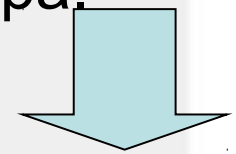
Рабочие вопросы внедрения DNSSEC в инфраструктуру DNS

Коваленко Дмитрий, ТЦИ
kovalenko@tcinet.ru

RIPE NCC Regional Meeting/ENOG, 06.06.2011-08.06.2011

DNS инфраструктура . RU, .РФ, .SU

- ЗАО «Технический Центр Интернет» (ТЦИ) обслуживает главный реестр и систему регистрации доменов RU, .РФ, .SU
- ЗАО «МСК-IX» предоставляет DNS-сеть серверов для размещения доменных зон .RU, .РФ, .SU , которая распределена не только по территории России, но и по другим странам мира.



Совместная работа над внедрением DNSSEC в инфраструктуру DNS

Технический Центр Интернет

Технология DNSSEC

MSK IX

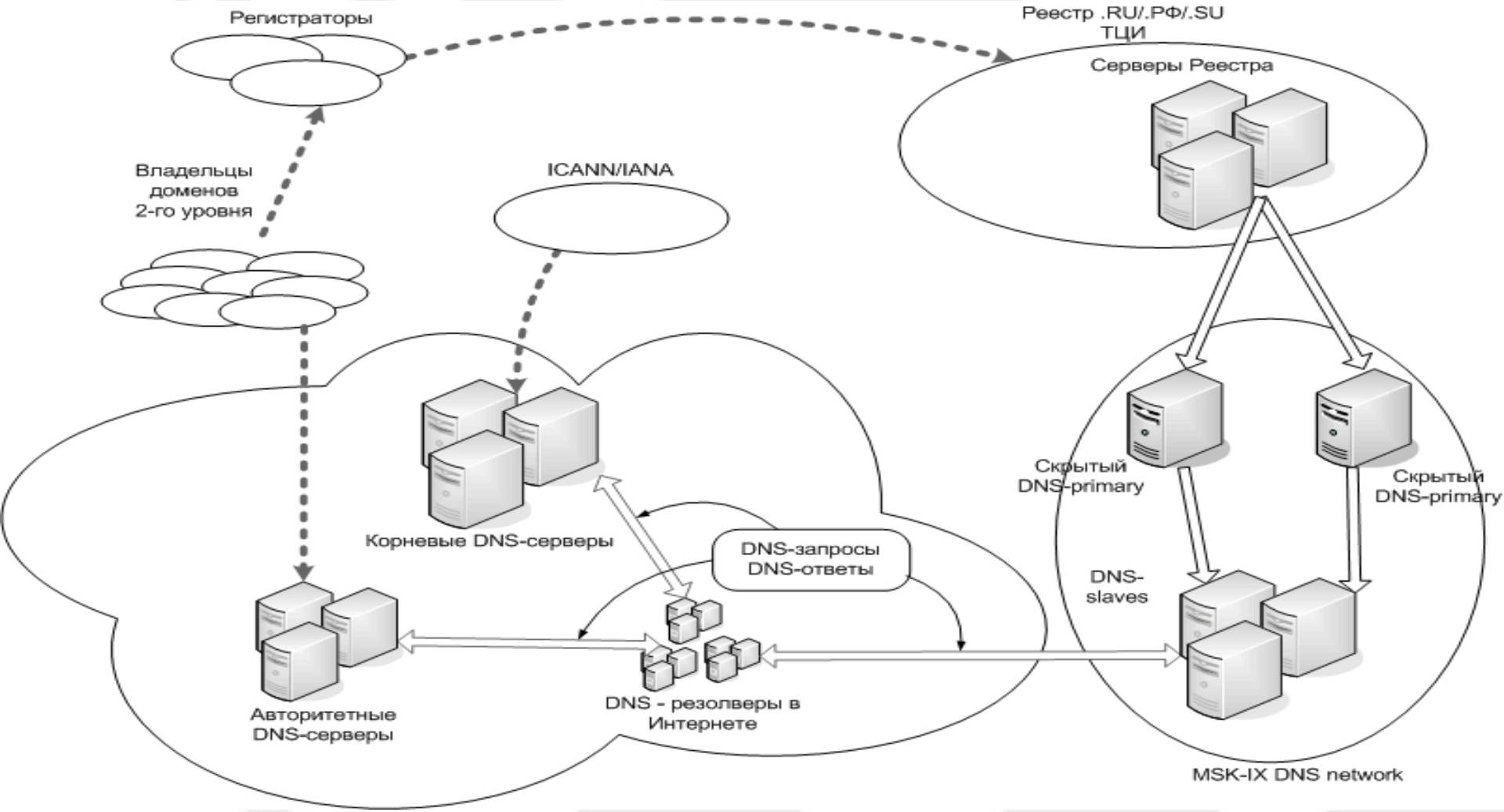
DNSSEC (DNS Security Extensions) – набор расширений протокола DNS, обеспечивающих контроль подлинности и целостности DNS данных.

