nic MX®

Network
Information
Center
México

DNSSEC en .mx

Agenda

1. About NIC México
2. .mx DNSSEC test bed
3. Education about DNSSEC
4. NSEC zone walking

About NIC México

- ccTLD operator of .mx (México).
- National Internet Registry (México).
- .mx registrations are possible under the following SLDs only:
  - com.mx (open)
  - edu.mx (restrictions apply)
  - gob.mx (restrictions apply)
  - net.mx (restrictions apply)
  - org.mx (restrictions apply)
  - test.mx (restrictions apply)

About NIC México

- .mx registrations are possible trough:
  - NIC México registrar.
  - Other registrars using API-MX.
- Almost all systems are developed and operated in house.
- IT infrastructure is developed and operated in house.
- 185,453 domains under .mx to date.

Network
Information
Center
México

.mx DNSSEC test bed

Goals of the project

- Analysis of system modifications needed in the Registrar and Registry areas of NIC México to support DNSSEC.
- Internal education about DNSSEC.
- Creation of tools for a smooth transition to DNSSEC.
- Education of the Mexican Internet Community about DNSSEC.

How the test bed works

- Began operation in May 2006.
- test.mx SLD was created with the sole purpose of new technology deployments.
- test.mx to date is a DNSSEC enabled zone.
- Registrations under test.mx are open and free.
- The only rule is that you can’t register a test.mx domain if that domain is present in another .mx SLD.
  - Example: you can’t register ibm.test.mx because ibm.com.mx exists.

