اعتماد استخدام الامتداد الآمن لأسماء النطاقات في أسماء النطاقات السعودية

Implementing DNSSEC in Saudi Domain Names

ICANN60 - Oct 2017

Raed Alfayez, SaudiNIC/CITC

What has been done so far

ما تم إنجازه من قبل المركز حتى الآن

مرحلة المتابعة
Follow up Phase

Before 2015

- التعلم من أخطاء الأخرين
- انتظار نضوج التقنية
- Learning from others' mistakes
- Waiting for application maturity and availability of tools

مرحلة الدراسة
Studying Phase

2015

- تجارب الدول
- المواصفات الدولية
- Country case studies
- International standards

مرحلة التنفيذ
Execution Phase

2016-2017

- أولا: كسب الخبرة المحلية
- ثانيا: التشغيل التجريبي
- ثالثا: التشغيل الفعلي
- Stage I: Gaining and building local expertise.
- Stage II: Prototype and experimental operation.
- Stage III: Launching the actual operation.

What has been done so far

- Starting with a balanced and forethought pace
  - Continuous follow-up to international developments
  - Why wait?
    - Rapid changes in specifications to this moment
    - Waiting for application maturity and availability of tools
    - Take advantage of the experience of others and learn from their mistakes.
    - The percentage of global use by the public was around 2%
- After the maturity of DNSSEC, SaudiNIC (2015) has:
  - Conducted an extensive and comprehensive study on how to adopt DNSSEC in the Saudi Domain Name System :
    - Gaining local experience about DNSSEC, how it works and its requirements
    - Studying international standards
    - Exploring some international experiences (eg: Netherlands, New Zealand, Canada, Australia, Austria).

ما تم إنجازه من قبل المركز حتى الآن

- البدء بخطى متزنة ومتروية
  - المتابعة المستمرة للتطورات الدولية
  - لماذا التريث
    - التغير السريع للمواصفات حتى هذه اللحظة
    - انتظار نضج التطبيقات و توفر الأدوات
    - الاستفادة من خبرة وتجارب الآخرين والتعلم من الأخطاء التي تعرضوا لها
    - نسبة الاستخدام العالمي من قبل العموم حوالي ٢%
- بعد نضوج تقنية الامتداد الآمن قام المركز (٢٠١٥م) :
  - بعمل دراسة مكثفة وشاملة حول كيفية تبني الامتداد الآمن (DNSSEC) في منظومة أسماء النطاقات السعودية لغرض:
    - كسب الخبرة المحلية للتعرف على الامتداد الآمن وكيفية عمله ومتطلباته
    - دراسة المواصفات والمعايير الدولية
    - التعرف على بعض التجارب الدولية (مثل: هولندا ، نيوزيلندا ، كندا ، أستراليا ، النمسا).

What has been done so far

- The study concluded with the development of a three-phase roadmap to adopt DNSSEC in Saudi domains:
  - Stage I: Gaining and building local expertise.
  - Stage II: Prototype and experimental operation.
  - Stage III: Launching the actual operation.
- Establishing an internal team
  - Read .. Meetings .. Brainstorming .. Tests .. Documentation
- Setting up an experimental environment for tests and experiments.
- Operational DNSSEC service

ما تم إنجازه من قبل المركز حتى الآن

- خلصت الدراسة إلى وضع خطة (خارطة طريق) مكونة من ثلاثة مراحل أساسية لتبني الامتداد الآمن لأسماء النطاقات:
  - المرحلة الأولى: كسب الخبرة المحلية
  - مرحلة الثانية: التشغيل التجريبي
  - مرحلة النهائية: التشغيل الفعلي
- إنشاء فريق داخلي (فني تأسيسي)
  - قراءة .. اجتماعات .. عصف ذهني .. اختبارات .. توثيق
- إنشاء بيئة تجريبية عبارة عن معمل للاختبارات والتجارب.
- التشغيل الفعلي للخدمة

Training and Workshops

عقد ورش عمل

- Coordinating with RIPE NCC to provide training workshops at the CITC headquarter:
  - Titled: "DNSSec Safe Extension"
- 3 Days course (14-16 Oct 2015):
  - For CITC and SaudiNIC employees and some specialists in the sector.
  - 25 participant from 11 government agencies and ICT operators
- 2 Days course (7-9 May 2017)
  - For ISPs, the banking sector, and some government agencies
  - 41 participant from 29 government agencies and ICT operators
- 1 Day public event (9 May 2017)
  - 120 participant