DNSSEC делает невозможным попытки злоумышленников с помощью системы DNS перенаправить пользовательские запросы на подставные серверы.

Технический Центр Интернет

Инфраструктура DNS

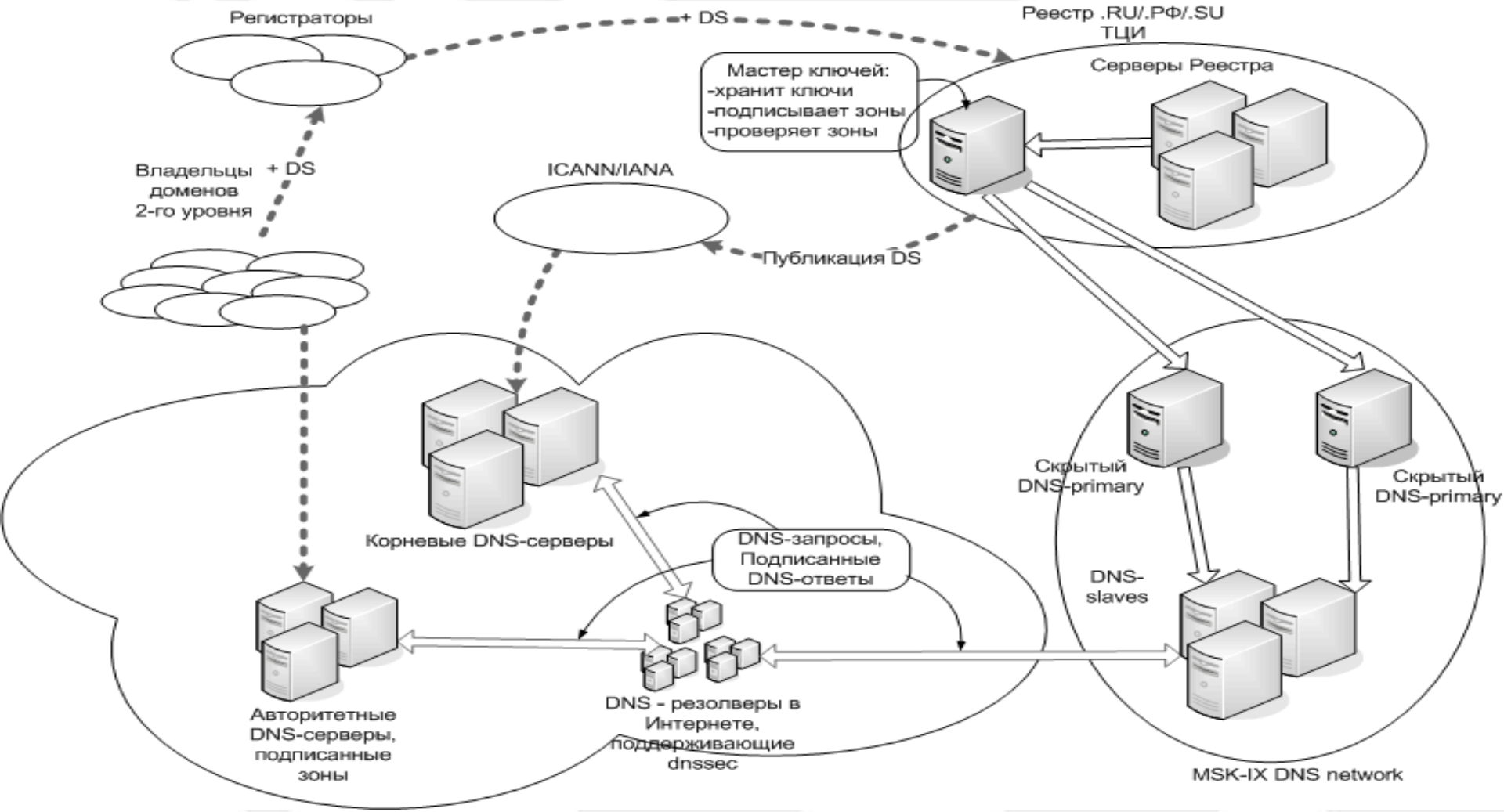
MSK IX



Технический Центр Интернет

Инфраструктура DNS+DNSSEC

MSK IX



Технический Центр Интернет

Внедрение DNSSEC

MSK IX

- Разработка технического решения;
- Разработка требований к техническим ресурсам, необходимым для развертывания DNSSEC в штатном режиме;
- Тестирование решений с помощью пилотной зоны;
- Разработка административно-технической документации;
- Взаимодействие с регистраторами.

Технический Центр Интернет

Результаты тестирования

MSK IX

- ПО — BIND;
- Алгоритм — RSA;
- Длина KSK — 2048 бит, Время жизни KSK — 1 год;
- Длина ZSK — 1024 бита, Время жизни ZSK — 3 месяца;
- NSEC3 Opt-Out;
- Каналы между master и slave серверами не менее 50 мбит/сек;
- Хранение ключей в аппаратном модуле безопасности (HSM), взаимодействие через интерфейс PKCS#11;
- Необходим интерфейс администрирования DNSSEC
- Реализовать возможность добавления DS записей в реестр доменной зоны.

Результаты тестирования

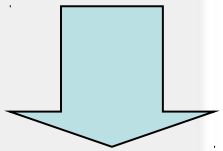
- ПО — BIND;
- Алгоритм — RSA;
- Длина KSK — 2048 бит, Время жизни KSK — 1 год;
- Длина ZSK — 1024 бита, Время жизни ZSK — 3 месяца;
- NSEC3 Opt-Out;