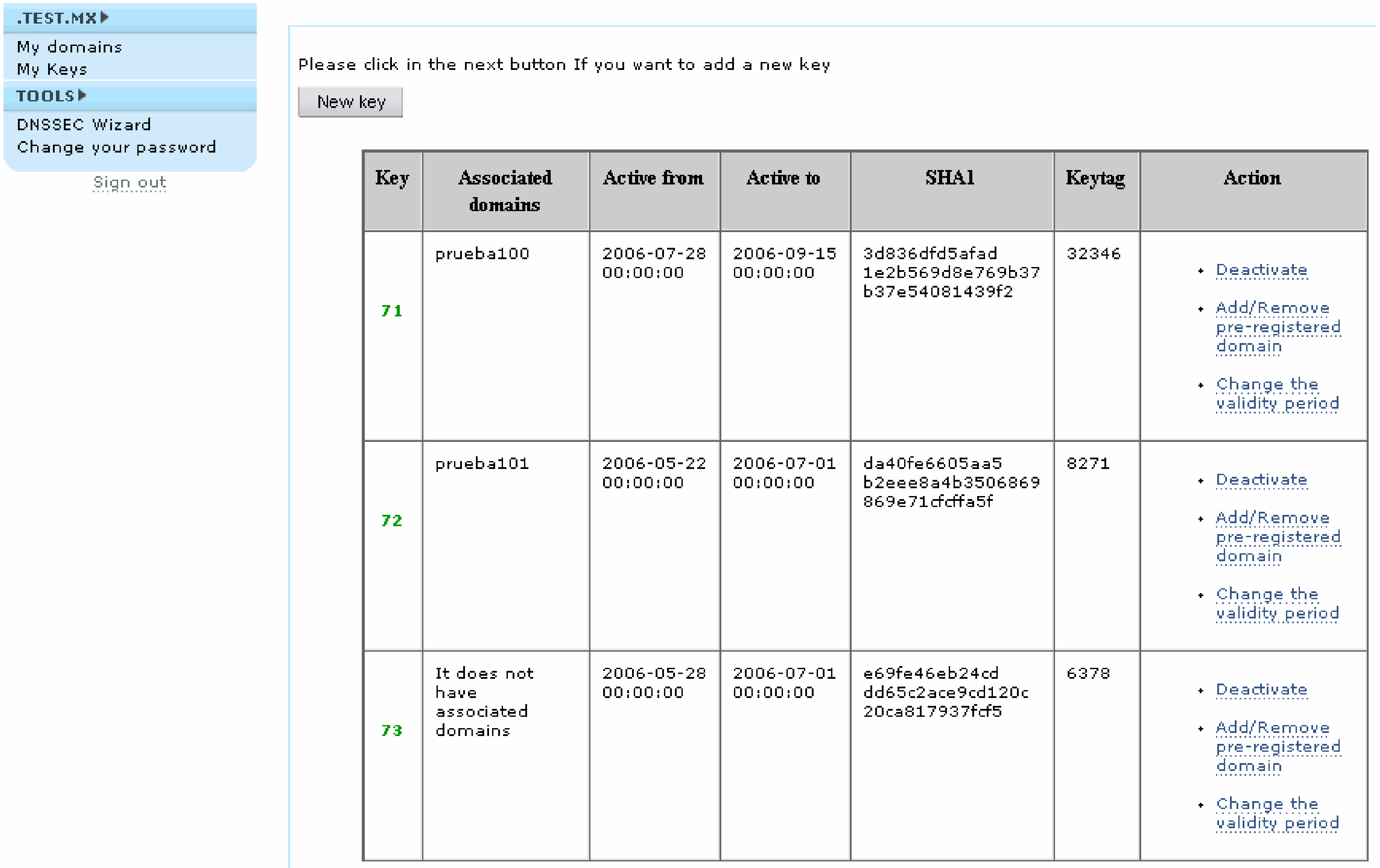
How the test bed works

- The focus of the test bed is registrar centric at the moment.
- DNS operators have expressed that probably they will use the same DNSKEY for all the zones they manage.
- The DNSSEC test bed systems is like a DNSKEY repository. The user assigns a previous loaded DNSKEY to an specific domain.
- When a DNSKEY is assigned to a domain a DS RR is created in the zone. A validation process takes places to verify that the server of the user is authoritative and DNSSEC enabled for the domain.

How the test bed works

- The user specifies a period of time of the key and domain assignation. The user can control for how long the DS record is going to be published with this option.

How the test bed works



Please click in the next button If you want to add a new key

Key	Associated domains	Active from	Active to	SHA1	Keytag	Action
71	prueba100	2006-07-28 00:00:00	2006-09-15 00:00:00	3d836dfd5afad1e2b569d8e769b37b37e54081439f2	32346	• Deactivate • Add/Remove pre-registered domain • Change the validity period
72	prueba101	2006-05-22 00:00:00	2006-07-01 00:00:00	da40fe6605aa5b2eee8a4b3506869869e71cfcffa5f	8271	• Deactivate • Add/Remove pre-registered domain • Change the validity period
73	It does not have associated domains	2006-05-28 00:00:00	2006-07-01 00:00:00	e69fe46eb24cddd65c2ace9cd120c20ca817937fcf5	6378	• Deactivate • Add/Remove pre-registered domain • Change the validity period

Technical details

- **Key administration system:**
- The key administration system is a tool that allows KSK and ZSK management.
- Keys are created in a server using hardware for random number generation.
- The private part of the KSK is stored in a smart card and the keyset signing is done in the smart card.
- The key administration server is not connected to the net and it is stored on a safe place.
- Keys and RRSIG RRs are transferred from the key administration server to the signing server with an USB memory card.

Technical details

- **Provisioning system:**
- The provisioning system allows the user to register test.mx domains and generate DS RRs.

