



REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of Viking Cloud, Inc.:

Scope

We have examined Viking Cloud, Inc., a Sysnet North America, Inc. subsidiary (“VikingCloud”), management’s [assertion](#) that in managing the key lifecycle events for its key pairs contained on assets in Chicago, Illinois and Dallas, Texas, in the United States of America, for its keys as enumerated in [Attachment B](#), VikingCloud has:

- disclosed its key lifecycle management requirements in the applicable versions of its VikingCloud Certificate Policy and Certification Practices Statement (“CP/CPS”) as enumerated in [Attachment A](#), and followed such key lifecycle management requirements.
- maintained effective controls to provide reasonable assurance that keys are backed up, stored, and recovered by authorized personnel in trusted roles using multiple person control in a physically secured environment.
- maintained effective controls to provide reasonable assurance that:
 - private keys that are physically transported from one facility to another remain confidential and maintain their integrity;
 - hardware containing keys and associated activation materials are prepared for transport in a physically secure environment by authorized personnel in trusted roles using multiple person controls, and are transported within sealed tamper evident packaging;
 - keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and
 - key transportation events are logged

throughout the September 1, 2023 to August 31, 2024, based on the applicable criteria in 4.2 and 4.10 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Certification Authority’s Responsibilities

VikingCloud’s management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the applicable criteria in 4.2 and 4.10 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Independent Accountant’s Responsibilities

Our responsibility is to express an opinion about management’s responsibility based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether



management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgement, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. Our examination included:

- obtaining an understanding of VikingCloud's documented plan of procedures to be performed for the key lifecycle management.
- reviewing the detailed key logs for conformance with industry standards and disclosed practices in the VikingCloud's CP/CPS.
- testing and evaluating the effectiveness of controls over the integrity, confidentiality, and availability of all keys pairs, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the service.
- performing such other procedures as we considered necessary in the circumstances.

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

The relative effectiveness and significance of specific controls at VikingCloud and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.



Independent Accountant's Opinion

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of VikingCloud's services other than its operations in in Chicago, Illinois, and Dallas, Texas, in the United States of America, nor the suitability of any of VikingCloud's services for any customer's intended purpose.

BDO USA

November 22, 2024



**ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE
POLICY VERSIONS IN-SCOPE**

Policy Name	Policy Version	Policy Date
VikingCloud Certificate Policy and Certification Practices Statement	Version 7.7	August 14, 2024
VikingCloud Certificate Policy and Certification Practices Statement	Version 7.6	November 29, 2023
VikingCloud Certificate Policy and Certification Practices Statement	Version 7.5	August 31, 2023



ATTACHMENT B - CA KEYS IN-SCOPE FOR KEY LIFECYCLE MANAGEMENT ACTIVITIES

CA Keys			
Key Gen Date	SPKI Hash	Key Type	Key Size
8/16/2023	425CD11886A7586A22C7A775FDA32601B6BBD1ABFCB288B4CB9C4F8CD1D4E2A	ECDSA	P256
8/16/2023	4EC91E33F6DE069BB79E428D4B8554E5C6BA3CEC0217E351B762D7F7A55B8739	ECDSA	P256
8/16/2023	AA3BC5A12A27B124FCA6BDD7A348D2C7789276F40D193D01EA0D5B5BD1EF9776	ECDSA	P256
8/16/2023	F3E09FDFD85A66FCEBA05E02096CC3B6678C39B7B098E55917CEB394C6874194	ECDSA	P256
8/16/2023	172BE700587ECA1163F5630EC99C1C6F7CA737E8B08207D90CB37D8E6BF9BBAD	ECDSA	P256
8/16/2023	CAAAA53DFEDB3B3EB18D8320E9D001B5298DA67BD4CEE89336542BA04D29BB2F	ECDSA	P256
8/16/2023	48ED176ECA5B0AB27634B0ADF2E05A70A42DDA0980B27F188C5FD6B1A40D4165	ECDSA	P256
8/16/2023	565C8A6A081DEC665EB46DBA225FDC3884C289E3F034ACD61AFBA66F1AE0C535	ECDSA	P384
8/16/2023	073DC50BE260B514B1BCE380082E1A60EB5B0A2605F2A6B188E9DDC792E9F1DB	ECDSA	P384
8/16/2023	1F93042AAA10463EA4E5DD5BD57D103CA527853B495C2739AE9A0049D464720D	ECDSA	P384
8/16/2023	351F2171B67D970153FDBCE28E3DC13CE0FCFD363E1438A80C1CA85FD325BEE6	ECDSA	P384
8/16/2023	F580EF25A2EB1D151057ADA518BD353B2B7CE81F7B5ABB513DC5F2EE93125DEB	RSA	4096
8/16/2023	8BBA8662BBEBE6B60BE98E33A286401742976EE1A6F13616C3C1B28DBCA0152C	RSA	4096
8/16/2023	1FDA3A9E7701627BFCEA47702C3D1B3AF129EDF05D1CD3F592F0EC169AEC5E9A	RSA	4096
8/16/2023	8FC575DF3E8C0655FA772EFBDF627C420100343B2958D10F28906B1A1F6C1E80	RSA	4096



VIKING CLOUD, INC. MANAGEMENT'S ASSERTION

Viking Cloud, Inc., a Sysnet North America, Inc. subsidiary ("VikingCloud"), has deployed a public key infrastructure. As part of this deployment, it was necessary to implement and maintain effective key lifecycle management controls in managing the key lifecycle events of its key pairs to ensure the integrity, confidentiality, and availability of private keys contained in assets in Chicago, Illinois and Dallas, Texas, in the United States of America, for its CA keys enumerated in [Attachment B](#).

