demographic information and a front-facing photograph of the client. A detailed explanation of these services is attached for your reference.

Both authentication services are available at **no cost** to interested government institutions and entities that register as Relying Parties of the National ID System. To avail of these services, entities must complete the onboarding process by submitting the required documentary

JPM Office Space Rental, National Rd., Brgy. Kaychanarianan, Basco, 3900, Batanes
Contact No.: +639287335226, +639950161926
Email Adress: batanes@psa.gov.ph
Website: www.psa.gov.ph

requirements[1] through the National ID eVerify website, accessible at https://everify.gov.ph/.

The PSA encourages the SDO to take advantage of these innovative solutions to enhance the efficiency and security of its service delivery. We are confident that this collaboration will contribute to our shared goal of delivering accessible, reliable, and secure public services to all Filipinos.

To better understand and appreciate the benefits and use cases of these authentication services, the PSA can assist the SDO in piloting your preferred authentication service at selected offices or schools. This pilot implementation will offer valuable insights into its integration, efficiency, and impact on SDO's operations.

The National ID Registry Unit of the Philippine Statistics Authority-Batanes may also arrange a meeting with you and your team to lay down all the details about the authentication services, onboarding process, implementation timelines, technical requirements, and any other support needed to ensure a smooth and successful integration of the National ID Authentication Services into SDO's systems and processes.

For any inquiries regarding the matters discussed above, please feel free to contact Mr. Dominic C. Gutierrez, Information Officer I via email at **batanes@psa.gov.ph** or through CP no. **0928 150 3570.**

Thank you very much!

Very truly yours,

RAMIL G. ABAD
Chief Statistical Specialist

/ADCG

Attachments:

1. *National ID Authentication Services*
2. *List of Regulatory Onboarding Requirements for the Government Sector*

Reference No. 24UCDMS00-03-019

NATIONAL ID AUTHENTICATION SERVICES

The National ID Authentication Services (NIDAS) offers solutions to optimize identity verification for greater efficiency, convenience, and an improved level of security for the relying parties and all registered persons. The NIDAS utilizes advanced authentication technology and robust protocols to ensure a seamless and accurate identity authentication experience.

The NIDAS comes in two distinct modes: offline and online.

Offline Authentication

Offline authentication or Tier 0 is verifying the identity of the registered person by checking the information reflected in the National ID (card, paper, or digital form) presented and ensuring its authenticity.

There are two ways to verify the authenticity of the National ID presented. First is through the use of the National ID Check - a web-based platform that ensures that the QR code printed in the National ID has not been tampered with, by checking that it recognizes the embedded digital signature in the QR code. Once verified, the demographic information from the QR code is aacompared against those printed on the National ID. The National ID Check is available for public use; hence, there is no need to apply with PSA to use the platform. Anyone with a smartphone, computer with a camera, or tablet connected to the internet can access and use National ID Check. The second means of verification is by checking the overt and covert features of the National ID. This means of verifying the authenticity of the National ID only applies to its PVC form.

Online Authentication

Online authentication involves the matching of individual credentials against those stored in the National ID Registry. These credentials include the National ID Card Number and the demographic, and biometric information or through a Short Message Service (SMS) One Time Password (OTP) via the registered mobile number. Likewise, credential combinations can consist of demographic and biometric information. Below are the acceptable credential combinations for identity verification:

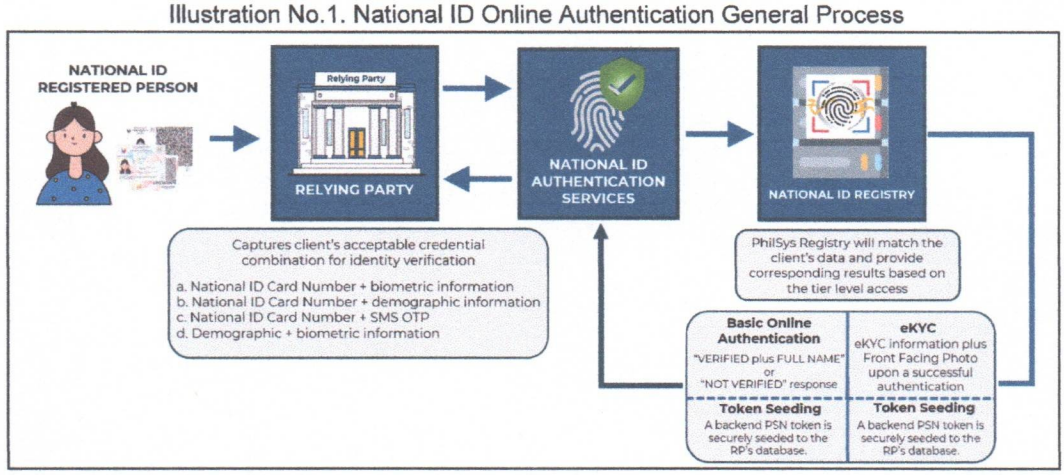
a. National ID Card Number + biometric information (iris scan or fingerprint or facial image)
b. National ID Card Number + demographic information (date of birth and last name)
c. National ID Card Number + SMS OTP via the registered mobile number

d. Demographic (full name and date of birth) + biometric information (iris scan or fingerprint or facial image)

Currently, NIDAS offers two online authentication services, Tier 1: Basic Online Authentication and Tier 2: electronic Know-Your-Customer (eKYC).

Illustrated below is the National ID Online Authentication general process.