- تم التنسيق مع منظمة الرايب (RIPE NCC) لتقديم برامج تدريبية في مقر الهيئة:
  - تحت عنوان "الامتداد الآمن لنظام أسماء النطاقات "DNSsec
- دورة ٣ أيام (٢٩-ذو الحجة-١٤٣٦هـ)
  - موجها لموظفي الهيئة في المركز السعودي لمعلومات الشبكة والمختصين في القطاع
  - ٢٥ مشارك يمثلون ١١جهة من الهيئات الحكومية والمنظمات ومقدمي خدمات الاتصالات وتقنية المعلومات في المملكة.
- دورة يومين (١١ شعبان ١٤٣٨هـ)
  - لمزودي الخدمات والقطاع المصرفي وبعض الجهات الحكومية
  - ٤١ مشارك يمثلون ٢٩ جهة من الهيئات الحكومية والقطاع المصرفي ومقدمي خدمات الاتصالات وتقنية المعلومات في المملكة.
- ورشة عمل ليوم واحد (١٣ شعبان ١٤٣٨هـ)
  - ١٢٠ مشارك من المختصين بأمن المعلومات

DNSSEC adoption methodology

عقد ورش عمل

DNSSEC adoption methodology

عقد ورش عمل

Some Deliverables

بعض المخرجات

- SaudiNIC DPS
- DNSSEC Setup
- SaudiNIC DNSSEC Procedures
- DNSSEC Credential Matrix
- DNSSEC Key Management Risks
- Website and Tools (Arabic + English)
- Fully operational

- وثيقة ممارسات المركز
- إعداد التصاميم وطريقة العمل
- وثيقة إجراءات الامتداد الآمن
- تحديد الصلاحيات
- خطة إدارة المخاطر
- موقع وأدوات خاص بالامتداد (باللغتين العربية والانجليزية)
- الاطلاق الفعلي للامتداد

SaudiNIC DPS

وثيقة ممارسات المركز

SaudiNIC DNSSEC Practice Statement

1 INTRODUCTION

The Domain Name System Security Extension (DNSSEC) Practice Statement (DPS) is a statement of security practices and provisions made by the Saudi Network Information Center (SaudiNIC). This DPS is intended to document the policy practices and procedures that are followed in conjunction with DNSSEC for the Saudi Top Level Domains (TLD) that are managed by SaudiNIC (.SA and .السعودية). It is based on the RFC 6841: A Framework for DNSSEC Policies and DNSSEC Practice Statements.

1.1 Overview

DNSSEC is an extension of the existing Domain Name System (DNS) that provides the capabilities to validate that the DNS data has not been tampered with or modified during Internet transit and it came for the actual source. This is accomplished by incorporating public key cryptography into the DNS hierarchy to form a chain of trust originating from the root zone.

1.2 Document Name and Identification

- Document Title: SaudiNIC DNSSEC Practice Statement
- Version: 1.0

ممارسات المركز السعودي لمعلومات الشبكة (SaudiNIC) لتطبيق الامتداد الآمن لنظام أسماء النطاقات (DNSSEC)

1 مقدمة

تهدف هذه الوثيقة إلى بيان وتوثيق الممارسات والإجراءات والضوابط الأمنية التي يعمل بها المركز السعودي لمعلومات الشبكة (SaudiNIC) لتطبيق الامتداد الآمن لنظام أسماء النطاقات (DNSSEC) وذلك على النطاقات العلوية السعودية والتي يديرها ويشرف عليها المركز السعودي لمعلومات الشبكة (sa. و .السعودية). وتعتمد هذه الوثيقة على الوثيقة المرجعية RFC 6841، وعنوانها: "A Framework for DNSSEC Policies and DNSSEC Practice Statements".