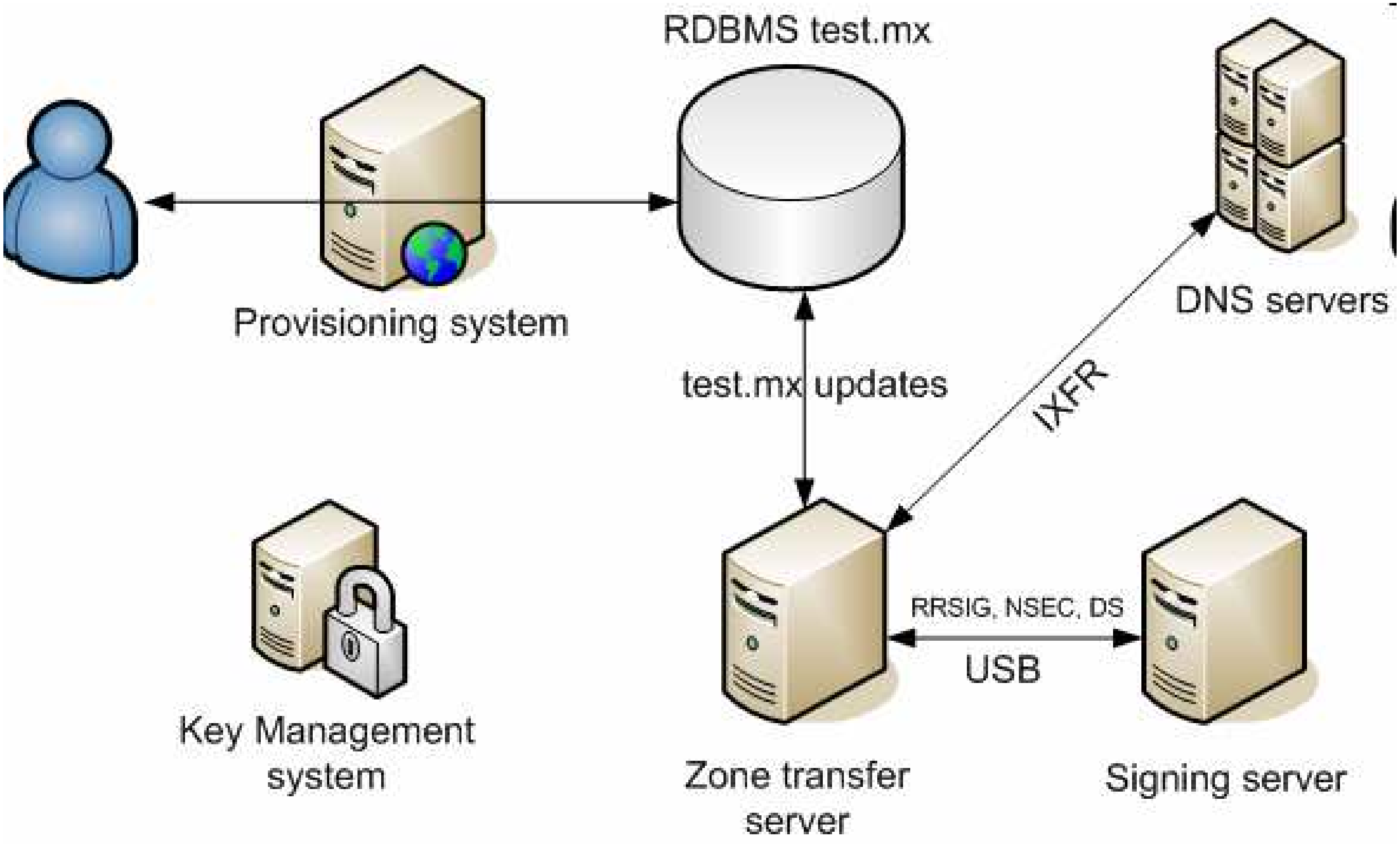
Technical details

- **Signing system:**
- Backend of the project.
- Two servers interconnected by a serial or USB cable.
- The signing server is totally isolated from the network and its function is to generate RRSIGs. The signing server has the private part of the test.mx ZSKs used in the zone and the RRSIGs of the keyset by the test.mx KSKs.
- The zone transfer server communicates directly with the provisioning RDBMS and when a zone change is detected it communicates with the signing server sending the RR changes (A, NS and DS RRs) and receiving the required RRSIGs.