- Каналы между master и slave серверами не менее 50 мбит/сек;
- Хранение ключей в аппаратном модуле безопасности (HSM), взаимодействие через интерфейс PKCS#11;
- Необходим интерфейс администрирования DNSSEC
- Реализовать возможность добавления DS записей в реестр доменной зоны.

Технический Центр Интернет

Безопасное хранение ключей

MSK IX

Непростая процедура ввоза криптографической продукции



- Аппаратные модули безопасности (HSM) на базе USB-токенов
- Программные реализации HSM

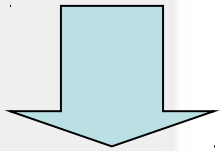
Технический Центр Интернет

USB-токены

MSK IX

Требования:

- Поддержка PKCS#11;
- Поддержка GNU/Linux, (опционально xBSD);
- Неизвлекаемый закрытый ключ;
- Поддержка RSA (до 2048 bit);
- Поддержка GOST (опционально).



Aladdin eToken PRO, Rutoken, ПСКЗИ ШИПКА

Технический Центр Интернет

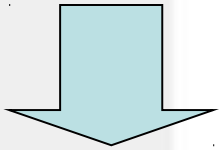
Программные реализации HSM

MSK IX

SoftHSM - часть проекта OpenDNSSEC

Особенности:

- Извлекаемый закрытый ключ
- Поддержка большинством Unix-like OS
- В следующих версиях заявлена поддержка GOST



FreeBSD + BIND + PKCS#11 + SoftHSM

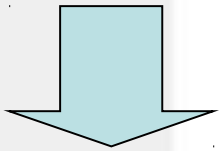
Технический Центр Интернет

Управление ключами DNSSEC

MSK IX

Требования к интерфейсу администрирования DNSSEC :

- Задание параметров DNSSEC для доменной зоны
- Управление состоянием ключей
- Управление ротацией ZSK и KSK