The keys were managed in accordance with key lifecycle management requirements described in applicable versions of the VikingCloud Certificate Policy and Certification Practices Statement ("CP/CPS") as enumerated in [Attachment A](#).

VikingCloud management has maintained effective CA Key Lifecycle Management Controls based on the applicable criteria in 4.2 and 4.10 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#). These controls were designed to provide reasonable assurance of adherence to these practices throughout the key lifecycle management process.


VikingCloud management is responsible for establishing and maintaining procedures over its CA Key Lifecycle Management Controls, and over the integrity and confidentiality of all private keys and activation materials (including physical keys, tokens, and passwords) used in the establishment of the VikingCloud private keys, and for the CA environmental controls relevant to the protection of its keys.

VikingCloud management has assessed the procedures and controls for the CA Key Lifecycle Management Controls. Based on that assessment, in management's opinion, in protecting its keys, VikingCloud has:

- disclosed its key lifecycle management requirements in the applicable versions of its VikingCloud CP/CPS as enumerated in [Attachment A](#), and followed such key lifecycle management requirements.
- maintained effective controls to provide reasonable assurance that keys are backed up, stored, and recovered by authorized personnel in trusted roles using multiple person control in a physically secured environment.
- maintained effective controls to provide reasonable assurance that:
 - private keys that are physically transported from one facility to another remain confidential and maintain their integrity;
 - hardware containing keys and associated activation materials are prepared for transport in a physically secure environment by authorized personnel in trusted roles using multiple person controls, and are transported within sealed tamper evident packaging;
 - keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and
 - key transportation events are logged



throughout the period September 1, 2023 to August 31, 2024 based on the applicable criteria in 4.2 and 4.10 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Signed by:

878AB99307394F5...

11/22/2024

Mark Brady
President and Chief Operating Officer, Viking Cloud, Inc



**ATTACHMENT A - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY
VERSIONS IN-SCOPE**

Policy Name	Policy Version	Policy Date
VikingCloud Certificate Policy and Certification Practices Statement	Version 7.7	August 14, 2024
VikingCloud Certificate Policy and Certification Practices Statement	Version 7.6	November 29, 2023
VikingCloud Certificate Policy and Certification Practices Statement	Version 7.5	August 31, 2023



ATTACHMENT B - CA KEYS IN-SCOPE FOR KEY LIFECYCLE MANAGEMENT ACTIVITIES

CA Keys			
Key Gen Date	SPKI Hash	Key Type	Key Size
8/16/2023	425CD11886A7586A22C7A775FDA32601B6BDDF1ABFCB288B4CB9C4F8CD1D4E2A	ECDSA	P256
8/16/2023	4EC91E33F6DE069BB79E428D4B8554E5C6BA3CEC0217E351B762D7F7A55B8739	ECDSA	P256
8/16/2023	AA3BC5A12A27B124FCA6BDD7A348D2C7789276F40D193D01EA0D5B5BD1EF9776	ECDSA	P256
8/16/2023	F3E09FDFD85A66FCEBA05E02096CC3B6678C39B7B098E55917CEB394C6874194	ECDSA	P256
8/16/2023	172BE700587ECA1163F5630EC99C1C6F7CA737E8B08207D90CB37D8E6BF9BBAD	ECDSA	P256
8/16/2023	CAAAA53DFEDB3B3EB18D8320E9D001B5298DA67BD4CEE89336542BA04D29BB2F	ECDSA	P256
8/16/2023	48ED176ECA5B0AB27634B0ADF2E05A70A42DDA0980B27F188C5FD6B1A40D4165	ECDSA	P256
8/16/2023	565C8A6A081DEC665EB46DBA225FDC3884C289E3F034ACD61AFBA66F1AE0C535	ECDSA	P384
8/16/2023	073DC50BE260B514B1BCE380082E1A60EB5B0A2605F2A6B188E9DDC792E9F1DB	ECDSA	P384
8/16/2023	1F93042AAA10463EA4E5DD5BD57D103CA527853B495C2739AE9A0049D464720D	ECDSA	P384
8/16/2023	351F2171B67D970153FDBCE28E3DC13CE0FCFD363E1438A80C1CA85FD325BEE6	ECDSA	P384
8/16/2023	F580EF25A2EB1D151057ADA518BD353B2B7CE81F7B5ABB513DC5F2EE93125DEB	RSA	4096
8/16/2023	8BBA8662BBEBE6B60BE98E33A286401742976EE1A6F13616C3C1B28DBCA0152C	RSA	4096
8/16/2023	1FDA3A9E7701627BFCEA47702C3D1B3AF129EDF05D1CD3F592F0EC169AEC5E9A	RSA	4096
8/16/2023	8FC575DF3E8C0655FA772EFBDF627C420100343B2958D10F28906B1A1F6C1E80	RSA	4096