1.1 نظرة عامة

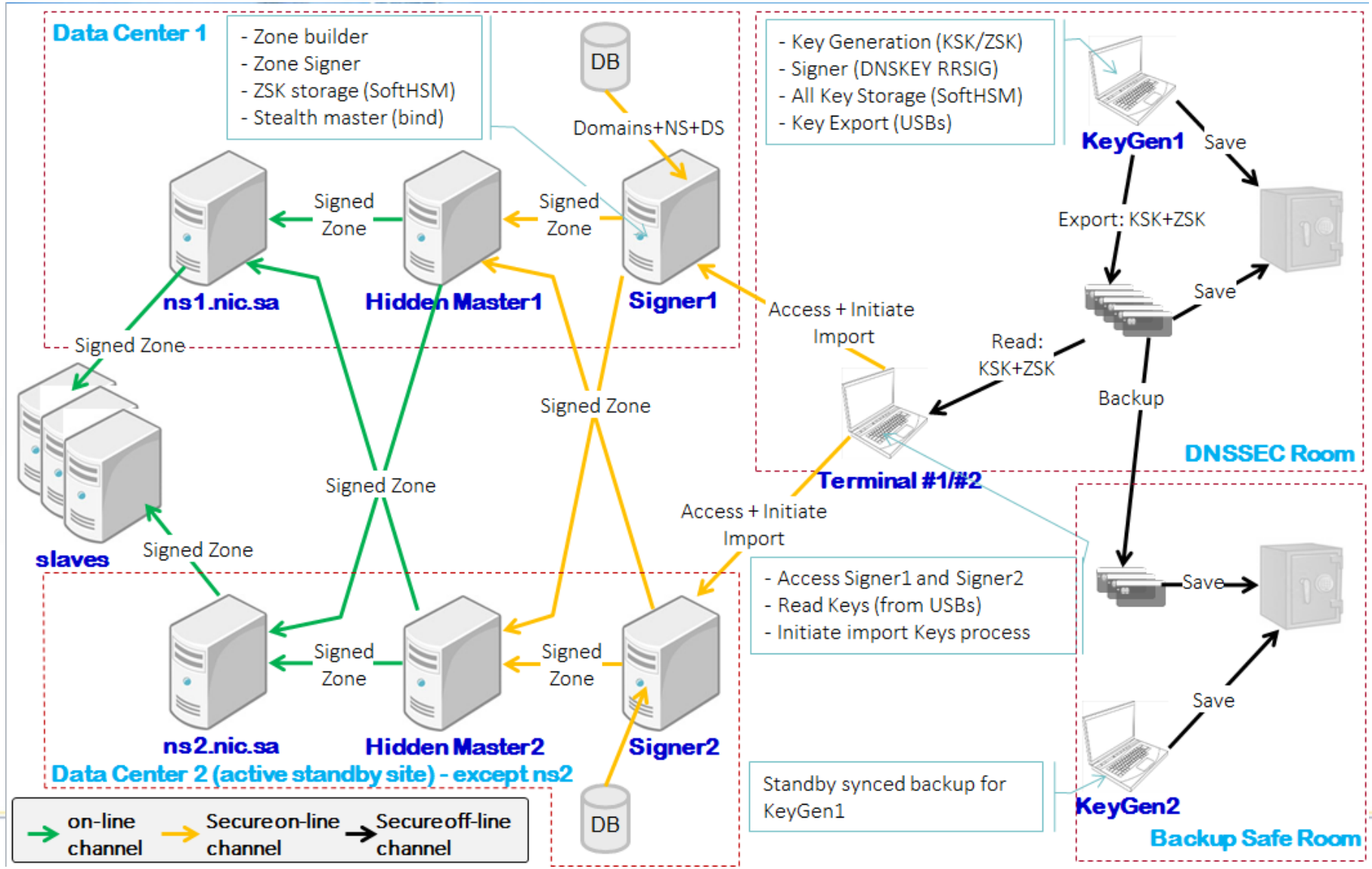
الامتداد الآمن لنظام أسماء النطاقات (DNSSEC) هو تطوير لنظام أسماء النطاقات الحالي (DNS) بحيث يوفر إمكانيات التحقق من صحة البيانات وأنها لم تُبدل ولم يعبث بها أثناء انتقالها خلال شبكة الإنترنت وأنها آتية من مصدرها الصحيح. ويتحقق ذلك من خلال تبني المفاتيح العامة للتشفير ضمن هيكلية خدمة أسماء النطاقات لتشكيل سلسلة موثوقة نابعة من منطقة الجذر (root zone).