Technical details

- **Signing system:**
- When the RRSIGs are received in the transfer server, it recreates the zone and then changes are sent via AXFR or IXFR to the test.mx authoritative servers.
- The signing server can initiate a ZSK scheduled rollover.

Technical details



Network
Information
Center
México

Education about DNSSEC

Education

- Two workshops were held in México City in the first semester of 2006. Telco companies, universities and private business attended the workshops.

- The first workshop had place the 8th and 9th of March of 2006. Persons from the following business attend this workshop:
  - **UNAM, LUX, EDS, BESTEL, Universidad La Salle, ANUIES and Telcel.**

- The second workshop was given to people from RedUno/Telmex, the biggest Telco in México, at their request.

- A third workshop took place in Monterrey.

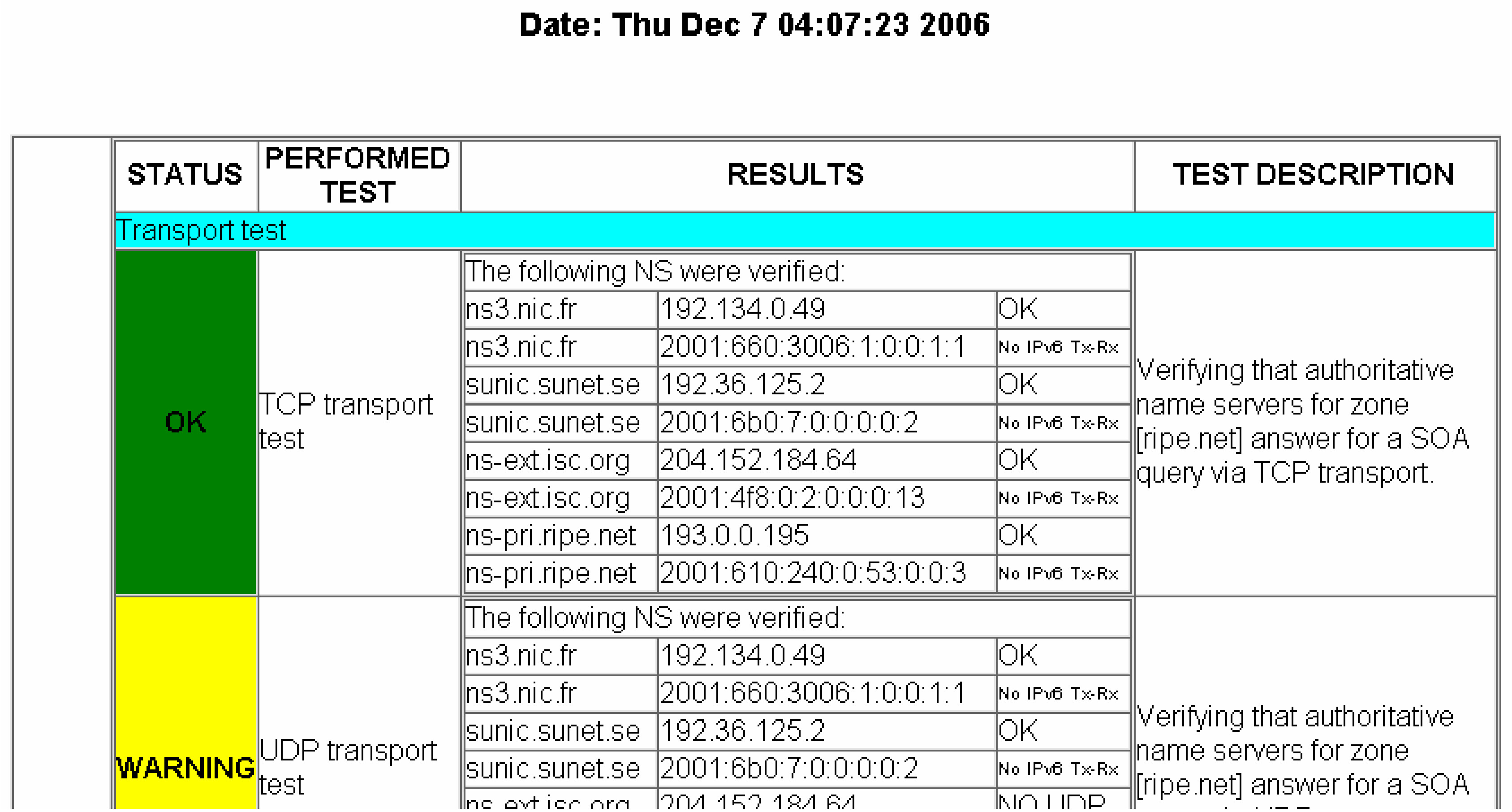
Workshop contents

- Attack vectors
- Cryptography theory
- DNSKEY creation
- Zone Signing
- DS generation
- TSIG
- Key Rollover

Feedback from the workshops

- When do I need to implement DNSSEC?
  - This question is reworded as: when market forces will force me to implement DNSSEC?, because DNS works very well right now.
- Personnel on ISPs uses dnsreport.com, checkdns.net, etc. to debug DNS and they want something similar for DNSSEC.
  - In response we created the DNSSEC verification tool. http://www.dnssec.org.mx/checkdnssec.html

DNSSEC verification tool



Date: Thu Dec 7 04:07:23 2006

STATUS	PERFORMED TEST	RESULTS			TEST DESCRIPTION
Transport test					
OK	TCP transport test	The following NS were verified:			Verifying that authoritative name servers for zone [ripe.net] answer for a SOA query via TCP transport.
		ns3.nic.fr	192.134.0.49	OK	
