Crowe FST Audit Kft.
Member of Crowe Horwath International

H-1124 Budapest
Jagelló út 14.
Hungary
Tel: +36 1 225-3490
Fax: +36 1 225-3491
www.crowehorwath.hu

INDEPENDENT ASSURANCE REPORT

To the management of NISZ National Infocommunications Service Company Limited By Shares Certification Authority. ("HunGOVCA"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on HunGOVCA management's assertion that for its Certification Authority (CA) operations at Budapest, Hungary, throughout the period 16-06-2016 to 15-06-2017 for its Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató, SSL Titkosító Tanúsítványkiadó 2014 - GOV CA, HunGOVCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - Certificate Policy for website authentication certificates (BR-WOT) version 1.0 and Certification Practice Statement for website authentication certificates (BSZ-WOT) version 1.0
- maintained effective controls to provide reasonable assurance that:
  - HunGOVCA s Certification Practice Statements are consistent with its Certificate Policies
  - HunGOVCA provides its services in accordance with its Certificate Policies and Certification Practice Statements,
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by HunGOVCA; and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the Webtrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, version 2.2

Crowe FST Audit Kft.
Member of Crowe Horwath International

H-1124 Budapest
Jagelló út 14.
Hungary
Tel: +36 1 225-3490
Fax: +36 1 225-3491
www.crowehorwath.hu

Certification authority's responsibilities

HunGOVCA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the Webtrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

Our independence and quality control

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 Control 1, 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.

Auditor'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 our 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 HunGOVCA's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;

(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;

(3) testing and evaluating the operating effectiveness of the controls; and

(4) 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.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at HunGOVCA 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.

Crowe FST Audit Kft.
Member of Crowe Horwath International

H-1124 Budapest
Jagelló út 14.
Hungary
Tel: +36 1 225-3490
Fax: +36 1 225-3491
www.crowehorwath.hu

Inherent limitations

Because of the nature and inherent limitations of controls, HunGOVCA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period 16-06-2016 to 15-06-2017, HunGOVCA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the Webtrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.
This report does not include any representation as to the quality of HunGOVCA's services beyond those covered by the Webtrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2., nor the suitability of any of HunGOVCA's services for any customer's intended purpose.

Use of the WebTrust seal

HunGOVCA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Crowe FST Audit Ltd.
Budapest, Hungary
28-07-2017

Crowe FST Audit Kft.
Member of Crowe Horwath International

H-1124 Budapest
Jagelló út 14.
Hungary
Tel: +36 1 225-3490
Fax: +36 1 225-3491
www.crowehorwath.hu

Annex

DN of Root CA	SHA256 fingerprint
CN = Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató O = NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. L = Budapest C = HU	C2:15:73:09:D9:AE:E1:7B:F3:4F:4D:F5:E8:8D:BA:EB A5:7E:03:61:EB:81:4C:BC:23:9F:4D:54:D3:29:A3:8D

DN of SSL CA	SHA256 fingerprint
CN = SSL Titkosító Tanúsítványkiadó 2014 - GOV CA O = NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. L = Budapest C = HU	44:CB:C0:5A:41:69:30:A4:A3:7F:6F:76:EF:49:E7:15 0B:8D:3D:78:60:56:41:51:41:8C:2C:7E:AB:7E:1D:53

NISZ NATIONAL INFOCOMMUNICATIONS SERVICE COMPANY LIMITED BY SHARES
MANAGEMENT'S ASSERTION

Hungarian Governmental Certification Authority ("HunGOVCA") is operated by NISZ National Infocommunications Service Company Limited by Shares, and has one Root CA server with Subject/CN=Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató, and one non-qualified intermediate CA servers related to website authentication certificates (SSL certificates): Subject/CN=SSL Titkosító Tanúsítványkiadó 2014 - GOV CA. Hungarian Governmental Certification Authority provides the following CA services:

- Subscriber registration
- Certificate issuance
- Certificate distribution
- Certificate validation
- Certificate revocation
- Subscriber key generation and management

The management of HunGOVCA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website (https://hiteles.gov.hu/szabalyzatok), CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and intermediate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to HunGOVCA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

HunGOVCA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in providing its Certification Authority (CA) services at Budapest, Hungary, throughout the period 16-06-2016 to 15-06-2017, HunGOVCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the following documents[1]:
  - Certificate Policy for website authentication certificates (BR-WOT) version 1.0 and
  - Certification Practice Statement for website authentication certificates (BSZ-WOT) version 1.0
- maintained effective controls to provide reasonable assurance that:
  - HunGOVCA's Certification Practice Statements are consistent with its Certificate Policies

[1] Out of these documents, BR-WOT and BSZ-WOT are available in English (http://hiteles.gov.hu/?lang=en)

  - HunGOVCA provides its services in accordance with its Certificate Policies and Certification Practice Statements,
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by HunGOVCA; and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the Webtrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, version 2.2 including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Escrow

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Attila Ferencz, Director of HunGOVCA

Budapest, 28-07-2017