1.2 التعريف واسم الوثيقة

عنوان الوثيقة: ممارسات المركز السعودي لمعلومات الشبكة (SaudiNIC) لتطبيق الامتداد الآمن لنظام أسماء النطاقات (DNSSEC)

SaudiNIC DNSSEC Setup

إعداد التصاميم وطريقة العمل



SaudiNIC DNSSEC Procedures

وثيقة إجراءات الامتداد الآمن

- إجراءات مراسيم إنشاء المفاتيح
- DNSSEC Keys Generation Ceremony
- إجراءات تركيب وتفعيل المفاتيح
- DNSSEC Keys Installation Procedure
- الإجراءات الطارئة لتركيب وتفعيل المفاتيح
- DNSSEC Emergency Keys Installation Procedure
- إجراءات تهيئة خزنة جديدة
- DNSSEC New Safe Arrangement Procedure
- إجراءات نقل مواد من خزنة
- DNSSEC Safe Content Transfer Procedure

Prototype

فترة التجربة

- SaudiNIC has successfully signed of the IDN ccTLD (السعودية.) - June – 2016
  - 1st GCC country to enable DNSSEC

- قام المركز – وبنجاح - بالتوقيع التجريبي للنطاق العربي (.السعودية) - رمضان-١٤٣٧هـ (يونيو-٢٠١٦م)
  - أول دولة خليجية تفعل الامتداد الآمن

- Operators have been invited to participate in the trial of signing their domain names for the purpose of gaining experience and learning how to deal with DNSSEC.

- تم دعوة المشغلين للمشاركة في تجريب توقيع أسماء نطاقاتهم لغرض كسب الخبرة والتعرف على كيفية التعامل مع الامتداد الآمن.

Official launch

التشغيل الفعلي

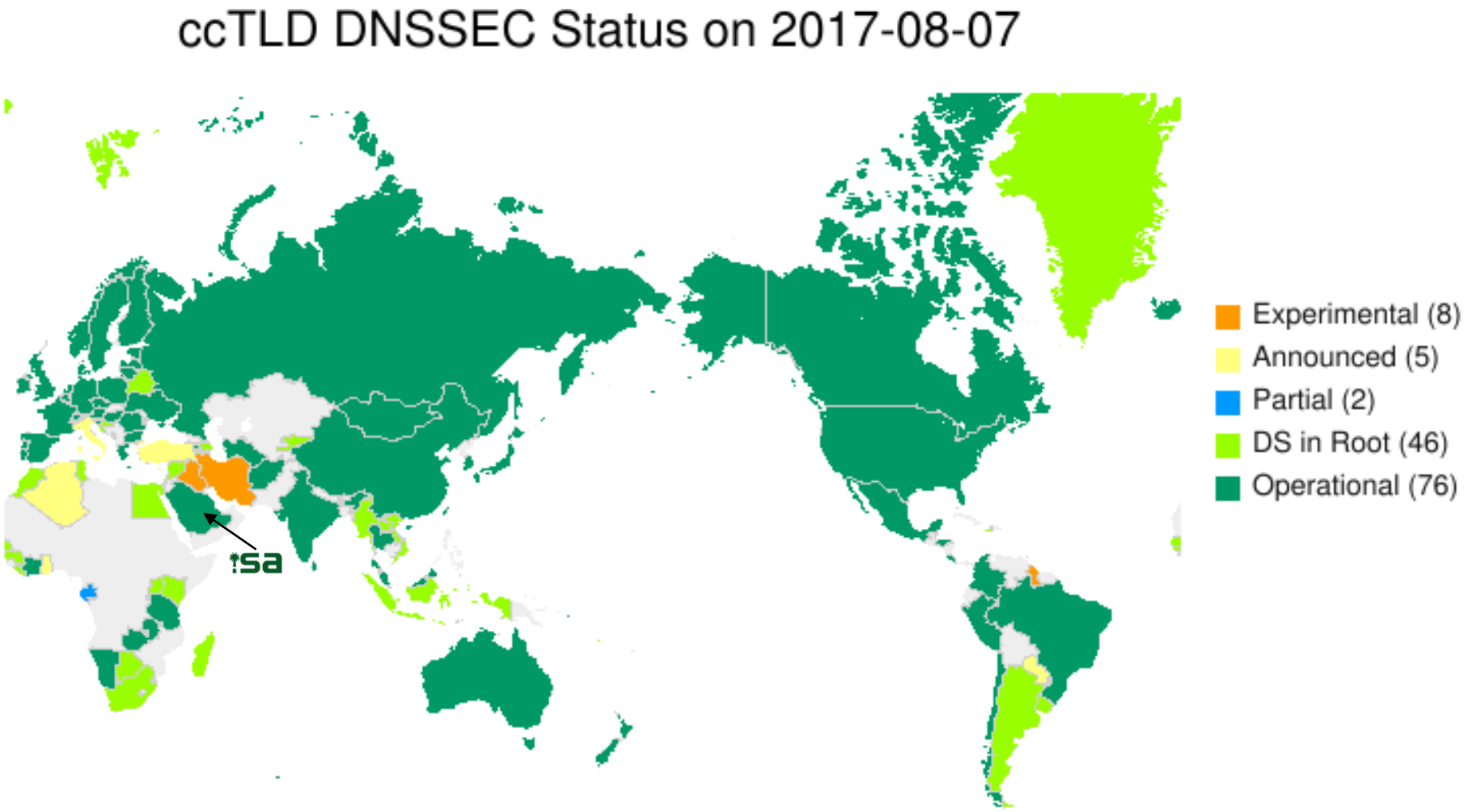
- SaudiNIC has successfully signed all the Saudi TLDs – 22 June 2017
  - 1st MENA country to open the service to all customers
- Conducting key-generation ceremony
- Signing ccTLDs (.sa) and (.السعودية)
- Publishing the public key with IANA
- Updating registration systems in preparation for the provision of DNSSEC services.
- Awareness and promotion
- Website (Arabic & English):
  - www.dnssec.sa