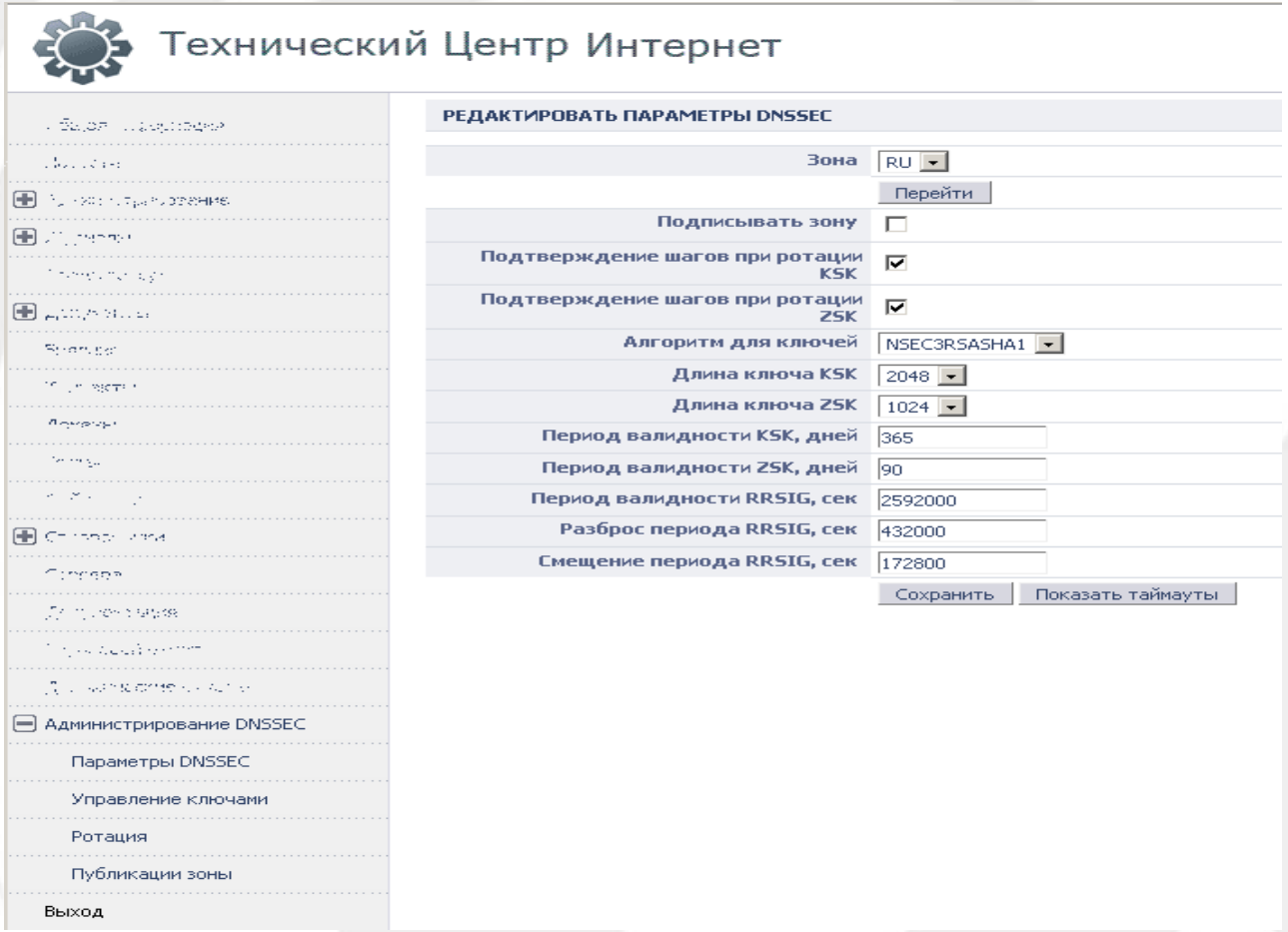


Разработан интерфейс администрирования DNSSEC (на этапе тестирования)

Технический Центр Интернет

Интерфейс администрирования DNSSEC

MSK IX

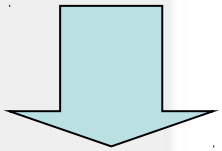


Технический Центр Интернет

Тестовый реестр

MSK IX

- В тестовом реестре реализована возможность публикации DS средствами протокола EPP
- Поддержка DS, сформированных алгоритмами SHA-1 (1), SHA-256 (2), GOST R 34.11-94 (3)
- Продолжает работу тестовый стенд DNSSEC



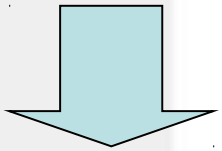
Присоединяйтесь
(заявка на noc-dns@ix.ru в свободной форме)

Технический Центр Интернет

MSK IX

Планы

- Протестировать возможность раздельного хранения ZSK и KSK при использовании BIND
- Завершить тестирование интерфейса администрирования DNSSEC
- Завершить разработку административно-технической документации



Создать надежную, безопасную и стабильную инфраструктуру для подписи TLD: RU,SU,РФ;

Ваши вопросы

?

Спасибо за внимание