

DNSSEC policy for .KZ and .қаз [xn--80ao21a] domains

1. INTRODUCTION

1.1 The following basic concepts and abbreviations are used in the document:

- 1) DNS - specialized software for servicing the domain name system, as well as the equipment on which the software is run;
- 2) DNSSEC - An extension to DNS that adds support for source authentication and data integrity check for the domain name system;
- 3) DS-record - the record points to the key that the zone located one level below (the delegated zone) should use to certify (sign) the address information;
- 4) DNSKEY-record - contains the public part of the key and its identifiers (ID, type and hash function used);
- 5) KSK - key for signing the DNSKEY resource record;
- 6) ZSK - key for signing resource records;
- 7) HSM - hardware protection module;
- 8) Subdomain - domain of the second, third and more levels.

2. GENERAL INFORMATION

2.1 This document describes the basic procedures for the operation of DNSSEC in the .KZ and .қаз [xn--80ao21a] TLDs.

2.2 The top-level domain registry itself determines the DNSSEC operation policy:

- 1) Manages KSK;
- 2) verifies and processes DNSSEC data received from an accredited registrar;
- 3) generates and signs resource records in the top-level domains file;
- 4) manages the ZSK and distributes the top-level domains file on the authorized DNS servers.

2.3 The registrar performs registration actions in the registry on behalf of the domain registrant. The registrar is responsible for verifying the KSK held by the domain name registrant.

2.4 Domain name registrants make the necessary changes with the help of accredited registrars and are responsible for the correctness of the signature of their domain zone, as well as for the relevance of the public keys placed in the registry in the form of DS records in accordance with their needs.

2.5 Concerned parties are participants in the Internet who rely on the work DNSSEC, example validating DNS servers, are responsible for setting up and updating the proper trusted public keys on their hardware.

2.6 The use of DNSSEC in subdomains is outside the scope of this document and is covered by the registrars of those domains.

3. OPERATIONAL REQUIREMENTS

3.1 The registry establishes a DNSSEC chain of trust by publishing a public KSK in the form of a DS record directly in the DNS root zone.

3.2 To activate DNSSEC in a subdomain, at least one DS-record must be placed in the top-level domains registry. The registry checks the data for correctness by checking whether the registry supports the algorithm by which the DS-record of the key tag is generated. If the verification of the DS record is successful, then the DS record of this domain will be published in DNS. The published DS record sets chain of trust to the subdomain.

3.3 It is the registrar's responsibility to securely identify and authenticate the subdomain registrant using appropriate methods.

3.4 The registry receives DS records from registrars using the EPP interface. DS and DNSKEY records must be correct and sent in the format described in RFC 4310. The Registry register supports the placement of DS records formed in accordance with RFC 4034 and RFC 5933.

3.5 The Registry does not perform additional checks in order to reliably determine that a subdomain registrant is in possession of a private key. It is the responsibility of the registrars to perform due checks.

3.6 The registry deletes the DS-record from the registry upon receipt of a corresponding request from the registrar through the EPP interface. Removing all DS records for a subdomain deactivates DNSSEC for that domain. Only the registrant of a subdomain, or a party officially authorized to represent the registrant, may, through the registrar, request the deletion of a DS record for that domain.

4. CONTROLS AND OPERATIONAL CONTROLS

4.1 The Registry has a Data Processing Center (DPC) on the territory of Kazakhstan. The data center includes tamper-proof server racks. Equipped with uninterruptible power supplies and air conditioning systems. A centralized fire extinguishing system is connected.

4.2 A room for procedures has been prepared in the office. Limited access is organized to the objects of the Registry, which is provided only to authorized personnel.

4.3 Critical media and backup copies are placed in safes, access to which is provided only to authorized personnel. Critical documents are destroyed by shredding. Electronic storage media before disposal are subjected to special formatting to exclude the possibility of recovering information previously recorded on these media.

4.4 To work with private KSK and ZSK keys, two trusted roles have been created: a crypto-officer and a crypto-operator, each of which consists of at least two authorized persons. Each of the authorized persons has a personal identifier and a password to it. An employee involved in working with private KSK and ZSK keys cannot simultaneously combine the roles of a crypto officer and a crypto operator.

4.5 To control the progress of the implementation of key procedures, a role has been created: Observer, which consists of at least two authorized persons. Observers provide transparency of the process and careful adherence to procedures when performing critical important operations with secret parts of KSK and ZSK keys.

4.6 The personnel described above are employees of the Registry. The personnel involved in the procedures should be experienced in the application of DNSSEC. New employees, before entering into the roles described above, should study internal documentation describing the implementation of DNSSEC. They must also take part in key procedures as observers before the start of performance of their duties.

4.7 Each fact of access to a specially designated work area with a critical DNSSEC information is stored in an automated accounting system. The automated access accounting systems is regularly reviewed and analyzed. The frequency of analysis is determined by the information security policy of the Registry.

4.8 If some event has led or may lead in security breaches, then an internal investigation is carried out in order to identify the causes of the incident and their elimination. If this event compromises critical DNSSEC information, then going on emergency keys change. The crypto operator initiates an emergency keys change procedure. If a key is compromised, the Registry will continue to operate that key until the emergency keys replacement procedure is completed.

5. TECHNICAL SAFETY

5.1 The create KSK keys are generated and stored in a specialized device called a HSM (Hardware Secure Module) which has not connection to the network infrastructure. All operations with using cryptographic conversion that require the participation of a closed KSK are performed on this device or on an identical one that is used as a backup. To ensure security, a closed KSK can leave the device only in encrypted type.

5.2 The create ZSK keys are generated and stored on the signing server, which connected to the

internal network of the top-level domain registry. All operations with using cryptographic conversions that require the participation of a closed ZSK, are performed on this device or on an identical device that used as reserve. For security, the closed ZSK can leave the device only encrypted.

5.3 An open KSK is distributed to the community using the DNS protocol.

Setting parameters and checking the quality of key information is carried out by the Registry.