- قام المركز – وبنجاح - بالتوقيع الفعلي لجميع النطاقات السعودية - رمضان-١٤٣٨هـ (٢٢يونيو ٢٠١٧م)
  - أول دولة في المنطقة تتيح الخدمة لجميع العملاء
- عقد مراسيم إنشاء المفاتيح
- التوقيع الفعلي لكل من (.sa) و (.السعودية).
- التنسيق مع أيانا لإضافة ونشر مفاتيح التشفير العامة
- تطوير أنظمة التسجيل استعدادا لتقديم الخدمات الخاصة بالامتداد الآمن للعملاء
- تطوير أداة تساعد العملاء
- التوعية و تشجيع الاستخدام
- موقع متخصص (عربي، انجليزي):
  - www.dnssec.sa

Official launch

.sa

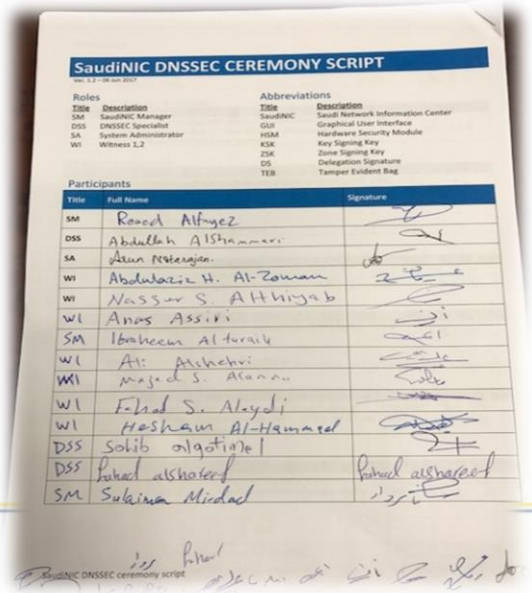
التشغيل الفعلي



Source: ISOC DNSSEC deployment map
https://elists.isoc.org/pipermail/dnssec-maps/attachments/20170807/462edb42/attachment-0012.png