		ns3.nic.fr	2001:660:3006:1:0:0:1:1	No IPv6 Tx-Rx	
		sunic.sunet.se	192.36.125.2	OK	
		sunic.sunet.se	2001:6b0:7:0:0:0:0:2	No IPv6 Tx-Rx	
		ns-ext.isc.org	204.152.184.64	OK	
		ns-ext.isc.org	2001:4f8:0:2:0:0:0:13	No IPv6 Tx-Rx	
		ns-pri.ripe.net	193.0.0.195	OK	
		ns-pri.ripe.net	2001:610:240:0:53:0:0:3	No IPv6 Tx-Rx	
WARNING	UDP transport test	The following NS were verified:			Verifying that authoritative name servers for zone [ripe.net] answer for a SOA
		ns3.nic.fr	192.134.0.49	OK	
		ns3.nic.fr	2001:660:3006:1:0:0:1:1	No IPv6 Tx-Rx	
		sunic.sunet.se	192.36.125.2	OK	
		sunic.sunet.se	2001:6b0:7:0:0:0:0:2	No IPv6 Tx-Rx	
		ns-ext.isc.org	204.152.184.64	NO UDP	

Network
Information
Center
México

NSEC zone walking

NSEC zone walking

- A RRtype called NSEC is used in DNSSECbis to allow denial of existence.
- The NSEC RR points to the next existent domain in the zone allowing the retrieval of zone’s content with simple DNS queries.
- Until NSEC zone walking problem is solved NIC México won’t implement DNSSEC in production zones.

NSEC zone walking

- A solution (RFC4470) exists to the zone walking problem but online signing is necessary.
- The IETF DNSEXT WG is working on an offline signing solution called NSEC3.

DNS proxy

- NIC México has an ongoing project called DNS proxy. A software that allows online signing is being developed.

- DNS proxy receives a DNS query then it send the query to the DNS server implementation (BIND, NSD, ANS) and when a NSEC RR is returned it will do RFC 4470 in order to not expose .mx zone.

- Plug-ins can be incorporated to DNS proxy to extent functionality, for example: statistical measurements, load balancing, etc.

Perguntas?

Obrigado!

Gustavo Lozano

glozano@nic.mx