



Telp : +62-21.5795 7300
Fax : +62-21.5795 7269
www.bdo.co.id

Tanubrata Sutanto Fahmi Bambang & Rekan
Certified Public Accountant
Licence No. 622/KM.1/2016

Head Office
Prudential Tower, 17th Floor
Jl. Jend. Sudirman Kav. 79
Jakarta 12910 - Indonesia

INDEPENDENT ASSURANCE REPORT

To the management of PT Indonesia Digital Identity ("VIDA-CA"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on VIDA-CA management's assertion that in generating and protecting its VIDA-CA SSL/TLS Root CAs on 24th February 2025 at Lintasarta Technopark Data Center, Komplek Pergudangan Taman Tekno Blok D No.8, BSD, Setu, Tangerang Selatan, Banten 15314, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
VIDA Root CA	5f8cbb4e86d55e3b5252f7052c050fea9ed0b87a	7c582a0ba0ef1b53eabb1d4ae16f6428
VIDA Domain Validation CA	fdf69a9a8980d4c84ddea64ce5449fc68ba3493f	74152f0bcfa497a2a0ae221050cb4161
VIDA Organization Validation CA	83b94093bbdf3b5540ce454f3770b70517678ca7	119376885d26e7f9c702e019d73971e8
VIDA Extended Validation CA	856f4b70ba2442a34323937dfb49785b85e9fcc2	38a2e3b4848d95cfd19ae86850b7f48a

VIDA-CA has:

- followed the CA key generation and protection requirements in its:
 - [VIDA Certificate Policy/Certification Practice Statement For TLS Certificates Version 1.0 with effective date on 1st May 2024](#)
- included appropriate, detailed procedures and controls in its SSL/TLS Root Key Generation Script(s):
 - Key Ceremony Script Activity TLS CA Version 1.0 with effective date on 24th February 2025
 - Envelope Distribution Version 1.0 with effective date on 24th February 2025
- maintained effective controls to provide reasonable assurance that the VIDA-CA SSL/TLS Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its SSL/TLS Root Key Generation Script(s)
- performed, during the root key generation process, all procedures required by the SSL/TLS Root Key Generation Script(s)

TANUBRATA SUTANTO FAHMI BAMBANG & REKAN

Tanubrata Sutanto Fahmi Bambang & Rekan (Certified Public Accountant), an Indonesian partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of international BDO network of Independent member firms.



- generated the CA keys in a physically secured environment as described in its CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Certification authority's responsibility

VIDA-CA's management is responsible for its assertion, including the fairness of its presentation, and for generating and protecting its CA keys in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Our independence and quality management

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform the procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of VIDA-CA's documented plan of procedures to be performed for the generation of the certification authority key pairs for the VIDA-CA SSL/TLS Root CAs;
2. reviewing the detailed CA key generation script(s) for conformance with industry standard practices;



3. testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
4. physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on 24th February 2025 were in accordance with the SSL/TLS Root Key Generation Script(s) for the VIDA-CA SSL/TLS Root CAs; and
5. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Opinion

In our opinion, throughout the 24th February 2025, VIDA-CA's management assertion, as referred to above, is fairly stated, in all material respects, in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

This report does not include any representation as to the quality of VIDA-CA's services beyond those covered by CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2, nor the suitability of any of VIDA-CA's services for any customer's intended purpose.

Susanto Bong

Partner at KAP Tanubrata Sutanto Fahmi Bambang & Rekan

Jakarta, Indonesia

11th March 2025





VIDA-CA MANAGEMENT'S ASSERTION

PT Indonesia Digital Identity ("VIDA-CA") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed SSL/TLS Root CAs known as "VIDA-CA SSL/TLS Root CAs". These CA's will serve as SSL/TLS Root CAs for client certificate services. In order to allow the CA's to be installed in a final production configuration, a SSL/TLS Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing key. This helps assure the non-refutability of the integrity of the VIDA-CA SSL/TLS Root CAs' key pairs, and in particular, the private signing keys.

VIDA-CA management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in VIDA-CA's Certificate Policy (CP) and Certification Practice Statement (CPS), and its SSL/TLS Root Key Generation Script(s), which are in accordance with CA Key Generation Criterion 4.1 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

VIDA-CA management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

VIDA-CA management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the VIDA-CA SSL/TLS Root CAs, and for the CA environment controls relevant to the generation and protection of its CA keys.

VIDA-CA management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the VIDA-CA SSL/TLS Root CA's on 24th February 2025 at Lintasarta Technopark Data Center, Komplek Pergudangan Taman Tekno Blok D No.8, BSD, Setu, Tangerang Selatan, Banten 15314, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
VIDA Root CA	5f8cbb4e86d55e3b5252f7052c050fea9ed0b87a	7c582a0ba0ef1b53eabb1d4ae16f6428
VIDA Domain Validation CA	fdf69a9a8980d4c84ddea64ce5449fc68ba3493f	74152f0bcfa497a2a0ae221050cb4161

PT Indonesia Digital Identity (VIDA)

World Trade Center 1, 13th Floor
Jl. Jend. Sudirman Kavling 29-31
Karet, Setiabudi, Jakarta Selatan 12950
Telp. +6221 2598 3275
Fax. +6221 2598 2531

www.vida.id



Root Name	Subject Key Identifier	Certificate Serial Number
VIDA Organization Validation CA	83b94093bbdf3b5540ce454f3770b70517678ca7	119376885d26e7f9c702e019d73971e8
VIDA Extended Validation CA	856f4b70ba2442a34323937dfb49785b85e9fcc2	38a2e3b4848d95cfd19ae86850b7f48a

VIDA-CA has:

- followed the CA key generation and protection requirements in its:
 - [VIDA Certificate Policy/Certification Practice Statement For TLS Certificates Version 1.0 with effective date on 1st May 2024](#)
- included appropriate, detailed procedures and controls in its SSL/TLS Root Key Generation Script(s):
 - Key Ceremony Script Activity TLS CA Version 1.0 with effective date on 24th February 2025
 - Envelope Distribution Version 1.0 with effective date on 24th February 2025
- maintained effective controls to provide reasonable assurance that the VIDA-CA SSL/TLS Root CAs were generated and protected in conformity with the procedures described in its CP/CPS and its SSL/TLS Root Key Generation Script(s)
- performed, during the root key generation process, all procedures required by the SSL/TLS Root Key Generation Script(s)
- generated the CA keys in a physically secured environment as described in its CP/CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Gajendran Kandasamy

Chief Risk Officer

11th March 2025

PT Indonesia Digital Identity (VIDA)

World Trade Center 1, 13th Floor

Jl. Jend. Sudirman Kavling 29-31

Karet, Setiabudi, Jakarta Selatan 12950

Telp. +6221 2598 3275

Fax. +6221 2598 2531

www.vida.id