Key Generation Ceremony

مراسيم إنشاء المفاتيح



SaudiNIC DNSSEC CEREMONY SCRIPT

Roles

Title	Description
SM	SaudiNIC Manager
DSS	DNSSEC Specialist
SA	System Administrator
WI	Witness 1,2

Abbreviations

Title	Description
SaudiNIC	Saudi Network Information Center
GUI	Graphical User Interface
HSM	Hardware Security Module
KSK	Key Signing Key
ZSK	Zone Signing Key
DS	Delegation Signature
TEB	Tamper Evident Bag

Participants

Title	Full Name	Signature
SM	Raeed Alfayez	
DSS	Abdullah Alshammari	
SA	Arun Natarajan	
WI	Abdulaziz H. Al-Zaman	
WI	Nassar S. Alhijab	
WI	Anas Assiri	
SM	Ibraheem Alturaiki	
WI	Ali Alshehri	
WI	Majed S. Alanazi	
WI	Faisal S. Alsaidi	
WI	Hesham Al-Hamaad	
DSS	Sohib algotiano	
DSS	Fahad alshateef	Fahad alshateef
SM	Sukirno Mardad	

SaudiNIC DNSSEC ceremony script

Website

موقع

English

المركز السعودي لمعلومات الشبكة
Saudi Network Information Center

الرئيسية | لوائح و قواعد | أدلة الخدمات | الأسئلة الشائعة | أدوات

النطاقات العربية .السعودية

حول الامتداد الآمن لنظام أسماء النطاقات...

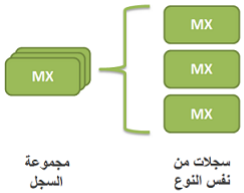
حول الامتداد الآمن لنظام أسماء النطاقات

- ورشة العمل التعريفية حول الامتداد الآمن لنظام أسماء النطاقات (DNSSEC) ومجال تطبيقه
- ماهو الامتداد الآمن؟
- ما هي أهم فوائد الامتداد الآمن؟
- كيف يعمل الامتداد الآمن؟
- كيف يتم تفعيل الامتداد الآمن؟
- منهجية المركز لتبني الامتداد الآمن (DNSSEC)
- التسجيل وإدارة خدمة الامتداد الآمن لنطاق سعودي مسجل لدى المركز
- المعايير الدولية
- مراجع للاستزادة حول الموضوع

ماهو الامتداد الآمن؟

نظام أسماء النطاقات (Domain Name System- DNS) عبارة عن قاعدة بيانات موزعة هرميا على ش
الرقمية (IP addresses) لكل نطاق بحيث يتم تقسيم هذه البيانات إلى أجزاء تدار محليا والوصول إلي
ويستخدم نظام أسماء النطاقات نموذج الخادم والعميل (client server model) حيث يحتفظ كل خادم
قاعدة البيانات ويوفرها للعميل (resolver). لذا فالمهمة الأساسية لنظام أسماء النطاقات هي ترجمة
والعكس. وهذا بدوره مكن من استبدال العناوين الرقمية صعبة التذكر (مثل 86.111.195.4) بأسماء نطا
شبكة الإنترنت من قبل البشر.

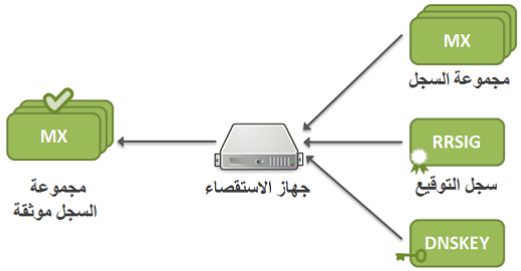
يعتبر نظام أسماء النطاقات من الخدمات الحرجة للبنية التحتية للإنترنت، ومع ذلك، فإنه كان لا يشمل
عرضة لعدد من الهجمات مثل: هجمات الخداع والتصيد، وهجمات "رجل في المنتصف"، أو حتى هجمات



2. توقيع ملف النطاق باستخدام مفتاح التوقيع (ZSK)

يستخدم الامتداد الآمن مفتاح توقيع ملف النطاق (ZSK) بكلا شقيه: الخاص والعمومي، بحيث يستخدم الجزء الخاص للتوقيع رقميا على كل مجموعة سجل (RRset) ضمن ملف النطاق على حدة ومن ثم نشر نتيجة التوقيع في سجل التوقيع (RRSIG) في نفس ملف النطاق. أما الجزء العمومي من مفتاح التوقيع (ZSK) فيتم نشره في ملف النطاق باستخدام سجل المفاتيح (DNSKEY)، حيث أنه سيستخدم في وقت لاحق من قبل أجهزة الاستقصاء (resolvers) للتحقق من صحة التوقيع.

