Сценарий церемонии генерации первого ключа DNSSEC для домена UA

2 декабря 2011 года

Участники церемонии

- церемонимейстер (CA) - читает сценарий церемонии (медленно), следит за выполнением.
- администратор протокола (PA) - ведет протокол (с указанием временных меток).
- администратор ключей (KA) - выполняет действие и дает знак, что оно выполнено.
- хранитель главного ключа (KEO) - сохраняет ключ для подписания ключей.
- представитель DNS оператора (DOR) - сохраняет ключ для подписания зоны.
- администратор UA (AUA) - хранит публичные данные о DNSSEC (для IANA)
- наблюдатели - следят за соблюдением процедуры полностью и в точном порядке.

Перед началом убедиться в наличии и готовности оборудования:

- компьютер
- загрузочный диск
- устройства для записи ключей
- сейф-пакеты

Шаги церемонии

1. участники размещаются на своих местах (CA, PA, KA, KEO, DOR, AUA)

2. администратор ключей (KA) - загрузить систему OpenBSD с CD-диска.
Компьютер не подключен к интернету. Войти в системную консоль.

3. администратор ключей - создать новый ключ (key signing key)
Алгоритм RSASHA512 (номер 10), длина ключа 2048 бит, флаг KSK.

Созданы **три** файла:
Kua.+010.NNNNN.private
Kua.+010.NNNNN.key
Kua.+010.NNNNN.ds

4. администратор ключей - **показать на экране** публичный ключ и DS.

5. администратор ключей - подсоединить устройство хранения ключа (KSDN1) и записать на него сгенерированный ключ (все файлы)

6. администратор ключей - передать устройство хранения ключа (KSDN1) хранителю главного ключа.

7. хранитель главного ключа - поместить устройство хранения ключа (KSDN1) в пакет N1, закрыть пакет, вслух прочинать номер пакета (для протокола)

8. хранитель главного ключа может удалиться (спрятав пакет N1 в надежное место)

9. представитель DNS оператора - передать устройство хранения ключа 2 (далее называемое KSDN2) администратору ключей.

10. администратор ключей - создать новый ZSK, параметры:
Алгоритм RSASHA512 (номер 10), длина ключа 1024 бита.

созданы **три** файла (значение номера ключа отличается от шага 3)
Kua.+010.KKKKK.private
Kua.+010.KKKKK.key
Kua.+010.KKKKK.ds (этот файл должен быть удален как неиспользуемый).

11. администратор ключей - **показать на экране** публичный ключ ZSK.
администратор ключей - прочитать номера созданных ключей для контроля.

12. администратор ключей - подписать ZSK с помощью KSK - файл K.ua.+010.KKKKK.rrsig.

13. администратор ключей - записать подписанный ключ (все файлы из 10 и 12) на устройство (KSDN2).

14. администратор ключей - передать KSDN2 представителю DNS оператора.

15. представитель DNS оператора - поместить устройство хранения ключа (KSDN2) в пакет N2,
закрыть пакет, вслух прочинать номер пакета (для протокола)

16. Представитель DNS оператора может удалиться (пакет N2 сохраняется в надежном месте).

17. администратор ключей - удалить все приватные файлы ключей; **показать список файлов на экране**.

18. администратор ключей - **показать на экране** значение DS hash.

19. администратор ключей - записать публичные ключи и значение DS hash на устройство хранения ключа (KSDN3)

20. администратор ключей - передать устройство KSDN3 администратору UA.

21. Администратор UA - поместить устройство хранения ключа (флешку KSDN3) в пакет, закрыть пакет, вслух прочитать номер пакета (для протокола)

22. Выключение компьютера. Окончание церемонии.

Подписи участников:

- церемонимейстер (CA)

- администратор протокола (PA)

- администратор ключей (KA)

- хранитель ключа (KEO)

- представитель DNS оператора (DOR)

- администратор UA (AUA)

Подписи наблюдателей:

Замечания о прохождении церемонии:

;; DNSSEC.UA.KSK.ZSK.20111202 ;;