Illustration No.1. National ID Online Authentication General Process

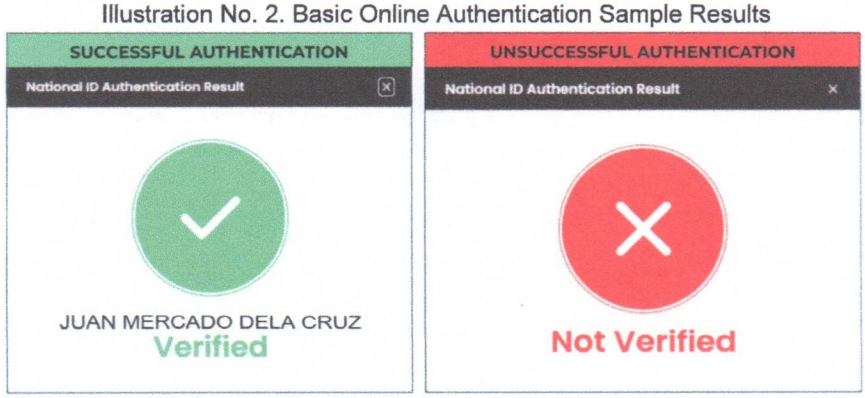


Tier 1: Basic Online Authentication

Tier 1 provides a simple VERIFIED plus Full Name and a back-end National ID Number token for successful authentication and NOT VERIFIED response, for unsuccessful authentication.

Under this tier, a National ID cardholder provides their National ID Card Number plus the biometric or demographic information, or OTP sent to their registered mobile number. This information is then sent to the National ID Registry for matching. The National ID Registry will return the corresponding response: the cardholder's full name plus VERIFIED and a back-end National ID Number token. However, a NOT VERIFIED response shall be issued from the National ID Registry if the National ID Card Number and the biometric or demographic information, or OTP do not match in the National ID Registry. This tier level is recommended for simple low-risk transactions.

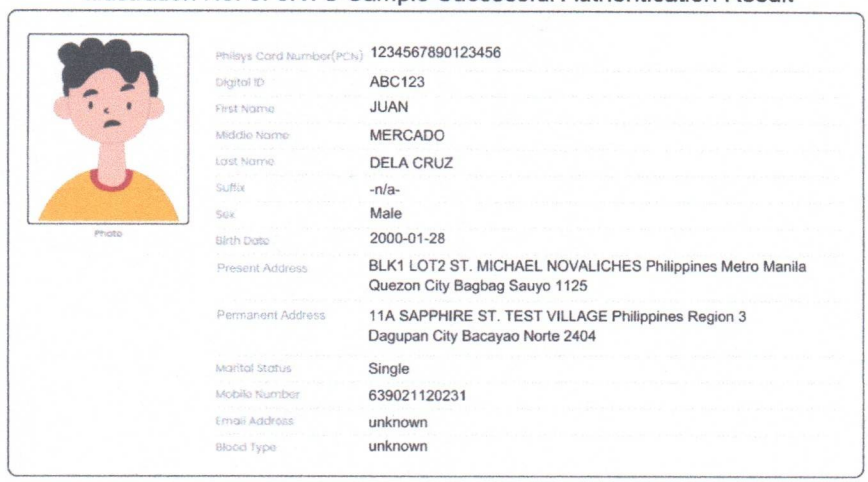
Illustration No. 2. Basic Online Authentication Sample Results



Tier 2: Electronic Know-your-customer

The Tier 2 or the eKYC service follows the same authentication process of Tier 1. However, in addition to the full name and back-end PSN token, the RP will also receive all the available demographic information (i.e., sex, date, and place of birth, blood type, address, marital status, mobile number, email address) and portrait photo of the National ID cardholder for every successful authentication. This information can be used to pre-populate online forms and/or saved in the RP's database.

Illustration No. 3. eKYC Sample Successful Authentication Result



Token Seeding

The National ID Registry generates a unique back-end PSN token when authentication is successful. This token can be seeded in the relying party's database and used to facilitate succeeding identity verifications of the same national ID cardholder. Additionally, sectoral tokens are applied, where each token is assigned to a specific sector such as healthcare, financial institution, or social welfare services. This ensures that a token used within one sector can facilitate identity verification and interoperability purposes with other onboarded relying parties within the same sector.

For more details, contact the following:

Government Services
Email: gsucd.staff@psa.gov.ph
Telephone Number: (02) 8710-8956

Social Protection
Email: spucd.staff@psa.gov.ph
Telephone Number: (02) 8775-9401

Private/Financial Institution
Email: fpsucd.staff@psa.gov.ph
Telephone Number: (02) 8533-7011

List of Regulatory Onboarding Requirements for the Government Sector

Requirements	Description
Letter of Intent (Tiers 1 and 2)	The LOI should be addressed to the National Statistician and Civil Registrar General and attention to the Deputy National Statistician of the PhilSys Registry Office, letter must be signed by the head of the agency.
Data Protection Officer (DPO) Certificate of Registration from the National Privacy Commission or DPO Designation/Special Order (Tiers 1)	The certificate/designation/special order shall be the latest copy. If issued by the NPC, the company name should match that stated in the application form.
Business Process Map (Tiers 1 and 2)	BPM should indicate how the PhilSys Registry would be incorporated into the Relying Party's system and how the National ID Authentication Services will work within the said system. BPM should be in narrative format with a detailed procedure for data sharing, including modes of transmittal. RP may also send an illustration of the PhilSys integration to its system provided with a narrative report/explanation.
Notarized Sworn Declaration (Tier 2)	Sworn Declaration attesting conduct/availability of the following: • Latest results of Privacy Impact Assessment (PIA) • Data Privacy Manual • Implementation of Data Privacy and Security Measures • Data Breach Protocols