وحالما يرسل جهاز الاستقصاء (resolver) طلب الاستعلام حول سجل ما (على سبيل المثال، MX)، فإن جهاز الخادم المستجيب يرد بالمعلومات حول السجل المطلوب مقترنة بسجل التوقيع (RRSIG) المقابل لذلك السجل. بعد ذلك، يطلب جهاز الاستقصاء من الجهاز المستجيب سجل المفاتيح (DNSKEY) والذي يحتوي على الجزء العمومي من المفتاح (ZSK). و إجمالا، يمكن القول أن مجموعة السجل (RRset) و سجل التوقيع (RRSIG) والجزء العمومي من (ZSK) يلعبون دورا مهما في التحقق من صحة الرد.



www.dnssec.sa

Tools

أدوات

DS Record Verifier

This tool is used to validate a DS Record and match it with either the DNSKEY that exists on the name server or by the manually provided DNSKEY.

Domain Information

Domain Name *

Captcha *

DNSKEY Record Information

Validate the DNSKEY from the server

Flags * Often is 256 or 257.

Protocol * Must be equal to 3.

Public key *

DS Record Information

Key Tag *

Key algorithm *

Digest Type *

Digest *

Verify

Tools

أدوات

DS Record Generator

This tool is used to generate a DS record for a given domain name and it`s DNSKEY. It has the ability to fetch the DNSKEY information from the name server.

Domain Information

Domain Name *

4 6

Captcha *

DNSKEY Record Information

Auto fill

Flags *

Protocol *

Key algorithm *

Public key *

DS Record Information

Generate DS record

Statistics

احصاءات

- Number of registered domains
  - 50,813 domain
- Number of DNSSEC enabled domains
  - 55 domain
    - .sa: 33
    - .السعودية: 8
    - .com.sa: 6
    - .net.sa:6
    - .org.sa: 1
    - .gov.sa:1

- عدد النطاقات المسجلة
  - ٥٠٬٨١٣ نطاق
- عدد النطاقات المفعلة
  - ٥٥ نطاق

Next Steps

الخطوات التالية

- Awareness and promotion.
- Monitor new enhancement to the DNSSEC protocols
- Keep an eye on the Keys rollovers

- استمرار التوعية و تشجيع الاستخدام.
- متابعة المستجدات في ما له علاقة بالامتداد الأمن
- متابعة تغيير المفاتيح التأكد من صحتها

Lesson learned

الدروس المستفادة

- Build local expertise
- Launch a test lab:
  - Testing systems
  - Testing configuration parameters (key roll over, signing, different scenarios, ...)
- Develop monitoring and testing tools for DNSSEC system , zone files, and validating signed zones before publishing them
- Automation for most/some of the key generation ceremony procedures
- Providing customer support with the help of tools to validate the correctness of key and signed zones.
  - Users may get confused

- بناء خبرة محلية حول الامتداد
- انشاء معمل اختبار
  - اختبار الأنظمة والتطبيقات
  - اختبار مفاهيم الامتداد (تغيير المفاتيح، طريقة التوقيع، اعدادات الامتداد، اختبار السناريوهات)
- تطوير أنظمة مراقبة وفحص دوري للنظام والملف الرئيسي وصحة التواقيع قبل النشر وبعده
- أتمته عمل مراسم إنشاء المفاتيح
- تقديم الدعم والمساعدة للعملاء مع توفير الأدوات للتحقق من صحة المفاتيح وصحة التوقيع
  - الخطأ وارد من العميل

Thank you

شكرًا

للمزيد من المعلومات يمكنكم زيارة:

For more information you can visit:

المركز السعودي لمعلومات الشبكة
Saudi Network Information Center

سجل.السعودية

www.nic.sa

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

هيئة-الاتصالات.السعودية

www.citc.gov.sa